Enveloppe convexe de $\mathcal{O}(E)$

Références : [FGN10] p.130-131 ([Tau05]).

Théorème 0.1 *Soit E un espace euclidien. Soit $B = \{u \in E, \| u \| \leq 1\}$.*
Alors $Conv(\mathcal{O}(E)) = B$.

Définition 0.1 *Soit E un espace euclidien.*

$$\mathcal{O}(E) = \{u \in \mathcal{L}(E); \forall x, y \in E, < u(x), u(y) >=< x, y >\}$$

Définition 0.2 *Soit $\mathcal{E}$ un espace affine euclidien. Soit $\mathcal{A}$ un convexe de $\mathcal{E}$. On dit que $M \in \mathcal{A}$ est un point extrémal de $\mathcal{A}$ ou que M est extrémal, si toute égalité $M = tP + (1-t)Q$ avec $t \in [0,1]$ et $P, Q \in \mathcal{A}$ implique $M = P$ ou $M = Q$ (donc si $P \neq Q$, on a $t = 0$ ou $t = 1$).*

Notation : $Extr(\mathcal{A})$ désigne l'ensemble des points extrémaux de $\mathcal{A}$.

Proposition 0.2 *Soit $\mathcal{A}$ un convexe de $\mathcal{E}$. Soit $M \in \mathcal{A}$. Alors les propositions suivantes sont équivalentes :*

1. *$M \in Extr(\mathcal{A})$;*
2. *$A \setminus \{M\}$ est convexe.*

Démonstration
(i) $\Rightarrow$ (ii) Montrons que $\mathcal{A} \setminus \{M\}$ est convexe.
Soient $P, Q \in \mathcal{A} \setminus \{M\}$ et soit $t \in [0,1]$. Alors $tP + (1-t)Q \in \mathcal{A}$ puisque $\mathcal{A}$ est convexe.
Montrons maintenant que $tP+(1-t)Q \notin \{M\}$, pour ce faire, on suppose le contraire, ie $tP+(1-t)Q \in \{M\}$.
Alors $M = tP + (1-t)Q$, or M est extrémal donc cela implique que $P = M$ ou $Q = M$ ce qui est impossible car $P, Q \in \mathcal{A} \setminus \{M\}$.
(ii) $\Rightarrow$ (i) Montrons que M est extrémal.
Soient $P, Q \in \mathcal{A}$ et soit $t \in [0,1]$ tels que $M = tP + (1-t)Q$ (on peut écrire une telle égalité puisque $\mathcal{A}$ est convexe).
Supposons de plus que $P, Q \neq M$. Alors $P, Q \in \mathcal{A} \setminus \{M\}$, d'où M combinaison convexe d'éléments de $\mathcal{A} \setminus \{M\}$ qui est convexe, ie $M \in \mathcal{A} \setminus \{M\}$. D'où une contradiction, par conséquent $M = P$ ou $M = Q$, ce qui signifie que M est extrémal.

Proposition 0.3 *Soit $\mathcal{A}$ un convexe de $\mathcal{E}$. Alors $\mathcal{A} \setminus \{M\}$ est convexe si et seulement si $M = \frac{1}{2}(P+Q)$ avec $P, Q \in \mathcal{A}$ implique $M = P = Q$.*

Démonstration
La première implication est évidente d'après la proposition que l'on vient de démontrer.
Réciproquement, il suffit de se rendre compte que M peut toujours s'écrire comme le milieu de deux points de $\mathcal{A} \setminus \{M\}$, puisque $\mathcal{A} \setminus \{M\}$ est convexe.

Démonstration du théorème

Étape 1 : Montrons que les points extrémaux de B sont exactement les éléments de $\mathcal{O}(E)$.

$\rightsquigarrow$ **Montrons qu'un élément $u \in \mathcal{O}(E)$ est extrémal.**

Tout d'abord $u \in B$ car $u \in \mathcal{O}(E)$, ie $\forall x \in E$, $< u(x), u(x) >=< x, x >$ d'où :

$$\| u \| = \sup_{\|x\|=1} \| u(x) \| = \sup_{\|x\|=1} \| x \| = 1$$

Ainsi $\| u \| \leq 1$ donc $u \in B$.

Supposons de plus, puisque B est convexe, que $u = \dfrac{1}{2}(v + w)$ avec $v, w \in B$. Soit $x \in E$ unitaire. On a :

$$\begin{aligned} \| x \| = 1 = \| u(x) \| &= \frac{1}{2} \| v(x) + w(x) \| \\ &\leq \frac{1}{2} \| v(x) \| + \frac{1}{2} \| w(x) \| \\ &\leq \frac{1}{2}(\| v \| + \| w \|) \leq 1 \end{aligned}$$

en utilisant l'inégalité triangulaire, la définition de la norme subordonnée, le fait que x est unitaire et que $v, w \in B$.

Donc toutes ces inégalités sont en fait des égalités, en particulier $\| v \| + \| w \| = 2$, or $\| v \| \leq 1$ et $\| w \| \leq 1$, donc nécessairement $\| v \| = \| w \| = 1$ et via le même raisonnement (car $\| v(x) \| \leq \| v \| \leq 1$) on obtient $\| v(x) \| = \| w(x) \| = 1$.

De plus, on est dans le cas d'égalité dans l'inégalité triangulaire, ie que $v(x)$ et $w(x)$ sont positivement liés, ie $\exists \lambda \geq 0$ tel que $v(x) = \lambda w(x)$ pour $x \in E$ unitaire. Ainsi, on en déduit que $v(x) = w(x)$ pour $x \in E$ unitaire (car puisque $\| v(x) \| = \| w(x) \| = \lambda \| v(x) \| = 1$, alors $\lambda = 1$). Si maintenant on considère $y \in E$ non nul, alors $\dfrac{y}{\| y \|}$ est unitaire et $v(y) = w(y)$ par linéarité. Donc $v = w$.

Ainsi $u = \dfrac{1}{2}(2v)$, ie $v = u = w$ donc u est bien extrémal.

$\rightsquigarrow$ **Inversement, soit $u \in B$ et $u \notin \mathcal{O}(E)$, montrons que u n'est pas extrémal.**

On considère A la matrice de u dans une base orthonormée de E et on considère sa décomposition polaire, ie $A = OS$ avec $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in S_n^+(\mathbb{R})$.

Comme S est symétrique positive, alors $\exists P \in \mathcal{O}_n(\mathbb{R})$ et il existe $D = diag(d_1, \ldots, d_n)$ une matrice diagonale telles que $S = {}^tPDP$.

Supposons les valeurs propres rangées dans l'ordre croissant, ie $d_1 \leq d_2 \leq \ldots \leq d_n$.

Déterminons la norme de A.

On a $A = OS$ avec $O \in \mathcal{O}_n(\mathbb{R})$, ie $\forall X \in \mathbb{R}^n$, $< OX, OX >=< X, X >$ donc :

$$\| AX \| = \| OSX \| = \| SX \|$$

Donc cette égalité implique que $\| A \| \leq \| S \|$, mais aussi que $\| S \| \leq \| A \|$, donc $\| A \| = \| S \|$.

De plus pour la même raison, on a $\| S \| = \| D \|$. Par conséquent puisque $A \in B$, alors $\| A \| = \| D \| \leq 1$, donc les $d_i \in [0, 1]$.

Par hypothèse A n'est pas orthogonale (car $u \notin \mathcal{O}(E)$) donc $d_1 < 1$, en effet sinon cela signifierait que $D = Id$, donc que $S = Id$ et que $A = O$ avec O orthogonale.

Comme $d_1 < 1$, on peut alors écrire d_1 sous la forme $d_1 = \dfrac{\alpha + \beta}{2}$ avec $-1 \leq \alpha < \beta \leq 1$ (car d_1 n'est pas un point extrémal du segment $[-1, 1]$).

Posons alors $D' = diag(\alpha, d_2, \ldots, d_n)$ et $D'' = diag(\beta, d_2, \ldots, d_n)$ (on a $D' \neq D''$), on a :

$$D = \frac{1}{2}(D' + D'')$$

Donc :

$$A = \frac{1}{2}(O\,{}^tPD'P + O\,{}^tPD''P)$$

Les matrices $O\,{}^tPD'P$ et $O\,{}^tPD''P$ sont de normes inférieures ou égales à 1, en effet $\forall X \in \mathbb{R}^n$ de norme 1 :

$$\| O\,{}^tPD'PX \|^2 = {}^tX\,{}^tPD'P\,{}^tOO\,{}^tPD'PX = {}^t(PX)D'^2(PX) \leq 1$$

car $\| PX \| = \| X \| = 1$ et les coefficients de D'^2 sont compris entre 0 et 1.
Donc $\| O\,{}^tPD'P \| \leq 1$.
De même, on obtient $\| O\,{}^tPD''P \| \leq 1$.
Ainsi en repassant aux endomorphismes, on a écrit u comme milieu de deux points distincts de B, donc u n'est pas extrémal.

Étape 2 : Conclusion.
On a donc montré que l'ensemble des points extrémaux de B sont exactement les éléments de $\mathcal{O}(E)$.
Par conséquent $Conv(\mathcal{O}(E)) = Conv(Extr(B))$.
Or B étant convexe, compacte et non vide, d'après le théorème de Krein-Millman, on sait que $B = Conv(Extr(B))$, donc l'enveloppe convexe de $\mathcal{O}(E)$ est la boule unité fermée B.

Lemmes utilisés

Lemme 0.1 (Théorème de Krein-Millman) *Pour tout convexe compact non vide $\mathcal{A}$ de $\mathcal{E}$ (espace affine euclidien), on a $\mathcal{A} = Conv(Extr(\mathcal{A}))$.*

Remarque : Ce résultat se démontre via une récurrence sur la dimension.

Lemme 0.2 *Les endomorphismes symétriques définis positifs sont diagonalisable en base orthonormée.*

Démonstration : cf le développement sur la réduction des endomorphismes auto-adjoints (ie symétrique !).

Lemme 0.3 (Décomposition polaire) *Soit $A \in GL_n(\mathbb{R})$. Alors il existe des uniques $P \in \mathcal{O}_n(\mathbb{R})$ et $S \in S_n^{++}(\mathbb{R})$ telles que $A = OS$.*
De plus, si $A \in \mathcal{M}_n(\mathbb{R})$, alors il existe $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in S_n^{+}(\mathbb{R})$ telles que $A = OS$.

Démonstration
Soit $A \in GL_n(\mathbb{R})$.
Unicité Supposons que le couple (O, S) réponde au problème. Alors on a :

$$ {}^tAA = {}^t(OS)(OS) = {}^tS\,{}^tOOS = {}^tSS = S^2 $$

Ainsi S est déterminée comme étant l'unique racine carrée de la matrice symétrique définie positive ${}^tAA$. Par conséquent l'unicité de O en découle.
Existence On pose S comme étant l'unique racine carré de la matrice symétrique définie positive ${}^tAA$ et on pose $O = AS^{-1}$. Par définition $S \in S_n^{++}(\mathbb{R})$, donc il reste à vérifier que O est orthogonale :

$$ {}^tOO = {}^tS^{-1}\,{}^tAAS^{-1} = S^{-1}S^2S^{-1} = Id $$

Donc le couple (O, S) répond au problème.
Remarque : Vérifions que ${}^tAA$ est bien symétrique définie positive.
Soit $X \in \mathbb{R}^n$,

$$ < {}^tAAX, X > = < AX, AX > = \| AX \|^2 \geq 0 $$

De plus A étant inversible, si $X \neq 0$, alors $AX \neq 0$ et donc $\| AX \|^2 \neq 0$.
Donc ${}^tAA$ est bien une matrice symétrique définie positive.

Remarque : Vérifions l'unicité de S.
Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de vecteurs propres de ${}^tAA$, $\lambda_i \in \mathbb{R}_+$ étant la valeur propre associée à e_i.
On définit s dans la base $\mathcal{B}$ en posant $s(e_i) = \sqrt{\lambda_i}e_i$. L'endomorphisme s est symétrique car diagonalisable dans une base orthonormale, positif et vérifie clairement $S^2 = {}^tAA$.
Soit k un endomorphisme symétrique positif vérifiant $K^2 = {}^tAA$, alors K commute avec ${}^tAA$, donc laisse invariant les sous-espaces propres de ${}^tAA$. La restriction de k à E_λ, espace propre de ${}^tAA$ relatif à la valeur propre λ, est un endomorphisme symétrique positif dont le carré est λid_{E_λ}.
Sa seule valeur propre (positive) possible est $\sqrt{\lambda}$. Comme il est diagonalisable, c'est $\sqrt{\lambda} id_{E_\lambda}$. Ainsi pour tout i, $k(e_i) = \sqrt{\lambda_i}e_i = s(e_i)$ donc $s = k$.

Soit $A \in \mathcal{M}_n(\mathbb{R})$.
Existence Comme $GL_n(\mathbb{R})$ est dense dans $\mathcal{M}_n(\mathbb{R})$, on peut considérer une suite $(A_p)_p$ de matrices inversibles qui converge vers A.
D'après ce qu'on vient de faire, on peut écrire $\forall p$, $A_p = O_p S_p$ avec $O_p \in \mathcal{O}_n(\mathbb{R})$ et $S_p \in S_n^{++}(\mathbb{R})$.
Comme la suite $(O_p)_p$ est contenue dans le compact $\mathcal{O}_n(\mathbb{R})$, on peut en extraire une sous-suite convergente qui converge vers $O \in \mathcal{O}_n(\mathbb{R})$. Quitte à considérer cette extraction, on peut considérer que O_p converge vers O.
Par conséquent la suite $S_p = O_p^{-1} A_p$ converge vers une matrice S. Ainsi par passage à la limite S est symétrique et $S = O^{-1}A$. De plus S est également positive car $\forall X \in \mathbb{R}^n$:

$$0 \leq < S_p X, X > \longrightarrow < SX, X >$$

par continuité du produit scalaire.
On obtient donc que $A = OS$ avec O orthogonale et S symétrique positive.

Références

[FGN10] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux x-ens algèbre 3*. Cassini, 2010.

[Tau05] Patrice Tauvel. *Géométrie*. Dunod, 2005.