# Les ellipsoïdes de John et de Löwner

Jean-Baptiste Campesato

4 juin 2010

Les ellipsoïdes de John et de Löwner permettent d'approximer les convexes compacts de $\mathbb{R}^n$. En effet, le premier est l'unique ellipsoïde de volume maximal contenu dans un convexe compact, et le second est l'unique ellipsoïde de volume minimal contenant un convexe compact donné. La convexité est une notion à la fois ancienne et très récente. Archimède en donne déjà une définition sommaire aux alentours de 250 avant J.-C., mais l'étude de la convexité se développe vraiment tout d'abord avec Minkowski qui en donne la première définition rigoureuse à la fin du XIX^e siècle et surtout à partir de 1950 où la convexité se retrouve dans de nombreux domaines mathématiques. C'est ce qui donne une certaine importance à l'étude de ces ellipsoïdes.
Nous présenterons donc d'abord le cadre d'étude où nous définirons tous les outils utilisés dans la suite, pour ensuite démontrer l'existence et l'unicité des deux ellipsoïdes suscités et enfin nous donnerons une application assez inattendue de l'ellipsoïde de Löwner qui permet de retrouver un résultat de la théorie des groupes et de la géométrie, mais qui ne fait toutefois pas appel à la convexité.

## 1 Définitions

Il y a plusieurs façons de définir la notion d'espace affine, nous optons ici pour la définition suivante.

**Définition : espace affine**

Soient :
- $(\mathbb{K}, +, \times, 0, 1)$ un corps commutatif dont les éléments seront nommés scalaires.
- $(V, \dot{+}, \cdot, \vec{0})$ un espace vectoriel sur $\mathbb{K}$ dont les éléments seront nommés vecteurs.
- Un ensemble $E$, dont les éléments seront nommés points.
- Une loi $\varphi : E \times E \to V$ vérifiant :
  $(A1)$ $\forall (A, B, C) \in E^3$, $\varphi(A, B) + \varphi(B, C) = \varphi(A, C)$ *(relation de Chasles)* .
  $(A2)$ $\forall A \in E$, $\forall \vec{v} \in V$, $\exists! B \in E$, $\varphi(A, B) = \vec{v}$.

Alors $\mathcal{E} = (E, \mathbb{K}, V, \varphi)$ est un espace affine sur $\mathbb{K}$ de dimension $\dim V$ et de direction $V$.
Soit $(A, B) \in E^2$, alors on notera $\overrightarrow{AB} = \varphi(A, B)$.
Lorsqu'il n'y aura pas de confusion possible, nous noterons simplement $E$ au lieu de $\mathcal{E}$.

Il en découle immédiatement :
$\overrightarrow{AB} = \vec{0} \Leftrightarrow A = B$
$\overrightarrow{AB} = -\overrightarrow{BA}$

Dans la suite nous noterons indifféremment $+$ pour $+$ et $\dot{+}$ et nous nous permettrons d'ommetre les symboles $\times$ et $\cdot$, le contexte déterminant le sens.

**Propriété-Définition : barycentre**

Soient $E$ un espace affine sur $\mathbb{K}$, $(A_i)_{i \in [\![1;n]\!]} \in E^n$ et $(a_i)_{i \in [\![1;n]\!]} \in \mathbb{K}^n$ tels que $a_1 + \ldots + a_n \neq 0$.
Il existe alors un unique point $G \in E$ vérifiant : $\displaystyle\sum_{i=1}^{n} a_i \overrightarrow{GA_i} = \vec{0}$
$G$ est nommé barycentre des points $(A_i)_i$ pondérés par les scalaires $(a_i)_i$ et on note $G = \mathrm{bar}\{(A_1, a_1), \ldots, (A_n, a_n)\}$.

<u>Démonstration :</u>

Soit un point $O$, d'après $(A1)$, la condition est équivalente à :
$\displaystyle\vec{0} = \sum_{i=1}^{n} a_i (\overrightarrow{GO} + \overrightarrow{OA_i}) \Leftrightarrow \overrightarrow{OG} = \frac{1}{\sum_{i=1}^{n} a_i} \sum_{i=1}^{n} a_i \overrightarrow{OA_i}$.
Puis d'après $(A2)$, il existe un unique point $G$ vérifiant cette condition.

■

**Définition : application affine**

Soient $\mathcal{E}_1 = (E_1, \mathbb{K}, V_1)$ et $\mathcal{E}_2 = (E_2, \mathbb{K}, V_2)$ deux espaces affines sur $\mathbb{K}$.
Une application $f : E_1 \to E_2$ est dite affine si et seulement s'il existe une application linéaire $\vec{f} : V_1 \to V_2$ telle que $\forall (M, N) \in E_1^2$, $\vec{f}\left(\overrightarrow{MN}\right) = \overrightarrow{f(M)f(N)}$.
De façon équivalente, une application entre deux espaces affines est affine si et seulement si elle conserve les barycentres.

**Définition : segment**

Soient $E$ un espace affine réel et $A$, $B$ deux points distincts de $E$.
On nomme segment joignant $A$ à $B$ l'ensemble

$$[AB] = \{\mathrm{bar}\{(A, \lambda), (B, \mu)\} \mid \lambda, \mu \in \mathbb{R}_+\} = \{\mathrm{bar}\{(A, \lambda), (B, 1 - \lambda)\} \mid \lambda \in [0, 1]\}.$$

Lorsque de plus $E$ est un espace vectoriel, on a aussi :

$$[AB] = \{\lambda A + (1 - \lambda)B \mid \lambda \in [0, 1]\}.$$

**Définition : partie convexe**

Une partie $C$ d'un espace affine réel est dite convexe si et seulement si pour tout $(A, B) \in C^2$, $[AB] \subset C$.

Dans la suite nous travaillerons dans $\mathbb{R}^n$ : il s'agit d'un espace affine pour $(\mathbb{R}^n, \mathbb{R}, \mathbb{R}^n)$ en considérant $\overrightarrow{AB} = B - A$ et d'un espace euclidien (espace vectoriel réel préhilbertien de dimension finie, nous utiliserons le produit scalaire euclidien usuel noté $\langle \cdot \mid \cdot \rangle$ de norme associée notée $\| \cdot \|$), ce qui nous permettra d'utiliser des notions topologiques.

Les ellipsoïdes généralisent la notion d'ellipse dans $\mathbb{R}^n$. On rappelle que les ellipses sont des coniques qui admettent dans une certaine base une équation cartésienne la forme : $\frac{(x-h)^2}{a^2} + \frac{(y-k)^2}{b^2} = 1$ où $(h, k)$ est le centre de l'ellipse (cette équation quadratique se généralise avec la propriété ci-dessous). On peut aussi voir les ellipses comme une perspective d'un cercle de rayon 1, c'est-à-dire comme l'image du cercle unité par une transformation affine du plan, d'où la définition.
Comme nous parlerons d'inclusion dans des ellipsoïdes, nous les définissons pleines.

**Définition : ellipsoïde**

Un ellipsoïde de $\mathbb{R}^n$ est l'image de la boule unité fermée par une transformation affine bijective de $\mathbb{R}^n$.
C'est-à-dire par $\Phi_{A,b} : \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ x & \longmapsto & Ax + b \end{array}$ avec $A \in \mathbf{GL}_n(\mathbb{R})$ et $b \in \mathbb{R}^n$.

Ainsi d'après le théorème du déterminant, le volume d'un ellipsoïde $\mathfrak{e} = \Phi_{A,b}(\mathcal{B})$ est donné par : $\mathrm{vol}(\mathfrak{e}) = \lambda_n(\Phi_{A,b}(\mathcal{B})) = |\det(A)|\lambda_n(\mathcal{B})$, où $\lambda_n$ est la mesure de Lebesgue sur $\mathbb{R}^n$ et $\mathcal{B}$ la boule unité fermée.

**Proposition**

Tout ellipsoïde de $\mathbb{R}^n$ peut s'écrire comme image de la boule unité fermée par une application $\begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ x & \longmapsto & Ax+b \end{array}$ avec $A \in \mathbf{M}_n(\mathbb{R})$ symétrique définie positive et $b \in \mathbb{R}^n$.
Les ellipsoïdes peuvent ainsi aussi se définir comme les ensembles de la forme $\{x \in \mathbb{R}^n \mid \langle A(x-b) \mid x-b\rangle \leq 1\}$ avec $A$ une matrice symétrique définie positive et $b \in \mathbb{R}^n$.

**Lemmes**

• Soit $A$ une matrice symétrique positive, alors il existe une unique matrice $B$ symétrique positive vérifiant $A = B^2$. On note alors $B = \sqrt{A}$.
• $A$ est symétrique définie positive si et seulement si $\sqrt{A}$ l'est aussi, et dans ce cas $\sqrt{A^{-1}} = \sqrt{A}^{-1}$.
• Toute matrice inversible $A$ peut s'écrire de façon unique comme produit d'une matrice symétrique définie positive $P$ et d'une matrice orthogonale $U$ ($A = PU$, décomposition polaire).

Démonstration des lemmes :

• Existence : Toute matrice symétrique réelle est orthogonalement diagonalisable, donc il existe $P$ orthogonale et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ diagonale avec $\lambda_i \geq 0$ telles que $A = {}^tPDP$. Posons $\Delta = \mathrm{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$, alors $B = {}^tP\Delta P$ convient.
Unicité : Soit $C$ une autre matrice symétrique positive vérifiant $C^2 = A$. Pour toute valeur propre $\lambda$ de $A$, comme $C$ commute avec $C^2 = A$ alors $E_\lambda = \ker(A - \lambda I_n)$ est stable par $C$. Alors l'endomorphisme induit par $C$ sur $E_\lambda$ vérifie $u = \sqrt{\lambda} I_{E_\lambda}$. Donc les endomorphismes associés à $B$ et $C$ coïncident sur les sous-espaces propres de $A$ dont $\mathbb{R}^n$ est somme directe. Donc $B = C$.
• Immédiat en remarquant que $\lambda_i > 0 \Leftrightarrow \sqrt{\lambda_i} > 0$.
• Soit $A$ inversible, alors $A^tA$ est symétrique et définie positive. En effet $\langle A^tAX \mid X\rangle = \|{}^tAX\|^2 > 0$. Posons alors $P = \sqrt{A^tA}$ et donc $U = P^{-1}A$. $U$ est bien orthogonale : $U^tU = P^{-1}(A^tA)P^{-1} = I_n$ (${}^t(P^{-1}) = P^{-1}$ car l'inverse d'une matrice symétrique définie positive est symétrique définie positive).

■

Démonstration de la proposition :

Soit un ellipsoïde définie par l'image de la boule unité fermée par
$\Phi_{A,b} : \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ x & \longmapsto & Ax+b \end{array}$ avec $A \in \mathbf{GL}_n(\mathbb{R})$ et $b \in \mathbb{R}^n$.
Par décomposition polaire on a : $A = PU$ avec $P$ symétrique définie positive et $U$ orthogonale.
Si on note $\mathcal{B}$ la boule unité fermée de $\mathbb{R}^n$ alors $\begin{array}{ccc} \mathcal{B} & \longrightarrow & \mathcal{B} \\ x & \longmapsto & Ux \end{array}$ est une bijection et donc $\Phi_{A,b}(\mathcal{B}) = A\mathcal{B} + b = PU\mathcal{B} + b = P\mathcal{B} + b = \Phi_{P,b}(\mathcal{B})$. ♦

Soient $A$ une matrice symétrique définie positive et $b \in \mathbb{R}^n$ :

$$\begin{aligned} x \in \Phi_{A,b}(\mathcal{B}) &\Leftrightarrow \|A^{-1}(x-b)\| \leq 1 \\ &\Leftrightarrow \langle A^{-1}(x-b), A^{-1}(x-b)\rangle \leq 1 \\ &\Leftrightarrow \langle {}^t(A^{-1})A^{-1}(x-b), (x-b)\rangle \leq 1 \\ &\Leftrightarrow \langle B(x-b), (x-b)\rangle \leq 1 \end{aligned}$$

Avec $B = (A^{-1})^2$ qui est symétrique définie positive (l'inverse d'une matrice symétrique définie positive est symétrique définie positive et le produit de deux matrices symétriques définies positives qui commutent est symétrique définie positive). On justifie bien la dernière équivalence, et donc la propriété, par unicité de la racine d'une matrice symétrique définie positive (qui est encore symétrique définie positive) et de l'inverse (de même).

■

Remarquons que le choix d'une matrice symétrique définie positive caractérise l'ellipsoïde pour chacune des deux définitions, c'est-à-dire :
Soient $A$ et $B$ deux matrices symétriques définies positives et $b \in \mathbb{R}^n$, alors
$A \neq B \Rightarrow \begin{cases} \Phi_{A,b}(\mathcal{B}) \neq \Phi_{B,b}(\mathcal{B}) \\ \{x \in \mathbb{R}^n \mid \langle A(x-b) \mid x-b\rangle \leq 1\} \neq \{x \in \mathbb{R}^n \mid \langle B(x-b) \mid x-b\rangle \leq 1\} \end{cases}$.
Comme $\Phi_{A,b}(\mathcal{B}) = \{x \mid \langle (A^{-1})^2(x-b), (x-b)\rangle \leq 1\}$, avec $\sqrt{(A^{-1})^2}$ symétrique définie positive qui est unique, vérifions le seulement pour la deuxième écriture. Supposons $A \neq B$ alors d'après le théorème de réduction simultanée, on peut se ramener à étudier le cas $A = I_n$ et $B = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ où il existe au moins un $i_0$ tel que $\lambda_{i_0}$ est différent de 1. Alors $x = b + (0, \ldots, 0, \max(1, \lambda_{i_0}), 0, \ldots, 0)$ appartient à l'un des ellipsoïdes mais pas à l'autre.

La seconde écriture permet aussi de retrouver la définition cartésienne d'un ellipsoïde, en effet, posons $\mathfrak{e} = \{x \in \mathbb{R}^n \mid \langle A(x-b) \mid x-b\rangle \leq 1\}$. Alors $A$ est orthogonalement diagonalisable, il existe donc une base telle que $A$ soit diagonale avec des éléments positifs, on peut donc écrire dans cette base $A = \mathrm{diag}(\frac{1}{a_1^2}, \ldots, \frac{1}{a_n^2})$ et alors : $\mathfrak{e} = \left\{x \in \mathbb{R}^n \middle| \frac{(x_1-b_1)^2}{a_1^2} + \ldots + \frac{(x_n-b_n)^2}{a_n^2} \leq 1\right\}$.
Dans ce cas, on a d'après la démonstration précédente $\mathrm{vol}(\mathfrak{e}) = \det(\sqrt{A^{-1}})\lambda_n(\mathcal{B}) = a_1 \ldots a_n \lambda_n(\mathcal{B})$.

# 2 Les ellipsoïdes de John et de Löwner

En 1938, Behrend montre que tout convexe compact d'intérieur non vide du plan admet une unique ellipse inscrite d'aire maximale et une unique ellipse circonscrite d'aire minimale [1]. Ces résultats ont ensuite été généralisés à $\mathbb{R}^n$ : John a démontré en 1948 dans [3] que tout convexe compact d'intérieur non vide de $\mathbb{R}^n$ contenait un ellipsoïde de volume maximal. À peu près à la même époque, Löwner (Loewner pour les anglophones) a démontré, sans jamais le publier, que tout convexe compact d'intérieur non vide était contenu dans un unique ellipsoïde de volume minimal (en fait la convexité n'est pas nécessaire à la démonstration). En utilisant la notion de polarité, dans le cas des convexes compacts, ces ellipsoïdes peuvent se déduire l'un de l'autre.
L'unicité de l'ellipsoïde de volume maximal semble être due à Danzer [4] et Zaguskin [7].
La nomenclature de ces deux ellipsoïdes est assez confuse, ici, nous nommerons l'ellipsoïde inscrite *ellipsoïde de John* et l'ellipsoïde circonscrite *ellipsoïde de Löwner*.

## 2.1 Ellipsoïde de John

**Théorème: Ellipsoïde de John**

Tout convexe compact de $\mathbb{R}^n$ d'intérieur non vide contient un unique ellipsoïde de volume maximal.

Cette démonstration est basée sur celle de [5], elle se déroule en deux étapes, d'abord l'existence, puis l'unicité. Cette dernière étape nécessite le lemme suivant :

**Lemme**

Soient $A$ et $B$ deux matrices symétriques définies positives et $\alpha \in [0,1]$, alors :

$$\det(\alpha A + (1-\alpha)B) \geq \det(A)^\alpha \det(B)^{1-\alpha}$$

De plus si $\alpha \in ]0,1[$ et $A \neq B$, l'inégalité devient stricte.

Démonstration :

D'après le théorème de réduction simultanée, il existe $P \in \mathbf{GL}_n(\mathbb{R})$ et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \in \mathbf{M}_n(\mathbb{R})$, avec $\lambda_i > 0$, telles que : $A = P^tP$ et $B = PD^tP$.
Donc $\det(\alpha A + (1-\alpha)B) = \det(P)^2\det(\alpha I_n + (1-\alpha)D)$ et $\det(A)^\alpha\det(B)^{1-\alpha} = \det(P)^2\det(D)^{1-\alpha}$.
$\det(P)^2$ étant strictement positif il suffit de démontrer le lemme dans le cas où $A = I_n$ et $B = D$.

On a $\det(\alpha I_n + (1-\alpha)D) = \prod_{i=1}^{n}(\alpha + (1-\alpha)\lambda_i)$ et $\det(D)^{1-\alpha} = \prod_{i=1}^{n}\lambda_i^{1-\alpha}$.
Par concavité du logarithme $\sum_{i=1}^{n}\ln(\alpha + (1-\alpha)\lambda_i) \geq \sum_{i=1}^{n}(1-\alpha)\ln(\lambda_i)$, on obtient l'inégalité recherchée en passant à l'exponentielle.
De plus si $\alpha \in ]0,1[$ et $A \neq B$, l'un des $\lambda_i$ est forcément différent de 1, et par stricte concavité de ln, l'inégalité est stricte.

■

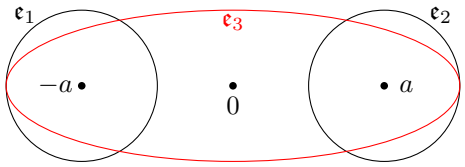
Démonstration du théorème :

Existence :
Soit $K$ un convexe compact de $\mathbb{R}^n$ d'intérieur non vide.
On note encore $\mathcal{B}$ la boule unité fermée, considérons alors l'ensemble des ellipsoïdes contenus dans $K$ : $\mathfrak{E} = \{(A,b) \in \mathbf{S}_n^+(\mathbb{R}) \times \mathbb{R}^n \mid A\mathcal{B} + b \subset K\} \neq \varnothing$ car $K$ d'intérieur non vide.
Comme $\mathbf{S}_n^{++}(\mathbb{R}) \subset \mathbf{S}_n^+(\mathbb{R})$, on a bien tous les ellipsoïdes contenus dans $K$. L'avantage de ce choix est que $\mathbf{S}_n^+(\mathbb{R})$ est un fermé alors que $\mathbf{S}_n^{++}(\mathbb{R})$ est ouvert (d'ailleurs $\overline{\mathbf{S}_n^{++}(\mathbb{R})} = \mathbf{S}_n^+(\mathbb{R})$), ainsi toute suite de matrices symétriques positives convergente, converge vers une matrice symétrique positive. Considérons alors une suite $(A_n, b_n)_{n\in\mathbb{N}}$ à éléments dans $\mathfrak{E}$ qui converge vers $(A,b) \in \mathbf{S}_n^+(\mathbb{R}) \times \mathbb{R}^n$. Soit $x \in \mathcal{B}$, comme pour tout $n \in \mathbb{N}$, $A_n x + b_n \in K$, on a $Ax + b \in K$ par fermeture de $K$. Ainsi $(A,b) \in \mathfrak{E}$. Et donc $\mathfrak{E}$ est fermé.
De plus $\mathfrak{E}$ est borné, en effet, $b \in K$ qui est borné et $|||A||| = \sup_{\|x\|=1}\|Ax\|$ avec $\|Ax\| \leq \|Ax+b\| + \|b\|$ avec $Ax+b, b \in K$ qui est borné. Il suffit ensuite de considérer une norme produit sur $\mathbf{M}_n(\mathbb{R}) \times \mathbb{R}^n$ induite par $|||\cdot|||$ et $\|\cdot\|$.
Il s'agit donc d'un compact de $\mathbf{S}_n^+(\mathbb{R}) \times \mathbb{R}^n$. Ainsi l'application $\begin{array}{ccc} \mathfrak{E} & \longrightarrow & \mathbb{R} \\ (A,b) & \longmapsto & |\det(A)| \end{array}$ est continue sur un compact, et est donc bornée et atteint ses bornes.
Il existe donc $(A_0, b_0) \in \mathfrak{E}$ tel que $A_0\mathcal{B} + b_0$ soit un ellipsoïde de volume maximal contenu dans $K$.

Unicité :
Supposons par l'absurde qu'il existe deux ellipsoïdes distincts $\mathfrak{e}_1 = \Phi_{A_1,b_1}(\mathcal{B})$ et $\mathfrak{e}_2 = \Phi_{A_2,b_2}(\mathcal{B})$ de volume maximal, on peut choisir $A_1$ et $A_2$ symétriques définies positives d'après la propriété de la partie 1 (on a $\det(A_1) = \det(A_2)$, vu qu'ils ont même volume).
• Si $A_1 \neq A_2$.
$K$ étant convexe $\mathfrak{E}$ l'est aussi et donc $\mathfrak{e}_3 = \Phi_{A_3,b_3}(\mathcal{B})$ avec $A_3 = \frac{1}{2}(A_1 + A_2)$ et $b_3 = \frac{1}{2}(b_1 + b_3)$ est encore un ellipsoïde contenu dans $K$.
D'après le lemme $\det(A_3) > \det(A_1)^{\frac{1}{2}}\det(A_2)^{\frac{1}{2}} = \det(A_1)$.
D'où une contradiction.
• Si $A_1 = A_2$ et donc forcément $b_1 \neq b_2$. On a ainsi deux ellipsoïdes identiques à une translation près.
Par une transformation linéaire et une translation, on peut se ramener au cas où :
$\mathfrak{e}_1 = \{x \in \mathbb{R}^n \mid \|x+a\| \leq 1\}$ et $\mathfrak{e}_2 = \{x \in \mathbb{R}^n \mid \|x-a\| \leq 1\}$ avec $a = (0,\ldots,0,\alpha)$ et $\alpha > 0$.
Considérons alors $\mathfrak{e}_3 = \left\{x \in \mathbb{R}^n \middle| x_1^2 + \ldots + x_{n-1}^2 + \frac{x_n^2}{(1+\alpha)^2} \leq 1\right\}$, il s'agit d'un ellipsoïde de volume supérieur à celui de $\mathfrak{e}_1$ et de $\mathfrak{e}_2$ car $1 + \alpha > 1$.
Puis $\mathfrak{e}_3$ est inclus dans l'enveloppe convexe de $\mathfrak{e}_1 \cup \mathfrak{e}_2$, en effet :
Soit $x \in \mathfrak{e}_3$, si $|x_n| \leq \alpha$, alors $x$ appartient au cylindre $x_1^2 + \ldots + x_{n-1}^2 \leq 1, |x_n| \leq \alpha$ qui est inclus dans l'enveloppe convexe de $\mathfrak{e}_1 \cup \mathfrak{e}_2$. Sinon si $x_n > \alpha$ alors $x_n \leq 1 + \alpha$ et $(x_n - \alpha)^2 \leq \frac{x_n^2}{(1+\alpha)^2}$ et donc $x \in \mathfrak{e}_2$. Si $x_n < \alpha$, de même $x \in \mathfrak{e}_1$.

$\mathbf{S}_n^{++}(\mathbb{R})$ est l'ensemble des matrices réelles symétriques définies positives et $\mathbf{S}_n^+(\mathbb{R})$ est l'ensemble des matrices réelles symétriques positives.

On a donc un ellipsoïde de volume supérieur à celui de $\mathfrak{e}_1$ et $\mathfrak{e}_2$ contenu dans leur enveloppe convexe, et donc dans $K$. D'où une contradiction.




■

## 2.2 Ellipsoïde de Löwner

Dans le cadre des convexes compacts, on peut passer de l'ellipsoïde de John à celui de Löwner (et réciproquement) à l'aide de la notion de polarité. En effet le polaire d'un ellipsoïde est un ellipsoïde, le polaire d'un convexe compact contenant l'origine et encore un convexe compact contenant l'origine et $C_1 \subset C_2 \Rightarrow C_2^* \subset C_1^*$. Comme nous voulons obtenir un résultat général (sans la convexité ici), nous ne passerons pas par la notion de polarité pour déduire l'ellipsoïde de Löwner à partir de celui de John. Cependant, on aurait très bien pu d'abord démontrer l'existence et l'unicité de l'ellipsoïde de Löwner (sans la convexité) et utiliser la polarité pour obtenir l'ellipsoïde de John (en rajoutant l'hypothèse de convexité).

**Théorème: Ellipsoïde de Löwner**

Tout compact de $\mathbb{R}^n$ d'intérieur non vide est contenu dans un unique ellipsoïde de volume minimal.

Démonstration du théorème :

Existence :
On considère $K$ un compact d'intérieur non vide, comme il est borné, il existe un ellipsoïde $\mathfrak{e}_0$ contenant $K$ (on peut prendre une boule de rayon suffisament grand).
Il suffit alors de considérer les ellipsoïdes contenant $K$ et contenu dans $\mathfrak{e}_0$, c'est-à-dire $\mathfrak{E} = \{(A,b) \in \mathbf{S}_n^+(\mathbb{R}) \times \mathbb{R}^n \mid K \subset A\mathcal{B} + b \subset \mathfrak{e}_0\}$.
On peut ainsi utiliser un argument de compacité comme précédemment : $\mathfrak{E}$ est borné (il suffit de reprendre le raisonnement dans le cas de l'ellipsoïde de John où $\mathfrak{e}_0$ remplace $K$) et $\mathfrak{E}$ est fermé. En effet soit $(A_n, b_n)_{n\in\mathbb{N}}$ une suite à éléments dans $\mathfrak{E}$ qui converge vers $(A,b) \in \mathbf{S}_n^+(\mathbb{R}) \times \mathbb{R}^n$. En utilisant le même raisonnement que pour l'ellipsoïde de John, on a que $A\mathcal{B} + b \subset \mathfrak{e}_0$. Puis soit $x \in K$, alors pour tout $n \in \mathbb{N}$, $x \in K \subset A_n\mathcal{B} + b_n$ donc il existe $e_n \in \mathcal{B}$ tel que $x = A_n e_n + b_n$. Par compacité de $\mathcal{B}$, on peut extraire une sous-suite $(e_{\varphi(n)})_n$ convergente vers $e \in \mathcal{B}$, et ainsi $x = A_{\varphi(n)} e_{\varphi(n)} + b_{\varphi(n)} \underset{n\infty}{\longrightarrow} Ae + b$. Donc $K \subset A\mathcal{B} + b$. D'où $(A,b) \in \mathfrak{E}$, ce qui permet de conclure.

Unicité, [6] :
Supposons par l'absurde qu'il existe deux ellipsoïdes distinctes $\mathfrak{e}_1$ et $\mathfrak{e}_2$ de volume minimal.
Par le théorème de réduction simultanée et par une translation on peut écrire :
$\mathfrak{e}_1 = \left\{x \mid (x_1 - b_1)^2 + \ldots + (x_n - b_n)^2 \leq 1\right\}$ et $\mathfrak{e}_2 = \left\{x \middle| \frac{x_1^2}{a_1^2} + \ldots + \frac{x_n^2}{a_n^2} \leq 1\right\}$.
Considérons : $\mathfrak{e} = \left\{x \in \mathbb{R}^n \middle| \frac{1}{2}\sum_{i=1}^n \left((x_i - b_i)^2 + \frac{x_i^2}{a_i^2}\right) \leq 1\right\}$.
Il est évident que $K \subset \mathfrak{e}_1 \cap \mathfrak{e}_2 \subset \mathfrak{e}$.
Puis $\mathfrak{e} = \left\{x \in \mathbb{R}^n \middle| \sum_{i=1}^n \frac{(x_i - \eta_i)^2}{\beta_i^2} \leq \gamma\right\}$ avec $\beta_i = \frac{2}{1+\frac{1}{\alpha_i^2}}$, $\eta_i = \frac{\beta_i b_i}{2} = \frac{\alpha_i^2 b_i}{1+\alpha_i^2}$ et
$\gamma = 1 - \frac{1}{2}\sum_{i=1}^n \frac{b_i^2}{1+\alpha_i^2}$.
Donc $\mathfrak{e}$ est bien un ellipsoïde.

Comme $K$ est d'intérieur non vide, les ellipsoïdes considérés ne sont pas aplatis par rapport à une direction, c'est ce qui permet d'utiliser ces équations.

L'inégalité arithmético-géométrique $m_a \leq m_g$ : soient $x_1, \ldots, x_n \in \mathbb{R}_+^*$ alors $\frac{x_1+\ldots+x_n}{n} \leq$

On remarque aussi que $\gamma \leq 1$ avec égalité si et seulement si $b = 0$, c'est à dire si $\mathfrak{e}_1$ et $\mathfrak{e}_2$ ont même centre. De même, l'inégalité arithmético-géométrique implique que $\frac{1}{\beta_i^2} \geq \frac{1}{\alpha_i}$, i.e. $\beta_i \leq \sqrt{\alpha_i}$ avec égalité si et seulement si $\alpha_i = 1$.
$\lambda_n(\mathfrak{e}) = \lambda_n(\mathfrak{e}_1)\gamma^{\frac{n}{2}} \prod_{i=1}^{n} \beta_i \leq \lambda_n(\mathfrak{e}_1) \prod_{i=1}^{n} \sqrt{\alpha_i} \leq \lambda_n(\mathfrak{e}_1)$.
Ces inégalités sont strictes sauf dans le cas où $b = 0$ et $\forall_i$, $\alpha_i = 1$, c'est-à-dire dans le cas où $\mathfrak{e}_1$ et $\mathfrak{e}_2$ coincident.
Par hypothèse, l'inégalité est donc stricte, et ainsi : $\lambda_n(\mathfrak{e}) < \lambda_n(\mathfrak{e}_1)$.
D'où une contradiction.

■

# 3 Application de l'ellipsoïde de Löwner [2]

Le résultat suivant est essentiel en géométrie et théorie des groupes : tout sous-groupe compact du groupe linéaire $GL(\mathbb{R}^n)$ des automorphismes de $\mathbb{R}^n$ laisse invariant au moins une structure euclidienne. On fera la démonstration avec des matrices, et donc avec $\mathbf{GL}_n(\mathbb{R})$ l'ensemble des matrices carrées de dimension $n \times n$ inversibles, et intuitivement cela revient à dire que tout sous-groupe compact du groupe linéaire est inclus dans le groupe orthogonal associé à une certaine structure euclidienne.
En effet, cela signifie qu'il doit exister une matrice $A_0$ symétrique définie positive vérifiant que pour tout $X, Y \in \mathbb{R}^n$ et pour tout $M$ du sous-groupe compact, ${}^tXM^tA_0MY = {}^tXA_0Y$, c'est-à-dire, en considérant les éléments d'une base, qu'il doit exister une matrice $A_0$ symétrique définie positive vérifiant pour tout $M$ du sous-groupe compact ${}^tMA_0M = A_0$. Ce qui, on le verra dans la démonstration, est bien équivalent au fait que dans une base orthonormée pour $A_0$, les éléments du sous-groupe compact sont orthogonaux.
On reformule donc la proposition de la façon suivante :

**Proposition**

Tout sous-groupe compact de $\mathbf{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe du groupe orthogonal.

Démonstration :

Soit $G$ un sous-groupe compact de $\mathbf{GL}_n(\mathbb{R})$.
L'application $\begin{array}{ccc} G \times \mathcal{B} & \longrightarrow & \mathbb{R}^n \\ (A, X) & \longmapsto & AX \end{array}$ est continue sur un compact, comme produit de compacts, donc son image $K = \bigcup_{A \in G} A\mathcal{B}$ est compacte. De plus $K$ contient $\mathcal{B}$, car $I_n \in G$, et est donc d'intérieur non vide.
Ainsi, il existe un unique ellipsoïde $\mathfrak{e} = \{x \in \mathbb{R}^n \mid \langle A_0(x-b) \mid x-b\rangle \leq 1\}$ de volume minimal contenant $K$ (avec $A_0$ symétrique définie positive).

Soit $M \in G$, alors par définition de $K$, $MK = K$ et donc $\forall p \in \mathbb{Z}$, $M^pK = K$. Puis $\mathcal{B} \subset K \subset \mathfrak{e}$, ainsi $\forall p \in \mathbb{Z}$, $\mathcal{B} \subset K = M^pK \subset M^p\mathfrak{e}$.
Donc $\forall p \in \mathbb{Z}$, $\lambda_n(\mathcal{B}) \leq \lambda_n(M^p\mathfrak{e}) = |\det(M)|^p\lambda_n(\mathfrak{e}) = |\det(M)|^p|\det(A_0)|^{-\frac{1}{2}}\lambda_n(\mathcal{B})$, d'où $\forall p \in \mathbb{Z}$, $1 \leq |\det(M)|^p|\det(A_0)|^{-\frac{1}{2}}$ et ainsi $|\det(M)| = 1$.

Donc si on pose $B = {}^tMA_0M$, alors :
• $B$ est symétrique définie positive : soit $x \neq 0$, alors ${}^txBx = {}^t(Mx)A_0Mx > 0$ car $Mx \neq 0$, du fait que $M$ soit inversible, et $A_0$ symétrique définie positive.
• $K \subset \{x \in \mathbb{R}^n \mid \langle B(x - M^{-1}b) \mid x - M^{-1}b\rangle \leq 1\}$ : soit $x \in K$, alors $Mx \in K \subset \mathfrak{e}$ puis $\langle B(x - M^{-1}b) \mid x - M^{-1}b\rangle = \langle A_0(Mx - b) \mid Mx - b\rangle \leq 1$.
• $\det(B) = \det({}^tMA_0M) = \det(M)^2\det(A_0) = \det(A_0)$ .
Donc par unicité de l'ellipsoïde de volume minimal, $M^{-1}b = b$ puis $A_0 = B$ (voir la remarque à la fin de la partie 1).

On a ainsi montré que pour tout $M \in G$, ${}^tMA_0M = A_0$. Ce que l'on voulait dans un premier temps, montrons maintenant que c'est équivalent à la proposition, ce qui justifiera aussi la remarque qui la précède :

Soit $P$ la matrice de passage de la base canonique à une base $\mathcal{B}$ orthonormale pour $A_0$, on a alors ${}^tPA_0P = I_n$ donc $A_0 = ({}^tP)^{-1}P^{-1} = {}^t(P^{-1})P^{-1} = {}^tRR$ avec $R = P^{-1}$.
Pour tout $M \in G$, on a alors :
${}^t(RMR^{-1})RMR^{-1} = {}^t(R^{-1}){}^tM{}^tRRMR^{-1} = {}^t(R^{-1}){}^tMA_0MA_0^{-1}{}^tR$
$= {}^t(R^{-1})A_0A_0^{-1}{}^tR = {}^t(R^{-1}){}^tR = I_n$, donc $RMR^{-1} \in O_n(\mathbb{R})$.
Donc $P^{-1}GP = RGR^{-1}$ est un sous-groupe de $O_n(\mathbb{R})$.

■

# Références


[1] Felix Behrend. Über die kleinste umbeschriebene und die größte einbeschriebene ellipse eines konvexen bereiches. Mathematische Annalen, 115(1) :379–411, 12 1938. En allemand, disponible sur springerlink.

[2] Marcel Berger. Convexity. The American Mathematical Monthly, 97 :650–678, 1990. Disponible sur MathDL.

[3] Collectif. Studies and Essays, presented to R. Courant on his 60th birthday, chapter Extremum problems with inequalities as subsidiary conditions, pages 187–204. Interscience Publishers, 01 1948. Reprinted in Fritz John, Collected papers, Volume2, pp. 543-560, edited by J. Moser, 1985.

[4] Ludwig Danzer, Detlef Laugwitz, and Lenz Hanfried. Über das löwnersche ellipsoid und sein analogon unter den einem eikörper einbeschriebenen ellipsoiden. Archiv der Mathematik, 8(3) :214–219, 08 1957. En allemand, disponible sur springerlink.

[5] Ralph Howard. John's theorem on ellipsoids in convex bodies. http://www.math.sc.edu/~howard/, 11 1997.

[6] Anthony C. Thompson. Minkowski Geometry, volume 63 of Encyclopedia of Mathematics and Its Applications, chapter 3.3 The Löwner ellipsoid. Cambridge University Press, 06 1996.

[7] V. L. Zaguskin. Circumscribed and inscribed ellipsoids of extremal volume. Uspehi Mat. Nauk, 13(6) :89–93, 1958. En russe.