Étude spectrale des automorphismes du tore

19 mai 2003

On se propose ici de présenter un exemple classique de système dynamique d'origine algébrique : les automorphismes du tore $\mathbb{T}^n$, et de voir comment leurs propriétés d'ergodicité et de mélange se déduisent de leur étude spectrale.

1 Les automorphismes du tore $\mathbb{T}^n$

1.1 Le tore $\mathbb{T}^n$

Soit n un entier naturel fixé, $n \geq 1$. On appelle *tore de dimension* n, noté $\mathbb{T}^n$, le groupe abélien quotient (pour l'addition) $\mathbb{R}^n/\mathbb{Z}^n$. Un point x de $\mathbb{T}^n$ est représenté par un n-uplet de coordonnées $(x_1, \ldots, x_n) \in [0,1[^n$, et l'addition sur $\mathbb{T}^n$ est simplement l'addition modulo 1 sur chacune des n coordonnées. Comme tout groupe abélien compact, $\mathbb{T}^n$ peut être muni d'une unique mesure de probabilité μ qui soit *invariante par rotation*, c'est-à-dire telle que pour toute partie mesurable A de $\mathbb{T}^n$ et tout $x \in \mathbb{T}^n$, $\mu(A+x) = \mu(A)$. Cette probabilité est appelée *mesure de Haar* sur $\mathbb{T}^n$, et coïncide dans le cas de $\mathbb{T}^n$ avec la mesure de Lebesgue λ_n sur $[0,1[^n$. Si on note $\mathscr{A}$ la tribu des boréliens de $\mathbb{T}^n$, complétée pour λ_n, $(\mathbb{T}^n, \mathscr{A}, \lambda_n)$ est un espace de Lebesgue.

1.2 Endomorphismes et automorphismes du groupe abélien $\mathbb{T}^n$

Soit $M = (m_{i,j})_{i,j=1,\ldots,n}$ une matrice à coefficients entiers. On note T_M la transformation du tore $\mathbb{T}^n$ définie par

$$x = (x_1, \ldots, x_n) \ \longmapsto \ Mx = \left(\sum_{j=1}^{n} m_{i,j} x_j \bmod 1 \right)_{i=1,\ldots,n}.$$

Alors T_M est un endomorphisme continu du groupe compact abélien $\mathbb{T}^n$. En effet, il est évident par définition de T_M que si x et y sont deux points de $\mathbb{T}^n$, $T_M(x+y) = T_M x + T_M y$. On peut d'ailleurs montrer que tous les endomorphismes continus de $\mathbb{T}^n$ sont de cette forme.

Proposition 1.1 *T_M est une surjection de $\mathbb{T}^n$ sur lui-même si et seulement si* $\det M \neq 0$, *et dans ce cas T_M préserve la mesure de Lebesgue λ_n.*

Preuve — Si $\det M = 0$, les vecteurs lignes $M_1, \ldots, M_n$ de M sont linéairement dépendants sur le corps des rationnels, et il existe donc des entiers $m_1, \ldots, m_n$ non tous nuls tels que $m_1 M_1 + \cdots + m_n M_n = 0$. Tout point y dans $T_M(\mathbb{T}^n)$ vérifie alors $m_1 y_1 + \cdots + m_n y_n = 0 \bmod 1$, et donc $T_M(\mathbb{T}^n) \subsetneq \mathbb{T}^n$. Supposons maintenant $\det M \neq 0$. Alors l'endomorphisme de $\mathbb{R}^n$ défini canoniquement par M est surjectif, et on en déduit immédiatement que T_M est également une surjection de $\mathbb{T}^n$ sur lui-même. Il reste à montrer que dans ce cas, T_M préserve λ_n.

Notons μ la mesure image de λ_n par T_M. Alors μ est une probabilité sur $\mathbb{T}^n$, et par unicité de la mesure de Haar, pour montrer que $\mu = \lambda_n$ il suffit de vérifier que μ est invariante par rotation. Soient donc A un borélien de $\mathbb{T}^n$, et $x \in \mathbb{T}^n$. Puisque T_M est surjective, il existe $z \in \mathbb{T}^n$ tel que $T_M z = x$. On a alors

$$\begin{aligned} T_M^{-1}(A+x) &= \{y \in \mathbb{T}^n \ / \ T_M y - x \in A\} \\ &= \{y \in \mathbb{T}^n \ / \ T_M(y-z) \in A\} \\ &= \left\{y \in \mathbb{T}^n \ / \ y - z \in T_M^{-1}A\right\} \\ &= T_M^{-1}A + z. \end{aligned}$$

On a donc

$$\begin{aligned} \mu(A+x) &= \lambda_n\left(T_M^{-1}(A+x)\right) \\ &= \lambda_n\left(T_M^{-1}A + z\right) \\ &= \lambda_n\left(T_M^{-1}A\right) \\ &= \mu(A). \end{aligned}$$

□

Ainsi, dans le cas où $\det M \neq 0$, T_M est à la fois un endomorphisme du groupe abélien $(\mathbb{T}^n, +)$, et un endomorphisme de l'espace de Lebesgue $(\mathbb{T}^n, \mathscr{A}, \lambda_n)$. Voyons maintenant le cas où T_M est une bijection.

Proposition 1.2 *Si $|detM| = 1$, T_M est une bijection de $\mathbb{T}^n$ sur lui-même. C'est donc un automorphisme du groupe abélien $(\mathbb{T}^n, +)$, et un automorphisme de l'espace de Lebesgue $(\mathbb{T}^n, \mathscr{A}, \lambda_n)$.*

Preuve — Puisque $|detM| = 1$, M est inversible et son inverse M^{-1} est aussi à coefficients entiers. On vérifie alors aisément que tout $y \in \mathbb{T}^n$ a un unique antécédent par T_M, qui est $T_{M^{-1}}y$. □

Remarque : on peut montrer que la condition $|\det M| = 1$ est à la fois nécessaire et suffisante pour que T_M soit bijective ; voir par exemple [1], p. 15.

Exemples :
- $x \mapsto 2x$ est un endomorphisme de $\mathbb{T} = \mathbb{R}/\mathbb{Z}$.
- En dimension 2, soit M la matrice

$$M \stackrel{\text{déf}}{=} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Alors T_M est un automorphisme de $\mathbb{T}^2$.

2 Étude spectrale

2.1 Les caractères

En général, si G est un groupe abélien localement compact, on appelle *caractère* de G un morphisme continu de G dans le cercle unité S^1 de $\mathbb{C}$ (vu comme un groupe multiplicatif), et on note $\hat{G}$ l'ensemble des caractères de G. Dans le cas où $G = (\mathbb{T}^n, +)$, les caractères sont les applications de la forme $\gamma_p = \gamma_{(p_1,\dots,p_n)}$, $p \in \mathbb{Z}^n$, où

$$\gamma_p \;:\; (x_1, \dots, x_n) \longmapsto e^{i2\pi(p_1x_1+\dots+p_nx_n)}.$$

(On peut admettre ce résultat, ou tout simplement prendre cette définition pour les caractères de $\mathbb{T}^n$.)

Comme ils sont à valeurs dans S^1, les caractères peuvent aussi être vus comme des éléments de $L^2(\lambda_n)$. Il est facile de voir que, sous l'action d'un endomorphisme T_M, un caractère est transformé en un autre caractère. Plus précisément, pour tout $p = (p_1, \dots, p_n) \in \mathbb{Z}^n$, on a

$$\gamma_p \circ T_M \;=\; U_{T_M}\gamma_p \;=\; \gamma_{({}^tM\,p)}. \tag{1}$$

De plus, la proposition qui suit montre que les caractères tiennent toujours dans l'étude de $L^2(\lambda_n)$ un rôle privilégié.

Proposition 2.1 *Les caractères de $\mathbb{T}^n$ forment un sustème orthonormal total dans $L^2(\lambda_n)$.*

Preuve — Un simple calcul montre que si $p = (p_1, \dots, p_n)$ et $q = (q_1, \dots, q_n)$ sont deux éléments distincts de $\mathbb{Z}^n$, alors

$$\langle \gamma_p \,,\, \gamma_q \rangle \;=\; \int_{\mathbb{T}^n} \gamma_{p-q}\, d\lambda_n \;=\; 0.$$

Par ailleurs, le théorème de Stone-Weierstrass assure que les combinaisons linéaires finies de caractères sont denses dans l'espace $C(\mathbb{T}^n)$ des fonctions continues de $\mathbb{T}^n$ dans $\mathbb{C}$. On en déduit facilement que le sous-espace de $L^2(\lambda_n)$ engendré par les caractères est dense dans $L^2(\lambda_n)$. □

Remarque : ce résultat ce généralise au cas d'un groupe abélien compact G, pour lequel $\hat{G}$ est forcément dénombrable, et forme aussi une base hilbertienne de $L^2(\mu)$ où μ est la mesure de *Haar* de G.

2.2 Condition d'ergodicité et de mélange d'un automorphisme de $\mathbb{T}^n$

On fixe maintenant une matrice $M \in \mathscr{M}_n(\mathbb{Z})$, et on cherche à quelle condition l'automorphisme T_M de $\mathbb{T}^n$ est ergodique. Puisque l'ensemble des caractères est stable par l'opérateur unitaire U_{T_M}, on peut partitionner cet ensemble en orbites, qui sont d'après (1) de la forme

$$\mathrm{orb}(\gamma_p) \;\stackrel{\text{déf}}{=}\; \left\{ U_{T_M}^k \gamma_p \;/\; k \in \mathbb{Z} \right\} \;=\; \left\{ \gamma_{({}^tM^k p)} \;/\; k \in \mathbb{Z} \right\}.$$

À chacune de ces orbites correspond un sous-espace cyclique $S(\gamma_p)$ qu'elle engendre, et grâce à la proposition 2.1 on peut écrire $L_0^2(\lambda_n)$ comme une somme directe de ces sous-espaces cycliques. L'étude spectrale de l'opérateur U_{T_M} sur $L_0^2(\lambda_n)$ se ramène ainsi à l'étude de ses restrictions aux sous-espaces $S(\gamma_p)$. Fixons donc un caractère γ_p (avec $p \neq 0$ puisque l'on se place directement dans L_0^2), et voyons comment peut agir U_{T_M} sur $S(\gamma_p)$.

Supposons tout d'abord que l'orbite de γ_p sous l'action de U_{T_M} est constituée de caractères deux à deux distincts. Alors, ces caractères étant orthogonaux, la mesure spectrale de γ_p est automatiquement la mesure de Lebesgue.

Dans le cas contraire, il existe un plus petit entier $r \geq 1$ tel que $U_{T_M}^r \gamma_p = \gamma_p$, c'est-à-dire tel que ${}^tM^r p = p$. Posons dans ce cas $f \stackrel{\text{déf}}{=} \sum_{k=0}^{r-1} U_{T_M}^k \gamma_p$. Alors $U_{T_M} f = f$, mais f ne peut pas être constante car $\langle f\,,\, \gamma_p \rangle = 1$. On en déduit alors que T n'est pas ergodique.

Il n'y a finalement que deux alternatives possibles : ou bien toutes les orbites des γ_p ($p \neq 0$) sont infinies, et alors T_M a spectre de Lebesgue (en particulier, T_M est mélangeant), ou bien il existe un $p \neq 0$ tel que l'orbite de γ_p est finie, et alors T_M n'est pas ergodique.

Il nous reste à voir à quelle condition une orbite d'un γ_p peut être finie, pour un $p \neq 0$. Si c'est le cas, on a vu qu'il existe un plus petit entier $r \geq 1$ tel que ${}^tM^r p = p$. Dans ce cas, la matrice M^r admet 1 comme valeur propre, et donc M admet une racine r-ième de l'unité comme valeur propre. Inversement, supposons qu'il existe un entier $r \geq 1$ tel que M possède une valeur propre racine r-ième de l'unité. Alors ${}^tM^r$ admet 1 comme valeur propre, et on peut trouver un vecteur propre associé dont les coefficients sont dans le corps des rationnels. On peut donc trouver un $p \in \mathbb{Z}^n$, $p \neq 0$, tel que ${}^tM^r p = p$, et dans ce cas l'orbite de γ_p est finie.

En conclusion de cette analyse, on peut énoncer le théorème suivant.

Théorème 2.2 *Soit M une matrice dans $\mathscr{M}_n(\mathbb{Z})$, de déterminant ± 1, et T_M l'automorphisme de $\mathbb{T}^n$ associé. Les conditions suivantes sont équivalentes.*

1. *M n'a pas de valeur propre racine de l'unité.*
2. *T_M est ergodique.*
3. *T_M est mélangeante.*
4. *T_M a spectre de Lebesgue.*

Remarque : on peut montrer que dans ce cas, la multiplicité du spectre de Lebesgue est infinie, c'est-à-dire que l'ensemble des caractères se partitionne en un nombre infini d'orbites. Pour cela, appelons *hauteur* du caractère γ_p le plus grand entier h pour lequel il existe un autre caractère γ_q vérifiant $\gamma_q^h = \gamma_p$. On voit facilement que la hauteur est constante le long d'une orbite. Par ailleurs, si $p = (p_1, \ldots, p_n)$, la hauteur de γ_p est tout simplement le pgcd de $p_1, \ldots, p_n$, et donc il existe des caractères de hauteur arbitrairement grande. On en déduit immédiatement que le nombre d'orbites ne peut être fini.

Références

[1] P. Walters, *An introduction to ergodic theory*, Springer-Verlag, 1982.