23. Théorème de Carathéodory [Gou08, §1.5, p54]

ÉNONCÉ

Théorème. [Théorème de Carathéodory] *Soit X un espace affine de dimension finie n. Alors pour tout $S \subset X$, $\operatorname{conv}(S)$ est l'ensemble des barycentres à coefficients positifs d'au plus $n+1$ points de S. Autrement dit :*

$$\operatorname{conv}(S) = \left\{ \sum_{i=1}^{n+1} \lambda_i x_i \,\middle|\, (x_i, \lambda_i)_{1\le i\le n+1} \in (S \times \mathbb{R}_+)^{n+1} \right\}$$

Corollaire. *Soit S un compact de X euclidien. Alors $\operatorname{conv}(S)$ est compact.*

Application. Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Notons $(C_j)_{1\le j\le n}$ ses colonnes. L'équation diophantienne $MX = 0$ admet une solution non nulle dans $\mathbb{N}^n$ si et seulement si $0 \in \operatorname{conv}(\{C_1, \dots, C_n\})$.

DÉVELOPPEMENT

1. Soit $S \subset X$ et $x \in \operatorname{conv}(S)$. Ecrivons $x = \sum_{i=1}^p \lambda_i x_i$ pour des $(x_i)_{1\le i\le p} \in S^p$, avec $(\lambda_i)_{1\le i\le p} \in (\mathbb{R}_+^*)^p$ et $\sum_{i=1}^p \lambda_i = 1$, de sorte que p soit minimal.
Supposons par l'absurde que $p \ge n+2$.
Les vecteurs $\{x_1, \dots, x_p\}$ sont liés dans X puisque $p \ge n+2$, donc :
$$\exists (\alpha_2, \dots, \alpha_p) \in \mathbb{R}^{p-1} \setminus \{0_{\mathbb{R}^{p-1}}\} \mid \sum_{i=2}^p \alpha_i \overrightarrow{x_1 x_i} = \vec{0}$$
Posant $\alpha_1 = -\sum_{i=2}^p \alpha_i$, on a $\sum_{i=1}^p \alpha_i x_i = 0$ et $\sum_{i=1}^p \alpha_i = 0$.
Ainsi pour $t \in \mathbb{R}$, on a $x = \sum_{i=1}^p (\lambda_i + t\alpha_i) x_i$ et $\sum_{i=1}^p \lambda_i + t\alpha_i = 1$. Considérons alors :
$$\begin{aligned} F &= \{ t \in \mathbb{R} \mid \forall i \in [\![1,p]\!], \lambda_i + t\alpha_i \ge 0 \} \\ &= \left(\bigcap_{i \mid \alpha_i > 0} \left[-\frac{\lambda_i}{\alpha_i}, +\infty \right[\right) \bigcap \left(\bigcap_{i \mid \alpha_i < 0} \left] -\infty, -\frac{\lambda_i}{\alpha_i} \right] \right) \end{aligned}$$
F contient 0 donc est non vide. Ce ne peut être $\mathbb{R}$ puisque l'un au moins des $(\alpha_i)_{1\le i\le p}$ est non nul. Donc F admet une borne inférieure et/ou[1] supérieure, de la forme $-\lambda_{i_0}/\alpha_{i_0}$ pour un certain i_0 et notée t_0. Il est clair que $t_0 \in F$ puisque F est fermé et on a :
$$x = \sum_{1\le i\le p} (\lambda_i - t_0\alpha_i) x_i = \sum_{1\le i\le p \mid i \ne i_0} (\lambda_i - t_0\alpha_i) x_i \qquad \text{et} \qquad \forall i, \lambda_i - t_0\alpha_i \ge 0$$
Ce qui contredit la minimalité de p. Donc $p \le n+1$, ce qui conclut.

2. Soit S un compact de X. Définissons :
$$f : \begin{array}{ccc} S^{n+1} \times \{ (\lambda_i)_{1\le i\le n+1} \in \mathbb{R}_+^{n+1} \mid \sum_i \lambda_i = 1 \} & \longrightarrow & \operatorname{conv}(S) \\ (x_1, \dots, x_{n+1}, \lambda_1, \dots, \lambda_{n+1}) & \longmapsto & \sum_{i=1}^{n+1} \lambda_i x_i \end{array}$$
Cette application est bien définie et est surjective par le théorème de Carathéodory. Comme elle est continue et définie sur un compact, son image $\operatorname{conv}(S)$ est compacte.

3. Soit $M \in \mathcal{M}_n(\mathbb{Z})$.
   - S'il existe $X \in \mathbb{N}^n$ non nul tel que $MX = 0$, alors :
   $$\sum_{i=1}^n x_i C_i = 0 \qquad \text{ou encore} \qquad \sum_{i=1}^n \frac{x_i}{\sum_j x_j} C_i = 0$$
   Donc $0 \in \operatorname{conv}(C_1, \dots, C_n)$.
   - Réciproquement, supposons que $0 \in \operatorname{conv}(C_1, \dots, C_n)$. Si l'une des colonnes est nulle, le résultat est évident.
   Sinon, soit p minimal[2] tel que $0 = \sum_{j=1}^p \lambda_j C_{i_j}$, avec $(\lambda_j)_{1\le j\le p} \in (\mathbb{R}_+^*)^p$.
   Notons $r = \operatorname{rg}(C_{i_1}, \dots, C_{i_p})$. On a $r < p$ puisque les colonnes sont liées.
   Par ailleurs $\operatorname{conv}(C_{i_1}, \dots, C_{i_p}) \subset \operatorname{Vect}(C_{i_1}, \dots, C_{i_p})$ espace de dimension r, donc par le théorème de Carathéodory $p \le r+1$. Ainsi $r = p-1$.
   $\ker_{\mathbb{Q}}(C_{i_1}, \dots, C_{i_p}) \subset \ker_{\mathbb{R}}(C_{i_1}, \dots, C_{i_p})$ sont donc des sous-espaces de dimension[3] 1 dirigés par $\Lambda = (\lambda_1, \dots, \lambda_p)$ (qui est un vecteur à coefficients réels).
   Ainsi il existe $\alpha \in \mathbb{R}_+^*$ tel que $(\mu_1, \dots, \mu_p) = \alpha\Lambda \in (\mathbb{Q}_+^*)^p$ et $\sum_{j=1}^p \mu_j M_{i_j} = 0$.
   En multipliant par le produit d des dénominateurs de $\alpha\Lambda$, on a donc :
   $$\sum_{j=1}^p d\mu_j M_{i_j} = 0 \qquad \text{où} \qquad \forall 1 \le j \le p, d\mu_j \in \mathbb{N}$$
   Ou encore si l'on définit $X = (x_1, \dots, x_n)$ par $x_{i_j} = d\mu_j$ et 0 pour les autres x_i, on a que $X \in \mathbb{N}^n$ est non nul (puisque $p \ge 1$) et $MX = 0$.

COMMENTAIRES

Il faut être à l'aise sur l'invariance du rang par extension de corps.

1. en fait *et* puisque la somme des $(\alpha_i)_{1\le i\le p}$ est nulle
2. ainsi $p \ge 1$
3. la dimension est la même par invariance du rang par extension de corps