Dauphine | PSL
UNIVERSITÉ PARIS

Algèbre linéaire 3

Guillaume Legendre

(version du 4 juin 2025)

Au regretté logo de l’université (2009-2019)

Table des matières

Dans tout ce document, on désigne par $\mathbb{K}$ un corps qui peut être $\mathbb{R}$, le corps de nombres réels, ou $\mathbb{C}$, le corps des nombres complexes.

Chapitre 1

Réduction des endomorphismes

Réduire un endomorphisme dans un espace vectoriel de dimension finie, c'est notamment trouver une base de l'espace dans laquelle cet endomorphisme est « aisément » étudiable et manipulable. En pratique, ceci revient à déterminer une base dans laquelle la matrice représentative de l'endomorphisme possède une forme particulièrement simple, c'est-à-dire *diagonale* (dans le meilleur des cas) ou *triangulaire*. On dira ainsi d'une matrice carrée qu'elle peut être réduite si elle est *semblable* à une matrice diagonale ou triangulaire. La réduction des endomorphismes (et des matrices qui leur sont associées) constitue un outil incontournable de l'étude de ces derniers.

1.1 Sous-espaces stables par un endomorphisme

La réduction d'un endomorphisme repose sur une propriété de *stabilité* de certains sous-espaces vectoriels sous l'action de cet endomorphisme, notion que l'on va maintenant introduire.

Définition 1.1 (sous-espace vectoriel stable par un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E et A un sous-espace vectoriel de E. On dit que A est **stable** (ou **invariant**) par u si et seulement si l'image de A par u est incluse dans A, c'est-à-dire*

$$\forall x \in E,\ x \in A \implies u(x) \in A.$$

Exemple 1.2 (sous-espaces stables triviaux) *L'ensemble réduit au vecteur nul et l'espace tout entier sont des sous-espaces stables par tout endomorphisme. De la même manière, le noyau* $\ker(u)$ *et l'image* $\mathrm{Im}(u)$ *d'un endomorphisme u sont stables par u.*

La définition ci-dessous fournit un exemple de classe de sous-espaces stables qui apparaîtra à plusieurs reprises dans la suite de ce chapitre.

Définition 1.3 (sous-espace cyclique) *Soit E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E et x un vecteur de E. On appelle **sous-espace cyclique de** u **engendré par** x, et on note $E_u(x)$, le plus petit sous-espace vectoriel de E stable par u et contenant x, engendré par la famille $\left\{u^k(x)\right\}_{k\in\mathbb{N}}$ où, pour tout entier naturel non nul k, on a posé $u^k = \underbrace{u \circ \cdots \circ u}_{k \text{ occurences}}$ (on a par convention $u^0 = id_E$).*

Le résultat suivant est immédiat.

Proposition et définition 1.4 *Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E. Si A est un sous-espace vectoriel stable par u, alors la restriction de u à A, notée $u_{|_A}$, définit un endomorphisme de A, appelé **endomorphisme induit par** u **sur** A.*

Une situation importante impliquant des sous-espaces vectoriels stables est celle dans laquelle on considère deux endomorphismes commutant entre eux.

Proposition 1.5 *Soit E un $\mathbb{K}$-espace vectoriel et u et v deux endomorphismes de E qui commutent entre eux, i.e. $u \circ v = v \circ u$. L'endomorphisme v laisse stable l'image de u, le noyau de u, et plus généralement tout sous-espace* $\ker(u - \lambda\, id_E)$*, avec λ un scalaire.*

DÉMONSTRATION. Puisque les endomorphismes u et v commutent entre eux, on a, pour tout vecteur x de E,

$$v(u(x)) = u(v(x)),$$

le dernier vecteur appartenant à l'image de u. On en déduit donc que $v(\mathrm{Im}\,(u))$ est inclus dans $\mathrm{Im}\,(u)$, qui est alors stable par v.

On considère à présent un vecteur x du noyau de u. On a $u(v(x)) = v(u(x)) = v(0_E) = 0_E$, d'où $v(\ker(u))$ est inclus dans $\ker(u)$, qui est alors stable par v.

Soit enfin un scalaire λ. On a

$$v \circ (u - \lambda\, id_E) = v \circ u - \lambda\, v = u \circ v - \lambda\, v = (u - \lambda\, id_E) \circ v,$$

et les endomorphismes $u - \lambda\, id_E$ et v commutent donc aussi entre eux, ce qui permet de conclure. □

En dimension finie, il est possible d'interpréter matriciellement la propriété de stabilité d'un sous-espace vectoriel par un endomorphisme. Pour le voir, on considère un $\mathbb{K}$-espace vectoriel E de dimension finie égale à n, u un endomorphisme de E, A un sous-espace vectoriel de E stable par u, de dimension égale à m. Soit B un sous-espace vectoriel de E supplémentaire de A, c'est-à-dire tel que $E = A \oplus B$, et $\mathscr{B}$ une base *adaptée* [1] à une telle décomposition. Dans ce cas, on peut montrer que la matrice représentative de l'endomorphisme u dans la base $\mathscr{B}$ est triangulaire supérieure par blocs,

$$\begin{pmatrix} M_{11} & M_{12} \\ 0_{n-m,m} & M_{22} \end{pmatrix},$$

où M_{11} est une matrice de $M_m(\mathbb{K})$, M_{12} est une matrice de $M_{m,n-m}(\mathbb{K})$ et M_{22} est une matrice de $M_{n-m}(\mathbb{K})$. Si l'on suppose de plus que le sous-espace B est stable par u, alors la matrice de l'endomorphisme dans la base adaptée $\mathscr{B}$ est diagonale par blocs,

$$\begin{pmatrix} M_{11} & 0_{m,n-m} \\ 0_{n-m,m} & M_{22} \end{pmatrix}.$$

Plus généralement, si on a décomposé E en une somme directe de sous-espaces stables par u, $E = \oplus_{i=1}^{p} A_i$ avec $u(A_i) \subset A_i$ pour tout entier i appartenant à $\{1, \ldots, p\}$, et si $\mathscr{B}$ est une base de E adaptée à cette décomposition, alors la matrice de l'endomorphisme dans la base $\mathscr{B}$ sera de la forme

$$\begin{pmatrix} M_{11} & 0 & \ldots & 0 \\ 0 & M_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & M_{pp} \end{pmatrix}.$$

1.2 Éléments propres d'un endomorphisme

Définitions 1.6 (éléments propres d'un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E. Un scalaire λ est une **valeur propre** de u si et seulement s'il existe un vecteur non nul x de E tel que $u(x) = \lambda x$. Un vecteur non nul x de E tel qu'il existe un scalaire λ vérifiant $u(x) = \lambda x$ est un **vecteur propre** de u associé à la valeur propre λ.*

Il est important de remarquer qu'un vecteur propre est associé à une *unique* valeur propre, mais qu'une valeur propre possède une infinité de vecteurs propres, tout multiple non nul d'un vecteur propre donné étant, par linéarité, lui-même un vecteur propre associé à la même valeur propre.

On notera également que la définition précédente est donnée pour un espace vectoriel de dimension quelconque. En considérant des espaces de dimension finie non nulle, il est possible de l'étendre à une matrice carrée en posant que les éléments propres de la matrice sont ceux de l'unique endomorphisme qui lui est *canoniquement associé* (voir la définition A.128). Ainsi, pour une matrice M d'ordre n, le scalaire λ est une valeur propre de M s'il existe une matrice colonne X non nulle de $M_{n,1}(\mathbb{K})$ telle que

$$MX = \lambda X.$$

1. Cette adaptation s'entend dans le sens où les m premiers vecteurs composant la base forment une base du sous-espace A et les $n-m$ suivants forment une base du sous-espace B.

De même, une matrice colonne X de $M_{n,1}(\mathbb{K})$ sera un vecteur propre de la matrice M si elle est non nulle et qu'il existe un scalaire λ tel que $MX = \lambda X$.

Tous les résultats énoncés pour des endomorphismes dans un espace vectoriel de dimension finie seront par conséquent valables *mutatis mutandis* pour des matrices carrées.

Définition 1.7 (spectre d'un endomorphisme) *L'ensemble des valeurs propres d'un endomorphisme u d'un $\mathbb{K}$-espace vectoriel s'appelle le* ***spectre*** *de u et se note* $\mathrm{Sp}(u)$. *C'est un sous-ensemble, éventuellement vide, de $\mathbb{K}$.*

Si cette dernière définition s'étend naturellement à toute matrice carrée M, la notation $\mathrm{Sp}(M)$ peut s'avérer ambigüe lorsque les coefficients de M sont des réels. En effet, suivant que l'on conçoit M comme une matrice à coefficients complexes ou réels, on cherchera ses valeurs dans $\mathbb{C}$ ou dans $\mathbb{R}$. Dans ce cas, on a recours aux notations $\mathrm{Sp}_{\mathbb{C}}(M)$ ou $\mathrm{Sp}_{\mathbb{R}}(M)$, qui sont plus explicites.

Proposition et définition 1.8 (sous-espace propre) *Soit E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E et λ un scalaire. Les assertions suivantes sont équivalentes.*

(i) Le scalaire λ est une valeur propre de u.

(ii) L'endomorphisme $u - \lambda\, id_E$ n'est pas injectif.

(iii) Le noyau $\ker(u - \lambda\, id_E)$ n'est pas réduit à $\{0_E\}$.

Dans ce cas, le sous-espace vectoriel $E_\lambda = \ker(u - \lambda\, id_E)$ est appelé ***sous-espace propre*** *de u associé à la valeur propre λ. Il est stable par u.*

DÉMONSTRATION. Si λ est une valeur propre de l'endomorphisme u, alors, par définition, il existe un vecteur x non nul tel que $u(x) = \lambda x$. Il existe par conséquent un vecteur x non nul tel que $(u - \lambda\, id_E)(x) = 0_E$, ce qui signifie encore que l'endomorphisme $u - \lambda\, id_E$ n'est pas injectif, ce qui signifie encore que le noyau de cet endomorphisme n'est pas réduit au vecteur nul.

Enfin, par linéarité de u, on a

$$\forall x \in E_\lambda,\ u(u(x)) = u(\lambda x) = \lambda\, u(x).$$

Le vecteur $u(x)$ appartient à E_λ, qui est donc stable par u. □

Lorsque l'espace E est de dimension finie, on déduit de ce résultat et du théorème du rang l'équivalence

$$\lambda \in \mathrm{Sp}(u) \iff u - \lambda\, id_E \notin GL(E).$$

Une autre observation importante à faire est qu'un endomorphisme n'est pas injectif si et seulement si 0 est l'une de ses valeurs propres.

Remarque 1.9 *Un sous-espace propre E_λ de u étant stable par u, la restriction de u à E_λ induit un endomorphisme sur E_λ (voir la proposition 1.4), qui est une* homothétie de rapport λ.

On énonce enfin une propriété des sous-espaces propres fondamentale pour la réduction.

Proposition 1.10 *Soit E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E. Soit k un entier naturel non nul et $\lambda_1, \ldots, \lambda_k$ des valeurs propres de u deux à deux distinctes. Alors, les sous-espaces propres E_{λ_i}, $i = 1, \ldots, k$, sont en somme directe.*

DÉMONSTRATION. On raisonne par récurrence sur l'entier k. Pour $k = 1$, il n'y a rien à montrer. Pour k un entier naturel non nul, on suppose que si $\lambda_1, \ldots, \lambda_k$ sont des valeurs propres de u deux à deux distinctes et $x_1, \ldots, x_k$ sont des éléments des sous-espaces propres qui leur sont respectivement associés, alors l'égalité $x_1 + \cdots + x_k = 0_E$ implique que $x_1 = \cdots = x_k = 0_E$. Soit alors λ_{k+1} une valeur propre de u distincte des précédentes et x_{k+1} un vecteur propre associé. Dans ce cas, on suppose que $x_1 + \cdots + x_{k+1} = 0_E$, ce qui équivaut à $x_{k+1} = -(x_1 + \cdots + x_k)$, d'où $u(x_{k+1}) = -u(x_1) - \cdots - u(x_k)$, par linéarité de u. On a par conséquent $\lambda_{k+1} x_{k+1} = -\lambda_1 x_1 - \cdots - \lambda_k x_k$, soit encore $0_E = (\lambda_{k+1} - \lambda_1) x_1 + \cdots + (\lambda_{k+1} - \lambda_k) x_k$. L'hypothèse de récurrence conduit alors à $(\lambda_{k+1} - \lambda_i) x_i = 0_E$ pour tout entier i dans $\{1, \ldots, k\}$ et, puisque $\lambda_{k+1} - \lambda_i \neq 0$ pour tout entier i dans $\{1, \ldots, k\}$, on en déduit que $x_i = 0_E$ pour tout entier i dans $\{1, \ldots, k\}$, d'où $x_{k+1} = 0_E$. □

Corollaire 1.11 *Soit n un entier naturel non nul, E un $\mathbb{K}$-espace vectoriel de dimension égale à n et u un endomorphisme de E. Alors, l'endomorphisme u possède au plus n valeurs propres distinctes.*

On conclut cette section avec plusieurs exemples remarquables.

Exemple 1.12 (spectres et sous-espaces propres de l'identité, d'une projection vectorielle et d'une symétrie vectorielle) *Il est clair que le spectre de id_E est $\{1\}$ et que le sous-espace propre associé est E. Étant donné un sous-espace vectoriel A, strict et non réduit à $\{0_E\}$, de E et B un supplémentaire de A, on rappelle que la* ***projection de E sur A parallèlement à B*** *est définie comme l'endomorphisme p de E tel que*

$$\forall x \in E,\ p(x) = x_A,$$

où $x = x_A + x_B$ est l'unique décomposition du vecteur x comme somme d'un vecteur x_A de A et d'un vecteur x_B de B. On a $\mathrm{Sp}(p) = \{0,1\}$, $E_0 = B$ et $E_1 = A$. Enfin, on rappelle que la ***symétrie par rapport à A parallèlement à B*** *est définie comme l'endomorphisme s de E tel que*

$$\forall x \in E,\ s(x) = x_A - x_B.$$

On a dans ce cas $\mathrm{Sp}(s) = \{-1,1\}$, $E_{-1} = B$ et $E_1 = A$.

Exemple 1.13 (spectre d'une rotation dans le plan) *On considère une rotation du plan centrée en l'origine et d'angle de rotation orienté de mesure θ, différent de 0 (qui correspond à l'identité) ou de π (qui correspond à la symétrie centrale) modulo 2π. Celle-ci peut naturellement être représentée par un endomorphisme de $\mathbb{R}^2$ dont la matrice représentative dans la base canonique est*[2]

$$M = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

La détermination des éléments propres de cette matrice passe par celle d'un sous-espace propre de l'endomorphisme. Matriciellement, cela revient à trouver les matrices colonnes non nulles X et les réels λ satisfaisant l'égalité $MX = \lambda X$. Le déterminant du système linéaire homogène dont les coordonnées de X sont solution est égal à $(\cos(\theta)-\lambda)^2+(\sin(\theta))^2 = \lambda^2 - 2\lambda\cos(\theta) + 1$ et doit être nul pour que le système admette une solution non triviale. Le discriminant de l'équation du second degré associé étant égal à $4((\cos(\theta))^2 - 1) = -4(\sin(\theta))^2$, il n'existe pas de réel λ valeur propre de M et le spectre de l'endomorphisme est donc égal l'ensemble vide. En posant le problème dans le plan complexe, c'est-à-dire en considérant les valeurs propres complexes d'un endomorphisme de $\mathbb{C}$ (vu comme un $\mathbb{C}$-espace vectoriel), on trouve que le spectre est formé des valeurs propres $e^{\pm i\theta}$. Cet exemple met en lumière l'importance du corps considéré dans la détermination du spectre d'un endomorphisme.

Exemple 1.14 (spectre d'un endomorphisme nilpotent) *On rappelle qu'un endomorphisme u d'un $\mathbb{K}$-espace vectoriel E est dit* ***nilpotent*** *s'il existe un entier naturel non nul k tel que $u^k = 0_{\mathscr{L}(E)}$. Le plus petit entier vérifiant cette propriété est alors appelé l'****indice de nilpotence*** *de u. Le spectre d'un tel endomorphisme est réduit à $\{0\}$.*
En effet, si $\mathrm{Sp}(u)$ ne contenait pas 0, alors $\ker(u)$ serait réduit à $\{0_E\}$. Soit x un vecteur de E et l l'indice de nilpotence de u. On a $u^l(x) = u(u^{l-1}(x)) = 0_E$, d'où $u^{l-1}(x) = 0_E$. En raisonnant par récurrence, on montre que $x = 0_E$, ce qui est absurde. Ainsi, on a $\{0\} \subset \mathrm{Sp}(u)$. Soit à présent λ une valeur propre de u et x un vecteur propre associé. On montre facilement que $u^k(x) = \lambda^k x$ pour toute entier naturel k et, en particulier, $u^l(x) = \lambda^l x = 0_E$, d'où $\lambda = 0$.

Exemple 1.15 (deux exemples « pathologiques » en dimension infinie) *On considère tout d'abord l'espace vectoriel réel $E = \mathscr{C}^\infty(\mathbb{R},\mathbb{R})$ des fonctions réelles d'une variable réelle indéfiniment dérivables et l'endomorphisme u de E qui associe à toute fonction f de E sa fonction dérivée f'. Alors, tout nombre réel λ est une valeur propre de u avec pour vecteur propre associée la fonction $x \mapsto e^{\lambda x}$. On a $\mathrm{Sp}(u) = \mathbb{R}$.*

On choisit ensuite $E = \mathbb{K}[X]$ et l'endomorphisme u de E qui associe à tout polynôme P de E le polynôme résultant de son produit avec le polynôme X. Écrire que $u(P) = \lambda P$ revient à écrire que $(X-\lambda)P = 0_E$. Comme $X - \lambda$ n'est pas le polynôme nul, il en résulte que $P = 0_E$. On a alors $\mathrm{Sp}(u) = \varnothing$.

1.3 Polynôme caractéristique

On a vu qu'un scalaire λ est une valeur propre d'un endomorphisme u d'un espace vectoriel E si et seulement si l'endomorphisme $u - \lambda\, id_E$ n'est pas injectif. Si l'espace E est de dimension finie, ceci équivaut encore à dire que le déterminant de $u - \lambda\, id_E$ est nul. Trouver les valeurs propres d'un endomorphisme en dimension finie revient donc à résoudre une équation polynomiale.

2. On renvoie au théorème 5.17 pour plus de détails.

Définition 1.16 (polynôme caractéristique) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. On appelle* ***polynôme caractéristique*** *de u le polynôme χ_u de $\mathbb{K}[X]$ défini par $\chi_u(X) = \det(X\,id_E - u)$.*

Remarque 1.17 *On trouve parfois la définition $\chi_u(X) = \det(u - X\,id_E)$, qui a comme défaut le fait que le polynôme ainsi défini n'est pas nécessairement* ***unitaire***[3]*, le coefficient du terme de plus haut degré étant égal à -1 élevé à une puissance égale à la dimension de l'espace. On renvoie à la proposition 1.22 pour plus de détails.*

Pour une matrice M d'ordre n, on a $\chi_M(X) = \det(X\,I_n - M)$.

Exemple 1.18 (polynôme caractéristique d'une matrice de rotation dans le plan) *En cherchant à déterminer le spectre de la matrice d'une rotation vectorielle de $\mathbb{R}$ d'angle θ dans l'exemple 1.13, on a vu que le polynôme caractéristique de cette matrice était donné par $\chi_M(X) = X^2 - 2\cos(\theta)X + 1$ et observé qu'il ne possédait pas de racine réelle lorsque θ était différent de 0 ou de π modulo 2π.*

Le résultat de caractérisation qui suit s'avère fondamental.

Théorème 1.19 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. Un scalaire λ est une valeur propre de u si et seulement si $\chi_u(\lambda) = 0$.*

DÉMONSTRATION. Il suffit d'utiliser la proposition 1.8 et la définition 1.16 : le scalaire λ est une valeur propre de u si et seulement si l'endomorphisme $u - \lambda\,id_E$ n'est pas injectif, c'est-à-dire si et seulement si $\det(u - \lambda\,id_E) = 0$. □

Exemple 1.20 (valeurs propres d'une matrice triangulaire) *Il découle de la définition 1.16, du dernier théorème et du fait que le déterminant d'une matrice triangulaire est le produit de ses coefficients diagonaux que les valeurs propres d'une matrice triangulaire sont ses coefficients diagonaux.*

Définition 1.21 (ordre de multiplicité algébrique d'une valeur propre) *On appelle* ***ordre de multiplicité algébrique*** *d'une valeur propre son ordre de multiplicité en tant que racine du polynôme caractéristique.*

Il découle des dernières définitions que deux matrices ayant le même polynôme caractéristique ont les mêmes valeurs propres, avec les mêmes ordres de multiplicité algébrique.

Proposition 1.22 (degré et coefficients du polynôme caractéristique d'une matrice) *Soit M une matrice d'ordre n à coefficients dans le corps $\mathbb{K}$. Le polynôme caractéristique de M est de degré égal à n et l'on a*

$$\chi_M(X) = X^n - \mathrm{tr}(M)X^{n-1} + \cdots + (-1)^n \det(M).$$

DÉMONSTRATION. Par la formule de Leibniz pour le déterminant (voir la définition A.118), on a

$$\chi_M(X) = \det(X\,I_n - M) = \sum_{\sigma\in\Sigma_n} \varepsilon(\sigma) \prod_{i=1}^{n} (X\,I_n - M)_{\sigma(i)\,i}.$$

Chacun des $n!$ termes de cette somme est le produit de n termes polynomiaux en X de degré inférieur ou égal à un. Le degré de χ_M est donc inférieur ou égal à n. De plus, un des termes de la somme est exactement de degré n si et seulement si chacun des facteurs le composant est de degré exactement égal à un. Ceci équivaut au fait que $\sigma = id_{\{1,\ldots,n\}}$. Ainsi, la somme correspondant au polynôme caractéristique de M contient un unique terme de degré n et des termes de degré inférieur ou égal à $n-1$. C'est ainsi un polynôme de degré n, s'écrivant sous la forme

$$\begin{aligned}\chi_M(X) &= (X - m_{11})\ldots(X - m_{nn}) + \text{termes de degré inférieur ou égal à } n-1\\ &= X^n + \text{termes de degré inférieur ou égal à } n-1.\end{aligned}$$

C'est donc bien un polynôme unitaire. Le coefficient du terme de degré nul de χ_M est par ailleurs donné par sa valeur en 0, qui est $\det(-M) = (-1)^n \det(M)$.

Enfin, pour déterminer le coefficient du terme de degré $n-1$, on observe que, quand la permutation σ n'est pas égale à l'identité, il existe un entier i de $\{1,\ldots,n\}$ tel que $\sigma(i) \neq i$. En posant alors $j = \sigma^{-1}(i)$, on a que

3. Un polynôme *unitaire*, ou *monique*, est un polynôme non nul dont le coefficient du terme de plus haut degré est égal à 1.

$(X\,I_n - M)_{\sigma(i)\,i} = -m_{\sigma(i)\,i}$ et $(X\,I_n - M)_{\sigma(j)\,j} = -m_{\sigma(j)\,j}$, et le terme $\varepsilon(\sigma)\prod_{i=1}^{n}(X\,I_n - M)_{\sigma(i)\,i}$ correspondant à cette permutation est de degré inférieur ou égal à $n-2$. Il en découle que

$$\begin{aligned}\chi_M(X) &= (X-m_{11})\dots(X-m_{nn}) + \text{termes de degré inférieur ou égal à } n-2\\ &= X^n - (m_{11}+\dots+m_{nn})X^{n-1} + \text{termes de degré inférieur ou égal à } n-2\\ &= X^n - \operatorname{tr}(M)X^{n-1} + \text{termes de degré inférieur ou égal à } n-2.\end{aligned}$$

□

Exemple 1.23 (polynôme caractéristique d'une matrice d'ordre 2) *Dans le cas particulier d'une matrice M d'ordre 2, on a $\chi_M(X) = X^2 - \operatorname{tr}(M)X + \det(M)$.*

On retrouve avec ce dernier résultat le fait qu'une matrice M d'ordre n possède au plus n valeurs propres distinctes (voir le corollaire 1.11), puisque qu'un polynôme de degré n possède au plus n racines distinctes. Par ailleurs, si $\mathbb{K} = \mathbb{C}$, cette matrice admet exactement n valeurs propres comptées avec leurs ordres de multiplicité respectifs. Il en va de même si $\mathbb{K} = \mathbb{R}$ et si le polynôme caractéristique est *scindé*, c'est-à-dire décomposable en un produit de facteurs de degré un. Dans ces deux cas, on peut écrire

$$\chi_M(X) = (X-\lambda_1)\dots(X-\lambda_n)$$

où les scalaires $\lambda_1,\dots,\lambda_n$ sont les valeurs propres, distinctes ou confondues, de la matrice M, ou bien

$$\chi_M(X) = (X-\lambda_1)^{m_{\lambda_1}}\dots(X-\lambda_p)^{m_{\lambda_p}}$$

où l'entier naturel p est inférieur ou égal à n, les scalaires $\lambda_1,\dots,\lambda_p$ sont les valeurs propres, distinctes deux à deux, de M et les entiers naturels $m_{\lambda_1},\dots,m_{\lambda_p}$ sont leurs ordres de multiplicité respectifs.

Proposition 1.24 (propriétés du polynôme caractéristique d'une matrice) *Soit A et B deux matrices carrées de même ordre. On a*

$$\chi_{A^\top} = \chi_A \text{ et } \chi_{AB} = \chi_{BA}.$$

Par ailleurs, si A et B sont semblables alors $\chi_A = \chi_B$.

DÉMONSTRATION. Soit A et B deux matrices d'ordre n. Le déterminant d'une matrice étant égal à celui de sa transposée, on a

$$\chi_{A^\top}(X) = \det\left(X\,I_n - A^\top\right) = \det\left((X\,I_n - A)^\top\right) = \det(X\,I_n - A) = \chi_A(X).$$

Pour la seconde assertion, si l'une des matrices, A par exemple, est inversible, alors $A^{-1}(AB)A = BA$, d'où AB et BA sont semblables et l'on conclut en utilisant la troisième assertion. Dans le cas général, on considère les matrices de $M_{2n}(\mathbb{K})$, écrites par blocs,

$$M = \begin{pmatrix} BA & -B \\ 0 & 0 \end{pmatrix},\ N = \begin{pmatrix} 0 & -B \\ 0 & AB \end{pmatrix} \text{ et } P = \begin{pmatrix} I_n & 0 \\ A & I_n \end{pmatrix}.$$

On vérifie que $PN = MP = \left(\begin{smallmatrix} 0 & -B \\ 0 & 0 \end{smallmatrix}\right)$ et que P est une matrice triangulaire inférieure à diagonale non nulle, donc inversible. Les matrice M et N sont donc semblables et, par la troisième assertion, leurs polynômes caractéristiques sont égaux. Le calcul par blocs de leurs polynômes caractéristiques respectifs laisse alors apparaître que $\chi_M(X) = \chi_{BA}(X)X^n$ et $\chi_N(X) = X^n\,\chi_{AB}(X)$, d'où la conclusion.

Enfin, si A et B sont semblables, il existe une matrice inversible P telle que $B = P^{-1}AP$ et l'on a

$$X\,I_n - B = X\,I_n - P^{-1}AP = P^{-1}(X\,I_n - A)P,$$

d'où $X\,I_n - A$ et $X\,I_n - B$ sont semblables, ce qui implique qu'elles ont le même déterminant. □

On notera que deux matrices ayant le même polynôme caractérisitique ne sont pas nécessairement semblables, comme on peut le voir en considérant

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

En effet, ces deux matrices ne sont clairement pas semblables, mais elles ont toutes deux $(X-1)^2$ pour polynôme caractéristique. Cet exemple montre que la dernière assertion de la proposition ci-dessus peut être utilisée pour prouver que deux matrices *ne sont pas* semblables, mais pas le contraire.

Remarque 1.25 *Si m et n sont des entiers naturels non nuls, tels que m est inférieur ou égal à n, et que A et B sont respectivement des matrices de $M_{m,n}(\mathbb{K})$ et $M_{m,n}(\mathbb{K})$, on peut montrer que $\chi_{BA}(X) = X^{n-m}\chi_{AB}(X)$. En effet, un calcul révèle que*

$$\begin{pmatrix} I_m & -A \\ 0_{n,m} & I_n \end{pmatrix}\begin{pmatrix} AB & 0_{m,n} \\ B & 0_n \end{pmatrix}\begin{pmatrix} I_m & A \\ 0_{n,m} & I_n \end{pmatrix} = \begin{pmatrix} 0_m & 0_{m,n} \\ B & BA \end{pmatrix},$$

et les matrices $\left(\begin{smallmatrix} AB & 0_{m,n} \\ B & 0_n \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0_m & 0_{m,n} \\ B & BA \end{smallmatrix}\right)$ sont par conséquent semblables. Leurs polynômes caractéristiques respectifs, $\chi_{AB}(X)X^n$ et $X^m\chi_{BA}(X)$, sont donc égaux. Il en résulte que les valeurs propres de la matrice BA d'ordre n sont données par les valeurs propres de la matrice AB d'ordre m, auxquelles s'ajoute 0.

1.4 Diagonalisation

Dans cette section, on s'interesse au cas de réduction d'endomorphisme le plus favorable : la *diagonalisation*.

Proposition 1.26 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. Si λ est une valeur propre de u d'ordre de multiplicité algébrique m_λ, on a*

$$1 \leq \dim(E_\lambda) \leq m_\lambda.$$

DÉMONSTRATION. Soit $\{e_1, \ldots, e_{\dim(E_\lambda)}\}$ une base du sous-espace propre E_λ, que l'on complète, si nécessaire, en une base $\mathscr{B}$ de E. La matrice représentative M de u dans la base $\mathscr{B}$ s'écrit

$$M = \begin{pmatrix} \lambda I_{\dim(E_\lambda)} & M_{12} \\ 0 & M_{22} \end{pmatrix},$$

où la matrice M_{22} est d'ordre $n - \dim(E_\lambda)$, avec n la dimension de E. En utilisant cette écriture par blocs, on trouve que

$$\chi_u(X) = \det(X I_n - M) = \det\left(\begin{pmatrix} (X-\lambda) I_{\dim(E_\lambda)} & -M_{12} \\ 0 & X I_{n-\dim(E_\lambda)} - M_{22} \end{pmatrix}\right) = (X-\lambda)^{\dim(E_\lambda)}\chi_{M_{22}}(X).$$

Par conséquent, le polynôme $(X-\lambda)^{\dim(E_\lambda)}$ divise $\chi_u(X)$ et l'ordre de multiplicité de λ est donc supérieur ou égal à $\dim(E_\lambda)$. □

On notera en particulier que le sous-espace propre E_λ est de dimension égale à 1 si λ est racine simple du polynôme caractéristique.

Remarque 1.27 *On nomme parfois* ***ordre de multiplicité géométrique*** *de la valeur propre λ l'entier $\dim(E_\lambda)$, en contraste avec l'ordre de multiplicité algébrique.*

Définition 1.28 (endomorphisme diagonalisable) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. On dit que u est* ***diagonalisable*** *s'il existe une base de E formée de vecteurs propres de u.*

Il résulte de la définition précédente qu'une matrice carrée est diagonalisable si l'endomorphisme qui lui est canoniquement associé est diagonalisable.

Le résultat suivant donne une justification du vocabulaire employé.

Proposition 1.29 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. Les conditions suivantes sont équivalentes.*

(i) L'endomorphisme u est diagonalisable.

(ii) Il existe une base de E dans laquelle la matrice représentative de u est diagonale.

DÉMONSTRATION. On note n la dimension de E. Si $\mathscr{B} = \{e_1, \ldots, e_n\}$ est une base de E formée de vecteurs propres de u associés aux valeurs propres $\lambda_1, \ldots, \lambda_n$, comptées avec leurs ordres de multiplicité algébrique respectifs, la matrice représentative de u dans la base $\mathscr{B}$ est la matrice diagonale

$$\begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \lambda_n \end{pmatrix}.$$

Réciproquement, si $\mathscr{B} = (e_1, \ldots, e_n)$ est une base de E, dire que la matrice représentative de u dans la base $\mathscr{B}$ est la matrice diagonale

$$D = \begin{pmatrix} d_{11} & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_{nn} \end{pmatrix}$$

revient à dire que $u(e_1) = d_{11}\, e_1, \ldots, u(e_n) = d_{nn}\, e_n$. Les vecteurs de cette base sont donc des vecteurs propres de u, associés aux valeurs propres $d_{11}, \ldots, d_{nn}$, et l'endomorphisme est donc diagonalisable. □

Compte tenu de ce résultat, on a qu'une matrice M d'ordre n est diagonalisable si et seulement si elle est semblable à une matrice diagonale. En notant $\mathscr{V}$ une base de $M_{n,1}(K)$ formée de vecteurs propres associés aux valeurs propres $\lambda_1, \ldots, \lambda_n$ de M, $\mathscr{B}$ la base canonique de $M_{n,1}(K)$, P la matrice de passage de la base $\mathscr{B}$ à la base $\mathscr{V}$ et D la matrice diagonale telle que $d_{ii} = \lambda_i$, $i = 1, \ldots, n$, on a alors l'égalité

$$M = PDP^{-1}. \tag{1.1}$$

Cette factorisation porte le nom de **décomposition en éléments propres** de la matrice M, des vecteurs propres de M apparaissant dans la matrice P et les valeurs propres de M apparaissant dans la matrice D.

Exemple 1.30 *On a vu avec l'exemple 1.12 que, dans des cas non triviaux, les sous-espaces propres d'une projection vectorielle ou d'une symétrie vectorielle étaient supplémentaires. Il en résulte que ces endomorphismes sont diagonalisables.*

Théorème 1.31 (condition nécessaire et suffisante de diagonalisabilité) *Soit un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle. Cet endomorphisme est diagonalisable si et seulement si son polynôme caractéristique est scindé sur $\mathbb{K}$ et l'ordre de multiplicité algébrique de chaque valeur propre est égal à la dimension du sous-espace propre correspondant.*

DÉMONSTRATION. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle égale à n et u un endomorphisme de E.

On fait tout d'abord l'hypothèse que le polynôme caractéristique χ_u est scindé sur $\mathbb{K}$ et que l'ordre de multiplicité algébrique de chaque valeur propre soit égal à la dimension du sous-espace propre correspondant. On pose $\chi_u(X) = \prod_{i=1}^{p} (X - \lambda_i)^{m_{\lambda_i}}$, où les scalaires $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres deux à deux distinctes de u et les entiers $m_{\lambda_1}, \ldots, m_{\lambda_p}$ sont leurs ordres de multiplicité respectifs. Par hypothèse, on a, pour tout entier i de $\{1, \ldots, p\}$, $\dim(E_{\lambda_i}) = m_{\lambda_i} =$, ce qui implique alors que

$$n = \deg(\chi_u) = \sum_{i=1}^{p} m_{\lambda_i} = \sum_{i=1}^{p} \dim(E_{\lambda_i}).$$

Les sous-espaces propres étant en somme directe en vertu de la proposition 1.10, il existe donc une base de E formée de vecteurs propres de u et la proposition 1.29 permet alors d'affirmer que l'endomorphisme est diagonalisable.

Réciproquement, on suppose que l'endomorphisme u soit diagonalisable. L'espace vectoriel E est somme directe des sous-espaces propres de u, c'est-à-dire

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p},$$

où les scalaires $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres deux à deux distinctes de u. Dans une base de E adaptée à cette décomposition en somme directe, la matrice représentative de u diagonale par blocs

$$D = \begin{pmatrix} \lambda_1 I_{\dim(E_{\lambda_1})} & 0 & \ldots & 0 \\ 0 & \lambda_2 I_{\dim(E_{\lambda_2})} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \lambda_p I_{\dim(E_{\lambda_p})} \end{pmatrix},$$

ce qui implique que

$$\chi_u(X) = \chi_D(X) = \prod_{i=1}^{p} (X - \lambda_i)^{\dim(E_{\lambda_i})}.$$

Le polynôme caractéristique de u est donc scindé sur $\mathbb{K}$ et l'ordre de multiplicité de chaque valeur propre correspond à la dimension du sous-espace propre associé. □

On a évidemment un résultat similaire pour une matrice carrée.

La preuve du résultat suivant est laissée au lecteur.

Corollaire 1.32 (condition suffisante de diagonalisabilité) *Soit un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle égale à n. Si cet endomorphisme possède n valeurs propres distinctes, alors il est diagonalisable et ses sous-espaces propres sont des droites vectorielles.*

La diagonalisation d'une matrice en pratique

Soit M une matrice d'ordre n à coefficients dans le corps $\mathbb{K}$.

1. Calculer le polynôme caractéristique χ_M, trouver ses racines et une factorisation associée du polynôme pour obtenir les valeurs propres avec leurs ordres de multiplicité algébrique respectifs. Si le polynôme n'est pas scindé, la matrice n'est pas diagonalisable.
2. Si le polynôme caractéristique est scindé, déterminer pour chaque valeur propre le sous-espace propre qui lui est associé.
3. Pour chacune des valeurs propres, comparer l'ordre de multiplicité algébrique de la valeur propre avec la dimension du sous-espace propre correspondant. Si ces deux nombres sont égaux pour *toutes* les valeurs propres, alors la matrice est diagonalisable. S'il existe au moins une valeur propre pour laquelle ce n'est pas le cas, la matrice n'est pas diagonalisable.
4. Si la matrice est diagonalisable et si $\{V_1, \ldots, V_n\}$ est une base de $M_{n,1}(\mathbb{K})$ formée de vecteurs propres associés aux valeurs propres $\lambda_1, \ldots, \lambda_n$ de M comptées avec leur ordre de multiplicité, alors la matrice P dont les colonnes sont les vecteurs V_i, $i = 1, \ldots, n$, est telle que

$$M = P \operatorname{diag}(\lambda_1, \ldots, \lambda_n) P^{-1}.$$

Exemple 1.33 *On considère la diagonalisation de la matrice*

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

On calcule tout d'abord le polynôme caractéristique de M. On trouve, en développant par rapport à la première ligne,

$$\chi_M(X) = \begin{vmatrix} X-1 & 0 & 0 \\ 0 & X-1 & 0 \\ -1 & 1 & X-2 \end{vmatrix} = (X-1)^2(X-2).$$

Ce polynôme est scindé sur $\mathbb{R}$ et les valeurs propres 1 et 2 ont respectivement un ordre de multiplicité égal à 2 et 1. On détermine alors les sous-espaces propres de M. On considère tout d'abord $E_1 = \ker(M - I_3)$. On a

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in E_1 \iff MX = X \iff \begin{cases} x_1 = x_1 \\ x_2 = x_2 \\ x_1 - x_2 + 2x_3 = x_3 \end{cases} \iff x_1 - x_2 + x_3 = 0,$$

d'où

$$E_1 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ -x_1 + x_2 \end{pmatrix} \mid (x_1, x_2) \in \mathbb{R}^2 \right\}$$

est un plan vectoriel dont, par exemple, les vecteurs $V_1 = \begin{pmatrix}1 & 0 & -1\end{pmatrix}^\top$ *et* $V_2 = \begin{pmatrix}0 & 1 & 1\end{pmatrix}^\top$ *forment une base. On s'intéresse ensuite à* $E_2 = \ker(M - 2I_3)$*. On a cette fois*

$$X = \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \in E_2 \iff MX = 2X \iff \begin{cases} x_1 = 2x_1\\ x_2 = 2x_2\\ x_1 - x_2 + 2x_3 = 2x_3\end{cases} \iff x_1 = 0 \text{ et } x_2 = 0,$$

d'où

$$E_2 = \left\{ \begin{pmatrix}0\\0\\x_3\end{pmatrix} \mid x_3 \in \mathbb{R} \right\}$$

est une droite vectorielle dont, par exemple, le vecteur $V_3 = \begin{pmatrix}0 & 0 & 1\end{pmatrix}^\top$ *est une base.*

Les dimensions des sous-espaces propres coïncidant avec les ordres de multiplicité des valeurs propres associées, la matrice M *est diagonalisable. Dans la base associée à la famille* (V_1, V_2, V_3)*, l'endomorphisme canoniquement associé à la matrice* M *est représenté par la matrice*

$$D = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 2\end{pmatrix}.$$

En notant P *la matrice de passage correspondante,*

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

on a que $M = PDP^{-1}$*, avec*

$$P^{-1} = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\1 & -1 & 1\end{pmatrix}.$$

On termine cette section en donnant un résultat qui s'avérera utile dans la suite.

Lemme 1.34 *Soit* E *un* $\mathbb{K}$*-espace vectoriel de dimension finie non nulle et deux endomorphismes* u *et* v *de* E *diagonalisables. Alors,* u *et* v *sont diagonalisables dans une même base (on dit encore qu'ils sont* codiagonalisables*) si et seulement s'ils commutent entre eux.*

DÉMONSTRATION. On suppose tout d'abord que les endomorphismes u et v commutent entre eux et l'on raisonne par récurrence sur la dimension de E, qu'on note n. Pour $n = 1$, le résultat est évident. On suppose ensuite que, pour un entier n supérieur ou égal à 2, le résultat est vrai pour tout espace de dimension inférieure ou égale à $n-1$. Dans ce cas, si u et v sont tous deux des homothéties, le résultat est évident. On suppose alors que l'un des endomorphismes n'est pas une homothétie, u par exemple. Puisque u est diagonalisable, l'espace E est somme directe des sous-espaces propres de u, chacun de ces sous-espaces étant de dimension strictement inférieure à n, puisque u n'est pas une homothétie. Par ailleurs, pour toute valeur propre λ de u, le sous-espace propre E_λ est stable par v en vertu de la proposition 1.5 et la restriction de v à E_λ, notée $v_{|_{E_\lambda}}$, est diagonalisable. La restriction de u à E_λ, notée $u_{|_{E_\lambda}}$, commute avec $v_{|_{E_\lambda}}$ et l'on peut donc utiliser l'hypothèse de récurrence pour affirmer qu'il existe une base de E_λ diagonalisant ces deux endomorphismes. Le résultat étant vrai pour tout choix de valeur propre λ de u, on obtient une base commune de diagonalisation de u et de v par réunion de ces bases de sous-espace propres.

On suppose à présent que les endomorphismes u et v sont codiagonalisables. On note $\mathscr{C}$ une base commune de diagonalisation et soit $\mathscr{B}$ une base quelconque de E. Il existe alors une matrice de passage P telle que $\mathrm{Mat}_{\mathscr{B}}(u) = P\mathrm{Mat}_{\mathscr{C}}(u)P^{-1}$ et $\mathrm{Mat}_{\mathscr{B}}(v) = P\mathrm{Mat}_{\mathscr{C}}(v)P^{-1}$, les matrices $\mathrm{Mat}_{\mathscr{C}}(u)$ et $\mathrm{Mat}_{\mathscr{C}}(v)$ étant diagonales. Le produit de matrices diagonales étant commutatif, on a ainsi

$$\begin{aligned}\mathrm{Mat}_{\mathscr{B}}(u)\mathrm{Mat}_{\mathscr{B}}(v) = P\mathrm{Mat}_{\mathscr{C}}(u)P^{-1}P\mathrm{Mat}_{\mathscr{C}}(v)P^{-1} = P\mathrm{Mat}_{\mathscr{C}}(u)\mathrm{Mat}_{\mathscr{C}}(v)P^{-1} = P\mathrm{Mat}_{\mathscr{C}}(v)\mathrm{Mat}_{\mathscr{C}}(u)P^{-1}\\ = P\mathrm{Mat}_{\mathscr{C}}(v)P^{-1}P\mathrm{Mat}_{\mathscr{C}}(u)P^{-1} = \mathrm{Mat}_{\mathscr{B}}(v)\mathrm{Mat}_{\mathscr{B}}(u),\end{aligned}$$

d'où u et v commutent entre eux. □

1.5 Trigonalisation

On a vu dans la section précédente que tout endomorphisme n'est pas nécessairement diagonalisable. On va maintenant montrer que l'on peut en revanche toujours trouver une base de l'espace dans laquelle la matrice d'un endomorphisme défini sur un $\mathbb{C}$-espace vectoriel est une matrice triangulaire. Cette réduction porte le nom de *trigonalisation*.

Définition 1.35 (endomorphisme trigonalisable) *Soit un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et un endomorphisme de E. On dit que cet endomorphisme est **trigonalisable** si et seulement s'il existe une base de l'espace dans laquelle sa matrice est triangulaire supérieure.*

Par extension, une matrice carrée sera dite trigonalisable l'endomorphisme qui lui est canoniquement associé est trigonalisable. En particulier, une matrice diagonalisable est trigonalisable.

Remarque 1.36 *Dans la définition précédente, on aurait pu tout aussi bien remplacer « triangulaire supérieure » par « triangulaire inférieure », toute matrice triangulaire supérieure étant semblable à une matrice triangulaire inférieure.*

Théorème 1.37 (condition nécessaire et suffisante de trigonalisabilité) *Un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle est trigonalisable si et seulement si son polynôme caractéristique est scindé sur $\mathbb{K}$. En particulier, tout endomorphisme d'un $\mathbb{C}$-espace vectoriel est trigonalisable.*

DÉMONSTRATION. On note n la dimension de l'espace. Soit M une matrice de $M_n(\mathbb{K})$ représentant l'endomorphisme dans une certaine base. Si l'endomorphisme est trigonalisable, il existe une matrice P de $GL_n(\mathbb{K})$ et une matrice T triangulaire supérieure telles que $M = PTP^{-1}$. En posant

$$T = \begin{pmatrix} \lambda_1 & * & \dots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \lambda_n \end{pmatrix},$$

les coefficients $\lambda_1, \dots, \lambda_n$ appartenant à $\mathbb{K}$, on trouve alors que $\chi_M(X) = \chi_T(X) = \prod_{i=1}^{n}(X - \lambda_i)$. Le polynôme caractéristique de l'endomorphisme est donc scindé sur $\mathbb{K}$.

On va à présent montrer l'implication réciproque en raisonnant par récurrence sur l'ordre de la matrice. Si $n = 1$, tout élément de $M_n(\mathbb{K})$ est triangulaire et donc trigonalisable. On suppose à présent que l'entier n soit supérieur ou égal à 1 et que tout élément de $M_n(\mathbb{K})$ dont le polynôme caractéristique est scindé sur $\mathbb{K}$ soit trigonalisable. Soit une matrice M de $M_{n+1}(\mathbb{K})$, telle que χ_M est scindé sur $\mathbb{K}$. L'endomorphisme de $\mathbb{K}^{n+1}$ canoniquement associé à M admet au moins une valeur propre λ_1 appartenant à $\mathbb{K}$. Soit v_1 un vecteur propre associé à λ_1. La famille $\{v_1\}$ étant libre, on peut la compléter en une base de $\mathbb{K}^{n+1}$, la matrice de l'endomorphisme dans cette base s'écrivant alors sous la forme par blocs

$$M' = \begin{pmatrix} \lambda_1 & L \\ 0 & M_1 \end{pmatrix},$$

avec L appartenant à $M_{1,n}(\mathbb{K})$ et M_1 appartenant à $M_n(\mathbb{K})$. Les matrices M et M' étant semblables, il existe une matrice P' de $GL_{n+1}(\mathbb{K})$ telle que

$$M = P'M'(P')^{-1},$$

et un calcul par blocs du déterminant montre que $\chi_{M'}(X) = (X - \lambda_1)\det(X\,I_n - M_1) = (X - \lambda_1)\chi_{M_1}(X)$. D'autre part, χ_M étant scindé sur $\mathbb{K}$, on peut poser $\chi_M(X) = \prod_{i=1}^{n+1}(X - \lambda_i)$, dont on déduit que $\chi_{M_1}(X) = \prod_{i=2}^{n+1}(X - \lambda_i)$. L'hypothèse de récurrence assure alors l'existence d'une matrice P_1 de $GL_n(\mathbb{K})$ et d'une matrice triangulaire supérieure T_1 telles que $M_1 = P_1 T_1 {P_1}^{-1}$.

Il suffit ensuite de poser

$$P'' = \begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix}.$$

Par un calcul par blocs, on a $\det(P'') = \det(P_1)$, d'où P'' est inversible et, toujours en calculant par blocs, il vient

$$(P'')^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & {P_1}^{-1} \end{pmatrix}$$

et

$$(P'')^{-1}M'P'' = \begin{pmatrix} \lambda_1 & LP_1 \\ 0 & T_1 \end{pmatrix} = T.$$

On pose finalement $P = P'P''$. Cette dernière matrice est inversible et l'on a

$$P^{-1}MP = (P'')^{-1}(P')^{-1}MP'P'' = (P'')^{-1}M'P'' = T.$$

L'endomorphisme représenté par M est donc trigonalisable.
Une conséquence du théorème fondamental de l'algèbre, encotre appelé théorème de d'Alembert–Gauss, étant que tout polynôme à coefficient complexe est scindé, c'est le cas pour le polynôme caractéristique de tout endomorphisme d'un $\mathbb{C}$-espace vectoriel, qui est donc un endomorphisme trigonalisable. □

Le dernier théorème s'applique à une matrice carrée à coefficient réels, pour peu que l'on factorise son polynôme caractéristique sur $\mathbb{C}$ et non sur $\mathbb{R}$. C'est en ce sens que l'on peut dire, comme on l'a écrit en début de section, que l'on peut toujours trouver une base dans laquelle la matrice d'un endomorphisme défini sur un $\mathbb{C}$-espace vectoriel est triangulaire.

La preuve du résultat suivant est laissée au lecteur.

Corollaire 1.38 *Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie non nulle, dont le polynôme caractéristique peut s'écrire*

$$\chi_u(X) = \prod_{i=1}^{p}(X-\lambda_i)^{m_{\lambda_i}}.$$

On a alors

$$\mathrm{tr}(u) = \sum_{i=1}^{p} m_{\lambda_i}\lambda_i \text{ et } \det(u) = \prod_{i=1}^{p} {\lambda_i}^{m_{\lambda_i}}.$$

La trigonalisation d'une matrice en pratique

Soit M une matrice d'ordre n à coefficients dans le corps $\mathbb{K}$.

1. Calculer le polynôme caractéristique χ_M, trouver ses racines et une factorisation associée du polynôme pour obtenir les valeurs propres. Si le polynôme caractéristique n'est pas scindé, la matrice n'est pas trigonalisable.
2. Si le polynôme caractéristique est scindé, trouver une base dans laquelle la matrice de l'endomorphisme représenté par M sera triangulaire supérieure. Pour cela, on peut faire comme suit.

   On a tout d'abord intérêt à placer dans la base le plus grand nombre possible de vecteurs propres de la matrice, en déterminant pour cela une base de chaque sous-espace propre. La réunion de ces bases constitue bien une partie de la base recherchée, puisque les sous-espaces propres sont en somme directe. Le choix de ces premiers vecteurs (ici au nombre de p) impose que la matrice triangulaire sera de la forme (on suppose ici que les scalaires $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de M comptées avec leur ordre de multiplicité algébrique)

$$T = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 & * & \ldots & \ldots & * \\ 0 & \ddots & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & & \vdots \\ \vdots & & \ddots & \lambda_p & * & & & \vdots \\ \vdots & & & \ddots & \lambda_{p+1} & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & & \ddots & \ddots & * \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \lambda_n \end{pmatrix}.$$

Il reste à compléter la famille obtenue pour arriver à une base. On peut procéder itérativement en supposant que l'on a déjà déterminé les vecteurs $V_1,\dots,V_j$, avec $p \le j \le n-1$. Afin de choisir le vecteur suivant, on commence par compléter la famille $\{V_1,\dots,V_j\}$ en une base $\{V_1,\dots,V_j,U_{j+1},\dots,U_n\}$ de $M_{n,1}(\mathbb{K})$, puis on cherche V_{j+1} sous la forme $V_{j+1}=\sum_{i=j+1}^{n}\alpha_i U_i$, la forme de la matrice T imposant que $MV_{j+1}=\sum_{i=1}^{j}t_{i\,j+1}V_i+\lambda_{j+1}V_{j+1}$. En explicitant cette relation, on obtient un système de n équations linéaires dont les inconnues sont les n coefficients $t_{1\,j+1},\dots,t_{j\,j+1},\alpha_{j+1},\dots,\alpha_n$:

$$\sum_{i=1}^{j}t_{i\,j+1}V_i+\sum_{i=j+1}^{n}\alpha_i(\lambda_{j+1}U_i-MU_i)=0.$$

Toute solution non nulle de ce système fournit un vecteur V_{j+1} possible et les coefficients, possiblement non nuls, correspondants de la $j+1^{\text{e}}$ colonne de T.

Exemple 1.39 *On considère la trigonalisation de la matrice*

$$M=\begin{pmatrix}1&4&-2\\0&6&-3\\-1&4&0\end{pmatrix}.$$

On calcule tout d'abord le polynôme caractéristique de M. On trouve, après calculs,

$$\chi_M(X)=\begin{vmatrix}X-1&-4&2\\0&X-6&3\\1&-4&X\end{vmatrix}=(X-2)^2(X-3).$$

Ce polynôme est scindé sur $\mathbb{R}$, la matrice M est donc trigonalisable sur $\mathbb{R}$, et les valeurs propres 2 et 3 ont respectivement un ordre de multiplicité égal à 2 et 1. On détermine alors les sous-espaces propres de M. On considère tout d'abord $E_3=\ker(M-3I_3)$. On a

$$X=\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\in E_3\iff MX=3X\iff\begin{cases}x_1+4x_2-2x_3=3x_1\\6x_2-3x_3=3x_2\\-x_1+4x_2=3x_3\end{cases}\iff x_1=x_2=x_3,$$

d'où E_3 est une droite vectorielle dont, par exemple, le vecteur $V_1=\begin{pmatrix}1&1&1\end{pmatrix}^\top$ est une base. On s'intéresse ensuite à $E_2=\ker(M-2I_3)$. On a

$$X=\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\in E_2\iff MX=2X\iff\begin{cases}x_1+4x_2-2x_3=2x_1\\6x_2-3x_3=2x_2\\-x_1+4x_2=2x_3\end{cases}\iff\begin{cases}x_1=x_3\\4x_2=3x_3\end{cases},$$

d'où E_2 est une droite vectorielle dont, par exemple, le vecteur $V_2=\begin{pmatrix}4&3&4\end{pmatrix}^\top$ est une base. Puisque la dimension de ce sous-espace propre n'est pas égale à l'ordre de multiplicité de la valeur propre associée, la matrice M n'est pas diagonalisable.

On complète enfin la famille libre constituée des vecteurs V_1 et V_2 en une base, en choisissant, par exemple, le vecteur $V_3=\begin{pmatrix}0&0&1\end{pmatrix}^\top$, et l'on exprime le vecteur MV_3 dans cette même base :

$$MV_3=\begin{pmatrix}1&4&-2\\0&6&-3\\-1&4&0\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}=\begin{pmatrix}-2\\-3\\0\end{pmatrix}=-2(-3V_1+V_2-V_3)-3(4V_1-V_2)=-6V_1+V_2+2V_3.$$

L'endomorphisme canoniquement associé à M est ainsi représenté dans la base associée à la famille (V_1,V_2,V_3) par la matrice

$$T=\begin{pmatrix}3&0&-6\\0&2&1\\0&0&2\end{pmatrix}.$$

En notant P la matrice de passage correspondante,

$$P = \begin{pmatrix} 1 & 4 & 0 \\ 1 & 3 & 0 \\ 1 & 4 & 1 \end{pmatrix},$$

on a trouvé que $M = PTP^{-1}$, avec

$$P^{-1} = \begin{pmatrix} -3 & 4 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

1.6 Polynômes annulateurs

Soit $P(X) = a_0 + a_1 X + \cdots + a_p X^p$ un polynôme de degré p de $\mathbb{K}[X]$. Pour tout endomorphisme u d'un $\mathbb{K}$-espace vectoriel E de dimension finie non nulle, on définit le *polynôme d'endomorphisme* $P(u)$ comme l'endomorphisme tel que

$$P(u) = a_0\, id_E + a_1\, u + \cdots + a_p u^p. \tag{1.2}$$

La preuve du prochain résultat est laissée en exercice au lecteur.

Proposition 1.40 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. L'application de $\mathbb{K}[X]$ dans $\mathscr{L}(E)$ qui a tout polynôme P associe l'application linéaire $P(u)$ définie par* (1.2) *est un* ***morphisme d'algèbres****, c'est-à-dire qu'elle est linéaire, i.e.*

$$\forall \lambda \in \mathbb{K},\ \forall (P,Q) \in (\mathbb{K}[X])^2,\ (\lambda P + Q)(u) = \lambda P(u) + Q(u),$$

et vérifie

$$\forall (P,Q) \in (\mathbb{K}[X])^2,\ (PQ)(u) = P(u) \circ Q(u).$$

On remarquera qu'il découle de la seconde propriété que, pour tous polynômes P et Q et tout endomorphisme u, les endomorphismes $P(u)$ et $Q(u)$ commutent entre eux.

On peut de la même manière définir un morphisme d'algèbres sur l'ensemble des matrices carrées en posant, pour toute matrice M de $M_n(\mathbb{K})$,

$$P(M) = a_0\, I_n + a_1\, M + \cdots + a_p\, M^p.$$

Exemple 1.41 (polynôme d'une matrice diagonale) *Soit n un entier naturel non nul et la matrice diagonale de $M_n(\mathbb{K})$*

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}.$$

Pour tout polynôme P de $\mathbb{K}[X]$, on a

$$P(D) = \begin{pmatrix} P(\lambda_1) & 0 & \dots & 0 \\ 0 & P(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & P(\lambda_n) \end{pmatrix}.$$

Définition 1.42 (polynôme annulateur) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E. On dit qu'un polynôme P est un* ***polynôme annulateur*** *de u si l'endomorphisme $P(u)$ est nul.*

Une définition similaire vaut bien entendu dans le cas d'une matrice carrée.

Remarque 1.43 *L'ensemble des polynômes annulateurs d'un même endomorphisme forme un* ***idéal***[4].

Exemple 1.44 (polynôme annulateur d'une projection vectorielle) *On rappelle qu'une projection u d'un espace vectoriel E est* idempotente*, c'est-à-dire que* $u \circ u = u$*. Le polynôme* $X^2 - X$ *est donc annulateur de u.*

Exemple 1.45 (polynôme annulateur d'endomorphisme nilpotent) *Un endomorphisme u nilpotent d'indice l d'un espace vectoriel E est tel que* $u^l = 0_{\mathscr{L}(E)}$*. Il en résulte que le polynôme* X^l *est annulateur de u.*

Le résultat suivant établit un lien entre les valeurs propres d'un endomorphisme et les racines de tout polynôme annulateur de cet endomorphisme.

Proposition 1.46 *Soit u un endomorphisme d'un* $\mathbb{K}$*-espace vectoriel de dimension finie non nulle et P un polynôme annulateur de u. On a l'inclusion*

$$\mathrm{Sp}(u) \subset \{\textit{racines de } P\}.$$

DÉMONSTRATION. Si x est un vecteur propre de u associé à une valeur propre λ, on a $u(x) = \lambda x$, ce qui implique que, pour tout entier naturel k, $u^k(x) = \lambda^k x$ et, plus généralement que, pour tout polynôme P de $\mathbb{K}[X]$, $P(u)(x) = P(\lambda)x$. En particulier, avoir $P(u)(x) = 0_E$ implique que $P(\lambda)x = 0_E$ et donc que $P(\lambda) = 0$, puisque le vecteur x est non nul. □

On prendra bien garde de retenir que toute racine d'un polynôme annulateur n'est pas nécessairement une valeur propre.

Théorème 1.47 (« théorème de Cayley–Hamilton ») *Soit u un endomorphisme d'un* $\mathbb{K}$*-espace vectoriel de dimension finie non nulle. On a*

$$\chi_u(u) = 0_{\mathscr{L}(E)}.$$

DÉMONSTRATION. On note E l'espace vectoriel de l'énoncé et n sa dimension. On va montrer que, pour tout vecteur x non nul de E, $\chi_u(u)(x) = 0_E$. Soit $\mathscr{E}$ le sous-ensemble de $\mathbb{N}$ défini par

$$\mathscr{E} = \left\{k \in \mathbb{N}^* \mid \{u^i(x)\}_{0 \leq i \leq k-1} \text{ est une famille libre}\right\}.$$

C'est une partie non vide de $\mathbb{N}$ (puisque x est non nul), majorée par n. Elle admet donc un plus grand élément, que l'on note p. Par définition de p, la famille $\{x, u(x), \ldots, u^{p-1}(x)\}$ est libre et on peut la compléter au besoin en une base $\mathscr{B} = \{x, u(x), \ldots, u^{p-1}(x), e_{p+1}, \ldots, e_n\}$ de E. Toujours par définition de p, la famille $\{x, u(x), \ldots, u^p(x)\}$ est liée et il existe des scalaires $a_0, \ldots, a_{p-1}$ non tous nuls tels que $u^p(x) + \sum_{i=0}^{p-1} a_i u^i(x) = 0_E$. La matrice de u dans la base $\mathscr{B}$ s'écrit ainsi par blocs

$$\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

avec

$$B = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{p-1} \end{pmatrix} \tag{1.3}$$

une matrice d'ordre p, et le calcul par blocs du déterminant définissant χ_u donne $\chi_u = \chi_B \chi_D$. On a

$$\chi_B(X) = \det(X I_p - B) = \begin{vmatrix} X & 0 & \ldots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & \vdots \\ 0 & \ldots & 0 & -1 & X + a_{p-1} \end{vmatrix} = \begin{vmatrix} 0 & 0 & \ldots & 0 & X^p + \sum_{i=0}^{p-1} a_i X^i \\ -1 & X & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & \vdots \\ 0 & \ldots & 0 & -1 & X + a_{p-1} \end{vmatrix},$$

4. Un *idéal* est un sous-ensemble remarquable d'un anneau : c'est un sous-groupe du groupe additif de l'anneau, qui est de plus stable par multiplication par les éléments de l'anneau.

la dernière égalité étant obtenue en additionnant à la première ligne du déterminant chacune des autres lignes, respectivement multipliée par X à la puissance de son indice diminué d'une unité. Un développement par rapport à la première ligne du déterminant conduit alors à

$$\chi_B(X) = (-1)^{p+1}\left(X^p + \sum_{i=0}^{p-1} a_i X^i\right)\begin{vmatrix} -1 & X & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & X \\ 0 & \dots & \dots & 0 & -1 \end{vmatrix} = (-1)^{2p}\left(X^p + \sum_{i=0}^{p-1} a_i X^i\right) = X^p + \sum_{i=0}^{p-1} a_i X^i,$$

et l'on trouve finalement

$$\chi_u(u) = \left(u^p - \sum_{i=0}^{p-1} a_i\, u^i\right) \circ \chi_D(u).$$

Puisque ces deux polynômes de u commutent entre eux, on a obtenu que

$$\chi_u(u)(x) = \chi_D(u)\left(u^p(x) - \sum_{i=0}^{p-1} a_i\, u^i(x)\right) = \chi_D(u)(0_E) = 0_E.$$

Cette égalité restant vraie pour $x = 0_E$, on a prouvé le résultat. □

Ce résultat montre que le polynôme caractéristique, ainsi que tous ses multiples, est un polynôme annulateur de l'endomorphisme auquel il est associé.

Remarque 1.48 *Dans la démonstration ci-dessus, on a déterminé le plus petit sous-espace vectoriel stable par u contenant le vecteur x (voir aussi l'exemple 1.3). Dans la base choisie pour ce dernier, la matrice de l'endomorphisme, dit* cyclique*, induit par u sur le sous-espace a la forme* (1.3) *d'une* ***matrice compagnon****, c'est-à-dire une matrice dont le polynôme caractéristique est le polynôme unitaire* $X^p + \sum_{i=0}^{p-1} a_i X^i$ *et qui est, en ce sens, la « compagne » de ce polynôme.*

Définition 1.49 (polynôme minimal) *Un* ***polynôme minimal*** *d'un endomorphisme est un polynôme annulateur de cet endomorphisme, unitaire et de degré minimal.*

Le résultat suivant justifie le fait de parler « du » polynôme minimal d'un endomorphisme.

Proposition 1.50 *Soit u un endomorphisme d'un* $\mathbb{K}$*-espace vectoriel de dimension finie non nulle. Il existe un unique polynôme minimal de u, noté* μ_u*, et celui-ci divise tout polynôme annulateur de u*

DÉMONSTRATION. On note E l'espace vectoriel de l'énoncé et n sa dimension. Soit l'ensemble des degrés des polynômes annulateurs de u :

$$\{\deg(P) \,|\, P \in \mathbb{K}[X],\ P \neq 0_{\mathbb{K}[X]},\ P(u) = 0_{\mathscr{L}(E)}\}.$$

C'est une partie non vide de $\mathbb{N}$, car elle contient l'entier n en vertu du théorème de Cayley–Hamilton. Soit m son plus petit élément et soit Π un polynôme annulateur de u de degré m. On va montrer que tout polynôme annulateur P de u est un multiple de Π. Pour cela, on effectue la division euclidienne de P par Π :

$$P = \Pi Q + R,$$

où $\deg(R) \leq m-1$. Si $P(u) = 0_{\mathscr{L}(E)}$ et $\Pi(u) = 0_{\mathscr{L}(E)}$, alors $R(u) = 0_{\mathscr{L}(E)}$, ce qui implique que R est nul et le polynôme P est donc multiple de Π.

Enfin, si Π_1 et Π_2 sont deux polynômes annulateurs de u de degré m, ils sont multiples l'un de l'autre et ne diffèrent par conséquent que d'une constante multiplicative. On a donc unicité du polynôme minimal si l'on suppose que le coefficient de son terme de plus haut degré est fixé, ce que l'on a fait en posant qu'il est égal à 1. □

Exemple 1.51 (polynôme minimal d'une projection vectorielle et d'une symétrie vectorielle) *Le polynôme minimal d'une projection vectorielle, distincte de* $0_{\mathscr{L}(E)}$ *et* id_E*, est* $X(X-1)$ *et celui d'une symétrie vectorielle, distincte de* id_E *et* $-id_E$*, est* $X^2 - 1 = (X-1)(X+1)$*.*

Proposition 1.52 *Soit un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle. Les racines du polynôme minimal de cet endomorphisme sont exactement les valeurs propres de cet endomorphisme.*

DÉMONSTRATION. Compte tenu de la proposition 1.46, on a juste à montrer que toute racine du polynôme minimal d'un endomorphisme est une valeur propre de cet endomorphisme. Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension finie non nulle dont le scalaire λ est racine du polynôme minimal. Dans ce cas, on a $\mu_u(X) = (X-\lambda)Q(X)$, avec $\deg(Q) \leq \deg(\mu_u) - 1$ et on a donc

$$0_{\mathscr{L}(E)} = \mu_u(u) = (u - \lambda\, id_E) \circ Q(u).$$

Puisque l'on a $Q(u) \neq 0_{\mathscr{L}(E)}$ par minimalité de μ_u, l'endomorphisme $u - \lambda\, id_E$ n'est pas injectif et λ est une donc valeur propre de u. □

Le résultat suivant caractérise le polynôme minimal d'un endomorphisme dont le polynôme caractéristique est scindé.

Théorème 1.53 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E dont le polynôme caractéristique est scindé, c'est-à-dire*

$$\chi_u(X) = \prod_{i=1}^{p} (X - \lambda_i)^{m_{\lambda_i}},$$

où les entiers naturels m_{λ_i}, $i = 1, \ldots, p$, sont non nuls et les valeurs propres λ_i, $i = 1, \ldots, p$, sont deux à deux distinctes. Alors on a

$$\mu_u(X) = \prod_{i=1}^{p} (X - \lambda_i)^{\ell_{\lambda_i}},$$

où les entiers naturels ℓ_{λ_i}, $i = 1, \ldots, p$, sont respectivement compris entre 1 et m_{λ_i}.

DÉMONSTRATION. On a précédemment montré que toute racine du polynôme minimal μ_u est une valeur propre de u. On a donc nécessairement que l'entier naturel ℓ_{λ_i} est supérieur ou égal à 1 pour tout entier i de $\{1, \ldots, p\}$. On sait par ailleurs que le polynôme minimal μ_u divise le polynôme caractéristique χ_u, d'où ℓ_{λ_i} est inférieur ou égal à m_{λ_i} pour tout entier i de $\{1, \ldots, p\}$. □

Remarque 1.54 (calcul pratique du polynôme minimal) *Pour calculer le polynôme minimal d'une matrice M d'ordre n, on peut chercher une relation de degré minimal entre les $n+1$ premières puissances de la matrice (I_n, M, M^2,..., M^n), en voyant chacune d'elles comme un vecteur à n^2 composantes. Cela revient à déterminer un noyau et peut se faire au moyen de l'élimination de Gauss, mais le procédé est coûteux en opérations car on l'applique à une matrice à n^2 lignes et $n+1$ colonnes.*
Une autre manière de faire consiste à tirer aléatoirement un vecteur V de $M_{n,1}(\mathbb{K})$ et à chercher, par exemple en utilisant l'élimination de Gauss[5]*, une relation entre les vecteurs V, MV, M^2V,..., M^nV, de manière à trouver un polynôme Π tel que $\Pi(M)V = 0_{M_{n,1}(\mathbb{K})}$. Si le degré de Π est égal à n, on peut montrer que Π est à la fois le polynôme caractéristique et le polynôme minimal de M. Si le degré de Π est strictement inférieur à n, on réitère la recherche avec d'autre(s) vecteur(s) tiré(s) aléatoirement, jusqu'à vérifier que le plus petit commun multiple des polynômes obtenus est annulateur de M.*
Enfin, le théorème 1.53 fournit une méthode de calcul possible lorsque le polynôme caractéristique est scindé et qu'il a été déterminé et factorisé, c'est-à-dire que l'on connaît les valeurs propres distinctes $\lambda_1, \ldots, \lambda_p$ de M avec leurs ordres de multiplicité respectifs $m_{\lambda_1}, \ldots, m_{\lambda_p}$. Il suffit alors de chercher parmi tous les polynômes du type $\prod_{i=1}^{p} (X - \lambda_i)^{s_{\lambda_i}}$, où les entiers naturels s_{λ_i}, $i = 1, \ldots, p$, sont respectivement compris entre 1 et m_{λ_i}, celui de plus bas degré qui est annulateur de M. On peut commencer par tester le polynôme $(X - \lambda_1) \ldots (X - \lambda_p)$, pour ensuite augmenter méthodiquement les puissances des facteurs jusqu'à trouver le polynôme minimal.

Exemple 1.55 (polynômes minimal et caractéristique d'une homothétie) *On considère une homothétie de rapport λ non nul d'un espace vectoriel E de dimension finie non nulle n, i.e $u = \lambda\, id_E$. La matrice de u dans n'importe quelle base de E est diagonale, de coefficients diagonaux tous égaux à λ, d'où $\mu_u(X) = X - \lambda$ et $\chi_u(X) = (X - \lambda)^n$.*

5. Le coût est ici raisonnable puisque l'on considère une matrice à n lignes et $n+1$ colonnes.

L'exemple précédent est particulièrement éclairant, car diagonaliser un endomorphisme revient à écrire l'espace comme une somme directe de sous-espaces propres de cet endomorphisme pour chacun desquels la restriction de l'endomorphisme est une homothétie. Cette observation conduit à une nouvelle caractérisation de la diagonalisation.

Théorème 1.56 *Un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle dont le polynôme caractéristique est scindé sur $\mathbb{K}$ est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples.*

DÉMONSTRATION. On note E l'espace vectoriel et u l'endomorphisme de l'énoncé. On considère le polynôme $P(X)=\prod_{i=1}^{p}(X-\lambda_i)$ dont les racines sont les valeurs propres de u. Soit x un vecteur propre de u associé à une valeur propre λ_j. L'image de x par $P(u)$ est $P(u)(x)=\prod_{i=1}^{p}(\lambda_j-\lambda_i)x=0_E$.

On suppose que u est diagonalisable. Il existe alors une base E formée de vecteurs propres de u et $P(u)$ s'annule sur chacun des vecteurs composant cette base. Le polynôme P est donc un polynôme annulateur de u, multiple du polynôme minimal μ_u. Or, par le théorème 1.53, on a que P divise μ_u, d'où $P=\mu_u$.

Réciproquement, on suppose que le polynôme minimal de u soit

$$\mu_u(X)=\prod_{i=1}^{p}(X-\lambda_i).$$

Les sous-espaces propres étant en somme directe, on doit simplement montrer que tout vecteur de E s'écrit comme une combinaison linéaire de vecteurs propres. Par une décomposition en éléments simples, on a

$$\frac{1}{\prod_{k=1}^{p}(X-\lambda_k)}=\sum_{i=1}^{p}\left(\frac{1}{\prod_{j=1,j\neq i}^{p}(\lambda_i-\lambda_j)}\right)\frac{1}{X-\lambda_i}.$$

En multipliant cette égalité par le dénominateur du membre de gauche, il vient[6]

$$1=\sum_{i=1}^{p}\left(\frac{1}{\prod_{j=1,j\neq i}^{p}(\lambda_i-\lambda_j)}\right)\prod_{k=1,k\neq i}^{p}(X-\lambda_k).$$

On pose alors $\alpha_i=\frac{1}{\prod_{j=1,j\neq i}^{p}(\lambda_i-\lambda_j)}$, $P_i(X)=\prod_{k=1,k\neq i}^{p}(X-\lambda_k)$. On a que

$$id_E=\sum_{i=1}^{p}\alpha_i\,P_i(u),$$

d'où

$$\forall x\in E,\ x=\sum_{i=1}^{p}\alpha_i\,P_i(u)(x).$$

Enfin, en utilisant que

$$\forall i\in\{1,\dots,p\},\ P_i(X)(X-\lambda_i)=\prod_{j=1}^{p}(X-\lambda_j)=\mu_u(X),$$

on trouve que

$$0_E=\mu_u(u)(x)=(u-\lambda_i\,id_E)(P_i(u)(x)),$$

d'où $P_i(u)(x)$ appartient à E_{λ_i}. □

Exemple 1.57 *On retrouve le fait qu'une projection vectorielle (ou une symétrie vectorielle) est un endomorphisme diagonalisable en utilisant le théorème 1.56 et le polynome minimal donné dans l'exemple 1.51.*

On va conclure cette section avec un résultat riche de conséquences. Avant de l'énoncer, on rappelle tout d'abord que deux polynômes P et Q de $\mathbb{K}[X]$ sont dits *premiers entre eux* si et seulement si

$$D \text{ divise } P \text{ et } Q \text{ dans } \mathbb{K}[X] \implies D \text{ est un polynôme constant.}$$

En particulier, deux polynômes à coefficients complexes sont premiers entre eux si et seulement s'ils n'ont pas de racines communes. Par un cas particulier de l'*identité de Bézout*, des polynômes P et Q sont premiers entre eux si et seulement s'il existe des polynômes R et S tels que $RP+SQ=1$.

6. C'est l'écriture du polynôme constant et égal à 1 dans la base des polynômes de Lagrange associés aux valeurs propres de u.

Proposition 1.58 (« lemme de décomposition des noyaux ») *Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E et P et Q des polynômes premiers entre eux. On a*

$$\ker((PQ)(u)) = \ker(P(u)) \oplus \ker(Q(u)).$$

DÉMONSTRATION. Soit x un vecteur appartenant à $\ker(P(u))$. On a

$$P(u)(x) = 0_E \implies Q(u)(P(u)(x)) = 0_E \implies (P(u) \circ Q(u))(x) = 0_E \implies (PQ)(u)(x) = 0_E,$$

d'où x appartient à $\ker((PQ)(u))$. Ainsi, on a prouvé que $\ker(P(u)) \subset \ker((PQ)(u))$. De la même manière, on a $\ker(Q(u)) \subset \ker((PQ)(u))$.

Les polynômes P et Q étant premiers entre eux, on a que

$$R(u) \circ P(u) + S(u) \circ Q(u) = id_E.$$

En évaluant cette dernière identité en un vecteur x de $\ker((PQ)(u))$, on obtient

$$(R(u) \circ P(u))(x) + (S(u) \circ Q(u))(x) = x.$$

On pose alors $y = (S(u) \circ Q(u))(x)$ et $z = (R(u) \circ P(u))(x)$. Il vient

$$P(u)(y) = P(u)((S(u) \circ Q(u))(x)) = S(u)((P(u) \circ Q(u))(x)) = S(u)(0_E) = 0_E,$$

et, de la même façon, $Q(u)(z) = 0_E$. On a ainsi que y appartient à $\ker(P(u))$ et que z appartient à $\ker(Q(u))$, d'où $\ker((PQ)(u)) = \ker(P(u)) + \ker(Q(u))$. Enfin, pour tout vecteur x de $\ker(P(u)) \cap \ker(Q(u))$, on a, toujours en utilisant l'identité, $x = 0_E + 0_E = 0_E$, d'où $\ker(P(u)) \cap \ker(Q(u)) = \{0_E\}$. □

Il est possible de généraliser ce résultat en raisonnant par récurrence.

Corollaire 1.59 (« lemme de décomposition des noyaux généralisé ») *Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel, k un entier naturel strictement plus grand que 1 et $P_1, \dots, P_k$ des polynômes deux à deux premiers entre eux. On a*

$$\ker((P_1 \dots P_k)(u)) = \ker(P_1(u)) \oplus \cdots \oplus \ker(P_k(u)).$$

Une ultime caractérisation de la diagonalisabilité découle de ce dernier résultat.

Théorème 1.60 *Un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle est diagonalisable si et seulement s'il existe un polynôme non nul, scindé sur $\mathbb{K}$ et à racines simples, annulateur de cet endomorphisme.*

DÉMONSTRATION. Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension finie non nulle.

L'implication directe du théorème découle du théorème 1.56. Pour montrer l'implication réciproque, on suppose qu'il existe un polynôme P annulateur de u, de la forme

$$P(X) = \prod_{i=1}^{p} (X - \mu_i),$$

les scalaires $\mu_1, \dots, \mu_p$ étant deux à deux distincts. Les monômes $X - \mu_1, \dots, X - \mu_p$ étant alors deux à deux premiers entre eux, le corollaire 1.59 permet d'écrire que

$$E = \ker(P(u)) = \bigoplus_{i=1}^{p} \ker(u - \mu_i \, id_E).$$

Une base de E adaptée[7] à cette décomposition en somme directe est une base de vecteurs propres de u, l'endomorphisme est donc diagonalisable. □

On peut à présent résumer les conditions de diagonalisabilité et de trigonalisation établies dans ce chapitre.

7. Si $\ker(u - \mu_i \, id_E)$ se trouve réduit au vecteur nul, on considère qu'une « base » de ce noyau est l'ensemble vide.

Conditions de diagonalisabilité et de trigonalisabilité d'un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie non nulle égale à n et u un endomorphisme de E. Ci-dessous, on a noté m_{λ_i} l'ordre de multiplicité algébrique de la valeur propre λ_i de u et n_{λ_i} la dimension du sous-espace propre associé $\ker(u-\lambda_i\, id_E)$, $i=1,\dots,p$, χ_u le polynôme caractéristique de u et μ_u le polynôme minimal de u.

u est diagonalisable $\iff$ il existe une base de E dans laquelle la matrice représentative de u est diagonale,
$\iff$ il existe une base de E constituée de vecteurs propres de u,
$\iff$ E est la somme directe des sous-espaces propres de u,
$\iff$ $n=\sum_{i=1}^{p} n_{\lambda_i}$,
$\iff$ χ_u est scindé sur $\mathbb{K}$ et, $\forall i\in\{1,\dots,p\}$, $n_{\lambda_i}=m_{\lambda_i}$,
$\iff$ μ_u est scindé sur $\mathbb{K}$ et à racines simples,
$\iff$ il existe un polynôme annulateur de u non nul, scindé sur $\mathbb{K}$ et à racines simples,
$\impliedby$ u possède n valeurs propres simples $\iff$ χ_u est scindé sur $\mathbb{K}$ et à racines simples.

u est trigonalisable $\iff$ il existe une base de E dans laquelle la matrice représentative de u est triangulaire supérieure,
$\iff$ χ_u est scindé sur $\mathbb{K}$,
$\iff$ E est la somme directe des sous-espaces caractéristiques de u.

1.7 Réduction de Jordan

On peut « raffiner » la trigonalisation d'un endomorphisme donné en construisant une base de l'espace dans laquelle la matrice de cet endomorphisme est diagonale par blocs, chacun des blocs étant une matrice triangulaire supérieure dont les coefficients diagonaux sont identiques. Cette matrice est dite *sous forme normale de Jordan* et l'on donne le nom de *réduction de Jordan* à cette trigonalisation aboutie. Pour démontrer son existence, on aura besoin d'un certain nombre de définitions et de résultats préliminaires, qui sont l'objet des deux prochaines sous-sections.

1.7.1 Sous-espaces caractéristiques d'un endomorphisme

On va à présent établir une nouvelle caractérisation de la trigonalisation d'un endomorphisme en introduisant la notion de vecteur propre *généralisé* d'un endomorphisme. Pour cela, on commence par établir un résultat fondamental concernant les noyaux d'une suite d'itérés d'un endomorphisme particulier.

Lemme 1.61 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, u un endomorphisme de E et λ une valeur propre de u. La suite de sous-espaces vectoriels $\left\{\ker\left((u-\lambda\, id_E)^k\right)\right\}_{k\in\mathbb{N}}$ est croissante au sens de l'inclusion et devient stationnaire exactement à partir du rang égal à l'ordre de multiplicité ℓ_λ de λ en tant que racine du polynôme minimal de u.*

DÉMONSTRATION. Pour tout entier naturel k et tout vecteur x, il est clair que $(u-\lambda\, id_E)^k(x)=0_E$ entraîne que $(u-\lambda\, id_E)^{k+1}(x)=0_E$ et on a donc l'inclusion de $\ker\left((u-\lambda\, id_E)^k\right)$ dans $\ker\left((u-\lambda\, id_E)^{k+1}\right)$.

On suppose à présent qu'il existe un entier naturel k pour lequel $\ker\left((u-\lambda\, id_E)^k\right)=\ker\left((u-\lambda\, id_E)^{k+1}\right)$. Soit x un vecteur de $\ker\left((u-\lambda\, id_E)^{k+2}\right)$. On a $u^{k+2}(x)=u^{k+1}(u(x))=0_E$, d'où $u(x)$ appartient à $\ker\left((u-\lambda\, id_E)^{k+1}\right)$ et donc à $\ker\left((u-\lambda\, id_E)^k\right)$. Il vient alors que $u^{k+1}(x)=u^k(u(x))=0_E$ et x appartient à $\ker\left((u-\lambda\, id_E)^{k+1}\right)$.

En raisonnant par récurrence, on montre ainsi que la suite d'entiers $\left\{\dim\left(\ker\left((u-\lambda\, id_E)^k\right)\right)\right\}_{k\in\mathbb{N}}$ est croissante et devient stationnaire dès que deux termes consécutifs sont égaux. Elle est de plus majorée par $\dim(E)$. Il existe donc un entier naturel ℓ, non nul et inférieur ou égal à $\dim(E)$, tel que cette suite est strictement croissante pour tout rang k strictement inférieur à ℓ et stationnaire à partir du rang ℓ.

Le polynôme minimal de u s'écrit

$$\mu_u(X)=(X-\lambda)^{\ell_\lambda}Q(X),$$

avec Q un polynôme tel que $(X-\lambda)^{\ell_\lambda}$, et *a fortiori* $X-\lambda$, et Q sont premiers entre eux. Il découle alors du lemme de décomposition des noyaux (voir la proposition 1.58) que

$$\ker((u-\lambda\, id_E)) \cap \ker(Q(u)) = \{0_E\}.$$

Par définition de ℓ, il existe un vecteur x appartenant à $\ker\left((u-\lambda\, id_E)^{\ell}\right)$ tel que $(u-\lambda\, id_E)^{\ell-1}(x)$ est non nul. Comme ce dernier vecteur appartient à $\ker((u-\lambda\, id_E))$, l'égalité ci-dessus assure qu'il n'appartient pas à $\ker(Q(u))$. Ainsi, le vecteur $Q(u)((u-\lambda\, id_E)^{\ell-1}(x))$ n'est pas nul. Le polynôme $(X-\lambda)^{\ell-1}Q(X)$ n'est donc pas annulateur de u et ℓ est inférieur ou égal à ℓ_λ. On en déduit que $\ker\left((u-\lambda\, id_E)^{\ell_\lambda}\right)$ coïncide avec $\ker\left((u-\lambda\, id_E)^{\ell}\right)$. Une nouvelle application du lemme de décomposition des noyaux conduit par conséquent à

$$E = \ker\left((u-\lambda\, id_E)^{\ell_\lambda}\right) \oplus \ker(Q(u)) = \ker\left((u-\lambda\, id_E)^{\ell}\right) \oplus \ker(Q(u)).$$

Ceci permet d'affirmer que le polynôme $(X-\lambda)^{\ell}Q(X)$ est annulateur de u, d'où ℓ est supérieur ou égal à ℓ_λ. □

Définition 1.62 (sous-espace caractéristique d'un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, u un endomorphisme de E et λ une valeur propre de u. On appelle* ***sous-espace caractéristique*** *(ou* ***sous-espace propre généralisé****) de u associé à λ le sous-espace vectoriel*

$$N_\lambda = \ker((u-\lambda\, id_E)^{m_\lambda}),$$

où l'entier m_λ est l'ordre de multiplicité algébrique de λ.

En vertu du lemme 1.61, on a

$$\ker\left((u-\lambda\, id_E)^{\ell_\lambda-1}\right) \subsetneq \ker\left((u-\lambda\, id_E)^{\ell_\lambda}\right) = \ker\left((u-\lambda\, id_E)^{\ell_\lambda+1}\right) = \dots$$

où l'entier ℓ_λ est l'ordre de multiplicité de la valeur propre λ en tant que racine du polynôme minimal de u. Les sous-espaces $\ker\left((u-\lambda\, id_E)^{k}\right)$ coïncident donc pour toute valeur de l'entier k supérieure ou égale à ℓ_λ et on a ici choisi d'utiliser l'ordre de multiplicité algébrique m_λ dans la définition 1.62, car on sait qu'il est supérieur ou égal à ℓ_λ d'après le théorème de Cayley–Hamilton (voir le théorème 1.47). On notera que, lorsque l'endomorphisme u est diagonalisable, on a $\ell_\lambda = 1$ pour toute valeur propre λ de u et les sous-espaces caractéristiques associés sont alors des sous-espaces propres.

Définition 1.63 (vecteur propre généralisé) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, u un endomorphisme de E et λ une valeur propre de u. Un vecteur non nul x de E appartenant à l'espace caractéristique N_λ est appelé* ***vecteur propre généralisé*** *de u associé à λ. L'**ordre** d'un tel vecteur propre généralisé est l'entier naturel, non nul et inférieur ou égal à l'ordre de multiplicité ℓ_λ de λ en tant que racine du polynôme minimal de u, k tel que ce vecteur appartient à $\ker\left((u-\lambda\, id_E)^{k}\right)$ et pas à $\ker\left((u-\lambda\, id_E)^{k-1}\right)$. En particulier, tout vecteur propre de u est un vecteur propre généralisé de u d'ordre* 1.

La proposition suivante énonce des propriétés des sous-espaces caractéristiques.

Proposition 1.64 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, u un endomorphisme de E et λ une valeur propre de u d'ordre de multiplicité algébrique m_λ. Alors, le sous-espace caractéristique N_λ de u associé à λ est stable par u et* $\dim(N_\lambda) = m_\lambda$. *De plus, si le polynôme caractéristique de u est scindé, on a*

$$E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} N_\lambda.$$

DÉMONSTRATION. Puisque l'ordre de multiplicité algébrique de λ est égal à m_λ, le polynôme caractéristique de u s'écrit

$$\chi_u(X) = (X-\lambda)^{m_\lambda}Q(X),$$

avec Q un polynôme tel que $X-\lambda$ et Q sont premiers entre eux. Par le théorème de Cayley–Hamilton (voir le théorème 1.47) et le lemme de décomposition des noyaux (voir la proposition 1.58), on a alors

$$E = N_\lambda \oplus \ker(Q(u)).$$

Par ailleurs, les endomorphismes u et $(u-\lambda id_E)^{m_\lambda}$ commutent entre eux et le sous-espace caractérisitique N_λ est donc, en vertu de la proposition 1.5, stable par u. De la même manière, les endomorphismes u et $Q(u)$ commutent entre eux, d'où $\ker(Q(u))$ est stable par u. En utilisant la matrice représentative de l'endomorphisme dans une base adaptée à la décomposition de l'espace ci-dessus, on obtient ainsi que $\chi_u = \chi_{u_{|N_\lambda}}\chi_{u_{|\ker(Q(u))}}$, dont on déduit que $\chi_{u_{|N_\lambda}}$ et $\chi_{u_{|\ker(Q(u))}}$ divisent tout deux χ_u. Par définition du sous-espace N_λ, le polynôme $(X-\lambda)^{m_\lambda}$ est annulateur de $u_{|N_\lambda}$. Il en résulte que le polynôme minimal de $u_{|N_\lambda}$ est scindé et que le spectre de cet endomorphisme est réduit à $\{\lambda\}$. On en conclut que $\chi_{u_{|N_\lambda}}(X) = (X-\lambda)^{\dim(N_\lambda)}$. D'autre part, le polynôme Q est annulateur de $u_{|\ker(Q(u))}$. Le scalaire λ ne peut alors être valeur propre de $u_{|\ker(Q(u))}$ (ce serait en effet une racine de Q, ce qui contredirait le fait que $X-\lambda$ et Q sont premiers entre eux). Par l'unicité de la factorisation en polynômes irréductibles, on a alors que $\dim(N_\lambda) = m_\lambda$.

Enfin, si l'on fait l'hypothèse que le polynôme caractéristique de u est scindé, on a

$$\chi_u(X) = \prod_{\lambda\in \mathrm{Sp}(u)} (X-\lambda)^{m_\lambda},$$

la décomposition découlant alors du théorème de Cayley–Hamilton et du lemme de décomposition des noyaux généralisé (voir le corollaire 1.59) □

On peut observer que ces derniers résultats permettent de prouver qu'un endomorphisme d'un espace vectoriel de dimension finie est trigonalisable si et seulement si l'espace est somme (directe) des sous-espaces caractéristiques de cet endomorphisme, c'est-à-dire si et seulement s'il existe une base de l'espace formée de vecteurs propres généralisés de l'endomorphisme. Cette caractérisation, déjà donnée dans le tableau récapitulatif en fin de section précédente, est en effet équivalente [8] à la condition nécessaire et suffisante basée sur le polynôme caractéristique, qui énonce que ce dernier doit être scindé pour que l'endomorphisme soit trigonalisable, donnée dans le théorème 1.37.

Lorsque l'endomorphisme u est diagonalisable, la décomposition en sous-espaces caractéristiques de la proposition 1.64 correspond à une décomposition en sous-espaces propres.

1.7.2 Réduction de Jordan

Il convient tout d'abord de préciser la structure particulière des matrices représentatives à laquelle amène la réduction de Jordan.

Définitions 1.65 (bloc et forme normale de Jordan) *Soit l un entier naturel non nul. On appelle* ***bloc de Jordan de taille*** *l une matrice de $M_l(\mathbb{K})$ de la forme*

$$J_l(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix} \text{ (avec } J_1(\lambda) = \big(\lambda\big)\text{)},$$

où λ est un scalaire.
Soit n un entier naturel non nul. Une matrice de $M_n(\mathbb{K})$ est dite sous ***forme normale (ou canonique) de Jordan*** *si elle est diagonale par blocs, chaque bloc diagonal étant un bloc de Jordan, c'est-à-dire qu'il existe des entiers naturels non nuls $l_1,\dots,l_q$, vérifiant $l_1+\dots+l_q = n$, et des scalaires $\lambda_1,\dots,\lambda_q$ tels que la matrice s'écrit*

$$\begin{pmatrix} J_{l_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{l_q}(\lambda_q) \end{pmatrix}.$$

On observe qu'il découle de ces définitions qu'une matrice sous forme normale de Jordan est diagonale si et seulement si chacun de ses blocs de Jordan est de taille 1.

8. L'implication directe s'obtient en utilisant la stabilité des sous-espaces caractéristiques par l'endomorphisme u (pour montrer que $\chi_u = \prod_{\lambda\in\mathrm{Sp}(u)}\chi_{u_{|N_\lambda}}$) et le fait que $\chi_{u_{|N_\lambda}} = (X-\lambda)^{m_\lambda}$. L'implication réciproque correspond à la dernière assertion de la proposition 1.64.

On va maintenant montrer, sous les hypothèses du théorème de trigonalisabilité 1.37, qu'il existe une base dans laquelle la matrice d'un endomorphisme est sous forme normale de Jordan. Pour cela, on doit au préalable énoncer un résultat qui est un cas particulier de *décomposition de Frobenius* dans le cadre spécifique d'un endomorphisme nilpotent.

Proposition 1.66 (décomposition de Frobenius pour un endomorphisme nilpotent) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme nilpotent de E. Il existe une base dans laquelle la matrice de u est diagonale par blocs, de la forme*

$$\begin{pmatrix} J_{l_1}(0) & & \\ & \ddots & \\ & & J_{l_q}(0) \end{pmatrix},$$

où les entiers naturels $l_1, \dots, l_q$ sont non nuls et vérifient $l_1 + \cdots + l_q = \dim(E)$ et les matrices $J_{l_1}(0), \dots, J_{l_q}(0)$ sont des blocs de Jordan.

DÉMONSTRATION. On raisonne par récurrence sur la dimension de E, qu'on note n. Pour $n = 1$, le résultat est évident puisque la matrice représentative de l'endomorphisme est nulle. On suppose ensuite que, pour un entier n supérieur ou égal à 2, le résultat est vrai pour tout endomorphisme nilpotent d'un espace de dimension inférieure ou égale à $n-1$. Si l'endomorphisme u est nul, le résultat est évident. Sinon, on note l l'indice de nilpotence de u, qui est donc strictement plus grand que 1. Soit x un vecteur de E n'appartenant pas à $\ker(u^{l-1})$ et F le sous-espace vectoriel de E défini par

$$F = \mathrm{Vect}\big(\{x, u(x), \dots, u^{l-1}(x)\}\big).$$

La famille génératrice de F est libre. En effet, si l'on suppose qu'il existe des scalaires $\alpha_0, \dots, \alpha_{l-1}$ non tous nuls tels que

$$\sum_{j=0}^{l-1} \alpha_j u^j(x) = 0_E,$$

et que l'on note i le plus petit indice des coefficients non nuls, alors, en appliquant u^{l-1-i} à l'égalité ci-dessus, on obtient que $\alpha_i u^{l-1}(x) = 0_E$, ce qui est absurde. Le sous-espace F est donc de dimension l, clairement stable par u et la matrice de la restriction $u_{|_F}$ dans la base $\{u^{l-1}(x), \dots, u(x), x\}$ est le bloc de Jordan $J_l(0)$. Si $l = n$, la preuve est terminée. Sinon, on conclut à l'aide de l'hypothèse de récurrence en trouvant un supplémentaire de F, également stable par u.

On va ici construire ce supplémentaire par dualité[9]. Soit une forme linéaire φ appartenant à E^* telle que

$$\big\langle \varphi, u^{l-1}(x) \big\rangle_{E^*,E} \neq 0.$$

On définit alors le sous-espace vectoriel H de E^* par

$$H = \mathrm{Vect}\big(\{\varphi, u^\top(\varphi), \dots, (u^\top)^{l-1}(\varphi)\}\big),$$

où $u^\top$ est le transposé de l'endomorphisme u (voir la définition B.14). De la même manière qu'on l'a précédemment fait pour F, on va montrer que ce sous-espace est de dimension l. On pose pour cela $G = H^\perp$. Le sous-espace G est stable par u, puisque H est clairement stable par $u^\top$ (voir la proposition B.15). Comme $\dim(F) + \dim(G) = \dim(F) + \dim(H^\perp) = \dim(F) + n - \dim(H) = n + n - l = n$, il reste alors à montrer que l'intersection $F \cap G$ est réduite au vecteur nul, ce que l'on fait en utilisant rigoureusement la même technique que pour les dimensions de F et de H.

On dispose ainsi de deux sous-espaces F et G, stables par u et en somme directe dans E. Soit $\{e_{l+1}, \dots, e_n\}$ une base de G. On note N la matrice représentative de u dans la base canonique de E et Q la matrice de passage de la base canonique de E à $\big\{x, u(x), \dots, u^{l-1}(x), e_{l+1}, \dots, e_n\big\}$. On a alors

$$N = Q \begin{pmatrix} J_l(0) & 0_{l,n-l} \\ 0_{n-l,l} & N' \end{pmatrix} Q^{-1},$$

9. On renvoie le lecteur à l'annexe B pour des rappels sur la dualité en dimension finie.

le bloc N' correspondant à la matrice représentative de la restriction de u à G. Cette dernière matrice étant nilpotente, l'hypothèse de récurrence s'applique : il existe une matrice de passage P' d'ordre $n-l$ telle que $N' = P'J'P'^{-1}$, où la matrice J' est diagonale par blocs et constituée de blocs de Jordan adéquats. On a finalement

$$N = Q\begin{pmatrix} I_l & 0_{l,n-l} \\ 0_{n-l,l} & P' \end{pmatrix}\begin{pmatrix} J_l(0) & 0_{l,n-l} \\ 0_{n-l,l} & J' \end{pmatrix}\begin{pmatrix} I_l & 0_{l,n-l} \\ 0_{n-l,l} & P'^{-1} \end{pmatrix}Q^{-1},$$

ce qui achève la preuve. □

Remarque 1.67 *La **décomposition de Frobenius** relative à un endomorphisme u d'un $\mathbb{K}$-espace vectoriel de dimension finie non nulle est une décomposition de l'espace E en une somme directe de sous-espaces cycliques de u, que l'on peut ordonner de manière à ce que la suite finie des polynômes minimaux des restrictions respectives de u aux sous-espaces de la somme soit telle que chaque élément divise son successeur, le dernier élément est le polynôme minimal de u, et le produit des élements est le polynôme caractéristique de u. Ces polynômes ne dépendent que de l'endomorphisme et pas du choix des vecteurs générant les sous-espaces cycliques de la décomposition. Ils sont appelés les **invariants de similitude** de l'endomorphisme.*

On est maintenant en mesure de prouver l'existence de la réduction de Jordan.

Théorème 1.68 (« réduction de Jordan » [Jor70]) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et u un endomorphisme de E, dont le polynôme caractéristique est scindé sur $\mathbb{K}$. Il existe une base de l'espace dans laquelle la matrice de u est sous forme normale de Jordan, les scalaires apparaissant dans les blocs étant les valeurs propres de u.*

DÉMONSTRATION. On note $\lambda_1, \ldots, \lambda_p$ les valeurs propres deux à deux distinctes de u et $N_{\lambda_1}, \ldots, N_{\lambda_p}$ les sous-espaces caractéristiques associés. Par hypothèse sur le polynôme caractéristique de u, il découle de la proposition 1.64 que l'espace est somme directe des sous-espaces caractéristiques,

$$E = \bigoplus_{i=1}^{p} N_{\lambda_i},$$

chacun de ces sous-espace étant stable par u. Pour tout sous-espace caractéristique N_λ de u, l'endomorphisme $u_{|_{N_\lambda}} - \lambda\, id_{N_\lambda}$ est nilpotent. D'après la proposition 1.66, il existe alors une base de N_λ dans laquelle la matrice représentative de cet endomorphisme est diagonale par blocs, composée de blocs de Jordan nilpotents. On en déduit que la matrice représentative de la restriction de u à N_λ dans cette base est diagonale par blocs, composée de blocs de Jordan relatifs à la valeur propre λ. En concaténant alors les bases de vecteurs propres généralisés ainsi construites pour chacun des sous-espaces caractéristiques de u, on obtient une base de E dans laquelle la matrice de l'endomorphisme est sous la forme normale de Jordan voulue. □

Cette réduction est unique, à permutation des blocs près, au sens où le nombre et la taille des blocs de Jordan de dépendent que de l'endomorphisme. En particulier, le nombre de blocs associés à une valeur propre λ de l'endomorphisme est égal à la dimension du sous-espace propre associé à λ, la taille du plus grand bloc associé à λ est égal à l'ordre de multiplicité ℓ_λ de λ en tant que racine du polynôme minimal et la somme des tailles des blocs associés à λ est égal à l'ordre de multiplicité m_λ de λ en tant que racine du polynôme caractéristique. La détermination du nombre et des tailles respectives des blocs de Jordan associés à chacune des valeurs propres constitue par conséquent une étape essentielle de la réduction de Jordan d'un endomorphisme.

La réduction de Jordan d'une matrice en pratique

Soit M une matrice d'ordre n à coefficients dans le corps $\mathbb{K}$.

1. Calculer le polynôme caractéristique χ_M, trouver ses racines et une factorisation associée du polynôme pour obtenir les valeurs propres avec leurs ordres de multiplicité algébrique respectifs. Si le polynôme caractéristique n'est pas scindé, la réduction sous forme normale de Jordan n'est pas possible.
2. Si le polynôme caractéristique est scindé, déterminer pour chaque valeur propre λ la dimension n_λ du sous-espace propre qui lui est associé, en utilisant par exemple la détermination du rang de la matrice $M - \lambda I_n$. Le nombre de blocs de Jordan associés à λ est égal n_λ.
3. Pour chaque valeur propre λ, obtenir la taille de chacun des n_λ blocs de Jordan associés à λ. Pour cela, on commence par déterminer successivement les rangs (décroissants, en vertu du lemme 1.61)

respectifs des matrices de la famille $M-\lambda I_n, (M-\lambda I_n)^2, \dots, (M-\lambda I_n)^{\ell_\lambda}$, l'entier ℓ_λ étant celui pour lequel le rang vaut $n-m_\lambda$, avec m_λ l'ordre de multiplicité algébrique de λ. On calcule ensuite les entiers

$$\forall k \in \{1,\dots,\ell_\lambda\},\ r_k = \operatorname{rang}((M-\lambda I_n)^{k-1}) - \operatorname{rang}((M-\lambda I_n)^k).$$

qui correspondent[a] respectivement au nombre de blocs de taille au moins égale à k associés à λ, la taille des plus grands blocs étant égale à ℓ_λ, qui se trouve être l'ordre de multiplicité de λ en tant que racine du polynôme minimal. On en déduit, par soustraction, combien de blocs de chaque taille sont associés à λ.

4. Il reste à trouver des vecteurs propres généralisés associés à chaque bloc de Jordan. Pour chaque valeur propre λ et pour chaque bloc qui lui est associé, on construit des *chaînes* de vecteurs de la manière suivante.

   Pour un bloc de taille k, on commence par trouver un vecteur propre généralisé V_k d'ordre k, c'est-à-dire tel que $(M-\lambda I_n)^k V_k = 0_{M_{n,1}(\mathbb{K})}$ et $(M-\lambda I_n)^{k-1} V_k \neq 0_{M_{n,1}(\mathbb{K})}$. Si des vecteurs propres généralisés ont déjà été obtenus pour d'autres blocs de Jordan associés à la même valeur propre, on s'assure que V_k n'est pas linéairement lié à ces derniers. On détermine ensuite les vecteurs de la chaîne en posant $V_{k-1} = (M-\lambda I_n)V_k, \dots, V_1 = (M-\lambda I_n)V_2$. Le vecteur V_i de la chaîne est un vecteur propre généralisé d'ordre i associé à λ et l'ensemble es vecteurs $V_1,\dots,V_k$ de la chaîne forme une famille libre.
   La réunion de toutes les familles de vecteurs propres généralisés ainsi construites est une base de $M_{n,1}(\mathbb{K})$ dans laquelle la matrice de l'endomorphisme canoniquement associé à M est sous forme réduite de Jordan.

a. On peut remarquer, en utilisant le théorème du rang, que l'on a encore $r_k = \dim(\ker((M-\lambda I_n)^k)) - \dim(\ker((M-\lambda I_n)^{k-1}))$. L'ensemble de ces quantités constitue par conséquent une partition de l'entier m_λ, au sens où $\sum_{k=1}^{\ell_\lambda} r_k = m_\lambda$, ce qui permet encore de faire appel à des objets combinatoires utilisés en théorie des représentations des groupes, les *tableaux*, ou *diagrammes*, *de Young* pour déterminer la taille des blocs de Jordan.

Exemple 1.69 *On considère le calcul d'une réduction de Jordan de la matrice*

$$M = \begin{pmatrix} 4 & 3 & -2 \\ -3 & -1 & 3 \\ 2 & 3 & 0 \end{pmatrix}.$$

On calcule tout d'abord le polynôme caractéristique de M. On trouve, après calculs,

$$\chi_M(X) = \begin{vmatrix} X-4 & -3 & 2 \\ 3 & X+1 & -3 \\ -2 & -3 & X \end{vmatrix} = (X+1)(X-2)^2.$$

Ce polynôme est scindé sur $\mathbb{R}$, la réduction de la matrice M sous forme normale de Jordan est donc réalisable sur $\mathbb{R}$, et les valeurs propres -1 et 2 ont respectivement un ordre de multiplicité égal à 1 et 2. On détermine alors les sous-espaces propres de M. On considère tout d'abord $E_{-1} = \ker(M+I_3)$. On a

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in E_{-1} \iff MX = -X \iff \begin{cases} 4x_1 + 3x_2 - 2x_3 = -x_1 \\ -3x_1 - x_2 + 3x_3 = -x_2 \\ 2x_1 + 3x_2 = -x_3 \end{cases} \iff x_1 = -x_2 = x_3,$$

d'où E_{-1} est une droite vectorielle dont, par exemple, le vecteur propre $V_1 = \begin{pmatrix} 1 & -1 & 1 \end{pmatrix}^\top$ est une base. La valeur propre -1 est associée à un bloc de Jordan de taille 1. On s'intéresse ensuite à $E_2 = \ker(M-2I_3)$. On a

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in E_2 \iff MX = 2X \iff \begin{cases} 4x_1 + 3x_2 - 2x_3 = 2x_1 \\ -3x_1 - x_2 + 3x_3 = 2x_2 \\ 2x_1 + 3x_2 = 2x_3 \end{cases} \iff x_1 = x_3 \text{ et } x_2 = 0,$$

d'où E_2 est une droite vectorielle dont, par exemple, le vecteur propre $V_2 = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}^\top$ est une base. Puisque la dimension de ce sous-espace propre n'est pas égale à l'ordre de multiplicité de la valeur propre associée, la matrice M n'est pas diagonalisable et la valeur propre 2 est nécéssairement associée à un bloc de Jordan de taille 2.

Pour trouver un vecteur propre généralisé V_3 d'ordre 2 associé à 2, il suffit ici de remarquer qu'il sera tel que $(M-2I_3)V_3 = V_2$. En posant $V_3 = \begin{pmatrix} x & y & z \end{pmatrix}^\top$, il vient

$$(M-2I_3)V_3 = V_2 \iff \begin{pmatrix} 2 & 3 & -2 \\ -3 & -3 & 3 \\ 2 & 3 & -2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \iff \begin{cases} 2x+3y-2z = 1 \\ -3x-3y+3z = 0 \\ 2x+3y-2z = 1 \end{cases}$$

$$\iff \begin{cases} 2x+3y-2z = 1 \\ x+y-z = 0 \end{cases} \iff \begin{cases} 2x+3y = 1+2z \\ x+y = z \end{cases} \iff \begin{cases} y = 1 \\ x = z-1 \end{cases}.$$

En prenant par exemple $z = 1$, on trouve $V_3 = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}^\top$. L'endomorphisme canoniquement associé à la matrice M est ainsi représenté dans la base associée à la famille (V_1, V_2, V_3) par la matrice

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

En notant P la matrice de passage correspondante,

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

on a trouvé que $M = PJP^{-1}$, avec

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

Exemple 1.70 *Dans cet exemple, tiré de [Bro91], on considère une réduction de Jordan de la matrice*

$$M = \begin{pmatrix} 2 & 1 & -1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

La matrice étant triangulaire, il est inutile de calculer le polynôme caractéristique pour déterminer les valeurs propres de M, qui sont 2, avec un ordre de multiplicité égal à 5, et 4, avec un ordre de multiplicité égal à 1. La matrice

$$M - 2I_6 = \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

a pour rang 4, la matrice

$$(M - 2I_6)^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

a pour rang 2 *et la matrice*

$$(M-2I_6)^3=\begin{pmatrix}0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&0&0&0&2\\0&0&0&0&0&4\\0&0&0&0&0&8\end{pmatrix}$$

a pour rang $1(=6-5)$. *Il y aura donc deux* $(=6-4)$ *blocs de Jordan associés à la valeur propre* 2*, le plus grand de ces blocs étant de taille* 3*, et un bloc de Jordan de taille* 1 *associé à la valeur propre* 4.

Pour déterminer la taille du second bloc associé à 2*, on calcule* $r_3=2-1=1$, $r_2=4-2=2$ *et* $r_1=6-4=2$. *On en déduit qu'il y a donc un bloc de taille au moins égale à* 3*, deux blocs de taille au moins égale à* 2 *et deux blocs de taille au moins égale à* 1*, ce qui correspond à un bloc de taille égale à* 3 *et un* $(=2-1)$ *bloc de taille égale à* 2 *(et zéro* $(=2-2)$ *bloc de taille égale à* 1*).*

On obtient à présent les vecteurs propres généralisés associés à la valeur propre 2*, en commençant par celui d'ordre* 3. *On cherche tout d'abord un vecteur* V_3 *de* $M_{6,1}(\mathbb{R})$ *tel que* $(M-2I_6)^3V_3=0_{M_{6,1}(\mathbb{R})}$ *et* $(M-2I_6)^2V_3\neq 0_{M_{6,1}(\mathbb{R})}$*, par exemple* $V_3=\begin{pmatrix}0&0&1&0&0&0\end{pmatrix}^\top$*, et l'on obtient les vecteurs propres généralisés d'ordres respectifs* 2 *et* 1 *de la chaîne correspondante,*

$$V_2=(M-2I_6)V_3=\begin{pmatrix}-1\\1\\0\\0\\0\\0\end{pmatrix},\ V_1=(M-2I_6)V_2=\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}.$$

Un second vecteur propre généralisé d'ordre 2 *associé à* 2 *est nécessaire pour le second bloc de Jordan (de taille* 2*) associé à cette valeur propre. On détermine donc un vecteur* V_2' *de* $M_{6,1}(\mathbb{R})$*, linéairement indépendant des vecteurs* V_1*,* V_2 *et* V_3 *déjà obtenus, tel que* $(M-2I_6)^2V_2'=0_{M_{6,1}(\mathbb{R})}$ *et* $(M-2I_6)V_2'\neq 0_{M_{6,1}(\mathbb{R})}$*, par exemple* $V_2'=\begin{pmatrix}0&0&0&0&1&0\end{pmatrix}^\top$*, et l'on obtient le dernier vecteur de la chaîne en posant*

$$V_1'=(M-2I_6)V_2'=\begin{pmatrix}0\\0\\0\\1\\0\\0\end{pmatrix}.$$

Il reste à déterminer le vecteur propre généralisé associé à la valeur propre 4*, qui est d'ordre* 1 *et se trouve donc être un vecteur propre associé à* 4*. On peut par exemple choisir le vecteur* $W_1=\begin{pmatrix}0&0&0&1&2&4\end{pmatrix}^\top$.

L'endomorphisme canoniquement associé à la matrice M *est ainsi représenté dans la base associée à la famille* $(V_1,V_2,V_3,V_1',V_2',W_1)$ *par la matrice*

$$J=\begin{pmatrix}2&1&0&0&0&0\\0&2&1&0&0&0\\0&0&2&0&0&0\\0&0&0&2&1&0\\0&0&0&0&2&0\\0&0&0&0&0&4\end{pmatrix}.$$

En notant P *la matrice de passage correspondante,*

$$P=\begin{pmatrix}1&-1&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&1\\0&0&0&0&1&2\\0&0&0&0&0&4\end{pmatrix},$$

on a trouvé que $M = PJP^{-1}$*, avec*

$$P^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 0 & 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{4} \end{pmatrix}.$$

1.7.3 Décomposition de Jordan–Chevalley

On donne enfin un résultat de décomposition d'endomorphisme que l'on nomme parfois *décomposition de Dunford*, en raison de la décomposition du même type introduite dans l'article [Dun54].

Théorème 1.71 (« décomposition de Jordan–Chevalley » d'un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E dont le polynôme caractéristique est scindé sur $\mathbb{K}$. Alors, il existe un unique couple (s,n) d'endomorphismes de E, avec s diagonalisable et n nilpotent, tels que $u = s+n$, $n \circ s = s \circ n$.*

DÉMONSTRATION. On observe tout d'abord que si $u = s+n$, alors $n = u-s$ et il suffit donc de montrer que l'endomorphisme s est entièrement déterminé par u. Pour cela, on note $\lambda_1, \dots, \lambda_p$ les valeurs propres deux à deux distinctes de u, $m_{\lambda_1}, \dots, m_{\lambda_p}$ les ordres de multiplicité algébrique associés et $N_{\lambda_1}, \dots, N_{\lambda_p}$ les sous-espaces caractéristiques associés. On définit alors s comme l'endomorphisme de E dont la restriction à chaque sous-espace N_{λ_i}, $i = 1, \dots, p$, est l'homothétie de rapport λ_i. Par hypothèse sur le polynôme caractéristique de u, il découle de la proposition 1.64 que $E = \bigoplus_{i=1}^{p} N_{\lambda_i}$ et s est ainsi défini sur l'espace E tout entier. Il reste à vérifier que les endomorphismes s et n ainsi définis satisfont aux propriétés énoncées.

Tout d'abord, l'endomorphisme s est diagonalisable, dans une base formée de vecteurs propres généralisés de u, par construction.

Ensuite, les sous-espaces caractéristiques de u étant à la fois stables par s (par la définition même de cet endomorphisme) et par u (voir la proposition 1.64), ils sont stables par n. On a alors

$$\forall i \in \{1, \dots, p\}, n_{|_{N_{\lambda_i}}} = (u-s)_{|_{N_{\lambda_i}}} = u_{|_{N_{\lambda_i}}} - \lambda_i \, id_{N_{\lambda_i}},$$

dont on déduit que, pour tout i de $\{1, \dots, p\}$, $N_{\lambda_i} = \ker\left((n_{|_{N_{\lambda_i}}})^{m_i} \right)$ et donc que $(n_{|_{N_{\lambda_i}}})^{m_i} = 0_{\mathscr{L}(N_{\lambda_i})}$. En posant $m = \max_{i \in \{1,\dots,p\}} m_i$, on obtient que n^m est l'endomorphisme nul sur chaque sous-espace caractéristique de u, c'est-à-dire que $n^m = 0_{\mathscr{L}(E)}$, ce qui prouve que n est nilpotent.

La restriction de l'endomorphisme s à tout sous-espace caractéristique de u étant définie comme une homothétie, elle commute avec tout autre endomorphisme de ce sous-espace. C'est en particulier le cas avec la restriction de l'endomorphisme n à ce sous-espace, puisque l'on a vu que chaque sous-espace caractéristique de u était stable par n. En utilisant que tout vecteur de E peut s'écrire comme une somme d'éléments appartenant respectivement aux sous-espaces caractéristiques de u, il en résulte alors que

$$\forall x \in E,\ s \circ n(x) = s \circ n\left(\sum_{i=1}^{p} x_i \right) = \sum_{i=1}^{p} s \circ n(x_i) = \sum_{i=1}^{p} n \circ s(x_i) = n \circ s\left(\sum_{i=1}^{p} x_i \right) = n \circ s(x),$$

d'où s et n commutent.

Pour montrer que cette décomposition de l'endomorphisme u est unique, on suppose qu'il existe un autre couple (s', n') d'endomorphismes de E vérifiant les différentes propriétés de la décomposition. On a

$$s' \circ u = s' \circ (s'+n') = (s')^2 + s' \circ n' = (s')^2 + n' \circ s' = (s'+n') \circ s' = u \circ s',$$

d'où u et s' commutent entre eux (on montre de la même façon que u et s commutent entre eux). On observe alors que, pour tout vecteur x de N_{λ_i}, avec i appartenant à $\{1, \dots, p\}$,

$$(u - \lambda_i \, id_E)^{m_i} \circ s'(x) = s' \circ (u - \lambda_i \, id_E)^{m_i}(x) = s'(0_E) = 0_E,$$

d'où N_{λ_i} est stable par s'. Il en découle que s commute avec s' sur chaque sous-espace caractéristique de u, et donc sur l'espace E tout entier. Ces deux endomorphismes étant diagonalisables, il existe, en vertu du lemme 1.34,

une base commune de diagonalisation, ce qui implique que l'endomorphisme $s-s'$ est diagonalisable. On voit de même que n' et n commutent entre eux et l'on peut donc utiliser la formule du binôme pour calculer $(n'-n)^k$ pour un entier naturel k supérieur ou égal à $2\dim(E)$. On a

$$(n'-n)^k = \sum_{i=0}^{k} \binom{k}{i} (n')^i \circ (-n)^{k-i}.$$

Pour tout entier i de $\{0,\dots,k\}$, l'un des deux entiers i et $k-i$ est nécessairement supérieur ou égal à $\dim(E)$, ce qui fait que l'endomorphisme $(n')^i \circ (-n)^{k-i}$ est nul. L'endomorphisme $n'-n$ est par conséquent nilpotent. Il en résulte que l'endomorphisme $s-s' = n'-n$ est à la fois diagonalisable et nilpotent, c'est donc l'endomorphisme nul. □

On notera que l'endomorphisme u est diagonalisable si et seulement si l'endomorphisme n est nul dans cette décomposition.

Remarque 1.72 *Ce théorème est un cas particulier d'un résultat dû à Claude Chevalley, qui apparaît dans le premier chapitre de l'ouvrage [Che51] traitant de la théorie des groupes algébriques. Dans ce dernier, on considère un endomorphisme u d'un espace vectoriel de dimension finie sur un corps* parfait $\mathbb{K}$*, l'élément s de la décomposition est* semi-simple*, c'est-à-dire que tout sous-espace stable par s admet un supplémentaire stable par s, et l'on montre que s et n peuvent être représentés comme des polynômes en u à coefficients dans* $\mathbb{K}$*. Un élément marquant de la preuve de Chevalley est qu'elle repose sur un calcul effectif de la décomposition basé sur la méthode de Newton–Raphson et qui ne nécessite pas la connaissance des valeurs propres de l'endomorphisme considéré. Le lecteur intéressé pourra consulter les articles [CEZ11, CEZ16] pour plus de détails.*

Remarque 1.73 *Il existe une version multiplicative de ce résultat lorsque l'application u est un automorphisme. L'endomorphisme s est en effet inversible dans ce cas et, en posant alors* $v = id_E + s^{-1} \circ n$*, on obtient sous les mêmes hypothèses que* $u = s \circ v$*, avec s diagonalisable et v unipotent*[10]*, commutant avec s. Cette factorisation joue un rôle important dans la théorie des groupes algébriques.*

On peut encore énoncer ce résultat sous forme matricielle.

Corollaire 1.74 (« décomposition de Jordan–Chevalley » d'une matrice) *Soit n un entier naturel non nul et M une matrice d'ordre n à coefficients dans le corps* $\mathbb{K}$*, dont le polynôme caractéristique est scindé. Il existe une matrice S diagonalisable et une matrice N nilpotente telles que*

$$M = S + N \text{ et } SN = NS,$$

cette décomposition étant unique.

On notera qu'il est possible de combiner ce dernier résultat avec la décomposition de Frobenius pour un endomorphisme nilpotent (voir le théorème 1.66) pour prouver l'existence de la réduction de Jordan.

La décomposition de Jordan–Chevalley d'une matrice en pratique

Soit M une matrice d'ordre n à coefficients dans le corps $\mathbb{K}$.

1. Calculer le polynôme caractéristique χ_M, trouver ses racines et une factorisation associée du polynôme pour obtenir les valeurs propres pour obtenir les valeurs propres avec leurs ordres de multiplicité algébrique respectifs. Si le polynôme caractéristique n'est pas scindé, la décomposition n'existe pas.
2. Si le polynôme caractéristique est scindé, déterminer pour chaque valeur propre le sous-espace caractéristique qui lui est associé. Ce faisant, s'assurer que la matrice n'est pas diagonalisable (si ce n'est pas le cas, la décomposition est triviale puisque sa partie nilpotente est nulle).
3. Si la matrice n'est pas diagonalisable, construire la matrice S de la partie diagonalisable de la décomposition en utilisant une base de $M_{n,1}(\mathbb{K})$ formée de vecteurs propres généralisés de M et le fait que la restriction de cet endomorphisme au sous-espace caractéristique N_λ est une homothétie de rapport λ. En notant $\lambda_1,\dots,\lambda_n$ les valeurs propres de M comptées avec leur ordre de multiplicité et P la matrice

10. Un endomorphisme v de E est dit *unipotent* si l'endomorphisme $v - id_E$ est nilpotent.

dont les colonnes sont les vecteurs propres généralisés correspondants, cette matrice est telle que

$$S = P\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)P^{-1}.$$

4. Obtenir la matrice N de la partie nilpotente de la décomposition en utilisant que $N = M - S$.

Exemple 1.75 *On considère le calcul de la décomposition de Jordan–Chevalley de la matrice*

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 3 & -4 \\ 3 & 1 & -2 \end{pmatrix}.$$

On calcule tout d'abord le polynôme caractéristique de M pour trouver $\chi_M(X) = (X+1)(X-2)^2$. Les valeurs propres -1 et 2 ont respectivement un ordre de multiplicité algébrique égal à 1 et 2. On détermine ensuite les sous-espaces propres de M. Après calculs, on obtient que les sous-espaces propres E_{-1} et E_2 sont respectivement engendrés par

$$V_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \text{ et } V_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

et la matrice M n'est donc pas diagonalisable. Pour obtenir une base du sous-espace caractéristique N_2, qui est de dimension 2, on conserve le vecteur propre V_2 engendrant E_2 et l'on cherche un vecteur V_3, appartenant à $\ker((A-2I_3)^2)$ et linéairement indépendant de V_2. On peut par exemple choisir $V_3 = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}^\top$.

La matrice de passage P s'écrit alors

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

et l'on définit la matrice S comme $S = PDP^{-1}$, où

$$D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ et } P^{-1} = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix},$$

le calcul de l'inverse de P se faisant, par exemple, par le procédé d'élimination de Gauss–Jordan. On a finalement

$$S = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 2 & -3 \\ 3 & 0 & -1 \end{pmatrix} \text{ et } N = M - S = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix}.$$

On sait déjà que S est diagonalisable. On peut vérifier que $N^2 = 0$ et que $SN = NS$.

1.8 Quelques applications de la réduction

On présente dans cette dernière partie quelques applications notables de la réduction des endomorphismes et des matrices.

1.8.1 Calcul des puissances d'une matrice

Étant donné un entier naturel n non nul et une matrice M de $M_n(\mathbb{K})$, on est parfois amené, pour diverses raisons[11], à devoir calculer les puissances positives de M. Connaître une matrice M', semblable à M et pour laquelle le calcul des puissances s'avère plus simple que celui des puissances de M, peut alors être un moyen de résoudre ce problème. Il est en effet élémentaire de montrer, en raisonnant par récurrence, que, si l'on a $M = PM'P^{-1}$, alors, pour tout entier naturel k, on a $M^k = PM'^kP^{-1}$ et l'on se trouve donc ramené au calcul des puissances de M'. On va a présent montrer que, si la matrice M' est diagonale (c'est le cas lorsque M est diagonalisable) ou encore la somme d'une matrice diagonale et d'une matrice nilpotente commutant entre elles (c'est le cas lorsque M est trigonalisable), ce calcul est *a priori* bien plus aisé qu'il ne l'est pour M.

11. Un exemple sera donné en fin de sous-section.

Cas où la matrice est diagonalisable

On suppose tout d'abord que la matrice M est diagonalisable[12]. On détermine alors les valeurs propres de M et une base de vecteurs propres associés, ce qui fournit une une matrice inversible P et une matrice diagonale D telles que $M = PDP^{-1}$, avec

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}.$$

Il vient immédiatement que

$$\forall k \in \mathbb{N},\ D^k = \begin{pmatrix} {\lambda_1}^k & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & {\lambda_n}^k \end{pmatrix},$$

et le calcul d'une puissance de M se résume alors à celui de l'inverse de P et suivi de celui de deux produits de matrices.

Exemple 1.76 *On considère le calcul des puissances de la matrice*

$$M = \begin{pmatrix} -1 & 4 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

On calcule tout d'abord le polynôme caractéristique de M pour trouver $\chi_M(X) = (X+2)(X-3)^2$. Les valeurs propres -2 et 3 ont respectivement un ordre de multiplicité algébrique égal à 1 et 2. On détermine ensuite les sous-espaces propres de M. Après calculs, on obtient

$$E_{-2} = \mathrm{Vect}\left(\left\{\begin{pmatrix} -4 \\ 1 \\ 0 \end{pmatrix}\right\}\right) \text{ et } E_3 = \mathrm{Vect}\left(\left\{\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}\right),$$

et la matrice M est donc diagonalisable. On peut alors former la matrice de passage P et la matrice diagonale D associées,

$$P = \begin{pmatrix} -4 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

de sorte à avoir $M = PDP^{-1}$. Il reste à calculer l'inverse de P (en utilisant par exemple le procédé d'élimination de Gauss–Jordan),

$$P^{-1} = \frac{1}{5}\begin{pmatrix} -1 & 1 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

pour arriver à

$$\forall k \in \mathbb{N},\ M^k = \begin{pmatrix} -4 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} (-2)^k & 0 & 0 \\ 0 & 3^k & 0 \\ 0 & 0 & 3^k \end{pmatrix}\frac{1}{5}\begin{pmatrix} -1 & 1 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} = \frac{1}{5}\begin{pmatrix} 4(-2)^k + 3^k & 4(3^k - (-2)^k) & 0 \\ 3^k - (-2)^k & (-2)^k + 4 \times 3^k & 0 \\ 0 & 0 & 5 \times 3^k \end{pmatrix}.$$

Remarque 1.77 *Lorsque la matrice M est de plus inversible, on notera que cette technique permet de calculer l'inverse de M ou, plus généralement, toute puissance* négative *de M.*

12. Si la matrice est à coefficients réels, il se peut qu'elle soit diagonalisable dans $\mathbb{C}$, mais pas dans $\mathbb{R}$. En pratique, rien n'empêche de la considérer comme une matrice à coefficients complexes pour le calcul des puissances, le résultat étant bien entendu une matrices à coefficients réels.

Cas où la matrice est seulement trigonalisable

Dans le cas où la matrice M est trigonalisable, mais pas diagonalisable, la décomposition de Jordan–Chevalley est utile [13]. D'après le théorème 1.71, cette dernière permet d'écrire que $M = S + N$, avec S une matrice diagonalisable et N une matrice nilpotente telles que $SN = NS$, ce qui autorise l'emploi de la formule du binôme :

$$\forall k \in \mathbb{N},\ M^k = \sum_{l=0}^{k} \binom{k}{l} S^l N^{k-l}.$$

La matrice N étant nilpotente, la somme ci-dessus contient au plus un nombre de termes égal à l'indice de nilpotence de N, le calcul des puissances de S étant par ailleurs « simple », puisque cette matrice est diagonalisable. En pratique, la méthode de détermination de la décomposition de M proposée dans la sous-section 1.7.3 fait que la matrice de passage P vers la base de diagonalisation est connue et l'on a donc intéret à poser

$$S = PDP^{-1} \text{ et } N = PN'P^{-1},$$

afin de travailler avec la matrice diagonale D et la matrice nilpotente N'. On a

$$\forall k \in \mathbb{N},\ M^k = P\left(\sum_{l=0}^{k} \binom{k}{l} D^l N'^{k-l}\right) P^{-1}.$$

Dans le pire des cas, il faudra considérer les $n-1$ premières puissances de la matrice N' pour évaluer cette expression.

Exemple 1.78 *On considère la matrice M de l'exemple 1.75, pour laquelle la décomposition de Jordan–Chevalley a été calculée. On a $M = S + N$, avec*

$$S = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 2 & -3 \\ 3 & 0 & -1 \end{pmatrix} \text{ et } N = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix},$$

et l'on connaît la matrice de passage P qui rend S diagonale,

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \text{ et } D = P^{-1}SP = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

On a

$$N' = P^{-1}NP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix},$$

avec $N'^2 = 0$. La formule du binôme ne contient donc dans ce cas que deux termes, d'où

$$\forall k \in \mathbb{N},\ M^k = P\left(D^k + \binom{k}{1} D^{k-1}N'\right)P^{-1} = P\left(D^k + kD^{k-1}N'\right)P^{-1}$$
$$= \begin{pmatrix} 2^k & k2^{k-1} & -k2^{k-1} \\ 2^k - (-1)^k & k2^{k-1} + 2^k & -k2^k - 2^k + (-1)^k \\ 2^k - (-1)^k & k2^{k-1} & -k2^k + (-1)^k \end{pmatrix}.$$

Application aux suites récurrentes linéaires à coefficients constants

Une application directe du calcul des puissances d'une matrice est celle de la détermination de l'expression du terme général d'une suite récurrente linéaire à coefficients constants.

13. On peut tout aussi bien se servir de la réduction de Jordan de la matrice, la structure diagonale par blocs de la forme normale de Jordan faisant que sa partie diagonale et sa partie nilpotente commutent entre elles.

Soit n un entier naturel non nul. Une *suite récurrente linéaire d'ordre n à coefficients constants* sur le corps $\mathbb{K}$ est une suite $(u_k)_{k\in\mathbb{N}}$ définie par la relation de récurrence

$$\forall k \in \mathbb{N},\ u_{k+n} + a_{n-1}u_{k+n-1} + \cdots + a_0 u_k = 0, \tag{1.4}$$

les termes $u_0, \ldots, u_{n-1}$ étant donnés et où $a_0, \ldots, a_{n-1}$ sont des scalaires, avec a_0 supposé non nul. Les suites récurrentes linéaires d'ordre 1 sont les suites géométriques.

On note $S_n(\mathbb{K})$ l'ensemble des suites vérifiant la relation de récurrence (1.4). Cette dernière relation étant linéaire, il est clair que $S_n(\mathbb{K})$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$. De plus, ce sous-espace est de dimension n. En effet, si l'on introduit l'application linéaire qui à toute suite $(u_k)_{k\in\mathbb{N}}$ de $S_n(\mathbb{K})$ associe le n-uplet $(u_0, \ldots, u_{n-1})$, on observe que cette application est bijective : la connaissance des n premiers termes d'une suite est nécessaire et suffisante pour déterminer entièrement celle-ci.

On peut ainsi chercher à déterminer l'expression du terme général u_k d'une suite à valeurs complexes (pour simplifier) en fonction de l'entier k, pour k plus grand que n. Pour cela, il convient tout d'abord de poser

$$\forall k \in \mathbb{N},\ U_k = \begin{pmatrix} u_k \\ u_{k+1} \\ \vdots \\ u_{k+n-1} \end{pmatrix}.$$

La relation de récurence (1.4) se réécrit alors matriciellement

$$\forall k \in \mathbb{N},\ U_{k+1} = MU_k,$$

avec

$$M = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & 1 \\ -a_0 & -a_1 & \ldots & \ldots & -a_{n-1} \end{pmatrix},$$

de sorte que le problème de détermination se ramène à celui du calcul des puissances de la matrice M, puisque

$$\forall k \in \mathbb{N},\ U_k = M^k U_0.$$

Remarque 1.79 *L'équation polynomiale de degré n*

$$r^n + a_{n-1}r^{n-1} + \cdots + a_0 = 0$$

*est appelée l'**équation caractéristique** associée à la relation de récurrence* (1.4)*. Cette dénomination s'explique en remarquant que la matrice M est une matrice* compagnon [14]*, dont le polynôme associé définit l'équation caractéristique.*

Lorsque la matrice M est diagonalisable, ce qui est le cas si et seulement si son polynôme caractéristique est (scindé et) à racines simples [15], on obtient que la suite récurrente linéaire est une combinaison linéaire de n suites géométriques ayant pour raisons respectives les n valeurs propres distinctes de M, les coefficients de cette combinaison étant obtenus en résolvant un système linéaire construit à partir de la donnée des n premiers termes de la suite.

Dans le cas figure où la matrice M possède au moins une valeur propre multiple, elle n'est que trigonalisable. On utilise alors le théorème 1.68 : il existe une matrice inversible P et une matrice J sous forme normale de Jordan

14. On pourra comparer sa transposée avec la matrice compagnon définie par (1.3) et conclure par propriété du déterminant.

15. On peut en effet montrer que le polynôme caractéristique d'une matrice compagnon est aussi son polynôme minimal. Pour cela, il suffit de considérer l'endomorphisme u de $\mathbb{K}^n$ canoniquement associé à la matrice M. Celui-ci est tel que $u(e_1) = e_2, \ldots, u(e_{n-1}) = e_n$, d'où $e_i = u^{i-1}(e_1)$ pour tout entier i de $\{1, \ldots, n\}$. Il en résulte que, pour tout polynôme Q de $\mathbb{K}[X]$, avoir $Q(u) = 0_{\mathscr{L}(\mathbb{K}^n)}$ équivaut à avoir $Q(u)(e_1) = 0_{\mathbb{K}^n}$. Cette dernière relation est clairement vérifiée pour $Q(X) = \chi_M(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, mais elle ne l'est pas pour un polynôme non nul de degré strictement inférieur à n, et donc $\mu_M = \chi_M$.

telles que la matrice M s'écrit $M = PJP^{-1}$. Pour un bloc de Jordan de taille l (strictement plus grande que 1) de J, la formule du binôme donne [16]

$$\forall k \in \mathbb{N},\ J_l(\lambda)^k = \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \dots & \binom{k}{l-1}\lambda^{k-l+1} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \binom{k}{1}\lambda^{k-1} \\ 0 & \dots & 0 & \lambda^k \end{pmatrix}.$$

La valeur λ étant non nulle [17], il est possible de la factoriser et l'on en déduit que les coefficients du bloc $J_l(\lambda)^k$ sont de la forme $Q(k)\lambda^k$, avec Q un polynôme à coefficients complexes de degré strictement inférieur à l, pour tout entier naturel k

En considérant tour à tour chaque bloc de Jordan de J, on obtient ainsi que le terme général de la suite $(u_k)_{k\in\mathbb{N}}$ est de la forme

$$\forall k \in \mathbb{N},\ u_k = \sum_{\lambda \in \mathrm{Sp}(M)} Q_\lambda(k)\lambda^k,$$

où le polynôme Q_λ est de degré strictement inférieur à la taille du plus grand bloc de Jordan associé à la valeur propre λ.

On peut illustrer ce résultat en considérant le cas des suites récurrentes linéaires d'ordre 2. Soit la suite $(u_k)_{k\in\mathbb{N}}$ de $\mathbb{C}^{\mathbb{N}}$ vérifiant la relation de récurrence linéaire à coefficients constants

$$\forall k \in \mathbb{N},\ u_{k+2} + a_1 u_{k+1} + a_0 u_k = 0, \tag{1.5}$$

les termes u_0 et u_1 étant donnés, où a_0 et a_1 sont des nombres complexes, avec a_0 supposé non nul. L'équation caractéristique associée à (1.5) est $X^2 + a_1 X + a_0 = 0$, de discriminant ${a_1}^2 - 4a_0$. Deux cas se présentent.

— Si ${a_1}^2 - 4a_0 \neq 0$, l'équation caractéristique admet deux racines distinctes non nulles λ_1 et λ_2. Il existe alors des nombres complexes α et β, solutions du système linéaire

$$\begin{cases} \alpha + \beta = u_0, \\ \lambda_1\alpha + \lambda_2\beta = u_1, \end{cases}$$

tels que

$$\forall k \in \mathbb{N},\ u_k = \alpha {\lambda_1}^k + \beta {\lambda_2}^k.$$

— Si ${a_1}^2 - 4a_0 = 0$, l'équation caractéristique admet une racine d'ordre de multiplicité double non nulle λ. Il existe alors [18] des nombres complexes α et β, solutions du système linéaire

$$\begin{cases} \alpha = u_0, \\ \lambda\alpha + \lambda\beta = u_1, \end{cases}$$

tels que

$$\forall k \in \mathbb{N},\ u_k = (\alpha + \beta k)\lambda^k.$$

Remarque 1.80 *Si les coefficients a_0 et a_1 sont réels, on peut facilement adapter le résultat précédent. Si $(u_k)_{k\in\mathbb{N}}$ est une suite réelle vérifiant la relation* (1.5)*, on a les alternatives suivantes.*

— *Si ${a_1}^2 - 4a_0 > 0$, l'équation caractéristique admet deux racines réelles non nulles distinctes λ_1 et λ_2 et il existe alors des nombres réels α et β tels que*

$$\forall k \in \mathbb{N},\ u_k = \alpha {\lambda_1}^k + \beta {\lambda_2}^k.$$

— *Si ${a_1}^2 - 4a_0 = 0$, l'équation caractéristique admet une racine réelle double λ et il existe alors des nombres réels α et β tels que*

$$\forall k \in \mathbb{N},\ u_k = (\alpha + \beta k)\lambda^k.$$

16. On utilise la convention que le coefficient binomial $\binom{n}{k}$ est nul si l'entier naturel k est strictement supérieur à l'entier naturel n.

17. Toute valeur propre de la matrice M est non nulle du fait de l'hypothèse $a_0 \neq 0$.

18. Dans ce cas particulier, la forme normale de Jordan associée à la matrice compagnon est constituée d'un unique bloc de Jordan de taille 2. L'expression du terme général de la suite fait donc intervenir un polynôme de degré 1 en k.

— *Si* ${a_1}^2 - 4a_0 < 0$*, l'équation caractéristique admet deux racines complexes non nulles conjuguées* $re^{i\theta}$ *et* $re^{-i\theta}$ *et il existe alors des nombres réels* α *et* β *tels que*

$$\forall k \in \mathbb{N},\ u_k = (\alpha\cos(k\theta) + \beta\sin(k\theta))\, r^k.$$

Pour montrer le dernier point, on peut utiliser que l'ensemble des suites récurrentes réelles linéaires d'ordre 2 *est un espace vectoriel réel de dimension* 2*. La suite complexe* $\left(r^k e^{ik\theta}\right)_{k\in\mathbb{N}}$ *satisfaisant la relation de récurrence, ses parties réelle et imaginaire sont des suites réelles satisfaisant la relation. Il suffit alors de remarquer que ces dernières sont linéairement indépendantes.*

Exemple 1.81 (suite de Fibonacci) *La* ***suite de Fibonacci*** *a été indroduite par Leonardo Fibonacci en 1202 au moyen d'un problème récréatif décrivant la croissance d'une population de lapins*[19]*, le* k^e *terme de la suite correspondant au nombre de paires de lapins au* k^e *mois. La population de lapins est idéalisée et l'on suppose que*

— *au début du premier mois, il n'y a qu'une paire de lapereaux ;*
— *les lapins ne peuvent procréer qu'à partir de l'âge de deux mois ;*
— *chaque début de mois, toute paire susceptible de procréer engendre exactement une nouvelle paire de lapereaux ;*
— *les lapins ne meurent jamais ;*

et la suite est par conséquent une suite récurrente linéaire à coefficients constants d'ordre 2*, satisfaisant la relation de récurrence*

$$\forall k \in \mathbb{N},\ u_{k+2} = u_{k+1} + u_k, \tag{1.6}$$

avec $u_0 = 0$ *et* $u_1 = 1$*. La technique décrite ci-dessus permet de déterminer une expression fonctionnelle du terme général de cette suite. L'équation caractéristique associée à* (1.6) *est* $r^2 - r - 1 = 0$*, de discriminant associé valant* 5*. On a donc*

$$\forall k \in \mathbb{N},\ u_k = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^k + \beta\left(\frac{1-\sqrt{5}}{2}\right)^k,$$

les nombres réels α *et* β *satisfaisant*

$$\begin{cases} \alpha + \beta = 0, \\ \alpha - \beta = \dfrac{2}{\sqrt{5}}, \end{cases}$$

d'où $\alpha = -\beta = \frac{1}{\sqrt{5}}$.

1.8.2 Lien entre rayon spectral et norme matricielle subordonnée

Soit M une matrice carrée à coefficients complexes. Le *rayon spectral* de M est le réel positif défini par

$$\rho(M) = \max\{|\lambda| \mid \lambda \in \mathrm{Sp}(M)\}.$$

Étant donné un entier naturel non nul n, on définit par ailleurs une *norme matricielle subordonnée* $\|\cdot\|$ sur $M_n(\mathbb{K})$ comme l'application qui a toute matrice carrée M d'ordre n associe le réel noté $\|M\|$ tel que

$$\|M\| = \sup_{\substack{X\in M_{n,1}(\mathbb{K}) \\ X\neq 0}} \frac{\|MX\|}{\|X\|} = \sup_{\substack{X\in M_{n,1}(\mathbb{K}) \\ \|X\|\leq 1}} \|MX\| = \sup_{\substack{X\in M_{n,1}(\mathbb{K}) \\ \|X\|=1}} \|MX\|,$$

où, par abus de notation, désigne également $\|\cdot\|$ une norme sur $M_{n,1}(\mathbb{K})$. Pour certains choix de normes sur $M_{n,1}(\mathbb{K})$, il est possible d'exprimer explicitement la norme matricielle qui lui est subordonnée en fonction des coefficients de la matrice. Par exemple, on a, pour la norme $\|\cdot\|_\infty$,

$$\forall M \in M_n(\mathbb{K}),\ \|M\|_\infty = \max_{1\leq i\leq n}\left(\sum_{j=1}^{n} \left|m_{ij}\right|\right).$$

19. En voici une version traduite du latin : *« Quelqu'un a déposé un couple de lapins dans un certain lieu, clos de toutes parts, pour savoir combien de couples seraient issus de cette paire en une année, car il est dans leur nature de générer un autre couple en un seul mois, et qu'ils enfantent dans le second mois après leur naissance. »*

En vertu de la définition ci-dessus, il est clair que, pour toute norme matricielle subordonnée $\|\cdot\|$, on a

$$\rho(M) \leq \|M\|. \tag{1.7}$$

Bien que l'inégalité réciproque soit généralement fausse, on peut montrer qu'il est possible d'approcher d'aussi près que voulu le rayon spectral d'une matrice par valeurs supérieures à l'aide d'une norme matricielle subordonnée convenablement choisie. Ce résultat, utile en analyse numérique pour l'étude de la convergence de certaines méthodes itératives de résolution de systèmes linéaires, est le suivant.

Théorème 1.82 *Soit M une matrice carrée à coefficients complexes et ε un nombre réel strictement positif. Il existe une norme matricielle subordonnée $\|\cdot\|_\varepsilon$ telle que*

$$\|M\|_\varepsilon \leq \rho(M) + \varepsilon.$$

DÉMONSTRATION. Si la matrice M est diagonalisable, l'inégalité de l'énoncé est valide si le nombre réel ε est nul, et donc *a fortiori* s'il est positif. En effet, il existe dans ce cas une matrice inversible P et une matrice diagonale D telles que $M = PDP^{-1}$, et la norme de matrice subordonnée à la norme définie par

$$\forall X \in M_{n,1}(\mathbb{C}),\ \|X\|_0 = \|P^{-1}X\|_\infty$$

convient alors. Si la matrice M n'est que trigonalisable, il existe, en vertu du théorème 1.68, une matrice inversible P et une matrice J sous forme normale de Jordan, dont les coefficients diagonaux sont les valeurs propres de M, telles que $M = PJP^{-1}$. Pour tout bloc de Jordan $J_l(\lambda)$ de taille l (strictement plus grande que 1) de J, on introduit la matrice diagonale

$$D_\varepsilon = \begin{pmatrix} \varepsilon & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \varepsilon^l \end{pmatrix}.$$

Il est facile de vérifier que cette matrice est inversible et que l'on a $D_\varepsilon J_l(\lambda) {D_\varepsilon}^{-1} = \lambda I_l + \varepsilon J_l(0)$. On pose

$$\forall Y \in M_{l,1}(\mathbb{C}),\ \|Y\|_0 = \|D_\varepsilon Y\|_\infty.$$

La norme subordonnée associée à la norme ainsi définie s'évalue alors aisément pour le bloc $J_l(\lambda)$:

$$\|J_l(\lambda)\|_\varepsilon = \sup_{\substack{Y \in M_{l,1}(\mathbb{C}) \\ \|Y\|_\varepsilon = 1}} \|J_l(\lambda)Y\|_\varepsilon = \sup_{\substack{Y \in M_{l,1}(\mathbb{C}) \\ \|Y\|_\varepsilon = 1}} \|{D_\varepsilon}^{-1}(\lambda I_l + \varepsilon J_l(0))D_\varepsilon Y\|_\varepsilon = \sup_{\substack{Y \in M_{l,1}(\mathbb{C}) \\ \|Y\|_\infty = 1}} \|(\lambda I_l + \varepsilon J_l(0))Y\|_\infty$$
$$= \|\lambda I_l + \varepsilon J_l(0)\|_\infty,$$

d'où $\|J_l(\lambda)\|_\varepsilon = |\lambda| + \varepsilon \leq \rho(M) + \varepsilon$.

On construit ainsi pour chaque bloc de Jordan une norme matricielle subordonnée convenable, qu'il suffit d'assembler pour obtenir une norme matricielle subordonnée satisfaisant la condition de l'énoncé. □

Remarque 1.83 *On a ici prouvé ce résultat dans le cas d'une matrice à coefficients complexes, car on sait qu'une telle matrice est toujours trigonalisable dans le pire des cas. La démonstration peut être adaptée au cas d'une matrice à coefficients réels dont le polynôme caractéristique n'est pas scindé sur $\mathbb{R}$, soit en plongeant $\mathbb{R}$ dans $\mathbb{C}$ afin de faire appel au théorème 1.68, soit en utilisant la réduction de Jordan dans le cas réel au prix de quelques complications techniques.*

Ce théorème et l'inégalité 1.7 montrent que, bien que l'application associant à toute matrice carrée son rayon spectral ne définisse pas une norme, le rayon spectral d'une matrice donnée est la plus grande borne inférieure des valeurs prises toute norme subordonnée de cette matrice.

Chapitre 2

Formes bilinéaires

Une *application bilinéaire* est l'analogue à deux variables d'une application linéaire.

2.1 Généralités sur les applications bilinéaires

Étant donné trois $\mathbb{K}$-espaces vectoriels E, F et G, une application b de $E \times F$ dans G est dite *bilinéaire* si et seulement si

$$\forall (x,x') \in E^2,\ \forall (y,y') \in F^2,\ \forall \lambda \in \mathbb{K},$$
$$b(x+x',y) = b(x,y) + b(x',y),\ b(x,y+y') = b(x,y) + b(x,y'),\ b(\lambda x, y) = b(x, \lambda y) = \lambda\, b(x,y).$$

On peut exprimer cette définition de manière un peu plus formelle en disant que l'application b est *linéaire par rapport à chacune de ses variables*. Ceci peut être rendu précis de la façon suivante.

Définition 2.1 *Soit E, F et G trois $\mathbb{K}$-espaces vectoriels. Une application b de $E \times F$ dans G est dite* ***bilinéaire*** *si et seulement si l'***application partielle à gauche de** *b, notée $L(b)$, de E dans $\mathscr{L}(F;G)$ définie par*

$$\forall x \in E,\ L(b)(x) = (y \mapsto b(x,y)),$$

*et l'***application partielle à droite de** *b, notée $R(b)$, de F dans $\mathscr{L}(E;G)$ définie par*

$$\forall y \in F,\ R(b)(y) = (x \mapsto b(x,y))$$

sont toutes deux linéaires.

Lorsque $G = \mathbb{K}$, on parle de **forme bilinéaire**.

L'ensemble des applications bilinéaires de $E \times F$ dans G, noté $\mathscr{L}(E,F;G)$, est un espace vectoriel sur $\mathbb{K}$. Il est en effet clair que la somme de deux applications bilinéaires est une application bilinéaire et que le produit d'une application bilinéaire par un scalaire est une application bilinéaire.

Remarque 2.2 *Dans la précédente définition, on a en fait défini une application $L : \mathscr{L}(E,F;G) \to \mathscr{L}(E;\mathscr{L}(F;G))$ (resp. $R : \mathscr{L}(E,F;G) \to \mathscr{L}(F;\mathscr{L}(E;G))$). Il est facile de vérifier qu'elle est linéaire et que c'est un isomorphisme (dit* canonique*). On notera qu'on a ici linéarité à trois niveaux différents, puisque les applications L, $L(b)$ et, pour tout vecteur x de E, $L(b)(x)$ (resp. R, $R(b)$ et, pour tout vecteur y de F, $R(b)(y)$) sont toutes trois linéaires.*

Définition 2.3 (application bilinéaire symétrique) *Soit E et G deux $\mathbb{K}$-espaces vectoriels et b une application bilinéaire de $E \times E$ dans G. On dit que l'application b est* ***symétrique*** *(resp.* ***antisymétrique****) si et seulement si*

$$\forall (x,y) \in E^2,\ b(x,y) = b(y,x) \text{ (resp. } b(x,y) = -b(y,x)).$$

Exemple 2.4 (produits bilinéaires) *En mathématiques, presque tout ce qui porte le nom de* produit *est bilinéaire. Ainsi, le* produit de deux nombres réels*,*

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & xy, \end{array}$$

est bilinéaire symétrique. Ceci résulte de l'associativité et de la commutativité de la multiplication et de la distributivité de la multiplication par rapport à l'addition. Pour tout triplet (m,n,p) *d'entiers naturels non nuls, le* produit matriciel de $M_{m,n}(\mathbb{R}) \times M_{n,p}(\mathbb{R})$ dans $M_{m,p}(\mathbb{R})$ *est, pour les mêmes raisons, une application bilinéaire. Pour tout quadruplet* (m,n,p,q) *d'entiers naturels non nuls, l'opération portant le nom de* produit de Kronecker*, qui associe à une matrice* M *de* $M_{m,n}(\mathbb{R})$ *et une matrice* N *de* $M_{p,q}(\mathbb{R})$ *la matrice* $M \otimes N$ *de* $M_{mp,nq}(\mathbb{R})$ *s'écrivant par blocs*

$$M \otimes N = \begin{pmatrix} m_{11}N & \dots & m_{1n}N \\ \vdots & & \vdots \\ m_{m1}N & \dots & m_{mn}N \end{pmatrix},$$

définit une application bilinéaire. Pour tout entier naturel n *non nul, le* produit scalaire euclidien sur $\mathbb{R}^n$*,*

$$\begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \to & \mathbb{R} \\ (x,y) & \mapsto & x \cdot y, \end{array}$$

défini par

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

où $x = (x_1, \dots, x_n)$ *et* $y = (y_1, \dots, y_n)$*, est une forme bilinéaire symétrique. L'*appariement dual[1] *(encore appelé* produit (ou crochet) de dualité*)* $\langle \cdot, \cdot \rangle_{E^*,E}$ *entre un espace vectoriel* E *et son dual* E^* *(c'est-à-dire l'espace des formes linéaires sur* E*), défini par*

$$\forall x \in E,\ \forall \varphi \in E^*,\ \langle \varphi, x \rangle_{E^*,E} = \varphi(x),$$

est une forme bilinéaire sur $E^* \times E$*. Enfin, un dernier exemple est celui du* produit vectoriel *(voir la proposition 5.20).*

2.2 Représentation matricielle d'une forme bilinéaire

On se limitera à partir de maintenant aux *formes* bilinéaires, c'est-à-dire qu'on aura $G = \mathbb{K}$ dans la suite. Dans ce cas particulier, considérant une forme bilinéaire b de $E \times F$ dans $\mathbb{K}$, l'application linéaire à gauche de b, $L(b)$, envoie E dans $\mathscr{L}(F;\mathbb{K})$, c'est-à-dire dans F^*, le dual de F. De la même manière, l'application linéaire à droite de b, $R(b)$, envoie F dans E^*.

On suppose que $\mathscr{B} = \{e_1, \dots, e_n\}$ est une base de E et que $\mathscr{C} = \{f_1, \dots, f_m\}$ est une base de F. On note alors $\mathscr{B}^*$ la base de E^* et $\mathscr{C}^*$ la base de F^* qui sont les bases duales respectives de $\mathscr{B}$ et de $\mathscr{C}$.

On considère la matrice N de l'application $L(b)$ dans les bases $\mathscr{B}$ et $\mathscr{C}^*$. De la même manière, la matrice M représente l'application $R(b)$ dans les bases $\mathscr{C}$ et $\mathscr{B}^*$. On a le résultat suivant.

Lemme 2.5 *La matrice* N *est la transposée de la matrice* M*, i.e.*

$$\forall i \in \{1, \dots, m\},\ \forall j \in \{1, \dots, n\},\ n_{ij} = m_{ji}.$$

DÉMONSTRATION. On remarque tout d'abord que la matrice N appartient à $M_{m,n}(\mathbb{K})$ puisque E est de dimension n et F^* de dimension m. De la même façon, la matrice M appartient à $M_{n,m}(\mathbb{K})$.

Ensuite, le coefficient n_{ij} est la i^{e} coordonnée de la forme $L(b)(e_j)$ dans la base duale $\mathscr{C}^*$. Par propriété de la base duale, il vaut par conséquent $L(b)(e_j)(f_i)$, soit encore $b(e_j, f_i)$. De la même façon, le coefficient m_{ji} est la j^{e} coordonnée de la forme $R(b)(f_i)$ dans la base duale $\mathscr{B}^*$ et vaut donc $R(b)(f_i)(e_j) = b(e_j, f_i)$. □

Définition 2.6 (matrice d'une forme bilinéaire) *Soit* E *et* F *deux espaces vectoriels de dimensions finies non nulles,* $\mathscr{B}$ *une base de* E*,* $\mathscr{C}$ *une base de* F *et* b *une forme bilinéaire sur* $E \times F$*. La* ***matrice de*** b ***relativement aux bases*** $\mathscr{B}$ ***et*** $\mathscr{C}$ *est celle de l'application* $R(b)$ *dans les bases* $\mathscr{C}$ *et* $\mathscr{B}^*$*.*

Remarque 2.7 *L'application* R *étant bijective, il y a une correspondance bijective entre les formes bilinéaires sur* $E \times F$ *et les matrices à* n *lignes et* m *colonnes quand les espaces* E *et* F *sont respectivement de dimension* n *et* m*. Cet isomorphisme* dépend *du choix des bases sur* E *et* F*, et n'est donc pas canonique.*

1. On renvoie à la section B.3 de l'annexe B pour davantage de détails.

Lemme 2.8 (expression des coefficients de la matrice d'une forme bilinéaire) *Soit E et F deux espaces vectoriels de dimensions finies non nulles, $\mathscr{B} = \{e_1, \dots, e_n\}$ une base de E et $\mathscr{C} = \{f_1, \dots, f_m\}$ une base de F. Le coefficient à la i^e ligne et la j^e colonne de la matrice de la forme bilinéaire b relativement aux bases $\mathscr{B}$ et $\mathscr{C}$ est égal à $b(e_i, f_j)$.*

DÉMONSTRATION. Le coefficient en question a précédemment été noté m_{ij} et l'on a vu dans la preuve du dernier lemme qu'il était égal à $b(e_i, f_j)$. □

Une conséquence de la précédente définition est que, si les matrices colonnes $\mathrm{Mat}_{\mathscr{B}}(x)$ de $M_{n,1}(\mathbb{K})$ et $\mathrm{Mat}_{\mathscr{C}}(y)$ de $M_{m,1}(\mathbb{K})$ contiennent les coordonnées respectives des vecteurs x de E dans la base $\mathscr{B}$ et y de F dans la base $\mathscr{C}$ et que la matrice M de $M_{n,m}(\mathbb{K})$ représente la forme bilinéaire b relativement à $\mathscr{B}$ et $\mathscr{C}$, on a

$$b(x, y) = (\mathrm{Mat}_{\mathscr{B}}(x))^\top M \mathrm{Mat}_{\mathscr{C}}(y),$$

moyennant un abus de notation consistant à identifier une matrice d'ordre 1 avec le seul scalaire qu'elle contient. Cette dernière formule montre comment calculer l'image d'un couple de vecteurs par une forme bilinéaire lorsque l'on dispose de la matrice de cette dernière relativement à des bases données. Elle montre en particulier qu'une forme bilinéaire b sur $\mathbb{R}^n \times \mathbb{R}^n$ s'écrit sous la forme

$$\forall (x, y) \in \mathbb{R}^n \times \mathbb{R}^n,\ b(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} m_{ij} x_i y_j,$$

c'est-à-dire comme une combinaison linéaire de monômes de degré un en x et y dont les coefficients sont ceux de la matrice de b relativement à la base canonique de $\mathbb{R}^n$.

La preuve du résultat suivant est laissée en exercice au lecteur.

Proposition 2.9 *Soit E un espace vectoriel de dimension finie non nulle, $\mathscr{B}$ une base de E et b une forme bilinéaire sur $E \times E$. La matrice de b relativement à la base $\mathscr{B}$ est symétrique (resp. antisymétrique) si et seulement si la forme b est symétrique (resp. antisymétrique).*

Changement de bases

On considère à présent une forme bilinéaire sur $E \times F$ et les bases $\mathscr{B}$ et $\mathscr{B}'$ de E, $\mathscr{C}$ et $\mathscr{C}'$ de F. On note P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$, c'est-à-dire qu'on a $\mathrm{Mat}_{\mathscr{B}}(x) = P\mathrm{Mat}_{\mathscr{B}'}(x)$ pour tout vecteur x de E, et Q la matrice de passage de $\mathscr{C}$ à $\mathscr{C}'$, c'est-à-dire qu'on a $\mathrm{Mat}_{\mathscr{C}}(y) = Q\mathrm{Mat}_{\mathscr{C}'}(y)$ pour tout vecteur y de F. En comparant la matrice de b relativement aux bases $\mathscr{B}$ et $\mathscr{C}$ d'une part avec celle relativement aux bases $\mathscr{B}'$ et $\mathscr{C}'$ d'autre part, on a

$$\begin{aligned}(\mathrm{Mat}_{\mathscr{B}'}(x))^\top M' \mathrm{Mat}'_{\mathscr{C}}(y) = b(x, y) &= (\mathrm{Mat}_{\mathscr{B}}(x))^\top M \mathrm{Mat}_{\mathscr{C}}(y) \\ &= (P\mathrm{Mat}_{\mathscr{B}'}(x))^\top M (Q\mathrm{Mat}_{\mathscr{C}'}(y)) = (\boldsymbol{x}')^\top P^\top M Q \mathrm{Mat}_{\mathscr{C}'}(y),\end{aligned}$$

dont on déduit, par identification, la formule de changement de bases suivante

$$M' = P^\top M Q. \tag{2.1}$$

On notera que la matrice transposée $P^\top$ est généralement différente de l'inverse P^{-1}. Par conséquent, même lorsque $F = E$ et $\mathscr{C} = \mathscr{B}$ (et donc $Q = P$), les matrices carrées M et M' ne sont généralement pas semblables (on dit qu'elles sont *congrues*). Ceci signifie en particulier que si la matrice d'un endomorphisme de E dans une base donnée est la même que celle d'une forme bilinéaire sur $E \times E$ relativement à cette base, il n'en sera pas nécessairement de même après changement de base.

2.3 Non dégénérescence

Définition 2.10 (non dégénérescence) *Une forme bilinéaire sur $E \times F$ est dite **non dégénérée à gauche** (resp. **à droite**) si et seulement si l'application linéaire associée à gauche (resp. à droite) est injective. Elle est dite **non dégénérée** si et seulement si elle est non dégénérée à gauche et à droite.*

Par conséquent, une forme bilinéaire b est non dégénérée à gauche (resp. à droite) si et seulement si son *noyau à gauche* $\ker(L(b)) = \{x \in E \mid \forall y \in F,\ b(x,y) = 0\}$ (resp. son *noyau à droite* $\ker(R(b)) = \{y \in F \mid \forall x \in E,\ b(x,y) = 0\}$) est réduit au vecteur nul.

Lemme 2.11 *Si $E = F$ et que la forme bilinéaire est symétrique, la non dégénérescence à gauche est équivalente à la non dégénérescence à droite et les noyaux à gauche et à droite coïncident.*

DÉMONSTRATION. Dans ce cas, on a $L(b) = R(b)$, d'où la conclusion. □

Proposition 2.12 *Si les espaces vectoriels E et F sont de dimensions finies et égales et b est une forme bilinéaire sur $E \times F$, les assertions suivantes sont équivalentes.*

(i) La forme b est non dégénérée à droite.

(ii) La forme b est non dégénérée à gauche.

(iii) L'application partielle à gauche $L(b)$ est injective.

(iv) L'application partielle à droite $R(b)$ est injective.

(v) L'application $L(b)$ est surjective.

(vi) L'application $R(b)$ est surjective.

DÉMONSTRATION. La proposition découle du fait que la matrice de l'application $R(b)$, qui est carrée dans ce cas particulier, est la transposée de la matrice de l'application $L(b)$ et du théorème du rang. □

Corollaire 2.13 *Si les espaces vectoriels E et F sont de dimensions finies et égales, une forme bilinéaire sur $E \times F$ est non dégénérée si et seulement si le déterminant de sa matrice relativement à des bases quelconques de E et de F est non nul.*

La restriction à un sous-espace vectoriel d'une forme bilinéaire non dégénérée peut être dégénérée, comme le montre l'exemple suivant.

Exemple 2.14 (restriction dégénérée d'une forme bilinéaire non dégénérée) *La forme définie sur $\mathbb{R}^2 \times \mathbb{R}^2$ par*

$$b(x,y) = x_1y_1 - x_2y_2,$$

de matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ relativement à la base canonique, est non dégénérée. En effet, l'application $R(b)$ envoie e_1 sur ${e_1}^*$ et e_2 sur $-{e_2}^*$, elle est donc surjective. Pourtant, sa restriction à la droite vectorielle engendrée par $e_1 + e_2$ est dégénérée, car identiquement nulle.

Définition 2.15 (rang d'une application bilinéaire) *Soit E et F des espaces vectoriels de dimensions finies et égales et b une forme bilinéaire sur $E \times F$. Le **rang** de la forme b est le rang de l'application linéaire associée à droite de b.*

On peut observer qu'on aurait tout aussi bien pu prendre pour définition du rang de b le rang de l'application linéaire associée à *gauche*, puisque $L(b)$ et $R(b)$ ont même rang d'après la preuve de la précédente proposition.

Par définition de la matrice représentative d'une forme bilinéaire, le rang d'une forme bilinéaire est égal au rang de sa matrice. Ce dernier est bien entendu indépendant du choix des bases, les matrices de changement de base étant inversibles.

2.4 Formes sesquilinéaires

Lorsque les espaces vectoriels considérés sont construits sur le corps $\mathbb{C}$, on fait couramment appel à la notion de *forme sesquilinéaire*, qui constitue un équivalent[2] complexe aux formes bilinéaires sur des espaces vectoriels réels.

Définition 2.16 (forme sesquilinéaire) *Soit E et F deux $\mathbb{C}$-espaces vectoriels. Une application s de $E \times F$ dans $\mathbb{C}$ est une **forme sesquilinéaire à gauche** si et seulement si*

2. Ceci apparaîtra plus clairement dans le prochain chapitre.

— *elle est linéaire à droite,*

$$\forall x \in E,\ \forall y \in F,\ \forall z \in F,\ \forall \lambda \in \mathbb{C},\ s(x, y + \lambda z) = s(x, y) + \lambda s(x, z),$$

— *elle est semi-linéaire à gauche,*

$$\forall x \in E,\ \forall z \in E,\ \forall y \in F,\ \forall \lambda \in \mathbb{C},\ s(x + \lambda z, y) = s(x, y) + \overline{\lambda} s(z, y),$$

De la même manière, on peut définir une forme sesquilinéaire ***à droite****.*

Remarque 2.17 *Cette définition justifie l'appellation utilisée, le préfixe sesqui- indiquant que le mot préfixé est* dans un rapport de un et demi*. En effet, la forme est linéaire par rapport à une des variables, mais, par rapport à l'autre, elle est seulement linéaire par rapport à la somme de vecteurs et pas par rapport à la multiplication par un scalaire, ce qui compte alors « pour moitié ». La convention d'une forme sesquilinéaire à gauche est largement utilisée en physique et trouve son origine avec la* notation bra-ket *[Dir39], introduite en mécanique quantique par Paul Adrien Maurice Dirac.*

Définition 2.18 (symétrie hermitienne) *Une forme sesquilinéaire s sur $E \times E$ vérifie la propriété de* ***symétrie hermitienne*** *si et seulement si*

$$\forall (x, y) \in E \times E,\ s(y, x) = \overline{s(x, y)}.$$

Une telle forme sesquilinéaire est dite ***hermitienne****.*

Avec cette notion de symétrie, on peut observer qu'on a en particulier

$$\forall x \in E,\ s(x, x) = \overline{s(x, x)},$$

pour toute forme sesquilinéaire hermitienne s, ce qui fait que ces quantités sont *réelles*. Cette propriété est fondamentale, car elle permet notamment d'imposer une condition de positivité, essentielle à la notion de *produit scalaire*.

Représentation matricielle d'une forme sesquilinéaire

La matrice d'une forme sesquilinéaire s relativement à des bases des espaces E et F est définie de manière identique à celle d'une forme bilinéaire. En revanche, c'est la transconjugaison qui intervient en place de la transposition dans l'expression matricielle du scalaire $s(x, y)$:

$$s(x, y) = X^* M Y = \overline{X}^\top M Y,$$

et dans la formule de changement de bases, analogue de (2.1), associée.

On peut montrer qu'une matrice M correspond à une forme sesquilinéaire hermitienne si et seulement si elle est telle que

$$M^* = \overline{M}^\top = M.$$

Non dégénérescence

L'intégralité des définitions et résultats de la section 2.3 s'appliquent directement aux formes sesquilinéaires.

Chapitre 3

Formes quadratiques

On aborde dans ce chapitre la notion de *forme quadratique*, fortement liée à celle de forme bilinéaire précédemment introduite. Celle-ci intervient dans de nombreux domaines des mathématiques et de la physique, puisqu'elle est notamment à la base de la géométrie euclidienne et de sa généralisation dans les espaces préhilbertiens et de Hilbert. L'étude arithmétique de ces formes a aussi été le point de départ de la théorie des nombres algébriques.

3.1 Définitions et premières propriétés

Définition 3.1 (forme quadratique) *Soit E un $\mathbb{K}$-espace vectoriel. Une application q de E dans $\mathbb{K}$ est appelée* ***forme quadratique*** *sur E s'il existe une forme bilinéaire b de $E \times E$ dans $\mathbb{K}$ telle que*

$$\forall x \in E,\ q(x) = b(x,x).$$

Toute forme bilinéaire b sur $E \times E$ donne naissance à une forme quadratique sur E en posant

$$\forall x \in E,\ q(x) = b(x,x).$$

On appelle alors q la *forme quadratique associée à b*. Une même forme quadratique peut ainsi être associée à plusieurs formes bilinéaires. On a toutefois le résultat suivant.

Proposition et définition 3.2 (forme polaire d'une forme quadratique) *Sur un espace vectoriel dont le corps est de caractéristique*[1] *différente de 2 (comme $\mathbb{R}$ ou $\mathbb{C}$), toute forme quadratique est associée à une unique forme bilinéaire symétrique, cette dernière étant appelée la* ***forme polaire*** *de la forme quadratique.*

DÉMONSTRATION. Soit q une forme quadratique sur un espace vectoriel E dont le corps est de caractéristique différente de 2. Par définition, il existe une forme bilinéaire b, non nécessairement symétrique, telle que

$$\forall x \in E,\ b(x,x) = q(x),$$

que l'on peut « symétriser » en introduisant la forme bilinéaire c définie par

$$\forall (x,y) \in E^2,\ c(x,y) = \frac{1}{2}\left(b(x,y) + b(y,x)\right).$$

On a alors

$$\forall x \in E,\ c(x,x) = b(x,x),$$

1. La *caractéristique* d'un anneau (unitaire) est par définition l'ordre pour la loi additive de l'élément neutre de la loi multiplicative si cet ordre est fini (s'il est infini, la caractéristique de l'anneau est nulle). Soit $(A,+,\times)$ un anneau unitaire d'élément neutre pour la loi additive « $+$ » noté 0_A et d'élément neutre pour la loi multiplicative « $\times$ » noté 1_A. La caractéristique de A est alors le plus petit entier naturel n non nul tel que

$$n \times 1_A = \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ occurences}} = 0_A$$

si un tel entier existe. Dans le cas contraire (autrement dit si 1_A est d'ordre infini), la caractéristique de A est nulle.

et q est donc aussi la forme quadratique associée à c. Par ailleurs, la forme c étant symétrique, on a

$$\begin{aligned}\forall (x,y)\in E^2,\ q(x+y)-q(x-y) &= c(x+y,x+y)-c(x-y,x-y)\\ &= c(x,x)+2\,c(x,y)+c(y,y)-c(x,x)+2\,c(x,y)-c(y,y)\\ &= 4\,c(x,y),\end{aligned}$$

ce qui donne

$$\forall (x,y)\in E^2,\ c(x,y)=\frac{1}{4}\left(q(x+y)-q(x-y)\right). \tag{3.1}$$

La forme c est donc définie de manière unique. □

La formule (3.1) obtenue dans la démonstration ci-dessus est appelée *identité de polarisation*. On notera que l'on a également

$$\begin{aligned}\forall (x,y)\in E^2,\ q(x+y)-q(x)-q(y) &= c(x+y,x+y)-c(x,x)-c(y,y)\\ &= c(x,x)+2\,c(x,y)+c(y,y)-c(x,x)-c(y,y)\\ &= 2\,c(x,y),\end{aligned}$$

d'où la formule

$$\forall (x,y)\in E^2,\ c(x,y)=\frac{1}{2}\left(q(x+y)-q(x)-q(y)\right),$$

qui constitue une deuxième identité de polarisation. Une troisième identité de polarisation est donnée par

$$\forall (x,y)\in E^2,\ c(x,y)=\frac{1}{2}\left(q(x)+q(y)-q(x-y)\right).$$

En pratique, si l'on exhibe une forme bilinéaire symétrique ayant une forme quadratique q associée, c'est nécessairement la forme polaire de q. On n'a donc pas toujours besoin d'utiliser les identités de polarisation.

Remarque 3.3 *Étant donné un corps $\mathbb{K}$ de caractéristique de différente de 2, on appelle $\mathbb{K}$-**espace quadratique** tout $\mathbb{K}$-espace vectoriel que l'on munit d'une forme quadratique.*

Un *polynôme homogène de degré deux* sur $\mathbb{K}$ en les variables $x_1,\dots,x_n$ est une expression de la forme

$$\sum_{i=1}^{n}\alpha_{ii}\,{x_i}^2+\sum_{i=1}^{n}\sum_{j=i+1}^{n}\alpha_{ij}\,x_ix_j,$$

où les coefficients α_{ij}, $1\le i\le j\le n$, appartiennent à $\mathbb{K}$.

Proposition 3.4 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et $\mathscr{B}=\{e_1,\dots,e_n\}$ une base de E. Les formes quadratiques sur E sont les applications q telles que, pour tout vecteur x de E, $q(x)$ est un polynôme homogène de degré deux en les coordonnées de x dans la base $\mathscr{B}$.*

DÉMONSTRATION. Soit b la forme polaire de q. On pose

$$\forall (i,j)\in\{1,\dots,n\}^2,\ m_{ij}=b(e_i,e_j)$$

et l'on introduit les coordonnées de tout vecteur x de E dans la base $\mathscr{B}$,

$$\forall x\in E,\ x=\sum_{i=1}^{n}x_ie_i.$$

On a alors

$$\begin{aligned}\forall x \in E,\ q(x) &= b\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} x_j e_j\right)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j\, b(e_i, e_j)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}\, x_i x_j\\ &= \sum_{i=1}^{n} m_{ii}\, {x_i}^2 + 2\sum_{i=1}^{n}\sum_{j=i+1}^{n} m_{ij}\, x_i x_j,\end{aligned}$$

car

$$\forall (i,j) \in \{1,\dots,n\}^2,\ m_{ij} = m_{ji}.$$

□

Remarque 3.5 *Une forme quadratique étant donnée par un polynôme homogène de degré deux, sa forme polaire peut être déterminée en* polarisant *chaque monôme de ce polynôme. Ainsi, un monôme de la forme $a\,{x_i}^2$ est polarisé en $a\,x_i y_i$, tandis qu'un monôme de la forme $a\,x_i x_j$ est polarisé en $\frac{a}{2}\left(x_i y_j + x_j y_i\right)$.*

La correspondance biunivoque entre les formes quadratiques et les formes polaires associées permet d'étendre aux formes quadratiques des notions initialement introduites pour les formes bilinéaires.

Définitions 3.6 (matrice, noyau et rang d'une forme quadratique) *Soit q une forme quadratique sur un $\mathbb{K}$-espace vectoriel, supposé de dimension finie. La matrice de q relativement à une base donnée de l'espace est celle de sa forme polaire. Le noyau et le rang de q sont aussi définis comme étant ceux de sa forme polaire.*

Il découle de ces définitions que l'on peut exprimer matriciellement cette dernière en utilisant ce qui a été vu dans le précédent chapitre. En notant M la matrice d'une forme quadratique q de A relativement à une base $\mathscr{B}$ de E et en notant X la matrice colonne représentant un élément x de E dans la base $\mathscr{B}$, on a

$$q(x) = X^\top M X.$$

Une autre conséquence est que l'espace vectoriel des formes quadratiques sur E, noté $\mathscr{Q}(E)$, est isomorphe à $S_n(\mathbb{K})$, l'ensemble des matrices symétriques à coefficients dans $\mathbb{K}$. En particulier, si l'espace E est de dimension n, alors l'espace $\mathscr{Q}(E)$ est de dimension $\frac{1}{2}n(n+1)$.

Définition 3.7 (forme quadratique non dégénérée) *Une forme quadratique est dite* ***non dégénérée*** *si et seulement si son noyau est réduit au vecteur nul.*

Définition 3.8 (formes quadratiques équivalentes) *Deux formes quadratiques q et q' sur un $\mathbb{K}$-espace vectoriel E sont dites* ***équivalentes*** *s'il existe un automorphisme u de E tel que*

$$\forall x \in E,\ q'(x) = q(u(x)).$$

En dimension finie, l'équivalence entre formes quadratiques se traduit matriciellement par le fait que les matrices des formes relativement à une même base sont congrues.

3.2 Orthogonalité

Dans toute cette section, E désigne un $\mathbb{K}$-espace vectoriel, q une forme quadratique sur E et b la forme polaire de q.

Définition 3.9 (cône isotrope) *Un vecteur x de E est dit* ***isotrope*** *pour q si et seulement si $q(x) = 0$. On appelle* ***cône isotrope*** *de q l'ensemble $\mathscr{C}_q$ des vecteurs isotropes pour q. On dit enfin que q est* ***définie*** *si et seulement si $\mathscr{C}_q = \{0_E\}$.*

Une forme bilinéaire b sur $E \times E$ est dite **alternée** si et seulement si tout vecteur de E est isotrope pour sa forme quadratique associée, c'est-à-dire si

$$\forall x \in E,\ b(x,x) = 0.$$

Bien que l'on ait toujours l'inclusion $\ker(q) \subset \mathscr{C}_q$, le cône isotrope $\mathscr{C}_q$ n'est généralement pas un sous-espace vectoriel de E. Il en découle qu'une forme quadratique définie est non dégénérée, mais que la réciproque est généralement fausse.

Exemple 3.10 *La forme quadratique q sur $\mathbb{R}^2$ telle que*

$$\forall x \in \mathbb{R}^2,\ q(x) = x_1 x_2,$$

est non dégénérée et a pour cône isotrope l'ensemble $\mathscr{C}_q = \{x \in \mathbb{R}^2 \,|\, x_1 = 0\} \cup \{x \in \mathbb{R}^2 \,|\, x_2 = 0\}$, qui n'est pas un sous-espace vectoriel.

Exemple 3.11 *La forme quadratique q sur $\mathbb{R}^2$ telle que*

$$\forall x \in \mathbb{R}^2,\ q(x) = {x_1}^2 - {x_2}^2,$$

est non dégénérée (on a étudié sa forme polaire dans l'exemple 2.14), mais on a $q((1,1)) = 1-1 = 0$ et elle n'est donc pas définie.

Définition 3.12 (orthogonalité) *On dit que deux vecteurs x et y de E sont **orthogonaux** pour la forme q (ou pour sa forme polaire b), ou simplement q-orthogonaux, si et seulement si $b(x,y) = 0$, ce que l'on note $x \perp y$.*

*Si A est une partie de E, on appelle **orthogonal** de A pour la forme q (ou pour sa forme polaire b), et on note $A^\perp$, la partie de E dont les éléments sont orthogonaux à ceux de A,*

$$A^\perp = \{y \in E \,|\, \forall x \in A,\ b(x,y) = 0\}.$$

Enfin, deux sous-ensembles A et B de E sont dits orthogonaux pour la forme q (ou pour sa forme polaire b) si et seulement si

$$\forall x \in A,\ \forall y \in B,\ b(x,y) = 0,$$

ce que l'on note encore $A \perp B$.

Il est immédiat[2] que la partie $A^\perp$ est un sous-espace vectoriel de E. Par ailleurs, pour toute partie A de E, l'orthogonal de A est égal[3] à celui du sous-espace vectoriel engendré par A, c'est-à-dire que

$$A^\perp = \mathrm{Vect}(A)^\perp.$$

Par conséquent, on considérera dans la suite uniquement des orthogonaux de parties qui sont des sous-espaces vectoriels de E.

On peut par ailleurs remarquer qu'il découle des précédentes définitions que

$$\ker(q) = E^\perp,$$

et que tout vecteur isotrope est orthogonal à lui-même.

Remarque 3.13 *La notion d'orthogonalité existe également pour les formes bilinéaires non symétriques et plus généralement définies sur $E \times F$, avec $E \neq F$. Par exemple, lorsque $F = E^*$ et que la forme correspond à l'appariement dual, l'orthogonal d'un sous-espace vectoriel A de E est l'ensemble des formes linéaires s'annulant sur A, noté A° (voir l'annexe B).*

Proposition 3.14 *Soit A et B des parties de E. On a*

2. Ceci découle de la bilinéarité de la forme polaire.

3. Ce résultat se prouve par double inclusion. Tout d'abord, on a $A \subset \mathrm{Vect}(A)$ et la deuxième assertion de la proposition 3.14 assure alors que $\mathrm{Vect}(A)^\perp \subset A^\perp$. Réciproquement, tout élément de $\mathrm{Vect}(A)$ s'écrit comme une combinaison d'éléments de A, auxquels tout vecteur de $A^\perp$ est orthogonal. En utilisant alors la bilinéarité de la forme polaire, on montre que tout élément de $A^\perp$ est orthogonal à tout élément de $\mathrm{Vect}(A)$, d'où $A^\perp \subset \mathrm{Vect}(A)^\perp$.

(i) $A \subset \left(A^\perp\right)^\perp$,

(ii) $A \subset B \implies B^\perp \subset A^\perp$.

DÉMONSTRATION.

(i) Soit x un vecteur de A. On a

$$\forall y \in A^\perp,\ b(x,y) = 0,$$

d'où x est orthogonal à tout vecteur de $A^\perp$ et appartient donc à $\left(A^\perp\right)^\perp$.

(ii) Soit y un vecteur de $B^\perp$. On a

$$\forall x \in B,\ b(x,y) = 0.$$

En particulier, cette égalité est vraie pour tout vecteur x de A, puisque A est inclus dans B. Par conséquent, le vecteur y appartient à $A^\perp$.

□

Proposition 3.15 *On suppose que l'espace E est de dimension finie. Pour tout sous-espace vectoriel A de E, on a*

(i) $\dim(A) + \dim\left(A^\perp\right) = \dim(E) + \dim(A \cap \ker(q))$,

(ii) $\left(A^\perp\right)^\perp = A + \ker(q)$.

DÉMONSTRATION.

(i) On considère la restriction de $R(b)$ au sous-espace A, que l'on note φ. Par le théorème du rang, on a

$$\dim(A) = \dim(\mathrm{Im}(\varphi)) + \dim(\ker(\varphi)).$$

On a $\ker(\varphi) = A \cap \ker(b)$ d'une part et $\mathrm{Im}(\varphi)^\circ = \{x \in E \mid \forall y \in A,\ b(x,y) = 0\} = A^\perp$ d'autre part, où $\mathrm{Im}(\varphi)^\circ$ désigne l'orthogonal (au sens de la dualité) du sous-espace vectoriel $\mathrm{Im}(\varphi)$ du dual E^* (voir la section B.4 de l'annexe B). En vertu du théorème B.13, on sait que $\dim(E) = \dim(\mathrm{Im}(\varphi)) + \dim(\mathrm{Im}(\varphi)^\circ)$ et on a donc

$$\begin{aligned}\dim\left(A^\perp\right) &= \dim(E) - \dim(\mathrm{Im}(\varphi)) \\ &= \dim(E) - (\dim(A) - \dim(\ker(\varphi))) \\ &= \dim(E) - \dim(A) + \dim(A \cap \ker(q)).\end{aligned}$$

(ii) On sait d'après la précédente proposition que $A \subset \left(A^\perp\right)^\perp$ et on a par ailleurs que $\ker(q) \subset \left(A^\perp\right)^\perp$. On a par conséquent que $A + \ker(\varphi) \subset \left(A^\perp\right)^\perp$. En appliquant à $A^\perp$ l'égalité obtenue dans la première partie de la proposition et en utilisant que $\ker(q) \subset A^\perp$, il vient alors

$$\dim\left(A^\perp\right) + \dim\left(\left(A^\perp\right)^\perp\right) = \dim(E) + \dim\left(A^\perp \cap \ker(q)\right) = \dim(E) + \dim(\ker(q)).$$

En retranchant à cette égalité celle obtenue dans la première partie de la proposition, on trouve

$$\dim\left(\left(A^\perp\right)^\perp\right) - \dim(A) = \dim(\ker(q)) - \dim(A \cap \ker(q)),$$

d'où, par la formule de Grassmann,

$$\dim\left(\left(A^\perp\right)^\perp\right) = \dim(A + \ker(q)),$$

ce qui permet de conclure.

□

Si E est de dimension finie et que la forme q est non dégénérée, on a obtenu que, pour tout sous-espace vectoriel A de E,

$$\dim\left(A^\perp\right) = \dim(E) - \dim(A) \text{ et } \left(A^\perp\right)^\perp = A.$$

Bien que les dimensions respectives de A et $A^\perp$ soient complémentaires, cela ne veut pas nécessairement dire que ces sous-espaces sont supplémentaires.

Exemple 3.16 *On a précédemment vu que la forme quadratique définie sur $\mathbb{R}^2$ par $q(x) = {x_1}^2 - {x_2}^2$, de forme polaire associée $b(x,y) = x_1y_1 - x_2y_2$, est non dégénérée. Pour cette forme, le sous-espace vectoriel engendré par le vecteur $(1,1)$ est son propre orthogonal.*

Lemme 3.17 *Une famille de vecteurs non isotropes et deux à deux q-orthogonaux est libre.*

DÉMONSTRATION. Soit m un entier naturel non nul et $\{\varepsilon_1, \dots, \varepsilon_m\}$ une famille de vecteurs non isotropes et deux à deux q-orthogonaux. Pour tout m-uplet de scalaires $(\alpha_1, \dots, \alpha_m)$ tel que $\sum_{j=1}^{m} \alpha_j \varepsilon_j = 0_E$, on a :

$$\forall i \in \{1, \dots, m\},\ 0 = b\left(\sum_{j=1}^{m} \alpha_j \varepsilon_j, \varepsilon_i\right) = \sum_{j=1}^{m} \alpha_j b(\varepsilon_j, \varepsilon_i) = \alpha_i q(\varepsilon_i),$$

d'où $\alpha_1 = \cdots = \alpha_m = 0$. La famille est donc libre. □

Définition 3.18 (base q-orthogonale) *Une base $\mathscr{B}$ de E est dite q-**orthogonale** si ses éléments sont deux à deux orthogonaux pour q.*

Si E est de dimension finie non nulle égale à n et que $\mathscr{B} = \{\varepsilon_1, \dots, \varepsilon_n\}$ est une base q-orthogonale de E, alors on a

$$q\left(\sum_{i=1}^{n} x_i\, \varepsilon_i\right) = \sum_{i=1}^{n} {x_i}^2\, q(\varepsilon_i).$$

Autrement dit, la matrice de q relativement à la base $\mathscr{B}$ est *diagonale*.

Théorème 3.19 *On suppose que l'espace E est de dimension finie non nulle. Alors, il existe une base q-orthogonale de E.*

DÉMONSTRATION. On va raisonner par récurrence sur la dimension de E, qu'on note n.

Si $n = 1$, il n'y a rien à montrer. On suppose donc que l'entier n est strictement plus grand que 1. Si la forme q est nulle, toute base est q-orthogonale. Sinon, il existe un vecteur ε_1 de E tel que $q(\varepsilon_1) \neq 0$ et l'hypothèse de récurrence suppose alors qu'il existe une base q-orthogonale de tout sous-espace vectoriel de E de dimension $n-1$. On pose

$$H = \{x \in E \mid b(\varepsilon_1, x) = 0\} = \{\varepsilon_1\}^{\perp}.$$

Le sous-espace H est un hyperplan de E (c'est le noyau d'une forme linéaire non nulle). En notant $\{\varepsilon_2, \dots, \varepsilon_n\}$ une base q-orthogonale de H, on a que $\{\varepsilon_1, \dots, \varepsilon_n\}$ est une base q-orthogonale de E. □

Ce résultat assure l'existence d'une base q-orthogonale en dimension finie.

Soit $\mathscr{B} = \{\varepsilon_1, \dots, \varepsilon_n\}$ une telle base. En posant $\mu_i = q(\varepsilon_i)$ pour tout entier i de $\{1, \dots, n\}$, on a

$$\forall x \in E,\ q(x) = q\left(\sum_{i=1}^{n} x_i\, \varepsilon_i\right) = \sum_{i=1}^{n} \mu_i\, {x_i}^2 = \sum_{i=1}^{n} \mu_i\, (\varepsilon_i^*(x))^2,$$

où $\{\varepsilon_i^*\}_{i=1,\dots,n}$ est la base duale de $\mathscr{B}$. On a ainsi écrit q comme une combinaison linéaire de carrés de formes linéaires linéairement indépendantes. En pratique, de telles formes linéaires peuvent être déterminées grâce à un procédé algorithmique de complétion des carrés portant le nom de *réduction de Gauss*.

Réduction de Gauss d'une forme quadratique

Soit E un espace vectoriel de dimension n sur un corps de caractéristique différente de 2 et q une forme quadratique sur E s'écrivant

$$\forall x \in E,\ q(x) = \sum_{i=1}^{n} a_{ii}\, {x_i}^2 + \sum_{i=1}^{n} \sum_{j=i+1}^{n} a_{ij}\, x_i x_j.$$

En procédant itérativement, on va écrire la forme q comme une combinaison linéaire de carrés de formes linéaires sur E linéairement indépendantes. Deux cas se présentent.

1. Il existe au moins un indice i dans $\{1, \dots, n\}$ pour lequel le coefficient a_{ii} est non nul, par exemple

$a_{11} = a \neq 0$. On peut alors écrire q sous la forme

$$\forall x \in E,\ q(x) = a\, {x_1}^2 + x_1 \ell(x_2, \dots, x_n) + \tilde{q}(x_2, \dots, x_n),$$

où ℓ et $\tilde{q}$ sont des formes respectivement linéaire et quadratique en les variables $x_2, \dots, x_n$, que l'on réécrit comme

$$\forall x \in E,\ q(x) = a \left(x_1 + \frac{1}{2a} \ell(x_2, \dots, x_n) \right)^2 + \tilde{q}(x_2, \dots, x_n) - \frac{1}{4a} (\ell(x_2, \dots, x_n))^2.$$

La forme q est alors la somme d'une constante multipliée par le carré d'une forme linéaire et d'une forme quadratique en les $n-1$ variables $x_2, \dots, x_n$. On réitère ensuite le procédé sur cette dernière forme jusqu'à arriver à la forme souhaitée.

2. Pour tout indice i dans $\{1, \dots, n\}$, le coefficient a_{ii} est nul. Si la forme q est nulle, on a achevé la réduction. Sinon, il existe au moins un coefficient a_{ij}, pour lequel l'indice i est strictement inférieur à l'indice j, non nul, par exemple $a_{12} = a \neq 0$. On peut alors écrire q sous la forme

$$\forall x \in E,\ q(x) = a\, x_1 x_2 + x_1 \ell_1(x_3, \dots, x_n) + x_2 \ell_2(x_3, \dots, x_n) + \tilde{q}(x_3, \dots, x_n),$$

où ℓ_1 et ℓ_2 sont des formes linéaires et $\tilde{q}$ est une forme quadratique en les variables $x_3, \dots, x_n$, que l'on réécrit comme[a]

$$\begin{aligned}
\forall x \in E,\ q(x) = {} & a \left(x_1 + \frac{1}{a} \ell_2(x_3, \dots, x_n) \right) \left(x_2 + \frac{1}{a} \ell_1(x_3, \dots, x_n) \right) + \tilde{q}(x_3, \dots, x_n) \\
& - \frac{1}{a} \ell_1(x_3, \dots, x_n) \ell_2(x_3, \dots, x_n) \\
= {} & \frac{a}{4} \left(x_1 + x_2 + \frac{1}{a} (\ell_1(x_3, \dots, x_n) + \ell_2(x_3, \dots, x_n)) \right)^2 \\
& - \frac{a}{4} \left(x_1 - x_2 + \frac{1}{a} (\ell_2(x_3, \dots, x_n) - \ell_1(x_3, \dots, x_n)) \right)^2 + \tilde{q}(x_3, \dots, x_n) \\
& - \frac{1}{a} \ell_1(x_3, \dots, x_n) \ell_2(x_3, \dots, x_n).
\end{aligned}$$

Le premier terme dans le membre de droite de la dernière égalité contient deux carrés de formes linéaires linéairement indépendantes et une forme quadratique en les $n-2$ variables $x_3, \dots, x_n$. On réitère ensuite le procédé sur cette dernière forme jusqu'à arriver à la forme souhaitée.

a. On peut noter qu'on utilise ici l'identité remarquable

$$\forall (a, b) \in \mathbb{R}^2,\ ab = \frac{1}{4} \left[(a+b)^2 - (a-b)^2 \right].$$

En appliquant le procédé de réduction de Gauss, on arrive à une *forme réduite* de q,

$$\forall x \in E,\ q(x) = \sum_{i=1}^{r} \alpha_i (\ell_i(x))^2, \tag{3.2}$$

c'est-à-dire l'écriture de q sous la forme d'une combinaison linéaire de r carrés de formes linéaires linéairement indépendantes (on n'a pas prouvé ce dernier point, mais il est facile de le vérifier), l'entier r étant alors[4] le rang de q.

Exemple 3.20 (réduction de Gauss d'une forme quadratique sur $\mathbb{R}^3$) *On considère la forme quadratique sur $\mathbb{R}^3$ donnée par*

$$\forall x \in E,\ q(x) = 2{x_1}^2 - 2{x_2}^2 - 6{x_3}^2 + 3x_1x_2 - 4x_1x_3 + 7x_2x_3.$$

4. Le noyau de q étant l'intersection des noyaux de r formes linéaires linéairement indépendantes, il est de dimension $\dim(E) - r$ et l'on conclut par le théorème du rang.

On a

$$\begin{aligned} q(x) &= 2{x_1}^2 + x_1(3x_2 - 4x_3) - 2{x_2}^2 - 6{x_3}^2 + 7x_2x_3 \\ &= 2\left(x_1 + \frac{3}{4}x_2 - x_3\right)^2 - \frac{9}{8}{x_2}^2 + 3x_2x_3 - 2{x_3}^3 - 2{x_2}^2 - 6{x_3}^2 + 7x_2x_3 \\ &= 2\left(x_1 + \frac{3}{4}x_2 - x_3\right)^2 - \frac{25}{8}{x_2}^2 + 10x_2x_3 - 8{x_3}^2 \\ &= 2\left(x_1 + \frac{3}{4}x_2 - x_3\right)^2 - \frac{25}{8}\left(x_2 - \frac{8}{5}x_3\right)^2 + 8{x_3}^2 - 8{x_3}^2 \\ &= 2\left(x_1 + \frac{3}{4}x_2 - x_3\right)^2 - \frac{25}{8}\left(x_2 - \frac{8}{5}x_3\right)^2. \end{aligned}$$

Exemple 3.21 (réduction de Gauss d'une forme quadratique sur $\mathbb{R}^4$) *On considère la forme quadratique sur $\mathbb{R}^4$ donnée par*

$$\forall x \in E,\ q(x) = x_1x_2 + x_2x_3 + x_3x_4 + x_1x_4.$$

Dans celle-ci, aucun carré n'apparaît et l'on se trouve par conséquent dans le second cas de figure décrit dans le procédé itératif de réduction. On a alors

$$q(x) = (x_1 + x_3)(x_2 + x_4) = \frac{1}{4}(x_1 + x_3 + x_2 + x_4)^2 - \frac{1}{4}(x_1 + x_3 - x_2 - x_4)^2.$$

Remarque 3.22 *L'article [BW66] décrit comment une réduction de Gauss d'une forme quadratique peut être obtenue en appliquant à la matrice de cette forme quadratique relativement à une base donnée une variante du procédé d'élimination de Gauss apparentée à la méthode de factorisation de Crout [Cro41], combinée selon les cas à une renumérotation des coordonnées ou des changements de coordonnées. On peut ici utiliser cette approche pour reprendre les exemples 3.20 et 3.21, qui illustrent les deux cas de figure auxquels on peut se trouver confronté en pratique. Dans le premier cas, la matrice de la forme quadratique relativement à la base canonique de $\mathbb{R}^3$ est*

$$\begin{pmatrix} 2 & \frac{3}{2} & -2 \\ \frac{3}{2} & -2 & \frac{7}{2} \\ -2 & \frac{7}{2} & -6 \end{pmatrix}.$$

En appliquant le procédé d'élimination de Gauss (sans échange de lignes) à cette matrice[5]*, on est conduit après deux étapes à la matrice triangulaire supérieure*

$$\begin{pmatrix} 2 & \frac{3}{2} & -2 \\ 0 & -\frac{25}{8} & 5 \\ 0 & 0 & 0 \end{pmatrix}.$$

Chaque ligne non nulle de la matrice est ensuite divisée par la valeur du pivot correspondant, qui est par ailleurs conservée. On trouve ainsi

$$\begin{pmatrix} 1 & \frac{3}{4} & -1 \\ 0 & 1 & -\frac{8}{5} \\ 0 & 0 & 0 \end{pmatrix},$$

avec les deux valeurs de pivot 2 et $-\frac{25}{8}$. Les coefficients des formes linéaires linéairement indépendantes de la forme réduite obtenue sont respectivement les coefficients des lignes non nulles de cette matrice et les coefficients associés dans la combinaison linéaire des carrés de ces formes sont les valeurs des pivots. On a

$$\forall x \in \mathbb{R}^3,\ q(x) = 2\left(x_1 + \frac{3}{4}x_2 - x_3\right)^2 - \frac{25}{8}\left(x_2 - \frac{8}{5}x_3\right)^2.$$

5. Ce n'est en effet pas nécessaire puisque les premiers deux pivots, apparaissant sur la diagonale de la matrice et permettant l'élimination, sont non nuls, ce qui traduit le fait qu'on a seulement eu à compléter deux carrés au cours de la réduction dans l'exemple 3.20.

Dans le second exemple, la matrice de la forme quadratique dans la base canonique de $\mathbb{R}^4$ *est*

$$\begin{pmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

Tous les coefficients diagonaux étant nuls, il n'est pas possible de trouver une renumérotation des coordonnées permettant d'effectuer l'élimination[6]*. En revanche, le coefficient situé à l'intersection de première ligne et la seconde colonne est non nul*[7]*. On fait alors les changements de coordonnées suivants :* $\tilde{x}_1 = \frac{1}{2}(-x_1 + x_2)$*,* $\tilde{x}_2 = \frac{1}{2}(x_1 + x_2)$*,* $\tilde{x}_3 = x_3$ *et* $\tilde{x}_4 = x_4$*, ce qui conduit à la matrice*

$$\begin{pmatrix} -1 & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}$$

pour la forme quadratique relativement à la base de $\mathbb{R}^4$ *induite par ces changements*[8]*. On est en mesure d'appliquer à cette matrice le procédé d'élimination et l'on trouve, après seulement deux étapes, la matrice triangulaire supérieure*

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

On en déduit une forme réduite de la forme quadratique dans le nouveau système de coordonnées, que l'on peut alors réécrire dans les coordonnées d'origine de la manière suivante :

$$\forall x \in \mathbb{R}^3,\ q(x) = -\left(\left(\frac{1}{2}(-x_1 + x_2)\right) - \frac{1}{2}x_3 + \frac{1}{2}x_4\right)^2 + \left(\left(\frac{1}{2}(x_1 + x_2)\right) + \frac{1}{2}x_3 + \frac{1}{2}x_4\right)^2.$$

Si le rang de q est strictement inférieur à n, on peut compléter la famille libre de formes linéaires trouvée à l'issue de la réduction en une base de E^* avec des formes linéaires $\ell_{r+1}, \dots, \ell_n$ bien choisies. Il existe alors une unique base $\{\varepsilon_i\}_{i=1,\dots,n}$ de E dont $\{\ell_i\}_{i=1,\dots,n}$ est la base duale, c'est-à-dire

$$\forall i \in \{1, \dots, n\},\ \varepsilon_i^* = \ell_i.$$

Cette base est bien telle que voulue puisque l'on a

$$\forall i \in \{1, \dots, n\},\ q(\varepsilon_i) = \begin{cases} \alpha_i & \text{si } i \in \{1, \dots, r\} \\ 0 & \text{sinon} \end{cases},$$

6. Ceci traduit le fait qu'on n'a pas été en mesure de compléter des carrés pour réaliser la réduction dans l'exemple 3.21 et qu'on a dû faire appel à une identité remarquable particulière pour faire apparaître simultanément deux carrés.

7. On peut observer que l'on trouvera toujours un coefficient extradiagonal non nul, faute de quoi la réduction serait achevée.

8. Plus généralement, en considérant une matrice d'ordre n, en notant k l'entier naturel correspondant à l'étape courante dans le procédé d'élimination et en supposant que tous les coefficients matriciels diagonaux $m_{ii}^{(k)}$ d'indice i supérieur ou égal à $k+1$ sont nuls et que (sans perte de généralité) le coefficient $m_{k+1\,k+2}^{(k)}$ est non nul, les coefficients du bloc symétrique restant à éliminer dans le nouveau système de coordonnées, notés $\tilde{m}_{ij}^{(k)}$, pour tout couple (i, j) dans $\{k+1, \dots, n\}^2$, s'expriment en fonction de ceux de la matrice $M^{(k)}$ comme suit (le bloc étant symétrique, on ne donne que les coefficients sur et au-dessus de la diagonale) :

$$\begin{aligned}
&\tilde{m}_{k+1\,k+1}^{(k)} = -2m_{k+1\,k+2}^{(k)}, \\
&\tilde{m}_{k+1\,k+2}^{(k)} = 0, \\
&\tilde{m}_{k+1\,j}^{(k)} = -m_{k+1\,j}^{(k)} + m_{k+2\,j}^{(k)},\ j = k+3, \dots, n, \\
&\tilde{m}_{k+2\,k+2}^{(k)} = 2m_{k+1\,k+2}^{(k)}, \\
&\tilde{m}_{k+2\,j}^{(k)} = m_{k+1\,j}^{(k)} + m_{k+2\,j}^{(k)},\ j = k+3, \dots, n, \\
&\tilde{m}_{ij}^{(k)} = m_{ij}^{(k)},\ i = k+3, \dots, n,\ j = i, \dots, n.
\end{aligned}$$

ce qui fournit les éléments diagonaux de la matrice de q. La forme polaire de q s'écrivant

$$\forall (x,y)\in E^2,\ b(x,y)=\sum_{i=1}^{r}\alpha_i\,\ell_i(x)\ell_i(y),$$

on a par ailleurs

$$\forall (i,j)\in\{1,\dots,n\}^2,\ i\neq j,\ b(\varepsilon_i,\varepsilon_j)=0.$$

Remarque 3.23 *Il existe d'autres moyens que la réduction de Gauss pour arriver à l'écriture d'une forme quadratique sous forme réduite. Il n'y a d'ailleurs pas unicité de cette dernière. Néanmoins, le procédé de Gauss possède l'avantage d'être systématique et de toujours conduire à des carrés de formes linéaires linéairement indépendantes.*

On revient sur le calcul effectif d'une base q-orthogonale de l'espace E à partir d'une forme réduite. Connaissant, après éventuellement avoir complété la famille libre issue de la réduction, n formes linéaires, linéairement indépendantes, $\ell_1,\dots,\ell_n$, il s'agit de chercher explicitement l'unique base $\{\varepsilon_1,\dots,\varepsilon_n\}$ de E vérifiant les conditions

$$\forall (i,j)\in\{1,\dots,n\}^2,\ \ell_i(\varepsilon_j)=\delta_{ij}.$$

On parle dans ce cas de base *antéduale* de $\{\ell_1,\dots,\ell_n\}$ (voir la proposition B.6).

Étant donnée une base $\{e_1,\dots,e_n\}$ de E, dans laquelle tout vecteur x de E a pour coordonnées $(x_1,\dots,x_n)$, et $\{e_1^*,\dots,e_n^*\}$ sa base duale, on connaît la matrice de passage R de la base $\{e_1^*,\dots,e_n^*\}$ à la base $\{\ell_1,\dots,\ell_n\}$. Pour déterminer les vecteurs $\varepsilon_1,\dots,\varepsilon_n$, il suffit alors de déterminer l'expression de chacun d'eux dans la base $\{e_1,\dots,e_n\}$, c'est-à-dire de déterminer la matrice de passage P de la base $\{e_1,\dots,e_n\}$ à la base $\{\varepsilon_1,\dots,\varepsilon_n\}$.

La matrice P est la matrice de l'application identique de E en choisissant $\{\varepsilon_1,\dots,\varepsilon_n\}$ comme base de E en tant qu'espace de départ et $\{e_1,\dots,e_n\}$ comme base de E en tant qu'espace d'arrivée. On peut alors vérifier que la matrice transposée de P est la matrice de l'application identique de E^* en choisissant $\{e_1^*,\dots,e_n^*\}$ comme base de E^* en tant qu'espace de départ et $\{\varepsilon_1^*,\dots,\varepsilon_n^*\}$, c'est-à-dire $\{\ell_1,\dots,\ell_n\}$, comme base de E^* en tant qu'espace d'arrivée. On en déduit alors que

$$P^\top=R^{-1},$$

ce qui équivaut à

$$P=\left(R^\top\right)^{-1}.$$

Exemple 3.24 (calcul d'une base q-orthogonale) *La forme quadratique q sur $\mathbb{R}^3$ considérée dans l'exemple 3.20 est de rang égal à 2. En complétant la famille libre constituée des formes linéaires $\ell_1(x)=x_1+\frac{3}{4}x_2-x_3$ et $\ell_2(x)=x_2-\frac{8}{5}x_3$, obtenues par réduction de Gauss, par la forme linéaire $\ell_3(x)=x_3$ pour obtenir une base du dual de $\mathbb{R}^3$, on peut former la matrice de passage*

$$R=\begin{pmatrix}1 & 0 & 0\\ \frac{3}{4} & 1 & 0\\ -1 & -\frac{8}{5} & 1\end{pmatrix},$$

d'où

$$P=\left(R^\top\right)^{-1}=\begin{pmatrix}1 & -\frac{3}{4} & -\frac{1}{5}\\ 0 & 1 & \frac{8}{5}\\ 0 & 0 & 1\end{pmatrix}.$$

Une base q-orthogonale est donc formée des vecteurs $\varepsilon_1=(1,0,0)$, $\varepsilon_2=\left(-\frac{3}{4},1,0\right)$ et $\varepsilon_3=\left(-\frac{1}{5},\frac{8}{5},1\right)$. Relativement à cette base, la matrice de q est

$$\begin{pmatrix}2 & 0 & 0\\ 0 & -\frac{25}{8} & 0\\ 0 & 0 & 0\end{pmatrix}.$$

Proposition 3.25 *On suppose que l'espace E est de dimension finie non nulle. Le noyau d'une forme quadratique q sur E est engendré par les vecteurs isotropes d'une base q-orthogonale de E.*

DÉMONSTRATION. Soit n la dimension de E et $\mathscr{B} = \{\varepsilon_1, \ldots, \varepsilon_n\}$ une base q-orthogonale de E pour laquelle $q(\varepsilon_i) \neq 0$ pour i appartenant à $\{1, \ldots, r\}$ et $q(\varepsilon_i) = 0$ pour i appartenant à $\{r+1, \ldots, n\}$, avec r un entier naturel supposé strictement inférieur à n. Pour tout vecteur x de E, on peut écrire $x = \sum_{i=1}^{n} x_i\, \varepsilon_i$, et le vecteur x appartient au noyau de q si et seulement si $b(x, y) = 0$ pour tout vecteur y de E, c'est-à-dire si et seulement si

$$\forall j \in \{1, \ldots, n\},\ b(x, \varepsilon_j) = \sum_{i=1}^{n} x_i\, b(\varepsilon_i, \varepsilon_j) = x_j\, q(\varepsilon_j) = 0,$$

soit encore

$$\forall j \in \{1, \ldots, r\},\ x_j = 0.$$

On en déduit que $\ker(q) = \mathrm{Vect}(\{\varepsilon_{r+1}, \ldots, \varepsilon_n\})$. □

Exemple 3.26 *Les calculs de l'exemple 3.24 montrent que le noyau de la forme quadratique q sur $\mathbb{R}^3$ considérée dans l'exemple 3.20 est* $\ker(q) = \mathrm{Vect}\left(\left\{\left(-\frac{1}{5}, \frac{8}{5}, 1\right)\right\}\right)$.

On déduit que cette proposition que le rang d'une forme quadratique est donné par le nombre de vecteurs *non isotropes* d'une base q-orthogonale. Il en découle une caractérisation du noyau d'une forme quadratique.

Corollaire 3.27 *Le noyau d'une forme quadratique q est l'intersection des noyaux des formes linéaires linéairement indépendantes apparaissant dans une forme réduite de q.*

DÉMONSTRATION. D'après la précédente proposition, le noyau de q est engendré par les vecteurs isotropes d'une base q-orthogonale de l'espace. On considère la base antéduale associée à la base de E^* obtenue, éventuellement par complétion, à partir des formes linéaires $\ell_1, \ldots, \ell_r$ apparaissant dans une forme réduite de q. Cette base est q-orthogonale et, par la propriété définissant la base antéduale, ses vecteurs isotropes $\varepsilon_{r+1}, \ldots, \varepsilon_n$ sont tels que

$$\forall i \in \{1, \ldots, r\},\ \ell_i(\varepsilon_j) = 0.$$

□

3.3 Classification des formes quadratiques complexes

Dans cette section, on suppose que E est un $\mathbb{C}$-espace vectoriel. On a le résultat suivant.

Théorème 3.28 *On suppose que l'espace E est de dimension finie égale à n. Soit q une forme quadratique sur E. Alors, il existe une base $\{\varepsilon_1, \ldots, \varepsilon_n\}$ de E telle que*

$$q(x) = \sum_{i=1}^{r} {x_i}^2$$

pour tout vecteur x de E tel que $x = \sum_{i=1}^{n} x_i\, \varepsilon_i$, l'entier r étant le rang de q.

DÉMONSTRATION. Il suffit de poser, à partir de la base de E^* obtenue en complétant éventuellement la famille libre de formes linéaires apparaissant dans une forme réduite (3.2) de q,

$$\tilde{\ell}_i = \begin{cases} \sqrt{\alpha_i}\, \ell_i & \text{si } i \in \{1, \ldots, r\} \\ \ell_i & \text{si } i \in \{r+1, \ldots, n\} \end{cases}$$

et de considérer la base antéduale associée à cette base. Relativement à cette dernière, la matrice de q s'écrit par blocs

$$\begin{pmatrix} I_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r} \end{pmatrix}$$

et est de rang r. □

Les formes quadratiques sur des $\mathbb{C}$-espaces vectoriels de dimension finie sont ainsi complètement classifiées par leur rang.

Corollaire 3.29 (équivalence des formes quadratiques complexes) *Deux formes quadratiques sur des $\mathbb{C}$-espaces vectoriels de dimension finie sont équivalentes si et seulement si elles ont même rang.*

3.4 Classification des formes quadratiques réelles

Dans cette section, on suppose que E est un $\mathbb{R}$-espace vectoriel.

Définition 3.30 *Une forme quadratique sur E est dite **positive** (resp. **négative**) si et seulement si*

$$\forall x \in E,\ q(x) \geq 0 \text{ (resp. } q(x) \leq 0).$$

*On dit qu'elle est **définie positive** (resp. **définie négative**) si et seulement si*

$$\forall x \in E,\ x \neq 0_E,\ q(x) > 0 \text{ (resp. } q(x) < 0).$$

Par extension, une matrice symétrique est dite définie positive/positive/définie négative/négative si c'est la matrice d'une forme quadratique définie positive/positive/définie négative/négative sur un $\mathbb{R}$-espace vectoriel de dimension finie.

Remarque 3.31 *Si la définition ci-dessus implique qu'une matrice symétrique (définie) positive (resp. négative) possède des coefficients diagonaux (strictement) positifs (resp. négatifs), elle ne dit en aucune manière qu'une matrice symétrique à coefficients (strictement) positifs (resp. négatifs) est (définie) positive (resp. négative), comme le montre le contre-exemple suivant. Les coefficients de la matrice*

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 2 \\ 0 & 2 & 3 \end{pmatrix}$$

sont positifs, mais l'on a

$$X^\top M X = -1 \text{ pour } X = \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix},$$

et elle n'est donc pas positive. On verra qu'il existe néanmoins des critères assurant qu'une matrice symétrique est (définie) positive (resp. négative).

Théorème et définition 3.32 (« loi d'inertie de Sylvester » [Syl52]) *On suppose que l'espace E est de dimension finie non nulle égale à n. Soit q une forme quadratique sur E. Il existe une base $\{\varepsilon_i\}_{i=1,\dots,n}$ de E et des entiers p et r, avec $0 \leq p \leq r \leq n$, tels que l'on a*

$$q(x) = \sum_{i=1}^{p} {x_i}^2 - \sum_{i=p+1}^{r} {x_i}^2$$

*pour tout vecteur x de E tel que $x = \sum_{i=1}^{n} x_i\, \varepsilon_i$ (dans cette expression, la première (resp. seconde) somme est nulle si $p = 0$ (resp. $p = r$)). De plus, les entiers p et r sont indépendants de la base choisie pour mettre q sous cette forme et r est en particulier le rang de q. Enfin, le couple d'entiers $(p, r-p)$ est appelé la **signature** de q.*

DÉMONSTRATION. Dans une forme réduite de q (voir (3.2)), on renumérote les termes de manière à ce que

$$\forall x \in E,\ q(x) = \sum_{i=1}^{p} \alpha_i\, (\ell_i(x))^2 + \sum_{i=p+1}^{r} \alpha_i\, (\ell_i(x))^2,$$

avec $\alpha_i > 0$ si i appartient à $\{1, \dots, p\}$ et $\alpha_i < 0$ si i appartient à $\{p+1, \dots, r\}$. En complétant au besoin la famille libre de formes linéaires apparaissant dans cette écriture de q par des formes linéaires $\ell_{r+1}, \dots, \ell_n$ de manière à obtenir une base de E^*, on pose alors

$$\tilde{\ell}_i = \begin{cases} \sqrt{\alpha_i}\, \ell_i & \text{si } i \in \{1, \dots, p\} \\ \sqrt{-\alpha_i}\, \ell_i & \text{si } i \in \{p+1, \dots, r\} \\ \ell_i & \text{si } i \in \{r+1, \dots, n\} \end{cases}$$

et on arrive à l'écriture voulue en considérant pour base $\{\varepsilon_i\}_{i=1,\dots,n}$ la base antéduale de $\{\tilde{\ell}_i\}_{i=1,\dots,n}$.

On montre ensuite l'unicité des entiers p et r. Soit $\{\varepsilon_i\}_{i=1,\dots,n}$ et $\{\varepsilon'_i\}_{i=1,\dots,n}$ deux bases de E. On a

$$\forall x \in E,\ x = \sum_{i=1}^{n} x_i\,\varepsilon_i = \sum_{i=1}^{n} x'_i\,\varepsilon'_i,\ q(x) = \sum_{i=1}^{p} {x_i}^2 - \sum_{i=p+1}^{r} {x_i}^2 = \sum_{i=1}^{p'} {x'_i}^2 - \sum_{i=p'+1}^{r'} {x'_i}^2.$$

Posons $F = \text{Vect}(\{\varepsilon_1,\dots,\varepsilon_p\})$, $G = \text{Vect}(\{\varepsilon_{p+1},\dots,\varepsilon_r\})$, $H = \text{Vect}(\{\varepsilon_{r+1},\dots,\varepsilon_n\})$, $F' = \text{Vect}(\{\varepsilon'_1,\dots,\varepsilon'_{p'}\})$, $G' = \text{Vect}(\{\varepsilon'_{p'+1},\dots,\varepsilon'_{r'}\})$ et $H' = \text{Vect}(\{\varepsilon'_{r'+1},\dots,\varepsilon'_n\})$. On a $F \cap G' = \{0_E\}$. En effet, s'il existe un vecteur x non nul appartenant à $F \cap G'$, on a $q(x) > 0$ et $q(x) < 0$, ce qui est impossible. On a aussi $F \cap H' = \{0_E\}$, car sinon, il existerait un vecteur x non nul tel que $q(x) > 0$ et $q(x) = 0$, ce qui est impossible. Il vient ainsi que F, G' et H' sont en somme directe et on a par conséquent $\dim(F) + \dim(G') + \dim(H') \leq \dim(E)$, soit encore

$$p + r' - p' + (n - r') \leq n \implies p \leq p'.$$

De la même manière, on a $F' \cap G = \{0_E\}$ et $F' \cap H = \{0_E\}$, ce qui permet de montrer que $p' \leq p$ et donc que $p = p'$. En utilisant le même raisonnement avec G et $F' \cup H'$ pour trouver que

$$(r - p) + (n - (r' - p)) \leq n \implies r \leq r',$$

puis avec G' et $F \cup H$ pour obtenir que

$$(r' - p) + (n - (r - p)) \leq n \implies r' \leq r,$$

on déduit que $r = r'$.

Enfin, la matrice de la forme q relativement à la base $\{\varepsilon_i\}_{i=1,\dots,n}$ introduite plus haut s'écrit par blocs

$$\begin{pmatrix} I_p & 0_{p,r-p} & 0_{p,n-r} \\ 0_{r-p,p} & -I_{r-p} & 0_{r-p,n-r} \\ 0_{n-r,p} & 0_{n-r,r-p} & 0_{n-r} \end{pmatrix}$$

et est donc de rang r. □

Remarque 3.33 *Le théorème précédent montre que la signature et le rang d'une forme quadratique ne dépendent pas de la base relativement à laquelle sa matrice est diagonale : on dit que ce sont des*[9] invariants *de la forme.*

On déduit du dernier théorème le résultat suivant.

Corollaire 3.34 (équivalence des formes quadratiques réelles) *Deux formes quadratiques sur des $\mathbb{R}$-espaces vectoriels de dimension finie sont équivalentes si et seulement si elles ont même signature.*

Les entiers p et $r - p$ sont respectivement la dimension maximale des sous-espaces de E sur lesquels la forme q est définie positive et la dimension maximale des sous-espaces de E sur lesquels la forme q est définie négative. On ne peut cependant parler du « plus grand » sous-espace vectoriel sur lequel q est définie positive car un tel sous-espace n'existe généralement pas, comme le montre l'exemple suivant.

Exemple 3.35 *Sur $\mathbb{R}^2$, la forme $q(x) = {x_1}^2 - {x_2}^2$, de forme polaire $b(x,y) = x_1y_1 - x_2y_2$, a pour signature $(1,1)$. On remarque que, si $|x_1| > |x_2|$, on a $q(x) > 0$. La restriction de q à toute droite dont la pente a une valeur absolue strictement plus petite que 1 est donc définie positive. De la même manière, sa restriction à toute droite dont la pente a une valeur absolue strictement plus grande que 1 est définie négative. Elle n'est cependant pas définie positive ou définie négative sur $\mathbb{R}^2$ (hormis $\{0_{\mathbb{R}^2}\}$ et $\mathbb{R}^2$ lui-même, les sous-espaces vectoriels de $\mathbb{R}^2$ sont des droites caractérisées par leurs pentes).*

Il découle du précédent résultat qu'une forme quadratique est
— positive si sa signature est $(r, 0)$,
— négative si sa signature est $(0, r)$,
— définie positive si sa signature est $(n, 0)$,

9. Ce ne sont pas les seuls.

— définie négative si sa signature est $(0,n)$,
— non dégénérée si sa signature est $(p,n-p)$, *i.e.* $r=n$.

Il est important de noter que la matrice d'une forme quadratique définie positive (ou définie négative), relativement à n'importe quelle base de l'espace, est inversible, puisque de rang égal à son ordre.

Un résultat utile pour montrer qu'une forme quadratique est définie positive est basé sur une propriété caractérisant les matrices réelles symétriques définies positives.

Théorème 3.36 (« critère de Sylvester ») *Soit n un entier naturel non nul. Une matrice réelle symétrique M d'ordre n est définie positive si et seulement si tous ses mineurs principaux dominants (ou primaires) sont strictement positifs, c'est-à-dire*

$$\forall k \in \{1,\dots,n\},\ \det(M_k) > 0,$$

où

$$M_k = \begin{pmatrix} m_{11} & \dots & m_{1k} \\ \vdots & & \vdots \\ m_{k1} & \dots & m_{kk} \end{pmatrix}.$$

DÉMONSTRATION. On montre tout d'abord que la condition est nécessaire. Pour cela, on introduit une forme quadratique q sur un espace vectoriel réel E de dimension égale à n, dont la matrice symétrique M est la matrice relativement à une base donnée de E. Si M est définie positive, alors q également et l'on sait (voir le théorème 3.32) qu'il existe une base $\{\varepsilon_i\}_{i=1,\dots,n}$ relativement à laquelle la matrice de q est la matrice identité, c'est-à-dire qu'il existe une matrice inversible P telle que

$$I_n = P^\top M P.$$

On a ainsi

$$1 = \det(P)^2 \det(M),$$

dont on déduit que $\det(M)$ est strictement positif. En considérant la restriction de la forme q au sous-espace vectoriel engendré $\mathrm{Vect}(\{\varepsilon_1,\dots,\varepsilon_k\})$ et en procédant de manière similaire pour k allant de 1 à $n-1$, on montre que tout mineur principal dominant de M est strictement positif.

Pour montrer que la condition est suffisante, on raisonne par récurrence sur l'ordre de la matrice, c'est-à-dire sur l'entier naturel non nul n. Pour $n=1$, c'est évident, puisque qu'on peut identifier M_1 à un réel strictement positif. Supposons le résultat vrai pour toute matrice d'ordre $n-1$, avec n un entier supérieur ou égal à 2, et considérons la matrice symétrique M_n, que l'on peut écrire par blocs sous la forme

$$M_n = \begin{pmatrix} M_{n-1} & m \\ m^\top & \alpha \end{pmatrix},$$

avec m appartenant à $M_{n-1,1}(\mathbb{R})$ et α appartenant à $\mathbb{R}$. La matrice M_{n-1} étant symétrique définie positive par hypothèse de récurrence, elle est inversible et ses colonnes forment une base de $M_{n-1,1}(\mathbb{R})$ et l'on peut par conséquent écrire m comme une (unique) combinaison linéaire de ces dernières, dont on note $\alpha_1,\dots,\alpha_{n-1}$ les coefficients. En considérant alors la matrice inversible d'ordre n

$$P = \begin{pmatrix} 1 & 0 & \dots & 0 & -\alpha_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & \ddots & -\alpha_{n-1} \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix},$$

on vérifie que

$$P^\top M_n P = \begin{pmatrix} M_{n-1} & 0 \\ 0^\top & \alpha \end{pmatrix},$$

d'où $\det(P^\top M_n P) = (\det(P))^2 \det(M_n) = \det(M_{n-1})\,\alpha$. Puisque les mineurs $\det(M_n)$ et $\det(M_{n-1})$ sont strictement positifs, on en déduit que α l'est aussi. Le caractère défini positif de M_n étant équivalent à celui de la matrice

$P^\top M_n P$, on peut alors conclure en écrivant que

$$\forall X \in M_{n,1}(\mathbb{R}),\ X^\top P^\top M_n P X = \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}^\top M_{n-1} \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} + \alpha\,(x_n)^2,$$

et en utilisant que la matrice M_{n-1} est définie positive et le réel α est strictement positif. □

Remarque 3.37 *L'article [Gio17] recense différentes preuves du critère de Sylvester existant dans la littérature.*

On tire de ce résultat un critère pour déterminer si une matrice symétrique réelle est définie *négative* en utilisant le fait que son opposée est définie positive.

Remarque 3.38 *On pourrait penser qu'un critère analogue au critère de Sylvester pour une matrice symétrique positive serait que tous les mineurs dominants principaux soient positifs. Ceci est faux, comme l'illustre le contre-exemple de la matrice*

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

dont les mineurs principaux dominants sont nuls, et par conséquent positifs, et qui est symétrique négative. On peut en revanche montrer (voir [Pru86]) qu'une condition nécessaire et suffisante est que tous[10] *les mineurs principaux de la matrice soient positifs.*

On termine cette section en se focalisant sur le cas des formes quadratiques *positives*.

Théorème 3.39 (« inégalité de Cauchy–Schwarz ») *Soit q une forme quadratique positive sur E, de forme polaire b. On a*

$$\forall (x,y) \in E^2,\ |b(x,y)| \leq \sqrt{q(x)}\sqrt{q(y)}.$$

Si de plus la forme q est définie, il y a égalité dans l'inégalité si et seulement si les vecteurs x et y sont linéairement dépendants.

DÉMONSTRATION. La forme q étant positive, on a

$$\forall t \in \mathbb{R},\ \forall (x,y) \in E^2,\ q(t\,x+y) = t^2\,q(x) + 2t\,b(x,y) + q(y) \geq 0.$$

Si $q(x) = 0$, l'inégalité ci-dessus devient

$$\forall t \in \mathbb{R},\ 2t\,b(x,y) + q(y) \geq 0,$$

ce qui entraîne que $b(x,y) = 0$. Sinon, le trinôme du second degré en t à gauche de l'inégalité possède un discriminant négatif, ce qui s'écrit encore

$$b(x,y)^2 - q(x)q(y) \leq 0,$$

conduisant à l'inégalité annoncée.

Si q est de plus définie, on suppose que le vecteur x est non nul (l'inégalité étant triviale lorsque ce n'est pas le cas). Le nombre réel $q(x)$ est alors non nul, de sorte qu'on a égalité si et seulement le discriminant ci-dessus est nul, c'est-à-dire si et seulement s'il existe un réel t_0 tel que $q(t_0\,x+y) = 0$, ce qui équivaut à $t_0\,x + y = 0_E$. □

Corollaire 3.40 *Soit q une forme quadratique positive sur E. Le cône isotrope de q est égal à son noyau.*

DÉMONSTRATION. On a toujours $\ker(q) \subset \mathscr{C}_q$ et il faut donc juste prouver l'inclusion réciproque. Soit x un vecteur appartenant à $\mathscr{C}_q$ et y un vecteur de E. En vertu de l'inégalité de Cauchy–Schwarz, en notant b la forme polaire de q, on a

$$0 \leq |b(x,y)| \leq \sqrt{q(x)}\sqrt{q(y)} = 0,$$

ce qui implique que $b(x,y) = 0$, d'où x appartient à $\ker(q)$. □

Ce résultat vaut également pour une forme quadratique négative. Une forme positive (ou négative) est donc non dégénérée si et seulement si elle est définie.

10. Pour une matrice d'ordre n, ces déterminants sont au nombre de $\sum_{k=1}^{n} \binom{n}{k} = 2^n - 1$.

Corollaire 3.41 (« inégalité de Minkowski ») *Soit q une forme quadratique positive sur E. On a*

$$\forall (x,y)\in E^2,\ \sqrt{q(x+y)}\leq \sqrt{q(x)}+\sqrt{q(y)}.$$

DÉMONSTRATION. C'est une conséquence directe de l'inégalité de Cauchy–Schwarz. En notant b la forme polaire de q, on a en effet

$$\forall (x,y)\in E^2,\ q(x+y)=q(x)+2\,b(x,y)+q(y)\leq q(x)+2\sqrt{q(x)}\sqrt{q(y)}+q(y)=\left(\sqrt{q(x)}+\sqrt{q(y)}\right)^2.$$

□

3.5 Formes quadratiques hermitiennes

En raison de leurs propriétés, les formes quadratiques définies positives sur un $\mathbb{R}$-espace vectoriel jouent un rôle important, notamment en physique mathématique. On verra dans le prochain chapitre qu'on peut par exemple les utiliser pour définir des *normes*. Sur un $\mathbb{C}$-espace vectoriel, il ne peut y avoir de forme quadratique positive, car si $q(x)$ est une quantité positive alors $q(\mathrm{i}x)=\mathrm{i}^2q(x)=-q(x)$ est une quantité négative. Néanmoins, on peut construire une théorie en tous points semblable à celle dans le cas réel en utilisant à la place de la notion de forme quadratique celle de forme quadratique *hermitienne*, associée à une forme sesquilinéaire à symétrie hermitienne.

Définition 3.42 (forme quadratiques hermitienne) *Soit E un $\mathbb{C}$-espace vectoriel. Une application h de E dans $\mathbb{R}$ est une **forme quadratique hermitienne** sur E si et seulement s'il existe une forme s sesquilinéaire hermitienne sur E telle que*

$$\forall x\in E,\ h(x)=s(x,x).$$

La forme s de cette définition est complètement déterminée par h. En effet, comme c'était le cas pour les formes quadratiques, on dispose d'identités de polarisation associées :

$$\begin{aligned}\forall (x,y)\in E^2,\ s(x,y)&=\frac{1}{4}\left(h(x+y)-h(x-y)-\mathrm{i}h(x+\mathrm{i}\,y)+\mathrm{i}h(x-\mathrm{i}\,y)\right),\\&=\frac{1}{2}\left(h(x+y)-\mathrm{i}h(x+\mathrm{i}\,y)-(1-\mathrm{i})(h(x)+h(y))\right),\\&=\frac{1}{2}\left((1-\mathrm{i})(h(x)+h(y))-h(x-y)+\mathrm{i}h(x-\mathrm{i}\,y)\right).\end{aligned}$$

On a pour les formes quadratiques hermitiennes les mêmes définitions de matrices représentatives, rang, noyau, etc. que pour les formes quadratiques.

Chapitre 4

Espaces euclidiens

La notion fondamentale d'*espace euclidien* généralise de manière naturelle la géométrie « classique », introduite par Euclide dans ses *Éléments*. Elle est définie par la donnée d'un espace vectoriel sur le corps des réels, de dimension finie, muni d'une forme bilinéaire possédant des propriétés spécifiques, et permet, entre autres choses, de « mesurer » des longueurs, des distances et des angles.

4.1 Définitions et premières propriétés

On commence par définir l'opération algébrique fondamentale conférant à l'espace vectoriel qui en est muni bon nombre de structures et propriétés additionnelles.

Définition 4.1 (produit scalaire) *Soit E un espace vectoriel sur $\mathbb{R}$. Une application $\langle \cdot, \cdot \rangle$ de $E \times E$ dans $\mathbb{R}$ est appelée un **produit scalaire** sur E si et seulement si elle est bilinéaire, symétrique, non dégénérée et positive.*

La définition précédente possède un analogue dans un espace vectoriel complexe, moyennant une modification technique. En effet, sur le corps $\mathbb{C}$, il n'existe plus de relation d'ordre compatible avec les opérations du corps, et le carré d'un nombre complexe peut être négatif. Pour pallier cette difficulté, on fait dans ce cas appel à une forme *sesquilinéaire hermitienne* (voir le chapitre 2).

Définition 4.2 (produit scalaire hermitien) *Soit E un espace vectoriel sur $\mathbb{C}$. On appelle **produit scalaire hermitien** une application $\langle \cdot, \cdot \rangle$ de $E \times E$ dans $\mathbb{C}$ qui est sesquilinéaire, à symétrie hermitienne, non dégénérée et positive.*

D'après un corollaire de l'inégalité de Cauchy–Schwarz (voir le corollaire 3.40), la forme polaire d'une forme quadratique q (resp. d'une forme quadratique hermitienne h) positive sur E est non dégénérée si et seulement si q (resp. h) est définie. À ce titre, on peut aussi définir un produit scalaire (resp. un produit scalaire hermitien) comme une forme bilinéaire (resp. sesquilinéaire), symétrique (resp. à symétrie hermitienne) et définie positive.

Nombre de propriétés et de résultats vus dans ce chapitre ne dépendent pas du fait que l'espace vectoriel dans lequel on travaille soit de dimension finie. Néanmoins, on appelle **espace préhilbertien** tout espace vectoriel (réel ou complexe) muni d'un produit scalaire. Si l'espace vectoriel est en outre de dimension finie, on parle d'espace **euclidien** lorsqu'il est réel ou d'espace **hermitien** lorsqu'il est complexe.

Exemple 4.3 (exemples d'espaces euclidiens et préhilbertiens) *Soit m et n deux entiers naturels non nuls. La forme définie par $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$ est un produit scalaire sur $\mathbb{R}^n$ (parfois dit usuel), qui munit cet espace vectoriel de sa structure euclidienne dite* canonique. *Son analogue sur l'espace de matrices $M_{m,n}(\mathbb{R})$ est donné par l'application $\langle M, N \rangle = \operatorname{tr}(M^\top N)$, qui fait de cet espace un espace euclidien, et une extension naturelle en dimension infinie est donnée par la forme définie par $\langle (u_k)_{k\in\mathbb{N}}, (v_k)_{k\in\mathbb{N}} \rangle = \sum_{k\in\mathbb{N}} u_k v_k$ sur l'ensemble des suites réelles de carré sommable, $\ell^2(\mathbb{N}) = \{(u_k)_{k\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \mid \sum_{k\in\mathbb{N}} (u_k)^2 < +\infty\}$, qui est donc un espace préhilbertien. Enfin, si $[a, b]$ désigne un intervalle borné de $\mathbb{R}$, la forme définie par $\langle f, g \rangle = \int_a^b f(t)g(t)\,\mathrm{d}t$ est un produit scalaire sur l'espace de fonctions $\mathscr{C}^0([a, b], \mathbb{R})$, qui est donc un espace préhilbertien.*

Si A est un sous-espace vectoriel d'un espace euclidien (resp. hermitien) E, alors la restriction du produit scalaire de E à A induit une structure d'espace euclidien (resp. hermitien) sur ce sous-espace.

Théorème 4.4 *Soit E un espace préhilbertien réel, de produit scalaire noté $\langle\cdot,\cdot\rangle$. L'application de E dans $\mathbb{R}$ définie par*

$$\forall x \in E,\ \|x\| = \sqrt{\langle x, x\rangle},$$

*est une **norme** sur E, c'est-à-dire une application satisfaisant aux propriétés suivantes :*
- *— **séparation** : $\forall x \in E,\ \|x\| = 0 \implies x = 0_E$,*
- *— **absolue homogénéité** : $\forall (\lambda, x) \in \mathbb{R} \times E,\ \|\lambda\, x\| = |\lambda|\,\|x\|$,*
- *— **sous-additivité** : $\forall (x, y) \in E^2,\ \|x + y\| \leq \|x\| + \|y\|$.*

*On l'appelle **norme associée au** (ou **dérivant du**) **produit scalaire**, encore dite **norme euclidienne**.*

DÉMONSTRATION. On a tout d'abord

$$\forall x \in E,\ \|x\| = 0 \iff \sqrt{\langle x, x\rangle} = 0 \iff \langle x, x\rangle = 0 \iff x = 0_E,$$

puisque la forme quadratique associée au produit scalaire est définie positive. On a ensuite

$$\forall \lambda \in \mathbb{R},\ \forall x \in E,\ \|\lambda\, x\| = \sqrt{\langle \lambda\, x, \lambda\, x\rangle} = \sqrt{\lambda^2\, \langle x, x\rangle} = |\lambda|\, \sqrt{\langle x, x\rangle} = |\lambda|\,\|x\|.$$

Enfin, la sous-additivité découle de l'inégalité de Minkowski. □

On pourra également observer qu'une norme est toujours positive. En effet, on a, compte tenu des propriétés démontrées plus haut,

$$\forall x \in E,\ 0 = \|0_E\| = \|x - x\| \leq \|x\| + \|-x\| = \|x\| + |-1|\,\|x\| = 2\,\|x\|.$$

Exemple 4.5 (norme de Frobenius) *Soit m et n deux entiers naturels non nuls. La norme sur $M_{m,n}(\mathbb{R})$ dérivant du produit scalaire introduit sur cet espace dans l'exemple 4.3 porte le nom de **norme de Frobenius**. On la note*

$$\|M\|_F = \sqrt{\mathrm{tr}(M^\top M)} = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} {m_{ij}}^2}$$

C'est la norme euclidienne usuelle sur $M_{m,n}(\mathbb{R})$.

Remarque 4.6 *Une application de E dans $\mathbb{R}$ qui ne satisfait que les propriétés d'homogénéité et de sous-additivité énoncées plus haut est appelée une **semi-norme**.*

L'introduction de la norme associée au produit scalaire fait de tout espace préhilbertien un espace vectoriel **normé**. On peut y réécrire l'inégalité de Cauchy–Schwarz sous la forme :

$$\forall (x, y) \in E^2,\ |\langle x, y\rangle| \leq \|x\|\|y\|.$$

Il est possible de définir, de la même manière, une norme sur un $\mathbb{C}$-espace vectoriel associée à un produit scalaire hermitien.

Remarque 4.7 (exemple de norme ne dérivant pas d'un produit scalaire) *Toute norme sur un espace vectoriel ne se trouve pas nécessairement associée à un produit scalaire. C'est par exemple le cas de la norme $\|\cdot\|_1$ sur l'espace $\mathbb{R}^n$, définie par*

$$\forall x \in \mathbb{R}^n,\ \|x\|_1 = \sum_{i=1}^{n} |x_i|\,,$$

ce que l'on montre par un raisonnement par l'absurde. En effet, si cette norme était issue d'un produit scalaire, alors, par une identité de polarisation, la forme donnée par

$$\forall (x, y) \in \mathbb{R}^n \times \mathbb{R}^n,\ b(x, y) = \frac{1}{2}\left(\|x + y\|_1{}^2 - \|x\|_1{}^2 - \|y\|_1{}^2\right)$$

serait un produit scalaire. Or, pour les vecteurs e_1 et e_2 de la base canonique, on a

$$b(e_1, e_2) = \frac{1}{2}(4 - 1 - 1) = 1 \text{ et } b(-e_1, e_2) = \frac{1}{2}(4 - 1 - 1) = 1,$$

ce qui contredit que b est une forme bilinéaire.

Proposition 4.8 *Soit E un espace préhilbertien réel. Pour tous vecteurs x et y de E, on a*

$$\|x+y\| = \|x\| + \|y\|$$

si et seulement si la famille $\{x,y\}$ est positivement liée, i.e. si $x=0$ ou s'il existe un réel positif λ tel que $y=\lambda x$.

DÉMONSTRATION. Si le vecteur x est nul, l'égalité est évidente. Si x est non nul et que $y=\lambda x$, avec λ un réel positif, on a

$$\|x+y\| = \|(1+\lambda)x\| = (1+\lambda)\|x\| = \|x\| + \lambda\|x\| = \|x\| + \|\lambda x\| = \|x\| + \|y\|.$$

Réciproquement, si on a égalité alors

$$\|x\|^2 + 2\langle x,y\rangle + \|y\|^2 = \|x+y\|^2 = (\|x\| + \|y\|)^2 = \|x\|^2 + 2\|x\|\|y\| + \|y\|^2,$$

d'où $\langle x,y\rangle = \|x\|\|y\|$, ce qui correspond au cas d'égalité dans l'inégalité de Cauchy-Schwarz et implique que la famille $\{x,y\}$ est liée. Ainsi, soit x est nul, soit $y=\lambda x$ avec λ un réel. On a donc

$$\lambda\|x\|^2 = \lambda\langle x,x\rangle = \langle x,y\rangle = \|x\|\|y\| \geq 0 \implies \lambda \geq 0.$$

□

L'application d de $E\times E$ dans $\mathbb{R}_+$, définie par $d(x,y)=\|x-y\|$, est appelée **distance associée** à la norme $\|\cdot\|$ sur E. Elle fait implicitement de tout espace normé un espace **métrique**.

Remarque 4.9 (espace de Hilbert) *Un espace préhilbertien qui est* ***complet*** [1] *pour la distance associée à sa norme est appelé un* ***espace de Hilbert****. Tout espace vectoriel de dimension* finie *et muni d'un produit scalaire est un espace de Hilbert.*

Le résultat suivant, valide dans tout espace préhilbertien, correspond à une propriété de géométrie élémentaire.

Théorème 4.10 (identité du parallélogramme) *Soit E un espace préhilbertien. On a*

$$\forall (x,y)\in E^2,\ \|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$

DÉMONSTRATION. On a d'une part

$$\forall (x,y)\in E^2,\ \|x+y\|^2 = \|x\|^2 + 2\langle x,y\rangle + \|y\|^2,$$

et d'autre part

$$\forall (x,y)\in E^2,\ \|x-y\|^2 = \|x\|^2 - 2\langle x,y\rangle + \|y\|^2.$$

L'égalité de l'énoncé s'obtient en sommant les deux précédentes. □

Remarque 4.11 *L'identité du parallélogramme s'interprète géométriquement de la manière suivante : la somme des carrés des longueurs des quatre côtés d'un parallélogramme est égale à la somme des carrés des longueurs de ses deux diagonales :* soit $ABCD$ un parallélogramme, alors

$$AC^2 + BD^2 = 2\left(AB^2 + BC^2\right).$$

Elle est par ailleurs équivalente au résultat connu sous le nom du ***théorème de la médiane*** *ou* ***d'Apollonius*** *(de Perge) :* soit ABC un triangle et I le milieu du segment $[BC]$, alors

$$AB^2 + AC^2 = 2\left(BI^2 + AI^2\right),$$

ou encore

$$AB^2 + AC^2 = \frac{1}{2}BC^2 + 2AI^2,$$

ce qui se traduit par

$$\forall (x,y,z)\in E^3,\ \|x-y\|^2 + \|x-z\|^2 = 2\left(\left\|y - \frac{y+z}{2}\right\|^2 + \left\|x - \frac{y+z}{2}\right\|^2\right) = \frac{1}{2}\|y-z\|^2 + 2\left\|x - \frac{y+z}{2}\right\|^2.$$

1. Un espace métrique est dit *complet* lorsque toute suite de Cauchy de cet espace y converge.

Remarque 4.12 *La réciproque du théorème 4.10 s'énonce :* soit $(E, \|\cdot\|)$ un espace vectoriel normé dans lequel l'identité du parallélogramme est vérifiée, alors la norme dérive d'un produit scalaire*, et porte le nom de* ***théorème de Fréchet–Jordan–von Neumann*** *[Fré35, JvN35].*

La définition suivante est une conséquence de l'inégalité de Cauchy–Schwarz.

Définition 4.13 (écart angulaire) *Soit E un espace préhilbertien réel. Pour tous vecteurs x et y de E, il existe un unique réel θ appartenant à l'intervalle $[0, \pi]$ tel que*

$$\cos(\theta) = \frac{\langle x, y\rangle}{\|x\|\|y\|}.$$

Ce réel est appelé ***écart angulaire entre*** *x* ***et*** *y et correspond à une mesure d'angle non orienté.*

4.2 Orthogonalité dans les espaces euclidiens

La notion d'orthogonalité telle qu'on l'a introduite pour une forme quadratique subsiste bien évidemment avec un produit scalaire (hermitien ou non), avec l'avantage qu'une telle forme est définie positive. Dans la suite, on note $\langle\cdot,\cdot\rangle$ le produit scalaire, éventuellement hermitien, de l'espace considéré.

4.2.1 Généralités

Définitions 4.14 *Soit E un espace préhilbertien. Deux vecteurs x et y de E sont dits* ***orthogonaux****, ce que l'on note $x \perp y$, si et seulement si $\langle x, y\rangle = 0$.*
Soit A une partie non vide de E. On appelle ***orthogonal de*** *A, et on note $A^\perp$, l'ensemble*

$$A^\perp = \{x \in E \,|\, \forall y \in A,\ \langle x, y\rangle = 0\}.$$

Il découle que la bilinéarité du produit scalaire que l'orthogonal $A^\perp$ d'une partie A est un sous-espace vectoriel.

Proposition 4.15 *Soit E un espace préhilbertien et A et B deux sous-espaces vectoriels de E. On a*

(i) $\{0_E\}^\perp = E$ *et* $E^\perp = \{0_E\}$,

(ii) $A \subset \left(A^\perp\right)^\perp$,

(iii) $A \subset B \implies B^\perp \subset A^\perp$,

(iv) $(A+B)^\perp = A^\perp \cap B^\perp$,

(v) $A^\perp + B^\perp \subset (A \cap B)^\perp$.

DÉMONSTRATION.

(i) Pour tout vecteur x de E, on a $\langle 0_E, x\rangle = 0$, d'où x appartient à $\{0_E\}^\perp$. On considère alors un vecteur x de $E^\perp$. Puisque x appartient à aussi à E, on a $\langle x, x\rangle = 0$, d'où $x = 0_E$. Ceci achève de montrer la première assertion.

(ii) Cette assertion correspond à la première assertion de la proposition 3.14 et a donc déjà été prouvée.

(iii) Cette assertion correspond à la deuxième assertion de la proposition 3.14 et a donc déjà été prouvée.

(iv) On a $A \subset A+B$ et $B \subset A+B$. En se servant de la troisième assertion, il vient alors que $(A+B)^\perp \subset A^\perp$ et $(A+B)^\perp \subset B^\perp$, ce qui implique que $(A+B)^\perp \subset A^\perp \cap B^\perp$. Réciproquement, soit x un vecteur de $A^\perp \cap B^\perp$. Pour tout vecteur y de $A+B$, on peut, par définition, écrire $y = y_A + y_B$, avec y_A appartenant à A et y_B appartenant à B, et il vient alors

$$\langle y, x\rangle = \langle y_A + y_B, x\rangle = \langle y_A, x\rangle + \langle y_B, x\rangle = 0 + 0 = 0,$$

d'où x appartient à $(A+B)^\perp$.

(v) Soit x un vecteur de $A^\perp + B^\perp$. Par définition, on peut écrire $x = x_{A^\perp} + x_{B^\perp}$, avec $x_{A^\perp}$ appartenant à $A^\perp$ et $x_{B^\perp}$ appartenant à $B^\perp$. Alors, pour tout vecteur y de $A \cap B$, il vient

$$\langle x, y\rangle = \langle x_{A^\perp} + x_{B^\perp}, y\rangle = \langle x_{A^\perp}, y\rangle + \langle x_{B^\perp}, y\rangle = 0 + 0 = 0,$$

d'où x appartient à $(A \cap B)^\perp$.

□

Corollaire 4.16 *On suppose, sous les hypothèses de la proposition 4.15, que l'espace E est de dimension finie. On a alors*

(i) $\dim(A) + \dim\left(A^\perp\right) = \dim(E)$,

(ii) $A = \left(A^\perp\right)^\perp$,

(iii) $A^\perp + B^\perp = (A \cap B)^\perp$.

DÉMONSTRATION.

(i) Cette assertion découle de la première assertion de la proposition 3.15, en utilisant que le noyau d'un produit scalaire est réduit au vecteur nul, et par conséquent de dimension nulle.

(ii) Cette assertion découle de la deuxième assertion de la proposition 3.15, en utilisant que le noyau d'un produit scalaire est réduit au vecteur nul.

(iii) La quatrième assertion de la proposition 4.15 affirme que $A^\perp + B^\perp \subset (A \cap B)^\perp$. En vertu de la formule de Grassman, on a d'une part $\dim(A \cap B) = \dim(A) + \dim(B) - \dim(A + B)$, et d'autre part $\dim\left(A^\perp + B^\perp\right) = \dim\left(A^\perp\right) + \dim\left(B^\perp\right) - \dim\left(A^\perp \cap B^\perp\right)$. Il vient alors, en faisant appel à la quatrième assertion de la proposition 4.15 ainsi qu'à la première assertion ci-dessus,

$$\begin{aligned}
\dim((A \cap B)^\perp) &= \dim(E) - \dim(A \cap B) \\
&= \dim(E) - (\dim(A) + \dim(B) - \dim(A + B)) \\
&= \dim(E) - \dim(A) + \dim(E) - \dim(B) - (\dim(E) - \dim(A + B)) \\
&= \dim\left(A^\perp\right) + \dim\left(B^\perp\right) - \dim\left((A + B)^\perp\right) \\
&= \dim\left(A^\perp\right) + \dim\left(B^\perp\right) - \dim\left(A^\perp \cap B^\perp\right) \\
&= \dim\left(A^\perp + B^\perp\right),
\end{aligned}$$

ce qui assure l'égalité entre les deux sous-espaces.

□

4.2.2 Bases orthonormées

Définitions 4.17 *Soit E un espace préhilbertien. Une famille de vecteurs non nuls* $\{e_i\}_{i \in I}$ *de E est dite* ***orthogonale*** *si elle vérifie*

$$\forall (i, j) \in I^2,\ i \neq j,\ \left\langle e_i, e_j \right\rangle = 0.$$

Une telle famille est dite ***orthonormale*** *(ou* ***orthonormée****) si l'on a de plus*

$$\forall i \in I,\ \|e_i\| = 1.$$

Proposition 4.18 (relation de Pythagore) *Soit E un espace préhilbertien, p un entier naturel non nul et* $\{e_i\}_{i=1,\dots,p}$ *une famille orthogonale de E. On a*

$$\left\| \sum_{i=1}^{p} e_i \right\|^2 = \sum_{i=1}^{p} \|e_i\|^2.$$

DÉMONSTRATION. On raisonne par récurrence sur l'entier naturel p. Si $p = 1$, il n'y a rien à montrer. On suppose alors que, pour un entier p est supérieur ou égal à 1, l'égalité est vraie pour une famille orthogonale formée de p vecteurs. On considère à présent la famille orthogonale $\{e_i\}_{i=1,\dots,p+1}$. On a, par orthogonalité de la famille,

$$\left\| \sum_{i=1}^{p+1} e_i \right\|^2 = \left\langle \sum_{i=1}^{p} e_i + e_{p+1}, \sum_{i=1}^{p} e_i + e_{p+1} \right\rangle = \left\| \sum_{i=1}^{p} e_i \right\|^2 + 2 \sum_{i=1}^{p} \left\langle e_i, e_{p+1} \right\rangle + \|e_{p+1}\|^2 = \left\| \sum_{i=1}^{p} e_i \right\|^2 + \|e_{p+1}\|^2.$$

On conclut alors en se servant de l'hypothèse de récurrence. □

Proposition 4.19 *Soit E un espace préhilbertien et p un entier naturel non nul. Toute famille orthogonale $\{e_i\}_{i=1,\dots,p}$ de E est libre.*

DÉMONSTRATION. Soit des scalaires $\alpha_1,\dots,\alpha_p$ tels que $\alpha_1 e_1+\cdots+\alpha_p e_p=0_E$. Par orthogonalité de la famille, on a

$$\forall i\in\{1,\dots,p\},\ 0=\left\langle e_i,\alpha_1 e_1+\cdots+\alpha_p e_p\right\rangle=\sum_{j=1}^{n}\alpha_j\left\langle e_i,e_j\right\rangle=\alpha_i\|e_i\|^2.$$

Les vecteurs $e_1,\dots,e_p$ étant non nuls, leurs normes respectives sont strictement positives et les scalaires $\alpha_1,\dots,\alpha_p$ sont donc tous nuls, ce qui achève la preuve. □

Il découle de cette dernière propriété que l'on peut parler de *base orthogonale* (ou *orthonormale*) d'un espace préhilbertien de dimension *finie*.

Exemple 4.20 (exemple de base orthonormée) *Soit n un entier naturel non nul. La base canonique de $\mathbb{R}^n$, muni de son produit scalaire usuel, est une base orthonormée.*

Proposition 4.21 (coordonnées dans une base orthonormée) *Soit n un entier naturel non nul. Si E est un espace euclidien (resp. hermitien) et si $\{e_1,\dots,e_n\}$ est une base orthonormée de E, on a*

$$\forall x\in E,\ x=\sum_{i=1}^{n}x_i e_i,\ \forall y\in E,\ y=\sum_{i=1}^{n}y_i e_i,\ \langle x,y\rangle=\sum_{i=1}^{n}x_i y_i\ (\textit{resp. }\langle x,y\rangle=\sum_{i=1}^{n}\overline{x_i}y_i).$$

De plus, les coordonnées d'un vecteur x de E dans cette base vérifient

$$\forall i\in\{1,\dots,n\},\ x_i=\langle x,e_i\rangle,$$

et l'on a

$$\|x\|^2=\sum_{i=1}^{n}\langle x,e_i\rangle^2.$$

DÉMONSTRATION. On prouve les résultat dans le cas euclidien, ceux du cas hermitien s'obtenant avec des modifications mineures.

Il découle tout d'abord de la définition 4.17 que le vecteurs de la base orthonormée $\{e_1,\dots,e_n\}$ satisfont

$$\forall(i,j)\in\{1,\dots,n\}^2,\ \left\langle e_i,e_j\right\rangle=\delta_{ij},$$

où δ_{ij} désigne le symbole de Kronecker. On a alors, par bilinéarité du produit scalaire,

$$\forall(x,y)\in E^2,\ \langle x,y\rangle=\sum_{i=1}^{n}\sum_{j=1}^{n}x_i y_j\left\langle e_i,e_j\right\rangle=\sum_{i=1}^{n}\sum_{j=1}^{n}x_i y_j\delta_{ij}=\sum_{i=1}^{n}x_i y_i,$$

et

$$\forall x\in E,\ \forall i\in\{1,\dots,n\},\ \langle x,e_i\rangle=\sum_{j=1}^{n}x_j\left\langle e_j,e_i\right\rangle=\sum_{j=1}^{n}x_j\delta_{ji}=x_i.$$

Enfin, il résulte de la relation de Pythagore (voir la proposition 4.18) et du précédent résultat que

$$\forall x\in E,\ \|x\|^2=\left\|\sum_{i=1}^{n}x_i e_i\right\|^2=\sum_{i=1}^{n}\|x_i e_i\|^2=\sum_{i=1}^{n}{x_i}^2\|e_i\|^2=\sum_{i=1}^{n}{x_i}^2=\sum_{i=1}^{n}\langle x,e_i\rangle^2.$$

□

On retiendra de cette proposition que la détermination des coordonnées d'un vecteur ou l'évaluation du produit scalaire entre deux vecteurs sont aisées lorsque l'on considère une base orthonormée.

Remarque 4.22 *Cette façon de déterminer les coordonnées d'un vecteur s'applique également lorsque l'on veut déterminer la matrice d'un endomorphisme u de E dans une base orthonormée $\mathscr{B}=\{e_1,\dots,e_n\}$. On a en effet*

$$\forall(i,j)\in\{1,\dots,n\}^2,\ (mat_{\mathscr{B}}(u))_{ij}=\left\langle u(e_j),e_i\right\rangle.$$

Une manière de construire une base orthonormée à partir d'une base quelconque de l'espace est donnée par le *procédé d'orthonormalisation de Gram–Schmidt*, décrit dans la preuve du théorème suivant.

Théorème 4.23 *Soit E un espace euclidien de dimension n non nulle et $\{f_1,\dots,f_n\}$ une base de E. Il existe une unique base orthonormée $\{e_1,\dots,e_n\}$ de E telle que*

$$\forall j\in\{1,\dots,n\},\ \mathrm{Vect}(\{e_1,\dots,e_j\})=\mathrm{Vect}(\{f_1,\dots,f_j\})\ \textit{et}\ \langle f_j,e_j\rangle>0.$$

DÉMONSTRATION. On va construire la base orthonormée par récurrence en procédant comme suit.

On pose tout d'abord $e_1=\frac{f_1}{\|f_1\|}$. On suppose ensuite avoir construit une famille $\{e_1,\dots,e_j\}$, avec j un entier de $\{1,\dots,n-1\}$. On définit alors

$$e_{j+1}=\frac{f_{j+1}-\sum_{k=1}^{j}\langle f_{j+1},e_k\rangle\,e_k}{\left\|f_{j+1}-\sum_{k=1}^{j}\langle f_{j+1},e_k\rangle\,e_k\right\|}.$$

On vérifie ensuite les différentes propriétés énoncées dans le théorème. Il est tout d'abord clair que chaque vecteur e_j, avec j appartenant à $\{1,\dots,n\}$, appartient à $\mathrm{Vect}(\{f_1,\dots,f_j\})$ en utilisant les formules ci-dessus et en raisonnant par récurrence. Réciproquement, chaque vecteur f_j, avec j appartenant à $\{1,\dots,n\}$, appartient à $\mathrm{Vect}(\{e_1,\dots,e_j\})$.

Le fait de pouvoir normaliser le vecteur à chaque étape en divisant $f_{j+1}-\sum_{k=1}^{j}\langle f_{j+1},e_k\rangle\,e_k$ par sa norme provient du fait que $\{f_1,\dots,f_n\}$ est une une famille libre et de la propriété précédente. Ceci permet en particulier d'assurer que le processus itératif qu'on a introduit est bien défini (on n'a pas de division par zéro).

Il faut ensuite montrer que la famille obtenue est orthogonale. Pour cela, il suffit de montrer que le vecteur e_j, avec j appartenant à $\{2,\dots,n\}$, est orthogonal à tout vecteur e_i, avec i appartenant à $\{1,\dots,j-1\}$, en raisonnant par récurrence. Pour $j=2$, on a

$$\langle e_2,e_1\rangle=\left\langle\frac{f_2-\langle f_2,e_1\rangle\,e_1}{\|f_2-\langle f_2,e_1\rangle\,e_1\|},e_1\right\rangle=\frac{1}{\|f_2-\langle f_2,e_1\rangle\,e_1\|}\left(\langle f_2,e_1\rangle-\langle f_2,e_1\rangle\,\|e_1\|^2\right)=0.$$

Pour j supérieur ou égal à 3, on fait l'hypothèse de récurrence

$$\forall(i,k)\in\{1,\dots,j-1\}^2,\langle e_i,e_k\rangle=\delta_{ik}.$$

On a alors

$$\begin{aligned}\forall i\in\{1,\dots,j-1\},\ \langle e_j,e_i\rangle&=\frac{1}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|}\left\langle f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k,e_i\right\rangle\\&=\frac{1}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|}\left(\langle f_j,e_i\rangle-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\langle e_k,e_i\rangle\right)\\&=\frac{1}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|}\left(\langle f_j,e_i\rangle-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,\delta_{ik}\right)\\&=\frac{1}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|}\left(\langle f_j,e_i\rangle-\langle f_j,e_i\rangle\right)\\&=0.\end{aligned}$$

Enfin, on a, pour tout entier j de $\{1,\dots,n\}$,

$$\|e_j\|^2=\langle e_j,e_j\rangle=\frac{1}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|}\left\langle f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k,e_j\right\rangle=\frac{\langle f_j,e_j\rangle}{\left\|f_j-\sum_{k=1}^{j-1}\langle f_j,e_k\rangle\,e_k\right\|},$$

d'où $\langle f_j,e_j\rangle>0$.

Il nous reste à montrer que la base est unique. Toute base $\{e_1,\dots,e_n\}$ satisfaisant aux propriétés précédentes est telle que le vecteur e_1 appartient à Vect($\{f_1\}$), c'est-à-dire que $e_1=\lambda f_1$. Puisque $\|e_1\|=1$ et $\langle e_1,f_1\rangle>0$, on trouve que $\lambda=\frac{1}{\|f_1\|}$.

On suppose ensuite que les vecteurs $e_1,\dots,e_j$ soient de la forme donnée pour j superieur ou égal à 1. On sait que e_{j+1} appartient à $\mathrm{Vect}(\{f_1,\dots,f_{j+1}\})=\mathrm{Vect}(\{e_1,\dots,e_j,f_{j+1}\})$, d'où

$$e_{j+1}=\sum_{k=1}^{j}\lambda_k e_k+\lambda f_{j+1}.$$

En considérant successivement les produits scalaires de ce vecteur avec les vecteurs e_i pour i appartenant à $\{1,\dots,j\}$, on trouve que $\lambda_i=-\lambda\left\langle f_{j+1},e_i\right\rangle$ et on a par conséquent

$$e_{j+1}=\lambda\left(f_{j+1}-\sum_{k=1}^{j}\left\langle f_{j+1},e_k\right\rangle e_k\right).$$

Les conditions $\|e_{j+1}\|=1$ et $\left\langle e_{j+1},f_{j+1}\right\rangle>0$ permettent alors de déterminer λ, conduisant à la forme donnée. □

Une conséquence directe du précédent théorème et du théorème A.76 est le résultat suivant.

Corollaire 4.24 *Un espace euclidien non réduit au vecteur nul possède une base orthonormée.*

Remarque 4.25 *Dans la construction proposée ci-dessus, on peut observer que la matrice de passage de la base $\{f_1,\dots,f_n\}$ à la base $\{e_1,\dots,e_n\}$ est* triangulaire supérieure*, à coefficients diagonaux strictement positifs (ce sont les inverses de normes de vecteurs). L'exploitation de ce fait conduit à la* ***factorisation QR*** *des matrices, qui consiste à écrire toute matrice sous la forme du produit d'une matrice orthogonale et d'une matrice triangulaire supérieure.*

Remarque 4.26 *Erhard Schmidt introduisit en 1907, dans un article sur les équations intégrales [Sch07], le procédé aujourd'hui dit de Gram–Schmidt pour construire, de manière théorique, une famille orthonormée de fonctions à partir d'une famille libre infinie. Faisant explicitement référence à des travaux de Jørgen Pedersen Gram [Gra83] sur le développement en série de fonctions par des méthodes de moindres carrés, il lui en attribua l'idée.*

Exemple 4.27 *On applique le procédé de Gram–Schmidt à la base $\{(1,0,1),(1,1,1),(-1,-1,0)\}$ de $\mathbb{R}^3$, muni du produit scalaire usuel. On normalise tout d'abord le premier vecteur,*

$$e_1=\frac{1}{\|(1,0,1)\|}(1,0,1)=\frac{1}{\sqrt{2}}(1,0,1).$$

On orthogonalise ensuite le deuxième vecteur par rapport au premier vecteur obtenu,

$$\tilde{e}_2=(1,1,1)-\langle(1,1,1),e_1\rangle\,e_1=(1,1,1)-(1,0,1)=(0,1,0),$$

et l'on normalise le vecteur résultant

$$e_2=\frac{1}{\|\tilde{e}_2\|}\tilde{e}_2=\frac{1}{\|(0,1,0)\|}(0,1,0)=(0,1,0).$$

Enfin, on orthogonalise ensuite le dernier vecteur par rapport aux deux vecteurs obtenus,

$$\tilde{e}_3=(-1,-1,0)-\langle(-1,-1,0),e_1\rangle\,e_1-\langle(-1,-1,0),e_2\rangle\,e_2=(-1,-1,0)+\frac{1}{2}(1,0,1)-(-1)(0,1,0)=\left(-\frac{1}{2},0,\frac{1}{2}\right),$$

et l'on normalise le vecteur trouvé

$$e_3=\frac{1}{\|\tilde{e}_3\|}\tilde{e}_3=\sqrt{2}\left(-\frac{1}{2},0,\frac{1}{2}\right)=\left(-\frac{\sqrt{2}}{2},0,\frac{\sqrt{2}}{2}\right).$$

Le procédé de Gram–Schmidt peut aussi s'appliquer en dimension infinie, quand on dispose d'une suite $(u_k)_{k\in\mathbb{N}}$ de vecteurs d'un espace préhilbertien, telle que $\{u_1,\dots,u_n\}$ soit libre pour tout entier naturel non nul n, pour former une suite de vecteurs orthonormés.

Exemple 4.28 (polynômes orthogonaux) *Soit $]a,b[$ un intervalle ouvert de $\mathbb{R}$ et w une fonction continue strictement positive définie sur $]a,b[$, appelée* ***poids****. On considère l'espace vectoriel $E=\mathbb{R}[X]$, muni du produit scalaire défini par*

$$\forall (P,Q)\in E^2,\ \langle P,Q\rangle = \int_a^b P(t)Q(t)w(t)\,\mathrm{d}t.$$

L'application du procédé de Gram–Schmidt à la suite de polynômes échelonnée en degré $(X^k)_{k\in\mathbb{R}}$ conduit à une unique suite $(P_k)_{k\in\mathbb{R}}$ de polynômes orthogonaux deux à deux, tels que $\deg(P_k)=k$ pour tout entier naturel k et appelés polynômes orthogonaux*. Parmi les familles de polynômes orthogonaux les plus connues, nommées en fonction des choix de a, de b et de w, on peut citer :*

- *les* ***polynômes de Legendre****, pour $]a,b[=]-1,1[$ et $w(x)=1$,*
- *les* ***polynômes de Tchebychev de première espèce****, pour $]a,b[=]-1,1[$ et $w(x)=\frac{1}{\sqrt{1-x^2}}$,*
- *les* ***polynômes de Jacobi****, pour $]a,b[=]-1,1[$ et $w(x)=(1-x)^\alpha(1+x)^\beta$, avec $\alpha>-1$ et $\beta>-1$,*
- *les* ***polynômes de Laguerre****, pour $]a,b[=]0,+\infty[$ et $w(x)=e^{-x}$,*
- *les* ***polynômes de Hermite****, pour $]a,b[=]-\infty,+\infty[$ et $w(x)=e^{-x^2}$.*

Il est à noter qu'il est standard de choisir d'autres normalisations lorsque l'on énumère les éléments de ces familles, typiquement en imposant leur valeur en un point fixé (par exemple, les polynômes de Legendre et de Chebychev de première espèce valent tous 1 en $x=1$) ou la valeur de leur coefficient de plus haut degré (par exemple, le coefficient du terme de plus haut degré du polynôme de Laguerre de degré n est $\frac{(-1)^n}{n!}$).

On introduit enfin une notion de sous-espace supplémentaire propre aux espaces euclidiens.

Proposition 4.29 *Soit E un espace euclidien et A un sous-espace vectoriel de E. On a*

$$E = A\oplus A^\perp$$

et le sous-espace $A^\perp$ est par conséquent appelé le ***supplémentaire orthogonal de*** *A.*

DÉMONSTRATION. On suppose que l'espace E est de dimension n et que le sous-espace A est de dimension $p\leq n$. En vertu du théorème de la base incomplète, il est possible de compléter toute base de A en une base de E. En appliquant le procédé d'orthonormalisation de Gram–Schmidt à une telle base, on obtient une base orthonormée de E dont il n'est pas difficile de voir (il suffit pour cela d'utiliser les propriétés énoncées dans le théorème 4.23) que ses p premiers vecteurs forment une base orthonormée de A et les $n-p$ suivants une base orthonormée de $A^\perp$, ce qui permet de conclure. □

Cette proposition reste vraie dans un espace préhilbertien si le sous-espace A est de dimension *finie*. Elle est également vraie si A est un sous-espace vectoriel *fermé* et l'espace E est *complet*, mais elle est fausse en général.

4.2.3 Projection orthogonale

Proposition et définition 4.30 (projection et symétrie orthogonales) *Soit E un espace euclidien et A un sous-espace vectoriel de E. Tout vecteur x de E s'écrit, de manière unique, comme la somme $x=x_A+x_{A^\perp}$, avec x_A appartenant à A et $x_{A^\perp}$ appartenant à $A^\perp$. On appelle* ***projection orthogonale de*** *x* ***sur*** *A le vecteur x_A ainsi défini, et on note p_A l'application de E dans E telle que $x\mapsto x_A=p_A(x)$ ainsi construite. On appelle* ***symétrie orthogonale de*** *x* ***par rapport à*** *A le vecteur $x_A-x_{A^\perp}$ et on note s_A l'application de E dans E telle que $x\mapsto x_A-x_{A^\perp}=2\,p_A(x)-x=s_A(x)$ ainsi construite.*

On notera que le projecteur orthogonal p_A est simplement le projecteur sur A parallèlement à son supplémentaire orthogonal $A^\perp$.

Proposition 4.31 (propriétés des projections orthogonales) *Soit A un sous-espace vectoriel d'un espace euclidien E. On a les propriétés suivantes.*

1. *$\forall x\in E,\ x=p_A(x)+p_{A^\perp}(x),\ x-p_A(x)\in A^\perp$ et $\|p_A(x)\|\leq\|x\|$.*
2. *Si $\{e_1,\dots,e_p\}$ est une base orthonormée de A, alors*

$$\forall x\in E,\ p_A(x)=\sum_{i=1}^{p}\langle x,e_i\rangle\ e_i.$$

3. *La projection orthogonale sur A se caractérise variationnellement par la propriété de minimalité suivante :*

$$\forall x \in E,\ \|x - p_A(x)\| = \inf_{y \in A} \|x - y\|.$$

On note $d(x,A) = \|x - p_A(x)\|$ *la distance de* x *à* A*.*

4. *Si* p *est un endomorphisme de* E *idempotent et si* $\mathrm{Im}(p)$ *et* $\ker(p)$ *sont orthogonaux, alors* p *est le projecteur orthogonal sur* $\mathrm{Im}(p)$*.*

DÉMONSTRATION. On démontre chacun des points.

1. C'est une conséquence du fait que $E = A \oplus A^\perp$ et de la définition de la projection orthogonale, l'inégalité découlant de la relation de Pythagore.
2. Il suffit d'écrire la projection de x comme une combinaison linéaire des vecteurs de la base orthonormée et on en détermine les coefficients en utilisant que $x - p_A(x)$ appartient à $A^\perp$, c'est-à-dire en écrivant que

$$\forall x \in E,\ \forall i \in \{1, \dots, p\},\ \langle x - p_A(x), e_i \rangle = 0.$$

3. Tout d'abord, pour tout vecteur x de E, l'ensemble $\{\|x - y\|,\ y \in A\}$ est non vide, puisque A contient 0_E, et constitué de réels positifs. Il est donc minoré et admet une borne inférieure. Il suffit ensuite d'écrire que

$$\forall x \in E,\ \forall y \in A,\ \|x - y\|^2 = \|x - p_A(x) + p_A(x) - y\|^2 = \|x - p_A(x)\|^2 + \|p_A(x) - y\|^2,$$

la seconde égalité découlant de la relation de Pythagore. Il est alors clair que la valeur $\|x - p_A(x)\|$ est le plus petit élément de l'ensemble $\{\|x - y\|,\ y \in A\}$, et donc aussi sa borne inférieure.

4. On démontre d'abord que les sous-espace $\ker(p)$ et $\mathrm{Im}(p)$ sont supplémentaires en voyant qu'ils sont en somme directe du fait de leur orthogonalité et en utilisant le théorème du rang [2]. On conclut par la définition de la projection orthogonale.

□

Remarque 4.32 (« inégalité de Bessel ») *Les preuves des résultats de la dernière proposition peuvent être adaptées pour montrer le résultat suivant dans un espace préhilbertien* E *:* soit p un entier naturel non nul et $\{e_1, \dots, e_p\}$ une famille orthonormale de E. On a

$$\forall x \in E,\ \sum_{i=1}^{p} (\langle x, e_i \rangle)^2 \leq \|x\|^2,$$

avec égalité si et seulement si x appartient au sous-espace vectoriel engendré par les vecteurs $e_1, \dots, e_n$.

Remarque 4.33 *La deuxième propriété de la dernière proposition permet d'interpréter la somme apparaissant dans la formule pour les vecteurs de la base orthonormée construite par le procédé de Gram-Schmidt comme une projection orthogonale sur le sous-espace vectoriel engendré par les vecteurs de la base déjà obtenus. On peut alors réécrire cette formule de la manière suivante*

$$\forall j \in \{1, \dots, n\},\ e_j = \frac{f_j - p_{\mathrm{Vect}(\{e_1, \dots, e_{j-1}\})}(f_j)}{\left\| f_j - p_{\mathrm{Vect}(\{e_1, \dots, e_{j-1}\})}(f_j) \right\|}.$$

Application à la résolution d'un problème de régression linéaire

On suppose que l'on dispose de m observations, représentées par les réels $y_1, \dots, y_m$, associées à m conditions, liées aux réels $x_1, \dots, x_m$. On souhaite approcher le nuage de points $\{(x_i, y_i)\}_{i=1,\dots,m}$ du plan par le graphe d'une fonction φ « simple » qui dépend linéairement de n coefficients $c_1, \dots, c_n$. Le *problème de régression linéaire* consiste à déterminer « au mieux » les coefficients de la fonction φ, c'est-à-dire de manière à minimiser (en un sens à préciser) la distance entre le vecteur $(y_1, \dots, y_m)$ et le vecteur $(\varphi(x_1), \dots, \varphi(x_m))$.

D'un point de vue algébrique, ce problème se pose comme la résolution d'un système linéaire que l'on

2. On peut autrement se servir de l'idempotence de p pour établir ce résultat. En effet, tout vecteur x de E s'écrit $x = p(x) + x - p(x)$ et $x - p(x)$ appartient à $\ker(p)$ puisque $p(x - p(x)) = p(x) - p^2(x) = p(x) - p(x) = 0_E$. C'est décomposition est par ailleurs unique puisque si x est un vecteur de E appartenant à $\ker(p) \cap \mathrm{Im}(p)$, alors, d'une part, $p(x) = 0_E$ et, d'autre part, il existe un vecteur z de E tel que $p(z) = x$, d'où $x = p(z) = p^2(z) = p(x) = 0_E$.

écrit sous la forme matricielle

$$MC = Y,$$

où $C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ et M est une matrice de $M_{m,n}(\mathbb{R})$ dépendant des points $x_1, \dots, x_m$.

Dans la pratique, on a souvent $m > n$. Le système linéaire est par conséquent sur-déterminé et n'admet en général pas de solution. En effet, l'image de M est un sous-espace vectoriel de $M_{m,1}(\mathbb{R})$ de dimension au plus égale à n et le vecteur Y n'en fait pas nécessairement partie. L'introduction du *problème aux moindres carrés* vise à pallier ce problème en considérant la détermination d'un vecteur C minimisant la distance (euclidienne) entre Y et MC.

Définition 4.34 (problème aux moindres carrés) *Étant donné une matrice M de $M_{m,n}(\mathbb{R})$, avec $m > n$, et un vecteur Y de $M_{m,1}(\mathbb{R})$, le **problème aux moindres carrés** consiste à trouver un vecteur C de $M_{n,1}(\mathbb{R})$ minimisant la norme euclidienne de $Y - MC$.*

Remarque 4.35 *En pratique, la fonction φ est souvent une fonction polynomiale et l'entier $n-1$ est son degré. Si $n = m$, il existe une unique fonction polynomiale de degré $m-1$, $\varphi(x) = \sum_{i=1}^{m} c_i\, x^{i-1}$, telle que $\varphi(x_i) = y_i$ pour $i = 1, \dots, m$. En effet, le système linéaire associé au problème s'écrit alors*

$$\begin{pmatrix} 1 & x_1 & {x_1}^2 & \dots & {x_1}^{m-1} \\ 1 & x_2 & {x_2}^2 & \dots & {x_2}^{m-1} \\ \vdots & \vdots & & \vdots & \\ 1 & x_m & {x_m}^2 & \dots & {x_n}^{m-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

et il possède une unique solution dès que les réels x_i sont deux à deux distincts[a]*. La fonction polynomiale ainsi obtenue est celle correspondant au* polynôme d'interpolation de Lagrange *associé aux couples (x_i, y_i). Cependant, dans les cas de figure qui se présentent en général, on a plutôt $m > n$, comme pour l'**ajustement affine**, dans lequel la fonction φ est affine (c'est-à-dire que $n = 2$ et $\varphi(x) = c_1 + c_2\, x$).*

On cherche alors un vecteur $\hat{C}$ réalisant

$$\inf_{C \in M_{n,1}(\mathbb{R})} \|Y - MC\|.$$

Par caractérisation variationnelle de la projection orthogonale (voir la proposition 4.31), un tel vecteur doit être tel que $M\hat{C}$ soit la projection orthogonale de Y sur $\mathrm{Im}(M)$, ce qui signifie encore que le résidu $Y - M\hat{C}$ doit être orthogonal au sous-espace $\mathrm{Im}(M)$, c'est-à-dire au vecteur MZ pour tout choix de vecteur Z de $M_{n,1}(\mathbb{R})$. On a ainsi

$$\forall Z \in M_{n,1}(\mathbb{R}),\ (MZ)^\top (Y - M\hat{C}) = 0 \iff \forall Z \in M_{n,1}(\mathbb{R}),\ Z^\top M^\top (Y - M\hat{C}) = 0,$$

ce qui équivaut à avoir

$$M^\top M\hat{C} = M^\top Y, \tag{4.1}$$

ce dernier système portant le nom d'*équations normales*. On peut montrer (à titre d'exercice) que la matrice $M^\top M$ est inversible si et seulement si le rang de M est égal à n. Il en découle que les équations normales possèdent une unique solution si et seulement si le rang de la matrice M est égal au nombre de colonnes de cette dernière. Lorsque c'est le cas, une solution de $MC = Y$ au sens des moindres carrés est donnée par

$$\hat{C} = (M^\top M)^{-1} M^\top Y, \tag{4.2}$$

la matrice à n lignes et m colonnes $M^+ = (M^\top M)^{-1} M^\top$ étant appelée le *pseudo-inverse* (ou l'*inverse généralisé*) de M.

a. La matrice du système linéaire est en effet une *matrice de Vandermonde*, dont le déterminant est $\prod_{1 \le i < j \le n} (x_j - x_i)$. Ce dernier est donc non nul si les réels x_i sont deux à deux distincts.

4.3 Structure du dual d'un espace euclidien

On considère, à titre d'exemple, l'espace $E = \mathbb{R}^3$. Étant donné trois réels α, β et γ, l'application $l_{\alpha,\beta,\gamma}(x) = \alpha x_1 + \beta x_2 + \gamma x_3$ est une forme linéaire sur E, et donc un élément du dual E^* de E. On peut alors remarquer qu'on peut écrire

$$\forall x \in E,\ l_{\alpha,\beta,\gamma}(x) = \langle x, y\rangle$$

en posant $y = (\alpha, \beta, \gamma)$. Ce résultat se généralise à tout espace euclidien.

Théorème 4.36 (théorème de représentation de Riesz) *Soit E un espace euclidien. Pour tout forme linéaire ℓ sur E, il existe un unique vecteur y de E tel que*

$$\forall x \in E,\ \ell(x) = \langle \ell, x\rangle_{E^*,E} = \langle y, x\rangle\,.$$

DÉMONSTRATION. Soit l'application linéaire i_E de E dans E^* définie par

$$\forall (x,y) \in E^2,\ i_E(y)(x) = \langle x, y\rangle\,.$$

Si $i_E(y) = 0_{E^*}$, on a en particulier que

$$0 = i_E(y)(y) = \langle y, y\rangle\,,$$

d'où $y = 0_E$. L'application est ainsi injective, et donc surjective, puisque $\dim(E) = \dim(E^*)$. □

4.4 Endomorphismes d'un espace euclidien

Dans toute cette section, sauf mention contraire, E désigne un espace euclidien de dimension n non nulle. Les analogues des définitions et résultats dans le cas d'un espace E hermitien seront donnés ou mentionnés sous forme de remarques.

4.4.1 Adjoint d'un endomorphisme

Théorème et définition 4.37 (adjoint d'un endomorphisme) *Soit u un endomorphisme de E. Il existe un unique endomorphisme de E, noté u^* et appelé **adjoint de** u, tel que*

$$\forall (x,y) \in E^2,\ \langle u(x), y\rangle = \langle x, u^*(y)\rangle\,.$$

DÉMONSTRATION. Soit $\mathscr{B} = \{e_1, \ldots, e_n\}$ une base orthonormée de E. Si l'endomorphisme u^* existe, on a en particulier

$$\forall i \in \{1,\ldots,n\},\ \forall y \in E,\ \langle u(e_i), y\rangle = \langle e_i, u^*(y)\rangle\,,$$

et l'on déduit alors de la proposition 4.21 qu'il est défini de façon unique par

$$\forall y \in E,\ u^*(y) = \sum_{i=1}^{n} \langle u(e_i), y\rangle\, e_i.$$

□

Exemple 4.38 (adjoints des multiplications à gauche et à droite) *Soit n un entier naturel non nul et A une matrice réelle d'ordre n. Dans $M_n(\mathbb{R})$ muni de sa structure euclidienne canonique, les endomorphismes de multiplication à gauche et à droite par A, respectivement définis par $L_A(M) = AM$ et $R_A(M) = MA$, ont pour adjoints respectifs ${L_A}^* = L_{A^\top}$ et ${R_A}^* = R_{A^\top}$. On a en effet*

$$\forall (M,N) \in (M_n(\mathbb{R}))^2,\ \langle L_A(M), N\rangle = \langle AM, N\rangle = \operatorname{tr}\left((AM)^\top N\right) = \operatorname{tr}\left(M^\top A^\top N\right) = \left\langle M, A^\top N\right\rangle,$$

$$\langle R_A(M), N\rangle = \langle MA, N\rangle = \operatorname{tr}\left((MA)^\top N\right) = \operatorname{tr}\left(A^\top M^\top N\right) = \operatorname{tr}\left(M^\top N A^\top\right) = \left\langle M, NA^\top\right\rangle.$$

Remarque 4.39 *La notion d'adjoint vaut aussi dans le cas d'un espace hermitien.*

Proposition 4.40 (propriétés de l'adjoint d'un endomorphisme) *Soit u et v deux endomorphismes de E. On a les propriétés suivantes.*

(i) $\forall \lambda \in \mathbb{R},\ \forall (u,v) \in (\mathscr{L}(E))^2,\ (\lambda u + v)^* = \lambda u^* + v^*$.

(ii) $\forall u \in \mathscr{L}(E),\ (u^*)^* = u$.

(iii) $\forall (u,v) \in (\mathscr{L}(E))^2,\ (u \circ v)^* = v^* \circ u^*$.

(iv) $\forall u \in \mathscr{L}(E),\ \ker(u^*) = (\mathrm{Im}\,(u))^\perp$ *et* $\mathrm{Im}\,(u^*) = (\ker(u))^\perp$. *En particulier,* $\mathrm{rang}(u^*) = \mathrm{rang}(u)$.

DÉMONSTRATION.

(i) On a, par bilinéarité du produit scalaire,

$$\begin{aligned}\forall (x,y) \in E^2,\ \langle x, (\lambda u + v)^*(y)\rangle = \langle (\lambda u + v)(x), y\rangle &= \langle \lambda u(x) + v(x), y\rangle = \lambda \langle u(x), y\rangle + \langle v(x), y\rangle \\ &= \lambda \langle x, u^*(y)\rangle + \langle x, v^*(y)\rangle = \langle x, \lambda u^*(y) + v^*(y)\rangle = \langle x, (\lambda u^* + v^*)(y)\rangle\,.\end{aligned}$$

Il résulte que, pour tout vecteur y de E, le vecteur $(\lambda u + v)^*(y) - (\lambda u^* + v^*)(y)$ appartient à $E^\perp = \{0_E\}$, d'où $(\lambda u + v)^* = \lambda u^* + v^*$.

(ii) On a d'une part

$$\forall (x,y) \in E^2,\ \langle u^*(x), y\rangle = \langle x, (u^*)^*(y)\rangle\,,$$

et d'autre part, par symétrie du produit scalaire,

$$\forall (x,y) \in E^2,\ \langle u^*(x), y\rangle = \langle y, u^*(x)\rangle = \langle u(y), x\rangle = \langle x, u(y)\rangle\,.$$

On en déduit que, pour tout vecteur y de E, le vecteur $(u^*)^*(y) - u(y)$ appartient à $E^\perp = \{0_E\}$, d'où $(u^*)^* = u$.

(iii) On a

$$\forall (x,y) \in E^2,\ \langle (u \circ v)(x), y\rangle = \langle u(v(x)), y\rangle = \langle v(x), u^*(y)\rangle = \langle x, v^*(u^*(y))\rangle = \langle x, (v^* \circ u^*)(y)\rangle\,.$$

On conclut par unicité de l'adjoint.

(iv) On a

$$\begin{aligned}x \in \ker(u^*) &\iff u^*(x) = 0_E \\ &\iff \forall y \in E,\ \langle y, u^*(x)\rangle = 0 \\ &\iff \forall y \in E,\ \langle u(y), x\rangle = 0 \\ &\iff x \in (\mathrm{Im}\,(u))^\perp.\end{aligned}$$

La seconde égalité se déduit de la première en utilisant que $(u^*)^* = u$ et que $((Im(u))^\perp)^\perp = \mathrm{Im}\,(u)$, puisque E est de dimension finie (voir le corollaire 4.16). Enfin, il découle du théorème du rang et d'un des résultats du corollaire 4.16 que

$$\mathrm{rang}(u^*) = \dim(\mathrm{Im}\,(u^*)) = \dim((\ker(u))^\perp) = \dim(E) - \dim(\ker(u)) = \dim(\mathrm{Im}\,(u)) = \mathrm{rang}(u).$$

□

Le prochain résultat sera utile dans la suite.

Lemme 4.41 *Soit u un endomorphisme de E. Si A est un sous-espace vectoriel de E stable par u, son orthogonal $A^\perp$ est stable par u^*.*

DÉMONSTRATION. Le sous-espace A étant stable par u, le vecteur $u(x)$ appartient à A pour tout vecteur x de A. On a alors

$$\forall x \in A,\ \forall y \in A^\perp,\ \langle x, u^*(y)\rangle = \langle u(x), y\rangle = 0,$$

d'où le vecteur $u^*(y)$ appartient à $A^\perp$ pour tout vecteur y de $A^\perp$. □

Proposition 4.42 (matrice représentative de l'adjoint d'un endormorphisme dans une base orthonormée) *Soit u un endomorphisme de E et $\mathscr{B}$ une base orthonormée de E. On a*

$$Mat_{\mathscr{B}}(u^*) = Mat_{\mathscr{B}}(u)^\top.$$

DÉMONSTRATION. La relation définissant l'adjoint s'écrit matriciellement

$$\begin{aligned} &\forall (x,y) \in E^2,\ (\mathrm{Mat}_{\mathscr{B}}(u)\mathrm{Mat}_{\mathscr{B}}(x))^\top \mathrm{Mat}_{\mathscr{B}}(y) = \mathrm{Mat}_{\mathscr{B}}(x)^\top \mathrm{Mat}_{\mathscr{B}}(u^*)\mathrm{Mat}_{\mathscr{B}}(y) \\ \iff &\forall (x,y) \in E^2,\ \mathrm{Mat}_{\mathscr{B}}(x)^\top \mathrm{Mat}_{\mathscr{B}}(u)^\top \mathrm{Mat}_{\mathscr{B}}(y) = \mathrm{Mat}_{\mathscr{B}}(x)^\top \mathrm{Mat}_{\mathscr{B}}(u^*)\mathrm{Mat}_{\mathscr{B}}(y), \end{aligned}$$

d'où la conclusion. □

Remarque 4.43 *Lorsque l'espace vectoriel E est hermitien, on a $Mat_{\mathscr{B}}(u^*) = Mat_{\mathscr{B}}(u)^*$.*

La notion d'endomorphisme adjoint dans un espace préhilbertien permet de définir plusieurs classes d'endomorphismes qui possédent une relation particulière avec leurs adjoints respectifs. La fin de ce chapitre est consacrée à trois de ces catégories importantes d'endomorphismes.

4.4.2 Isométries vectorielles

Définition 4.44 (isométrie vectorielle) *Soit E un espace préhilbertien et u un endomorphisme de E. On dit que u est une **isométrie vectorielle** (ou encore un **endomorphisme orthogonal**) si*

$$\forall x \in E,\ \|u(x)\| = \|x\|.$$

*On appelle **groupe orthogonal** de E, et on note $O(E)$, l'ensemble des isométries vectorielles de E.*

On déduit immédiatement de cette définition que les seules valeurs propres réelles possibles pour une isométrie vectorielle sont -1 et 1.

Exemple 4.45 *Les seules homothéties qui sont des isométries vectorielles sont $-id_E$ et id_E.*

Remarque 4.46 *Toute application conservant la norme n'est pas nécessairement linéaire, et n'est donc pas une isométrie vectorielle. Un exemple est donné par l'application $x \mapsto \|x\| e$, avec e un vecteur de norme égale à 1.*

Remarque 4.47 (endomorphisme unitaire) *Si l'espace vectoriel E est hermitien, on parle d'endomorphisme **unitaire**. On appelle **groupe unitaire** de E, et on note $U(E)$, l'ensemble des endomorphismes unitaires de E.*

Proposition 4.48 *Soit E un espace préhilbertien. Une application u de E dans E est une isométrie vectorielle si et seulement si*

$$\forall (x,y) \in E^2,\ \langle u(x), u(y)\rangle = \langle x, y\rangle .$$

DÉMONSTRATION. On suppose que u est une isométrie vectorielle de E. Par définition, c'est un endomorphisme de E vérifiant

$$\forall x \in E,\ \|u(x)\| = \|x\|.$$

On a alors, en vertu d'une identité de polarisation associée au produit scalaire sur E,

$$\begin{aligned} \forall (x,y) \in E^2,\ \langle u(x), u(y)\rangle &= \frac{1}{4}\left(\|u(x)+u(y)\|^2 - \|u(x)-u(y)\|^2\right) \\ &= \frac{1}{4}\left(\|u(x+y)\|^2 - \|u(x-y)\|^2\right) \\ &= \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right) \\ &= \langle x, y\rangle . \end{aligned}$$

Réciproquement, en choisissant $x = y$ dans l'égalité de l'énoncé, on trouve que

$$\forall x \in E,\ \|u(x)\|^2 = \|x\|^2,$$

et l'application u préserve la norme. Il reste à montrer qu'elle est linéaire. On a, pour tout scalaire λ et tous vecteurs x et y de E,

$$\begin{aligned}
\|u(\lambda x+y)-\lambda u(x)-u(y)\|^2 &= \|u(\lambda x+y)\|^2+\|\lambda u(x)\|^2+\|u(y)\|^2 \\
&\qquad -2\langle u(\lambda x+y),\lambda u(x)\rangle-2\langle u(\lambda x+y),u(y)\rangle+2\langle \lambda u(x),u(y)\rangle \\
&= \|u(\lambda x+y)\|^2+|\lambda|^2\,\|u(x)\|^2+\|u(y)\|^2 \\
&\qquad -2\lambda\langle u(\lambda x+y),u(x)\rangle-2\langle u(\lambda x+y),u(y)\rangle+2\overline{\lambda}\langle u(x),u(y)\rangle \\
&= \|\lambda x+y\|^2+|\lambda|^2\,\|x\|^2+\|y\|^2-2\lambda\langle \lambda x+y,x\rangle-2\langle \lambda x+y,y\rangle+2\overline{\lambda}\langle x,y\rangle \\
&= \|\lambda x+y\|^2+\|\lambda x\|^2+\|y\|^2-2\langle \lambda x+y,\lambda x\rangle-2\langle \lambda x+y,y\rangle+2\langle \lambda x,y\rangle \\
&= \|\lambda x+y-\lambda x-y\|^2 \\
&= 0.
\end{aligned}$$

Par propriété de la norme, il vient alors que

$$\forall \lambda\in\mathbb{K},\ \forall (x,y)\in E^2,\ u(\lambda x+y)-\lambda u(x)-u(y)=0_E,$$

d'où la conclusion. □

Dans la précédente proposition, on peut observer que l'application n'est pas supposée linéaire. Comme on peut le voir dans la preuve, sa linéarité est une conséquence de sa préservation du produit scalaire.

Il découle de cette caractérisation qu'une isométrie vectorielle conserve l'orthogonalité, mais toute application conservant l'orthogonalité n'est pas nécessairement une isométrie vectorielle, comme le montre l'exemple d'une homothétie de rapport différent de -1 ou 1.

Théorème 4.49 *Une isométrie vectorielle de E est un automorphisme de E, dont l'inverse est donné par son adjoint.*

DÉMONSTRATION. Soit u une isométrie vectorielle de E. Pour tout vecteur x appartenant au noyau de u, on a

$$0=\|u(x)\|=\|x\| \implies x=0_E,$$

et l'endomorphisme est donc injectif. L'espace E étant de dimension finie, ceci équivaut à dire que u est bijectif.

Enfin, on a, d'après la précédente proposition,

$$\forall (x,y)\in E^2,\ \langle x,y\rangle=\langle u(x),u(y)\rangle=\langle x,u^*(u(y))\rangle,$$

d'où $u^*\circ u=id_E$. □

Remarque 4.50 *On peut montrer (voir le théorème 5.3) que $O(E)$ est un sous-groupe de $GL(E)$, le groupe des automorphismes de E (que l'on munit de la composition des applications et dont l'élément neutre est l'application identité). Ceci explique le nom donné à $O(E)$. En revanche, en dimension infinie, une isométrie vectorielle est injective, mais pas nécessairement surjective, et l'ensemble des isométries vectorielles n'est donc pas toujours un groupe.*

Proposition 4.51 *Soit u une isométrie vectorielle de E. Si A est un sous-espace vectoriel de E stable par u, son supplémentaire orthogonal $A^\perp$ est aussi stable par u.*

DÉMONSTRATION. L'endomorphisme u étant injectif, on a $\dim(u(A))=\dim(A)$ et, par stabilité de A par u, on peut conclure que $u(A)=A$. Soit x un vecteur de $A^\perp$. On a

$$\forall y\in A,\ \langle u(x),u(y)\rangle=\langle x,y\rangle=0,$$

d'où $u(x)$ appartient à $(u(A))^\perp=A^\perp$. □

Remarque 4.52 *Ce résultat reste vrai si A est un sous-espace vectoriel de dimension* finie *d'un espace préhilbertien.*

Proposition 4.53 *Un endomorphisme u de E est une isométrie vectorielle si et seulement si l'image d'une base orthonormale de E par u est une base orthonormale de E.*

DÉMONSTRATION. Soit $\mathscr{B} = \{e_1, \dots, e_n\}$ une base orthonormale de E. On suppose que l'endomorphisme u est une isométrie vectorielle. On a

$$\forall (i,j) \in \{1,\dots,n\}^2,\ \left\langle u(e_i), u(e_j)\right\rangle = \left\langle e_i, e_j\right\rangle = \delta_{ij}.$$

La famille $\{u(e_1), \dots, u(e_n)\}$ est ainsi une famille libre de n vecteurs, c'est donc une base de E.

Réciproquement, on suppose que l'endomorphisme u transforme la base $\mathscr{B}$ en une base orthonormale de E. On a alors

$$\forall x \in E,\ x = \sum_{i=1}^{n} x_i\, e_i,\ \|u(x)\|^2 = \left\|\sum_{i=1}^{n} x_i\, u(e_i)\right\|^2 = \sum_{i=1}^{n} {x_i}^2 \|u(e_i)\|^2 = \sum_{i=1}^{n} {x_i}^2 = \|x\|^2,$$

et u est une isométrie vectorielle. □

Proposition 4.54 (propriétés matricielles d'une isométrie vectorielle) *Soit $\mathscr{B}$ une base orthonormale de E. Un endomorphisme de E est une isométrie vectorielle si et seulement si sa matrice M dans la base $\mathscr{B}$ est telle que*

$$M^\top M = M M^\top = I_n.$$

DÉMONSTRATION. On pose $\mathscr{B} = \{e_1, \dots, e_n\}$. Soit u un endomorphisme de E de matrice M dans la base $\mathscr{B}$. On suppose tout d'abord que u est une isométrie vectorielle. On a

$$\forall (i,j) \in \{1,\dots,n\}^2,\ (M^\top M)_{ij} = {C_i}^\top C_j,$$

où C_i et C_j sont respectivement les i^{e} et j^{e} colonnes de la matrice M, et par conséquent

$$\forall (i,j) \in \{1,\dots,n\}^2,\ (M^\top M)_{ij} = \left\langle u(e_i), u(e_j)\right\rangle = \left\langle e_i, e_j\right\rangle = \delta_{ij},$$

ce qui signifie encore que $M^\top M = I_n$. La matrice M est donc inversible, d'inverse $M^\top$, et on a par conséquent $M M^\top = I_n$.

Réciproquement, si la matrice M est telle que $M^\top M = M M^\top = I_n$, cela signifie que

$$\forall (i,j) \in \{1,\dots,n\}^2,\ \left\langle u(e_i), u(e_j)\right\rangle = \delta_{ij}.$$

L'image de la base $\mathscr{B}$ par l'endomorphisme u est donc une base orthonormée de E. On en déduit que u est une isométrie vectorielle en utilisant la proposition 4.53. □

Définition 4.55 (matrice orthogonale) *Soit n un entier naturel non nul. On appelle **matrice orthogonale** une matrice d'ordre n à coefficients réels telle que*

$$M^\top M = M M^\top = I_n.$$

On note $O(n,\mathbb{R})$ l'ensemble des matrices orthogonales d'ordre n.

Une telle définition implique que toute matrice orthogonale M est inversible, d'inverse $M^{-1} = M^\top$. Par conséquent, pour tout entier n non nul, l'ensemble $O(n,\mathbb{R})$ est un sous-ensemble de $GL(n,\mathbb{R})$.

Remarque 4.56 (matrice unitaire) *Toute matrice M représentant dans une base orthonormée un endomorphisme unitaire d'un espace hermitien de dimension n vérifie les égalités $M^* M = M M^* = I_n$. Elle est dite **unitaire**. L'ensemble des matrices unitaires est noté $U(n,\mathbb{C})$.*

La proposition 4.54 affirme qu'un endomorphisme d'un espace euclidien E est une isométrie vectorielle si et seulement si sa matrice dans une base orthonormale de E est une matrice orthogonale (resp. unitaire). De la même manière, on peut montrer qu'un endomorphisme d'un espace hermitien E est unitaire si et seulement si sa matrice dans une base orthonormale de E est une matrice unitaire. Il en découle que, pour tout espace euclidien (resp. hermitien) de dimension n non nulle, $O(E)$ (resp. $U(E)$) est isomorphe à $O(n,\mathbb{R})$ (resp. $U(n,\mathbb{C})$).

Enfin, une conséquence directe des deux dernières propositions et de la définition est la caractérisation suivante des matrices orthogonales.

Corollaire 4.57 (caractérisation des matrices orthogonales) *Une matrice est orthogonale si et seulement si c'est la matrice de passage d'une base orthonormale à une autre base orthonormale.*

On reviendra plus en détails sur les propriétés des isométries vectorielles et les matrices orthogonales dans le chapitre 5.

4.4.3 Endomorphismes auto-adjoints

Définition 4.58 (endomorphisme auto-adjoint) *Un endomorphisme u de E est dit* ***auto-adjoint*** *(ou* ***symétrique****) si et seulement si $u^* = u$, ce qui équivaut encore à avoir*

$$\forall (x,y) \in E^2,\ \langle u(x), y\rangle = \langle x, u(y)\rangle .$$

Par ailleurs, l'endomorphisme u est dit ***anti-auto-adjoint*** *(ou* ***antisymétrique****) si et seulement si $u^* = -u$, c'est-à-dire si et seulement si*

$$\forall (x,y) \in E^2,\ \langle u(x), y\rangle = -\langle x, u(y)\rangle .$$

Exemple 4.59 *On a précédemment vu (voir la proposition 4.31) que le projecteur orthogonal sur un sous-espace vectoriel A, de base orthonormée $\{e_1, \ldots, e_p\}$, d'un espace euclidien E pouvait s'écrire*

$$\forall x \in E,\ p_A(x) = \sum_{i=1}^{p} \langle x, e_i\rangle\, e_i.$$

On a alors

$$\forall (x,y) \in E^2,\ \langle p_A(x), y\rangle = \left\langle \sum_{i=1}^{p} \langle x, e_i\rangle\, e_i, y \right\rangle = \sum_{i=1}^{p} \langle x, e_i\rangle \langle e_i, y\rangle = \left\langle x, \sum_{i=1}^{p} \langle e_i, y\rangle\, e_i \right\rangle = \langle x, p_A(y)\rangle ,$$

ce qui fait de p_A un endomorphisme auto-adjoint.

On peut montrer, en utilisant la proposition 4.42, qu'une matrice carrée représente un endomorphisme auto-adjoint (resp. anti-auto-adjoint) d'un espace euclidien dans une base orthonormale si et seulement si elle est réelle symétrique (resp. antisymétrique).

Remarque 4.60 *Dans un espace hermitien, un endomorphisme est auto-adjoint si et seulement si sa matrice dans une base orthonormale est* complexe hermitienne*, c'est-à-dire qu'elle est égale à sa transposée conjuguée.*

Proposition 4.61 *Soit E un espace euclidien et u un endomorphisme auto-adjoint (ou anti-auto-adjoint) de E. Si A est un sous-espace vectoriel de E stable par u, alors son supplémentaire orthogonal $A^\perp$ est aussi stable par u.*

DÉMONSTRATION. Il suffit de reprendre la preuve de la proposition 4.51, en utilisant que

$$\forall x \in A^\perp, \forall y \in A,\ \langle u(x), y\rangle = \pm \langle x, u(y)\rangle = 0,$$

selon que l'endomorphisme u est auto-adjoint ou anti-auto-adjoint. □

Théorème 4.62 (diagonalisation des endomorphismes auto-adjoints) *Soit un espace euclidien (ou hermitien) et un endomorphisme auto-adjoint de cet espace. Alors, l'endomorphisme est diagonalisable, en particulier ses valeurs propres sont réelles, et ses sous-espaces propres sont deux à deux orthogonaux. Il existe donc une base orthonormale de l'espace formée de vecteurs propres.*

DÉMONSTRATION. On note E l'espace et u l'endomorphisme auto-adjoint de l'énoncé. On montre tout d'abord que le polynôme caractéristique de l'endomorphisme est scindé sur $\mathbb{R}$. On choisit pour cela une base orthonormée de E et on note M la matrice de l'endomorphisme u dans cette base. La matrice M est réelle symétrique (ou complexe hermitienne). Il existe une valeur propre λ de M, *a priori* complexe, et une matrice colonne non nulle Z, telles que $MZ = \lambda Z$. On a alors [3]

$$(MZ)^* Z = \overline{\lambda}\, Z^* Z = \overline{\lambda}\, \|Z\|^2 \text{ et } (MZ)^* Z = Z^* M^* Z = Z^* M Z = \lambda\, Z^* Z = \lambda\, \|Z\|^2,$$

d'où λ est réelle.

On montre ensuite que les sous-espaces propres sont deux à deux orthogonaux. Soit λ et ν deux valeurs propres distinctes de u, respectivement associées à des vecteurs propres x et y. On a alors

$$\lambda \langle x, y\rangle = \langle u(x), y\rangle = \langle x, u(y)\rangle = \nu \langle x, y\rangle ,$$

3. Lorsque E est un espace euclidien, et par conséquent réel, on doit se placer sur le *complexifié* de E, c'est-à-dire l'espace vectoriel sur $\mathbb{C}$ correspondant à $E \times E$ muni de l'addition usuelle et d'une multiplication externe par les nombre complexes, pour effectuer ces calculs.

d'où $(\lambda - \nu)\langle x, y\rangle = 0$ et donc $\langle x, y\rangle = 0$.

On montre enfin que u est diagonalisable. Pour cela, on suppose que l'endomorphisme possède p valeurs propres distinctes $\lambda_1, \ldots, \lambda_p$ et l'on considère la somme des sous-espaces propres

$$A = E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_p}.$$

Il est clair que le sous-espace $u(A)$ est inclus dans A et, par la proposition 4.61, on a de plus que l'orthogonal $A^\perp$ est stable par u. La restriction de u à $A^\perp$, qui est un endomorphisme autoadjoint, possède alors une valeur propre si $A^\perp$ n'est pas réduit au vecteur nul. Ceci est impossible, puisque tous les vecteurs propres de u appartiennent à A par construction. Ainsi, le sous-espace A est égal à E et l'endomorphisme est par conséquent diagonalisable. □

On en déduit immédiatement le résultat suivant.

Corollaire 4.63 (diagonalisation des matrices réelles symétriques ou complexes hermitiennes) *Pour toute matrice M réelle symétrique (resp. complexe hermitienne), il existe une matrice orthogonale O (resp. matrice unitaire U) telle que $O^\top MO$ (resp. $U^* MU$) est une matrice réelle diagonale.*

La diagonalisation d'une matrice réelle symétrique en pratique

Soit M une matrice réelle symétrique d'ordre n.

1. Calculer le polynôme caractéristique χ_M, trouver ses racines et une factorisation associée du polynôme pour obtenir les valeurs propres avec leurs ordres de multiplicité algébrique respectifs. Ce polynôme est nécessairement scindé.
2. Déterminer pour chaque valeur propre le sous-espace propre qui lui est associé. La dimension de chacun des sous-espaces est égale à l'ordre de multiplicité algébrique de la valeur propre associée.
3. Toute base de $M_{n,1}(\mathbb{K})$ formée de vecteurs propres de M n'est pas nécessairement une base orthonormée. Deux vecteurs propres associés à des valeurs propres distinctes étant orthogonaux, on normalise (en le divisant par sa norme) tout vecteur propre associé à une valeur propre simple et on orthonormalise (en utilisant le procédé de Gram–Schmidt) toute famille libre de vecteurs propres associés à une valeur propre multiple. On obtient de cette façon une base orthonormée $\{V_1, \ldots, V_n\}$ de vecteurs propres de M, associés aux valeurs propres $\lambda_1, \ldots, \lambda_n$ comptées avec leur ordre de multiplicité. La matrice P dont les colonnes sont les vecteurs V_i, $i = 1, \ldots, n$, est orthogonale et telle que

$$M = P \operatorname{diag}(\lambda_1, \ldots, \lambda_n) P^\top.$$

Ce procédé est applicable à tout matrice M complexe hermitienne, avec des adaptations idoines.

Exemple 4.64 *On considère la diagonalisation d'une matrice réelle symétrique*

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

On calcule tout d'abord le polynôme caractéristique de M. On trouve

$$\chi_M(X) = (X-1)^2(X-4)$$

On détermine ensuite les sous-espaces propres de M, ainsi que des bases orthonormées associées. On considère tout d'abord $E_1 = \ker(M - I_3)$. On a

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in E_1 \iff MX = X \iff x_1 + x_2 + x_3 = 0,$$

d'où une base de E_1 est formée, par exemple, des vecteurs $\tilde{V}_1 = \begin{pmatrix}1 & -1 & 0\end{pmatrix}^\top$ et $\tilde{V}_2 = \begin{pmatrix}1 & 0 & -1\end{pmatrix}^\top$. Cette base n'étant cependant pas orthonormée, on lui applique le procédé de Gram–Schmidt pour obtenir les vecteurs $V_1 = \begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0\end{pmatrix}^\top$ et $\tilde{V}_2 = \begin{pmatrix}\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{6}}\end{pmatrix}^\top$. On s'intéresse ensuite à $E_4 = \ker(M - 4I_3)$. On a cette fois

$$X = \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \in E_4 \iff MX = 2X \iff x_1 = x_2 = x_3,$$

d'où une base orthonormée de E_4 est formée du vecteur unitaire $V_3 = \begin{pmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}}\end{pmatrix}^\top$.

Dans la base associée à la famille (V_1, V_2, V_3), l'endomorphisme canoniquement associé à la matrice M est représenté par la matrice

$$D = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 4\end{pmatrix}.$$

En notant P la matrice de passage correspondante,

$$P = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}}\\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}}\\ 0 & -\frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}}\end{pmatrix},$$

on a que $M = PDP^\top$.

On rappelle qu'une matrice M réelle symétrique (resp. complexe hermitienne) est dite positive si la forme quadratique (resp. quadratique hermitienne) qui lui est canoniquement associée est positive. Elle est dite définie positive si la même forme quadratique est définie positive. Le dernier corollaire montre par conséquent que M est positive si et seulement si toutes ses valeurs propres sont positives, et définie positive si et seulement si toutes ses valeurs propres sont strictement positives. Plus généralement, la signature d'une forme quadratique est donnée par les nombres de valeurs propres strictement positives et strictement négatives d'une matrice qui la représente.

Corollaire 4.65 *Soit une forme quadratique (resp. hermitienne) sur un espace euclidien (resp. hermitien). Alors, il existe une base orthonormale de l'espace relativement à laquelle la matrice de la forme est diagonale.*

DÉMONSTRATION. On note E l'espace euclidien et q la forme quadratique de l'énoncé. Soit $\mathscr{B}$ une base orthonormée de E et M la matrice de la forme q relativement à la base $\mathscr{B}$. Cette dernière est réelle symétrique (resp. complexe hermitienne) et, d'après le précédent corollaire, il existe une matrice orthogonale O (resp. unitaire U) telle que la matrice $O^\top MO$ (resp. U^*MU) est réelle diagonale. La matrice O (resp. U) définit alors un changement de base faisant passer de $\mathscr{B}$ à une autre base orthonormée de E, qui est orthogonale pour la forme q (puisque la matrice de cette dernière relativement à cette nouvelle base est diagonale). □

On peut relever une différence entre ce corollaire et le théorème 3.19 assurant l'existence d'une base q-orthogonale. En effet, la base diagonalisant la forme quadratique a ici la propriété additionnelle d'être orthonormée pour le produit scalaire sur l'espace. En contrepartie, les coefficients diagonaux de la matrice diagonale résultante ne peuvent alors être autres que les valeurs propres de la matrice.

Décomposition en valeurs singulières

Une des conséquences importantes du résultat de diagonalisation d'un endomorphisme auto-adjoint dans une base orthonormée est de conduire à une généralisation à toute matrice réelle (ou complexe) de la décomposition en éléments propres d'une matrice réelle symétrique (ou complexe hermitienne) (voir le corollaire 4.63). Celle-ci est l'objet du corollaire suivant.

Corollaire 4.66 (décomposition en valeurs singulières) *Soit m et n des entiers naturels non nuls et soit M une matrice de $M_{m,n}(\mathbb{R})$ (resp. $M_{m,n}(\mathbb{C})$), que l'on suppose être de rang égal à r. Il existe des matrices orthogonales (resp.*

unitaires) U et V, respectivement d'ordre m et n, et une matrice diagonale Σ_r d'ordre r,

$$\Sigma_r = \begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \sigma_r \end{pmatrix},$$

dont les coefficients diagonaux sont réels et tels que $\sigma_1 \geq \cdots \geq \sigma_r > 0$, telles que l'on a

$$M = U\Sigma V^\top \text{ (resp. } M = U\Sigma V^*), \tag{4.3}$$

où Σ est la matrice de $M_{m,n}(\mathbb{R})$, écrite par blocs,

$$\Sigma = \begin{pmatrix} \Sigma_r & 0_{r,n-r} \\ 0_{m-r,r} & 0_{m-r,n-r} \end{pmatrix}.$$

La factorisation (4.3) *porte le nom de* ***décomposition en valeurs singulières*** *de la matrice M. Les réels $\sigma_1, \dots, \sigma_r$ sont appelés les* ***valeurs singulières*** *de M et sont les racines carrées des valeurs propres non nulles, triées par convention dans l'ordre décroissant, des matrices $MM^\top$ ou $M^\top M$ (resp. MM^* ou M^*M). Les colonnes de la matrice U sont appelées les* ***vecteurs singuliers à gauche*** *de M et sont des vecteurs propres orthonormés de $MM^\top$ (resp. MM^*). Celles de la matrice V sont appelées les* ***vecteurs singuliers à droite*** *de M et sont des vecteurs propres orthonormés de $M^\top M$. On a*

$$\forall i \in \{1, \dots, r\},\ MV_i = \sigma_i U_i \text{ et } M^\top U_i = \sigma_i V_i \text{ (resp. } M^* U_i = \sigma_i V_i).$$

DÉMONSTRATION. Les matrices $M^\top M$ et $MM^\top$ (resp. M^*M et MM^*) sont toutes deux réelles symétriques (resp. complexes hermitiennes) et positives. Elles sont donc diagonalisables dans des bases orthonormées en vertu du corollaire 4.63 et possèdent les mêmes valeurs propres strictement positives d'après la remarque 1.25, que l'on note $\lambda_1 \geq \cdots \geq \lambda_r > 0$. Il existe ainsi une matrice orthogonale (resp. unitaire) V d'ordre n telle que

$$V^\top M^\top M V = \begin{pmatrix} \Lambda_r & 0_{r,n-r} \\ 0_{n-r,n} & 0_{n-r,n-r} \end{pmatrix} \text{ (resp. } V^* M^* M V = \begin{pmatrix} \Lambda_r & 0_{r,n-r} \\ 0_{n-r,n} & 0_{n-r,n-r} \end{pmatrix}),$$

où Λ_r est la matrice diagonale d'ordre r dont les coefficients diagonaux sont $\lambda_1, \dots, \lambda_r$. En notant $V_1, \dots, V_n$ les colonnes de la matrice V et en posant $\sigma_1 = \sqrt{\lambda_1}, \dots, \sigma_r = \sqrt{\lambda_r}$, on a que les vecteurs $MV_1, \dots, MV_n$ de $M_{m,1}(\mathbb{R})$ (resp. $M_{m,1}(\mathbb{C})$) sont deux à deux orthogonaux et tels que

$$\forall j \in \{1, \dots, r\},\ \|MV_j\| = \sigma_j \text{ et, } \forall j \in \{r+1, n\},\ MV_j = 0.$$

On pose alors

$$\forall j \in \{1, \dots, r\},\ U_j = \frac{MV_j}{\sigma_j}.$$

Par construction, ces vecteurs sont orthonormés, puisque l'on a

$$\forall (i,j) \in \{1, \dots, r\}^2,\ {U_i}^\top U_j = \frac{1}{\sigma_i \sigma_j} (MV_i)^\top MV_j = \frac{1}{\sigma_i \sigma_j} {V_i}^\top M^\top M V_j = \frac{\lambda_j}{\sigma_i \sigma_j} {V_i}^\top V_j = \frac{{\sigma_j}^2}{\sigma_i \sigma_j} \delta_{ij},$$

et l'on peut compléter la famille qu'ils forment par des vecteurs $U_{r+1}, \dots, U_m$ de manière à obtenir une base orthonormée de $M_{m,1}(\mathbb{R})$ (resp. $M_{m,1}(\mathbb{C})$). La matrice U dont les colonnes sont les vecteurs $U_1, \dots, U_m$ est alors une matrice orthogonale (resp. unitaire) d'ordre m, telle que

$$MV = U\Sigma,$$

où Σ est la matrice de $M_{m,n}(\mathbb{R})$ de l'énoncé, ce qui conduit à l'identité (4.3). □

Remarque 4.67 *La décomposition en valeurs singulières d'une matrice n'est pas unique. Les valeurs singulières étant ordonnées par convention, la matrice Σ dans l'identité* (4.3) *est bien définie de manière unique, mais les matrices U et V ne le sont pas.*

Exemple 4.68 *On considère le calcul d'une décomposition en valeurs singulières de la matrice rectangulaire*

$$M = \begin{pmatrix} 1 & 1 \\ 2 & 1 \\ -1 & 1 \end{pmatrix}.$$

On a tout d'abord

$$M^\top M = \begin{pmatrix} 6 & 2 \\ 2 & 3 \end{pmatrix},$$

d'où $\chi_{M^\top M}(X) = X^2 - 9X + 14 = (X-2)(X-7)$. *Les valeurs singulières de la matrice M sont par conséquent* $\sigma_1 = \sqrt{7}$ *et* $\sigma_2 = \sqrt{2}$.
Les colonnes de la matrice V dans l'identité (4.3) *formant une base orthonormées de vecteurs propres de la matrice* $M^\top M$, *on détermine ensuite les sous-espaces propres de* $M^\top M$. *On a, d'une part,*

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \ker(M^\top M - 7I_2) \iff \begin{cases} 6x_1 + 2x_2 = 7x_1 \\ 2x_1 + 3x_2 = 7x_2 \end{cases} \iff x_2 = \frac{1}{2}x_1,$$

on choisit alors, par exemple, $V_1 = \frac{1}{\sqrt{5}}(2,1)^\top$, *et, d'autre part,*

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \ker(M^\top M - 2I_2) \iff \begin{cases} 6x_1 + 2x_2 = 2x_1 \\ 2x_1 + 3x_2 = 2x_2 \end{cases} \iff x_2 = -2x_1,$$

on choisit alors, par exemple, $V_2 = \frac{1}{\sqrt{5}}(1,-2)^\top$. *Les colonnes de la matrices U sont enfin données par* $U_1 = \frac{1}{\sigma_1}MV_1$, $U_2 = \frac{1}{\sigma_2}MV_2$, *c'est-à-dire*

$$U_1 = \frac{1}{\sqrt{35}}\begin{pmatrix} 3 \\ 5 \\ -1 \end{pmatrix} \text{ et } U_2 = \frac{1}{\sqrt{10}}\begin{pmatrix} -1 \\ 0 \\ -3 \end{pmatrix},$$

la colonnes U_3 *de façon à ce que la famille formée par les vecteurs* U_1, U_2 *et* U_3 *soit une base orthonormée. On choisit, par exemple,* $U_3 = \frac{1}{\sqrt{14}}(-3,2,1)^\top$, *d'où*

$$M = \begin{pmatrix} \frac{3}{\sqrt{35}} & -\frac{1}{\sqrt{10}} & -\frac{3}{\sqrt{14}} \\ \frac{5}{\sqrt{35}} & 0 & \frac{2}{\sqrt{14}} \\ -\frac{1}{\sqrt{35}} & -\frac{3}{\sqrt{10}} & \frac{1}{\sqrt{14}} \end{pmatrix} \begin{pmatrix} \sqrt{7} & 0 \\ 0 & \sqrt{2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} \end{pmatrix}.$$

Le lecteur intéressé trouvera dans l'article [Ste93] l'histoire de l'introduction de la décomposition en valeurs singulières. Cette décomposition est particulièrement utile dans de nombreux domaines scientifiques en raison de ses diverses applications mathématiques, dont quelques-unes sont présentées ci-après. On mentionne enfin qu'elle peut être calculée numériquement via des techniques basées sur la *méthode de Golub et Kahan* [GK65].

Détermination du rang, de l'image et du noyau d'une matrice. L'identité (4.3) et la preuve de son existence ont pour conséquence des caractérisations explicites du rang, de l'image et du noyau de toute matrice M. On peut en effet voir que le rang de M est égal[4] au nombre de ses valeurs singulières (c'est-à-dire au nombre de coefficients non nuls sur la diagonale de la matrice Σ), que l'image de M est engendrée[5] par les vecteurs singuliers à gauche (c'est-à-dire les colonnes de la matrice U) associés aux valeurs singulières, et que le noyau de M engendré[6] par les vecteurs singuliers à droite (c'est-à-dire les colonnes de la matrice V) qui ne sont pas associés aux valeurs singulières. D'un point de vue numérique, le rang déterminé n'est qu'*effectif* dans le cas d'une matrice dont le rang n'est pas maximal, car les erreurs d'arrondi peuvent entraîner l'apparition de coefficients diagonaux de la matrice Σ non nuls, mais petits, qui ne correspondent pas à des valeurs singulières de la matrice. En pratique, lors du compte des valeurs singulières, on choisit généralement d'ignorer les coefficients diagonaux dont la valeur est en dessous d'un seuil judicieusement choisi[7].

4. On a en effet $\operatorname{rang}(M) = \operatorname{rang}(\Sigma)$.
5. Ceci découle du fait que l'image de Σ est engendrée par les r premiers vecteurs de la base canonique de $M_{m,1}(\mathbb{R})$, où r est le rang de M.
6. Ceci découle du fait que le noyau de Σ est engendré par les $n-r$ derniers vecteurs de la base canonique de $M_{n,1}(\mathbb{R})$, où r est le rang de M.
7. Un choix courant pour ce seuil est $\sigma_1 \max(m,n)\varepsilon$, où ε est l'epsilon (ou unité d'arrondi) du processeur de calcul.

Calcul effectif du pseudo-inverse d'une matrice. Le *pseudo-inverse de Moore–Penrose* [Moo20, Bje51, Pen55] d'une matrice de rang non nul qui est un objet généralisant la notion d'inverse à des matrices rectangulaires, ou carrées mais non inversibles. Étant donné une matrice M de $M_{m,n}(\mathbb{R})$ (resp. $M_{m,n}(\mathbb{C})$), son pseudo-inverse est l'unique matrice M^+ de $M_{n,m}(\mathbb{R})$ (resp. $M_{n,m}(\mathbb{C})$) satisfaisant les conditions, dites de Moore–Penrose, suivantes :

1. $MM^+M = M$,
2. $M^+MM^+ = M^+$,
3. $(MM^+)^\top = MM^+$(resp. $(MM^+)^* = MM^+$),
4. $(M^+M)^\top = M^+M$ (resp. $(M^+M)^* = M^+M$).

La décomposition en valeurs singulières fournit une façon simple de calculer ce pseudo-inverse. Celui-ci est en effet donné, avec les notations du corollaire 4.66, par

$$M^+ = V\Sigma^+U^\top \text{ (resp. } M^+ = V\Sigma^+U^*), \tag{4.4}$$

où Σ^+ est la matrice de $M_{n,m}(\mathbb{R})$, écrite par blocs,

$$\Sigma^+ = \begin{pmatrix} {\Sigma_r}^{-1} & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix}.$$

Le pseudo-inverse intervient dans la résolution du problème aux moindres carrés (voir la sous-section 4.2.3), en permettant d'exprimer une solution des équations normales (4.1), qui constituent une condition nécessaire et suffisante satisfaite par les solutions du problème aux moindres carrés. On a en effet, en reprenant les notations matricielles utilisées pour le problème aux moindres carrés et celles du corollaire 4.66,

$$M^\top M(M^+Y) = V\Sigma^\top\Sigma\Sigma^+U^\top Y = V\Sigma^\top \begin{pmatrix} I_r & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix} U^\top Y = M^\top Y,$$

et $\hat{C} = M^+Y$ est donc une solution des équations normales. Il découle par ailleurs de la caractérisation (4.4) que cette solution est l'unique solution de norme euclidienne minimale des équations normales. Pour le voir, on considère une solution C des équations normales. La différence $C - \hat{C}$ appartient par conséquent au noyau de $M^\top M$, dont on sait qu'il est engendré par les colonnes $V_{r+1}, \ldots, V_n$ de la matrice V. On a

$$\forall i \in \{r+1, \ldots, n\},\ {V_i}^\top \hat{C} = {V_i}^\top M^+Y = {V_i}^\top V\Sigma^+U^\top Y = \left(U{\Sigma^+}^\top V^\top V_i\right)^\top Y = \left(U{\Sigma^+}^\top E_i\right)^\top Y = 0,$$

où E_i désigne le i^{e} vecteur de la base canonique de $M_{m,1}(\mathbb{R})$, car les $n-r$ dernières colonnes de la matrice ${\Sigma^+}^\top$ sont nulles. Par conséquent, le vecteur $\hat{C}$ est orthonogonal à $\ker(M^\top M)$ et il vient, par utilisation de la relation de Pythagore (voir la proposition 4.18),

$$\|C\|^2 = \|C - \hat{C} + \hat{C}\|^2 = \|C - \hat{C}\|^2 + \|\hat{C}\|^2 \geq \|\hat{C}\|^2,$$

avec égalité si et seulement si $C = \hat{C}$.

Approximation de rang faible. On considère le problème d'approximation d'une matrice donnée par une matrice dont le rang est plus faible. Dans le cas où l'approximation est construite par minimisation de la norme de Frobenius (voir l'exemple 4.5) de la différence entre les deux matrices sous contrainte de rang, ce problème s'énonce de la manière suivante : *étant donné m et n des entiers naturels non nuls et M une matrice de $M_{m,n}(\mathbb{K})$, on cherche une matrice N réalisant*

$$\inf_{\substack{N \in M_{m,n}(\mathbb{K}) \\ \operatorname{rang}(N) \leq k}} \|M - N\|_F, \tag{4.5}$$

où l'entier naturel k est tel que $k \leq \operatorname{rang}(M)$ et $\|\cdot\|_F$ désigne la norme de Frobenius. La décomposition en valeurs singulières permet de résoudre ce problème. On a plus précisement la caractérisation suivante.

Théorème 4.69 (« théorème d'Eckart–Young » [EY36]) *La solution du problème* (4.5) *est donnée par*

$$\tilde{M} = U\tilde{\Sigma}V^{\top} \text{ si } \mathbb{K} = \mathbb{R},\ \tilde{M} = U\tilde{\Sigma}V^{*} \text{ si } \mathbb{K} = \mathbb{C},$$

où U et V sont les matrices orthogonales si $\mathbb{K} = \mathbb{R}$, unitaires si $\mathbb{K} = \mathbb{C}$, d'une décomposition en valeurs singulières de M et où $\tilde{\Sigma}$ est une matrice de $M_{m,n}(\mathbb{R})$ définie par blocs,

$$\tilde{\Sigma} = \begin{pmatrix} \Sigma_k & 0_{k,n-k} \\ 0_{m-k,k} & 0_{m-k,n-k} \end{pmatrix},$$

où Σ_k est la matrice diagonale d'ordre k dont les coefficients diagonaux sont les k premières valeurs singulières $\sigma_1, \ldots, \sigma_k$ de M.

Pour démontrer ce résultat, on a besoin d'établir la propriété suivante pour la norme de Frobenius.

Lemme 4.70 *La norme de Frobenius est invariante par transformation orthogonale (resp. unitaire), c'est-à-dire que pour tous entiers naturels non nuls m et n, pour toute matrice réelle (resp. complexe) à m lignes et n colonnes, pout toutes matrices orthogonales (resp. unitaires) U d'ordre m et V d'ordre n, on a*

$$\|UMV\|_F = \|M\|_F.$$

DÉMONSTRATION. On prouve l'égalité dans le cas réel, l'adaptation au cas complexe se faisant en remplaçant les transpositions de matrice par des transconjugaisons. Par définition de la norme de Frobenius et par propriétés de la trace et des matrices orthogonales, il vient

$$\begin{aligned}\|UMV\|_F{}^2 = \operatorname{tr}\left((UMV)^{\top}UMV\right) &= \operatorname{tr}\left(V^{\top}M^{\top}U^{\top}UMV\right) \\ &= \operatorname{tr}\left(V^{\top}M^{\top}MV\right) = \operatorname{tr}\left(VV^{\top}M^{\top}M\right) = \operatorname{tr}\left(M^{\top}M\right) = \|M\|_F{}^2.\end{aligned}$$

□

DÉMONSTRATION DU THÉORÈME 4.69. On prouve le résultat dans le cas réel, l'adaptation au cas complexe étant immédiate On emploie les mêmes notations que dans le corollaire 4.66. En vertu de ce dernier, la matrice M admet une décomposition en valeurs singulières. En utilisant le lemme 4.70, on a, pour toute matrice N de $M_{m,n}(\mathbb{R})$,

$$\|M-N\|_F = \left\|U\Sigma V^{\top} - N\right\|_F = \left\|\Sigma - U^{\top}NV\right\|_F.$$

En posant $N' = U^{\top}NV$, le problème d'approximation de rang faible se ramène à la minimisation de la norme de Frobenius de la différence $\Sigma - N'$, où N' est une matrice de $M_{m,n}(\mathbb{R})$ de rang inférieur ou égal à k. Il vient alors

$$\left\|\Sigma - N'\right\|_F{}^2 = \sum_{i=1}^{m}\sum_{j=1}^{n}((\Sigma)_{ij} - (N')_{ij})^2 = \sum_{i=1}^{r}(\sigma_i - (N')_{ii})^2 + \sum_{i=r+1}^{\min(m,n)}((N')_{ii})^2 + \sum_{i=1}^{m}\sum_{\substack{j=1 \\ j\neq i}}^{n}((N')_{ij})^2.$$

Cette dernière somme à termes positifs est minimale sous la contrainte de rang pour N' lorsque les coefficients extra-diagonaux de cette matrice sont nuls, chacun de ses k premiers coefficients diagonaux est égal à la valeur singulière de M correspondante et les coefficients diagonaux restants sont nuls. Ceci correspond à prendre N' égale à $\tilde{\Sigma}$, ce qui permet de conclure. □

Une des applications du théorème d'Eckart–Young concerne la *compression d'image avec perte*. Toute image en niveaux de gris[8] composée de pixels (abbréviation de la locution anglaise *picture elements*) peut être représentée par une matrice, dont le nombre de lignes correspond au nombre de pixels sur la hauteur de l'image, le nombre de colonnes correspond au nombre de pixels sur la largeur de l'image et dont chaque coefficient est un entier, donnant l'intensité lumineuse d'un pixel de l'image, codé sur un octet[9]. En effectuant une décomposition en valeurs singulières de la matrice de l'image d'origine et en calculant de meilleures approximations de rang faible de

8. Pour une image en couleurs encodée dans le système rouge-vert-bleu, la représentation utilise trois matrices dont les coefficients respectifs donnent les intensités lumineuses des pixels de l'image dans chacune des trois couleurs primaires rouge, vert et bleu, de manière à reproduire les couleurs par trichromie.

9. Ceci autorise 256 nuances de gris, du noir (0) au blanc (255).

celle-ci, il est possible de produire des images conservant une qualité visuellement acceptable et dont le stockage requiert moins de mémoire que celui de l'image d'origine. Un exemple est donné dans la figure 4.1.

FIGURE 4.1 – Exemple de compression d'image en niveaux de gris avec perte utilisant la décomposition en valeurs singulières. La première image numérique gauche de la première ligne est l'originale (l'image 5.3.01 du volume *miscellaneous* de la *SIPI Image Database*). Sa taille est de 1024 par 1024 pixels. Les images suivantes correspondent à la meilleure approximation (au sens de la norme de Frobenius) de la matrice de l'image d'origine par une matrice de rang respectivement égal à (en allant de gauche à droite) 1 et 4 pour la première ligne et 16, 64 et 256 pour la seconde ; elles ont été obtenues grâce à une décomposition en valeurs singulières.

4.4.4 Endomorphismes normaux

Définition 4.71 (endomorphisme normal) *Soit E un espace euclidien (ou hermitien) et u un endomorphisme de E. On dit que u est* ***normal*** *si u et u^* commutent entre eux, i.e. $u \circ u^* = u^* \circ u$.*

Exemple 4.72 (exemples d'endomorphisme normal) *Les endomorphismes auto-adjoints ($u^* = u$), anti-auto-adjoints ($u^* = -u$) et les isométries vectorielles ($u^* = u^{-1}$) sont des endomorphismes normaux.*

Définition 4.73 (matrice normale) *Une matrice carrée réelle (resp. complexe) M est dite* ***normale*** *si M et $M^\top$ (resp. M et M^*) commutent entre elles, i.e. $MM^\top = M^\top M$ (resp. $MM^* = M^*M$).*

Les matrices réelles symétriques, antisymétriques ou orthogonales sont des matrices normales. Les matrices complexes hermitiennes, antihermitiennes ou unitaires sont des matrices normales.

Théorème 4.74 (réduction d'un endomorphisme normal d'un espace euclidien) *Soit u un endomorphisme normal d'un espace euclidien E de dimension non nulle n. Il existe une base orthonormée de E dans laquelle la matrice représentative de u est diagonale par blocs, les blocs étant d'ordre 1 et au nombre de p ou d'ordre 2, de la forme*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ avec } (a,b) \in \mathbb{R} \times \mathbb{R}^*, \tag{4.6}$$

et au nombre de r, où p et r sont des entiers naturels tels que $p + 2r = n$.

DÉMONSTRATION. On raisonne par récurrence sur la dimension n de E. Pour $n = 1$, il n'y a rien à montrer. On suppose ensuite que, pour un entier n supérieur ou égal à 2, le résultat est vrai pour tout endomorphisme normal d'un espace euclidien de dimension inférieure ou égale à $n-1$. Deux cas se présentent alors, selon que l'endomorphisme u possède des valeurs propres ou pas.

On considère tout d'abord le cas pour lequel le spectre de u n'est pas vide. Soit λ une valeur propre de u. Alors, le sous-espace vectoriel ${E_\lambda}^\perp$ est stable par u et u^*. En effet, le sous-espace propre E_λ étant stable par u, le lemme 4.41 assure que son orthogonal est stable par u^*. De plus, on a

$$\forall x \in E_\lambda,\ u(u^*(x)) = u^*(u(x)) = u^*(\lambda x) = \lambda\, u^*(x),$$

d'où $u^*(x)$ appartient à E_λ pour tout x de E_λ. Ainsi, le sous-espace propre E_λ est stable par u^* et le lemme 4.41 assure alors que son orthogonal est stable par $(u^*)^* = u$ (voir la proposition 4.40).

Ceci permet de définir la restriction $u_{|_{{E_\lambda}^\perp}}$ qui, par unicité de l'adjoint, est un endomorphisme normal. Comme le sous-espace ${E_\lambda}^\perp$ est de dimension inférieure ou égale à $n-1$, il possède une base orthonormée dans laquelle la matrice de $u_{|_{{E_\lambda}^\perp}}$ est de la forme voulue. En concaténant cette base avec une base de E_λ, on obtient une base orthonormée de E dans laquelle la matrice de u est de la forme annoncée.

On considère à présent le cas pour lequel le spectre de u est vide. Dans ce cas, soit $Q(X) = X^2 + \alpha X + \beta$, avec $\alpha^2 < 4\beta$, un diviseur irréductible de χ_u dans $\mathbb{R}[X]$. Ce polynôme est scindé dans $\mathbb{C}$: il existe un nombre complexe λ tel que $Q(X) = (X-\lambda)(X-\overline{\lambda})$, d'où λ appartient à $\mathrm{Sp}_{\mathbb{C}}(u)$ et $\det(u - \lambda id_E) = 0$. Par suite, on a $\det(Q(u)) = \det(u-\lambda id_E)\det(u-\overline{\lambda} id_E) = 0$ et $\ker(Q(u))$ n'est donc pas réduit au vecteur nul.

L'endomorphime $Q(u)$ commutant avec u et u^*, le sous-espace $\ker(Q(u))$ est stable par u et u^* par la proposition 1.5. On peut donc définir $v = u_{|_{\ker(Q(u))}}$ et on a alors $v^* = {u^*}_{|_{\ker(Q(u))}}$, d'où l'endomorphisme $v^*v = (u^*u)_{|_{\ker(Q(u))}}$ est auto-adjoint. Soit ν une valeur propre (réelle) de v^*v, x un vecteur propre associé et $A = \mathrm{Vect}(\{x, u(x)\})$. Par hypothèse sur le spectre réel de u, le sous-espace vectoriel A est de dimension égale à 2 et, comme x appartient à $\ker(Q(u))$, on a $u^2(x) = -\alpha u(x) - \beta x$ et A est donc stable par u. On a même $A = \mathrm{Vect}\left(\left\{u(x), u^2(x)\right\}\right)$, car β est non nul, et il s'ensuit que $u^*(u(x)) = \nu x$ et $u^*(u^2(x)) = u(u^*u(x)) = u(\nu x) = \nu u(x)$, d'où A est aussi stable par u^*. On peut ainsi définir l'endomorphisme normal $u_{|_A}$ et il existe alors une base orthonormée de A dans laquelle la matrice de $u_{|_A}$ est de la forme (4.6). Soit en effet la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

représentant $u_{|_A}$ dans une base orthonormée de A. On a nécessairement que b est non nul puisque le spectre de u est vide, et, par normalité de l'endomorphisme, on a également

$$\begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & a^2+c^2 \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix},$$

d'où $c = \pm b$ et $d = \pm a$. Si $c = b$, la matrice est réelle symétrique, ce qui contredit l'hypothèse faite sur le spectre réel de u. On a par conséquent $c = -b$, et on déduit de la relation $ab + cd = ac + bd$ que $2(a-d)b = 0$, puis que $a = d$, puisque b est non nul.

En vertu du lemme 4.41, le sous-espace $A^\perp$ est stable par u^* et $(u^*)^* = u$ et l'on peut donc définir l'endomorphisme normal $u_{|_{A^\perp}}$. Puisque $A^\perp$ est de dimension égale à $n-2$, il existe une base orthonormée de $A^\perp$ dans laquelle la matrice de $u_{|_{A^\perp}}$ est de la forme attendue. La concaténation de cette dernière avec une base orthonormée de A fournit une base de E dans laquelle la matrice de u est de la forme annoncée. □

Chapitre 5

Compléments sur les isométries vectorielles

Dans ce chapitre, on revient sur l'ensemble des transformations géométriques d'un espace euclidien qui préservent la norme (et donc les distances) et ses propriétés, en mettant en avant la structure de *groupe* de cet ensemble. Les cas particuliers des groupes $O(2,\mathbb{R})$ en dimension deux et $O(3,\mathbb{R})$ en dimension trois sont considérés, ainsi que la réduction des isométries vectorielles.

5.1 Rappels sur les groupes

On rappelle tout d'abord qu'un **groupe** $(G,\circ)$ est un couple formé d'un ensemble G et d'une opération $\circ$ sur cet ensemble (parfois appelée *loi de composition*), qui à deux éléments a et b de G associe un élément $a\circ b$, satisfaisant aux quatre axiomes suivants :

- **loi de compostion interne** : $\forall (a,b)\in G^2,\ a\circ b\in G$,
- **associativité** : $\forall (a,b,c)\in G^3,\ (a\circ b)\circ c = a\circ(b\circ c)$,
- **élément neutre** : $\exists e\in G, \forall a\in E,\ e\circ a = a\circ e = a$, e étant appelé l'**élément neutre** du groupe,
- **symétrique** : $\forall a\in G,\ \exists b\in G,\ a\circ b = b\circ a = e$, où e est l'élément neutre du groupe, b étant appelé le **symétrique** de a.

Un groupe pour lequel on a de plus la propriété

$$\forall (a,b)\in G^2,\ a\circ b = b\circ a,$$

est dit **commutatif** ou **abélien**.

Remarque 5.1 (vocabulaire et notations communément utilisés) *Il y a unicité de l'élément neutre et, pour chaque élément du groupe, unicité du symétrique. L'emploi d'article défini est dans les définition ci-dessus est donc correct.*
Lorsque la loi de composition est notée additivement (on écrit $a+b$ pour $a\circ b$), le symétrique est appelé opposé (le symétrique de a est noté $-a$) et l'élément neutre est appelé zéro (et noté 0). Lorsque la loi est notée multiplicativement, (on écrit généralement $a\times b$ ou ab pour $a\circ b$), le symétrique est appelé l'inverse (le symétrique de a est noté a^{-1}), l'élément neutre est appelé unité (et noté 1).

Exemple 5.2 (exemples de groupe) *Un exemple commun de groupe est $(\mathbb{Z},+)$, l'ensemble des entiers relatifs muni de l'addition. En effet, l'addition de deux entiers est un entier, ajouter un entier c à la somme de deux entiers a et b donne le même résultat qu'ajouter l'entier a à la somme de b et de c, 0 est l'élément neutre pour l'addition et le symétrique de tout entier est son opposé.*
*Si E est un espace vectoriel sur le corps $\mathbb{K}$, l'ensemble des automorphismes de E muni la composition d'applications, noté $(GL(E),\circ)$, est un groupe appelé **groupe linéaire** de E.*

5.2 Groupe des isométries vectorielles

On va montrer que l'ensemble des isométries vectorielles d'un espace vectoriel possède une structure de groupe, qui en fait un sous-groupe du groupe linéaire de cet espace.

Théorème 5.3 *Soit E un espace euclidien de dimension non nulle. L'ensemble des isométries vectorielles $O(E)$, muni de la composition d'applications $\circ$, est un sous-groupe du groupe linéaire $(GL(E),\circ)$ appelé* ***groupe orthogonal*** *de E.*

DÉMONSTRATION. Il suffit de montrer que $O(E)$ est une partie non vide de $(GL(E),\circ)$, stable par composition et symétrisation.

Tout d'abord, l'application id_E appartient à $O(E)$, car, pour tout vecteur x de E, $id_E(x)=x$ et donc $(id_E)^{-1}=id_E$.

On considère ensuite des endomorphismes u et v appartenant à $O(E)$. On a

$$\forall x\in E,\ \|u(x)\|=\|x\|=\|v(x)\|,$$

d'où

$$\forall x\in E,\ \|u\circ v(x)\|=\|u(v(x))\|=\|v(x)\|=\|x\|,$$

le même résultat valant bien entendu pour $v\circ u$.

Enfin, soit u un endomorphisme appartenant à $O(E)$ et u^* son symétrique. On a, par définition, $u\circ u^*=u^*\circ u=id_E$, d'où

$$\forall x\in E,\ \|u\circ u^*(x)\|=\|x\|,$$

et donc

$$\forall x\in E,\ \|x\|=\|u(u^*(x))\|=\|u^*(x)\|.$$

□

Ce résultat signifie en particulier que la composée de deux isométries vectorielles et la réciproque d'une isométrie vectorielle sont des isométries vectorielles.

5.3 Matrices orthogonales

Soit n un entier naturel non nul. On rappelle (voir la définition 4.55) qu'une matrice M de $M_n(\mathbb{R})$ est dite orthogonale si et seulement si $M^\top M=MM^\top=I_n$, ce qui implique qu'une telle matrice est inversible, d'inverse $M^{-1}=M^\top$. Une telle matrice représente une isométrie vectorielle d'un espace vectoriel euclidien de dimension n dans une base orthonormée (voir la proposition 4.54). L'ensemble des matrices orthogonales à coefficients réels d'ordre n est noté $O(n,\mathbb{R})$.

Le résultat suivant constitue l'analogue matriciel du théorème 5.3.

Théorème 5.4 *Soit n un entier naturel non nul. Pour toute matrice M de $O(n,\mathbb{R})$, on a*

$$\det(M)=\pm 1.$$

et l'ensemble $O(n,\mathbb{R})$ est un sous-groupe de $GL(n,\mathbb{R})$, appelé ***groupe orthogonal réel de degré*** *n.*

DÉMONSTRATION. Par propriété du déterminant, on a

$$\forall M\in M_n(\mathbb{R}),\ \det(M)=\det\left(M^\top\right),$$

et donc

$$\forall M\in O(n,\mathbb{R}),\ (\det(M))^2=\det\left(MM^\top\right)=\det(I_n)=1.$$

Il en résulte que $O(n,\mathbb{R})$ est un sous-ensemble de $GL(n,\mathbb{R})$. Par ailleurs, la matrice I_n appartient à $O(n,\mathbb{R})$ et on a

$$\forall (M,n)\in(O(n,\mathbb{R}))^2,\ \left(M^{-1}\right)^{-1}=\left(M^\top\right)^{-1}=\left(M^{-1}\right)^\top \text{ et } (MN)^{-1}=N^{-1}M^{-1}=N^\top M^\top=(MN)^\top,$$

ce qui permet de montrer que $O(n,\mathbb{R})$ est un sous-groupe de $GL(n,\mathbb{R})$. □

Corollaire 5.5 *Soit E un espace euclidien de dimension non nulle. Si u est une isométrie vectorielle de E, alors*

$$\det(u) = \pm 1.$$

DÉMONSTRATION. La matrice représentative de u dans une base orthonormée de E étant orthogonale, le résultat découle directement du précédent théorème. □

Remarque 5.6 (groupe spécial orthogonal) *L'ensemble des isométries vectotorielles d'un espace euclidien E (resp. des matrices orthogonales d'ordre n) de déterminant égal à 1 forme un sous-groupe du groupe orthogonal de E (resp. groupe orthogonal réel de degré n), appelé* ***groupe spécial orthogonal*** *et noté $SO(E)$ (resp. $SO(n,\mathbb{R})$).*

Remarque 5.7 (groupe unitaire de degré n) *On peut montrer de la même manière que l'ensemble $U(n,\mathbb{C})$ des matrices unitaires d'ordre n est un sous-groupe de $GL(n,\mathbb{C})$, appelé le* ***groupe unitaire de degré*** *n. Le sous-ensemble des matrices unitaires d'ordre n de déterminant égal à 1 forme le* ***groupe spécial unitaire*** *$SU(n,\mathbb{C})$.*

Exemple 5.8 (le groupe spécial unitaire $SU(2,\mathbb{C})$) *Pour $n = 2$, l'ensemble $SU(2,\mathbb{C})$ est explicitement défini comme*

$$SU(2,\mathbb{C}) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} | \, (\alpha,\beta) \in \mathbb{C}^2, \ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

Les matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \ \textit{et} \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

dites ***de Pauli****, forment une base de ce sous-espace vectoriel.*

On peut caractériser une matrice orthogonale de diverses façons. On a déjà rappelé qu'une matrice orthogonale peut être interprétée comme la matrice représentative d'une isométrie vectorielle dans une base orthonormale. On a par ailleurs établi dans le précédent chapitre qu'une matrice orthogonale pouvait être vue comme la matrice de passage d'une base orthonormale à une autre base orthonormale (voir le corollaire 4.57). Une troisième caractérisation, souvent utile en pratique, est fournie par le résultat ci-après.

Proposition 5.9 *Soit n un entier naturel non nul. La famille des colonnes (resp. des lignes) d'une matrice orthogonale d'ordre n est une base orthonormale de l'espace $M_{n,1}(\mathbb{R})$ (resp. $M_{1,n}(\mathbb{R})$) muni de sa structure euclidienne canonique.*

DÉMONSTRATION. Soit M une matrice orthogonale d'ordre n dont on note $C_1, \ldots, C_n$ les colonnes. L'égalité $M^\top M = I_n$ écrite coefficient par coefficient est

$$\forall (i,j) \in \{1,\ldots,n\}^2, \ {C_i}^\top C_j = \delta_{ij},$$

ce que l'on peut encore écrire

$$\forall (i,j) \in \{1,\ldots,n\}^2, \ \left\langle C_i, C_j \right\rangle = \delta_{ij},$$

en faisant appel au produit scalaire de $M_{n,1}(\mathbb{R})$, d'où la conclusion.

On obtient le même résultat pour les lignes de la matrice en transposant l'égalité matricielle utilisée. □

Une conséquence de cette proposition est que les coefficients d'une matrice orthogonale sont inférieurs ou égal à 1 en valeur absolue.

5.4 Orientation et produit mixte

Dans cette section, on désigne par E un espace euclidien de dimension n non nulle.

Définition 5.10 (orientation) *Soit $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et P la matrice de passage de la première à la seconde de ces bases. On dit que $\mathscr{B}$ et $\mathscr{B}'$ ont la même* ***orientation*** *si et seulement si le déterminant de P est strictement positif.*

Orienter un espace vectoriel consiste à choisir arbitrairement une base de référence. Les bases de même orientation que cette base sont alors dites **directes** et les autres **indirectes**.

Remarque 5.11 *Se placer dans* « l'espace $\mathbb{R}^n$, muni de sa structure euclidienne usuelle et orienté »*, signifie que l'on a muni $\mathbb{R}^n$ du produit scalaire usuel (i.e., canonique) et considéré que la base canonique (qui est une base orthonormale pour le produit scalaire usuel) est directe.*

Proposition et définition 5.12 (produit mixte) *On suppose l'espace vectoriel E orienté et que $\mathscr{B}$ est une base orthonormale directe de E. Le* ***produit mixte*** *de la famille $\{f_1, \dots, f_n\}$ de vecteurs de E, noté $[f_1, \dots, f_n]$, est le scalaire*

$$[f_1, \dots, f_n] = \det_{\mathscr{B}}(f_1, \dots, f_n).$$

Celui-ci ne dépend pas de la base orthonormale directe choisie.

DÉMONSTRATION. Soit $\mathscr{B}$ et $\mathscr{B}'$ deux bases orthonormales directes de E. La matrice de passage P de $\mathscr{B}$ à $\mathscr{B}'$ est une matrice orthogonale, dont le déterminant vaut 1 puisque les bases ont la même orientation. On a par conséquent

$$\det_{\mathscr{B}}(f_1, \dots, f_n) = \det(P) \det_{\mathscr{B}'}(f_1, \dots, f_n) = \det_{\mathscr{B}'}(f_1, \dots, f_n).$$

□

En démontrant cette proposition, on a au passage prouvé que que le produit mixte d'une base orthonormale directe est égal à 1. Plus généralement, le produit mixte d'une base directe est strictement positif. On observe en outre que, par la formule de transformation des volumes, on a, pour tout endomorphisme u de E,

$$[u(f_1), \dots, u(f_n)] = \det(u)[f_1, \dots, f_n]. \tag{5.1}$$

Remarque 5.13 (interprétation géométrique du produit mixte en dimension 2 et 3) *Dans $\mathbb{R}^2$ muni de sa structure euclidienne canonique, le produit mixte $[x, y]$ de deux vecteurs x et y représente l'aire algébrique du parallélogramme défini par x et y. Dans $\mathbb{R}^3$ muni de sa structure euclidienne canonique, le produit mixte $[x, y, z]$ de trois vecteurs x, y et z représente le volume algébrique du parallélépipède défini par x, y et z.*

Remarque 5.14 (orientation d'un hyperplan) *Dans un espace orienté, le choix d'un vecteur normal à un hyperplan affine permet d'orienter cet hyperplan. En effet, si si v est un vecteur normal à un hyperplan affine $\mathscr{H}$, alors on dira qu'une base $\{e_1, \dots, e_{n-1}\}$ de $\mathscr{H}$ est directe si et seulement si $[e_1, \dots, e_{n-1}, v]$ est strictement positif. En choisissant $-v$ comme vecteur normal, la même base est indirecte.*

5.5 Étude des isométries vectorielles

Soit n un entier naturel non nul. On a précédemment vu que l'on pouvait définir le sous-ensemble de matrices

$$SO(n, \mathbb{R}) = \{M \in O(n, \mathbb{R}) \mid \det(M) = 1\},$$

qui est un sous-groupe de $O(n, \mathbb{R})$ appelé groupe spécial orthogonal. Celui-ci permet d'introduire le sous-ensemble complémentaire

$$O^-(n) = O(n) \setminus SO(n) = \{M \in O(n) \mid \det(M) = -1\}.$$

Si E est un espace euclidien de dimension n, les matrices de $SO(n)$ et $O^-(n)$ représentent, dans toute base orthonormée, les isométries vectorielles de E respectivement dites *positives*, c'est-à-dire appartenant à l'ensemble $SO(E)$, et *négatives*, c'est-à-dire appartenant à l'ensemble $O^-(E) = O(E) \setminus SO(E)$. Il découle de la formule (5.1) que les isométries vectorielles positives préservent l'orientation.

5.5.1 Le groupe $O(2, \mathbb{R})$

On s'intéresse aux isométries vectorielles en dimension deux en considérant une matrice

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

appartenant au groupe $O(2, \mathbb{R})$. Puisque $M^\top M = I_2$, les coefficients de la matrice sont solution du système

$$\begin{cases} a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \\ ab + cd = 0 \end{cases}.$$

On en déduit qu'il existe des réels θ et φ, tous deux définis modulo 2π, tels que $a=\cos(\theta)$, $b=\cos(\varphi)$, $c=\sin(\theta)$, $d=\sin(\varphi)$ et $\cos(\theta)\cos(\varphi)+\sin(\theta)\sin(\varphi)=0$, soit encore $\cos(\theta-\varphi)=0$. Ceci signfie qu'il existe un réel ε valant ± 1 tel que $\varphi=\theta+\varepsilon\frac{\pi}{2}$ modulo 2π. Or, on a

$$\cos\left(\theta+\varepsilon\frac{\pi}{2}\right)=-\varepsilon\sin(\theta) \text{ et } \sin\left(\theta+\varepsilon\frac{\pi}{2}\right)=\varepsilon\cos(\theta),$$

et l'on conclut à l' existence d'un réel θ, défini modulo 2π, et d'un réel ε, prenant les valeurs ± 1, tels que

$$M=\begin{pmatrix}\cos(\theta) & -\varepsilon\sin(\theta)\\ \sin(\theta) & \varepsilon\cos(\theta)\end{pmatrix}.$$

On a alors $\det(M)=\varepsilon\left((\cos(\theta))^2+(\sin(\theta))^2\right)=\varepsilon$.

On vient de démontrer le résultat suivant.

Théorème 5.15 *Toute matrice de $SO(2,\mathbb{R})$ est de la forme*

$$\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}$$

pour un certain réel θ, défini modulo 2π. Toute matrice de $O^-(2,\mathbb{R})$ est de la forme

$$\begin{pmatrix}\cos(\theta) & \sin(\theta)\\ \sin(\theta) & -\cos(\theta)\end{pmatrix}$$

pour un certain réel θ, défini modulo 2π.

Lemme 5.16 *Le groupe $SO(2,\mathbb{R})$ est commutatif.*

DÉMONSTRATION. Soit M et N des matrices de $SO(2,\mathbb{R})$. En vertu du théorème 5.15, il existe des réels θ et θ' tels que

$$M=\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix} \text{ et } N=\begin{pmatrix}\cos(\theta') & -\sin(\theta')\\ \sin(\theta') & \cos(\theta')\end{pmatrix}.$$

En se servant des formules trigonométriques d'addition, il vient alors

$$\begin{aligned}MN&=\begin{pmatrix}\cos(\theta)\cos(\theta')-\sin(\theta)\sin(\theta') & -\cos(\theta)\sin(\theta')-\sin(\theta)\cos(\theta')\\ \sin(\theta)\cos(\theta')+\cos(\theta)\sin(\theta') & \cos(\theta)\cos(\theta')-\sin(\theta)\sin(\theta')\end{pmatrix}\\ &=\begin{pmatrix}\cos(\theta+\theta') & -\sin(\theta+\theta')\\ \sin(\theta+\theta') & \cos(\theta+\theta')\end{pmatrix}\\ &=NM.\end{aligned}$$

□

Corollaire 5.17 (classification des isométries vectorielles en dimension deux) *Soit E un espace euclidien orienté de dimension égale à 2 et u une isométrie vectorielle de E. Si u appartient à $SO(E)$, il existe un nombre réel θ, unique dans $]-\pi,\pi]$ modulo 2π, tel que la matrice représentative de u dans toute base orthonormale directe est de la forme*

$$Mat_{\mathscr{B}}(u)=\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}.$$

*On dit alors que u est une **rotation vectorielle** d'angle orienté de mesure θ. Si u appartient à $O^-(E)$, la matrice représentative de u dans une base orthonormale donnée est de la forme*

$$\begin{pmatrix}\cos(\theta) & \sin(\theta)\\ \sin(\theta) & -\cos(\theta)\end{pmatrix}$$

*avec θ un nombre réel unique modulo 2π. On dit alors que u est une **réflexion**, c'est-à-dire une symétrie orthogonale par rapport à une droite.*

DÉMONSTRATION. Soit u une isométrie vectorielle de $SO(E)$. On va tout d'abord montrer que la matrice représentative de u est indépendante de la base orthonormale directe choise. Soit $\mathscr{B}$ et $\mathscr{B}'$ deux bases orthonormales directes de E. Les matrices de u dans ces bases sont des éléments de $SO(2,\mathbb{R})$. C'est aussi le cas de la matrice de passage P de $\mathscr{B}$ à $\mathscr{B}'$. Par la formule changement de base, on a alors, en utilisant que le groupe $SO(2,\mathbb{R})$ est commutatif,

$$\mathrm{Mat}_{\mathscr{B}'}(u) = P^{-1}\mathrm{Mat}_{\mathscr{B}}(u)P = P^{\top}\mathrm{Mat}_{\mathscr{B}}(u)P = P^{\top}P\mathrm{Mat}_{\mathscr{B}}(u) = \mathrm{Mat}_{\mathscr{B}}(u).$$

On conclut en utilisant le théorème 5.15 et en observant que l'orientation du plan permet d'attibuer à l'angle de rotation une mesure dans l'intervalle $]-\pi,\pi]$ modulo 2π.

Soit à présent u une isométrie vectorielle de $O^{-}(E)$ et $\mathscr{B} = \{e_1, e_2\}$ une base orthonormale de E. En vertu du théorème 5.15, il existe un réel θ tel que la matrice de u dans la base $\mathscr{B}$ est de la forme donnée dans l'énoncé et l'on a $u(e_1) = \cos(\theta)\,e_1 + \sin(\theta)\,e_2$ et $u(e_2) = \sin(\theta)\,e_1 - \cos(\theta)\,e_2$. On pose alors $f_1 = \cos\left(\frac{\theta}{2}\right)e_1 + \sin\left(\frac{\theta}{2}\right)e_2$ et $f_2 = -\sin\left(\frac{\theta}{2}\right)e_1 + \cos\left(\frac{\theta}{2}\right)e_2$. Il est clair que la famille $\{f_1, f_2\}$ est une base orthonormale de E et l'on a

$$\begin{aligned} u(f_1) &= \left(\cos\left(\frac{\theta}{2}\right)\cos(\theta) + \sin\left(\frac{\theta}{2}\right)\sin(\theta)\right)e_1 + \left(\cos\left(\frac{\theta}{2}\right)\sin(\theta) - \sin\left(\frac{\theta}{2}\right)\cos(\theta)\right)e_2 \\ &= \cos\left(\theta - \frac{\theta}{2}\right)e_1 + \sin\left(\theta - \frac{\theta}{2}\right)e_2 = f_1 \end{aligned}$$

et

$$\begin{aligned} u(f_2) &= \left(-\sin\left(\frac{\theta}{2}\right)\cos(\theta) + \cos\left(\frac{\theta}{2}\right)\sin(\theta)\right)e_1 + \left(-\sin\left(\frac{\theta}{2}\right)\sin(\theta) - \cos\left(\frac{\theta}{2}\right)\cos(\theta)\right)e_2 \\ &= \sin\left(\theta - \frac{\theta}{2}\right)e_1 - \cos\left(\theta - \frac{\theta}{2}\right)e_2 = -f_2. \end{aligned}$$

La matrice de u dans la base $\{f_1, f_2\}$ est donc

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

ce qui signifie que l'isométrie vectorielle est la symétrie orthogonale par rapport à la droite vectorielle engendrée par le vecteur f_1. □

Remarque 5.18 *On peut interpréter géométriquement certains des résultats que l'on vient d'établir. Tout d'abord, la commutativité du groupe $SO(2,\mathbb{R})$ reflète le fait que deux rotations vectorielles commutent entre elles. D'autre part, l'indépendance de la matrice d'une rotation vectorielle, et donc de l'angle de rotation θ, par rapport au choix d'une base orthonormale directe signifie que cette rotation agit uniformément sur tous les vecteurs du plan, c'est-à-dire de la même manière dans toutes les directions. En revanche, l'angle θ apparaissant dans une matrice représentant une réflexion* dépend *de la base orthonormale (directe ou non) choisie et celui-ci n'est donc pas une caractéristique de l'endomorphisme comme il l'est pour une rotation.*

Dans le théorème 5.17, on a parlé d'« angle orienté de mesure θ » sans avoir défini cette notion. On peut la relier à celle d'écart angulaire, introduite dans la définition 4.13, en la résumant de la manière suivante.

Théorème 5.19 *Soit E un espace euclidien orienté de dimension égale à 2 et x et y deux vecteurs non nuls de E. Il existe une unique rotation vectorielle u, d'angle orienté de mesure θ, telle que*

$$\frac{y}{\|y\|} = u\left(\frac{x}{\|x\|}\right).$$

On alors $\cos(\theta) = \dfrac{\langle x, y\rangle}{\|x\|\|y\|}$.

DÉMONSTRATION. On pose $e_1 = \frac{x}{\|x\|}$ et on complète $\{e_1\}$ en une base orthonormale directe $\{e_1, e_2\}$ de E. On note (a_1, a_2) les coordonnées du vecteur $\frac{y}{\|y\|}$ dans cette base. On a en particulier que ${a_1}^2 + {a_2}^2 = 1$. Si u est la rotation vectorielle de matrice

$$\begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix}$$

dans la base $\{e_1, e_2\}$, on a le résultat voulu. On a par ailleurs unicité, car la forme d'une matrice de rotation dans une base orthonormale directe est telle qu'on a seulement besoin de connaître sa première colonne pour la connaître entièrement. Enfin, par définition de u et de θ, il vient

$$\frac{y}{\|y\|} = \cos(\theta)\, e_1 + \sin(\theta)\, e_2,$$

d'où

$$\langle x, y\rangle = \|x\|\|y\| \left\langle \frac{x}{\|x\|}, \frac{y}{\|y\|} \right\rangle = \|x\|\|y\| \,\langle e_1, \cos(\theta)\, e_1 + \sin(\theta)\, e_2\rangle = \|x\|\|y\| \cos(\theta).$$

□

5.5.2 Le groupe $O(3, \mathbb{R})$

Pour l'analyse de ce groupe, on aura besoin d'une opération propre aux espaces euclidiens orientés de dimension trois : le *produit vectoriel*.

Proposition et définition 5.20 (produit vectoriel) *Soit E un espace euclidien orienté de dimension égale à 3 et x et y deux vecteurs de E. Il existe un unique vecteur de E, noté $x \wedge y$ et appelé* ***produit vectoriel*** *de x et y, pour lequel*

$$\forall z \in E,\ [x, y, z] = \langle x \wedge y, z\rangle\,. \tag{5.2}$$

DÉMONSTRATION. On a déjà vu (voir le théorème 4.36) que l'application i_E de E dans E^* définie par

$$\forall (x, y) \in E^2,\ i_E(y)(x) = \langle x, y\rangle\,.$$

était un isomorphisme. À présent, pour tous vecteurs x et y de E, l'application $z \mapsto [x, y, z]$ est une forme linéaire sur E, qui possède par conséquent un unique antécédent par i_E, que l'on note $x \wedge y$. Par définition, le vecteur $x \wedge y$ est donc le seul vecteur de E tel que

$$\forall z \in E,\ [x, y, z] = i_E(x \wedge y)(z) = \langle z, x \wedge y\rangle\,.$$

□

Remarque 5.21 *Le symbole $\wedge$, ici utilisé pour noter le produit vectoriel, est généralement employé en France. Son inconvénient est d'entrer en conflit avec la notation du produit extérieur. Dans la littérature anglophone et allemande (ainsi qu'au Canada francophone, en Suisse, et parfois en Belgique), le produit vectoriel est noté avec le symbole $\times$. Cette notation est due à Josiah Willard Gibbs, à qui l'on doit l'introduction du produit vectoriel. Son inconvénient est d'induire une éventuelle confusion avec le produit de nombres réels ou le produit cartésien, ces derniers ne portant pas sur des objets de même nature.*

Proposition 5.22 (propriétés du produit vectoriel) *Soit E un espace euclidien orienté de dimension égale à 3 et x, y et z trois vecteurs de E. On a les propriétés suivantes.*

1. *Le vecteur $x \wedge y$ est orthogonal aux vecteurs x et y.*
2. *Le vecteur $x \wedge y$ est nul si et seulement si les vecteurs x et y sont colinéaires.*
3. *Le produit vectoriel est une application bilinéaire alternée de $E \times E$ dans E.*
4. *Si les vecteurs x et y ne sont pas colinéaires, la famille $\{x, y, x \wedge y\}$ est une base directe de E.*
5. *Si la famille $\{x, y\}$ est orthonormale, la famille $\{x, y, z\}$ est une base orthonormale directe de E si et seulement si $z = x \wedge y$.*
6. *Si $\mathscr{B}$ est une base orthonormale directe de E dans laquelle les vecteurs x et y ont pour coordonnées respectives (x_1, x_2, x_3) et (y_1, y_2, y_3), le vecteur $x \wedge y$ a pour coordonnées $(x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_3)$ dans cette même base.*

DÉMONSTRATION. Avant tout chose, on rappelle que tout produit mixte est un déterminant, qui est donc nul pour tout famille liée.

1. Les vecteurs $x \wedge y$ et x sont orthogonaux, car on a
$$\langle x \wedge y, x \rangle = [x, y, x] = 0.$$
Il en va de même pour $x \wedge y$ et y.
2. Si les vecteurs x et y sont colinéaires, toute famille les contenant est liée et l'on a donc
$$\|x \wedge y\|^2 = \langle x \wedge y, x \wedge y \rangle = [x, y, x \wedge y] = 0.$$
Réciproquement, on suppose que le vecteur $x \wedge y$ soit nul. La dimension du sous-espace vectoriel engendré par les vecteurs x et y étant inférieure ou égale à 2, il existe un vecteur z appartenant à $E \setminus \mathrm{Vect}(\{x, y\})$. La famille $\{x, y, z\}$ est alors liée, puisque $[x, y, z] = \langle x \wedge y, z \rangle = \langle 0_E, z \rangle = 0$. Le vecteur z n'étant pas combinaison linéaire de x et y, il en découle que la famille $\{x, y\}$ est liée.
3. D'après le point précédent, si le produit vectoriel est bilinéaire, il est aussi alterné. Il reste à montrer sa linéarité par rapport à la seconde variable. Pour tous vecteurs x, y et z de E et tout réel λ, on a
$$\begin{aligned} \forall x' \in E,\ \left\langle x \wedge (\lambda y + z) - \lambda(x \wedge y) - x \wedge z, x' \right\rangle &= \left\langle x \wedge (\lambda y + z), x' \right\rangle - \lambda \left\langle x \wedge y, x' \right\rangle - \left\langle x \wedge z, x' \right\rangle \\ &= [x, \lambda y + z, x'] - \lambda [x, y, x'] - [x, z, x'] \\ &= 0. \end{aligned}$$
Le vecteur $x \wedge (\lambda y + z) - \lambda(x \wedge y) - x \wedge z$ est ainsi orthogonal à tout vecteur de E et donc nul, d'où
$$\forall (x, y, z) \in E^3,\ \forall \lambda \in \mathbb{R},\ x \wedge (\lambda y + z) = \lambda(x \wedge y) + x \wedge z.$$
4. On suppose que les vecteurs x et y sont non colinéaires. Montrer que la famille $\{x, y, x \wedge y\}$ est une base directe de E équivaut à montrer que son déterminant dans une base directe de E est strictement positif, ce qui est le cas, puisque l'on a
$$[x, y, x \wedge y] = \langle x \wedge y, x \wedge y \rangle = \|x \wedge y\|^2 > 0.$$
5. On suppose que la famille $\{x, y\}$ soit orthonormale. La famille $\left\{x, y, \frac{x \wedge y}{\|x \wedge y\|}\right\}$ est alors une base orthogonale directe d'après les premier et quatrième points de la proposition. Par ailleurs, on a
$$\|x \wedge y\| = \left\langle x \wedge y, \frac{x \wedge y}{\|x \wedge y\|} \right\rangle = \left[x, y, \frac{x \wedge y}{\|x \wedge y\|} \right] = 1.$$
Réciproquement, on suppose que la famille $\{x, y, z\}$ soit une base orthonormale directe de E. Le sous-espace vectoriel engendré par les vecteurs x et y étant de dimension égale à 2, son orthogonal est une droite vectorielle contenant à la fois z et $x \wedge y$, d'où $x \wedge y = \lambda z$ pour un certain réel λ. On a alors
$$\lambda = \langle \lambda z, z \rangle = \langle x \wedge y, z \rangle = [x, y, z] = 1.$$
6. On note e_1, e_2 et e_3 les vecteurs de la base $\mathscr{B}$. Les coordonnées du vecteur $x \wedge y$ dans la base $\mathscr{B}$ sont alors données par $(\langle x \wedge y, e_1 \rangle, \langle x \wedge y, e_2 \rangle, \langle x \wedge y, e_3 \rangle)$. On a
$$\langle x \wedge y, e_1 \rangle = [x, y, e_1] = \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 0 \\ x_3 & y_3 & 0 \end{vmatrix} = x_2 y_3 - x_3 y_2,$$
et il en va de même pour les coordonnées restantes.

□

Remarque 5.23 *On peut interpréter géométriquement l'égalité* (5.2) *définissant le produit vectoriel. En supposant que les vecteur $x \wedge y$ est non nul, on sait déjà (voir la remarque 5.13) que le produit mixte $[x, y, z]$ dans le membre de gauche correspond au volume algébrique du parallélépipède engendré par les vecteurs x, y et z. Dans le membre de droite, on voit, en écrivant $\langle x \wedge y, z \rangle = \|x \wedge y\| \left\langle \frac{x \wedge y}{\|x \wedge y\|}, z \right\rangle$, que le nombre réel $\left\langle \frac{x \wedge y}{\|x \wedge y\|}, z \right\rangle$ n'est autre que la hauteur (algébrique) du parallélépipède au-dessus du parallélogramme engendré par x et y. Ainsi, $\|x \wedge y\|$ correspond à la valeur de l'aire parallélogramme engendré par x et y.*

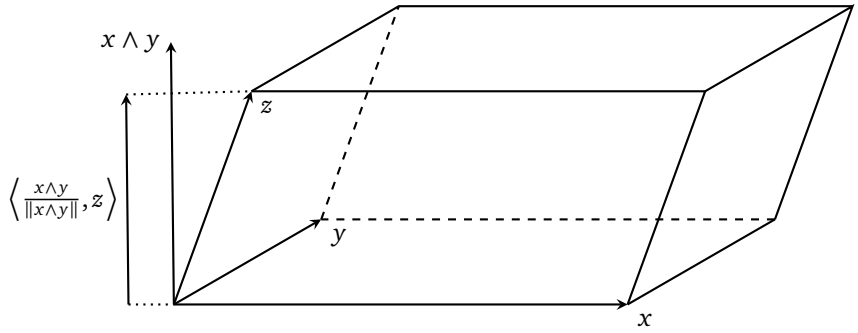

FIGURE 5.1 – Interprétation géométrique du produit vectoriel de deux vecteurs x et y.

Nous sommes à présent en mesure de réaliser l'étude des isométries vectorielles en dimension trois.

Théorème 5.24 (classification des isométries vectorielles en dimension trois) *Soit E un espace euclidien orienté de dimension égale à 3 et u une isométrie vectorielle de E. Il existe une base orthonormale directe $\mathscr{B}$ de E et un réel θ, défini modulo 2π, tels que*

$$Mat_{\mathscr{B}}(u) = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Par conséquent, une isométrie vectorielle u est :

- *une rotation vectorielle si son déterminant vaut 1,*
- *une* ***antirotation*** [1]*, c'est-à-dire la composée commutative d'une rotation vectorielle et de la symétrie orthogonale (ou réflexion) par rapport au plan orthogonal à l'axe de rotation, si son déterminant vaut -1.*

La mesure de l'angle orienté de rotation est fixée par l'orientation du plan orthogonal à l'axe de rotation, celle-ci étant donnée par l'orientation de l'espace et le choix d'un vecteur directeur de l'axe.

DÉMONSTRATION. On suppose tout d'abord que l'isométrie vectorielle u appartient à $SO(E)$ et on considère l'application φ de $\mathbb{R}$ dans lui-même définie par $\varphi(t) = \det(u - t\, id_E)$. Quelle que soit la base choisie pour le calcul de ce déterminant, l'application est une fonction polynomiale de degré 3 de coefficient de terme de plus haut degré égal à -1, valant $\det(u) = 1$ en $t = 0$. Cette fonction étant continue et tendant vers $-\infty$ en $+\infty$, le théorème des valeurs intermédiaires assure l'existence d'un réel λ strictement positif tel que $\varphi(\lambda) = 0$. Le réel λ est une valeur propre de u et il existe donc un vecteur x non nul de E tel que $u(x) = \lambda\, x$. L'endomorphisme u étant une isométrie vectorielle, on a nécessairement $|\lambda| = 1$ et, par suite, $\lambda = 1$. Par ailleurs, le sous-espace vectoriel engendré par le vecteur x étant stable par u, son orthogonal $H = \{x\}^{\perp}$ l'est également (voir la proposition 4.51) et la restriction u à H est un endomorphisme orthogonal de H.

Soit $\{e_2, e_3\}$ une base orthonormale de H et soit

$$R = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

la matrice de $u_{|_H}$ dans cette base ; on sait que R appartient à $O(2, \mathbb{R})$. En posant $e_1 = \frac{x}{\|x\|}$ et $\mathscr{B} = \{e_1, e_2, e_3\}$, il vient alors

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}.$$

Puisque $\det(u) = 1$, on a $\det(R) = 1$ et la matrice R appartient à $SO(2, \mathbb{R})$, ce qui impose sa forme et fixe le signe de l'angle de rotation orienté si la base $\mathscr{B}$ ainsi construite est orthonormale directe. Si ce n'est pas le cas, il suffit de remplacer dans $\mathscr{B}$ le vecteur e_1 par son opposé.

On suppose à présent que u appartient à $O^-(E)$. Par des arguments similaires à ceux employés ci-dessus, on peut montrer que -1 est valeur propre de l'application u. On note x un vecteur propre associé. Par des considérations

1. On parle aussi de *rotation impropre*, de *roto-réflexion* ou de *rotation-réflexion*.

de signe du déterminant, la restriction u à $H = \{x\}^\perp$ appartient alors à $SO(E)$. En se plaçant dans une base orthonormale directe $\mathscr{B} = \{e_1, e_2, e_3\}$ de E telle que $e_1 = \frac{x}{\|x\|}$, on a

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix},$$

pour un certain réel θ appartenant à $]-\pi, \pi]$ modulo 2π.
Si $\theta = 0$, l'application u est simplement une réflexion par rapport au plan $H = \{x\}^\perp$. Si $\theta = \pi$, alors $u = -id_E$. Sinon, on a

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix},$$

l'isométrie vectorielle étant alors la composée de la réflexion par rapport au plan $H = \{x\}^\perp$ et de la rotation d'axe dirigé et orienté par le vecteur x et d'angle θ. □

Caractérisation géométrique d'une isométrie vectorielle en dimension trois

Soit M une matrice orthogonale d'ordre 3 représentant une isométrie vectoriel dans une base orthonormée de l'espace. On va caractériser géométriquement l'endomorphisme canoniquement associé à M.

On détermine tout si la matrice appartient à $SO(3,\mathbb{R})$ ou à $O^-(3,\mathbb{R})$. Pour cela, on n'a besion d'évaluer son déterminant : il suffit en effet de calculer le produit vectoriel des deux premières colonnes de M, qui sera égal à la troisième colonne de M si la matrice appartient à $SO(3,\mathbb{R})$ ou à son opposée si la matrice appartient à $O^-(3,\mathbb{R})$ (le signe de la première composante du produit vectoriel permet d'ailleurs de conclure si elle est non nulle). On procède alors de manière distincte suivant le cas qui se présente.

- Si M appartient à $SO(3,\mathbb{R})$, c'est la matrice d'une rotation vectorielle. On trouve son axe de rotation en déterminant le sous-espace vectoriel invariant $\ker(M - I_3)$ et une mesure θ de son angle non orienté à l'aide de sa trace (puisque $\mathrm{tr}(M) = 1 + 2\cos(\theta)$). On oriente ensuite l'axe en faisant le choix d'un vecteur directeur U_1 et l'on détermine le signe de θ (à valeurs dans $]-\pi, \pi]$ modulo 2π), en faisant le choix d'un vecteur U_2 non colinéaire à U_1 et en regardant le signe du produit mixte entre U_1, U_2 et MU_2.
- Si M appartient à $O^-(3,\mathbb{R})$, on reconnaît facilement les cas $M = -I_3$ ($\theta = \pi$) ou celui d'une réflexion ($\theta = 0$), puisque M est alors symétrique. Dans ce dernier cas, on trouve l'hyperplan de la réflexion en déterminant $\ker(M - I_3)$. Sinon on a affaire à une antirotation non triviale. On trouve son axe de rotation (et par conséquent le plan de réflexion, puisqu'il lui est orthogonale) en déterminant $\ker(M + I_3)$. On obtient enfin la mesure de l'angle de rotation orienté en adaptant la procédure suivie dans le cas d'une rotation vectorielle.

Exemple 5.25 *On considère tout d'abord la matrice orthogonale d'ordre* 3

$$M = \frac{1}{4}\begin{pmatrix} 3 & 1 & \sqrt{6} \\ 1 & 3 & -\sqrt{6} \\ -\sqrt{6} & \sqrt{6} & 2 \end{pmatrix}.$$

La première composante du produit vectoriel des deux premières colonnes de M vaut $\frac{1}{4}\left(\sqrt{6} - (-3\sqrt{6})\right) = \sqrt{6}$*, on en déduit que* $\det(M) = 1$ *et l'endomorphisme canoniquement associé à M est une rotation vectorielle. On trouve son axe de rotation en déterminant* $\ker(M - I_3)$*. On a*

$$X \in \ker(M - I_3) \iff \begin{cases} x_1 - x_2 - \sqrt{6}x_3 = 0 \\ -\sqrt{6}x_1 + \sqrt{6}x_2 - 2x_3 = 0 \end{cases} \iff x_1 = x_2 \text{ et } x_3 = 0,$$

et l'axe de rotation est engendré par le vecteur $(1,1,0)$*. La trace de M est égale à* 2*, d'où la mesure* θ *de l'angle orienté*

de rotation est telle que $\cos(\theta)=\frac{1}{2}$ *et donc* θ *est égal à* $\frac{\pi}{3}$ *ou à* $-\frac{\pi}{3}$ *modulo* 2π*. Enfin, on a*

$$\left\langle M\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix}\wedge\begin{pmatrix}1\\0\\0\end{pmatrix}\right\rangle=\left\langle\frac{1}{4}\begin{pmatrix}3\\1\\-\sqrt{6}\end{pmatrix},\begin{pmatrix}0\\0\\-1\end{pmatrix}\right\rangle=\frac{\sqrt{6}}{4},$$

d'où $\theta=\frac{\pi}{3}$ *modulo* 2π*.*

On considère ensuite la matrice orthogonale d'ordre 3

$$N=-\frac{1}{3}\begin{pmatrix}-2&-1&2\\2&-2&1\\1&2&2\end{pmatrix}.$$

La première composante du produit vectoriel des deux premières colonnes de N *vaut* $-\frac{1}{3}(4-(-2))=-2$*, on en déduit que* $\det(N)=-1$ *et l'endomorphisme canoniquement associé à* N *est la composée commutative d'une rotation vectorielle et d'une réflexion par rapport au plan orthogonal à l'axe de rotation. On trouve cet axe en déterminant* $\ker(N+I_3)$*. On a*

$$X\in\ker(N+I_3)\iff\begin{cases}-5x_1-x_2-2x_3=0\\2x_1-5x_2+x_3=0\\x_1+2x_2-x_3=0\end{cases}\iff x_1=x_2\text{ et }x_3=3x_1,$$

et l'axe de rotation est engendré par le vecteur $(1,1,3)$*. La trace de* N *est égale à* $\frac{2}{3}$*, d'où la mesure* θ *de l'angle orienté de rotation est telle que* $\cos(\theta)=\frac{5}{6}$ *et donc* θ *est égal à* $\arccos\left(\frac{5}{6}\right)$ *ou à* $-\arccos\left(\frac{5}{6}\right)$ *modulo* 2π*. Enfin, on a*

$$\left\langle N\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\3\end{pmatrix}\wedge\begin{pmatrix}1\\0\\0\end{pmatrix}\right\rangle=\left\langle-\frac{1}{3}\begin{pmatrix}-2\\2\\1\end{pmatrix},\begin{pmatrix}0\\3\\-1\end{pmatrix}\right\rangle=-\frac{5}{3},$$

d'où $\theta=-\arccos\left(\frac{5}{6}\right)$ *modulo* 2π*.*

5.5.3 Réduction des isométries vectorielles

On termine cette section avec un résultat général de réduction des isométries vectorielles.

Théorème 5.26 (réduction d'une isométrie orthogonal) *Soit* E *un espace euclidien de dimension* n *non nulle et* u *une isométrie vectorielle de* E*. Il existe une base orthonormale de* E *dans laquelle la matrice de* u *a la forme*

$$\begin{pmatrix}I_p&&&&\\&-I_q&&&\\&&R_1&&\\&&&\ddots&\\&&&&R_r\end{pmatrix}$$

où p*,* q *et* r *sont des entiels naturels tels que* $p+q+2r=n$ *(si l'un des entiers est nul, le (ou les) bloc(s) correspondant(s) n'existe(nt) pas) et où*

$$\forall i\in\{1,\dots,r\},\ R_i=\begin{pmatrix}\cos(\theta_i)&-\sin(\theta_i)\\\sin(\theta_i)&\cos(\theta_i)\end{pmatrix}\text{ avec }\theta_i\text{ un nombre réel défini modulo }2\pi.\tag{5.3}$$

DÉMONSTRATION. La preuve se fait en raisonnant par récurrence sur la dimension de l'espace. Pour $n=1$, il n'y a rien à montrer. Le résultat a déjà été démontré pour $n=2$ (voir le théorème 5.17) et $n=3$ (voir le théorème 5.24). On suppose à présent que l'entier n est supérieur ou égal à 4 et que le résultat est vrai pour toute isométrie vectorielle d'un espace euclidien de dimension inférieure ou égale à $n-1$.

Si l'isométrie vectorielle u admet 1 ou -1 comme valeur propre, alors, pour tout vecteur propre unitaire e_1 associé à cette valeur propre, le sous-espace vectoriel $H = \{e_1\}^\perp$ est stable par u et il existe une base orthonormée $\mathscr{B}_H$ de H dans laquelle la matrice de la restriction de u à H est de la forme voulue. Dans la base orthonormale $\{e_1\} \cup \mathscr{B}_H$, la matrice de u est alors de la forme

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \mathrm{Mat}_{\mathscr{B}_H}(u_{|_H}) \end{pmatrix},$$

qui, en échangeant au besoin le vecteur e_1 avec l'un de ceux de $\mathscr{B}_H$, est bien celle souhaitée.

Si toutes les valeurs propres de u sont complexes non réelles, on a la décomposition $E = \bigoplus_{i=1}^{r} V_i$, où les sous-espaces vectoriels $V_1, \dots, V_r$ sont de dimension égale à 2, deux à deux orthogonaux et stables par u. L'étude du cas $n = 2$ montre alors que, pour chaque entier i de $\{1, \dots, r\}$, il existe une base orthonormale de $\mathscr{B}_i$ de V_i dans laquelle la matrice de la restriction de u à V_i est de la forme (5.3). En concaténant l'ensemble de ces bases, on obtient une base orthonormée de E dans laquelle la matrice de u est

$$\begin{pmatrix} R_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & R_r \end{pmatrix}.$$

□

On peut observer qu'on a $p = \dim(\ker(u - id_E))$ et $q = \dim(\ker(u + id_E))$. De plus, on a que u appartient à $SO(E)$ (resp. à $O^-(E)$) si et seulement si q est pair (resp. impair).

Annexe A

Rappels d'algèbre

On rappelle dans cette annexe un certain nombre de définitions et de résultats d'algèbre linéaire en dimension finie et de calcul matricielle. Tout comme dans le reste du document, on désigne par $\mathbb{N}$ l'ensemble des nombres entiers naturels, par $\mathbb{Z}$ l'ensemble des nombres entiers relatifs et par $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{Q} = \{\frac{p}{q} \,|\, p \in \mathbb{Z},\ q \in \mathbb{Z} \setminus \{0\}\}$, par $\mathbb{R}$ l'ensemble des nombres réels et par $\mathbb{C}$ l'ensemble des nombres complexes.

A.1 Ensembles et applications

On commence par des notions relatives aux ensembles et aux applications, en adoptant le point de vue de la théorie *naïve* des ensembles.

A.1.1 Généralités sur les ensembles

En mathématiques, on étudie des objets de différents types : des nombres, des points ou encore des vecteurs par exemple. Ces *éléments* forment, en vertu de certaines propriétés, des collections appelées *ensembles*. Dans la suite, on désignera généralement un élément par une lettre minuscule (l'élément x par exemple) et un ensemble par une lettre majuscule (l'ensemble E par exemple). L'*appartenance* d'un élément à un ensemble est par ailleurs notée avec le symbole $\in$ (on a ainsi $x \in E$) et la *non-appartenance* par $\notin$.

Un ensemble peut être *fini* ou *infini*, selon que le nombre d'éléments qui le constituent est fini ou infini (voir la sous-section A.1.4). S'il est fini, il peut être donné en *extension*, c'est-à-dire par la liste (non ordonnée) de ses éléments, *a priori* supposés distincts. S'il est infini (ou même fini), l'ensemble peut être donné en *compréhension*, c'est-à-dire par une ou des propriétés caractérisant ses éléments.

Un cas particulier d'ensemble fini est le *singleton*, qui est formé d'un unique élément. Si cet élément est noté x, on désigne l'ensemble par $\{x\}$.

Une première notion essentielle est la relation d'**égalité** entre ensembles.

Définition A.1 (égalité entre ensembles) *On dit qu'un ensemble E est **égal à** un ensemble F, et l'on note $E = F$, si tout élément de E est un élément de F et si tout élément de F est un élément de E. Lorsque les ensembles E et F ne sont pas égaux, ils sont dits **distincts** et l'on note $E \neq F$.*

Une autre notion importante, la relation d'**inclusion**, se définit de la manière suivante.

Définition A.2 (inclusion entre ensembles) *On dit qu'un ensemble E est **inclus** dans un ensemble F, ce que l'on note $E \subset F$, si et seulement si tout élément de E appartient à F,*

$$E \subset F \iff (\forall x \in E,\ x \in F).$$

L'inclusion d'un ensemble E dans un ensemble F peut encore se noter $F \supset E$ tandis que la négation de cette relation se note $E \not\subset F$. Pour tout ensemble E, on a $E \subset E$, et si E, F et G trois ensembles tels que $E \subset F$ et $F \subset G$, alors $E \subset G$. On dit que l'inclusion est une relation *transitive* (voir la sous-section A.1.2).

Le résultat suivant est immédiat. Il permet de démontrer l'égalité entre deux ensembles par un principe de double inclusion.

Proposition A.3 *Étant donné deux ensembles E et F, on a $E = F$ si et seulement si l'on a simultanément $E \subset F$ et $F \subset E$.*

Définition A.4 (partie d'un ensemble) *Soit E un ensemble. On appelle **partie** (ou **sous-ensemble**) de E tout ensemble A vérifiant $A \subset E$.*

On nomme **ensemble vide**, et l'on note $\varnothing$, l'ensemble n'ayant aucun élément. C'est[1] une partie de tout ensemble E.

Lorsque $E \subset F$ et qu'il existe au moins un élément de F qui n'appartient pas à E, on dit que E est un sous-ensemble *propre* de F, ce qu'on note encore $E \subsetneq F$.

Toutes les parties d'un ensemble E constituent un nouvel ensemble, noté $\mathscr{P}(E)$, que l'on nomme **ensemble des parties de** E. Pour tout ensemble E, E et $\varnothing$ appartiennent à $\mathscr{P}(E)$.

On introduit à présent des opérations sur les parties d'un ensemble, en commençant par définir deux *lois de composition internes* (voirla sous-section A.2.1) dans l'ensemble de ses parties.

Définition A.5 (intersection d'ensembles) *Soit E un ensemble et A et B deux parties de E. On appelle **intersection des ensembles** A **et** B l'ensemble des éléments qui appartiennent à la fois à A et à B. On le note noté $A \cap B$. Lorsque $A \cap B = \varnothing$ (c'est-à-dire lorsque A et B n'ont aucun élément commun), on dit que A et B sont **disjoints**.*

Définition A.6 (réunion d'ensembles) *Soit E un ensemble et A et B deux parties de E. On appelle **réunion des ensembles** A **et** B l'ensemble des éléments qui appartiennent à A ou à B. Cet ensemble est noté $A \cup B$.*

Soit A, B et C trois sous-ensembles d'un ensemble E. L'intersection et la réunion d'ensembles sont des lois *commutatives*,

$$A \cap B = B \cap A,\ A \cup B = B \cup A,$$

et *associatives*,

$$A \cup (B \cup C) = (A \cup B) \cup C,\ A \cap (B \cap C) = (A \cap B) \cap C.$$

Elles sont également *distributives* l'une pour l'autre,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Pour prouver ces propriétés, on fait appel aux *tableaux de vérité* et aux *synonymies* utilisés en logique. Si l'on définit la proposition $(P(x))$ (resp. $(Q(x))$, resp. $(R(x))$) comme étant vraie si et seulement si $x \in A$ (resp. $x \in B$, resp. $x \in C$), la proposition $x \in B \cap C$ est alors équivalente à $(P(x)$ et $Q(x))$ et $x \in B \cup C$ à $(P(x)$ ou $Q(x))$. Ainsi, $x \in A \cup (B \cap C)$ est équivalente à $(P(x)$ ou $(Q(x)$ et $R(x)))$, ce qui est équivalent à $((P(x)$ ou $Q(x))$ et $(P(x)$ ou $R(x)))$, ou encore à $x \in (A \cup B) \cap (A \cup C)$. On procède de manière identique pour démontrer les autres assertions.

Définition A.7 (partition d'un ensemble) *Soit E un ensemble et $\mathscr{P}$ une partie de $\mathscr{P}(E)$. On dit que $\mathscr{P}$ est une **partition de** E si et seulement si*

- $\forall A \in \mathscr{P},\ A \neq \varnothing$ *(aucune des parties n'est vide),*
- $\forall A \in \mathscr{P},\ \forall B \in \mathscr{P},\ (A \neq B \iff A \cap B = \varnothing)$ *(les parties sont deux à deux disjointes),*
- $\forall x \in E,\ \exists A \in \mathscr{P},\ x \in A$ *(l'union des parties est égale à E).*

On continue avec les notions de *différence* d'ensembles et de *complémentaire* d'une partie d'un ensemble.

Définition A.8 (différence de deux ensembles) *Soit A et B deux parties d'un ensemble E. On appelle **différence de** A **et de** B, et on note $A \setminus B$, l'ensemble des éléments de E appartenant à A mais pas à B.*

Définition A.9 (complémentaire d'une partie) *Soit A une partie d'un ensemble E. On appelle **complémentaire de** A **dans** E, et l'on note $E \setminus A$, l'ensemble des éléments de E qui n'appartiennent pas à A.*

Les démonstrations des propriétés suivantes sont laissées en exercice au lecteur. Soit A et B deux parties d'un ensemble E. On a

- $A \cap \varnothing = \varnothing$, $A \cap A = A$, $A \cap E = A$ (on dit que E est l'*élément neutre* pour $\cap$), $A \cap B = B \iff A \subset B$,

1. En effet, si cela n'était pas le cas, il existerait au moins un élément appartenant à $\varnothing$ qui n'appartiendrait pas à E. Or, ceci est impossible, puisque l'ensemble vide n'a pas d'élément. L'assertion $\varnothing \subset E$ est donc vraie.

- $A \cup \varnothing = A$ (on dit que $\varnothing$ est l'*élément neutre* pour $\cup$), $A \cup A = A$, $A \cup E = E$, $A \cup B = B \iff A \subset B$,
- $A \cap (A \cup B) = A \cup (A \cap B) = A$,
- $E \setminus \varnothing = E$, $E \setminus E = \varnothing$, $E \setminus (E \setminus A) = A$, $A \cap E \setminus A = \varnothing$, $A \cup E \setminus A = E$ (on déduit de ces deux dernières égalités que $\{A, E \setminus A\}$ est une partition de E),
- $E \setminus (A \cap B) = E \setminus A \cup (E \setminus B)$, $E \setminus (A \cup B) = E \setminus A \cap (E \setminus B)$ (ce sont les *lois de De Morgan*),
- $E \setminus A = E \setminus A$, $A \setminus B = \varnothing \iff A \subset B$, $A \setminus B = A \cap (E \setminus B) = A \setminus (A \cap B)$.

Étant donnés deux ensembles E et F, on peut associer à tous éléments x de E et y de F le couple ordonné (x, y). Ce couple est lui-même un élément d'un ensemble, que l'on définit ci-après.

Définition A.10 (ensemble produit) *Soit E et F deux ensembles. On appelle **ensemble produit de E par F**, et l'on note $E \times F$, l'ensemble défini par*

$$E \times F = \{(x, y) \mid x \in E \text{ et } y \in F\}.$$

L'ensemble produit de deux ensembles est encore appelé *produit cartésien*, en hommage à Descartes qui généralisa l'usage des coordonnées en posant les bases de la géométrie analytique. L'égalité entre couples d'un même ensemble produit est définie par l'équivalence logique suivante

$$(a, b) = (c, d) \iff (a = c \text{ et } b = d).$$

Lorsque $E = F$, on a coutume d'écrire E^2 pour l'ensemble produit $E \times F$. Par extension, étant donnés un entier naturel non nul n et des ensembles $E_1, \ldots, E_n$, on appelle *produit de $E_1, \ldots, E_n$* l'ensemble de tous les *n-uplets* $(x_1, \ldots, x_n)$ tels que x_1 appartient à E_1,..., x_n appartient à E_n, que l'on note $E_1 \times \cdots \times E_n$, ou encore $\prod_{i=1}^{n} E_i$. Lorsque $E_1 = \cdots = E_n = E$, l'ensemble produit résultant est noté E^n.

A.1.2 Relations

On va à présent formaliser et généraliser la notion de relation précédemment introduite avec l'inclusion.

Définitions A.11 *Soit E et F deux ensembles non vides. Une **relation binaire $\mathscr{R}$ de E vers F** (**dans** E lorsque $E = F$) est définie par une partie R de l'ensemble produit $E \times F$, appelée **graphe** de la relation. Pour tout couple (x, y) appartenant à R, on dit que l'élément x de E est **en relation par $\mathscr{R}$** avec l'élément y de F, ce que l'on note encore $x \mathscr{R} y$. Enfin, l'**ensemble de définition** de la relation $\mathscr{R}$ est la partie de E définie par*

$$\{x \in E \mid \exists y \in F,\ x \mathscr{R} y\}$$

*et son **ensemble image** est la partie de F définie par*

$$\{y \in F \mid \exists x \in E,\ x \mathscr{R} y\}.$$

On remarque que l'on n'utilise généralement pas une notation ensembliste pour décrire une relation binaire, mais plutôt l'écriture $x \mathscr{R} y$, introduite avec les dernières définitions.

Définition A.12 (relation composée) *Soit E, F et G trois ensembles non vides, $\mathscr{R}$ (resp. $\mathscr{S}$) une relation de E vers F (resp. de F vers G). On définit la **relation composée de $\mathscr{S}$ avec $\mathscr{R}$**, notée $\mathscr{S} \circ \mathscr{R}$, de E vers G par*

$$\forall (x, z) \in E \times G,\ (x \mathscr{S} \circ \mathscr{R} z \iff (\exists y \in F,\ x \mathscr{R} y \text{ et } y \mathscr{S} z)).$$

On a le résultat d'associativité suivant.

Proposition A.13 *Soit E, F, G et H des ensembles non vides et $\mathscr{R}$, $\mathscr{S}$ et $\mathscr{T}$ des relations, respectivement de E vers F, de F vers G et de G vers H. On a*

$$(\mathscr{T} \circ \mathscr{S}) \circ \mathscr{R} = \mathscr{T} \circ (\mathscr{S} \circ \mathscr{R}).$$

DÉMONSTRATION. On remarque tout d'abord que les relations $(\mathscr{T} \circ \mathscr{S}) \circ \mathscr{R}$ et $\mathscr{T} \circ (\mathscr{S} \circ \mathscr{R})$ ont les mêmes ensembles de départ (E) et d'arrivée (H). Pour tout couple (x, t) de $E \times H$, on a alors

$$\begin{aligned}
x (\mathscr{T} \circ \mathscr{S}) \circ \mathscr{R} t &\iff (\exists y \in F,\ (x \mathscr{R} y \text{ et } y \mathscr{T} \circ \mathscr{S} t)) \\
&\iff (\exists y \in F,\ \exists z \in G,\ (x \mathscr{R} y \text{ et } y \mathscr{S} z \text{ et } z \mathscr{T} t)) \\
&\iff (\exists z \in G,\ (x \mathscr{S} \circ \mathscr{R} z \text{ et } z \mathscr{T} t)) \\
&\iff x \mathscr{T} \circ (\mathscr{S} \circ \mathscr{R}) t.
\end{aligned}$$

□

Définition A.14 (relation réciproque) *Soit E et F deux ensembles non vides et $\mathscr{R}$ une relation de E vers F. On définit la* ***relation réciproque de*** *$\mathscr{R}$, notée $\mathscr{R}^{-1}$, de F vers E par*

$$\forall (x,y) \in E \times F,\ (y \mathscr{R}^{-1} x \iff x \mathscr{R} y).$$

Proposition A.15 *On a les assertions suivantes.*

1. *Pour toute relation $\mathscr{R}$, on a $(\mathscr{R}^{-1})^{-1} = \mathscr{R}$.*
2. *Soit E, F, G trois ensembles et $\mathscr{R}$ (resp. $\mathscr{S}$) une relation de E vers F (resp. de F vers G). On a $(\mathscr{S} \circ \mathscr{R})^{-1} = \mathscr{R}^{-1} \circ \mathscr{S}^{-1}$.*

DÉMONSTRATION.

1. C'est immédiat.
2. On a, pour tout couple (x,z) de $E \times G$,

$$z(\mathscr{S} \circ \mathscr{R})^{-1} x \iff x(\mathscr{S} \circ \mathscr{R}) z \iff (\exists y \in F,\ (x \mathscr{R} y \text{ et } y \mathscr{S} z))$$
$$\iff (\exists y \in F,\ (z \mathscr{S}^{-1} y \text{ et } y \mathscr{R}^{-1} x)) \iff z \mathscr{R}^{-1} \circ \mathscr{S}^{-1} x.$$

□

Définitions A.16 *Une relation binaire $\mathscr{R}$ dans un ensemble E est dite*

- ***réflexive*** *si et seulement si*
$$\forall x \in E,\ x \mathscr{R} x,$$
- ***symétrique*** *si et seulement si*
$$\forall (x,y) \in E^2,\ (x \mathscr{R} y \implies y \mathscr{R} x),$$
- ***antisymétrique*** *si et seulement si*
$$\forall (x,y) \in E^2,\ ((x \mathscr{R} y \text{ et } y \mathscr{R} x) \implies x = y),$$
- ***transitive*** *si et seulement si*
$$\forall (x,y,z) \in E^3,\ ((x \mathscr{R} y \text{ et } y \mathscr{R} z) \implies x \mathscr{R} z).$$

Définition A.17 (relation induite) *Soit E un ensemble, $\mathscr{R}$ une relation binaire sur E et A une partie de E. La relation binaire dans A, notée $\mathscr{R}_A$, définie par*

$$\forall (x,y) \in A^2,\ (x \mathscr{R}_A y \iff x \mathscr{R} y),$$

est appelée ***relation induite par $\mathscr{R}$ sur*** *A.*

Définition A.18 (relation d'équivalence) *Soit $\mathscr{R}$ une relation binaire dans un ensemble E. On dit que $\mathscr{R}$ est une* ***relation d'équivalence*** *si et seulement si elle est réflexive, symétrique et transitive.*

Étant donnée une relation d'équivalence, on identifie les éléments qui sont en relation en introduisant le concept de *classe d'équivalence*.

Définitions A.19 (classe d'équivalence et ensemble quotient) *Soit $\mathscr{R}$ une relation d'équivalence dans un ensemble E. Pour chaque élément x de E, on appelle* ***classe d'équivalence de*** *x* ***(modulo $\mathscr{R}$)*** *le sous-ensemble de E défini par $\mathscr{C}(x) = \{y \in E \mid x \mathscr{R} y\}$. Tout élément de $\mathscr{C}(x)$ est appelé un* ***représentant de la classe*** *$\mathscr{C}(x)$. L'ensemble des classes d'équivalence modulo $\mathscr{R}$ se nomme* ***ensemble quotient de*** *E* ***par*** *$\mathscr{R}$ et se note $E/\mathscr{R}$.*

Théorème A.20 *À toute relation d'équivalence $\mathscr{R}$ dans un ensemble E correspond une partition de E en classes d'équivalence et réciproquement, toute partition de E définit sur E une relation d'équivalence $\mathscr{R}$, dont les classes coïncident avec les éléments de la partition donnée.*

DÉMONSTRATION. Soit $\mathscr{R}$ une relation d'équivalence dans E. Pour tout élément x de E, l'ensemble $\mathscr{C}(x)$ est non vide car il contient x. Soit un couple (x,y) de E^2 tel que $\mathscr{C}(x)\cap\mathscr{C}(y)\neq\emptyset$; il existe donc un élément z dans $\mathscr{C}(x)\cap\mathscr{C}(y)$. On a alors $x\mathscr{R}z$ et $y\mathscr{R}z$, d'où $x\mathscr{R}y$ (par symétrie et transitivité de la relation). On en déduit que $\mathscr{C}(x)$ est inclus dans $\mathscr{C}(y)$. Soit en effet un élément t de $\mathscr{C}(x)$, on a $x\mathscr{R}t$ et $x\mathscr{R}y$, d'où $y\mathscr{R}t$, et t appartient à $\mathscr{C}(y)$. Les éléments x et y jouant des rôles symétriques, on a l'égalité $\mathscr{C}(x)=\mathscr{C}(y)$. Puisque chaque élément x de E appartient à $\mathscr{C}(x)$, la réunion des éléments de $E/\mathscr{R}$ est E et l'on a montré la première partie du théorème.

Soit à présent $\mathscr{P}$ une partition de E. On note $\mathscr{R}$ la relation définie dans E par

$$\forall(x,y)\in E^2,\ (x\mathscr{R}y \iff (\exists A\in\mathscr{P},\ (x\in A \text{ et } y\in A))).$$

Par définition, il existe, pour chaque x de E, un élément A de $\mathscr{P}$ auquel x appartient, on a donc $x\mathscr{R}x$. Lla relation $\mathscr{R}$ est réflexive.

Pour tout couple (x,y) de E^2, on a

$$x\mathscr{R}y \iff (\exists P\in\mathscr{P},\ (x\in P \text{ et } y\in P)) \iff (\exists P\in\mathscr{P},\ (y\in P \text{ et } x\in P)) \iff y\mathscr{R}x,$$

et la relation $\mathscr{R}$ est symétrique.

Soit (x,y,z) un triplet d'éléments de E tels que $x\mathscr{R}y$ et $y\mathscr{R}z$. Il existe alors A et B dans $\mathscr{P}$ tels que

$$((x\in A \text{ et } y\in A) \text{ et } (y\in B \text{ et } z\in B)).$$

Comme $A\cap B\neq\emptyset$ et que $\mathscr{P}$ est une partition, on a nécessairement $A=B$, d'où x et z appartiennent à A, et donc $x\mathscr{R}z$. Ainsi, la relation $\mathscr{R}$ est transitive, ce qui achève de prouver que c'est une relation d'équivalence.

Enfin, soit x un élément de E. Il existe A de $\mathscr{P}$ tel que x appartienne à A et l'on a alors $\mathscr{C}(x)=A$. En effet, pour tout y de A, x et y appartiennent à A, d'où $x\mathscr{R}y$.

Pour tout élément y de $\mathscr{C}(x)$, il existe une partie A appartenant à $\mathscr{P}$ telle que x et y appartiennent à A. Ceci implique alors, pour les mêmes raisons que précédemment, $A=\mathscr{C}(x)$. Ceci prouve que $E/\mathscr{R}\subset\mathscr{P}$. Réciproquement, soit une partie A appartenant à $\mathscr{P}$. Il existe un élément x de E appartenant à A et l'on a alors $\mathscr{C}(x)=A$. Ceci montre que $\mathscr{P}\subset E/\mathscr{R}$, ce qui conclut la preuve. □

Définition A.21 (relation d'ordre) *Soit $\mathscr{R}$ une relation binaire dans un ensemble E. On dit que $\mathscr{R}$ est une **relation d'ordre** si et seulement si $\mathscr{R}$ est réflexive, antisymétrique et transitive.*

Une relation d'ordre est généralement notée $\leq$. Le couple $(E,\leq)$, où E désigne un ensemble et $\leq$ est une relation d'ordre, est appelé un **ensemble ordonné**. Enfin, on note $x<y$ la relation $(x\leq y \text{ et } x\neq y)$.

Définitions A.22 (relation d'ordre total et d'ordre partiel) *Soit $(E,\leq)$ un ensemble ordonné. La relation $\leq$ est dite **relation d'ordre total** si deux éléments quelconques de E sont **comparables**,*

$$\forall(x,y)\in E^2,\ (x\leq y \text{ ou } y\leq x).$$

*Dans le cas contraire, l'ordre est dit **partiel**.*

Soit $(E,\leq)$ un ensemble (totalement) ordonné et A une partie de E. La relation induite par $\leq$ dans A est une relation d'ordre (total) appelée **relation d'ordre induite par $\leq$ sur A**.

L'introduction d'une relation d'ordre sur un ensemble rend certains éléments des parties de cet ensemble remarquables. Ils sont l'objet des définitions suivantes.

Définitions A.23 *Soit $(E,\leq)$ un ensemble ordonné et A une partie de E.*

- *Un élément x de E est appelé un **majorant** (resp. **minorant**) de A dans E si et seulement si*

$$\forall y\in A,\ y\leq x \quad (\text{resp. } \forall y\in A,\ x\leq y).$$

- *On dit que A est **majorée** (resp. **minorée**) dans E si et seulement si cette partie admet au moins un majorant (resp. minorant) dans E, c'est-à-dire*

$$\exists x\in E,\ \forall y\in A,\ y\leq x \quad (\text{resp. } \exists x\in E,\ \forall y\in A,\ x\leq y).$$

- *Un élément x de E est appelé un **plus grand** (resp. **plus petit**) élément de A si et seulement s'il appartient à A et majore (resp. minore) A, c'est-à-dire*

$$(x \in A \text{ et } (\forall y \in A,\ y \leq x)) \quad \text{(resp. } (x \in A \text{ et } (\forall y \in A,\ x \leq y))).$$

- *Un élément x de A est dit **maximal** (resp. **minimal**) si et seulement si*

$$\forall y \in A,\ (x \leq y \implies x = y) \quad \text{(resp. } \forall y \in A,\ (y \leq x \implies x = y)).$$

Définition A.24 (bornes supérieure et inférieure) *Soit $(E, \leq)$ un ensemble ordonné et A une partie de E. On dit qu'un élément M de E est la **borne supérieure de** A **dans** E, notée* $\sup A$*, si l'ensemble des majorants de A dans E admet M comme plus petit élément. Un élément m de E est appelé la **borne inférieure de** A **dans** E, notée* $\inf A$*, si l'ensemble des minorants de A dans E admet m comme plus grand élément.*

A.1.3 Applications

On s'intéresse à présent aux relations particulières nommées *applications*.

Définitions A.25 *On appelle **fonction** d'un ensemble E dans un ensemble F une relation qui à un élément de E associe au plus un élément de F. L'ensemble des éléments de E auxquels une fonction associe exactement un élément dans F est appelé l'**ensemble**, ou le **domaine, de définition** de cette fonction.*

Définitions A.26 *Soit E et F deux ensembles et u une fonction de E dans F. Tout élément y de F associé par la fonction u à un élément x de E est appelé l'**image de x par** u, ce que l'on note $y = u(x)$, tandis que x est un **antécédent** de y par u. On dit encore que E (resp. F) est l'**ensemble de départ** (resp. l'**ensemble d'arrivée**) de u. Enfin, le **graphe** de u est l'ensemble des couples $(x, u(x))$ lorsque x parcourt E.*

Définition A.27 (application) *Une fonction de E dans F est une **application** si et seulement si son domaine de définition est égal à E.*

On utilise la notation $u : E \to F$ pour indiquer que u est une application d'un ensemble E dans un ensemble F. La définition de l'égalité entre deux ensembles (voir la définition A.1) implique que deux applications u et v de E dans F sont égales si, pour chaque élément x de E, on a $u(x) = v(x)$.

L'**application identité** d'un ensemble E est l'application de E dans lui-même, qui associe tout élément de E à lui-même.

Définition A.28 (restriction d'une application) *Soit E et F deux ensembles, u une application de E dans F et A une partie de E. On appelle **restriction de u à** A l'application, notée $u_{|_A}$, définie par*

$$\begin{array}{rccc} u_{|_A} : & A & \to & F \\ & x & \mapsto & u(x). \end{array}$$

Définition A.29 (prolongement d'une application) *Soit E et F deux ensembles, u une application de E dans F et G un ensemble tel que $E \subset G$. On appelle **prolongement de u à** G toute application $\widetilde{u}$ de G dans F telle que*

$$\forall x \in E,\ \widetilde{u}(x) = u(x).$$

Définition A.30 (stabilité par une application) *Une partie A d'un ensemble E est dite **stable par** une application u de E dans E si et seulement si, pour tout élément x de A, l'image $u(x)$ appartient à A.*

Définition A.31 (application surjective) *Une application u d'un ensemble E dans un ensemble F est dite **surjective** (on dit encore que c'est une **surjection**) si et seulement si*

$$\forall y \in F,\ \exists x \in E,\ u(x) = y,$$

c'est-à-dire si tout élément de F est l'image par u d'au moins un élément de E.

Définition A.32 (application injective) *Une application u d'un ensemble E dans un ensemble F est dite* ***injective*** *(on dit encore que c'est une* ***injection****) si et seulement si*

$$\forall (x,x') \in E^2,\ u(x) = u(x') \implies x = x',$$

c'est-à-dire si deux éléments distincts de E ont des images distinctes.

Définition A.33 (application bijective) *Une application est dite* ***bijective*** *(on dit encore que c'est une* ***bijection****) si et seulement si elle est à la fois surjective et injective.*

Une bijection d'un ensemble E dans lui-même est appelée une **permutation** et l'ensemble des permutations de E est noté $\mathfrak{S}(E)$.

Proposition A.34 *Une application u d'un ensemble E dans un ensemble F est bijective si et seulement si tout élément de F possède un unique antécédent par u dans E, c'est-à-dire*

$$\forall y \in F,\ \exists! x \in E,\ u(x) = y.$$

DÉMONSTRATION. Si l'application u est bijective, alors elle est surjective. Par conséquent, tout élément y appartenant à F admet au moins un antécédent x par f dans E. On suppose maintenant que y possède deux antécédents x et x'. On a alors $y = u(x) = u(x')$, d'où $x = x'$, puisque u est injective, et l'élément n'admet donc y qu'un seul antécédent.
Réciproquement, si tout élément y de F admet un unique antécédent x par u dans E, alors l'application u est surjective de E dans F. Soit x et x' des éléments de E tels que $u(x) = u(x')$. En posant $y = u(x) = u(x')$, on a que x et x' sont deux antécédents de y. Par unicité de l'antécédent, on a $x = x'$, ce qui prouve l'injectivité de f. L'application u est donc bijective de E dans F. □

On introduit maintenant les notions d'application *composée* et d'application *réciproque*.

Définition A.35 (application composée) *Soit E, F et G trois ensembles, u une application de E dans F et v une application de F dans G. L'application $v \circ u$ de E dans G, définie par $v \circ u(x) = v(u(x))$ pour tout x de E, est appelée* ***composée de v et de u****.*

Pour pouvoir définir l'application composée $v \circ u$, il est nécessaire que l'ensemble de départ de v soit égal à l'ensemble d'arrivée de u. L'ordre de composition est également important. Même dans le cas où l'on peut composer dans les deux sens, on a en général $v \circ v \neq v \circ u$.

Proposition A.36 *Soit E, F, G et H quatre ensembles, u une application de E dans F, v une application de F dans G et w une application de G dans H. On a*

$$(w \circ v) \circ u = w \circ (v \circ u).$$

On se référera à la preuve de la proposition A.13 pour une démonstration de ce dernier résultat.

Proposition A.37 *La composée de deux injections (resp. surjections, resp. bijections) est une injection (resp. surjection, resp. bijection).*

DÉMONSTRATION. Soit u une application d'un ensemble E dans un ensemble F et v une application de F dans un ensemble G, que l'on suppose dans un premier temps toutes deux injectives. On a

$$\forall (x,x') \in E^2,\ (v \circ u)(x) = (v \circ u)(x') \iff v(u(x)) = v(f(x')) \implies u(x) = u(x') \implies x = x',$$

d'où $v \circ u$ est injective.

On suppose à présent que u et v sont surjectives. Soit z un élément de G. Puisque l'application v est surjective, il existe un élément y de F tel que $v(y) = z$. L'application u étant surjective, il existe alors un élément x de E tel que $u(x) = y$. On a donc $z = v(u(x)) = (v \circ u)(x)$, ce qui montre que $v \circ u$ est surjective.

Enfin, on a, en se servant des deux assertions qui viennent d'être démontrées,

$$(u \text{ et } v \text{ bijectives}) \implies \begin{cases} u \text{ et } v \text{ injectives} \\ u \text{ et } v \text{ surjectives} \end{cases} \implies \begin{cases} v \circ u \text{ injective} \\ v \circ u \text{ surjective} \end{cases} \implies (v \circ u \text{ bijective}).$$

□

Proposition A.38 *Soit E, F et G trois ensembles, u une application de E dans F et v une application de F dans G. Si $v \circ u$ est injective (resp. surjective), alors u est injective (resp. v est surjective).*

DÉMONSTRATION. On suppose que $v \circ u$ est injective. On a, pour tout couple (x, x') de E^2,

$$u(x) = u(x') \implies v(u(x)) = v(u(x')) \iff (v \circ u)(x) = (v \circ u)(x') \implies x = x',$$

ce qui montre que l'application u est injective.

On suppose maintenant que $v \circ u$ surjective. Pour tout élément z de G, il alors existe un élément x de E tel que $z = (v \circ u)(x) = v(u(x))$. L'application g est donc surjective. □

Définition A.39 (application réciproque) *Soit u une application d'un ensemble E dans un ensemble F. On appelle* ***application réciproque*** *(ou* ***inverse) de*** *u toute application v de F dans E telle que*

$$\forall x \in E,\ v(u(x)) = x \text{ et } \forall y \in F,\ u(v(y)) = y.$$

Proposition A.40 *Toute application admet au plus une application réciproque.*

DÉMONSTRATION. Soit u une application d'un ensemble E dans un ensemble F, v et w deux applications de F dans E satisfaisant aux conditions de la définition A.39. En particulier, on a, pour tout élément y de F, $u(v(y)) = y$ et, pour tout élément x de E, $w(u(x)) = x$. En composant la première de ces relations par l'application w et en posant $x = v(y)$ dans la seconde, il vient alors $w(y) = w(u(v(y))) = v(y)$. □

Si u est une application d'un ensemble E dans un ensemble F admettant application réciproque, on note u^{-1} cette dernière. Dans ce cas, l'application u^{-1} est elle-même inversible et l'on a que $\left(u^{-1}\right)^{-1} = u$.

Proposition A.41 *Une application d'un ensemble E dans un ensemble F admet une application réciproque si et seulement si elle est bijective.*

DÉMONSTRATION. Soit u une application de E dans F admettant une application réciproque. Pour tout élément y de F, on a $u\left(u^{-1}(y)\right) = y$ et u est donc surjective. Soit deux éléments x et x' de E tels que $u(x) = u(x')$. Il vient alors $x = u^{-1}(u(x)) = u^{-1}(u(x')) = x'$, dont on déduit que l'application u est injective.

Réciproquement, soit u une application bijective et v l'application de F dans E définie de la façon suivante : pour tout élément y de F, on pose $v(y) = x$ où x est l'unique antécédent de y par u. On vérifie alors de manière immédiate que, pour tout élément y de F, on a $u(v(y)) = y$ et, pour tout élément x de E, $v(u(x)) = x$, d'où $v = u^{-1}$. □

La proposition suivante est une conséquence directe des propositions A.37 et A.15.

Proposition A.42 *Soit E, F et G trois ensembles, u une application de E dans F et v une application de F dans G, toutes deux bijectives. L'application $v \circ u$ est alors bijective et l'on a $(v \circ u)^{-1} = u^{-1} \circ v^{-1}$.*

Définition A.43 (involution) *Soit E un ensemble. On appelle* ***involution de*** *E toute application u de E dans E telle que $u \circ u = id_E$, où id_E désigne l'application identité de E.*

Définitions A.44 (images directe et réciproque d'une partie par une application) *Soit E et F deux ensembles, A une partie de E, B une partie de F et u une application de E dans F. L'****image directe de*** *A* ***par*** *u, ou, plus simplement, l'****image de*** *A* ***par*** *u, notée u(A), est le sous-ensemble de F contenant l'image des éléments de A par u,*

$$u(A) = \{y \in F \mid \exists x \in A,\ y = u(x)\}.$$

*L'****image réciproque de*** *B* ***par*** *u, notée $u^{-1}(B)$, est le sous-ensemble de E contenant les antécédents des éléments de B par u,*

$$u^{-1}(B) = \{x \in E \mid u(x) \in B\}.$$

Pour toute application u d'un ensemble E dans un ensemble F, il est toujours possible de définir $u^{-1}(B)$, même si l'application n'est pas bijective. Lorsque c'est cependant le cas, c'est-à-dire lorsque l'application réciproque u^{-1} existe, on pourra vérifier que l'image directe d'une partie B de F par u^{-1} est aussi l'image réciproque $u^{-1}(B)$ de B par u. En effet, dire que x est un élément de $u^{-1}(B)$ signifie que $u(x)$ appartient à B et réciproquement, si l'on pose $y = u(x)$, on aura $x = u^{-1}(y)$ avec y un élément de B, ce qui équivaut à dire que x appartient à $u^{-1}(B)$.

La proposition qui suit est utile en pratique pour déterminer si une application est surjective ou non.

Proposition A.45 *Une application u d'un ensemble E dans un ensemble F est surjective si et seulement si $u(E) = F$.*

DÉMONSTRATION. On a toujours $u(E) \subset F$. Par ailleurs, l'ensemble F est inclus dans $u(E)$ si et seulement si tout élément de F est l'image d'au moins un élément de E par l'application f, ce qui signifie que u est surjective. □

La définition suivante constitue une généralisation de la notion de *suite*.

Définition A.46 (famille) *Soit E et I des ensembles. On appelle **famille d'éléments de** E **indexées par** I toute application de I à valeurs dans E, les éléments de I étant appelés les **indices**.*

Une famille $(x_i)_{i\in I}$ est dite *finie* ou *infinie*, selon que l'ensemble I de ses indices est fini ou infini (voir la sous-section A.1.4). On note $(x_i)_{i\in I}$ la famille d'éléments x_i d'un ensemble E indexée par les éléments i d'un ensemble I. On veillera à ne pas confondre la famille $(x_i)_{i\in I}$ et l'ensemble $\{\{x_i\} \mid i \in I\}$, qui est l'ensemble image de l'application en question.

Définitions A.47 (réunion et intersection de parties) *Soit E un ensemble et $(A_i)_{i\in I}$ une famille de parties de E. La **réunion** (resp. l'**intersection**) de la famille $(A_i)_{i\in I}$, notée $\bigcup_{i\in I} A_i$ (resp. $\bigcap_{i\in I} A_i$) est définie par*

$$\bigcup_{i\in I} A_i = \{x \in E \mid \exists i \in I,\ x \in A_i\} \text{ (resp. } \bigcap_{i\in I} A_i = \{x \in E \mid \forall i \in I,\ x \in A_i\}).$$

Définition A.48 *Soit E un ensemble. Une famille $(A_i)_{i\in I}$ de parties de E est appelée **partition de** E si et seulement si*

- *aucun des ensembles A_i n'est vide,*
- *les ensembles A_i sont disjoints deux à deux,*
- *la réunion des ensembles A_i est égale à E.*

Il est à retenir de cette définition que tout élément d'un ensemble appartient à un unique élément de sa partition. On notera par ailleurs que cet énoncé est cohérent avec la définition A.7, car, pour que la famille $(A_i)_{i\in I}$ soit une partition au sens de la définition ci-dessus, il faut, et il suffit, que l'ensemble image $\{A_i \mid i \in I\}$ soit une partition de E au sens de la définition précedemment donnée pour une partition d'un ensemble.

A.1.4 Cardinalité, ensembles finis et infinis

On termine cette section en donnant quelques propriétés élémentaires relatives à la *cardinalité* des ensembles, notion qui permet d'appréhender le nombre d'élements (on dit encore la « taille ») d'un ensemble.

Définition A.49 (relation d'équipotence) *On dit qu'un ensemble E est **équipotent** à un ensemble F si et seulement s'il existe une bijection de E sur F.*

La relation d'équipotence constitue une relation d'équivalence entre les ensembles. Elle va permettre de formaliser la *dénombrabilité* et la *finitude* d'un ensemble.

Définition A.50 (ensemble dénombrable) *On dit qu'un ensemble est **dénombrable** si et seulement s'il est équipotent à l'ensemble des entiers naturels $\mathbb{N}$.*

Définition A.51 (ensembles finis et infinis) *On dit qu'un ensemble E est **fini** si et seulement s'il existe un entier naturel n tel que E est équipotent à $\{1, \ldots, n\}$. Il est dit **infini** si et seulement s'il n'est pas fini.*

On admet le résultat suivant, dont la preuve s'appuie sur les propriétés de l'ensemble des entiers naturels.

Proposition A.52 *Soit (n, p) un couple d'entiers naturels. On a les assertions suivantes.*

1. *Il existe une injection de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$ si et seulement si $n \leq p$.*
2. *Il existe une surjection de $\{1, \ldots, n\}$ sur $\{1, \ldots, p\}$ si et seulement si $n \geq p$.*
3. *Il existe une bijection de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$ si et seulement si $n = p$.*

La dernière assertion de cette proposition amène la définition suivante.

Définition A.53 (cardinal d'un ensemble) *Soit E un ensemble fini. Il existe alors un entier naturel n, appelé le **cardinal** de E et noté* $\mathrm{card}(E)$*, tel que E soit équipotent à $\{1, \ldots, n\}$.*

Par convention, le cardinal de l'ensemble vide est égal à 0.

Proposition A.54 *Si E est un ensemble fini, toute partie A de E est finie, et l'on a* $\mathrm{card}(A) \leq \mathrm{card}(E)$.

Proposition A.55 *Si E et F sont deux ensembles finis, alors l'ensemble $E \cup F$ est fini et l'on a*

$$\mathrm{card}(E \cup F) + \mathrm{card}(E \cap F) = \mathrm{card}(E) + \mathrm{card}(F).$$

DÉMONSTRATION. On établit tout d'abord un résultat préliminaire. Soit A et B deux ensembles finis *disjoints*. Il existe alors des bijections u de $\{1, \ldots, \mathrm{card}(A)\}$ dans A et v de $\{1, \ldots, \mathrm{card}(B)\}$ dans B, et il est clair que l'application w de $\{1, \ldots, \mathrm{card}(A) + \mathrm{card}(B)\}$ dans $A \cup B$, définie par

$$\forall i \in \{1, \ldots, \mathrm{card}(A) + \mathrm{card}(B)\},\ w(i) = \begin{cases} u(i) & \text{si } 1 \leq i \leq \mathrm{card}(A) \\ v(i - \mathrm{card}(A)) & \text{si } \mathrm{card}(A) + 1 \leq i \leq \mathrm{card}(A) + \mathrm{card}(B) \end{cases}$$

est une bijection. Il en résulte que l'ensemble $A \cup B$ est fini et que $\mathrm{card}(A \cup B) = \mathrm{card}(A) + \mathrm{card}(B)$.

En appliquant ce résultat aux ensembles E et $E \setminus F$, il vient que l'ensemble $E \cup F$ est fini et

$$\begin{aligned} \mathrm{card}(E \cup F) + \mathrm{card}(E \cap F) &= \mathrm{card}(E \cup (F \setminus E)) + \mathrm{card}(E \cap F) = (\mathrm{card}(E) + \mathrm{card}(F \setminus E)) + \mathrm{card}(E \cap F) \\ &= \mathrm{card}(E) + (\mathrm{card}(F \setminus E) + \mathrm{card}(E \cap F)) = \mathrm{card}(E) + \mathrm{card}(F). \end{aligned}$$

□

Corollaire A.56 *Soit E un ensemble fini et A une partie de E. Si* $\mathrm{card}(A) = \mathrm{card}(E)$ *alors $A = E$.*

DÉMONSTRATION. L'identité de la proposition précédente appliquée aux ensembles A et $E \setminus A$ s'écrit $\mathrm{card}(E) = \mathrm{card}(A) + \mathrm{card}(E \setminus A)$ dans le cas présent. Si $\mathrm{card}(A) = \mathrm{card}(E)$, on en déduit que $\mathrm{card}(E \setminus A) = 0$, d'où $E \setminus A = \varnothing$ et donc $E = A$. □

Cette dernière propriété est particulièrement importante et possède un analogue portant sur des dimensions d'espaces vectoriels en algèbre linéaire.

Proposition A.57 *Soit E et F des ensembles finis ayant même cardinal et u une application de E dans F. Les assertions suivantes sont équivalentes.*

i) L'application u est injective.

ii) L'application u est surjective.

iii) L'application u est bijective.

DÉMONSTRATION. On montre tout d'abord que l'assertion i implique ii et iii. Si l'application u est injective, alors la *corestriction* $u^{|u(E)}$ de u, c'est-à-dire l'application de E dans $u(E)$ qui à un élément x de E associe $u(x)$ est bijective, d'où $\mathrm{card}(u(E)) = \mathrm{card}(E) = \mathrm{card}(F)$ et donc $u(E) = F$ d'après le corollaire A.56. L'application u est ainsi surjective, et par conséquent bijective.

On prouve ensuite que l'assertion ii implique i et iii. On suppose pour cela que l'application u est surjective, mais non injective. Il existe dans ce cas un couple (x, x') de E^2 tel que $x \neq x'$ et $u(x) = u(x')$. L'application de $E \setminus \{x'\}$ dans F, qui à un élément de E différent de x' associe son image par u, est surjective, d'où $\mathrm{card}(E \setminus \{x'\}) \geq \mathrm{card}(F)$. Or, on a $\mathrm{card}(E \setminus \{x'\}) = \mathrm{card}(E) - 1$ et $\mathrm{card}(E) = \mathrm{card}(F)$, d'où une contradiction.

Enfin, l'assertion iii implique i et ii de manière triviale. □

A.2 Structures algébriques

On va maintenant considérer des ensembles munis d'une ou de plusieurs « opérations » satisfaisant à un certain nombre d'axiomes.

A.2.1 Lois de composition

On commence par introduire les applications particulières que sont les *lois de composition*. Tout d'abord, étant donnés trois ensembles E, F et G non vides, toute application de l'ensemble produit $E \times F$ à valeurs dans l'ensemble G est appelée loi de composition de $E \times F$ dans G. Cependant, dans toute la suite, nous aurons systématiquement $E = F = G$ ou bien encore $E = G \neq F$. Ces deux cas particuliers sont les objets des définitions suivantes.

Définition A.58 (loi de composition interne) *Soit E un ensemble non vide. On appelle **loi de composition interne sur** E toute application de $E \times E$ dans E.*

Les opérations d'addition et de multiplication sur l'ensemble des entiers naturels $\mathbb{N}$ sont deux exemples de loi de composition interne.

Définition A.59 (loi de composition externe) *Soit E et F des ensembles non vides. On appelle **loi de composition externe sur** E **à opérateurs dans** F toute application de $F \times E$ à valeurs dans E.*

On dit encore d'une telle loi qu'elle est une *action de l'ensemble F sur l'ensemble E*. Dans la définition ci-dessus, on remarque que l'on a choisi de placer le *domaine des opérateurs* F en premier dans le produit $F \times E$, c'est-à-dire qu'on a considéré, de manière implicite, que la loi de composition était externe *à gauche*, mais des lois de composition externes *à droite* sont également possibles. Ajoutons que lorsque les *opérateurs externes*, c'est-à-dire les éléments de l'ensemble F, sont des nombres réels ou complexes (ou, plus généralement, les éléments d'un *corps*), ceux-ci sont appelés *scalaires* et l'on a coutume de noter la loi de composition externe multiplicativement et généralement, comme on le verra plus loin, sans symbole.

Un ensemble muni d'une loi de composition interne est appelé un *magma*.

Définitions A.60 (associativité et commutativité d'une loi de composition interne) *Soit E un ensemble muni de la loi de composition interne $\star$. Cette loi est dite **associative** si*

$$\forall (x,y,z) \in E^3,\ (x \star y) \star z = x \star (y \star z).$$

*Elle est **commutative** si*

$$\forall (x,y) \in E^2,\ x \star y = y \star x.$$

Un magma est dit *associatif* (resp. *commutatif*) si sa loi est associative (resp. commutative).

Définition A.61 (élément neutre) *Soit E un ensemble muni de la loi de composition interne $\star$. Un élément e de E est un **élément neutre** (resp. **neutre à gauche**, resp. **neutre à droite**) pour cette loi si*

$$\forall x \in E,\ e \star x = x \star e = x \text{ (resp. } e \star x = x,\ \text{resp. } x \star e = x).$$

Un magma possédant un élément neutre est dit *unifère* et cet élement est alors unique. On appelle **monoïde** un magma associatif unifère.

Définition A.62 (élément symétrique) *Soit E un ensemble muni de la loi de composition interne $\star$ et admettant un élément neutre e. On dit qu'un élément x de E possède un **élément symétrique** (resp. **élément symétrique à gauche**, resp. **élément symétrique à droite**) pour la loi $\star$ s'il existe un élément y de E tel que*

$$x \star y = y \star x = e \text{ (resp. } y \star x = e,\ \text{resp. } x \star y = e).$$

En général, un élément donné d'un magma unifère peut avoir plusieurs éléments symétriques à gauche ou à droite et même plusieurs éléments symétriques à gauche *et* à droite. Cependant, si l'on travaille sur un monoïde, c'est-à-dire si la loi de composition interne considérée est associative, et qu'un élément possède à la fois un élément symétrique à droite et un élément symétrique à gauche, ceux-ci sont égaux et l'élément symétrique est unique. Dans ce cas, l'élément symétrique d'un élément x est généralement noté $-x$ lorsque la loi de composition est notée additivement, x^{-1} ou $\frac{1}{x}$ si elle est notée multiplicativement.

Lorsque un ensemble est muni de deux lois de composition internes, une propriété particulièrement intéressante est la *distributivité* d'une des lois par rapport à l'autre.

Définition A.63 (distributivité d'une loi de composition interne) *Soit E un ensemble non vide muni de deux lois de composition internes $\star$ et $\circ$. La loi $\star$ est dite* ***distributive à gauche*** *(resp.* ***distributive à droite****) par rapport à la loi $\circ$ si on a*

$$\forall (x,y,z) \in E^3,\ x \star (y \circ z) = (x \star y) \circ (x \star z) \text{ (resp. } (y \circ z) \star x = (y \star x) \circ (z \star x)).$$

On dit que la loi $\star$ est ***distributive par rapport à la loi*** *$\circ$ si elle est à la fois distributive à gauche et à droite.*

Les dernières définitions restent valables lorsque $\star$ est une loi de composition externe à opérateurs dans un ensemble F non vide et $\circ$ une loi de composition interne sur E, à condition que l'élément x considéré dans l'énoncé appartienne à F.

A.2.2 Groupe

Parmi les structures algébriques les plus simples, c'est-à-dire des ensembles munis d'une loi de composition interne satisfaisant à des axiomes, on trouve la notion de *groupe*. Celle-ci occupe une place centrale en mathématiques en raison du lien étroit qu'elle possède avec la notion de *symétrie*, que l'on retrouve par exemple en physique.

Définition A.64 (groupe) *On appelle* ***groupe*** *tout ensemble E muni d'une loi de composition interne $\star$ vérifiant les propriétés suivantes :*

- *la loi est associative,*
- *il existe un élément neutre,*
- *tout élément possède un élément symétrique.*

Lorsque la loi de composition interne d'un groupe est commutative, on dit que le groupe est *commutatif*, ou encore *abélien*.

A.2.3 Anneau

Un autre exemple de structure aljouant un rôle fondamental en mathématiques est celui des *anneaux*, qui interviennent notamment dans l'étude des équations algébriques et des nombres algébriques.

Définition A.65 (anneau) *On appelle* ***anneau*** *tout ensemble E non vide muni deux lois de composition internes $+$ et $*$ tel que*

- *$(E,+)$ est un groupe commutatif, c'est-à dire que*
  - *la loi $+$ est associative,*
  - *il existe un élément neutre, noté 0_E, pour cette loi,*
  - *tout élément possède un élément symétrique pour cette loi,*
- *$(E,*)$ est un monoïde, c'est-à dire que*
  - *la loi $*$ est associative,*
  - *il existe un élément neutre, noté 1_E, pour cette loi $*$,*
- *la loi $*$ est distributive par rapport à la loi $+$.*

Les lois $+$ et $*$ d'un anneau sont souvent appelées *addition* et *multiplication*, et l'on note généralement 0_E et 1_E les éléments unitaires respectifs pour ces lois. On parle d'anneau *commutatif* lorsque la multiplication est de plus commutative.

A.2.4 Corps

La structure algébrique qui servira en algèbre linéaire est le *corps*.

Définition A.66 (corps) *On appelle* ***corps*** *tout anneau $(E,+,*)$ tel que $(E \setminus \{0_E\},*)$ est un groupe.*

On dit qu'un corps est *commutatif* si la multiplication est commutative. Des exemples de corps commutatifs sont donnés par les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition et de la multiplication usuelles.

A.2.5 Espace vectoriel

On s'intéresse maintenant à une structure possédant, à la manière des anneaux, à la fois des lois de composition internes *et* externes, ce qui permet, en autres choses, d'effectuer des *combinaisons linéaires* de ses éléments. C'est celle d'*espace vectoriel*, qui est à la base de l'algèbre linéaire.

Dans toute la suite, on note par $\mathbb{K}$ un corps commutatif $(\mathbb{K}, +, *)$, appelé le corps des *scalaires*, où $\mathbb{K} = \mathbb{R}$ ou bien $\mathbb{C}$ et où les lois $+$ et $*$ sont respectivement l'addition et la multiplication usuelles.

Définition A.67 (espace vectoriel) *Un **espace vectoriel sur un corps commutatif** $\mathbb{K}$ (ou **$\mathbb{K}$-espace vectoriel**) est un ensemble non vide E muni d'une loi de composition interne, appelée **addition** et notée $+$, et d'une loi de composition externe à opérateurs dans $\mathbb{K}$, appelée **multiplication par un scalaire**, possédant les propriétés suivantes :*

- $(E, +)$ *est un groupe commutatif,*
- $\forall (\lambda, \mu) \in \mathbb{K}^2,\ \forall x \in E,\ (\lambda + \mu)x = \lambda x + \mu x,$
- $\forall \lambda \in \mathbb{K},\ \forall (x, y) \in E^2,\ \lambda(x + y) = \lambda x + \lambda y,$
- $\forall (\lambda, \mu) \in \mathbb{K}^2,\ \forall x \in E,\ \lambda(\mu x) = (\lambda\mu)x,$
- $\forall x \in E,\ 1_{\mathbb{K}} x = x,$

*où le scalaire $1_{\mathbb{K}}$ étant l'élément unitaire du corps $\mathbb{K}$. Les éléments d'un espace vectoriel sont appelés des **vecteurs**.*

Dans cette définition, on observera qu'on a employé, par abus, le même symbole « + » pour les lois additives sur $\mathbb{K}$ et E. On a également omis d'écrire le symbole de la loi externe lorsqu'on multiplie un vecteur par un scalaire. Dans la suite, on utilisera la seule lettre E pour désigner le triplet, formé d'un ensemble E et de deux lois de composition, constituant un espace vectoriel, comme c'est souvent le cas en pratique.

Définition A.68 (sous-espace vectoriel) *On dit qu'une partie non vide F d'un espace vectoriel E sur $\mathbb{K}$ est un **sous-espace vectoriel** de E si et seulement si*

$$\forall \lambda \in \mathbb{K},\ \forall (x, y) \in F^2,\ \lambda x + y \in F.$$

On dit encore qu'un sous-espace vectoriel d'un espace vectoriel E est un sous-ensemble de E stable par les lois de composition interne et externe dont E est muni. On montre facilement qu'une intersection de sous-espaces vectoriels est un sous-espace vectoriel.

Définition A.69 (combinaison linéaire) *Soit E un $\mathbb{K}$-espace vectoriel, p un entier naturel non nul et $\{e_1, \ldots, e_p\}$ une famille d'éléments de E. On dit qu'un élément de E est une **combinaison linéaire** de la famille lorsqu'il peut s'écrire sous la forme $\alpha_1 e_1 + \cdots + \alpha_p e_p$, où $\alpha_1, \ldots, \alpha_p$ sont des élements de $\mathbb{K}$. Plus généralement, si I est un ensemble et $\{e_i\}_{i \in I}$ une famille de vecteurs de E, on dit qu'un vecteur de E est combinaison linéaire de la famille $\{e_i\}_{i \in I}$ s'il existe une sous-famille finie de $\{e_i\}_{i \in I}$ dont le vecteur est combinaison linéaire.*

Il découle des deux dernières définitions qu'un sous-espace vectoriel est aussi stable par combinaison linéaire.

Définition A.70 (sous-espace vectoriel engendré par une partie) *Soit E un espace vectoriel sur $\mathbb{K}$ et $\{e_i\}_{i \in I}$ une famille d'éléments de E. L'ensemble des vecteurs qui sont combinaison linéaire de $\{e_i\}_{i \in I}$ est appelé **sous-espace vectoriel engendré** par cette famille de vecteurs. On le note* $\mathrm{Vect}(\{e_i\}_{i \in I})$.

On vérifie facilement que, pour toute partie A de E, $\mathrm{Vect}(A)$ est bien un sous-espace vectoriel de E. C'est même le *plus petit* sous-espace vectoriel qui contienne A, au sens de la relation d'inclusion : il est inclus dans tous les sous-espaces vectoriels de E qui contiennent A.

Définition A.71 (famille génératrice) *Soit E un espace vectoriel sur $\mathbb{K}$ et $\{e_i\}_{i \in I}$ une famille de vecteurs de E. On dit que cette famille **engendre** E, ou qu'elle en est **génératrice**, lorsque $E = \mathrm{Vect}(\{e_i\}_{i \in I})$. Une telle famille est dite **minimale** lorsqu'il est impossible de lui ôter un vecteur sans lui faire perdre son caractère générateur.*

Définitions A.72 (famille libre, famille liée) *Soit E un espace vectoriel sur $\mathbb{K}$, m un entier naturel non nul et $\{e_i\}_{i=1,\ldots,m}$ une famille de m vecteurs de E. Cette famille est dite **libre** si les vecteurs $e_1, \ldots, e_m$ sont **linéairement indépendants**, c'est-à-dire si la relation*

$$\alpha_1 e_1 + \cdots + \alpha_m e_m = 0_E,$$

*où 0_E est l'élément nul de E et $\alpha_1, \ldots, \alpha_m$ sont des éléments de $\mathbb{K}$, implique que $\alpha_1 = \cdots = \alpha_m = 0$. Dans le cas contraire, la famille est dite **liée**. Plus généralement, une famille $\{e_i\}_{i \in I}$ de vecteurs de E est dite libre si toute sous-famille de $\{e_i\}_{i \in I}$ est libre. Une telle famille est dite **maximale** lorsqu'il est impossible de lui ajouter un vecteur sans lui faire perdre sa liberté.*

Définition A.73 (base) *On dit qu'une famille de vecteurs d'un espace vectoriel E sur $\mathbb{K}$ est une* ***base*** *de E si elle est à la fois libre et génératrice de E.*

On peut caractériser une base d'un espace vectoriel comme une famille génératrice minimale de cet espace ou comme une famille libre maximale. Il en découle qu'une famille de vecteurs est une base d'un espace vectoriel si et seulement si tout vecteur de cet espace peut s'écrire de façon unique comme une combinaison linéaire des vecteurs de la famille. Les coefficients de cette combinaison linéaire sont alors appelés les **coordonnées** du vecteur dans la base.

Définition A.74 (espace vectoriel de dimension finie) *Un espace vectoriel sur $\mathbb{K}$ est dit* ***de dimension finie*** *si et seulement s'il admet une famille génératrice de cardinal fini. Sinon, il est dit* ***de dimension infinie****.*

Le résultat ci-après est clé pour prouver un résultat fondamental sur le cardinal des bases d'un espace vectoriel de dimension finie.

Lemme A.75 (« lemme d'échange de Steinitz ») *Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie, $\mathscr{L}$ une famille libre de E de cardinal m et $\mathscr{G}$ une famille génératrice de E de cardinal p. Alors, on a nécessairement $m \leq p$ et l'on peut échanger m des vecteurs de la famille $\mathscr{G}$ avec les m vecteurs de la famille $\mathscr{L}$.*

DÉMONSTRATION. On note $\mathscr{L} = \{x_1, \dots, x_m\}$ et $\mathscr{G} = \{y_1, \dots, y_p\}$ et on raisonne par récurrence. Pour $m = 0$, il n'y a rien à montrer. Soit m un entier naturel non nul ; on suppose le résultat vrai pour un entier naturel k inférieur ou égal à $m-1$. Il existe ainsi une renumérotation des vecteurs de la famille $\mathscr{G}$ telle que la famille $\{x \dots, x_k, y_{k+1}, \dots, y_p\}$ engendre E. On considère alors le vecteur x_{k+1}, pour lequel il existe des scalaires $\alpha_1, \dots, \alpha_k$ et $\beta_{k+1}, \dots, \beta_p$ tels que

$$x_{k+1} = \sum_{i=1}^{k} \alpha_i x_i + \sum_{j=k+1}^{p} \beta_j y_j.$$

On remarque qu'au moins l'un des coefficients de la seconde somme ne peut être nul, faute de quoi la famille $\mathscr{L}$ ne pourrait être libre. Ceci implique que $k+1 \leq p$. De plus, quitte à renuméroter, on peut supposer que le coefficient β_{k+1} est non nul, et l'on a

$$y_{k+1} = \frac{1}{\beta_{k+1}} \left(x_{k+1} - \sum_{i=1}^{k} \alpha_i x_i - \sum_{j=k+2}^{p} \beta_j y_j \right).$$

Le vecteur y_{k+1} appartient donc à $\mathrm{Vect}\big(\{x_1, \dots, x_{k+1}, y_{k+2}, \dots, y_p\}\big)$. Les vecteurs $x_1, \dots, x_k, y_{k+1}, \dots, y_p$ appartiennent donc à $\mathrm{Vect}\big(\{x_1, \dots, x_{k+1}, y_{k+2}, \dots, y_p\}\big)$, qui contient par conséquent $\mathrm{Vect}\big(\{x_1, \dots, x_k, y_{k+1}, \dots, y_p\}\big) = E$, ce qui achève la preuve. □

Théorème A.76 (existence de base dans un espace de dimension finie) *Un espace vectoriel de dimension finie admet une base de cardinal fini de vecteurs, et toutes ses bases ont le même cardinal.*

DÉMONSTRATION. Soit une famille génératrice $\{e_1, \dots, e_p\}$ d'un espace vectoriel E de dimension finie. Si celle-ci ne comporte que le vecteur nul, on a, par convention, $E = \mathrm{Vect}(\varnothing)$. Sinon, elle contient au moins un vecteur non nul et on considère alors l'ensemble des cardinaux des sous-familles libres de la famille. Ce dernier ensemble est non vide, puisqu'il existe une famille libre à un seul vecteur, et majoré par l'entier p ; il admet donc un plus grand élément, que l'on note n. Quitte à renuméroter les éléments de la famille, soit $\mathscr{B} = \{e_1, \dots, e_n\}$ un sous-famille libre à n éléments. Pour tout indice i appartenant à $\{n+1, \dots, p\}$, la sous-famille $\{e_1, \dots, e_n, e_i\}$ est liée par définition de n et il existe donc des scalaires $\alpha_1, \dots, \alpha_n, \alpha_i$ non tous nuls tels que $\alpha_1 e_1 + \dots + \alpha_n e_n + \alpha_i e_i = 0_E$, le coefficient α_i ne pouvant être nul, car sinon la liberté de $\mathscr{B}$ entraînerait la nullité de tous les coefficients. Le vecteur e_i peut donc s'écrire comme une combinaison linéaire des vecteurs $e_1, \dots, e_n$, dont on déduit que la sous-famille $\mathscr{B}$ est génératrice de E, ce qui achève de montrer que c'est une base.

Soit à présent $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E. D'une part, la famille $\mathscr{B}$ est libre et la famille $\mathscr{B}'$ est génératrice, on a donc $\mathrm{card}\,\mathscr{B} \leq \mathrm{card}\,\mathscr{B}'$ par le lemme d'échange précédent. On obtient l'inégalité renversée en échangeant les rôles respectifs des familles. □

La définition suivante est une conséquence directe du dernier résultat.

Définition A.77 (dimension d'un espace vectoriel) *Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie. On appelle* ***dimension de*** *E, et on note* $\dim E$*, le cardinal commun de toutes les bases de E.*

On a les résultats suivants.

Théorème A.78 (« théorème de la base incomplète ») *Soit E un espace vectoriel de dimension finie. Toute famille libre de vecteurs de E peut être complétée en une base de E.*

DÉMONSTRATION. Il suffit de montrer que l'on peut compléter la famille libre en lui ajoutant des vecteurs d'une famille génératrice de E, que l'on peut considérer *finie*. En effet, soit $\mathscr{G} = \{x_i,\ i \in I\}$ une famille génératrice de E arbitraire. Si celle-ci n'est pas finie, l'espace E étant supposé de dimension finie, on sait qu'il existe une famille génératrice finie $\mathscr{G}' = \{x'_1, \dots, x'_p\}$. Si les vecteurs de la famille $\mathscr{G}'$ n'ont aucune raison d'appartenir à $\mathscr{G}$, ce sont néanmoins de vecteurs de E et ils peuvent donc s'écrire comme une combinaison linéaire d'un nombre fini de vecteurs de $\mathscr{G}$:

$$\forall k \in \{1, \dots, p\},\ \exists J_k \subset I,\ \mathrm{card}(J_k) < +\infty,\ x'_k \in \mathrm{Vect}(\{x_i,\ i \in J_k\}).$$

On définit alors la famille $\mathscr{G}'' = \{x_i,\ i \in J_1 \cup \dots J_p\}$. C'est une sous-famille finie de $\mathscr{G}$, telle que tout vecteur de $\mathscr{G}'$ appartient au sous-espace vectoriel qu'elle engendre, ce qui en fait une famille génératrice de E. On peut ainsi considérer $\mathscr{G}''$ en place de $\mathscr{G}$ lorsque cette dernière n'est pas finie.

On considère à présent une famille libre $\mathscr{L}$ et une famille génératrice finie $\mathscr{G} = \{x_1, \dots, x_p\}$. Pour construire une base à partir de ces deux familles, on applique l'algorithme suivant. On pose $\mathscr{B}_0 = \mathscr{L}$. Pour l'entier i qui prend les valeurs 1 à p, on vérifie si le vecteur x_i appartient à $\mathrm{Vect}(\mathscr{B}_{i-1})$. Si ce n'est pas le cas, on pose $\mathscr{B}_i = \mathscr{B}_{i-1} \cup \{x_i\}$, sinon $\mathscr{B}_i = \mathscr{B}_{i-1}$.

À l'issue de p étapes, on obtient une famille $\mathscr{B} = \mathscr{B}_p$ libre et telle que $\mathrm{Vect}(\mathscr{B})$ contient $\mathbb{G}$; elle engendre E et c'est donc une base de E. □

Remarque A.79 *Un résultat similaire au théorème de la base incomplète, nommé parfois « théorème de la base extraite », affirme qu'on peut extraire une base de toute famille génératrice.*

Théorème A.80 (cardinal d'une famille libre ou génératrice en dimension finie) *Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie égale à n. Si la famille $\{x_1, \dots, x_m\}$ de E est libre, alors on a $m \leq n$. Si la famille $\{x_1, \dots, x_p\}$ de E est génératrice de E, alors on a $p \geq n$. De plus, les assertions suivantes sont équivalentes*

i) la famille $\{x_1, \dots, x_n\}$ est une base de E,

ii) la famille $\{x_1, \dots, x_n\}$ est libre,

iii) la famille $\{x_1, \dots, x_n\}$ est génératrice de E.

DÉMONSTRATION. Si $\{x_1, \dots, x_m\}$ est une famille libre de vecteurs de E, alors il existe une base de E qui la contient (c'est une conséquence du théorème A.78). Comme une base de E contient n vecteurs, la famille $\{x_1, \dots, x_m\}$ contient au plus n vecteurs. De même, si $\{x_1, \dots, x_p\}$ est une famille génératrice de E, alors elle contient une base de E (A VOIR) et comporte donc au moins n vecteurs.
Pour montrer les équivalences, il suffit d'utiliser la caractérisation des bases parmi les familles libres ou génératrices. Si $\{x_1, \dots, x_n\}$ est une famille libre de n vecteurs de E, alors c'est une famille libre maximale d'après la première partie du théorème et donc ii implique i. De même, $\{x_1, \dots, x_n\}$ est une famille génératrice de E, c'est une famille génératrice minimale d'après la seconde partie du théorème et donc iii implique i. Enfin, il est évident que i implique ii et iii. □

Proposition A.81 (dimension d'un sous-espace vectoriel) *Soit E un espace vectoriel de dimension finie. Soit A est un sous-espace vectoriel de E, alors A est de dimension finie et* $\dim(A) \leq \dim(E)$. *Si de plus* $\dim(A) = \dim(E)$, *alors $A = E$.*

DÉMONSTRATION. Comme A est un sous-espace vectoriel de E, toute famille libre de A est une famille libre de E. Par conséquent, toute famille libre de A, et donc toute base de A, est de cardinal fini et inférieur à $\dim(E)$. Puisque toute les bases de A possèdent le même cardinal, on en déduit que $\dim(A) \leq \dim(E)$.
Si $\dim(A) = \dim(E) = n$, on considère une base $\{e_1, \dots, e_n\}$ de A. C'est une famille libre de n vecteurs dans un espace vectoriel de dimension n, et donc une base de E. On a ainsi $F = \mathrm{Vect}(\{e_1, \dots, e_n\}) = E$. □

Proposition A.82 (dimension d'un espace produit) *Si E et F sont deux espaces vectoriels de dimension finie, alors*

$$\dim(E \times F) = \dim(E) + \dim(F).$$

DÉMONSTRATION. On considère une base $\{e_1,\dots,e_n\}$ de E et une base $\{f_1,\dots,f_p\}$ de F. Les $n+p$ vecteurs $(e_1,0_F),\dots,(e_n,0_F)$, $(0_E,f_1),\dots,(0_E,f_p)$ sont des vecteurs de $E\times F$. On va montrer qu'ils forment une base de cet espace vectoriel. Soit (x,y) un élément de $E\times F$. On cherche un unique $n+p$-uplet $(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_p)$ tel que

$$(x,y)=\alpha_1(e_1,0_F)+\cdots+\alpha_n(e_n,0_F)+\beta_1(0_E,f_1)+\cdots+\beta_p(0_E,f_p)=\left(\sum_{i=1}^{n}\alpha_i e_i,\sum_{j=1}^{p}\beta_j f_j\right),$$

ce qui revient à déterminer les n-uplets $(\alpha_1,\dots,\alpha_n)$ tels que $x=\sum_{i=1}^{n}\alpha_i e_i$ et les p-uplets $(\beta_1,\dots,\beta_p)$ tels que $y=\sum_{j=1}^{p}\beta_j f_j$. Puisque la famille $\{e_1,\dots,e_n\}$ est une base de E, il y a bien unicité de la solution du premier système, donnée par les coordonnées du vecteur x dans cette base. De même, il y a unicité de la solution du second système : ce sont les coordonnées du vecteur y dans la base $\{f_1,\dots,f_p\}$. Il existe donc bien une base de $E\times F$ dont le cardinal est $\dim(E)+\dim(F)$. □

Définition A.83 (rang d'une famille de vecteurs) *Le **rang** d'une famille finie de vecteurs d'un espace vectoriel correspond au cardinal d'une plus grande sous-famille libre de cette famille.*

Proposition A.84 (caractérisation du rang d'une famille de vecteurs) *Le rang d'une famille finie de vecteurs d'un espace vectoriel est égal à la dimension du sous-espace vectoriel engendré par cette famille.*

DÉMONSTRATION. Soit p un entier naturel non nul. On considère une famille $\{x_1,\dots,x_p\}$ de vecteurs d'un espace vectoriel E et on note r son rang. Quitte à renuméroter les vecteurs de la famille, on peut supposer que la sous-famille $\{x_1,\dots,x_r\}$ est une plus grande sous-famille libre. Pour tout indice i appartenant à $\{r+1,\dots,p\}$, la sous-famille $\{x_1,\dots,x_r,x_i\}$ est liée et il existe donc des scalaires $\alpha_1,\dots,\alpha_r,\alpha_i$ non tous nuls tels que $\alpha_1x_1+\cdots+\alpha_rx_r+\alpha_ix_i=0_E$. Le coefficient α_i ne peut être nul, car sinon la liberté de la famille $\{x_1,\dots,x_r\}$ entraînerait la nullité de tous les coefficients. Le vecteur x_i peut donc s'écrire comme une combinaison linéaire des vecteurs $x_1,\dots,x_r$, dont on déduit que $\mathrm{Vect}\big(\{x_1,\dots,x_p\}\big)\subset\mathrm{Vect}\,(\{x_1,\dots,x_r\})$. L'inclusion réciproque étant clair, on a égalité entre ces deux sous-espaces vectoriels. La famille $\{x_1,\dots,x_r\}$ étant libre et génératice de $\mathrm{Vect}\big(\{x_1,\dots,x_p\}\big)$, elle en constitue une base et l'on a $\dim\big(\mathrm{Vect}\big(\{x_1,\dots,x_p\}\big)\big)=r$. □

Définition A.85 (sous-espace somme de deux sous-espaces vectoriels) *Soit E un espace vectoriel, A et B deux sous-espaces vectoriels de E. Le **sous-espace somme de A et B**, noté $A+B$, est l'esemble des vecteurs qui peuvent s'écrire comme la somme d'un vecteur de A et d'un vecteur de B.*

On peut généraliser cette définition au cas où l'on somme strictement plus de deux sous-espaces vectoriels $A_1,\dots,A_k$, avec k un entier naturel supérieur ou égal à 3, en posant que le sous-espace somme $A_1+\cdots+A_k$ est l'ensemble

$$\{x_1+\cdots+x_k\,|\,x_1\in A_1,\dots,\ x_k\in A_k\}.$$

On montre facilement qu'un sous-espace somme est un sous-espace vectoriel. C'est même le plus petit sous-espace vectoriel qui contienne les deux sous-espace vectoriels dont il est la somme.

Théorème A.86 (« formule de Grassman ») *Soit E un espace vectoriel. Si A et B deux sous-espaces vectoriels de dimension finie de E, alors les sous espaces $A+B$ et $A\cap B$ sont tous deux de dimension finie et on a*

$$\dim(A+B)=\dim(A)+\dim(B)-\dim(A\cap B).$$

DÉMONSTRATION. Puisque A et B sont de dimension finie, ils admettent tous deux une famille génératrice finie et la réunion de ces deux familles est une famille génératrice finie de $A+B$, qui est donc de dimension finie. Le sous-espace $A\cap B$ étant inclus dans A (et dans B), il est lui-même de dimension finie.

Soit $\mathscr{B}=\{e_1,\dots,e_n\}$ une base de $A\cap B$. En vertu du théorème de la base incomplète (voir le théorème A.78), il existe une base $\mathscr{B}_1=\{e_1,\dots,e_n,x_1,\dots,x_p\}$ de A contenant $\mathscr{B}$ et une base $\mathscr{B}_2=\{e_1,\dots,e_n,y_1,\dots,y_q\}$ de B contenant $\mathscr{B}$. La famille $\mathscr{B}_1\cup\mathscr{B}_2$ est ainsi génératrice de $A+B$. Elle est également libre. En effet, soit des scalaires $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_p$ et $\gamma_1,\dots,\gamma_q$ tels que

$$\sum_{i=1}^{n}\alpha_ie_i+\sum_{j=1}^{p}\beta_jx_j+\sum_{k=1}^{q}\gamma_ky_k=0_E.$$

On a alors

$$\sum_{k=1}^{q} \gamma_k y_k = -\left(\sum_{i=1}^{n} \alpha_i e_i + \sum_{j=1}^{p} \beta_j x_j \right).$$

Le membre de gauche de cette égalité est un vecteur de B en tant que combinaison linéaire de vecteurs de ce sous-espace et le membre de droite est un vecteur de A en tant que combinaison linéaire de vecteurs de ce sous-espace. Par conséquent, le vecteur $\sum_{k=1}^{q} \gamma_k y_k$ appartient à $A \cap B$ et on en déduit qu'il existe des scalaires $\lambda_1, \ldots, \lambda_n$ tels que

$$\sum_{i=1}^{q} \gamma_i y_i = \sum_{j=1}^{n} \lambda_j e_j.$$

La famille $\mathscr{B}_2$ étant une base, on déduit de l'égalité

$$\sum_{i=1}^{q} \gamma_i y_i - \sum_{j=1}^{n} \lambda_j e_j = 0_E$$

que les scalaires $\gamma_1, \ldots, \gamma_q$ et $\lambda_1, \ldots, \lambda_n$ sont nuls. L'égalité de départ devient alors

$$\sum_{i=1}^{n} \alpha_i e_i + \sum_{j=1}^{p} \beta_j x_j = 0_E,$$

d'où les coefficients $\alpha_1, \ldots, \alpha_n$ et $\beta_1, \ldots, \beta_p$ sont nuls, puisque $\mathscr{B}_1$ est une base. Il en résulte que $\mathscr{B}_1 \cup \mathscr{B}_2$ est une base de $A+B$, $\mathscr{B}_1$ est une base de A, $\mathscr{B}_2$ est une base de B et $\mathscr{B} = \mathscr{B}_1 \cap \mathscr{B}_2$ est une base de $A \cap B$. Il découle alors de la formule de la proposition A.55 que

$$\operatorname{card}(\mathscr{B}_1 \cup \mathscr{B}_2) = \operatorname{card}(\mathscr{B}_1) + \operatorname{card}(\mathscr{B}_2) - \operatorname{card}(\mathscr{B}_1 \cap \mathscr{B}_2),$$

dont on déduit l'égalité de l'énoncé par définition de la dimension. □

Définition A.87 (sous-espaces en somme directe) *Soit E un espace vectoriel. On dit que deux sous-espaces vectoriels A et B de E sont **en somme directe** si la propriété suivante est vérifiée*

$$\forall x \in A,\ \forall y \in B,\ x + y = 0_E \implies x = 0_E \text{ et } y = 0_E.$$

On note alors $A \oplus B$ au lieu de $A+B$ le sous-espace somme correspondant.

Là encore, on peut généraliser cette définition à strictement plus de deux sous-espaces vectoriels. On dit alors que $A_1, \ldots, A_k$, avec k un entier naturel supérieur ou égal à 3, sont en somme directe, et l'on note $A_1 \oplus \cdots \oplus A_k$ le sous-espace somme, lorsque

$$\forall x_1 \in A_1, \ldots,\ \forall x_k \in A_k,\ x_1 + \cdots + x_k = 0_E \implies x_1 = \cdots = x_k = 0_E.$$

On notera qu'il ne suffit pas que ces sous-espaces soient deux à deux en somme directe pour que tous soient en somme directe.

Proposition A.88 *Soit E un espace vectoriel de dimension finie, A et B deux sous-espaces vectoriels de E. Les asssertions suivantes sont équivalentes.*

i) A *et* B *en somme directe,*

ii) pour tout vecteur z de $A+B$, il existe un unique vecteur de A et un unique vecteur de B dont z est la somme,

iii) $A \cap B = \{0_E\}$,

iv) $\dim(A+B) = \dim(A) + \dim(B)$,

v) si $\mathscr{B}$ est une base de A et $\mathscr{C}$ est une base de B, $\mathscr{B} \cap \mathscr{C} = \varnothing$ et $\mathscr{B} \cup \mathscr{C}$ est une base de $A+B$.

DÉMONSTRATION. On montre tout d'abord que i équivaut à ii. Soit z un vecteur de $A+B$. Par définition, il existe un vecteur X de A et un vecteur y de B tels que $z = x + y$. S'il existe un autre couple de vecteurs x' de A et y' de B tel que $z = x' + y'$, alors on a $(x - x') + (y - y') = 0_E$, avec $x - x'$ appartenant à A et $y - y'$ appartenant à B. Les sous-espaces A et B étant en somme directe, on en déduit que $x - x' = y - y' = 0_E$ et l'on a bien unicité de l'écriture de z. Réciproquement, si $x + y = 0_E$ avec x appartenant à A et y appartenant à B, on dispose d'une écriture du vecteur nul de $A+B$ comme somme d'un vecteur de A et d'un vecteur de B. Par unicité de cette écriture, on obtient que $x = y = 0_E$ et les sous-espaces sont en somme directe.

On montre à présent que i et iii sont équivalentes. Soit x un vecteur de $A \cap B$. On a alors $x + 0_E = 0_E + x$, qui sont deux écritures d'un même vecteur de l'espace somme $A+B$. Les sous-espaces $A+B$ étant en somme directe et i impliquant ii, l'unicité de cette écriture montre que $x = 0_E$. Réciproquement, soient x un vecteur de A et y un vecteur de B tels que $x + y = 0_E$, d'où $x = -y$. On en déduit que x appartient à B et que y appartient à A, d'où $x = y = 0_E$ puisque $A \cap B = \{0_E\}$.

L'équivalence entre i et iv résulte de l'équivalence entre i et iii par application de la formule de Grassman.

Enfin, v implique iv, qui implique i. Il reste par conséquent à montrer que i implique v. Si $\mathscr{B}$ est une base de A, $\mathscr{C}$ est une base de B et s'il y a un vecteur dans $\mathscr{B} \cap \mathscr{C}$, alors ce dernier appartient à $A \cap B$ et il ne peut être nul puisqu'une famille contenant le vecteur nul est liée. Par conséquent, la famille $\mathscr{B} \cap \mathscr{C}$ est vide. Par ailleurs, il apparaît dans la preuve de la formule de Grassman (voir le théorème A.86) que l'union d'une base de A et d'un base de B contenant toutes deux une base de $A \cap B$ est une base de $A+B$. Une base de $A \cap B$ étant l'ensemble vide, les bases $\mathscr{B}$ et $\mathscr{C}$ font ici l'affaire et l'assertion est démontrée. □

Définition A.89 (supplémentaire d'un sous-espace vectoriel) *Soit E un espace vectoriel et A un sous-espace vectoriel de E. Un **supplémentaire de** A dans E est un sous-espace vectoriel S de E tel que $E = A \oplus S$.*

On prendra garde à ne pas confondre la notion de supplémentaire avec la notion ensembliste de complémentaire[2] (voir la définition A.9). En dimension finie, il découle d'une des assertions de la proposition ci-dessus que les éventuels supplémentaires d'un sous-espace A d'un espace vectoriel E sont tous de dimension $\dim(E) - \dim(A)$, appelée la **codimension** de A dans E.

A.2.6 Algèbre

On termine ce tour d'horizon sur les structures algébriques en introduisant un cas particulier d'*algèbre*.

Définition A.90 (algèbre sur un corps commutatif) *On appelle **algèbre sur un corps commutatif** $\mathbb{K}$ tout ensemble E non vide muni de deux lois de composition internes $+$ et $*$ et d'une loi de composition externe $\cdot$ à opérateurs dans $\mathbb{K}$ tels que*

- *$(E, +, *)$ est un anneau,*
- *$(E, +, \cdot)$ est un espace vectoriel sur $\mathbb{K}$,*
- *$\forall \lambda \in \mathbb{K}$ et $\forall (x, y) \in E^2$, $\lambda(x * y) = (\lambda x) * y = x * (\lambda y)$.*

Lorsque la loi $*$ est commutative, l'algèbre est dite *commutative*.

A.3 Applications linéaires

On considère à présent une classe d'applications entre deux espaces vectoriels qui respecte les opérations d'addition de vecteurs et de multiplication d'un vecteur par un scalaire, et étend par conséquent la notion de fonction linéaire en analyse réelle.

Définition A.91 (application linéaire) *Soit E et F deux espaces vectoriels sur un même corps $\mathbb{K}$ et u une application de E dans F. On dit que u est une **application linéaire**, ou **morphisme**, si*

$$\forall \lambda \in \mathbb{K},\ \forall (x, y) \in E^2,\ u(\lambda x + y) = \lambda u(x) + u(y).$$

*L'ensemble des applications linéaires de E dans F est noté $\mathscr{L}(E, F)$. Lorsque $F = \mathbb{K}$, on parle de **forme linéaire** et d'**endomorphisme** lorsque $E = F$.*

2. On pourra noter qu'on a unicité du complémentaire, mais généralement pas des supplémentaires, et que le complémentaire d'un sous-espace vectoriel n'est jamais un sous-espace vectoriel. Par ailleurs, l'intersection d'un sous-espace vectoriel avec un de ses supplémentaires n'est jamais vide, mais contient le vecteur nul (et uniquement ce vecteur). Enfin, la réunion d'un sous-espace vectoriel et d'un des ses supplémentaires n'est pas égale à tout l'espace, mais elle l'engendre.

On montre facilement que l'ensemble $\mathscr{L}(E,F)$ est un espace vectoriel. On note par ailleurs $\mathscr{L}(E)$ l'ensemble des endomorphismes de E.

Si E, F et G trois espaces vectoriels sur un même corps, u est une application de E dans F et v est une application linéaire de F dans G, il est également simple de montrer que l'application composée $v \circ u$ de E dans G est linéaire, ou encore, si l'application u est bijective, que l'application réciproque u^{-1} est linéaire de F dans E.

Proposition A.92 (image et image réciproque d'un sous-espace vectoriel par une application linéaire) *Soit u une application linéaire d'un espace E dans un espace F, A un sous-espace vectoriel de E et B un sous-espace vectoriel de F. L'image de A par u est un sous-espace vectoriel de F et l'image réciproque de B par u est un sous-espace vectoriel de E.*

Définitions A.93 (noyau et image d'une application linéaire) *Soit u une application linéaire d'un espace E dans un espace F. On appelle **noyau** (**kernel** en anglais) de u, et l'on note* $\ker(u)$*, l'ensemble*

$$\ker(u) = \{\boldsymbol{x} \in E \,|\, u(x) = 0_F\}.$$

*On appelle **image** de u, et l'on note* $\mathrm{Im}(u)$*, l'ensemble*

$$\mathrm{Im}(u) = \{y \in F \,|\, \exists x \in E,\ y = u(x)\}.$$

Il est aisé de montrer que, pour une application linéaire de d'un espace vectoriel E dans un espace F, le noyau est un sous-espace vectoriel de E et l'image est un sous-espace vectoriel de F.

Proposition A.94 (caractérisation de l'injectivité et de la surjectivité d'une application linéaire) *Soit u une application linéaire d'un espace E dans un espace F. L'application u injective si et seulement si* $\ker(u) = \{0_E\}$ *et surjective si et seulement si* $\mathrm{Im}(u) = F$.

DÉMONSTRATION. On suppose tout d'abord que u soit injective. Le vecteur 0_F possède alors un unique antécédent par u qui 0_E et donc $\ker(u) = \{0_E\}$. Réciproquement, si $\ker(u) = \{0_E\}$, on a

$$\forall (x,x') \in E^2,\ u(x) = u(x') \implies u(x-x') = 0_F \implies x - x' \in \ker(u) \implies x - x' = 0_E \iff x = x'$$

et l'application est injective.
Enfin, l'application u est surjective si et seulement si

$$\forall y \in F,\ \exists x \in E,\ u(x) = y,$$

ce qui est équivalent à $F = \mathrm{Im}(u)$. □

D'autres caractérisations de l'injectivité d'une application linéaire sont possibles, en voici une.

Proposition A.95 (injectivité d'une application linéaire et familles libres) *Une application linéaire d'un espace E dans un espace F est injective si et seulement si l'image de toute famille libre de E par cette application est une famille libre de F.*

DÉMONSTRATION. Soit u une application linéaire d'un espace E dans un espace F. On suppose tout d'abord que u est injective. Soit $\{x_i\}_{i\in I}$ une famille libre de E. On va vérifier que $\{u(x_i)\}_{i\in I}$ est une famille libre de F. Pour cela, il faut montrer que toute sous-famille de cette famille est libre. On considère ainsi une famille à p éléments $\{u(x_{i_1}), \ldots, u(x_{i_p})\}$ et on suppose que les scalaires $\lambda_1, \ldots, \lambda_p$ soient tels que $\sum_{k=1}^{p} \lambda_k u(x_{i_k}) = 0_F$. Par linéarité de u, on a alors $u\left(\sum_{k=1}^{p} \lambda_k x_{i_k}\right) = 0_F$, ce qui implique, par injectivité de u, que la combinaison linéaire $\sum_{k=1}^{p} \lambda_k x_{i_k}$ est nulle. On conclut alors par liberté de la famille.

Réciproquement, on suppose que l'image de toute famille libre par u soit libre. Si x est un vecteur non nul de E, la famille $\{x\}$ est libre et, par conséquent, la famille $\{u(x)\}$ est libre, ce qui n'est possible que si $u(x)$ est non nul. Ainsi, le seul vecteur x pour lequel $u(x) = 0_F$ est le vecteur nul de E. □

Pour une caractérisation alternative de la surjectivité, on aura besoin du résultat suivant.

Proposition A.96 (famille génératrice de l'image d'une application linéaire) *Soit u une application linéaire d'un espace E dans un espace F. Si $\{x_i\}_{i\in I}$ est une famille de vecteurs de E, alors $u(\mathrm{Vect}(\{x_i\}_{i\in I})) = \mathrm{Vect}(\{u(x_i)_{i\in I}\})$. En particulier, l'image d'une famille génératrice de E est une famille génératrice de l'image de u.*

Corollaire A.97 (surjectivité d'une application linéaire et familles génératrices) *Une application linéaire d'un espace E dans un espace F est surjective si et seulement si l'image de toute famille génératrice de E par cette application est une famille génératrice de F.*

DÉMONSTRATION. Soit u une application linéaire surjective d'un espace E dans un espace F et $\{x_i\}_{i\in I}$ une famille génératrice de E. Il découle alors de la proposition A.96 que $\text{Vect}\left(\{u(x_i)\}_{i\in I}\right) = u\left(\text{Vect}\left(\{x_i\}_{i=1,\dots,p}\right)\right) = u(E) = F$.

Réciproquement, si l'image de toute famille génératrice de E par u est une famille génératrice de F, on a pour une famille génératrice donnée $\{x_i\}_{i\in I}$, $F = \text{Vect}\left(\{u(x_i)\}_{i\in I}\right)$ et, en vertu de la proposition A.96, $F = u\left(\text{Vect}\left(\{x_i\}_{i=1,\dots,p}\right)\right) = u(E)$, d'où u est surjective. □

On déduit aisément de la proposition A.95 et du dernier corollaire qu'une application linéaire d'un espace E dans un espace F est bijective si et seulement si l'image de toute base de E par cette application est une base de F.

Théorème A.98 (caractérisation d'une application linéaire par les images des vecteurs d'une base) *Soit n un entier naturel non nul, E et F deux espaces vectoriels sur un même corps, E étant supposé de dimension finie égale à n, $\mathscr{B} = \{e_1, \dots, e_n\}$ une base de E. Étant donnée une famille $\{u_1, \dots, u_n\}$ de vecteurs de F, il existe une unique application linéaire u de E dans F telle que*

$$\forall i \in \{1, \dots, n\},\ u(e_i) = u_i.$$

Autrement dit, une application linéaire est entièrement définie par les images des vecteurs d'une base de l'espace de départ.

DÉMONSTRATION. Il suffit de constater que la propriété de linéarité fait qu'il est nécessaire et suffisant que l'application recherchée soit définie par

$$\forall x \in E,\ x = \sum_{i=1}^{n} x_i e_i,\ u(x) = \sum_{i=1}^{n} x_i u_i.$$

□

Définition A.99 (rang d'une application linéaire) *Une application linéaire u entre deux espaces vectoriels est dite **de rang fini** si le sous-espace $\text{Im}(u)$ est de dimension finie, sinon elle est dite **de rang infini**. Lorsqu'elle est de rang fini, on appelle **rang** de u, et on note $\text{rang}(u)$, la dimension de $\text{Im}(u)$.*

Cette définition est cohérente avec celle du rang d'une famille de vecteurs. En effet, si $\{e_i\}$ est une base de E, on a en vertu de la proposition A.95 que le rang d'une application linéaire d'un espace E dans un espace F est égal au rang de l'image de cette base par l'application.

Définition A.100 (isomorphisme) *Soit E et F deux espaces vectoriels. Une l'application linéaire bijective de E dans F est appelée un **isomorphisme entre** E **et** F, ou encore **automorphisme** si $E = F$.*

Deux espaces vectoriels sont dits *isomorphes* s'il existe un isomorphisme entre eux.

L'ensemble des automorphismes d'un espace vectoriel E est appelé le *groupe linéaire de E*, noté $GL(E)$. Il constitue en effet un groupe (voir la sous-section A.2.2) pour la composition d'applications.

Théorème A.101 *Soit E et F deux espaces vectoriels de dimension finie sur un même corps $\mathbb{K}$. L'espace $\mathscr{L}(E,F)$ est de dimension finie et*

$$\dim(\mathscr{L}(E,F)) = \dim(E)\dim(F).$$

DÉMONSTRATION. On considère une base $\mathscr{B} = \{e_1, \dots, e_m\}$ de E et une base $\mathscr{C} = \{f_1, \dots, f_n\}$ de F. Soit U la famille $\{u_{i,j},\ i \in \{1, \dots, m\},\ j \in \{1, \dots, n\}\}$ d'applications de $\mathscr{L}(E,F)$ définies par la donnée des images de vecteurs de $\mathscr{B}$ de la manière suivante

$$\forall i \in \{1, \dots, m\},\ \forall j \in \{1, \dots, n\},\ \forall k \in \{1, \dots, m\},\ u_{i,j}(e_k) = \delta_{ik} f_j,$$

où δ_{ik} désigne le symbole de Kronecker. Cette famille est une base de $\mathscr{L}(E,F)$. En effet, si on a $\sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{i,j} u_{i,j} = 0_{\mathscr{L}(E,F)}$, alors il vient

$$\forall k \in \{1, \dots, m\},\ \sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{i,j} u_{i,j}(e_k) = \sum_{j=1}^{n} \lambda_{k,j} f_j = 0_F,$$

dont on déduit que les scalaires $\lambda_{k,j}$ sont nuls puisque $\mathscr{C}$ est une famille libre. Par ailleurs, toute application u de $\mathscr{L}(E,F)$ étant définie par la donnée par ses images des vecteurs de $\mathscr{B}$, on peut écrire

$$\forall k \in \{1,\dots,m\},\ u(e_k) = \sum_{j=1}^{n} a_{k,j} f_j = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{k,j} u_{i,j}(e_k) = \left(\sum_{i=1}^{m}\sum_{j=1}^{n} a_{k,j} u_{i,j}\right)(e_k),$$

où, pour tout couple d'entier (k,j) de $\{1,\dots,m\}\times\{1,\dots,n\}$ le scalaire $a_{k,j}$ est la coordonnée selon f_j du vecteur $u(e_k)$. La famille est donc à la fois libre et génératrice : c'est bien une base. L'espace $\mathscr{L}(E,F)$ est donc de dimension finie et sa dimension est égale au nombre d'éléments dans la base considérée ci-dessus. □

Le résultat suivant, dit *théorème du rang*, lie les dimensions respectives du noyau et de l'image d'une application linéaire.

Théorème A.102 (« théorème du rang ») *Soit E et F deux espaces vectoriels de dimension finie sur un même corps $\mathbb{K}$. Pour toute application u de $\mathscr{L}(E,F)$, on a*

$$\dim(\ker(u)) + \dim(\mathrm{Im}(u)) = \dim(E).$$

DÉMONSTRATION. On note $n = \dim(E)$. Le sous-espace vectoriel $\ker(u)$ de E admet au moins une base $\{e_i\}_{i=1,\dots,p}$ que l'on peut compléter en une base $\{e_i\}_{i=1,\dots,n}$ de E. On va montrer que $\{u(e_{p+1}),\dots,u(e_n)\}$ est une base de $\mathrm{Im}(u)$. Les vecteurs $u(e_i)$, $p+1 \le i \le n$, sont à l'évidence des éléments de $\mathrm{Im}(u)$. Soit des scalaires $\lambda_{p+1},\dots,\lambda_n$ tels que

$$\sum_{i=p+1}^{n} \lambda_i\, u(e_i) = 0_F.$$

On a $u\left(\sum_{i=p+1}^{n} \lambda_i\, e_i\right) = 0_F$, et $\sum_{i=p+1}^{n} \lambda_i\, e_i$ appartient donc à $\ker(u)$. Il existe par conséquent des scalaires $\mu_1,\dots,\mu_p$ tels que $\sum_{i=p+1}^{n} \lambda_i\, e_i = \sum_{i=1}^{p} \mu_i\, e_i$, soit encore $\mu_1\, e_1 + \dots + \mu_p\, e_p - \lambda_{p+1}\, e_{p+1} - \dots - \lambda_n\, e_n = 0_E$. Comme la famille $\{e_1,\dots,e_p\}$ est libre, on en déduit que $\lambda_{p+1} = \dots = \lambda_n = 0$, ce qui montre que $\{u(e_{p+1}),\dots,u(e_n)\}$ est libre.

Soit à présent un élément y de $\mathrm{Im}(u)$. Par définition, il existe un vecteur x dans E tel que $y = u(x)$. Puisque la famille $\{e_1,\dots,e_n\}$ engendre E, on peut trouver des scalaires $\alpha_1,\dots,\alpha_n$ tels que $x = \sum_{i=1}^{n} \alpha_i\, e_i$. On a alors

$$y = u(x) = u\left(\sum_{i=1}^{n} \alpha_i\, e_i\right) = \sum_{i=1}^{n} \alpha_i\, u(e_i) = \sum_{i=p+1}^{n} \alpha_i\, u(e_i),$$

les vecteurs $e_1,\dots,e_p$ appartenant au noyau de u. La famille $\{u(e_{p+1}),\dots,u(e_n)\}$ engendre donc $\mathrm{Im}(u)$, c'est une base de ce sous-espace de F et l'on conclut alors que

$$\dim(\mathrm{Im}(u)) = n - p = \dim E - \dim(\ker(u)).$$

□

Corollaire A.103 (caractérisation des isomorphismes entre espaces de dimension finie) *Soit E et F deux espaces vectoriels de dimension finie sur un même corps $\mathbb{K}$ et u une application linéaire de E dans F. On a équivalence entre les assertions suivantes :*

i) *u est un isomorphisme,*

ii) *u est injective et $\dim(E) = \dim(F)$,*

iii) *u est surjective et $\dim(E) = \dim(F)$.*

DÉMONSTRATION. Si l'application u est un isomorphisme de E dans F, alors elle est surjective et injective, c'est-à-dire que, d'après la proposition A.94, $\ker(u) = \{0_E\}$ et $\mathrm{Im}(u) = F$. Par le théorème du rang, on a donc $\dim(E) = \dim(\ker(u)) + \dim(\mathrm{Im}(u)) = \dim(F)$.

Réciproquement, si l'application u est injective et que $\dim(E) = \dim(F)$, alors $\ker(u) = \{0_E\}$ et, par le théorème du rang, $\dim(\mathrm{Im}(u)) = \dim(F)$. Puisque $\mathrm{Im}(u)$ est un sous-espace vectoriel de F, on en déduit que $\mathrm{Im}(u) = F$ et donc u est surjective, ce qui en fait un isomorphisme. De même, si l'application u est surjective et que $\dim(E) = \dim(F)$, alors $\dim(\ker(u)) = 0$ par le théorème du rang, et donc u est injective, ce qui en fait un isomorphisme. □

Proposition A.104 (conservation du rang par un isomorphisme) *Soit E et F deux espaces vectoriels de dimension finie sur un même corps $\mathbb{K}$ et u un isomorphisme de E dans F. Pour toute famille $\{x_1,\dots,x_n\}$ de vecteurs de E, on a* $\operatorname{rang}(\{x_1,\dots,x_n\}) = \operatorname{rang}(\{u(x_1),\dots,u(x_n)\})$.

DÉMONSTRATION. Soit p le rang de la famille $\{x_1,\dots,x_n\}$ et $\{e_1,\dots,e_p\}$ une base de $\operatorname{Vect}(\{x_1,\dots,x_n\})$. Il suffit de montrer que la famille $\{u(e_1),\dots,u(e_p)\}$ est une base de $\operatorname{Vect}(\{u(x_1),\dots,u(x_n)\})$. Soit y un vecteur de $\operatorname{Vect}(\{u(e_1),\dots,u(e_p)\})$. Il existe des scalaires $\alpha_1,\dots,\alpha_p$ tels que

$$y = \alpha_1 u(e_1) + \cdots + \alpha_p u(e_p) = u(\alpha_1 e_1 + \cdots + \alpha_p e_p).$$

Puisque le vecteur $\alpha_1 e_1 + \cdots + \alpha_p e_p$ appartient à $\operatorname{Vect}(\{x_1,\dots,x_n\})$, il peut s'écrire comme une combinaison linéaire des vecteurs $x_1,\dots,x_n$ et son image par u est donc une combinaison linéaire des vecteurs $u(x_1),\dots,u(x_n)$. À ce titre, le vecteur y appartient à $\operatorname{Vect}(\{u(x_1),\dots,u(x_n)\})$. Soit à présent z un vecteur de $\operatorname{Vect}(\{u(x_1),\dots,u(x_n)\})$. Il existe des scalaires $\beta_1,\dots,\beta_n$ tels que

$$z = \beta_1 u(x_1) + \cdots + \beta_n u(x_n) = u(\beta_1 x_1 + \cdots + \beta_p x_n).$$

Comme le vecteur $\beta_1 x_1 + \cdots + \beta_p x_n$ appartient à $\operatorname{Vect}(\{x_1,\dots,x_n\})$, on peut l'écrire d'unique manière comme une combinaison linéaire des éléments de la base $\{e_1,\dots,e_p\}$ et son image par u est donc une combinaison linéaire des vecteurs $u(e_1),\dots,u(e_p)$. En d'autres mots, le vecteur z appartient à $\operatorname{Vect}(\{u(e_1),\dots,u(e_p)\})$.

La famille $\{u(e_1),\dots,u(e_p)\}$ est par ailleurs libre puisque, par injectivité de u, on a

$$\gamma_1 u(e_1) + \cdots + \gamma_p u(e_p) = 0_F \iff u(\gamma_1 e_1 + \cdots + \gamma_p e_p) = 0_F \iff \gamma_1 e_1 + \cdots + \gamma_p e_p = 0_E,$$

ce qui implique que les scalaires $\gamma_1,\dots,\gamma_p$ sont tous nuls, puisque la famille $\{e_1,\dots,e_p\}$ est une base. Ainsi, la famille $\{u(e_1),\dots,u(e_p)\}$ est bien une base de $\operatorname{Vect}(\{u(x_1),\dots,u(x_n)\})$, et l'on a par conséquent

$$\operatorname{rang}(\{u(x_1),\dots,u(x_n)\}) = \dim\big(\operatorname{Vect}(\{u(e_1),\dots,u(e_p)\})\big) = \dim\big(\operatorname{Vect}(\{e_1,\dots,e_p\})\big) = \operatorname{rang}(\{x_1,\dots,x_n\}).$$

□

A.4 Matrices

Soit m et n deux entiers strictement positifs. Une **matrice**[3] M **à** n **lignes et** m **colonnes à coefficients dans un corps** $\mathbb{K}$ est une application définie sur l'ensemble $\{1,\dots,n\}\times\{1,\dots,m\}$ à valeurs dans $\mathbb{K}$, représentée par le tableau suivant

$$M = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1m} \\ m_{21} & m_{22} & \dots & m_{2m} \\ \vdots & \vdots & & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nm} \end{pmatrix}.$$

Les mn scalaires m_{ij}, $i = 1,\dots,n$, $j = 1,\dots,m$, sont appelés les **coefficients** ou **éléments** de la matrice M, le premier indice i étant celui de la **ligne** de la matrice à laquelle appartient l'élément considéré et le second j étant celui de la **colonne**. Ainsi, l'ensemble des coefficients $m_{i1},\dots,m_{im}$ forme la i^{e} ligne de la matrice et l'ensemble $m_{1j},\dots,m_{nj}$ la j^{e} colonne. Les éléments d'une matrice M sont notés $(M)_{ij}$ ou, plus simplement, m_{ij} lorsque qu'aucune confusion ou ambiguïté n'est possible.

On note $M_{n,m}(\mathbb{K})$ l'ensemble des matrices à n lignes et m colonnes dont les coefficients appartiennent à $\mathbb{K}$. Une matrice est dite **réelle** ou **complexe** selon que ses éléments sont dans $\mathbb{R}$ ou $\mathbb{C}$. Si $m = n$, la matrice est dite **carrée d'ordre** n et l'on note $M_n(\mathbb{K})$ l'ensemble des matrices correspondant. Lorsque $m \neq n$, on parle de matrice **rectangulaire**.

On appelle **diagonale principale** d'une matrice M de $M_{n,m}(\mathbb{K})$ l'ensemble des coefficients m_{ii}, pour i appartenant à $\{1,\dots,\min(m,n)\}$. Cette diagonale divise la matrice en une partie **sur-diagonale**, composée des éléments

3. L'introduction de ce terme est attribuée à James Joseph Sylvester, son plus ancien ancien usage connu étant dans la publication [Syl50], à la page 369, où il désigne un objet donnant naissance aux déterminants de sous-matrices carrées appelés mineurs : *"For this purpose we must commence, not with a square, but with an oblong arrangement of terms consisting, suppose, of m lines and n columns. This will not in itself represent a determinant, but is, as it were, a Matrix out of which we may form various systems of determinants by fixing upon a number p, and selecting at will p lines and p columns, the squares corresponding to which may be termed determinants of the pth order."*.

dont l'indice de ligne est strictement inférieur à l'indice de colonne, et une partie **sous-diagonale** formée des éléments pour lesquels l'indice de ligne est strictement supérieur à l'indice de colonne.

Étant donné une matrice M de $M_{n,m}(\mathbb{R})$, on note $M^\top$ la matrice de $M_{m,n}(\mathbb{R})$ dite **transposée**[4] de M telle que

$$(M^\top)_{ij} = (M)_{ji},\ 1 \leq i \leq m,\ 1 \leq j \leq n.$$

On notera que l'on a $(M^\top)^\top = M$. De même, étant donné une matrice M de $M_{n,m}(\mathbb{C})$, on note M^* la matrice de $M_{m,n}(\mathbb{C})$ dite **adjointe**, ou **transconjuguée**) de M telle que

$$(M^*)_{ij} = \overline{(M)_{ji}},\ 1 \leq i \leq m,\ 1 \leq j \leq n,$$

le scalaire $\overline{z}$ désignant le nombre complexe conjugué du nombre complexe z. On a alors $(M^*)^* = M$.

Par abus de langage, on appelle **vecteur ligne** (resp. **vecteur colonne**) une matrice n'ayant qu'une ligne (resp. colonne). Un vecteur colonne à n lignes représente un vecteur d'un espace vectoriel de dimension n écrit dans une base donnée de cet espace, alors qu'un vecteur ligne à n colonne est la matrice représentative d'une forme linéaire d'un espace vectoriel de dimension n, dans une base donnée de cet espace.

Il est souvent utile de considérer un sous-ensemble de coefficients d'une matrice. On introduit pour cette raison la notion de *sous-matrice*.

Définition A.105 (sous-matrice) *Soit M une matrice de $M_{n,m}(\mathbb{K})$. Étant donnés un sous-ensemble ordonné $I = \{i_1, \ldots, i_p\}$ d'éléments de $\{1, \ldots, n\}$ et un sous-ensemble ordonné $J = \{j_1, \ldots, j_q\}$ d'éléments de $\{1, \ldots, m\}$, la matrice de $M_{p,q}(\mathbb{K})$, notée $M_{I,J}$ et ayant pour coefficients*

$$(M_{I,J})_{kl} = m_{i_k j_l},\ k = 1, \ldots, p,\ l = 1, \ldots, q,$$

*est appelée une **sous-matrice** de M.*

Il est courant d'associer à une matrice une partition en sous-matrices.

Définition A.106 (matrice par blocs) *Une matrice M de $M_{n,m}(\mathbb{K})$ est dite **par blocs** ou **partitionnée** si elle s'écrit*

$$M = \begin{pmatrix} M_{11} & M_{12} & \ldots & M_{1p} \\ M_{21} & M_{22} & \ldots & M_{2p} \\ \vdots & \vdots & & \vdots \\ M_{q1} & M_{q2} & \ldots & M_{qp} \end{pmatrix},$$

*où les **blocs** M_{ij}, $i = 1, \ldots, q$, $j = 1, \ldots, p$, sont des sous-matrices de M.*

L'intérêt de telles partitions réside dans le fait que certaines opérations définies sur les matrices restent formellement les mêmes avec des matrices par blocs, les coefficients respectifs des matrices étant remplacés par leurs sous-matrices, sous réserve que les dimensions des diverses sous-matrices respectent des conditions permettant que les opérations soient possibles (on parle alors de *partitions compatibles*).

A.4.1 Opérations sur les matrices

On introduit quelques opérations essentielles définies sur les matrices.

Définition A.107 (égalité de matrices) *Soit M et N deux matrices de $M_{n,m}(\mathbb{K})$. On dit que M est **égale** à N si $m_{ij} = n_{ij}$ pour $i = 1, \ldots, n$, $j = 1, \ldots, m$.*

Définition A.108 (somme de matrices) *Soit M et N deux matrices de $M_{n,m}(\mathbb{K})$. On appelle **somme** des matrices M et N la matrice de $M_{n,m}(\mathbb{K})$, notée $M+N$, dont les coefficients sont $(M+N)_{ij} = m_{ij} + n_{ij}$, $i = 1, \ldots, n$, $j = 1, \ldots, m$.*

L'élément neutre pour la somme de matrices de $M_{n,m}(\mathbb{K})$ est la **matrice nulle**, notée $0_{n,m}$, dont les coefficients sont tous égaux à zéro. On a par ailleurs

$$\forall M \in M_{n,m}(\mathbb{K}),\ \forall N \in M_{n,m}(\mathbb{K}),\ (M+N)^\top = M^\top + N^\top \text{ et } (M+N)^* = M^* + N^*.$$

4. On peut aussi définir la matrice transposée d'une matrice à coefficients complexes, mais c'est plutôt la notion de matrice *adjointe* qui est d'intérêt dans ce cas.

Définition A.109 (multiplication d'une matrice par un scalaire) *Soit M une matrice de $M_{n,m}(\mathbb{K})$ et α un scalaire. Le résultat de la* ***multiplication de la matrice*** *M* ***par le scalaire*** *α est la matrice de $M_{n,m}(\mathbb{K})$, notée αM, dont les coefficients sont $(\alpha M)_{ij} = \alpha\, m_{ij}$, $i = 1,\dots,n$, $j = 1,\dots,m$.*

On a

$$\forall \alpha \in \mathbb{K},\ \forall M \in M_{n,m}(\mathbb{K}),\ (\alpha M)^\top = \alpha M^\top \text{ et } (\alpha M)^* = \overline{\alpha} M^*,$$

ce qui permet de conclure que la transposition est une application *linéaire*, alors que la transconjugaison est une application *anti-linéaire*.

Muni des deux dernières opérations, l'ensemble $M_{n,m}(\mathbb{K})$ est un espace vectoriel sur $\mathbb{K}$. La **base canonique de** $M_{n,m}(\mathbb{K})$ l'ensemble des mn matrices E_{kl}, $k = 1,\dots,n$, $l = 1,\dots,m$, de $M_{n,m}(\mathbb{K})$ dont les éléments sont définis par

$$(E_{kl})_{ij} = \delta_{ik}\delta_{jl} = \begin{cases} 0 & \text{si } i \neq k \text{ ou } j \neq l \\ 1 & \text{si } i = k \text{ et } j = l \end{cases},\ i = 1,\dots,n,\ j = 1,\dots,m,$$

où δ_{ij} désigne le *symbole de Kronecker*,

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases} \tag{A.1}$$

Définition A.110 (produit de matrices) *Soit M une matrice de $M_{n,p}(\mathbb{K})$ et N une matrice de $M_{p,m}(\mathbb{K})$. Le* ***produit*** *des matrices M et N est la matrice de $M_{n,m}(\mathbb{K})$, notée MN, dont les coefficients sont*

$$(MN)_{ij} = \sum_{k=1}^{p} m_{ik} n_{kj},\ i = 1,\dots,n, j = 1,\dots,m. \tag{A.2}$$

Le produit de matrices est associatif et distributif par rapport à la somme de matrices.

Dans le cas de matrices *carrées*, on dit que deux matrices M et N **commutent** (pour le produit de matrices) si $MN = NM$. Toujours dans ce cas, l'élément neutre pour le produit de matrices d'ordre n est la matrice carrée, appelée **matrice identité**, notée I_n et définie par

$$I_n = (\delta_{ij})_{1 \leq i,j \leq n}.$$

Cette matrice est, par définition, la seule matrice d'ordre n telle que $MI_n = I_n M = M$ pour toute matrice A d'ordre n. Muni de la multiplication par un scalaire, de la somme et du produit de matrices l'ensemble $M_n(\mathbb{K})$ est une algèbre sur $\mathbb{K}$, en général non commutative, comme le montre l'exemple suivant.

Exemple de non-commutativité du produit de matrices carrées. Soit $M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $N = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$. On a

$$MN = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 4 \\ 0 & 0 \end{pmatrix} = NM.$$

Si M est une matrice carrée d'ordre n et p un entier, on définit la matrice M^p comme étant le produit de M par elle-même répété $p-1$ fois, en posant par convention $M^0 = I_n$. On note que l'on a

$$\forall M \in M_{n,p}(\mathbb{K}),\ \forall N \in M_{p,m}(\mathbb{K}),\ (MN)^\top = N^\top M^\top \text{ et } (MN)^* = N^* M^*.$$

Toutes les opérations précédemment définies s'étendent au cas de matrices par blocs, pourvu que la taille de chacun des blocs soit telle que l'opération considérée soit correctement définie. On a notamment le résultat suivant.

Lemme A.111 (produit de matrices par blocs) *Soit M et N deux matrices de tailles compatibles pour effectuer le produit MN. Si M admet une décomposition en blocs M_{ik}, $i = 1,\dots,q$, $k = 1,\dots,r$, possédant respectivement r_i lignes et s_k colonnes, et N admet une décomposition compatible en blocs N_{kj}, $k = 1,\dots,r$, $j = 1,\dots,p$, possédant respectivement s_k lignes et t_j colonnes, alors le produit MN peut aussi s'écrire comme une matrice par blocs,*

$$MN = \begin{pmatrix} \sum_{k=1}^r M_{1k}N_{k1} & \dots & \sum_{k=1}^r M_{1k}N_{kp} \\ \vdots & & \vdots \\ \sum_{k=1}^r M_{qk}N_{k1} & \dots & \sum_{k=1}^r M_{qk}N_{kp} \end{pmatrix}.$$

Exemple. Soit les matrices carrées M et N d'ordre n admettant les partitions compatibles

$$M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \text{ et } N = \begin{pmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{pmatrix}.$$

On a alors

$$MN = \begin{pmatrix} M_{11}N_{11} + M_{12}N_{21} & M_{11}N_{12} + M_{12}N_{22} \\ M_{21}N_{11} + M_{22}N_{21} & M_{21}N_{12} + M_{22}N_{22} \end{pmatrix}.$$

Enfin, il existe d'autres types de produit que le produit « usuel » de matrices introduit ci-dessus, notamment le produit coefficient par coefficient de deux matrices de même dimension ou encore le produit tensoriel de deux matrices quelconques.

Définition A.112 (« produit d'Hadamard » ou « produit de Schur ») *Soit M et N deux matrices de $M_{n,m}(\mathbb{K})$. Le **produit d'Hadamard** des matrices M et N est la matrice de $M_{n,m}(\mathbb{K})$, notée $M \circ N$, dont les coefficients sont $(M \circ N)_{ij} = m_{ij} n_{ij}$, $i = 1, \ldots, n$, $j = 1, \ldots, m$.*

Définition A.113 (« produit de Kronecker ») *Soit M une matrice de $M_{n,m}(\mathbb{K})$ et N une matrice de $M_{p,q}(\mathbb{K})$. Le **produit de Kronecker** des matrices M et N est la matrice de $M_{np,mq}(\mathbb{K})$, notée $M \otimes N$, écrite par blocs, possédant chacun p lignes et q colonnes, suivante*

$$M \otimes N = \begin{pmatrix} m_{11}N & \ldots & m_{1m}N \\ \vdots & & \vdots \\ m_{n1}N & \ldots & m_{n1}N \end{pmatrix}.$$

A.4.2 Inverse d'une matrice

Définitions A.114 *Soit M une matrice d'ordre n. On dit que M est **inversible** s'il existe une (unique) matrice, notée M^{-1} et appelée la **matrice inverse** de M, telle que $MM^{-1} = M^{-1}M = I_n$. Une matrice non inversible est dite **singulière**.*

Il ressort de cette définition qu'une matrice inversible est la matrice d'un endomorphisme bijectif. Par conséquent, une matrice M d'ordre n est inversible si et seulement si $\text{rang}(M) = n$.

Si une matrice M est inversible, son inverse est évidemment inversible et $(M^{-1})^{-1} = M$. Par ailleurs, si M et N sont deux matrices inversibles de même ordre, on a les égalités suivantes :

$$(MN)^{-1} = N^{-1}M^{-1},\ (M^\top)^{-1} = (M^{-1})^\top,\ (M^*)^{-1} = (M^{-1})^* \text{ et, } \forall \alpha \in \mathbb{K}^*,\ (\alpha M)^{-1} = \frac{1}{\alpha} M^{-1}.$$

L'ensemble des matrices inversibles de $M_n(\mathbb{K})$, muni du produit matriciel, est appelé le *groupe général linéaire* et noté $GL(n, \mathbb{R})$.

A.4.3 Matrices équivalentes et matrices semblables

Définition A.115 (matrices équivalentes) *Soit m et n deux entiers naturels non nuls. Deux matrices A et B à m lignes et n colonnes sont dites **équivalentes** s'il existe deux matrices inversibles P et Q, respectivement d'ordre m et n, telles que $B = PAQ$.*

L'équivalence entre matrices au sens de cette définition est effectivement une relation d'équivalence, que l'on peut interpréter en disant que deux matrices sont équivalentes si et seulement si elles représentent une même application linéaire dans des bases différentes, les matrices P et Q de la définition pouvant être vues comme des matrices de passage. De même, deux matrices sont équivalentes si et seulement si elles ont même rang.

Pour des matrices carrées, il est plus courant de faire appel à la définition suivante.

Définition A.116 (matrices semblables) *On dit que deux matrices A et B d'ordre n sont **semblables** s'il existe une matrice inversible P telle que*

$$A = PBP^{-1}.$$

Il est clair que des matrices semblables sont équivalentes.

A.4.4 Trace et déterminant d'une matrice

On introduit à présent les notions de *trace* et de *déterminant* d'une matrice carrée.

Définition A.117 (trace d'une matrice) *La **trace** d'une matrice M d'ordre n, notée* $\mathrm{tr}(M)$*, est la somme de ses coefficients diagonaux,*

$$\mathrm{tr}(M) = \sum_{i=1}^{n} m_{ii}.$$

On montre facilement les relations

$$\forall \alpha \in \mathbb{K},\ \forall M \in M_n(\mathbb{K}),\ \forall N \in M_n(\mathbb{K}),\ \mathrm{tr}(\alpha M + N) = \alpha\,\mathrm{tr}(M) + \mathrm{tr}(N) \text{ et } \mathrm{tr}(MN) = \mathrm{tr}(NM),$$

la première prouvant que l'application de $M_n(\mathbb{K})$ dans $\mathbb{K}$ qui à une matrice M d'ordre n associe $\mathrm{tr}(M)$ est linéaire, la seconde ayant comme conséquence le fait que des matrices semblables (voir la définition A.116) possèdent la même trace. En effet, pour toute matrice M et tout matrice inversible P de même ordre, on a

$$\mathrm{tr}(PMP^{-1}) = \mathrm{tr}(P^{-1}PM) = \mathrm{tr}(M).$$

Définition A.118 (déterminant d'une matrice) *On appelle **déterminant** d'une matrice M d'ordre n le scalaire défini par la **formule de Leibniz***

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i)i},$$

où $\varepsilon(\sigma)$ désigne la signature d'une permutation[5] *σ de $\mathfrak{S}_n$.*

Par propriété des permutations, on a $\det(M^\top) = \det(M)$ et $\det(M^*) = \overline{\det(M)}$, pour toute matrice M d'ordre n.

On peut voir le déterminant d'une matrice M d'ordre n comme une forme des n colonnes (ou des n lignes, puisque $\det(M) = \det(M^\top)$) de cette matrice,

$$\det(M) = \det(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_n),$$

où $(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_n)$ est la famille formée par les colonnes de M, qui est *multilinéaire*, c'est-à-dire linéaire en chacune de ses n variables. En particulier, multiplier une colonne de M par un scalaire α multiplie le déterminant par ce scalaire. On a ainsi

$$\forall \alpha \in \mathbb{K},\ \forall M \in M_n(\mathbb{K}),\ \det(\alpha M) = \alpha^n \det(M).$$

Cette forme est de plus *alternée* : échanger deux colonnes (ou deux lignes) de M entre elles entraîne la multiplication de son déterminant par -1 et si deux colonnes (ou deux lignes) sont égales ou, plus généralement, si les colonnes (ou les lignes) de M vérifient une relation non triviale de dépendance linéaire, le déterminant de M est nul.

Il en résulte qu'ajouter à une colonne (resp. une ligne) d'une matrice une combinaison linéaire des autres colonnes (resp. lignes) ne modifie pas le déterminant de cette matrice. Ces dernières propriétés expliquent à elles seules le rôle essentiel que joue le déterminant en algèbre linéaire.

Enfin, le déterminant est un *morphisme de groupes*, c'est-à-dire une application entre deux groupes respectant la structure de ces derniers, du groupe linéaire $GL(n, \mathbb{K})$ des matrices inversibles d'ordre n dans $\mathbb{K}^*$ (muni de la multiplication). Ainsi, si M et N sont deux matrices d'ordre n, on a

$$\det(MN) = \det(NM) = \det(M)\det(N),$$

et, si M est inversible,

$$\det(M^{-1}) = \frac{1}{\det(M)},$$

ces propriétés permettant de prouver que des matrices semblables ont le même déterminant. Tout comme la trace, le déterminant est un *invariant de similitude*.

5. Rappelons qu'une permutation est une bijection d'un ensemble dans lui-même (voir la sous-section A.1.3). On note $\mathfrak{S}_n$ le groupe (pour la loi de composition $\circ$) des permutations de l'ensemble $\{1, \ldots, n\}$, avec n un entier naturel non nul. La *signature* d'une permutation σ de $\mathfrak{S}_n$ est le nombre, égal à 1 ou -1, défini par

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Définition A.119 (mineur d'une matrice) *Soit M une matrice de $M_{n,m}(\mathbb{K})$ et p un entier strictement positif inférieur à m et à n. On appelle* ***mineur d'ordre*** *p de M le déterminant de n'importe quelle sous-matrice de M d'ordre p obtenue en éliminant $n-p$ lignes et $m-p$ colonnes.*

Étant donnés une matrice M de $M_{n,m}(\mathbb{K})$, un sous-ensemble I de p éléments de $\{1,\dots,m\}$ et un sous-ensemble J de p éléments $\{1,\dots,n\}$, le scalaire $\det(A_{I,J})$ est un mineur d'ordre p de M. Lorsque $I=J$, on dit que ce mineur est un *mineur principal* de M et, si la partie I est de plus de la forme $\{1,\dots,p\}$, que c'est un mineur principal *dominant*.

La démonstration du résultat suivant est immédiate.

Proposition A.120 *Le rang d'une matrice est égal au plus grand ordre d'un mineur non nul de cette matrice.*

On déduit de cette caractérisation et des propriétés du déterminant que $\operatorname{rang}(M)=\operatorname{rang}(M^\top)=\operatorname{rang}(M^*)$.

Définitions A.121 (cofacteur et comatrice) *Soit M une matrice d'ordre n. On appelle* ***cofacteur*** *associé à l'élément m_{ij} de M, avec (i,j) appartenant à $\{1,\dots,n\}^2$, le mineur d'ordre $n-1$ de la matrice obtenue par suppression de la i^e et de la j^e colonne de M, multiplié par le facteur $(-1)^{i+j}$, c'est-à-dire*

$$\operatorname{cof}_{ij}(M)=(-1)^{i+j}\begin{vmatrix} m_{11} & \dots & m_{1j-1} & m_{1j+1} & \dots & m_{1n}\\ \vdots & & \vdots & \vdots & & \vdots\\ m_{i-11} & \dots & m_{i-1j-1} & m_{i-1j+1} & \dots & m_{i-1n}\\ m_{i+11} & \dots & m_{i+1j-1} & m_{i+1j+1} & \dots & m_{i+1n}\\ \vdots & & \vdots & \vdots & & \vdots\\ m_{n1} & \dots & m_{nj-1} & m_{nj+1} & \dots & m_{nn}\end{vmatrix}.$$

La ***matrice des cofacteurs****, ou* ***comatrice****, de M est la matrice d'ordre n constituée de l'ensemble des cofacteurs de M, c'est-à-dire*

$$\operatorname{com}(M)=\left(\operatorname{cof}_{ij}(M)\right)_{1\le i,j\le n}.$$

On remarque que si M est une matrice d'ordre n, α un scalaire et E_{ij}, avec (i,j) appartenant à $\{1,\dots,n\}^2$, un élément de la base canonique de $M_n(\mathbb{K})$, on a, par multilinéarité du déterminant,

$$\det(M+\alpha E_{ij})=\det(M)+\alpha\begin{vmatrix} m_{11} & \dots & m_{1j-1} & 0 & m_{1j+1}\dots & m_{1n}\\ \vdots & & \vdots & \vdots & \vdots & \vdots\\ m_{i-11} & \dots & m_{i-1j-1} & 0 & m_{i-1j+1}\dots & m_{i-1n}\\ m_{i1} & \dots & m_{ij-1} & 1 & m_{ij+1}\dots & m_{in}\\ a_{i+11} & \dots & a_{i+1j-1} & 0 & a_{i+1j+1}\dots & m_{i+1n}\\ \vdots & & \vdots & \vdots & \vdots & \vdots\\ m_{n1} & \dots & m_{nj-1} & 0 & m_{nj+1}\dots & m_{nn}\end{vmatrix}=\det(M)+\alpha\operatorname{cof}_{ij}(M).$$

Cette observation conduit à une méthode récursive de calcul d'un déterminant d'ordre n par développement, ramenant ce calcul à celui de n déterminants d'ordre $n-1$, et ainsi de suite.

Proposition A.122 (« formules de Laplace » pour le calcul d'un déterminant) *Soit M une matrice d'ordre n. On a*

$$\forall (i,j)\in\{1,\dots,n\}^2,\ \det(M)=\sum_{k=1}^{n} m_{ik}\operatorname{cof}_{ik}(M)=\sum_{k=1}^{n} m_{kj}\operatorname{cof}_{kj}(M),$$

selon que l'on développe par rapport à la i^e ligne ou à la j^e colonne.

DÉMONSTRATION. Quitte à transposer la matrice, il suffit de prouver la formule du développement par rapport à une colonne. On considère alors la matrice, de déterminant nul, obtenue en remplaçant la j^e colonne de M, avec j dans $\{1,\dots,n\}$, par une colonne nulle. Pour passer de cette matrice à M, on doit lui ajouter les n matrices $m_{kj}E_{kj}$, $k=1,\dots,n$. On en déduit que pour passer du déterminant (nul) de cette matrice à celui de M, on doit lui ajouter les n termes $m_{kj}\operatorname{cof}_{kj}(M)$, $k=1,\dots,n$, d'où le résultat. □

Proposition A.123 *Soit M une matrice d'ordre n. On a*

$$M(\mathrm{com}(M))^\top = (\mathrm{com}(M))^\top M = \det(M)\, I_n.$$

DÉMONSTRATION. On considère tout d'abord le produit $M(\mathrm{com}(M))^\top$, dont les coefficients sont, par définition de la comatrice,

$$\forall (i,j) \in \{1,\dots,n\}^2,\ \sum_{k=1}^{n} m_{ik}\,\mathrm{cof}_{kj}(M).$$

Si $i = j$, le coefficient vaut $\det(M)$ en vertu des formules de Laplace (voir la proposition A.122). Si $i \neq j$, le coefficient est égal au déterminant de la matrice M dans lequel on a remplacé la j^{e} colonne par la i^{e}, qui est nul, puisque deux de ses colonnes sont identiques. On a donc bien $M(\mathrm{com}(M))^\top = \det(M)\, I_n$. La seconde égalité se démontre de manière similaire, en raisonnant cette fois par rapport aux lignes de la matrice produit. □

Lorsque la matrice M est inversible, ce dernier résultat fournit une formule pour son inverse,

$$M^{-1} = \frac{1}{\det(M)}\,(\mathrm{com}(M))^\top, \tag{A.3}$$

qui ne nécessite que des calculs de déterminants.

A.4.5 Matrice représentative d'un vecteur dans une base

La définition suivante, à la base du calcul matriciel en l'algèbre linéaire, permet de représenter un vecteur par une matrice colonne à partir de son écriture dans une base donnée de l'espace.

Définition A.124 (matrice d'un vecteur) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle égale à n et soit $\mathscr{B} = \{e_1,\dots,e_n\}$ une base de E. La* ***matrice d'un vecteur*** *x* ***de*** *E* ***dans la base*** *$\mathscr{B}$ est la matrice de $M_{n,1}(\mathbb{K})$ définie par*

$$Mat_{\mathscr{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

où les scalaires $x_1,\dots,x_n$ sont les coordonnées de x dans la base $\mathscr{B}$.

A.4.6 Matrice de changement de base

On est maintenant en mesure de donner une traduction matricielle du changement de bases pour l'écriture d'un vecteur.

Définition A.125 (matrice de passage) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle égale à n, $\mathscr{B} = \{e_1,\dots,e_n\}$ et $\mathscr{B}' = \{e'_1,\dots,e'_n\}$ deux bases de E. On appelle* ***matrice de passage*** *(ou* ***matrice de changement de base) de*** *$\mathscr{B}$* ***à*** *$\mathscr{B}'$ la matrice de $M_n(\mathbb{K})$ dont la j^{e} colonne, pour j appartenant à $\{1,\dots,n\}$, recense les coordonnées du vecteur e'_j dans la base $\mathscr{B}$.*

Proposition A.126 (lien entre les coordonnées d'un vecteur dans deux bases différentes) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$. Pour tout vecteur x de E, on a*

$$Mat_{\mathscr{B}}(x) = P\,Mat_{\mathscr{B}'}(x).$$

DÉMONSTRATION. On note n la dimension de l'espace E, $\mathscr{B} = \{e_1,\dots,e_n\}$ et $\mathscr{B}' = \{e'_1,\dots,e'_n\}$ les deux bases de E considérées. Il suffit alors d'écrire tout vecteur x de E donné dans ce basess et d'utiliser la définition de la matrice de passage P. On a

$$\forall x \in E,\ x = \sum_{i=1}^{n} x_i e_i = \sum_{j=1}^{n} x'_j e'_j = \sum_{j=1}^{n} x'_j \sum_{i=1}^{n} p_{ij} e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} p_{ij} x'_j \right) e_i,$$

d'où

$$\forall i \in \{1,\dots,n\},\ x_i = \sum_{j=1}^{n} p_{ij} x'_j,$$

ce qui correspond à l'identité matricielle de l'énoncé. □

A.4.7 Matrice représentative d'une application linéaire

On va à présent établir qu'une matrice est la représentation d'une application linéaire dans des bases données de deux espaces vectoriels de dimension finie, ces espaces. Pour ce faire, on suppose que E et F sont deux espaces vectoriels, de dimensions finies respectives m et n. Étant donné $\mathscr{B} = \{e_i\}_{i=1,\dots,m}$ une base de E et $\mathscr{C} = \{f_i\}_{i=1,\dots,n}$ une base de F, on peut écrire, pour toute application linéaire u de E dans F, que

$$\forall j \in \{1,\dots,m\},\ u(e_j) = \sum_{i=1}^{n} m_{ij} f_i. \tag{A.4}$$

On est ainsi en mesure de traduire matriciellement le lien entre un vecteur de l'espace et son image par un morphisme au moyen de la définition suivante.

Définition A.127 (représentation matricielle d'une application linéaire) *Soit E et F deux espaces vectoriels sur un même corps $\mathbb{K}$, de dimensions respectivement égales à m et n. On appelle **représentation matricielle** de l'application linéaire u de $\mathscr{L}(E,F)$, relativement aux bases $\mathscr{B} = \{e_i\}_{i=1,\dots,m}$ et $\mathscr{C} = \{f_i\}_{i=1,\dots,n}$, la matrice de $M_{n,m}(\mathbb{K})$, notée $Mat_{\mathscr{B},\mathscr{C}}(u)$, ayant pour coefficients les scalaires m_{ij}, $i = 1,\dots,n$, $j = 1,\dots,m$, définis de manière unique par les relations* (A.4).

Une application de $\mathscr{L}(E,F)$ étant complètement caractérisée par la donnée d'une matrice et d'un couple de bases pour sa représentation, on en déduit que $\mathscr{L}(E,F)$ est isomorphe à $M_{n,m}(\mathbb{K})$. Cet isomorphisme n'est cependant pas intrinsèque, puisque la représentation matricielle dépend des bases respectivement choisies pour E et pour F.

Réciproquement, si on se donne une matrice, alors il existe une infinité de choix d'espaces vectoriels et de bases qui permettent de définir une infinité d'applications linéaires dont elle sera la représentation matricielle. Par commodité, on a néanmoins la définition suivante.

Définition A.128 (application linéaire canoniquement associée à une matrice) *Soit m et n deux entiers natuels non nuls et M une matrice de $M_{n,m}(\mathbb{K})$. On appelle **application linéaire canoniquement associée** à M l'application linéaire de $\mathbb{K}^m$ dans $\mathbb{K}^n$ qui admet M pour matrice représentative dans les bases canoniques respectives de ces espaces.*

Cette dernière permet d'étendre aux matrices toutes les définitions précédemment introduites pour les applications linéaires.

Définitions A.129 (noyau, image et rang d'une matrice) *Soit M une matrice de $M_{n,m}(\mathbb{K})$. Le **noyau** de M est le sous-espace vectoriel de $M_{m,1}(\mathbb{K})$ défini par*

$$\ker(M) = \left\{ \boldsymbol{x} \in M_{m,1}(\mathbb{K}) \mid M\boldsymbol{x} = \boldsymbol{0} \right\}.$$

*L'**image** de M est le sous-espace vectoriel de $M_{n,1}(\mathbb{K})$ défini par*

$$\mathrm{Im}(M) = \left\{ \boldsymbol{y} \in M_{n,1}(\mathbb{K}) \mid \exists \boldsymbol{x} \in M_{m,1}(\mathbb{K}) \text{ tel que } M\boldsymbol{x} = \boldsymbol{y} \right\},$$

*et le **rang** de M est la dimension de cette image, c'est-à-dire*

$$\mathrm{rang}(M) = \dim(\mathrm{Im}(M)).$$

En vertu du théorème du rang (voir le théorème A.102), on a, pour toute matrice M de $M_{n,m}(\mathbb{K})$, la relation

$$\dim(\ker(M)) + \mathrm{rang}(M) = m,$$

dont on déduit que $\mathrm{rang}(M) \leq \min(m,n)$, la matrice étant dite *de rang maximal* si $\mathrm{rang}(M) = \min(m,n)$.

Proposition A.130 (traduction matricielle du lien entre un vecteur et son image par une application linéaire) *Soit E et F deux espaces vectoriels sur un même corps $\mathbb{K}$, de dimensions respectives finies non nulles, u une application linéaire de E dans F, $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F. Si x est un vecteur de E, les coordonnées du vecteur $u(x)$ dans la base $\mathscr{C}$ sont données en fonction des coordonnées du vecteur x dans la base $\mathscr{B}$ par le produit matriciel*

$$Mat_{\mathscr{C}}(u(x)) = Mat_{\mathscr{B},\mathscr{C}}(u) Mat_{\mathscr{B}}(x).$$

DÉMONSTRATION. On note respectivement n et m les dimensions de E et de F et on considère les coordonnées $x_1, \ldots, x_n$ d'un vecteur x de E dans la base $\mathscr{B} = \{e_i\}_{i=1,\ldots,n}$. Par linéarité de u, on a

$$u(x) = u\left(\sum_{j=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} x_j u(e_j).$$

Par conséquent, pour tout entier i dans $\{1, \ldots, m\}$, le i^{e} élément de la matrice $\text{Mat}_{\mathscr{C}}(u(x))$ est une combinaison linéaire des éléments correspondants dans les colonnes de la matrice $\text{Mat}_{\mathscr{B},\mathscr{C}}(u)$, avec les coordonnées de x pour coefficients. C'est précisement à cette combinaison linéaire que correspond le produit de matrices $\text{Mat}_{\mathscr{B},\mathscr{C}}(u)\text{Mat}_{\mathscr{B}}(x)$. □

Proposition A.131 (matrice de la composée de deux applications linéaires) *Soit E, F et G trois espaces vectoriels sur un même corps $\mathbb{K}$, de dimensions respectives finies non nulles, $\mathscr{B}$, $\mathscr{C}$ et $\mathscr{D}$ des bases de E, F et G, respectivement, u une application linéaire de E dans F et v une application linéaire de F dans G. On a alors*

$$Mat_{\mathscr{B},\mathscr{D}}(v \circ u) = Mat_{\mathscr{C},\mathscr{D}}(v) Mat_{\mathscr{B},\mathscr{C}}(u).$$

DÉMONSTRATION. Pour tout vecteur x de E, on peut, en utilisant la proposition A.130, décrire les coordonnées du vecteur $v \circ u(x)$ dans la base $\mathscr{D}$ de deux façons différentes. On a d'une part $\text{Mat}_{\mathscr{D}}(v \circ u(x)) = \text{Mat}_{\mathscr{B},\mathscr{D}}(v \circ u)\text{Mat}_{\mathscr{B}}(x)$, et d'autre part $\text{Mat}_{\mathscr{D}}(v \circ u(x)) = \text{Mat}_{\mathscr{D}}(v(u(x))) = \text{Mat}_{\mathscr{C},\mathscr{D}}(v)\text{Mat}_{\mathscr{B},\mathscr{C}}(u)\text{Mat}_{\mathscr{B}}(x)$. On a ainsi

$$\forall x \in E,\ \text{Mat}_{\mathscr{B},\mathscr{D}}(v \circ u)\text{Mat}_{\mathscr{B}}(x) = \text{Mat}_{\mathscr{C},\mathscr{D}}(v)\text{Mat}_{\mathscr{B},\mathscr{C}}(u)\text{Mat}_{\mathscr{B}}(x).$$

dont on déduit que les matrices $\text{Mat}_{\mathscr{B},\mathscr{D}}(v \circ u)$ et $\text{Mat}_{\mathscr{C},\mathscr{D}}(v)\text{Mat}_{\mathscr{B},\mathscr{C}}(u)$ sont identiques. □

Proposition A.132 (interprétation théorique d'une matrice de changement de base) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E. La matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ correspond à $Mat_{\mathscr{B}',\mathscr{B}}(id_E)$.*

DÉMONSTRATION. C'est une conséquence directe des définitions A.125 et A.127. □

De cette interprétation découle le fait qu'une matrice de passage est inversible, car elle représente de l'application bijective id_E, et que l'inverse de la matrice de passage de $\mathscr{B}$ à $\mathscr{C}$ est la matrice de passage de $\mathscr{C}$ à $\mathscr{B}$, puisque ${id_E}^{-1} = id_E$.

Théorème A.133 (changement de bases pour la matrice d'une application linéaire) *Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimensions respectives finies non nulles, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E, $\mathscr{C}$ et $\mathscr{C}'$ deux bases de F, et u une application linéaire de E dans F. On a*

$$Mat_{\mathscr{B}',\mathscr{C}'}(u) = Q^{-1} Mat_{\mathscr{B},\mathscr{C}}(u) P,$$

où P est la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ et Q est la matrice de passage de $\mathscr{C}$ à $\mathscr{C}'$.

DÉMONSTRATION. En se servant la proposition A.131, on montre que

$$\text{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = \text{Mat}_{\mathscr{C},\mathscr{C}'}(id_F)\text{Mat}_{\mathscr{B},\mathscr{C}}(u)\text{Mat}_{\mathscr{B}',\mathscr{B}}(id_E)$$

et il suffit alors d'utiliser la proposition A.132. □

Le résultat suivant est immédiat.

Corollaire A.134 (changement de base pour la matrice d'un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E, et u un endomorphisme de E. On a*

$$Mat_{\mathscr{B}'}(u) = P^{-1} Mat_{\mathscr{B}}(u) P,$$

où P est la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$.

Une conséquence de cette dernière formule de changement de base et des définitions A.116 et A.127 est que des matrices semblables représentent un même endomorphisme dans des bases différentes. Ceci conduit à la définition suivante.

Proposition et définition A.135 (déterminant d'un endomorphisme) *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle égale à n, u un endomorphisme de E et $\mathscr{B}$ une base de E. Le scalaire* $\det(Mat_{\mathscr{B}}(u))$ *est indépendant de la base $\mathscr{B}$ choisie. On l'appelle le* ***déterminant*** *de l'endomorphisme u et on le note* $\det(u)$.

Annexe B

Dualité en dimension finie

On collecte dans cette annexe quelques définitions et résultats concernant la dualité en dimension finie, qui sont utilisés dans le manuscrit. Sauf mention du contraire, on désigne par E un $\mathbb{K}$-espace vectoriel de dimension *finie* non nulle égale à n. On rappelle que, au travers de la multiplication, le corps $\mathbb{K}$ est lui-même un $\mathbb{K}$-espace vectoriel, de dimension égale à 1.

B.1 Espace dual

Définition B.1 (forme linéaire) *Soit E un espace vectoriel de dimension quelconque. Une **forme linéaire** sur E est une application linéaire de E dans $\mathbb{K}$.*

Définition B.2 (espace dual) *Soit E un espace vectoriel de dimension quelconque. On appelle **espace dual de** E, ou plus simplement **dual de** E, et on note E^*, l'ensemble des formes linéaires sur E.*

Il découle de la dernière définition que $E^* = \mathscr{L}(E;\mathbb{K})$. Le dual de E possède donc une structure d'espace vectoriel sur $\mathbb{K}$, avec pour loi interne la somme de formes linéaires et pour loi externe la multiplication d'une forme linéaire par un scalaire. Lorsque l'espace E est de dimension finie, il vient

$$\dim(E^*) = \dim(\mathscr{L}(E;\mathbb{K})) = \dim(E)\dim(\mathbb{K}) = \dim(E),$$

et le dual de E a alors la même dimension que E. Dans ce cas particulier, l'espace E^* est isomorphe à E.

B.2 Base duale

Proposition et définition B.3 (base duale) *Soit $\mathscr{B} = \{e_1, \dots, e_n\}$ une base de E. Pour tout entier i appartenant à $\{1, \dots, n\}$, on note e_i^* la forme linéaire sur E définie par*

$$\forall j \in \{1, \dots, n\},\ e_i^*(e_j) = \delta_{ij},$$

*où δ_{ij} désigne le symbole de Kronecker. Alors, la famille $\{e_1^*, \dots, e_n^*\}$ est une base de E^*, appelée **base duale de** $\mathscr{B}$, et l'on a*

$$\forall x \in E,\ x = \sum_{i=1}^{n} e_i^*(x) e_i,$$

et

$$\forall \varphi \in E^*,\ \varphi = \sum_{i=1}^{n} \varphi(e_i) e_i^*.$$

DÉMONSTRATION. Puisque l'espace E^* est de dimension égale à n, il suffit de montrer que la famille $\{e_1^*, \dots, e_n^*\}$ est libre pour prouver que c'est une base. Soit des scalaires $\lambda_1, \dots, \lambda_n$ tels que $\lambda_1 e_1^* + \cdots + \lambda_n e_n^* = 0_{E^*}$. On a

$$\forall j \in \{1, \dots, n\},\ 0 = \left(\sum_{i=1}^{n} \lambda_i e_i^*\right)(e_j) = \sum_{i=1}^{n} \lambda_i e_i^*(e_j) = \sum_{i=1}^{n} \lambda_i \delta_{ij} = \lambda_j,$$

ce qui montre bien que la famille est libre.

On considère ensuite, pour tout vecteur x de E, la décomposition $x = x_1e_1 + \ldots, +x_ne_n$ dans la base $\mathscr{B}$. On a

$$\forall i \in \{1,\ldots,n\}, e_i^*(x) = e_i^*\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j e_i^*(e_j) = \sum_{j=1}^n x_j \delta_{ij} = x_i,$$

ce qui achève de montrer la première identité. Soit enfin une forme linéaire φ sur E. En se servant de la première identité, il vient

$$\forall x \in E,\ \varphi(x) = \varphi\left(\sum_{i=1}^n e_i^*(x)e_i\right) = \sum_{i=1}^n e_i^*(x)\varphi(e_i) = \sum_{i=1}^n \varphi(e_i)e_i^*(x),$$

dont on déduit la seconde identité. □

Remarque B.4 (forme coordonnée) *Dans la preuve de la proposition B.3, on a établi que*

$$\forall x \in E,\ \forall i \in \{1,\ldots,n\},\ e_i^*(x) = x_i,$$

*où $\{e_1^*,\ldots,e_n^*\}$ est la base duale de la base $\mathscr{B}$ et $x_1,\ldots,x_n$ sont les coordonnées du vecteur x dans la base $\mathscr{B}$. Pour cette raison, on donne parfois le nom de i^e **forme coordonnée relative à la base** $\mathscr{B}$ à l'élément e_i^* de la base duale de $\mathscr{B}$.*

Le résultat suivant sera utile pour la preuve de la proposition à venir.

Lemme B.5 *Si x est un vecteur non nul de E, il existe une forme linéaire φ de E^* telle que $\varphi(x) = 1$.*

DÉMONSTRATION. Soit $\{e_1,\ldots,e_n\}$ une base de E et soit $x = \sum_{i=1}^n x_i e_i$ la décomposition du vecteur x dans celle-ci. Si x est non nul, il existe un indice i_0 dans $\{1,\ldots,n\}$ tel que le scalaire x_{i_0} est non nul. En notant $\{e_1^*,\ldots,e_n^*\}$ la base duale de $\{e_1,\ldots,e_n\}$, la forme linéaire $\varphi = \frac{1}{e_{i_0}(x)}e_{i_0}^*$ satisfait la propriété de l'énoncé. □

Proposition et définition B.6 (base antéduale) *Soit $\mathscr{B}' = \{\varphi_1,\ldots,\varphi_n\}$ une base de E^*. Il existe une unique base $\{f_1,\ldots,f_n\}$ de E telle que*

$$\forall (i,j) \in \{1,\ldots,n\}^2,\ \varphi_i(f_j) = \delta_{ij},$$

*où δ_{ij} désigne le symbole de Kronecker. Cette base est appelée **base antéduale de** $\mathscr{B}'$.*

DÉMONSTRATION. On introduit l'application Φ de E dans $\mathbb{K}^n$, définie par

$$\forall x \in E,\ \Phi(x) = (\varphi_1(x),\ldots,\varphi_n(x)),$$

qui est clairement linéaire. Elle est aussi injective. En effet, soit x un vecteur du noyau de Φ. On a alors $\varphi_1(x) = \cdots = \varphi_n(x) = 0$. D'après le lemme B.5, si x est non nul, il existe une forme linéaire φ sur E telle que $\varphi(x) = 1$, que l'on peut écrire dans la base $\mathscr{B}'$ sous la forme $\varphi = \sum_{i=1}^n \lambda_i\varphi_i$. On a par conséquent $1 = \varphi(x) = \sum_{i=1}^n \lambda_i\varphi_i(x) = 0$, ce qui est absurde. On en déduit que le noyau de Φ est réduit au vecteur nul et l'application Φ est un isomorphisme.

Soit $\{\varepsilon_1,\ldots,\varepsilon_n\}$ la base canonique de $\mathbb{K}^n$. La famille $\{f_1,\ldots,f_n\}$, définie par

$$\forall i \in \{1,\ldots,n\},\ \Phi(f_i) = \varepsilon_i,$$

est alors une base de E, la seule vérifiant la propriété de l'énoncé. □

Proposition B.7 (changement de base duale) *Soit $\mathscr{B}$ et $\mathscr{C}$ deux bases de E et soit $\mathscr{B}^*$ et $\mathscr{C}^*$ leurs bases duales respectives. La matrice de passage de $\mathscr{B}^*$ et $\mathscr{C}^*$ est $\left(P^\top\right)^{-1}$, où P est la matrice de passage de $\mathscr{B}$ et $\mathscr{C}$.*

DÉMONSTRATION. On pose $\mathscr{B} = \{e_1,\ldots,e_n\}$ et $\mathscr{C} = \{f_1,\ldots,f_n\}$ et on note Q la matrice de passage de de $\mathscr{B}^*$ et $\mathscr{C}^*$. Par définition d'une matrice de passage, on a

$$\forall j \in \{1,\ldots,n\},\ f_j = \sum_{i=1}^n p_{ij}e_i \text{ et } f_j^* = \sum_{i=1}^n q_{ij}e_i^*,$$

et, par celle de la base duale, on a

$$\forall (i,j) \in \{1,\ldots,n\}^2,\ \delta_{ij} = f_i^*(f_j) = \left(\sum_{k=1}^n q_{kj}e_k^*\right)\left(\sum_{\ell=1}^n p_{\ell i}e_\ell\right) = \sum_{k=1}^n\sum_{\ell=1}^n p_{\ell i}q_{kj}e_k^*(e_\ell) = \sum_{k=1}^n\sum_{\ell=1}^n p_{\ell i}q_{kj}\delta_{k\ell} = \sum_{k=1}^n p_{ki}q_{kj},$$

ce qu'on traduit matriciellement par $I_n = P^\top Q$, d'où $Q = \left(P^\top\right)^{-1}$. □

B.3 Espace bidual

L'espace dual d'un espace vectoriel étant un espace vectoriel, on peut à son tour en définir l'espace dual. Ceci donne lieu à la définition suivante.

Définition B.8 (espace bidual) *Soit E un espace vectoriel de dimension quelconque et E^* son espace dual. L'espace dual de E^*, noté E^{**}, est appelé l'**espace bidual de** E.*

Proposition B.9 (injection canonique) *Soit E un espace vectoriel de dimension quelconque. L'application définie par*

$$i_E : \begin{cases} E \to E^{**} \\ x \mapsto \begin{cases} E^* \to \mathbb{K} \\ \varphi \mapsto \varphi(x) \end{cases} \end{cases}$$

est linéaire et injective.

DÉMONSTRATION. On observe tout d'abord que l'application i_E est bien définie, puisque, pout tout vecteur x de E, l'application $i_E(x)$ est une forme linéaire sur E^* :

$$\forall \lambda \in \mathbb{K},\ \forall (\varphi, \psi) \in (E^*)^2,\ i_E(x)(\lambda\varphi + \psi) = (\lambda\varphi + \psi)(x) = \lambda\varphi(x) + \psi(x) = \lambda\, i_E(\varphi) + i_E(\psi).$$

On montre ensuite que l'application est linéaire. Pour tout scalaire λ et tout couple (x, y) de vecteurs de E, on a, par linéarité d'une forme linéaire,

$$\forall \varphi \in E^*,\ i_E(\lambda x + y)(\varphi) = \varphi(\lambda x + y) = \lambda\varphi(x) + \varphi(y) = \lambda\, i_E(x)(\varphi) + i_e(y)(\varphi) = (\lambda\, i_E(x) + i_E(y))(\varphi).$$

Il reste à prouver que l'application est injective. Soit x un vecteur du noyau de i_E. Si x est non nul, il existe, en vertu du lemme B.5, une forme linéaire φ sur E telle que

$$1 = \varphi(x) = i_E(x)(\varphi) = 0,$$

ce qui est absurde. Le noyau de i_E se trouve donc réduit au vecteur nul. □

Lorsque l'espace E est dimension finie, il résulte de cette proposition que l'application i_E, dite **injection canonique de** E **dans** E^{**}, est un isomorphisme. Ainsi, un espace vectoriel de dimenson finie est canoniquement isomorphe à son espace bidual, ce qui permet en pratique de les identifier.

Cette identification conduit à l'emploi courant de la notation suivante. Pour tout vecteur x de E et toute forme linéaire φ de E^*, on note

$$\langle \varphi, x \rangle_{E^*,E} = \varphi(x).$$

On parle alors d'**appariement dual** ou de, **produit (ou crochets) de dualité**, **entre** E **et** E^* pour la forme bilinéaire ainsi définie. L'intérêt d'une telle notation est de faire référence à celle couramment utilisée pour le produit scalaire (voir la section 4.1 du chapitre 4).

B.4 Orthogonalité

L'appariement dual permet d'introduire « naturellement » les notions d'orthogonalité suivantes.

Définition B.10 (orthogonal au sens de la dualité) *Soit E un espace vectoriel de dimension quelconque et E^* son espace dual. Pour toute partie A de E (resp. B de E^*), l'ensemble*

$$A^\perp = \left\{\varphi \in E^* \,|\, \forall x \in A,\ \langle \varphi, x \rangle_{E^*,E} = 0\right\} = \{\varphi \in E^* \,|\, \forall x \in A,\ \varphi(x) = 0\}$$
$$\textit{(resp. } B^\circ = \left\{x \in E \,|\, \forall \varphi \in B,\ \langle \varphi, x \rangle_{E^*,E} = 0\right\} = \{x \in E \,|\, \forall \varphi \in B,\ \varphi(x) = 0\}\textit{)}$$

*est appelé l'**orthogonal de** A (resp. B).*

Remarque B.11 *Lorsque l'espace E est de dimension finie, le fait de parler à la fois d'orthogonal pour une partie de E ou une partie de l'espace dual E^* se justifie par l'identification de E avec son espace bidual E^{**}, au moyen de l'injection canonique i_E introduite dans la proposition B.9. On a en effet, pour tout partie B de E^*,*

$$\begin{aligned} B^\perp &= \left\{y \in E^{**} \,|\, \forall \varphi \in B,\ \langle y, \varphi\rangle_{E^{**},E^*} = 0\right\} \\ &= \left\{i_E(x) \in E^{**} \,|\, \forall \varphi \in B,\ \langle i_E(x), \varphi\rangle_{E^{**},E^*} = 0\right\} \\ &= \{i_E(x) \in E^{**} \,|\, \forall \varphi \in B,\ \varphi(x) = 0\} \\ &= \{i_E(x) \in E^{**} \,|\, x \in B^\circ\} \\ &= i_E(B^\circ). \end{aligned}$$

Théorème B.12 *Soit A une partie de E.*

1. *Si A' est une partie de E telle que $A \subset A'$, alors on a $(A')^\perp \subset A^\perp$.*
2. *On a $A^\perp = (\mathrm{Vect}(A))^\perp$ et $\left(A^\perp\right)^\circ = \mathrm{Vect}(A)$. En particulier, si A est un sous-espace vectoriel de E, on a $\left(A^\perp\right)^\circ = A$.*
3. *Si A est un sous-espace vectoriel de E, on a $\dim(A) + \dim\left(A^\perp\right) = n$.*

DÉMONSTRATION.

1. On suppose que $A \subset A'$. On a alors
$$\varphi \in \left(A'\right)^\perp \iff \forall x \in A',\ \varphi(x) = 0 \implies \forall x \in A,\ \varphi(x) = 0 \iff \varphi \in A^\perp.$$
2. Soit λ un scalaire, φ et ψ deux éléments de $A^\perp$. On a
$$\forall x \in A,\ (\lambda\varphi + \psi)(x) = \lambda\varphi(x) + \psi(x) = 0,$$
d'où $\lambda\varphi + \psi$ appartient à $A^\perp$. On en déduit que $A^\perp$ est un sous-espace vectoriel de E^*. Pour tout vecteur de x de A, on a, par définition de $A^\perp$,
$$\forall \varphi \in A^\perp,\ \varphi(x) = 0,$$
et donc A est inclus dans $\left(A^\perp\right)^\circ$, qui est un sous-espace vectoriel de E (voir le théorème B.13). On a donc $\mathrm{Vect}(A) \subset \left(A^\perp\right)^\circ$. Pour prouver l'inclusion réciproque, on va passer par les complémentaires et établir que $E \setminus \mathrm{Vect}(A) \subset E \setminus \left(A^\perp\right)^\circ$. Si $\mathrm{Vect}(A) = E$, il n'y a rien à montrer. Sinon, soit x un vecteur de $E \setminus \mathrm{Vect}(A)$. On doit montrer que x n'appartient pas à $\left(A^\perp\right)^\circ$, c'est-à-dire qu'il existe une forme linéaire φ s'annulant sur $\mathrm{Vect}(A)$ et non nulle en x. Soit $\{e_1, \ldots, e_{\dim(A)}\}$ une base de $\mathrm{Vect}(A)$. On pose $e_{\dim(A)+1} = x$ et l'on complète la famille libre $\{e_1, \ldots, e_{\dim(A)+1}\}$ en une base $\{e_1, \ldots, e_n\}$ de E. La forme linéaire définie par
$$\forall i \in \{1, \ldots, n\} \setminus \{\dim(A) + 1\} \varphi(e_i) = 0 \text{ et } \varphi(e_{\dim(A)+1}) = 1$$
vérifie alors les conditions requises.
3. Soit $\{e_1, \ldots, e_{\dim(A)}\}$ une base de A, que l'on complète en une base $\{e_1, \ldots, e_n\}$ de E. Soit $\{e_1^*, \ldots, e_n^*\}$ la base duale de cette dernière. On pose alors $B = \mathrm{Vect}\left(\left\{e_1^*, \ldots, e_{\dim(A)}^*\right\}\right)$, de sorte que $\dim(B) = \dim(A)$. Pour tout élément φ de B, il existe des scalaires $\lambda_1, \ldots, \lambda_{\dim(A)}$ tels que $\varphi = \sum_{i=1}^{\dim(A)} \lambda_i e_i^*$. Par conséquent, pour une forme φ appartenant à $B \cap A^\perp$, on a $\lambda_1 = \varphi(e_1) = 0$,..., $\lambda_{\dim(A)} = \varphi(e_{\dim(A)}) = 0$, ce qui montre que $\varphi = 0_{E^*}$. Enfin, pour toute forme linéaire ψ sur E, il existe des scalaires $\alpha_1, \ldots, \alpha_n$ tels que $\psi = \sum_{i=1}^n \alpha_i e_i^*$. Il est clair que $\sum_{i=1}^{\dim(A)} \alpha_i e_i^*$ appartient à B et que $\sum_{i=\dim(A)+1}^n \alpha_i e_i^*$ appartient à $A^\perp$. On a ainsi montré que $B + A^\perp = E^*$, d'où
$$n = \dim(E^*) = \dim(B) + \dim(A^\perp) = \dim(A) + \dim(A^\perp).$$

□

La preuve du théorème suivant est similaire à celle du précédent et laissée en exercice.

Théorème B.13 *Soit B une partie de E^*.*

1. *Si A' est une partie de E telle que $B \subset B'$, alors on a $(B')^\circ \subset B^\circ$.*
2. *On a $B^\circ = (\mathrm{Vect}(B))^\circ$ et $(B^\circ)^\perp = \mathrm{Vect}(B)$. En particulier, si B est un sous-espace vectoriel de E^*, on a $(B^\circ)^\perp = B$.*
3. *Si B est un sous-espace vectoriel de E^*, on a $\dim(B) + \dim(B^\circ) = n$.*

B.5 Application transposée

Dans cette section, on considère deux $\mathbb{K}$-espaces vectoriels E et F de dimension finie non nulle.

Définition B.14 (application transposée) *Soit u une application linéaire de E dans F. On appelle* ***application transposée de*** *u l'application $u^\top$ de F^* dans E^* définie par*

$$\forall \varphi \in F^*,\ u^\top(\varphi) = \varphi \circ u.$$

On a le résultat utile suivant.

Proposition B.15 *Soit A un sous-espace vectoriel de E et u un endomorphisme de E. On a l'équivalence*

$$A \text{ stable par } u \iff A^\perp \text{ stable par } u^\top.$$

DÉMONSTRATION. On suppose que le sous-espace A est stable par u. Soit φ un élément de l'orthogonal $A^\perp$. On a

$$\forall x \in A,\ \left\langle u^\top(\varphi), x\right\rangle_{E^*,E} = \langle \varphi \circ u, x\rangle_{E^*,E} = (\varphi \circ u)(x)\varphi(u(x)) = \langle \varphi, u(x)\rangle_{E^*,E} = 0,$$

puisque $u(x)$ appartient à A. On en déduit que $u^\top(\varphi)$ appartient à $A^\perp$.

Réciproquement, on suppose que le sous-espace $A^\perp$ est stable par $u^\top$. On montre tout d'abord que l'on peut écrire A comme une intersection d'hyperplans. Pour cela, on considère une base $\{\varphi_1, \dots, \varphi_{n-\dim(A)}\}$ de $A^\perp$. Il vient alors

$$\begin{aligned}
x \in A &\iff \forall \varphi \in A^\perp,\ \langle \varphi, x\rangle_{E^*,E} = 0 \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \langle \varphi_i, x\rangle_{E^*,E} = 0 \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \varphi_i(x) = 0 \\
&\iff x \in \cap_{i=1}^{n-\dim(A)} \ker(\varphi_i).
\end{aligned}$$

Par hypothèse, on a

$$\forall i \in \{1, \dots, n-\dim(A)\},\ \varphi_i \in A^\perp \implies \forall i \in \{1, \dots, n-\dim(A)\},\ u^\top(\varphi_i) \in A^\perp,$$

d'où

$$\begin{aligned}
x \in A &\iff x \in \cap_{i=1}^{n-\dim(A)} \ker(\varphi_i) \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ x \in \ker(\varphi_i) \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \varphi_i(x) = 0 \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \langle \varphi_i, x\rangle_{E^*,E} = 0 \\
&\implies \forall i \in \{1, \dots, n-\dim(A)\},\ \left\langle u^\top(\varphi_i), x\right\rangle_{E^*,E} = 0 \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \varphi_i(u(x)) = 0 \\
&\iff \forall i \in \{1, \dots, n-\dim(A)\},\ \ u(x) \in \ker(\varphi_i) \\
&\iff u(x) \in \cap_{i=1}^{n-\dim(A)} \ker(\varphi_i) \\
&\iff u(x) \in A.
\end{aligned}$$

Le sous-espace A est donc stable par u. □

Bibliographie

[Bje51] A. BJERHAMMAR. Rectangular reciprocal matrices, with special reference to geodetic calculations. *Bull. Géodésique*, 20(1) :188-220, 1951. DOI : 10.1007/BF02526278.

[Bro91] R. BRONSON. *Matrix methods. An introduction*. Academic Press, seconde édition, 1991.

[BW66] C. S. BEIGHTLER et D. J. WILDE. Diagonalization of quadratic forms by Gauss elimination. *Management Sci.*, 12(5) :371-379, 1966. DOI : 10.1287/mnsc.12.5.371.

[CEZ11] D. COUTY, J. ESTERLE et R. ZAROUF. Décomposition effective de Jordan-Chevalley. *Gaz. Math.*, 129 :29-49, 2011.

[CEZ16] D. COUTY, J. ESTERLE et R. ZAROUF. Réduction ou décomposition : de Jordan à Chevalley. *Gaz. Math.*, 148 :15-24, 2016.

[Che51] C. CHEVALLEY. *Théorie des groupes de Lie. Tome II Groupes algébriques*. Hermann, 1951.

[Cro41] P. D. CROUT. A short method for evaluating determinants and solving systems of linear equations with real or complex coefficients. *Trans. Amer. Inst. Elec. Eng.*, 60(12) :1235-1241, 1941. DOI : 10.1109/T-AIEE.1941.5058258.

[Dir39] P. A. M. DIRAC. A new notation for quantum mechanics. *Math. Proc. Cambridge Philos. Soc.*, 35(3) :416-418, 1939. DOI : 10.1017/S0305004100021162.

[Dun54] N. DUNFORD. Spectral operators. *Pacific J. Math.*, 4(3) :321-354, 1954.

[EY36] C. ECKART et G. YOUNG. The approximation of one matrix by another of lower rank. *Psychometrika*, 1(3) :211-218, 1936. DOI : 10.1007/BF02288367.

[Fré35] M. FRÉCHET. Sur la définition axiomatique d'une classe d'espaces vectoriels distanciés applicables vectoriellement sur l'espace de Hilbert. *Ann. Math. (2)*, 36(3) :705-718, 1935. DOI : 10.2307/1968652.

[Gio17] G. GIORGI. Various proofs of the Sylvester criterion for quadratic forms. *J. Math. Res.*, 9(6) :55-66, 2017. DOI : 10.5539/jmr.v9n6p55.

[GK65] G. GOLUB et W. KAHAN. Calculating the singular values and pseudo-inverse of a matrix. *J. SIAM Ser. B Numer. Anal.*, 2(2) :205-224, 1965. DOI : 10.1137/0702016.

[Gra83] J. P. GRAM. Ueber die Entwicklung reeller Functionen in Reihen mittelst der Methode der kleinsten Quadrate. *J. Reine Angew. Math.*, 1883(94) :41-73, 1883. DOI : 10.1515/crll.1883.94.41.

[Jor70] C. JORDAN. *Traité des substitutions et des équations algébriques*. Gauthier-Villars, 1870.

[JvN35] P. JORDAN et J. von NEUMANN. On inner products in linear, metric spaces. *Ann. Math. (2)*, 36(3) :719-723, 1935. DOI : 10.2307/1968653.

[Moo20] E. H. MOORE. On the reciprocal of the general algebraic matrix (abstract). *Bull. Amer. Math. Soc.*, 26(9) :385-396, 1920. DOI : 10.1090/S0002-9904-1920-03322-7.

[Pen55] R. PENROSE. A generalized inverse for matrices. *Math. Proc. Cambridge Philos. Soc.*, 51(3) :406-413, 1955. DOI : 10.1017/S0305004100030401.

[Pru86] J. E. PRUSSING. The principal minor test for semidefinite matrices. *J. Guidance Control Dynam.*, 9(1) :121-122, 1986. DOI : 10.2514/3.20077.

[Sch07] E. SCHMIDT. Zur Theorie der linearen und nichtlinearen Integralgleichungen. I. Teil : Entwicklung willkürlicher Funktionen nach Systemen vorgeschriebener. *Math. Ann.*, 63(4) :433-476, 1907. DOI : 10.1007/BF01449770.

[Ste93] G. W. STEWART. On the early history of the singular value decomposition. *SIAM Rev.*, 35(4) :551-566, 1993. DOI : 10.1137/1035134.

[Syl50] J. J. SYLVESTER. XLVII. Additions to the articles in the September number of this journal, "On a new class of theorems," and on Pascal's theorem. *Philos. Mag. (3)*, 37(251) :363-370, 1850. DOI : 10.1080/14786445008646629.

[Syl52] J. J. SYLVESTER. XIX. A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares. *Philos. Mag. (4)*, 4(23) :138-142, 1852. DOI : 10.1080/14786445208647087.