Le théorème de Molien

Laurent DIETRICH *

17 juin 2011

Réf. : Gabriel Peyré – l'algèbre discrète de la transformée de Fourier.

Remarque.

i) Il faut adapter les notations de la référence en mettant des caractères là où il y a des traces afin de rentrer le développement dans les leçons de représentations – où il a le plus sa place !

ii) Penser à conclure en sommant à la fin, et attention, il manque un $\frac{1}{|G|}$ dans l'énoncé du livre.

iii) Merci à Tristan Vaccon pour une reformulation claire, de laquelle je me suis largement inspiré !

iv) Attention, il faut bien mettre un A^{-1} pour avoir une action (sinon c'est une action à droite), et cela change clairement le deuxième lemme où l'on a tendance à mettre un A... Heureusement, on retombe sur nos pattes au final en sommant, car l'inversion est une bijection de G.

v) On peut penser que le lemme 1 tue à lui seul la question de la dimension des V_d^G. Question possible du jury ? Que dire niveau complexité de calcul ? Un déterminant c'est dur à calculer mais avec le lemme 1 il faut appliquer chaque matrice à toute une base de V_d^G...

vi) Il faut savoir calculer $\dim(V_d)$. C'est le nombre de n-uplets dont la somme des éléments vaut d. On peut voir cela comme le nombre de façons de mettre d objets dans n boîtes, ou encore si on dessine ces objets sur une ligne et qu'on les sépare par des barres pour signifier un changement de boîte, comme le nombre de façons de choisir les $n-1$ séparations parmi les $d+n-1$ items qui apparaitront. On tombe donc sur $\binom{d+n-1}{n-1}$ soit encore $\binom{d+n-1}{d}$.

Théorème. *Soit G un sous-groupe fini de $GL_n(\mathbb{C})$. Il agit linéairement sur le sous espace $V_d \subset \mathbb{C}[X_1, \cdots, X_n]$ des polynômes homogènes de degré d par :*

$$A \cdot P(X_1, \cdots, X_n) = P((A^{-1}(X_1, \cdots, X_n)')')$$

qui est une notation pratique pour dire que l'on substitue $\sum_{j=1}^{n} \alpha_{ji} X_j$ à X_i si l'on note $A^{-1} = ((\alpha_{ij}))$. On note que V_d n'est qu'un sous-espace vectoriel de $\mathbb{C}[X_1, \cdots, X_n]$ stable par la même action plus générale sur $\mathbb{C}[X_1, \cdots, X_n]$ tout entier (une substitution linéaire des variables dans un polynôme homogène reste homogène de même degré). On cherche un moyen pratique (algorithmique ?) de déterminer la dimension de V_d^G, le sous-espace des invariants de cette représentation. Le théorème de Molien est l'égalité des séries formelles :

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

*http://perso.eleves.bretagne.ens-cachan.fr/~ldiet783 *avec rayon de convergence au moins 1. On notera $\rho_d : G \to GL(V_d)$ la représentation de groupes correspondante et $\chi_d(g)$ les caractères. On notera rho l'action générale sur $\mathbb{C}[X_1, \cdots, X_n]$. On remarque que cette action est clairement compatible avec la multiplication des polynômes.*

Démonstration.

Lemme.

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

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. Soit $y = R_G(x) \in Im(R_G)$. Alors pour $s \in G$ par linéarité : $\rho_d(s)(y) = \frac{1}{|G|} \sum_{g \in G} \rho_d(s)\rho_d(g)(x) = \frac{1}{|G|} \sum_{g \in G} \rho_d(sg)(x) = R_G(x) = y$ car $s \mapsto sg$ est une bijection de G, donc $y \in V_d^G$. La réciproque est évidente : si $x \in V_d^G$ alors $R_G(x) = \frac{1}{|G|}|G|x = x$ donc $x \in Im(R_G)$. Ainsi R_G est d'image V_d^G, et le calcul précédent (l'image est constituée de points fixes sous l'action) montre que $R_G^2 = R_G$. Ainsi en écrivant la matrice du projecteur 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 $Tr(R_G) = \frac{1}{|G|} \sum_{A \in G} \chi_d(A)$ ce qui conclut. □

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

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

Démonstration. Comme G est fini, par le théorème de Lagrange, $X^{|G|} - 1$ 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 racines de l'unité, donc de module 1. Soit $A \in G$ de valeurs propres $\lambda_1, \cdots, \lambda_n$. On a

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

où la dernière égalité est obtenue par produit de Cauchy des séries, argument assurant aussi que le rayon de convergence est au moins 1 (le rayon de convergence de chacune des séries étant 1 car les λ_i sont de module 1).

D'autre part soit un élément de la base canonique de V_d, $P = X_1^{k_1} \cdots X_n^{k_n}$ avec $k_1 + \cdots + k_n = d$, en supposant A diagonale pour simplifier les calculs [1] (avec les valeurs propres dans l'ordre de leur numérotation) on a $\rho_d(A^{-1})(X_1^{k_1} \cdots X_n^{k_n}) = \rho(A^{-1})(X_1)^{k_1} \cdots \rho(A^{-1})(X_n)^{k_n} = (\lambda_1 X_1)^{k_1} \cdots (\lambda_n X_n)^{k_n} = \lambda_1^{k_1} \cdots \lambda_n^{k_n} P$ et donc $\chi_d(A^{-1}) = Tr(\rho_d(A^{-1})) = \sum_{k_1 + \cdots + k_n = d} \lambda_1^{k_1} \cdots \lambda_n^{k_n}$ ce qui conclut sur l'égalité des séries.

□

1. Sinon soit $(v_1, \cdots, v_n)$ une base de $\mathbb{C}^n$ qui diagonalise A, et notons $v_i = \sum_{j=1}^n \mu_{ij} e_j$ c.à.d μ_{ij} est le terme général de la matrice P^{-1} inverse de la matrice de passage de la base canonique à v ($A = PDP^{-1}$), et posons $V_i = \sum_{j=1}^n \mu_{ij} X_j$. Alors $A \cdot V_i = \sum_{j=1}^n \mu_{ij} A \cdot X_j = \sum_{j=1}^n \sum_{t=1}^n \mu_{ij} a_{jt} X_t = \sum_{t=1}^n (\sum_{j=1}^n \mu_{ij} a_{jt}) X_t = \sum_{t=1}^n (P^{-1}A)_{it} X_t = \sum_{t=1}^n (DP^{-1})_{it} X_t = \sum_{t=1}^n \lambda_i \mu_{it} X_t = \lambda_i V_i$. On montre aisément que $(V_1^{k_1} \cdots V_n^{k_n})_{k_1 + \cdots + k_n = d}$ est une base de V_d, et la compatibilité de l'action avec le produit permet le même calcul du caractère que dans le cas diagonal traité juste après, en remplaçant X par V.

Pour conclure il suffit d'écrire

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

où l'on a interverti les sommes car l'une était finie, et où on a appliqué les deux lemmes (en disant bien que l'inversion est une bijection de G, pour appliquer la 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.

$\square$