Développement: Théorème de Molien

Adrien Fontaine

11 octobre 2013

Référence : Gabriel Peyré, L'algèbre discrète de la transformée de Fourier
Eric Leichtnam, Xavier Schauer, Exercices corrigés de Mathématiques posés à l'oral des concours de Polytechnique et des Écoles Normales Supérieures

Théorème 1

Soit G un sous-groupe fini de $GL_n(\mathbb{C})$. Il agit linéairement sur $\mathbb{C}[X_1, ..., X_n]$ via :

$$\forall A \in G, \forall P \in \mathbb{C}[X_1, ..., X_n], A.P(X_1, ..., X_n) = P({}^t(A^{-1t}(X_1, ..., X_n)))$$

qui est une notation pratique pour dire que l'on substitue $\sum_{j=1}^n \alpha_{j,i} X_j$ à X_i, si l'on note $A^{-1} = (\alpha_{i,j})$. Soit V_d le sous-espace (de dimension finie!) de $\mathbb{C}[X_1, ..., X_n]$ des polynômes homogènes de degré d. On remarque que V_d est stable par l'action de G sur $\mathbb{C}[X_1, ..., X_n]$, i.e

$$\forall A \in G, \forall P \in V_d, A.P \in V_d$$

(une substitution linéaire des variables dans un polynômes homogènes reste homogène de degré d). La restriction de l'action de G sur $\mathbb{C}[X_1, ..., X_n]$ à V_d induit un morphisme de groupe

$$\begin{array}{cccc} \rho_d & : & G & \rightarrow & GL(V_d) \\ & & A & \mapsto & (P \mapsto A.P) \end{array}$$

On note

$$V_d^G = \{P \in V_d, \forall A \in G, A.P = P\} = \{P \in V_d, \forall A \in G, \rho_d(A)(P) = P\}$$

l'ensemble des polynômes $P \in V_d$ invariants sous l'action de G.
Le théorème de Molien est l'égalité des séries formelles :

$$\frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - tA)} = \sum_{d \geq 0} dim(V_d^G) t^d$$

avec rayon de convergence au moins 1.

Démonstration : Il est facile de voir que ρ_d est compatible avec la multiplication des polynômes.

Notons par ailleurs

$$\begin{array}{cccc} \xi_d & : & G & \rightarrow & \mathbb{C} \\ & & A & \mapsto & Tr(\rho_d(A)) \end{array}$$

On a d'abord besoin du lemme suivant :

Lemme 1

$$dim(V_d^G) = \frac{1}{|G|} \sum_{A \in G} \chi_(A)$$

Démonstration : Soit $R_G = \frac{1}{|G|}\sum_{g\in G}\rho_d(g)$ (l'opérateur de Reynolds). On va montrer que R_G est un projecteur sur V_d^G.
Montrons tout d'abord que $Im(R_G) = V_d^G$.
Soit $y = R_G(x) \in Im(R_g)$. Alors, pour tout $s \in G$, on a :

$$\begin{aligned}\rho_(s)(y) &= \frac{1}{|G|}\sum_{g\in G}\rho_d(s)(\rho_d(g)(x)) \\ &= \frac{1}{|G|}\sum_{g\in G}\rho_d(sg)(x) \\ &= \frac{1}{|G|}\sum_{h\in G}\rho_d(h)(x) \\ &= R_G(x) = y\end{aligned}$$

car $g \in G \mapsto sg$ est une bijection de G sur lui même.
Donc, $y \in V_d^G$.
Réciproquement, si $x \in V_d(G)$, alors pour tout $g \in G$, $\rho_d(g)(x) = x$ et donc,

$$R_G(x) = \frac{1}{|G|}|G|x = x$$

et donc $x \in Im(R_G)$.
Ainsi, R_G est d'image V_d^G. Par ailleurs, le calcul précédent donne $R_g^2 = R_G$. Donc, R_G est un projecteur sur V_d^G.
Alors, en écrivant la matrice de R_G dans une base adaptée à son image et à son noyau, on obtient que $Tr(R_G) = dim(V_d^G)$. Or, par linéarité de la trace,

$$Tr(R_G) = \frac{1}{|G|}\sum_{g\in G}\chi_d(g)$$

ce qui donne le résultat annoncé. ■

Lemme 2

Pour tout $A \in G$, on a l'égalité des séries suivantes, avec de plus rayon de convergence au moins 1 :

$$\frac{1}{det(I-tA)} = \sum_{d\geq 0}\chi_d(A^{-1})t^d$$

Démonstration : Comme G est fini, on a d'après le théorème de Lagrange, $X^{|G|}-1$ qui est un polynôme annulateur pour tous les éléments de G. Comme il est scindé à racines simples, les éléments de G sont tous diagonalisables et à valeurs propres dans l'ensemble des racines de l'unité. En particulier, toutes les valeurs propres sont de module 1. Soit alors $A \in G$, et $\lambda_1, ..., \lambda_n$ les valeurs propres de A. On a :

$$\frac{1}{det(I-tA)} = \prod_{i=1}^{n}\frac{1}{1-t\lambda_i} = \prod_{i=1}^{n}\sum_{k\geq 0}\lambda_i^k t^k = \sum_{k\geq 0}\left(\sum_{k_1+...+k_n=k}\lambda_1^{k_1}...\lambda_n^{k_n}\right)t^k$$

où la dernières série est obtenue par produit de Cauchy des n séries, argument permettant également d'obtenir que le rayon de convergence est au moins 1, chacune des séries étant de rayon de convergence 1, puisque les λ_i sont de module 1).
D'autre part, soit un élément de la base canonique de V_d, $X_1^{k_1}...X_n^{k_n}$ avec $K_1+...+k_n = d$.

Quitte à considérer $V_1^{k_1}...V_n^{k_n}$ ou $(V_1,...,V_n) = P.(X_1,...,X_n)$ (avec P matrice de passage dans une base de diagonalisation pour A), on peut supposer que A est diagonale (avec les valeurs propres dans l'ordre de leur numérotation). On a alors

$$\rho_d(A^{-1})(X_1^{k_1}...X_n^{k_n}) = \rho(A^{-1})(X_1)^{k_1}...\rho(A^{-1})(X_n)^{k_n} = (\lambda_1 X_1)^{k_1}...(\lambda_n X_n)^{k_n} = \lambda_1^{k_1}...\lambda_n^{k_n}(X_1^{k_1}...X_n^{k_n})$$

Et donc,

$$\chi_d(A^{-1}) = \rho_d(A^{-1}) = \sum_{k_1+...k_n=d} \lambda_1^{k_1}...\lambda_n^{k_n}$$

Ce qui conclut sur l'inégalité des séries. ■

Pour conclure, il suffit d'écrire

$$\frac{1}{|G|}\sum_{A\in G}\frac{1}{det(I-tA)} = \frac{1}{|G|}\sum_{A\in G}\sum_{d\geq 0}\chi_d(A^{-1})t^d = \sum_{d\geq 0}\left(\frac{1}{|G|}\sum_{A\in G}\chi_d(A^{-1})\right)t^d = \sum_{d\geq 0} dim(V_d^G)t^d$$

où l'on a interverti les sommes car l'une était finie, et où l'on a appliqué les deux lemmes (en disant bien que l'inversion est une bijection de G sur lui même pour pouvoir appliquer le premier lemme). Le rayon de convergence est évidemment au moins 1, puisque la série est somme finie de séries avec un tel rayon de convergence. ■

Remarque 1

(i) Le fait que V_d soit de dimension finie est important. En effet, quel sens donner à la trace d'un automorphisme d'espace vectoriel de dimension infinie ?

(ii) Il faut également être capable de trouver la dimension de V_d. Pour rappel, c'est la quantité

$$\binom{d-1}{n+d-1}$$

(iii) Le développement peut évidemment se réécrire avec le vocabulaire des représentations (ρ_d est la représentation de G, et ξ_d la caractère associé), mais cela n'apporte rien à la démonstration. Cela permet néanmoins de replacer ce développement dans les leçons de représentation.