Oral 1 — convexité

• Sous-groupes compacts du groupe linéaire

Lemme (Dépendance affine) : Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n. Soient Soient $a_1, \dots, a_{n+2} \in E$. Il existe $(\mu_1, \dots, \mu_{n+2}) \in \mathbb{R}^{n+2} \backslash \{0\}$ tel que $\displaystyle\sum_{i=1}^{n+2} \mu_i a_i = 0$ et $\displaystyle\sum_{i=1}^{n+2} \mu_i = 0$.

□ La famille $(a_i - a_{n+2})_{i \in [\![1,n+1]\!]}$ est liée. Il existe donc des réels non tous nuls $\mu_1, \dots, \mu_{n+1}$ tel que $\displaystyle\sum_{i=1}^{n+1} \mu_i (a_i - a_{n+2}) = 0$. On pose alors $\mu_{n+2} = -\displaystyle\sum_{i=1}^{n+1} \mu_i$, ce qui donne le résultat.

□

Le lemme de dépendance affine s'adapte pour $p \geqslant n+2$ vecteurs.

Théorème (Carathéodory) : Soient E un $\mathbb{R}$-espace vectoriel de dimension finie n et $A \subset E$. Tout élément de $\mathrm{Conv}(A)$ s'écrit comme combinaison convexe de $n+1$ éléments de A.

□ On montre que si $x \in \mathrm{Conv}(A)$ est combinaison convexe de $p \geqslant n+2$ points de A, alors x est combinaison convexe d'au plus $p-1$ points de A. Cela permet de conclure par récurrence descendante, en s'arrêtant à $p = n+2$.
Supposons que x s'écrive comme une combinaison convexe $x = \displaystyle\sum_{i=1}^{p} \lambda_i a_i$ avec $p \geqslant n+2$ et $a_1, \dots, a_p \in A$. Le lemme de dépendance affine assure l'existence de $(\mu_1, \dots, \mu_p) \in \mathbb{R}^p \backslash \{0\}$ vérifiant $\displaystyle\sum_{i=1}^{p} \mu_i a_i = 0$ et $\displaystyle\sum_{i=1}^{p} \mu_i = 0$. Au moins l'un des μ_i est > 0. Pour $t \in \mathbb{R}$ quelconque, on peut écrire $x = \displaystyle\sum_{i=1}^{p} (\lambda_i + t\mu_i) a_i$. On aimerait choisir t tel que les $\lambda_i + t\mu_i$ soient tous positifs et que l'un soit nul, disons $\lambda_{i_0} + t\mu_{i_0} = 0$.
On prend $t < 0$. On cherche t tel que : $\forall i \in [\![1,p]\!]$, $\mu_i > 0 \Longrightarrow \lambda_i + t\mu_i \geqslant 0$. Il faut donc que, pour tout $\mu_i > 0$, $t \geqslant -\dfrac{\lambda_i}{\mu_i}$. On pose $t = \max\left\{ -\dfrac{\lambda_i}{\mu_i},\ i \in [\![1,p]\!],\ \mu_i > 0 \right\}$. On a alors la condition voulue, avec pour i_0 l'indice $i \in [\![1,p]\!]$ réalisant le max. Cela permet d'écrire x comme combinaison convexe de $p-1$ points de A (pris parmi $a_1, \dots, a_p$).

□

Lemme : On a $A \in \mathcal{S}_n^{++}(\mathbb{R})$ si et seulement si il existe $R \in \mathcal{GL}_n(\mathbb{R})$ telle que $A = R^T R$.

□ Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. On écrit $A = PDP^T$ où $D = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ est à coefficients diagonaux > 0 et $P \in O_n(\mathbb{R})$. On pose $D' = \mathrm{Diag}\left(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n}\right)$, de sorte que $A = (PD')(PD')^T$. Alors $R = (PD')^T$ est inversible et $A = R^T R$.

Réciproquement, soit $R \in \mathcal{GL}_n(\mathbb{R})$ et $A = R^T R \in \mathcal{S}_n(\mathbb{R})$. Si $X \in \mathcal{M}_{n,1}(\mathbb{R})\backslash\{0\}$, $X^T A X = (RX)^T RX = \|RX\|_2^2 > 0$ donc $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

□

Lemme : Dans E un $\mathbb{R}$-espace vectoriel normé de dimension finie, l'enveloppe convexe d'un compact est compacte.

□ Notons $\mathcal{H} = \left\{ (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{R}_+^{n+1} : \sum_{i=1}^{n+1} \lambda_i = 1 \right\}$ et $\Phi : \begin{cases} \mathbb{R}^{n+1} \times E^{n+1} & \longrightarrow & E \\ ((\lambda_i)_{i\in[\![1,n+1]\!]}, (x_i)_{i\in[\![1,n+1]\!]}) & \longmapsto & \sum_{i=1}^{n+1} \lambda_i x_i \end{cases}$

Soit $K \subset E$ un compact. D'après le théorème de Carathéodory, $\mathrm{Conv}(K) = \Phi(\mathcal{H} \times K^{n+1})$. L'hyperplan affine $\mathcal{H}'$ d'équation $\lambda_1 + \ldots + \lambda_{n+1} = 1$ est un fermé de $\mathbb{R}^{n+1}$, donc c'est aussi le cas de $\mathcal{H} = \mathcal{H}' \cap [0, +\infty[$. De plus, $\mathcal{H}$ est borné, donc il est compact. Ainsi, $\mathcal{H} \times K^{n+1}$est un compact de $\mathbb{R}^{n+1} \times E^{n+1}$. Comme Φ est continue (elle est $2n+2$ linéaire), on en conclut que $\mathrm{Conv}(K)$ est compact.

□

On va montrer que tout sous-groupe compact G de $\mathcal{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$. On cherche donc $N \in \mathcal{GL}_n(\mathbb{R})$ et G_1 un sous-groupe de $O_n(\mathbb{R})$ tels que $G = N^{-1} G_1 N$.

Pour $A \in G$, on note $\rho_A : \begin{cases} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longmapsto & A^T M A \end{cases}$. On a $\rho_A \in \mathcal{GL}(\mathcal{M}_n(\mathbb{R}))$ et $(\rho_A)^{-1} = \rho_{A^{-1}}$.

On pose $H = \{\rho_A : A \in G\}$. C'est un sous-groupe de $\mathcal{GL}(\mathcal{M}_n(\mathbb{R}))$. (Comme I_n est dans G, on a $\mathrm{Id}_{\mathcal{GL}(\mathcal{M}_n(\mathbb{R}))} = \rho_{I_n} \in H$; si $A, A' \in G$, comme $AA' \in G$, on a $\rho_A \rho_{A'} = \rho_{AA'} \in H$; si $A \in G$, comme $A^{-1} \in G$, on a $(\rho_A)^{-1} = \rho_{A^{-1}} \in H$).

Comme $\rho : A \longmapsto \rho_A$ est continue sur $\mathcal{M}_n(\mathbb{R})$, $H = \rho(G)$ est un compact de $\mathcal{L}(\mathcal{M}_n(\mathbb{R}))$.

$f : A \longmapsto \rho_A(I_n) = A^T A$ est continue sur $\mathcal{M}_n(\mathbb{R})$, donc $f(G) = \{A^T A : A \in G\} := \Delta \subset \mathcal{S}_n^{++}(\mathbb{R})$ est compact. Ainsi, $K = \mathrm{Conv}(\Delta)$ est compact. Et comme $\mathcal{S}_n^{++}(\mathbb{R})$ est convexe, on a $K \subset \mathcal{S}_n^{++}(\mathbb{R})$.

Soient $A, A' \in G$. On a $\rho_{A'}(A^T A) = A'^T (A^T A) A' = (AA')^T (AA') \in \Delta$ puisque $AA' \in G$. Donc Δ est stable par les éléments de H. Ainsi, $K = \mathrm{Conv}(\Delta)$ est stable par les éléments de H. On applique alors le théorème de Markov-Kakutani :

Théorème : Soient E un $\mathbb{R}$-espace vectoriel de dimension finie, H un sous-groupe compact de $\mathcal{GL}(E)$ et K un compact convexe non vide de E stable par H. H admet un point fixe dans K.

□ Soit $\|\cdot\|_0$ une norme euclidienne sur E. On note $\|x\| = \max_{h\in H} \|h(x)\|_0$, bien défini puisque H est compact et $h \longmapsto h(x)$ est continue. On définit ainsi une norme sur E invariante par H et strictement convexe : si

$\|x\| = \|y\| = c > 0$ avec $x \neq y$, alors $\left\| \frac{x+y}{2} \right\| < c$. En effet, soit $h \in H$ tel que $\left\| \frac{x+y}{2} \right\| = \left\| h\left(\frac{x+y}{2}\right) \right\|_0$.

On a $\left\| \frac{x+y}{2} \right\|^2 = \frac{\|h(x)+h(y)\|_0^2}{4} = \frac{\|h(x)\|_0^2 + \|h(y)\|_0^2}{2} - \frac{\|h(x)-h(y)\|_0^2}{4} < c^2$.

Prenons $s \in K$ avec $\|s\|$ minimal. Par stricte convexité, ce s est unique. Comme K est stable par H et que $\|\cdot\|$ est invariante par H, s est un point fixe de H.

$\square$

Comme K est un compact convexe de $\mathscr{M}_n(\mathbb{R})$ stable par tous les éléments du groupe compact H, le théorème de Markov-Kakutani affirme qu'il existe $M \in K$ telle que : $\forall \rho \in H, \rho(M) = M$. Autrement dit : $\forall A \in G, \rho_A(M) = M$. On fixe désormais un tel M.

Comme $M \in \mathscr{S}_n^{++}(\mathbb{R})$, il existe $N \in \mathscr{GL}_n(\mathbb{R})$ telle que $M = N^T N$. Si $A \in G$, on a $\rho_A(M) = M$ i.e. $A^T M A = M$ i.e. $A^T N^T N A = N^T N$ i.e. $(NAN^{-1})^T(NAN^{-1}) = I_n$ i.e. $NAN^{-1} \in O_n(\mathbb{R})$. On pose $G_1 = NGN^{-1}$. G_1 est un sous-groupe de $O_n(\mathbb{R})$, image de G par le morphisme de groupes $\begin{cases} G & \longrightarrow & O_n(\mathbb{R}) \\ A & \longmapsto & NAN^{-1} \end{cases}$. Ainsi, G est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

- **Ellipsoïde de John-Loewner**

On va établir le résultat suivant :

Théorème : Soient E un espace euclidien et K une partie compacte de E contenant une base de E. Pour $u \in \mathcal{S}^+(E)$, on pose $C_u = \{x \in E : \langle x, u(x)\rangle \leqslant 1\}$. L'ensemble $A = \{u \in \mathcal{S}^+(E) : K \subset C_u\}$ est un compact de $\mathcal{L}(E)$. La fonction $\det$ atteint son maximum sur A en un unique point u, et ce point appartient à $\mathcal{S}^{++}(E)$.

L'ensemble C_u est un ellipsoïde dont le volume vaut $\alpha(\det u)^{-1/2}$, où α est le volume de la boule unité. Ce théorème signifie donc que K est inclus dans un unique ellipsoïde de volume minimal, appelé ellipsoïde de John-Loewner.

□ Calculons le volume de C_u. Il existe une base orthonomée $e = (e_1, \dots, e_n)$ dans laquelle $q(x) := \langle x, u(x)\rangle$ s'écrit $q(x) = \displaystyle\sum_{i=1}^{n} a_i x_i^2$ avec $a_i > 0$. On a $\mathrm{Vol}(C_u) = \displaystyle\int \dots \int_{a_1x_1^2+\dots+a_nx_n^2 \leqslant 1} dx_1 \dots dx_n$. On effectue le changement de variable $x_i = \dfrac{t_i}{\sqrt{a_i}}$, dont le jacobien est $\dfrac{1}{\sqrt{a_1 \dots a_n}}$. Si S est la matrice de q dans une base orthonormée quelconque de $\mathbb{R}^n$, il existe $P \in O_n(\mathbb{R})$ telle que $S = P\,\mathrm{Diag}(a_1, \dots, a_n)P^T$. On a $\det S = a_1 \dots a_n := D(q)$.
On obtient $\mathrm{Vol}(C_u) = \displaystyle\int \dots \int_{x_1^2+\dots+x_n^2 \leqslant 1} \frac{dx_1 \dots dx_n}{\sqrt{D(q)}} = \frac{\alpha}{\sqrt{D(q)}}$.

□

Comme on est en dimension finie, il suffit de montrer que A est fermé et borné. Si $(u_k)_{k \in \mathbb{N}}$ est une suite d'éléments de A convergeant vers u, on a pour tout $x \in E$, $\langle x, u(x)\rangle = \displaystyle\lim_{k \to +\infty} \langle x, u_k(x)\rangle \leqslant 1$ par continuité de l'application $u \longmapsto \langle x, u(x)\rangle$ pour tout x. Ainsi, A est fermé.

Soient $(e_1, \dots, e_n)$ une base de E incluse dans K, $u \in A$ et $x = \displaystyle\sum_{i=1}^{n} x_i e_i$ un vecteur quelconque de E. On a $\langle x, u(x)\rangle = \displaystyle\sum_{i,j \in [\![1,n]\!]} x_i x_j \langle e_i, u(e_j)\rangle$ avec $|\langle e_i, u(e_j)\rangle| \leqslant \sqrt{\langle e_i, u(e_i)\rangle \langle e_j, u(e_j)\rangle} \leqslant 1$ par inégalité de Cauchy-Schwarz (l'application $(x, y) \longmapsto \langle x, u(y)\rangle$ est une forme bilinéaire symétrique positive). Donc $\langle x, u(x)\rangle \leqslant \displaystyle\sum_{i,j \in [\![1,n]\!]} |x_i x_j| = \left(\sum_{i=1}^{n} |x_i|\right)^2$. Par équivalence des normes, il existe $k > 0$ tel que $\|\cdot\|_1 \leqslant k\|\cdot\|$ où $\|\cdot\|$ désigne la norme euclidienne sur E. Si x est un vecteur propre de u relatif à la valeur propre λ, on obtient $\langle x, u(x)\rangle = \lambda\|x\|^2 \leqslant k^2\|x\|^2$ et donc $0 \leqslant \lambda \leqslant k^2$. Comme $u \in \mathcal{S}^+(E)$, on a $|\!|\!| u |\!|\!| = \displaystyle\max_{\lambda \in \mathrm{Sp}(u)} \lambda \leqslant k^2$. Donc A est borné.

La fonction continue $\det$ atteint son maximum sur le compact A en un point u. Montrons que $\det u > 0$ (i.e. $u \in \mathcal{S}^{++}(E)$). Il suffit pour cela de montrer que A contient un élément de $\mathcal{S}^{++}(E)$. L'ensemble K est borné. Soit $m > 0$ tel que : $\forall x \in K,\ \|x\| \leqslant m$. Si $f \in \mathcal{S}^{++}(E)$, alors pour tout $x \in K$, on a $0 \leqslant \langle x, f(x)\rangle \leqslant \|\!| f \|\!| \|x\|^2 \leqslant \|\!| f \|\!| m^2$. Pour que $f \in A$, il suffit que $\|\!| f \|\!| \leqslant 1/m^2$, c'est-à-dire que la plus grande valeur propre de f soit $\leqslant 1/m^2$. Il existe de tels f.

Reste à montrer l'unicité de u. On sait que si $u, v \in \mathcal{S}^{++}(E)$, alors $\det\left(\dfrac{u+v}{2}\right) \geqslant \sqrt{\det u \det v}$ avec une inégalité stricte si $u \neq v$. Si le maximum de $\det$ sur A est atteint en u et v distincts, on a $\det\left(\dfrac{u+v}{2}\right) > \sqrt{\det u \det v} = \det u$. Mais $\left\langle x, \dfrac{u(x)+v(x)}{2}\right\rangle = \dfrac{\langle x, u(x)\rangle + \langle x, v(x)\rangle}{2} \leqslant 1$ donc $\dfrac{u+v}{2} \in A$. Absurde : cela contredit la maximalité de $\det u$.

Démontrons maintenant l'inégalité de convexité sur le déterminant utilisée précédemment.
Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n^{++}(\mathbb{R})$. Il existe $P \in \mathcal{GL}_n(\mathbb{R})$ et $D = \operatorname{Diag}(\lambda_1, \dots, \lambda_n)$ telles que $A = P^T P$ et $B = P^T D P$. En effet, en notant C la racine symétrique positive de A, la matrice $C^{-1}BC^{-1}$ est symétrique, donc il existe $Q \in O_n(\mathbb{R})$ telle que $Q^{-1}C^{-1}BC^{-1}Q = D$ avec D diagonale. On pose $P = Q^{-1}C$. On a alors $P^T P = CQQ^T C = C^2 = A$.

Proposition : Soient $A, B \in \mathcal{S}_n^{+}(\mathbb{R})$ et $\alpha, \beta \in \mathbb{R}_+$ tels que $\alpha + \beta = 1$.
On a $\det(\alpha A + \beta B) \geqslant \det(A)^\alpha \det(B)^\beta$.

☐ Si l'une des deux matrices n'est pas définie positive, le résultat est immédiat. On suppose donc $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ et on se donne P et D comme ci-dessus. Les λ_i (valeurs propres de B) sont alors strictement positifs. On a $\det(A)^\alpha \det(B)^\beta = (\det P^2)^\alpha (\det P^2 \det D)^\beta = \det(P^2)\det(D)^\beta$ et $\det(\alpha A + \beta B) = \det P^2 \det(\alpha I_n + \beta D)$. On est ramené à montrer que $\det(\alpha I_n + \beta D) \geqslant \det(D)^\beta$ i.e. $\displaystyle\prod_{i=1}^n (\alpha + \beta\lambda_i) \geqslant \left(\prod_{i=1}^n \lambda_i\right)^\beta$ i.e. $\displaystyle\sum_{i=1}^n \ln(\alpha + \beta\lambda_i) \geqslant \beta \sum_{i=1}^n \ln \lambda_i$.
Or, par concavité du logarithme, on a pour tout i, $\ln(\alpha + \beta\lambda_i) \geqslant \alpha \ln 1 + \beta \ln \lambda_i = \beta \ln \lambda_i$. D'où le résultat.

☐

Si $\alpha \in\,]0,1[$ et $A \neq B$, l'un des λ_i est différent de 1 donc, par stricte concavité du logarithme, l'une des inégalités est stricte et $\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$.

Le résultat sur l'ellipsoïde de Loewner se généralise aux ellipsoïdes $\mathcal{E}_q = \{x \in \mathbb{R}^n : q(x) \leqslant 1\}$ où q est une forme quadratique. On en déduit le résultat suivant :

Corollaire : Soient E un $\mathbb{R}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et G un sous-groupe compact de $\mathcal{GL}(E)$. Il existe un produit scalaire associé à une forme quadratique q tel que $G \subset O(q) := \{u \in \mathcal{GL}(E) : q \circ u = q\}$.