ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Formes bilinéaires et quadratiques

Leçons directement concernées (2019)

(106) Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
(158)* Matrices symétriques réelles, matrices hermitiennes.
(160)* Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)
(170) Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
(171)* Formes quadratiques réelles. Coniques. Exemples et applications.

Leçons directement liées, dans lesquelles on doit évoquer les formes bilinéaires ou quadratiques (2019)

(150)* Exemples d'actions de groupes sur les espaces de matrices.
(154)* Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
(155)* Endomorphismes diagonalisables en dimension finie.
(156) Exponentielle de matrices. Applications.
(159) Formes linéaires et dualité en dimension finie. Exemples et applications.
(161)* Distances et isométries d'un espace affine euclidien.
(183) Utilisation des groupes en géométrie.

Leçons où des formes quadratiques peuvent également apparaître sporadiquement (2019)

(151) Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
(153) Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
(181)* Barycentres dans un espace affine réel de dimension finie, convexité. Applications.
(182) Applications des nombres complexes à la géométrie.

Ce qui est dans le programme

(a) Formes bilinéaires. Formes bilinéaires alternées. Formes bilinéaires symétriques, formes quadratiques, forme polaire d'une forme quadratique (en caractéristique différente de 2). Éléments orthogonaux, interprétation géométrique. Formes non dégénérées. Adjoint d'un endomorphisme. Représentation matricielle, changement de base. Rang d'une forme bilinéaire.

(b) Orthogonalité. Sous-espaces isotropes. Décomposition d'une forme quadratique en somme de carrés. Théorème d'inertie de Sylvester. Classification dans le cas de $\mathbb{R}$ ou $\mathbb{C}$. Procédés d'orthogonalisation.

(c) Espaces vectoriels euclidiens, espaces vectoriels hermitiens. Isomorphisme d'un espace vectoriel euclidien avec son dual. Supplémentaire orthogonal. Inégalité de Cauchy-Schwarz. Norme. Bases orthonormales.

(d) Groupe orthogonal, groupe spécial orthogonal. Exemple de générateurs du groupe orthogonal : décomposition d'un automorphisme orthogonal en produit de réflexions. Endomorphismes symétriques, endomorphismes normaux. Diagonalisation d'un endomorphisme symétrique. Réduction simultanée de deux formes quadratiques réelles, l'une étant définie positive. Décomposition polaire dans $\mathrm{GL}(n,\mathbb{R})$. Espaces vectoriels euclidiens de dimension 2, classification des éléments de $\mathcal{O}(2,\mathbb{R})$. Espaces vectoriels euclidiens de dimension 3, classification des éléments de $\mathcal{O}(3,\mathbb{R})$; produit mixte, produit vectoriel.

(e) Groupe unitaire, groupe spécial unitaire. Diagonalisation des endomorphismes normaux. Décomposition polaire dans $\mathrm{GL}(n, \mathbb{C})$.

Bibliographie

- À suivre...

1 Formes quadratiques sur un corps quelconque

Hypothèse fondamentale : K est un corps de caractéristique différente de 2 !
Dans toute la suite, V est un K-espace vectoriel de dimension finie n.

1.1 Définitions : formes, espaces quadratiques et morphismes

Définition 1.1. Une *forme quadratique* q sur V est une application $q : V \to K$ telle qu'il existe une forme bilinéaire symétrique $b_q : V \times V \to K$ telle que $\forall v \in V,\ q(v) = b_q(v, v)$.

Proposition 1.2 (Formules de polarisation)**.** *La forme b_q est uniquement déterminée par les formules*

$$b_q(x, y) = \frac{q(x+y) - q(x) - q(y)}{2} = \frac{q(x+y) - q(x-y)}{4}.$$

Démonstration. Par définition, il existe b bilinéaire telle que $b(v, v) = q(v)$. On a alors :

$$\begin{aligned} q(x+y) - q(x) - q(y) &= b(x+y, x+y) - b(x, x) - b(y, y) \\ &= b(x, y) + b(y, x) && \text{par bilinéarité,} \\ &= 2b(x, y) && \text{par symétrie.} \end{aligned}$$

D'où l'unicité. De même, on a :

$$\begin{aligned} q(x+y) - q(x-y) &= b(x+y, x+y) - b(x-y, x-y) \\ &= \Big(b(x, x) + b(x, y) + b(y, x) + b(y, y)\Big) \\ &\quad - \Big(q(x, x) - q(y, x) - q(x, y) + q(y, y)\Big) && \text{par bilinéarité,} \\ &= 4b(x, y) && \text{par symétrie.} \end{aligned}$$

□

Corollaire 1.3. *L'ensemble des formes quadratiques sur $V \simeq K^n$ est un K-espace vectoriel isomorphe au K-espace vectoriel des formes bilinéaires symétriques, donc de dimension $\frac{n(n+1)}{2}$.*

Définition 1.4 (Espaces et morphismes)**.** Un *espace quadratrique* sur K est un couple (V, q) formé d'un espace vectoriel V de dimension finie sur K et d'une forme quadratique q sur V.

Un *morphisme d'espaces quadratiques* $f : (V_1, q_1) \to (V_2, q_2)$ est une application linéaire $f : V_1 \to V_2$ telle que $b_2(f(x), f(y)) = b_1(x, y)\ \forall x, y \in V_1$, autrement dit $q_2 \circ f = q_1$.

Une *isométrie* est un morphisme bijectif entre espaces quadratiques.

Fait 1.5. *L'inverse d'une isométrie est une isométrie.*

L'ensemble des isométries d'un espace quadratique (V, q) forme un sous-groupe de $\mathrm{GL}(V)$*. On l'appelle* groupe orthogonal *et on le note $\mathcal{O}(V, q)$ ou plus simplement $\mathcal{O}(q)$.*

Démonstration. L'inverse d'une application linéaire est toujours linéaire et $q_2 \circ f = q_1 \Leftrightarrow q_1 \circ f^{-1} = q_2$.

On a $\mathcal{O}(q) = \{u \in \mathrm{GL}(V),\ q \circ u = q\} = \{u \in \mathrm{GL}(V),\ b_q(u(x), u(y)) = b_q(x, y)\}$. Ainsi, pour $u, v \in \mathcal{O}(q)$, on a $u \circ v^{-1} \in \mathrm{GL}(V)$ satisfait $q \circ \big(u \circ v^{-1}\big) = (q \circ u) \circ v^{-1} = q \circ v^{-1} = q$. □

Définition 1.6. Deux formes quadratiques q_1, q_2 sur un même espace vectoriel V sont dites *équivalentes* si les espaces quadratiques (V, q_1) et (V, q_2) sont isométriques, autrement dit s'il existe $f \in \mathrm{GL}(V)$ telle que $q_2 \circ f^{-1} = q_1$.

L'un des enjeux de la théorie – la classification des formes quadratique – consistera à décrire les classes d'équivalences de formes quadratique sur K^n, autrement dit, à trouver un invariant total de l'action sur groupe $\mathrm{GL}_n(K)$ sur l'espace vectoriel des formes quadratiques.

1.2 Orthogonalité

Soit (V, q) un espace quadratique fixé.

Définition 1.7. On dit que deux vecteurs $x, y \in V$ sont *q-orthogonaux* si $b_q(x, y) = 0$.

Si W est une partie (typiquement un sous-espace vectoriel) de V, on appelle *orthogonal* de W dans V l'ensemble $W^\perp = \{v \in V,\ b(w, v) = 0\ \forall w \in W\}$.

Fait 1.8. *L'orthogonal $W^\perp$ est un sous-espace vectoriel de V.*

Démonstration. On a $0 \in W^\perp$ et si $x, y \in W^\perp$, si $\lambda, \mu \in K$, alors $b_q(\lambda x + \mu y, w) = 0\ \forall w \in W$ par bilinéarité. Donc $\lambda x + \mu y \in W^\perp$. $\square$

Définition 1.9. On appelle *noyau* (ou radical) de q le sous-espace vectoriel $\ker(q) = V^\perp$.

On appelle *rang* de q la quantité $\mathrm{rg}(q) = \dim(V) - \dim(\ker q)$.

On dit que q est non dégénérée si $\ker q = \{0\}$.

Fait 1.10. *La forme quadratique q est non dégénérée si, et seulement si, $\forall v \in V \setminus \{0\},\ \exists w \in V,\ b_q(v, w) \neq 0$.*

Toute forme quadratique q induit une forme quadratique non dégénérée sur $V/\ker q$.

Définition 1.11. On appelle *morphisme K-linéaire fondamental* l'application

$$\begin{array}{rccc} \Phi : & V & \to & V^* \\ & v & \mapsto & b(v, \cdot) \end{array}$$

Théorème 1.12. *(1) On a $\ker \Phi = \ker q$.*

(2) Si q est non dégénérée, alors pour tout sous-espace vectoriel W de V :

(a) l'application Φ induit un isomorphisme $\Phi : W^\perp \to (V/W)^*$.

(b) $\dim W^\perp = \dim V - \dim W$

(c) $\left(W^\perp\right)^\perp = W$.

Démonstration. L'application Φ est K-linéaire.

(1) Soit $v \in V$. On a $\Phi(v) = 0 \Leftrightarrow \forall w \in V,\ b_q(v, w) = 0 \Leftrightarrow v \in V^\perp = \ker q$.

(2) On suppose désormais $\ker q = 0$. Soit W un sous-espace vectoriel de V et $\phi = \Phi_{|W^\perp}$. Alors $\forall v \in W^\perp,\ \forall w \in W,\ \phi(v)(w) = b_q(v, q) = 0$. Comme $(V/W)^*$ est isomorphe à l'espace vectoriel des formes linéaires nulles sur W, on en déduit que $\phi(v)$ passe au quotient en $\varphi(v) \in (V/W)^*$.

Si $f \in (V/W)^*$ est vue comme une forme linéaire sur V nulle sur W, comme Φ est injective entre espaces vectoriels de même dimension, elle est surjective. Ainsi, il existe $v \in V$ tel que $f = \Phi(v) = b_q(v, \cdot)$. Pour tout $w \in W$, on a $0 = f(w) = b_q(v, w)$. Donc $v \in W^\perp$. Ainsi $f = \varphi(w)$ donc $\phi : W^\perp \to (V/W)^*$ est un isomorphisme, ce qui donne (a).

En particulier, $\dim W^\perp = \dim (V/W)^* = \dim V - \dim W$ donne (b).

Enfin, $\dim \left(W^\perp\right)^\perp = \dim \left(V^*/(V/W)^*\right) = \dim V^* - \dim (V/W)^* = \dim W$. Comme $\left(W^\perp\right)^\perp \subset W$ sont des espaces vectoriels de même dimension, on a l'égalité (c). $\square$

1.3 Isotropie

Définition 1.13. Un vecteur $v \in V$ est dit *isotrope* si $q(v) = 0$ et *anisotrope* sinon.

On appelle *cône isotrope* de q l'ensemble $C(q) = \{v \in V,\ q(v) = 0\}$.

On dit que q est *isotrope* si $C(q) \neq \{0\}$ et *anisotrope* sinon.

Fait 1.14. *L'ensemble $C(q)$ est un cône.*

Démonstration. $q(\lambda x) = \lambda^2 q(x)$. $\square$

Remarque 1.15. En général, $C(q)$ n'est pas convexe. Par exemple, pour $V = K^2$ et $q(x, y) = x^2 - y^2$ on a $C(q) = \{(x, y),\ x^2 - y^2 = 0\}$ est l'union des deux droites $K(1, 1)$ et $K(1, -1)$ car $x^2 - y^2 = (x + y)(x - y)$.

Définition 1.16. Soit W un sous-K-espace vectoriel de V.

On dit que W est *singulier* (ou isotrope) si $q_{|W}$ est dégénérée.

On dit que W est *totalement isotrope* si $q_{|W} = 0$.

Exemple 1.17. Considérons $(V, q) = \left(K^3, q(x, y, z) = x^2 + y^2 - z^2\right)$. q est isotrope car $q(1, 0, 1) = 0$. Soit $W = K(1, 0, 1) \oplus K(1, 1, 1)$ hyperplan de V. Alors W est un sous-espace singulier de V car $b_q((1, 0, 1), (x, y, z)) = 0$ pour tout $(x, y, z) \in W$, car on peut le tester sur la base $((1, 0, 1), (1, 1, 1))$ de W mais ce n'est pas un espace totalement isotrope car $q(1, 1, 1) = 1$.

Fait 1.18. *Soit W un sous-espace vectoriel de V. S'équivalent*

(i) W *n'est pas singulier ;*

(ii) $q_{|W}$ *est non dégénérée ;*

(iii) $W \cap W^{\perp} = 0$ *;*

(iv) $V = W \oplus W^{\perp}$.

Démonstration. $(i) \Leftrightarrow (ii) \Leftrightarrow (iii) \Leftarrow (iv)$ par définition.

$(iii) \Rightarrow (iv)$ car $\dim W^{\perp} = \dim V - \dim W$. □

1.4 Symétries orthogonales

Définition 1.19 (Symétries)**.** Soit W un sous-espace vectoriel non singulier. On appelle *symétrie orthogonal* par rapport à W l'élément de $\mathcal{O}(q)$:

$$s_W : \begin{array}{ccc} V = W \oplus W^{\perp} & \to & V \\ w + w' & \mapsto & w - w' \end{array}$$

Si $\operatorname{codim}_V W = 1$, on dit que s_W est une *réflexion orthogonale*.

Si $\operatorname{codim}_V W = 2$, on dit que s_W est un *renversement*.

Fait 1.20 (Action par conjugaison de $\mathcal{O}(q)$)**.** *On a* $u \circ s_W \circ u^{-1} = s_{u(W)}$.

Fait 1.21. *Si $v \in V$ est anisotrope, alors l'espace vectoriel $W = (Kv)^{\perp}$ n'est pas singulier et*

$$s_{(Kv)^{\perp}}(x) = x - 2\frac{b_q(x, v)}{q(v)}v \qquad \forall x \in V.$$

Démonstration. Soit $x \in V$ qu'on écrit $x = y + \lambda v$ avec $y \in (Kv)^{\perp}$ et $\lambda \in K$. Alors $s_{(Kv)^{\perp}}(x) = y - \lambda v = x - 2\lambda v$. Or $b_q(x, v) = \lambda q(v)$. Donc $\lambda = \frac{b_q(x,v)}{q(v)}$ car $q(v) \neq 0$ par anisotropie de v. □

Proposition 1.22. *Les symétries orthogonales sont exactement les éléments $u \in \mathcal{O}(q)$ tels que* $u^2 = \mathrm{id}$.

Démonstration. Par construction, les symétries orthogonales s_W vérifient $s_W^2 = \mathrm{id}_V$.

Soit $u \in \mathcal{O}(q)$ tel que $u^2 = \mathrm{id}$. Le polynôme minimal de u est simplement scindé de valeurs propres ± 1 car $\operatorname{car}(K) \neq 2$ et $V = \ker(u - \mathrm{id}) \oplus \ker(u + \mathrm{id})$. Posons $W = \ker(u - \mathrm{id})$ et $W' = \ker(u + \mathrm{id})$ et montrons que $W' = W^{\perp}$.

Si $x \in W$ et $y \in W'$, alors

$$\begin{aligned} b_q(u(x) - x, y) = 0 & \\ &= b_q(u(x), y) - b_q(x, y) && \text{par linéarité} \\ &= -b_q(u(x), u(y)) - b_q(x, y) && \text{car } y = -u(y) \\ &= -2b_q(x, y) && \text{car } u \in \mathcal{O}(q) \end{aligned}$$

Donc $W' = W^{\perp}$ et il s'en suit que $u = s_W$. □

2 Éléments de classification des formes quadratiques

On se propose désormais étant donner un corps K de caractéristique différente de 2 et un entier $n \in \mathbb{N}^*$, de chercher à établir des invariants sous le groupe linéaire $\mathrm{GL}(V)$ des formes quadratiques sur $V = K^n$, voire une classification sous de bonnes conditions.

2.1 Écriture matricielle

Définition 2.1. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une K-base de V et $\mathcal{B}^* = (e_1^*, \dots, e_n^*)$ la base duale dans V^* de $\mathcal{B}$. On définit $\mathrm{Mat}_{\mathcal{B}}(q) = (b_q(e_i, e_j))_{1 \leq i,j \leq n}$.

Fait 2.2. *On a* $\mathrm{Mat}_{\mathcal{B}}(q) = \mathrm{Mat}_{\mathcal{B},\mathcal{B}^*}(\Phi)$. *où* Φ *désigne le morphisme fondamental* $\Phi(v) = (w \mapsto b_q(v, w))$.

Démonstration. Soit $w = \sum_{j=1}^n w_j e_j \in V$. Alors pour tout $i \in [\![1, n]\!]$, on a $\Phi(e_i)(w) = b_q(e_i, w) = \sum_{j=1}^n b_q(e_i, e_j) w_j = \sum_{j=1}^n b_q(e_i, e_j) e_j^*(w)$. Donc $\Phi(e_i) = \sum_{j=1}^n b_q(e_i, e_j) e_j^*$. D'où l'égalité matricielle. □

Corollaire 2.3. *Si* $x, y \in V$ *et* $X = \mathrm{Mat}_{\mathcal{B}}(x), Y = \mathrm{Mat}_{\mathcal{B}}(y) \in \mathcal{M}_{n,1}(K)$, *alors* $b_q(x, y) = {}^tX \cdot \mathrm{Mat}_{\mathcal{B}}(q) \cdot Y$ *et* $q(x) = {}^tX \cdot \mathrm{Mat}_{\mathcal{B}}(q) \cdot Y$.

Proposition 2.4. q *est non dégénérée* $\Leftrightarrow \mathrm{Mat}_{\mathcal{B}}(q) \in \mathrm{GL}_n(K)$.

Ceci ne dépend pas de la base choisie.

Démonstration. On le fait par contraposition.

$\Rightarrow$: Si $\mathrm{Mat}_{\mathcal{B}}(q)$ n'est pas inversible, alors il existe $Y \in \mathcal{M}_{n,1}(K)$ non nulle telle que $\mathrm{Mat}_{\mathcal{B}}(q)Y = 0$. Donc pour tout $X \in \mathcal{M}_{n,1}(K)$, on a ${}^tX \cdot \mathrm{Mat}_{\mathcal{B}}(q) \cdot Y = 0$. Ainsi, la matrice Y représente un vecteur $y \in V^\perp \setminus \{0\}$.

$\Leftarrow$: Si q est dégénérée, alors il existe $x \in V^\perp \setminus \{0\}$. Ainsi, pour tout $u \in V$, on a $b_q(x, y) = 0$. Soit $j \in [\![1, b]\!]$ tel que $x_j \neq 0$. Si, par l'absurde $\mathrm{Mat}_{\mathcal{B}}(q)$ est inversible, alors il existe $y \in V$ tel que $\mathrm{Mat}_{\mathcal{B}}(q)Y = E_j$. Donc $b_q(x, y) = {}^tXE_j = x_j = 0$. Contradiction. □

Proposition 2.5 (Formule de changement de base)**.** *Si* $\mathcal{B}, \mathcal{B}'$ *sont deux bases, si* $P = (\lambda_{i,j})_{1 \leq i,j \leq n}$ *où* $e'_j = \sum_{i=1}^n \lambda_{i,j} e_i$, *alors* ${}^tP \,\mathrm{Mat}_{\mathcal{B}}(q) P = \mathrm{Mat}_{\mathcal{B}'}(q)$.

Démonstration.

$$\begin{aligned}
\mathrm{Mat}_{\mathcal{B}'}(q) &= \left[b_q(e'_i, e'_j)\right]_{i,j} \\
&= \left[\sum_{k=1}^n \sum_{l=1}^n \lambda_{k,i}\lambda_{l,j} b_q(e_k, e_l)\right]_{i,j} \\
&= \left[\sum_{k=1}^n \lambda_{k,i} \sum_{l=1}^n b_q(e_k, e_l)\lambda_{l,j}\right]_{i,j} \\
&= \left({}^tP \left[\sum_{l=1}^n b_q(e_k, e_l)\lambda_{l,j}\right]\right)_{i,j} \\
&= {}^tP \,\mathrm{Mat}_{\mathcal{B}}(q) P
\end{aligned}$$

□

Définition 2.6. On dit que deux matrices M, M' sont congruentes, s'il existe une matrice $P \in \mathrm{GL}_n(K)$ telle que ${}^tPMP = M'$.

Proposition 2.7. *Deux formes quadratiques* q, q' *sont équivalentes si, et seulement si, les matrices* $\mathrm{Mat}_{\mathcal{B}}(q)$ *et* $\mathrm{Mat}_{\mathcal{B}}(q')$ *sont congruentes.*

Démonstration.

$$\begin{aligned}
q' = q \circ u &\Leftrightarrow b_{q'}(e_i, e_j) = b_q(u(e_i), u(e_j)) \quad \forall 1 \leq i, j \leq n \\
&\Leftrightarrow \mathrm{Mat}_{\mathcal{B}}(q') = {}^t\,\mathrm{Mat}_{\mathcal{B}}(u) \,\mathrm{Mat}_{\mathcal{B}}(q) \,\mathrm{Mat}_{\mathcal{B}}(u)
\end{aligned}$$

□

2.2 Algorithme de Gauss de réduction des formes quadratiques

Soit V un K-espace vectoriel de dimension finie n avec $\mathrm{car}(K) \neq 2$.

Définition 2.8 (Bases orthogonales)**.** Soit q une forme quadratique. Une base $\mathcal{B} = (e_1, \ldots, e_n)$ de V est dite *q-orthogonale* (ou orthogonale par rapport à q) si pour tous $i \neq j \in [\![1, n]\!]$, on a $b_q(e_i, e_j) = 0$.

Si, de plus, on a pour tout $i \in [\![1, n]\!]$ l'égalité $b_q(e_i, e_i) = q(e_i) = 1$, alors on dit que $\mathcal{B}$ est *q-orthonormale* (ou orthonormée par rapport à q).

Fait 2.9. *$\mathcal{B}$ est q-orthogonale si, et seulement si,* $\mathrm{Mat}_{\mathcal{B}}(q)$ *est diagonale.*

Théorème 2.10 (Théorème de réduction de Gauss)**.** *Soit q une forme quadratique sur V. Alors il existe une base $\mathcal{B}$ qui est q-orthogonale.*

De plus, le rang de q est le rang de $\mathrm{Mat}_{\mathcal{B}}(q)$*, autrement dit si* $\mathrm{Mat}_{\mathcal{B}}(q) = \mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0)$ *est de rang r, alors $r = \dim V - \dim \ker q$.*

Démonstration. Soit $(e_1, \ldots, e_n)$ une base V.

Comme $\mathrm{car}(K) \neq 2$, on a vu dans la solution d'un exercice de la Feuille n°9 qu'on peut identifier les formes linéaires aux polynômes homogènes de degré 1 en n variables et les formes quadratiques aux polynômes homogènes de degré 2.

Il suffit de montrer que tout polynôme homogène Q de degré 2 en n variables $X_1, \ldots, X_n$ s'écrit sous la forme

$$Q = \sum_{i=1}^{n} \lambda_i L_i^2, \tag{1}$$

où $L_1, \cdots, L_n$ sont des polynômes homogènes de degré 1 en $X_1, \cdots, X_n$ linéairement indépendants et $\lambda_1, \cdots, \lambda_n \in K^\times$. En effet, si cette assertion est vraie, alors les formes linéaires associées aux L_i forment une base de V^*, et il suffit de considérer la base $\mathcal{B}' = (e'_1, \cdots e'_n)$ antéduale de celle-ci. On a alors

$$q(x) = \sum_{i=1}^{n} \lambda_i (x'_i)^2$$

où x est de coordonnées $(x'_1, \cdots, x'_n)$ dans $\mathcal{B}'$ par construction. On en déduit immédiatement que $\mathcal{B}'$ est orthogonale pour q.

Nous allons donc démontrer le théorème de Gauss pour les polynômes homogènes de degré 2 en n variables par récurrence sur n.

Si $n = 0$ ou 1, c'est immédiat. Supposons maintenant que le théorème est vrai jusqu'au rang $n - 1$ avec $n \geq 2$, nous allons le montrer pour n.

Soit $Q \in K[X_1, \ldots, X_n]$ homogène de degré 2, on l'écrit sous la forme

$$Q = \sum_{i=1}^{n} a_i X_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij} X_i X_j.$$

• Premier cas : il existe i tel que $a_i \neq 0$.

Quitte à permuter les variables, on peut supposer que $a_1 \neq 0$ puis même que $a_1 = 1$ (car si Q/a_1 vérifie (1), Q également en multipliant les coefficients λ_i par a_1).

On peut alors écrire

$$Q = X_1^2 + 2X_1 \sum_{j=2}^{n} a_j X_j + 2 \sum_{2 \leq i < j \leq n} a_{ij} X_i X_j$$
$$Q = X_1^2 + 2X_1 L + Q_1$$

avec L et Q_1 des formes respectivement linéaire et quadratique en $n - 1$ variables $X_2, \ldots, X_n$. On écrit alors

$$Q = (X_1 + L)^2 + (Q_1 - L^2),$$

et on choisit $\lambda_1 = 1, L_1 = x_1 + L$. Par hypothèse de récurrence, comme $Q_1 - L^2$ est une forme quadratique en $n - 1$ variables $X_2, \ldots, X_n$, on a

$$Q_1 - L^2 = \sum_{i=2}^{n} \lambda_i L_i^2,$$

et il ne reste plus qu'à montrer que $L_1, \cdots, L_n$ sont bien linéairement indépendantes. Les formes $L_2, \cdots, L_n$ le sont par construction, mais elles s'annulent toutes en $(1, 0, \cdots, 0)$ alors que L_1 non. On a donc bien l'indépendance linéaire.

• Deuxième cas : pour tout i, on a $a_i = 0$.

A moins que Q soit nul (cas immédiatement résolu), on peut supposer quitte à permuter les variables et normaliser que $a_{12} = 1/2$. Ceci permet d'écrire (suivant les mêmes idées qu'auparavant)

$$Q = x_1 x_2 + x_1 L^{(1)} + x_2 L^{(2)} + Q_1$$

avec L, L', Q_1 respectivement linéaire, linéaire et quadratique, qui dépendent seulement des variables $X_3, \ldots, X_n$. On peut réécrire ceci

$$\begin{aligned} Q &= (x_1 + L^{(2)})(x_2 + L^{(1)}) + (Q_1 - L^{(1)} L^{(2)}) \\ &= \frac{1}{4}\left(L_1^2 - L_2^2\right) + Q_2 \end{aligned}$$

avec

$$L_1 = x_1 + x_2 + L^{(1)} + L^{(2)}, \qquad L_2 = x_1 - x_2 - L^{(1)} + L^{(2)}, \qquad Q_2 = Q_1 - L^{(1)} L^{(2)}.$$

Par hypothèse de récurrence, on peut écrire

$$Q_2 = \sum_{i=3}^{n} \lambda_i L_i^2,$$

avec $L_3, \cdots, L_n$ linéaires en $X_3, \ldots, X_n$ et linéairement indépendantes. En insérant cette formule dans l'expression ci-dessus, on obtient (1) pour Q. Pour l'indépendance linéaire, on observe que $L_3, \cdots, L_n$ engendrent en fait toutes les formes linéaires en $x_3, \cdots, x_n$, en particulier les formes $X_3, \ldots, X_n$. En conséquence, vu les définitions de L_1 et L_2, les formes linéaires $L_1, \cdots, L_n$ engendrent $X_1 + X_2$ et $X_1 - X_2$, donc X_1, X_2. Ceci prouve que cette famille engendre les polynômes linéaires en n variables, de dimension n, donc la famille est une base, en particulier libre. □

2.3 Application à la classification des formes quadratiques

Notation 2.11. On note $K^{\times 2}$ le sous-groupe de $K^{\times}$ constitué par les carrés de K.

Corollaire 2.12. *Si K est un corps algébriquement clos de caractéristique $\operatorname{car}(K) \neq 2$, alors le rang est un invariant total pour l'action de $\mathrm{GL}(V)$ par équivalence sur les formes quadratiques sur V.*

En particulier, il y a exactement $n+1$ classes d'équivalences.

Enfin, une forme quadratique q admet une base q-orthonormée si, et seulement si, elle est non dégénérée.

Démonstration. Comme K est algébriquement clos, on a $K^{\times} = K^{\times 2}$.

Si q est une forme quadratique, alors il existe $\mathcal{B} = (e_1, \ldots, e_n)$ une base q-orthogonale telle que $\mathrm{Mat}_{\mathcal{B}}(q) = \operatorname{diag}(\lambda_1, \ldots, \lambda_r, 0, \ldots, 0)$ avec $\lambda_i \in K^{\times}$. On note $\lambda_i = q(e_i)$ et $\mu_i \in K^{\times}$ tel que $\mu_i^2 = \lambda_i$. Alors la base $\mathcal{B}'$ donnée par $e'_i = \begin{cases} \frac{e_i}{\mu_i} & \text{si } i \leq r \\ e_i & \text{sinon } \lambda_i \neq 0 \end{cases}$ vérifie $\mathrm{Mat}_{\mathcal{B}'}(q) = (\underbrace{1, \ldots, 1}_{r \text{ termes}}, 0, \ldots, 0)$.

q et q' sont équivalentes $\iff$ $\mathrm{Mat}_{\mathcal{B}'}(q)$ et $\mathrm{Mat}_{\mathcal{B}'}(q')$ sont congruentes. Les orbites sont alors décrites par le rang. □

Théorème 2.13 (Loi d'inertie de Sylvester)**.** *Si $K = \mathbb{R}$, alors toute forme quadratique sur $V \simeq \mathbb{R}^n$ est équivalente à $\operatorname{diag}(\underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{r-s}, 0, \ldots, 0)$ avec $0 \leq s \leq r = \operatorname{rg}(q)$.*

De plus s est la dimension maximale d'un sous-espace de V sur lequel q est définie positive.

La quantité $q \mapsto (r, s)$ est un invariant totale d'équivalence des formes quadratiques réelles. On l'appelle la signature *de q.*

Démonstration. Il suffit de voir que $\mathbb{R}^{\times 2} = \mathbb{R}_+^*$. □

Corollaire 2.14. *Sur $\mathbb{R}^n$, il y a exactement $\frac{(n+1)(n+2)}{2}$ classes d'équivalences.*

Démonstration. Ce nombre est $\sum_{r=0}^{n} \sum_{s=0}^{r} 1 = \sum_{r=0}^{n} (r+1)$. □

Théorème 2.15. *Si K est un corps fini de caractéristique* $\mathrm{car}(K) \neq 2$*, alors* $\mathrm{Mat}_{\mathcal{B}}(q)$ *est congruente à* $\mathrm{diag}(\underbrace{1, \ldots, 1}_{r-1}, d, 0, \ldots, 0)$ *avec* $d = \mathrm{disc}(q)$ *et* $r = \mathrm{rg}(q)$.

Ainsi, $q \mapsto (r, d) = (\mathrm{rg}(q), \mathrm{disc}(q))$ *est un invariant total classifiant les formes quadratiques sur un corps fini.*

3 Formes hermitiennes, groupe unitaire et espaces hermitiens

On suppose dans ce chapitre que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et que V est un $\mathbb{K}$-espace vectoriel de dimension finie.

Remarque 3.1. Plus généralement, on pourrait supposer seulement que K est un corps de sous-corps premier k et σ est un élément d'ordre 2 de $\mathrm{Aut}_k(K)$. Dans notre cas particulier, σ désigne la conjugaison complexe.

On notera que $\mathbb{C}^n$ est aussi naturellement un $\mathbb{R}$-espace vectoriel de dimension $2n$, en oubliant sa structure complexe.

3.1 Formes hermitiennes

Les formes hermitiennes jouent un rôle analogue aux formes quadratiques à ceci près qu'elles tiennent, en plus, compte de la structure complexe sur V.

Définition 3.2. Une *forme sesquilinéaire* sur V est une application $\varphi : V \times V \to \mathbb{C}$ telle que :
- $\forall x \in V,\ y \mapsto \varphi(x, y)$ est $\mathbb{C}$-linéaire ;
- $\forall y \in V,\ x \mapsto \varphi(x, y)$ est semi-linéaire, c'est-à-dire que

$$\forall z, z' \in V,\ \forall \lambda, \mu \in \mathbb{C},\ \varphi(\lambda z + \mu z', y) = \overline{\lambda}\varphi(z, y) + \overline{\mu}\varphi(z', y).$$

On généralise naturellement les notions d'orthogonalités des sous-$\mathbb{C}$-espaces vectoriels de V par rapport à φ. Une forme sesquilinéaire est dite *non dégénérée* si les espaces orthogonaux de V par rapport à φ sont nuls, c'est-à-dire si

$$\text{pour tout } x \in V, \text{ on a } \forall y \in V,\ \varphi(x, y) = 0 \Rightarrow x = 0$$

et

$$\text{pour tout } y \in V, \text{ on a } \forall x \in V,\ \varphi(x, y) = 0 \Rightarrow y = 0$$

Enfin, on dit que φ est *anisotrope* si $\varphi(x, x) = 0 \Rightarrow x = 0$ et qu'elle est *définie positive* si

$$\forall x \in V \setminus \{0\},\ \varphi(x, x) > 0.$$

Remarque 3.3. Une forme sesquilinéaire définie positive est toujours non dégénérée.

Notation 3.4. La matrice d'une forme sesquilinéaire φ dans une $\mathbb{C}$-base $\mathcal{B} = (e_1, \ldots, e_n)$ de V, est

$$\mathrm{Mat}_{\mathcal{B}}(\varphi) = [\varphi(e_i, e_j)]_{1 \leq i,j \leq n}.$$

Pour toute matrice $M = [m_{i,j}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{m,n}(\mathbb{C})$, on note $\overline{M} = [\overline{m_{i,j}}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{n,m}(\mathbb{C})$ et $M^* = {}^t\overline{M}$.

Fait 3.5. *Soit φ une forme sesquilinéaire sur V. Pour $x, y \in V$, si $X, Y \in \mathcal{M}_{n,1}(\mathbb{C})$ représentent x, y respectivement, alors $\varphi(x, y) = X^* \mathrm{Mat}_{\mathcal{B}}(\varphi) Y$.*

Définition 3.6. Une forme sesquilinéaire φ est dite *hermitienne* (resp. *antihermitienne*) si $\forall x, y \in V$ on a $\varphi(x, y) = \overline{\varphi(y, x)}$ (resp. $\varphi(x, y) = -\overline{\varphi(y, x)}$).

Fait 3.7. *Matriciellement,*

$$\varphi \textit{ est hermitienne } \iff \mathrm{Mat}_{\mathcal{B}}(\varphi)^* = \mathrm{Mat}_{\mathcal{B}}(\varphi)$$

et

$$\varphi \textit{ est antihermitienne } \iff \mathrm{Mat}_{\mathcal{B}}(\varphi)^* = -\mathrm{Mat}_{\mathcal{B}}(\varphi)$$

Remarque 3.8. Toute forme sesquilinéaire se décompose de manière unique en somme d'une forme hermitienne et d'une forme antihermitienne.

En effet, $(x, y) \mapsto \varphi(x, y) \pm \overline{\varphi(y, x)}$ sont respectivement hermitienne et antihermitienne, ce qui donne l'existence. On laisse l'unicité en exercice au lecteur.

Remarque 3.9. Si $\mathbb{K} = \mathbb{R}$, alors une forme sesquilinéaire est en fait $\mathbb{R}$-bilinéaire et une forme hermitienne est la forme polaire d'une forme quadratique réelle.

Définition 3.10. On appelle *espace hermitien* un couple (H, φ) formé d'un $\mathbb{C}$-espace vectoriel de dimension finie et d'une forme hermitienne définie positive φ.

On appelle *espace euclidien* un couple (E, φ) formé d'un $\mathbb{R}$-espace vectoriel de dimension finie et d'une forme bilinéaire symétrique définie positive φ.

Sur un tel espace, la forme φ permet de définir une norme $\|\cdot\| : x \mapsto \varphi(x, x)$. On dit que φ est un produit scalaire hermitien (resp. euclidien).

Proposition 3.11 (Inégalité de Cauchy-Schwarz)**.** *Soit (H, φ) un espace hermitien. Alors pour tous $x, y \in H$, on a*

$$|\varphi(x, y)| \leq \|x\|\|y\|$$

avec égalité si, et seulement si, la famille (x, y) est liée.

Corollaire 3.12. *Une forme hermitienne positive est définie si, et seulement si, elle est non dégénérée.*

3.2 Endomorphismes remarquables

Dans cette section, on se fixe φ une forme sesquilinéaire (ou hermitienne) non dégénérée sur V.

Fait 3.13. *Pour toute forme linéaire $f \in V^*$, il existe un unique $x = x_f \in V$ tel que $\varphi(x, \cdot) = f$.*

Proposition-définition 3.14. Soit $u \in \mathrm{End}_{\mathbb{C}}(V)$. Il existe un unique endomorphisme $u^* \in \mathrm{End}_{\mathbb{C}}(V)$ tel que $\forall x, y \in V,\ \varphi(u^*(x), y) = \varphi(x, u(y))$. On l'appelle *endomorphisme adjoint* de u.

Démonstration. Matriciellement, on a $M = \mathrm{Mat}_{\mathcal{B}}(\varphi) \in \mathrm{GL}_n(\mathbb{C})$ car φ est non dégénérée. Donc $\mathrm{Mat}_{\mathcal{B}}(u^*) = M^{-1}\,\mathrm{Mat}_{\mathcal{B}}(u)^* M$ convient. □

Corollaire 3.15. *Soit $u, v \in \mathrm{End}_{\mathbb{C}}(V)$ et $\lambda \in \mathbb{C}$. On a les égalités :*

1. $(u^*)^* = u$;
2. $(\lambda u)^* = \overline{\lambda} u^*$;
3. $(u_1 + u_2)^* = u_1^* + u_2^*$;
4. $(u_1 \circ u_2)^* = u_2^* \circ u_1^*$.

Définition 3.16 (Endomorphismes remarquables)**.** Soit $u \in \mathrm{End}_{\mathbb{C}}(V)$. On dit que u est :

– *normal* si $u^* \circ u = u \circ u^*$;
– *hermitien* si $u^* = u$;
– *antihermitien* si $u^* = -u$;
– *unitaire* si $u^* \circ u = \mathrm{id}_V$.

L'ensemble $\mathcal{U}(\varphi)$ des endomorphismes unitaires pour φ est un sous-groupe de $\mathrm{GL}(V)$ appelé *groupe unitaire. On note également $\mathcal{SU}(\varphi)$ le sous-groupe des endomorphismes unitaires de déterminant* 1*, appelé* groupe spécial unitaire.

Fait 3.17. *Les endomorphismes hermitiens, antihermitiens, unitaires sont normaux.*

Remarque 3.18. Si on remplace partout $\mathbb{C}$ par $\mathbb{R}$, alors une forme hermitienne est simplement une forme quadratique et on parle alors d'endomorphisme *symétrique* pour hermitien, *antisymétrique* pour antihermitien, *orthogonal* pour unitaire.

On trouve aussi parfois la terminologie *endomorphisme auto-adjoint* – au lieu de symétrique, hermitien – mais ceci s'intéresse davantage aux espaces de dimension infinie provenant de l'analyse.

3.3 Réduction des endomorphismes normaux

On suppose désormais que φ est une forme hermitienne anisotrope.

Lemme 3.19. *Si u est un endomorphisme normal et $P \in \mathbb{C}[X]$, alors $P(u)$ est normal.*

Démonstration. $P(u)^* = \overline{P}(u^*)$. Donc si u et u^* commutent, alors $P(u)$ et $P(u^*)$ aussi. □

Proposition 3.20. *Si u est un endomorphisme normal et $P \in \mathbb{C}[X]$, alors $(\ker P(u))^{\perp}$ est stable par u.*

Démonstration. Soit $y \in (\ker P(u))^{\perp}$ et $x \in \ker P(u)$. On veut montrer que $\varphi(x, u(y)) = 0$. On a $\varphi(x, u(y)) = \varphi(u^*(x), y)$. Mais $P(u) \circ u^*(x) = u^* \circ P(u)(x) = 0$. Donc $u^*(x) \in \ker P(u)$. Donc $\varphi(u^*(x), y) = 0$. □

Proposition 3.21. *On a* $\ker u^* = (\operatorname{im} u)^{\perp}$ *et* $\operatorname{im}(u^*) = (\ker u)^{\perp}$.

Démonstration.

$$\begin{aligned} y \in \ker u^* &\Leftrightarrow \forall x \in V,\ \varphi(u^*(y), x) = 0 \\ &\Leftrightarrow \forall x \in V,\ \varphi(y, u(x)) = 0 \\ &\Leftrightarrow y \in (\operatorname{im} u)^{\perp} \end{aligned}$$

En échangeant u et u^*, on a $\ker u = (\operatorname{im} u^*)^{\perp}$. On conclut car en dimension finie $\left(W^{\perp}\right)^{\perp} = W$ pour tout sous-espace vectoriel W de V. □

Proposition 3.22. *Si u est normal, alors* $\operatorname{im} u = (\ker u)^{\perp}$.

Démonstration. Soit $x \in (\operatorname{im} u)^{\perp}$. On a

$$\begin{aligned} \varphi(u(x), u(x)) &= \varphi(u^*(u(x)), x) \\ &= \varphi(u(u^*(x)), x) && \text{car } u \text{ est normal} \\ &= \overline{\varphi(x, u(u^*(x)))} && \text{car } \varphi \text{ est hermitienne} \\ &= 0 && \text{car } x \in (\operatorname{im} u)^{\perp} \end{aligned}$$

Comme φ est anisotrope, on a $u(x) = 0$ donc $x \in \ker u$. Ainsi $(\operatorname{im} u)^{\perp} \subset \ker u$. On a égalité par égalité des dimensions en appliquant le théorème du rang : $\dim \operatorname{im} u = \dim V - \dim \ker u = \dim (\ker u)^{\perp}$. □

Théorème 3.23. *Soit u un endomorphisme normal ($K = \mathbb{R}$ ou $\mathbb{C}$) et $\chi_u = \prod_{i=1}^{m} P_i^{m_i}$ la décomposition du polynôme caractéristique de u en puissances de polynômes irréductibles unitaires deux à deux premiers entre eux. Alors* $V = \overset{\perp}{\bigoplus\limits_{i \in [\![1,m]\!]}} \ker P_i(u)$.

En particulier, u normal est diagonalisable en base orthonormée pour φ si, et seulement si, χ_u est scindé.

Démonstration. On a vu que $P_i(u)$ est normal et que $\operatorname{im} P_i(u) = (\ker P_i(u))^{\perp}$. De plus, $\operatorname{im} P_i(u) \cap \ker P_i(u) = 0$ car φ est anisotrope. Donc on en déduit par récurrence immédiate que $\ker P_i(u)^j = \ker P_i(u)$ pour tous $i, j \geq 1$. Le lemme des noyaux nous donne $V = \bigoplus\limits_{i \in [\![1,m]\!]} \ker P_i(u)^{m_i} = \bigoplus\limits_{i \in [\![1,m]\!]} \ker P_i(u)$. Il suffit de vérifier que la somme directe est orthogonale.

Par Bézout, il existe des polynômes $U, V \in \mathbb{K}[X]$ tels que $UP_i + VP_j = 1$. Soit $x \in \ker P_j(u)$ qu'on écrit $x = U(u) \circ P_i(u)(x) + V(u) \circ P_j(u)(x) = P_i(u) \circ U(u)(x) \in \operatorname{im} P_i(u) = (\ker P_i(u))^{\perp}$. Ainsi $\ker P_j(u) \subset (\ker P_i(u))^{\perp}$, donc la somme directe est orthogonale. □

Théorème 3.24 (Théorème spectral)**.** *Soit V un $\mathbb{K}$-espace vectoriel et φ une forme sesquilinéaire non dégénérée sur V. Soit u un endomorphisme φ-autoadjoint. Alors u est diagonalisable sur $\mathbb{K}$ et admet une base φ-orthogonale de vecteurs propres.*

Corollaire 3.25 (Théorème spectral hermitien)**.**
On suppose que φ est hermitienne définie positive. Soit $u \in \operatorname{End}_{\mathbb{C}}(V)$. Alors

$$u \text{ est normal} \iff u \text{ est diagonalisable en base } \varphi\text{-orthonormée}$$

et

$$u \text{ est unitaire} \iff u \text{ est diagonalisable en base } \varphi\text{-orthonormée et ses valeurs propres sont de module } 1.$$

Corollaire 3.26 (Théorème spectral euclidien)**.**
On suppose que (V, φ) est un espace euclidien. Soit $u \in \operatorname{End}_{\mathbb{R}}(V)$. Alors

$$u \text{ est symétrique} \iff u \text{ est diagonalisable en base } \varphi\text{-orthonormée},$$

$$u \text{ est normal } \iff u \text{ est diagonalisable par blocs en base orthonormée,}$$

$$\text{avec des blocs de la forme } M_i = \begin{cases} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \text{avec } b \in \mathbb{R}^* \text{ et } a \in \mathbb{R} \\ (a) & \text{avec } a \in \mathbb{R} \end{cases}, \text{ et}$$

$$u \text{ est orthogonal } \iff u \text{ est diagonalisable par blocs en base } \varphi\text{-orthonormée}$$

$$\text{avec des blocs de la forme } M_i = \begin{cases} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} & \text{avec } \theta \in \mathbb{R} \\ (a) & \text{avec } a \in \{\pm 1\} \end{cases},$$

Les démonstrations de ces deux corollaires sont laissées en exercice au lecteur.

Pour conclure voici un procédé pour obtenir des bases orthonormées.

Proposition 3.27 (Procédé d'orthonormalisation de Gram-Schmidt)**.** *Soit (H, φ) un espace hermitien et $(e_1, \dots, e_n)$ une base quelconque de H. Alors il existe une $\mathbb{K}$-base $(f_1, \dots, f_n)$ de H qui est φ-orthonormée et telle que* $\mathrm{Vect}(f_1, \dots, f_m) = \mathrm{Vect}(e_1, \dots, e_m)$ *pour tout $1 \leq m \leq n$.*

Démonstration. Pour $m = 1$, on pose $f_1 = \frac{e_1}{\sqrt{\varphi(e_1, e_1)}}$.

Supposons $(f_1, \dots, f_m)$ construite de sorte que $\varphi(f_i, f_i) = 1$ et $\varphi(f_i, f_j) = 0$ pour $1 \leq i \neq j \leq m$ et $\mathrm{Vect}(f_1, \dots, f_m) = \mathrm{Vect}(e_1, \dots, e_m)$. Soit $g_{m+1} = e_{m+1} - \sum_{i=1}^{m} \varphi(e_{m+1}, f_i) f_i \neq 0$ car $e_{m+1} \notin \mathrm{Vect}(f_1, \dots, f_m)$. On pose $f_{m+1} = \frac{g_{m+1}}{\sqrt{\varphi(g_{m+1}, g_{m+1}}}$. On vérifie alors par linéarité de f_{m+1} convient. ☐

3.4 Interprétation matricielle du théorème spectral, décomposition polaire

On note $\mathcal{S}_n(\mathbb{R})$ l'espace vectoriel des matrices symétriques réelles, $\mathcal{S}_n^+(\mathbb{R})$ le cône des matrices symétriques positives (i.e. ${}^tXMX$ et $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies positives. Le théorème spectral se réécrit :

Théorème 3.28 (Théorème spectral matriciel et réduction simultanée)**.**

(1) Toute matrice $M \in \mathcal{S}_n(\mathbb{R})$ s'écrit $M = P^{-1}DP$ avec $P \in \mathcal{O}_n(\mathbb{R})$ et D diagonale.

(2) Si $M \in \mathcal{S}_n(\mathbb{R})$ et $Q \in \mathcal{S}_n^{++}(\mathbb{R})$, alors il existe $P \in \mathrm{GL}_n(\mathbb{R})$ et D diagonale tels que $Q = {}^tPP$ et $Q = {}^tPDP$.

Démonstration. (1) On montre d'abord que toutes les valeurs propres complexes de M sont réelles. En effet, si $\lambda \in \mathbb{C}$ est valeur propre, de vecteur propre complexe $X \in \mathcal{M}_{n,1}(\mathbb{C})$, alors $MX = \lambda X$ donc $\overline{\lambda} X^* X = (\lambda X)^* X = (MX)^* X = X^* M X = \lambda X^* X$. Comme $X^* X = \|X\| > 0$, on en déduit que $\overline{\lambda} = \lambda$ est réel.

Ainsi, M admet un vecteur propre réel X et comme M est normal, on a également une décomposition en somme directe orthogonale de sous-espaces M-stables $\mathbb{R}X \overset{\perp}{\oplus} X^{\perp} = \mathbb{R}^n$. On conclut par récurrence sur la dimension.

(1) $\Rightarrow$ (2) : y réfléchir. ☐

Corollaire 3.29 (Unicité de la racine carrée)**.** *Toute matrice $M \in \mathcal{S}_n^+(\mathbb{R})$ admet une racine carrée $N \in \mathcal{S}_n^+(\mathbb{R})$, c'est-à-dire $N^2 = M$.*

Si $M \in \mathcal{S}_n^{++}(\mathbb{R})$, alors $N \in \mathcal{S}_n^{++}(\mathbb{R})$ est unique.

Démonstration. On écrit $M = P^{-1}DP$ avec $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ diagonale constituée des valeurs propres de M, donc (resp. strictement) positives.

Existence : $N = P^{-1} \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) P$ convient.

Unicité : Soit $S \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $S^2 = M$. Alors S est diagonalisable et commute à M. Soit Q le polynôme interpolateur de Lagrange donné par $Q(\lambda_i) = \sqrt{\lambda_i}$. Alors $Q(M) = Q(P^{-1}DP) = P^{-1}Q(D)P = P^{-1}\sqrt{D}P = N$. Comme S et $Q(S^2) = Q(M) = N$ commutent, ils sont codiagonalisables. Soit $U = S^{-1}N$. Alors $U \in \mathcal{S}_n^{++}$ car ${}^t(S^{-1}N) = {}^tN {}^tS^{-1} = NS^{-1} = S^{-1}N$ et les valeurs propres de U sont des produits d'une valeur propre de N et d'une valeur propre de S^{-1} donc strictement positives. De plus $U^2 = S^{-2}N^2 = M^{-1}M = I_n$, donc les valeurs propres de U sont dans $\{\pm 1\}$. Ainsi $U = I_n$ donc $S = N$. ☐

Théorème 3.30 (Décomposition polaire)**.** *Pour toute matrice $M \in \mathrm{GL}_n(\mathbb{R})$, il existe un unique couple $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$ tel que $M = OS$.*

$$\textit{De plus, l'application } \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array} \textit{ est un homéomorphisme.}$$

Pour toute matrice $M \in \mathcal{M}_n(\mathbb{R})$, il existe un couple $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^+(\mathbb{R})$ tel que $M = OS$, ce couple n'est pas nécessairement unique.

Démonstration. **Unicité :** Si $M = OS$, alors ${}^tMM = {}^tS^tOOS = {}^tSS = S^2$. Ainsi nécessairement $S = \sqrt{{}^tMM}$ et donc $O = MS^{-1}$.

Existence : Il reste à montrer que $O = MS^{-1}$ est orthogonale.

$$O^tO = (MS^{-1})^t(MS^{-1}) = MS^{-1t}S^{-1t}M = MS^{-2t}M = M\left({}^tMM\right)^{-1}M = I_n$$

Ainsi l'application $(O, S) \mapsto OS$ est bijective, continue. Il reste à montrer que son inverse est continue. On utilise un critère métrique de caractérisation. Soit $M_k \underset{k\to\infty}{\longrightarrow} M$. On écrit $M_k = O_kS_k$ avec $O_k \in \mathcal{O}_n(\mathbb{R})$ et $S_k \in \mathcal{S}_n^{++}(\mathbb{R})$. Comme $\mathcal{O}_n(\mathbb{R})$ est compact, on peut extraire une sous-suite convergente $O_{\varphi(k)} \underset{k\to\infty}{\longrightarrow} O'$. Alors $\lim_{k\to\infty} O_{\varphi(k)}^{-1}M_{\varphi(k)} = {O'}^{-1}M$ est symétrique comme limite de matrices dans l'espace vectoriel des matrices symétriques (fermé de $\mathrm{GL}_n(\mathbb{R})$ donc, par unicité $O' = O$ est la seule valeur d'adhérence de la suite (O_k). Ainsi $O_k \underset{k\to\infty}{\longrightarrow} O$ et donc $S_k = O_k^{-1}M_k \underset{k\to\infty}{\longrightarrow} S$. □

Corollaire 3.31. *Le groupe $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe compact maximal de $\mathrm{GL}_n(\mathbb{R})$.*