

A. Produit scalaire de matrices

- (1) Soit $(e_1, e_2, \dots, e_n)$ une base orthonormée. La i -ième composante d'un vecteur x de $\mathbb{R}^n$ dans est donnée par $\langle x, e_i \rangle$.

En particulier, $\langle Ae_i, e_i \rangle$ représente la i -ième composante du vecteur Ae_i , où u_A désigne l'endomorphisme de $\mathbb{R}^n$ canoniquement associé à A .

Par suite, $\sum_{i=1}^n \langle Ae_i, e_i \rangle$ est la somme des éléments diagonaux de la matrice de u_A dans la base $(e_1, e_2, \dots, e_n)$; il s'agit de la trace de u_A , et donc de la trace $\text{Tr}(A)$.

- (2) Soient A et B deux matrices symétriques réelles positives. Par le théorème spectral, on peut considérer $(e_1, \dots, e_n)$ une base orthonormée de vecteurs propres de B : pour tout $1 \leq i \leq n$, $Be_i = \lambda_i e_i$ (avec les $\lambda_i \geq 0$).

D'après la question A1

$$\begin{aligned} (A|B) &= \text{Tr}(^tAB) = \sum_{i=1}^n \langle ^tABe_i, e_i \rangle = \sum_{i=1}^n \lambda_i \langle ^tAe_i, e_i \rangle \\ &= \sum_{i=1}^n \lambda_i \langle e_i, Ae_i \rangle. \end{aligned}$$

Comme pour tout $1 \leq i \leq n$, $\lambda_i \geq 0$ et $\langle e_i, Ae_i \rangle \geq 0$, on peut conclure que $(A|B) \geq 0$.

B. Décomposition polaire

- (1) On constate immédiatement que $^t(^tAA) = ^tAA$. Puis, pour tout X , $^tX^tAAX = \|AX\|^2 \geq 0$, donc tAA est symétrique positive.

Soient $\lambda_1 \leq \dots \leq \lambda_n$ les valeurs propres de tAA ; on introduit $(e_j)_{1 \leq j \leq n}$ une base orthonormée associée.

Tout vecteur $X \in \mathbb{R}^n$ se décompose sur cette base : $X = \sum_{i=1}^n x_i e_i$; on a

alors on a $\|AX\|^2 = ^tX^tAAX = \sum_{i=1}^n \lambda_i x_i^2 \leq \lambda_n \|X\|^2$. On en déduit donc

$$\|A\|_2 \leq \sqrt{\lambda_n}.$$

Or, il existe un cas d'égalité : $\|Ae_n\|^2 = ^t e_n ^t A A e_n = \lambda_n$, et $\|e_n\| = 1$. Finalement, $\|A\|_2^2$ est la plus grande valeur propre de tAA .

- (2) Par le théorème spectral, on écrit $^tAA = PDP^{-1} = PD^tP$, où $P \in O_n(\mathbb{R})$, D diagonale, ses éléments étant positifs. On peut alors choisir une

matrice diagonale à éléments positifs, Δ , telle que $\Delta^2 = D$. On obtient alors $^tAA = B^2$, où $B = P\Delta P^{-1} = P\Delta^tP$. On vérifie immédiatement que B est une matrice symétrique, à spectre inclus dans $\mathbb{R}_+$, donc positive. Soit h l'endomorphisme dont la matrice dans la base orthonormée e est B . On a bien que h est symétrique positif et $f^* \circ f = h^2$.

- (3) Comme h est symétrique (vu en compléments du cours), $\ker(h) = (\text{Im}(h))^\perp$. En effet, soit $(x, y) \in \ker(h) \times \text{Im}(h)$; on écrit $y = h(z)$ et

$$\langle y, x \rangle = \langle h(z), x \rangle = \langle z, h(x) \rangle = 0.$$

On a donc une inclusion $\ker(h) \subset (\text{Im}(h))^\perp$, et par égalité des dimensions, on a bien $\ker(h) = (\text{Im}(h))^\perp$.

Ainsi $\text{Im}(h)$ est un supplémentaire du noyau $\ker(h)$ et on sait donc que la restriction de h à $\text{Im}(h)$ induit un isomorphisme de $\text{Im}(h)$ sur lui-même, et donc un automorphisme de $\text{Im}(h)$. On notera cet automorphisme $\tilde{h}$.

- (4) Pour tout $x \in E$,

$$\|f(x)\|^2 = \langle f^* \circ f(x), x \rangle = \langle h^2(x), x \rangle = \langle h^* \circ h(x), x \rangle = \|h(x)\|^2.$$

On en déduit en particulier que $\ker h = \ker f$, d'où $\dim \ker h = \dim \ker f = \dim(\text{Im} f)^\perp$. Ainsi, on peut choisir une application linéaire v envoyant une base orthonormée de $\ker h$ sur une base orthonormée de $(\text{Im} f)^\perp$; elle conserve alors la norme et réalise un isomorphisme de $\ker h$ sur $(\text{Im} f)^\perp$.

- (5) On a vu que $E = \ker(h) \oplus \text{Im}(h)$ et $E = (\text{Im}(f))^\perp \oplus \text{Im}(f)$.

Or, on a construit un isomorphisme v de $\ker h$ sur $(\text{Im} f)^\perp$, qui préserve la norme. Par ailleurs, $\tilde{h}^{-1}$ est un isomorphisme de $\text{Im}(h)$ vers lui-même. Et comme $(\ker(f))^\perp = (\ker(h))^\perp = \text{Im}(h)$, la restriction de f à $\text{Im}(h)$ (supplémentaire du noyau $\ker(f)$) réalise un isomorphisme de $\text{Im}(h)$ vers $\text{Im}(f)$. Ainsi $f \circ \tilde{h}^{-1}$ est un isomorphisme de $\text{Im}(h)$ vers $\text{Im}(f)$. En posant u l'unique application linéaire qui coïncide avec $f \circ \tilde{h}^{-1}$ sur $\text{Im}(h)$ et avec v sur $\ker(h)$, on obtient bien un isomorphisme de E .

On remarque que $f \circ \tilde{h}^{-1}$ conserve la norme : en effet, d'après la question B4, pour tout $x \in \text{Im} h$, $\|f \circ \tilde{h}^{-1}(x)\| = \|h \circ \tilde{h}^{-1}(x)\| = \|x\|$.

Or tout vecteur $x \in E$ se décompose en $x = y + z$ avec $(y, z) \in \ker(h) \times \text{Im}(h)$ et on a alors $u(x) = v(y) + f \circ \tilde{h}^{-1}(z)$. En utilisant le théorème de Pythagore et la conservation de la norme par v et $f \circ \tilde{h}^{-1}$, on obtient finalement que u préserve la norme; il s'agit donc d'un automorphisme orthogonal.

Par ailleurs, pour tout $x \in \ker(h) = \ker(f)$, on a bien $f(x) = 0_E = u \circ h(x)$. Et pour tout $x \in \text{Im}(h)$, $h(x) = \tilde{h}(x)$ et donc $u \circ h(x) = f \circ \tilde{h}^{-1} \circ \tilde{h}(x) = f(x)$.

Ainsi les endomorphismes f et $u \circ h$ coïncident sur les sous-espaces supplémentaires $\ker h$ et $\text{Im} h$, donc sont égaux.

- (6) Il s'agit de l'interprétation matricielle du résultat de la question précédente : si f est l'endomorphisme canoniquement associé à A , la relation $f = u \circ h$ se traduit matriciellement par $A = US$, avec $U \in O_n(\mathbb{R})$ et S symétrique positive (puisque la base canonique est orthonormée pour le produit scalaire usuel).

On admet que si A est inversible, cette écriture est unique.

C. Projeté sur un convexe compact

- (1) L'application $d_x : h \mapsto \|x - h\|$, est 1-lipschitzienne donc continue de E dans $\mathbb{R}$. Comme H est compact, d_x est bornée et atteint sa borne inférieure sur H d'après le théorème des bornes, d'où l'existence de $h_0 \in H$ tel que $d(x, H) = \|x - h_0\|$.

On suppose l'existence de $h_1 \in H$, un autre élément de H tel que $d(x, H) = \|x - h_1\|$. La fonction $q : t \mapsto \|x - (1-t)h_0 - th_1\|^2$ est polynomiale en t : $q(t) = at^2 + 2bt + c$ avec $a = \|h_1 - h_0\|^2$, $b = \langle x - h_0, h_0 - h_1 \rangle$, $c = \|x - h_0\|^2$. Si $h_1 \neq h_0$, q est de degré 2 en t , de coefficient dominant strictement positif, et $q(0) = q(1) = d^2(x, H)$. Mais alors, pour tout $t \in]0, 1[$, on a $q(t) < q(0) = q(1)$, ce qui est absurde, car $q(t) = \|x - k_t\|^2$ où $k_t = (1-t)h_0 + th_1$ est un élément de H par convexité. Ainsi, h_0 est bien l'unique point où le minimum est atteint.

On pouvait également utiliser comme en TD-Cours le cas d'égalité dans l'inégalité triangulaire ou encore l'identité du parallélogramme :

$$\begin{aligned} \left\| x - \frac{1}{2}(h_0 + h_1) \right\|^2 &= \frac{1}{2} \|x - h_0\|^2 + \frac{1}{2} \|x - h_1\|^2 - \frac{1}{4} \|h_0 - h_1\|^2 \\ &< \frac{1}{2} \|x - h_0\|^2 + \frac{1}{2} \|x - h_1\|^2 = (d(x, H))^2. \end{aligned}$$

Comme H est convexe, $\frac{1}{2}(h_0 + h_1) \in H$, ce qui conduit à une contradiction avec la définition de la borne inférieure.

- (2) On suppose que $h_0 \in H$ vérifie $d(x, H) = \|x - h_0\|$. Pour tout $h_1 \in H$, on introduit la fonction q définie ci-dessus. On a vu que pour tout $t \in [0, 1]$, comme $k_t = (1-t)h_0 + th_1 \in H$, on a $q(t) \geq d(x, H) = q(0)$. Or, pour tout $t \in]0, 1[$,

$$\begin{aligned} q(t) &= \|x - h_0 + t(h_0 - h_1)\|^2 \\ &= \|x - h_0\|^2 + 2t\langle x - h_0, h_0 - h_1 \rangle + t^2\|h_0 - h_1\|^2. \end{aligned}$$

Ainsi pour tout $t \in [0, 1]$, $2t\langle x - h_0, h_0 - h_1 \rangle + t^2\|h_0 - h_1\|^2 \geq 0$, soit (comme $t > 0$) $2\langle x - h_0, h_0 - h_1 \rangle + t\|h_0 - h_1\|^2 \geq 0$. En faisant tendre t vers 0, on obtient $\langle x - h_0, h_0 - h_1 \rangle \geq 0$, ce qui fournit la condition demandée.

Réciproquement, on suppose que pour tout $h_1 \in H$, $\langle x - h_0, h_0 - h_1 \rangle \geq 0$. Ainsi en considérant la fonction q associée à h_0 et h_1 , on obtient d'après l'expression ci-dessus que pour tout $t \in [0, 1]$, $q(t) \geq \|x - h_0\|^2$. En particulier, $q(1) \geq \|x - h_0\|^2$, ce qui signifie que pour tout $h_1 \in H$, $\|x - h_1\| \geq \|x - h_0\|$ et h_0 est bien (l'unique) point de H tel que $d(x, H) = \|x - h_0\|$.

D. Théorème de Carathéodory et compacité

- (1) Voir cours.

On souhaite montrer que l'enveloppe convexe $\text{conv}(H)$ est constituée des combinaisons convexes d'au plus $n + 1$ éléments de H .

Soit $x = \sum_{j=1}^p \lambda_j x_j$ une combinaison convexe de $x_1, \dots, x_p \in H$, avec $p \geq n + 2$.

- (2) Comme $p \geq n + 2$, la famille de vecteurs $(x_j - x_1)_{2 \leq j \leq p}$ est liée. On peut donc trouver des réels non tous nuls $(\mu_i)_{2 \leq i \leq p}$, tels que $\sum_{j=1}^p \mu_j (x_j - x_1) = 0$.

En posant $\mu_1 = -\sum_{j=2}^p \mu_j$, on a bien p réels non tous nuls $(\mu_i)_{1 \leq i \leq p}$ tels que

$$\sum_{j=1}^p \mu_j x_j = 0 \quad \text{et} \quad \sum_{j=1}^p \mu_j = 0.$$

- (3) Comme $x = \sum_{j=1}^p \lambda_j x_j$ et que $\sum_{j=1}^p \mu_j x_j = 0$, pour tout $\theta \in \mathbb{R}$, $x = \sum_{j=1}^p (\lambda_j - \theta \mu_j) x_j$, avec $\sum_{j=1}^p (\lambda_j - \theta \mu_j) = 0$. Toutefois, on n'a pas nécessairement que

les $\lambda_i - \theta\mu_i \geq 0$. On cherche donc $\theta \in \mathbb{R}$ qui annule l'un des $\lambda_k - \theta\mu_k$ (pour n'avoir plus que $p-1$ points) et tel que les autres $\lambda_i - \theta\mu_i \geq 0$. Pour cela on considère $k \llbracket 1, p \rrbracket$ tel que

$$\frac{\lambda_k}{\mu_k} = \min \left\{ \frac{\lambda_i}{\mu_i}, i \in \llbracket 1, p \rrbracket, \mu_i > 0 \right\}.$$

Cet ensemble est fini et non vide car comme $\sum_{j=1}^p \mu_j = 0$ et que les μ_j sont non tous nuls, il existe au moins un $\mu_i > 0$.

Ainsi $\theta \in \mathbb{R}_+$. Par définition $\lambda_k - \theta\mu_k = 0$. Et pour tout $i \in \llbracket 1, p \rrbracket$, si $\mu_i \leq 0$, $\lambda_i - \theta\mu_i \geq \lambda_i \geq 0$, et si $\mu_i > 0$, $\lambda_i - \theta\mu_i \geq \lambda_i - \frac{\lambda_i}{\mu_i}\mu_i = 0$.

On a donc écrit x comme combinaison convexe d'au plus $p-1$ éléments de H . Si ce nombre d'éléments est encore supérieur ou égal à $n+2$, on peut recommencer le raisonnement et, par une itération finie, on se ramène à une combinaison convexe d'au plus $n+1$ éléments de H .

- (4) Soit H est une partie compacte de E . On introduit $\Lambda = \left\{ (t_i)_{1 \leq i \leq n+1} \in \mathbb{R}_+^{n+1}, \sum_{i=1}^{n+1} t_i = 1 \right\}$.

L'application $S : (\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{R}^{n+1} \mapsto \sum_{k=1}^{n+1} \lambda_k$ est continue car linéaire.

Or $\Lambda = [0, 1]^n \cap S^{-1}(\{1\})$. Comme l'image réciproque par une application continue d'un fermé est un fermé, Λ est un fermé dans le compact $[0, 1]^n$ donc compact.

Par produit de compacts, $\Lambda \times H^{n+1}$ est un compact.

On pose $\Phi : \begin{cases} \mathbb{R}^{n+1} \times E^{n+1} & \longrightarrow E \\ (\lambda_1, \dots, \lambda_{n+1}, a_1, \dots, a_{n+1}) & \longmapsto \sum_{i=1}^{n+1} \lambda_i a_i \end{cases}$. L'application

Φ est continue car bilinéaire en dimension finie.

Or, $\text{Conv}(H) = \Phi(\mathcal{H} \times H^{n+1})$; donc $\text{Conv}(H)$ est compact, comme image d'une partie compacte par une application continue.

E. Enveloppe convexe de $O_n(\mathbb{R})$

- (1) On redémontre (cf cours) que $O_n(\mathbb{R})$ est compact et on en déduit (d'après la question précédente) que $\text{conv}(O_n(\mathbb{R}))$ est compacte.

- (2) Soit $A \in O_n(\mathbb{R})$. Pour tout X de norme 1, $\|AX\| = \|X\| = 1$. Donc $\|A\|_2 \leq 1$ et ainsi $O_n(\mathbb{R})$ est contenu dans la boule $\mathcal{B}$. Or, une boule est convexe. Cette boule $\mathcal{B}$ contient alors par définition le plus petit convexe qui contient $O_n(\mathbb{R})$, soit $\text{Conv}(O_n(\mathbb{R}))$.

- (3) Soit $V \in \text{conv}(O_n(\mathbb{R}))$. D'après la caractérisation du projeté orthogonal N , on a $\langle M - N, V - N \rangle \leq 0$, soit $\langle M - N, V \rangle \leq \langle M - N, N \rangle$, ce qui se traduit par : $\text{Tr}(AV) \leq \text{Tr}(AN)$.

Par ailleurs, $M \neq N$, donc $\langle M - N, M - N \rangle > 0$, soit $\langle M - N, N \rangle < \langle M - N, M \rangle$, ce qui se traduit par $\text{Tr}(AN) < \text{Tr}(AM)$.

Ainsi, pour tout $V \in \text{Conv}(O_n(\mathbb{R}))$, $\text{Tr}(USV) < \text{Tr}(USM)$. On peut choisir $V = U^{-1}$ et on obtient alors $\text{Tr}(S) = \text{Tr}(VUS) = \text{Tr}(USV) < \text{Tr}(USM)$.

- (4) Comme S est symétrique réelle, on peut introduire une base orthonormée $(e_1, e_2, \dots, e_n)$ formée de vecteurs propres de S . Ainsi $Se_i = \lambda_i e_i$, avec $\lambda_i \geq 0$. L'inégalité de Cauchy-Schwarz donne alors :

$$\langle MUSE_i, e_i \rangle = \lambda_i \langle MUE_i, e_i \rangle \leq \lambda_i \|MUE_i\| \times \|e_i\| \leq \lambda_i \|Ue_i\| \times \|e_i\| = \lambda_i \|e_i\|^2 = \lambda_i.$$

En appliquant la question A1, on obtient

$$\text{Tr}(MUS) = \sum_{i=1}^n \langle MUSE_i, e_i \rangle \leq \sum_{i=1}^n \lambda_i = \text{Tr}(S).$$

- (5) Or $\text{Tr}(MUS) = \text{Tr}(USM)$: on obtient alors $\text{Tr}(S) < \text{Tr}(S)$. L'hypothèse $M \notin \text{conv}(O_n(\mathbb{R}))$ amenant à une contradiction, on en déduit que $\mathcal{B} \subset \text{conv}(O_n(\mathbb{R}))$, d'où finalement $\text{conv}(O_n(\mathbb{R})) = \mathcal{B}$.

F. Points extrémaux

- (1) On suppose que $U \in O_n(\mathbb{R})$ s'écrit sous la forme $U = \frac{1}{2}(V + W)$, avec V, W appartenant à $\mathcal{B}$. Soit $X \in \mathbb{R}^n$. Par inégalité triangulaire,

$$\|X\| = \|UX\| = \frac{1}{2}\|VX + WX\| \leq \frac{1}{2}(\|VX\| + \|WX\|) \leq \frac{1}{2}(\|X\| + \|X\|) = \|X\|.$$

Toutes les inégalités sont donc des égalités. La norme $\|\cdot\|$ étant euclidienne, les vecteurs VX et WX sont donc colinéaires (et de même sens). Et de plus, pour tout X , $\|VX\| = \|X\|$ et $\|WX\| = \|X\|$. On en déduit d'une part que V et $W \in O_n(\mathbb{R})$. Et comme VX et WX sont positivement liés et de même norme, nécessairement $VX = WX$, et ce pour tout X donc $V = W$, puis $V = W = U$. Ainsi U est extrémal dans $\mathcal{B}$.

- (2) En utilisant la décomposition polaire, A s'écrit sous la forme US avec $U \in O_n(\mathbb{R})$ et S symétrique positive. Alors, d'après le théorème spectral, on peut introduire $Q \in O_n(\mathbb{R})$ et D diagonale à coefficients diagonaux positifs tels que $S = Q^{-1}DQ$.

On obtient alors $A = (UQ^{-1})DQ$ et il suffit de poser $P = UQ^{-1} \in O_n(\mathbb{R})$ pour conclure.

On retrouve la décomposition en valeurs singulières de A , mais comme A est une matrice carrée, la décomposition polaire nous donne une démonstration plus rapide.

- (3) Soit $i \in \llbracket 1, n \rrbracket$. On considère $X = Q^{-1}e_i$, où e_i désigne le i -ième vecteur de la base canonique de $\mathbb{R}^n$. On a alors $\|QX\| = \|X\| = 1$ et comme A appartient à $\mathcal{B}$, il vient $\|AX\| \leq 1$.

Or $AX = PDe_i = P(d_ie_i)$ donc, comme d_i est positif, $\|AX\| = d_i\|Pe_i\| = d_i\|e_i\| = d_i$, ce qui conduit à $d_i \leq 1$.

Si tous les coefficients d_i valaient 1, D serait égale à la matrice identité I_n , d'où $A = PQ \in O_n(\mathbb{R})$: impossible. Il existe donc un indice $j \in \llbracket 1, n \rrbracket$ tel que $d_j < 1$.

- (4) On pose un tel indice j , et on note $\alpha = 1 - d_j > 0$. On introduit D_α , *resp.* $D_{-\alpha}$, la matrice diagonale dont les coefficients diagonaux sont les mêmes que ceux de D , à l'exception du j -ième qui vaut $d_j + \alpha$, *resp.* $d_j - \alpha$. Enfin, on définit $A_\alpha = PD_\alpha Q$ et $A_{-\alpha} = PD_{-\alpha} Q$.

Comme D_α et $D_{-\alpha}$, ont toutes leurs valeurs propres comprises entre -1 et 1 , $A_\alpha = PD_\alpha Q$ et $A_{-\alpha} = PD_{-\alpha} Q$ sont dans $\mathcal{B}$. En effet, avec G une

telle matrice diagonale, pour tout X , $\|GX\|^2 = \sum_{i=1}^n g_i^2 x_i^2 \leq \|X\|^2$. Puis

$$\|PGQX\| = \|GQX\| \leq \|QX\| = \|X\|.$$

Or on a $A = \frac{1}{2}(A_\alpha + A_{-\alpha})$ et $A_\alpha \neq A$: la matrice A n'est donc pas extrême.

Finalement, les points extrémaux de $\mathcal{B}$ sont exactement les matrices orthogonales $A \in O_n(\mathbb{R})$.