Théorème de Molien

Références : Leichtnam, *exercices corrigés de Mathématiques posés à l'oral des concours de Polytechnique et des ENS - Tome algèbre et géométrie*, p 95

Théorème.

On note $A = \mathbb{C}[X_1, ..., X_n]$ et A_k l'espace des polynômes homogènes de A de degré k. On se donne G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$.

Pour $g \in G$, on pose $\sigma_g : \begin{array}{ccc} A & \to & A \\ P(X) & \mapsto & P({}^{\mathrm{t}}gX) \end{array}$ (où on considère X comme un vecteur colonne), alors $\forall k \in \mathbb{N}$, σ_g induit un automorphisme de A_k et si on note $A_k^G := \{P \in A_k, \forall g \in G, \sigma_g(P) = P\}$, $a_k = \dim(A_k)$ et $a_k(G) = \dim(A_k^G)$, alors on a l'égalité suivante dans $\mathbb{C}[[Z]]$:

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - Zg)} = \sum_{k=0}^{\infty} a_k(G) Z^k.$$

Démonstration. • Montrons que σ_g induit un automorphisme sur chaque A_k.
Il est déjà clair que σ_g est un morphisme d'algèbre.[1] Puis on remarque que $\sigma_{gg'} = \sigma_g \circ \sigma_{g'}$ et $\sigma_e = Id$. On a ainsi $(\sigma_g)^{-1} = \sigma_{g^{-1}}$ et $\sigma_g \in \mathrm{Aut}(A)$.
Enfin σ_g envoie un monôme de degré k sur un polynôme homogène de degré k, donc $\sigma_g(A_k) \subset A_k$. On peut donc construire la restriction de σ_g à A_k. Or σ_g est injectif (sur A donc sur A_k), par égalité des dimensions, σ_g induit un automorphisme sur chaque A_k.
En fait, on a montré que $\sigma : \begin{array}{ccc} G & \to & GL(A) \\ g & \mapsto & \sigma_g \end{array}$ définit une représentation de G et que l'on peut définir les représentations induites $\sigma_{|A_k}$ sur les A_k[2].

• Montrons à présent que $\dfrac{1}{\det(I_n - Zg)} = \displaystyle\sum_{k=0}^{\infty} \chi_k(g) Z^k$ où $\chi_k(g) = \mathrm{Tr}(\sigma_{|A_k}(g))$ est le caractère de $\sigma_{|A_k}$ en g.
Le groupe G est fini, donc par le théorème de Lagrange, $\forall g \in G$, $g^{|G|} = e$. Il en résulte que le polynôme $X^{|G|} - 1$ annule toutes les matrices de G, mais il est scindé à racines simples, donc pour $g \in G$, il existe $u \in \mathrm{GL}_n(\mathbb{C})$ telle que ugu^{-1} soit diagonale. On a $\chi_k(g) = \mathrm{Tr}(\sigma_{|A_k}(g)) = \mathrm{Tr}(\sigma_{|A_k}(u)\sigma_{|A_k}(g)\sigma_{|A_k}(u^{-1})) = \chi_k(ugu^{-1})$.[3] En fait, on peut juste dire que les caractères sont des fonctions centrales, ce qui évite d'écrire ces formules.
On peut donc supposer g diagonale : $g = \mathrm{Diag}(\lambda_1, ..., \lambda_n)$. Alors

$$\frac{1}{\det(I_n - Zg)} = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i Z} = \prod_{i=1}^{n} \sum_{p=0}^{\infty} \lambda_i^p Z^p = \sum_{p=0}^{\infty} v_p Z^p$$

avec $v_p = \displaystyle\sum_{k_1 + ... + k_n = p} \lambda_1^{k_1} ... \lambda_n^{k_n}$.

Puis on remarque que pour $k_1 + ... + k_n = p$, on a $\sigma_{|A_p}(g)(X_1^{k_1} ... X_n^{k_n}) = (\lambda_1^{k_1} ... \lambda_n^{k_n}) X_1^{k_1} ... X_n^{k_n}$, donc si on prend la base de A_k constituée des $X_1^{k_1} ... X_n^{k_n}$ avec $k_1 + ... + k_n = p$, alors on voit que $\chi_p(g) = \mathrm{Tr}(\sigma_{|A_p}(g)) = v_p$.

La formule précédente donne donc $\dfrac{1}{\det(I_n - Zg)} = \displaystyle\sum_{k=0}^{\infty} \chi_k(g) Z^k$.

• Pour conclure, on utilise le lemme suivant.

1. Attention, $\sigma_h(P({}^{\mathrm{t}}gX)) = P({}^{\mathrm{t}}g{}^{\mathrm{t}}hX)$. C'est l'indéterminée X qui est multipliée par ${}^{\mathrm{t}}h$!
2. C'est en fait une action de groupe.
3. On peut faire cela en étendant l'ensemble de définition de σ à $\mathrm{GL}_n(\mathbb{C})$. On vérifie que les identités faites auparavant sont toujours vérifiées.

Lemme.

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation d'un groupe G fini avec V un $\mathbb{C}$-espace vectoriel de dimension finie, alors
$$\dim(V^G) = \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

Si on applique ce lemme à $\sigma_{[A_k}$, on a $\dim(A_k^G) = a_k(G) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi_k(g)$.

On a donc
$$\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I_n - Zg)} = \frac{1}{|G|}\sum_{g\in G}\sum_{k=0}^{\infty}\chi_k(g)Z^k = \sum_{k=0}^{\infty}\frac{1}{|G|}\sum_{g\in G}\chi_k(g)Z^k = \sum_{k=0}^{\infty}a_k(G)Z^k.$$

□

Prouvons à présent le lemme.

Démonstration. On pose $p_G = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\rho(g) \in \mathrm{GL}(V)$ l'opérateur de Reynolds.[4] Alors en utilisant la bijection $h \mapsto gh$, on a $\rho(h)p_G(v) = p_G(v)$, donc $p_G(V) \subset V^G$. Comme $p_G(v) = v$ pour $v \in V^G$, on a $p_G(V) = V^G$. De plus, en sommant, on a $p_G \circ p_G = p_G$, donc p_G est un projecteur sur V^G. En trouvant une bonne base pour le projecteur, on a vite $\mathrm{rg}(p_G) = \mathrm{Tr}(p_G) = \dim(V^G)$, donc, en appliquant l'application trace à p_G, on a $\dim(V^G) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi(g)$. □

Remarques : • Le théorème de Molien donne le lien entre un objet simple : le déterminant, et les $a_k(G)$ qui sont les dimensions des sous-espaces d'invariants.
• La série des invariants est nommée série de Molien.
• On a l'impression qu'il serait plus naturel de poser $\sigma_g(P)(X) = P(gX)$ mais ça n'est pas le cas ! Par exemple, prenons le 3-cycle (123). Sa matrice de permutation associée est
$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Si on se place dans $\mathbb{C}[X_1, X_2, X_3]$, on a
$$P(AX) = \begin{pmatrix} X_3 \\ X_1 \\ X_2 \end{pmatrix} \text{ et } P({}^{\mathrm{t}}AX) = \begin{pmatrix} X_2 \\ X_3 \\ X_1 \end{pmatrix}.$$

La deuxième approche donne la permutation intuitive.
• Faisons un exemple avec $\mathcal{S}_3$:
On considère l'action classique de $\mathcal{S}_3$ sur $\mathbb{R}^3$ pour obtenir un sous-groupe fini de matrices dans $\mathrm{GL}_3(\mathbb{C})$.
Alors $\det(I_3 - Z\sigma_e) = (1-Z)^3$, $\det(I_3 - Z\sigma_{(12)}) = \det\begin{pmatrix} 1 & -Z & 0 \\ -Z & 1 & 0 \\ 0 & 0 & 1-Z \end{pmatrix} = (1-Z)(1-Z^2)$ et enfin $\det(I_3 - Z\sigma_{(123)}) = \det\begin{pmatrix} -Z & 0 & 1 \\ 1 & -Z & 0 \\ 0 & 1 & -Z \end{pmatrix} = (1-Z^3)$. Comme le déterminant est invariant sur les classes de conjugaison, on a :
$$\sum_{k=0}^{\infty}a_k(\mathcal{S}_3)Z^k = \frac{1}{6}\left(\frac{1}{(1-Z)^3} + \frac{3}{(1-Z)(1-Z^2)} + \frac{2}{1-Z^3}\right) = \frac{1}{(1-Z)(1-Z^2)(1-Z^3)}.$$

4. Ouioui, c'est le même qu'en mécanique des fluides ! Mais au lieu de moyenner un flot sur l'action d'un groupe de translations en temps, on moyennise une représentation sur son groupe associé.

En fait, on peut étendre ce résultat à $\mathcal{S}_n$ avec $\displaystyle\sum_{k=0}^{\infty} a_k(\mathcal{S}_n)Z^k = \frac{1}{(1-Z)...(1-Z^n)}$.

• Pour $\mathcal{A}_3$, on a

$$\sum_{k=0}^{\infty} a_k(\mathcal{A}_3)Z^k = \frac{1}{3}\left(\frac{1}{(1-Z)^3} + \frac{2}{1-Z^3}\right) = \frac{1+Z^3}{(1-Z)(1-Z^2)(1-Z^3)}.$$

On peut aussi étendre ce résultat à $\mathcal{S}_n$ avec $\displaystyle\sum_{k=0}^{\infty} a_k(\mathcal{A}_n)Z^k = \frac{1+Z^{\frac{n(n-1)}{2}}}{(1-Z)...(1-Z^n)}$.

• On peut montrer que si A^G est engendré par des polynômes homogènes f_1,...,f_r de degrés d_1,...,d_r, alors la série de Molien de G est le développement en série formelle d'une fraction rationnelle de la forme

$$\frac{F(Z)}{(1-Z^{d_1})...(1-Z^{d_r})}, \text{ avec } F \in \mathbb{Z}[Z].$$

Le théorème de Molien permet d'avoir une idée de où chercher les invariants.

• On rappelle que le fait que A^G soit engendré par des polynômes homogènes f_1,...,f_r veut juste dire que pour tout $P \in A$, il existe $Q \in \mathbb{C}[Y_1, ..., Y_r]$ tel que

$$P(X_1, ..., X_n) = Q(f_1(X_1, ..., X_n), ..., f_r((X_1, ..., X_n)).$$

A^G est engendrée en tant qu'**algèbre**.

• Pour l'exemple de $\mathcal{S}_n$, les invariants de A sont les polynômes symétriques et ils sont engendrés par les polynômes symétriques élémentaires $\Sigma_i = \displaystyle\sum_{1\leqslant k_1<...<k_i\leqslant n} X_1^{k_1}...X_n^{k_n}$. On a bien $\deg(\Sigma_i) = i$, ce qui confirme les résultats précédents.

• Pour $\mathcal{A}_n$, on peut montrer que les polynômes invariants sous son action sont engendrés par les polynômes symétriques élémentaires et le polynôme de Vandermonde (de degré n). Il faut un peu modifier la fraction rationnelle précédente pour le faire apparaître en multipliant par $(1-Z^n)$ au numérateur et au dénominateur. C'est à dire

$$\sum_{k=0}^{\infty} a_k(\mathcal{A}_n)Z^k = \frac{(1+Z^{\frac{n(n-1)}{2}})(1-Z^n)}{(1-Z)...(1-Z^{n-1})(1-Z^n)^2}.$$