Théorème de Molien

Laura GAY ♡ Camille FRANCINI

Référence : LEICHTNAM : Exercices corrigés de mathématiques posés à l'oral des concours Polytechnique et des ENS Tome Algèbre et Géométrie p. 95 (ou PEYRÉ : L'algèbre discrète de la transformée de Fourier : Niveau M1)

Définition

On note A_k l'espace des polynômes homogènes à n variables de degré k. On note $a_k = \dim A_k$.

Définition

Soit G un groupe fini de $\mathcal{GL}_n(\mathbb{C})$. Soit W un $\mathbb{C}$-espace vectoriel de dimension finie et $(e_1, ..., e_n)$ une base de W.
Alors $\mathcal{GL}_n(\mathbb{C}) \simeq \mathcal{GL}(W)$.
On définit une action de G sur les A_k par :

$$\begin{array}{ccc} G \times A_k & \to & A_k \\ (g, P) & \mapsto & \sigma_g(P) \end{array}$$

où, pour $g \in G$, on définit σ_g tel que si $g(e_h) = \displaystyle\sum_{1 \leq j \leq n} u_{j,h} e_j$, $P \in A$, on pose

$$\sigma_g(P)(X_1, .., X_n) = P\left(\sum_{1 \leq j \leq n} u_{j,1} X_j, ..., \sum_{1 \leq j \leq n} u_{j,n} X_j\right)$$

On a déjà $\sigma_I(P) = P$. On vérifiera plus tard les autres axiomes de la définition :
- $g.(g'.P) = g.\sigma_{g'}(P) = \sigma_g(\sigma_{g'}(P)) = \sigma_{gg'}(P) = (gg').P$
- $\sigma_g(A_k) \subset A_k$.

On note $a_k(G) = \dim A_k^G = \dim\{P \in A_k \mid \forall g \in G, \sigma_g(P) = P\}$.

Théorème (*Théorème de Molien - 1897 ?*)

Sous les conditions de la définition ci-dessus, on a :

$$\sum_{k \geq 0} a_k(G) X^k = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gX)}$$

Lemme 1

Pour $|z| < 1$, $\dfrac{1}{(1-z)^n} = \displaystyle\sum_{k=0}^{+\infty} a_k z^k$

Preuve du Lemme 1

A_k admet pour base $\{X_1^{i_1} ... X_n^{i_n} / i_1, .. i_n \in \mathbb{N} \text{ et } i_1 + ... + i_n = k\}$. Ainsi

$$a_k = \dim A_k = \mathrm{card}\{(i_1, ..., i_n) \in \mathbb{N}^n / i_1 + ... + i_n = k\}$$

D'une part, pour $|z| < 1$ on a : $\left(\displaystyle\sum_{p=0}^{+\infty} z^p\right)^n = (\dfrac{1}{1-z})^n$.

D'autre part, le produit de Cauchy de ces n séries entières donne :

$$\left(\sum_{p=0}^{+\infty} z^p\right)^n = \sum_{k=0}^{+\infty} \left(\sum_{i_1 + ... + i_n = k} 1\right) z^k$$

Donc a_k est le coefficient de z^k dans le développement de $(\frac{1}{1-z})^n$. Donc :

$$\underline{\sum_{k\geq 0} a_k z^k = (\frac{1}{1-z})^n} \qquad \blacksquare$$

Lemme 2

Soit V un $\mathbb{C}$-espace vectoriel de dimension finie. Soit $\varphi : G \to \mathcal{GL}(V)$ un morphisme de groupe. On note $V^G = \{v \in V \mid \forall g \in G, \varphi(g)(v) = v\}$.
Alors :

$$\dim V^G = \frac{1}{|G|} \sum_{g\in G} \operatorname{tr}(\varphi(g))$$

Preuve du Lemme 2

On pose pour cela : $p_G = \frac{1}{|G|} \sum_{g\in G} \varphi(g)$
Alors, on remarque que $\forall v \in V, \forall h \in G$ on a :

$$\varphi(h)(p_G(v)) = \frac{1}{|G|} \sum_{g\in G} \varphi(h)\varphi(g)(v)$$

Mais $g \mapsto hg$ est une permutation de G et $\varphi(h)\varphi(g) = \varphi(hg)$
Nous avons donc que $\varphi(h)(p_G(v)) = p_G(v)$ donc $p_G(V) \subset V^G$.
De plus, pour tout $v \in V^G$, on a : $p_G(v) = v$, donc $p_G(V) = V^G$.
Comme $\varphi(h)p_G = p_G$ pour tout $h \in G$ on a $p_G \circ p_G = p_G$.
Ainsi p_G est un projecteur d'image V^G et donc :

$$\underline{\operatorname{rg}(p_G) = \dim V^G = \operatorname{tr}(p_G) = \frac{1}{|G|} \sum_{g\in G} \operatorname{tr}(\varphi(g))} \qquad \blacksquare$$

Preuve du théorème

Étapes :
1) Création d'un automorphisme g_k de A_k

2) A partir du **Lemme 1**, on montre que pour $|z| < 1$, $\frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} \operatorname{tr}(g_k) z^k$

3) On conclut alors sur l'égalité avec le **Lemme 2**.

Étape 1 :
Soit $\sigma : \begin{array}{ccc} \mathcal{GL}(W) & \to & \text{Aut } A \\ g & \mapsto & \sigma_g \end{array}$ (ie $\sigma_g = \sigma(g)$). Vérifions déjà que l'application σ est bien définie (et donc que l'on avait bien une action). Déjà :

$$\begin{aligned} \sigma_g \circ \sigma_{g'}(P) &= \sigma_g(\sigma_{g'}(P)) \\ &= \sigma_{g'}(P) \left(\sum_{1\leq j\leq n} u_{j,1} X_j, ..., \sum_{1\leq j\leq n} u_{j,n} X_j \right) \\ &= \sigma_{gg'}(P) \end{aligned}$$

De plus on a $\sigma_I = I$ donc $\forall g \in G$, $(\sigma_g)^{-1} = \sigma_{g^{-1}}$. Comme de plus σ_g est linéaire, σ_g est bien dans $\operatorname{Aut}(A)$.
De plus $\forall k \in \mathbb{N}$, $\forall g \in G$, on a $\sigma_g(A_k) \subset A_k$. Or A_k est de dimension finie et σ_g est injective.
σ_g est surjective par $(\sigma_g)^{-1} = \sigma_{g^{-1}}$.
Donc σ_g induit un isomorphisme *(sert à dire qu'on est bien dans $\mathcal{GL}$)* de A_k que l'on appelle g_k $(= \sigma(g)_{|A_k})$.

Étape 2 :

On sait que $0 \leq a_k(G) \leq a_k$, donc (d'après le **Lemme 1**) la série $\sum_0^{+\infty} a_k(G) z^k$ converge pour $|z| < 1$.

De plus, d'après le théorème de Lagrange $\forall g \in G$, $g^{|G|} = I$. Or le polynôme $X^{|G|} - 1$ est scindé à racines simples sur $\mathbb{C}$. Ainsi, g est diagonalisable, il existe donc $u \in \mathcal{GL}(W)$ tel que : ugu^{-1} admette une matrice diagonale dans la base $(e_1, .., e_n)$. Alors, comme : $\sigma(ugu^{-1})_{|A_k} = \sigma(u)_{|A_k} \sigma(g)_{|A_k} \sigma(u^{-1})_{|A_k}$, on a :

$$\mathrm{tr}(g_k) = \mathrm{tr}(\sigma(ugu^{-1})_{|A_k})$$

On peut ainsi se ramener au cas où $g \in G$ est une matrice diagonale dans la base $(e_1, .., e_n)$: $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

Les λ_i sont de module 1 (car $g^{|G|} = I$).
Ainsi pour $|z| < 1$ on a :

$$\frac{1}{\det(I - zg)} = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i z} = \prod_{i=1}^{n} \left(\sum_{p=0}^{+\infty} \lambda_i^p z^p \right) = \sum_{p=0}^{+\infty} v_p z^p$$

Avec $v_p = \sum_{\substack{k_1, \dots k_n \in \mathbb{N}, \\ k_1 + .. + k_n = p}} \lambda_1^{k_1} \dots \lambda_n^{k_n}$ (produit de Cauchy des séries)

Or $g_p(X_1^{k_1} \dots X_n^{k_n}) = \lambda_1^{k_1} \dots \lambda_n^{k_n} X_1^{k_1} .. X_n^{k_n}$.

Ainsi, comme $\{X_1^{i_1} \dots X_n^{i_n} / i_1, .. i_n \in \mathbb{N}$ et $i_1 + \dots + i_n = p\}$ est une base de A_p, $v_p = \mathrm{tr}(g_p)$ et donc $\underline{\frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} \mathrm{tr}(g_k) z^k}$

Étape 3 :

Pour tout $k \in \mathbb{N}$, $\varphi : \begin{array}{ccc} G & \to & \mathcal{GL}(A_k) \\ g & \mapsto & g_k \end{array}$ est un morphisme de groupe.
Ainsi, on peut appliquer le **Lemme 2**, et on a :

$$a_k(G) = \dim(A_k^G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(g_k)$$

Donc pour $|z| < 1$:

$$\underline{\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} a_k(G) z^k} \qquad \blacksquare$$

Bonus :

$$a_p = \binom{p}{p+n-1}$$

En effet on a $\sum_{p \geq 0} a_p z^p = \left(\frac{1}{1-z} \right)^n$ et $\left(\frac{1}{1-z} \right)^{(n-1)} = \frac{(n-1)!}{(1-z)^n} = \sum_{p=0}^{+\infty} (p+n-1)..(p+1) z^p$.
Ainsi en associant les deux on obtient :

$$a_p = \frac{(p+n-1) \dots (p+1)}{(n-1)!} = \binom{p}{p+n-1}$$

Notes :

✓ **A l'oral**, on ne fait pas les lemmes. Il faut introduire l'action dès le début. Dire les étapes à l'oral mais ne pas les écrire car sinon lemme + étapes = beaucoup avant de commencer vraiment.
✓ Il faut savoir justifier pourquoi V doit être de dimension finie (car sinon tr n'existe pas...)
✓ On peut faire toute la démo avec les séries formelles (qui n'imposent aucun domaine de convergence) : cela

simplifie.
✓ z ou X est un scalaire ! (du coup on se moque de l'ordre gX ou Xg).
✓ Le développement peut se réécrire avec le vocabulaire des représentations.
♣ Theodor Molien (1861 - 1941) est un mathématicien germano-balte. Il étudiait les algèbres commutatives et les polynômes invariants de groupes finis.