Théorème de Molien

Références : [Lei] ([Gou94], [Cal06] et [Ser98]).

Théorème 0.1 *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Soit G un sous-groupe fini de $GL(V)$. On fixe $(e_1, \ldots, e_n)$ une base de V. On note $A = \mathbb{C}[X_1, \ldots, X_n]$. À tout $g \in G$, on associe $\rho_g : A \longrightarrow A$ définie par : si pour $1 \leq h \leq n$, $g(e_h) = \sum_{j=1}^n u_{j,h} e_j$ alors on pose :*

$$\rho_g(P)(X_1, \ldots, X_n) = P\left(\sum_{j=1}^n u_{j,1} X_j, \ldots, \sum_{j=1}^n u_{j,n} X_j\right)$$

Pour tout $k \in \mathbb{N}$, on pose A_k l'espace des polynômes homogènes à n variables de A de degré k. On note $a_k = \dim A_k$ et $a_k(G) = \dim A_k^G$ où A_k^G est l'ensemble des $P \in A_k$ tels que $\rho_g(P) = P$. Alors :

1. *$\rho : G \longrightarrow Aut(A)$ est un morphisme de groupes (ie une représentation linéaire) et pour tout $k \in \mathbb{N}$, pour tout $g \in G$, ρ_g induit un automorphisme de A_k qu'on notera ρ_{g_k}.*
2. *$\forall z \in \mathbb{C}$ tels que $|z| < 1$, on a :*
$$\frac{1}{(1-z)^n} = \sum_{k=0}^{+\infty} a_k z^k$$
3. *$\forall g \in G$, $\forall z \in \mathbb{C}$ tels que $|z| < 1$, on a :*
$$\frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} trace(\rho_{g_k}) z^k$$

De plus, on en déduit que $\forall g \in G$, $\forall z \in \mathbb{C}$ tels que $|z| < 1$, on a :

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

Démonstration

Étape 1 : démontrons un lemme général sur les représentations.

Lemme 0.1 *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Soit G un groupe fini. Soit $\rho : G \longrightarrow GL(V)$ une représentation linéaire de G. On pose $V^G = \cap_{g \in G} \ker(\rho(g) - id)$. Alors :*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) = \frac{1}{|G|} \sum_{g \in G} trace \rho(g)$$

On pose :

$$p_G = \frac{1}{|G|} \sum_{g \in G} \rho(g)$$

c'est un endomorphisme de V.
$\rightsquigarrow$ Montrons que $p_G(V) = V^G$.
($\subset$) Soit $v \in V$, soit $h \in G$, on a :

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

car ρ est un morphisme de groupes par définition de représentation linéaire et car l'application $\psi : g \longmapsto hg$ est une bijection de G.
Donc $p_G(V) \subset V^G$.

($\supset$) Soit $v \in V^G$, on a :

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

par définition de V^G.
Donc $p_G(V) = V^G$.
$\rightsquigarrow$ Conclusion.
L'égalité $\rho(h)p_G = p_G$ pour tout $h \in G$, montre que $p_G \circ p_G = p_G$. Donc p_G est un projecteur d'image V^G. On a donc $V = \ker p_G \oplus V^G$ et par propriété des projecteurs, on sait que $rang(p_G) = \dim V^G = trace(p_G)$. Donc :

$$\dim V^G = \frac{1}{|G|}\sum_{g\in G} trace \rho(g)$$

par linéarité de la trace.

Étape 2 : démonstration du (1)**.**
On considère l'application :

$$\begin{aligned} \rho : G &\longrightarrow Aut(A) \\ g &\longmapsto \rho_g : P \longmapsto \rho_g(P) \end{aligned}$$

$\rightsquigarrow$ Montrons que ρ est un morphisme de groupes.
Soient $g, g' \in G$ tels que pour tout $1 \leq h \leq n$, on ait :

$$g(e_h) = \sum_{j=1}^{n} u_{j,h} e_j \quad \text{et} \quad g'(e_h) = \sum_{j=1}^{n} v_{j,h} e_j$$

Soit $P \in A$, on a :

$$\begin{aligned} \rho_g \circ \rho_{g'}(P)(X_1, \dots, X_n) &= \rho_g\left(\rho_{g'}(P)(X_1, \dots, X_n)\right) \\ &= \rho_g\left(P\left(\sum_{j=1}^{n} v_{j,1}X_j, \dots, \sum_{j=1}^{n} v_{j,n}X_j\right)\right) \\ &= \rho_g(P)\left(\tilde{X}_1, \dots, \tilde{X}_n\right) \\ &= P\left(\sum_{i=1}^{n} u_{i,1}\tilde{X}_i, \dots, \sum_{i=1}^{n} u_{i,n}\tilde{X}_i\right) \\ &= P\left(\sum_{i=1}^{n} u_{i,1}\sum_{j=1}^{n} v_{j,i}X_i, \dots, \sum_{i=1}^{n} u_{i,n}\sum_{j=1}^{n} v_{j,i}X_i\right) \end{aligned}$$

On remarque également que :

$$g \circ g'(e_h) = g\left(\sum_{j=1}^{n} v_{j,h}e_j\right) = \sum_{j=1}^{n} v_{j,h} g(e_j) = \sum_{j=1}^{n} v_{j,h}\sum_{i=1}^{n} u_{i,j}e_i$$

Donc pour tout $P \in A$:

$$\rho_{g\circ g'}(P)(X_1, \dots, X_n) = P\left(\sum_{j=1}^{n} v_{j,1}\sum_{i=1}^{n} u_{i,j}X_i, \dots, \sum_{j=1}^{n} v_{j,n}\sum_{i=1}^{n} u_{i,j}X_i\right)$$

D'où ρ morphisme de groupes.
$\rightsquigarrow$ Montrons que ρ est à valeurs dans $Aut(A)$.
On a $\rho_{id} = id$ donc pour tout $g \in G$, $(\rho_g)^{-1} = \rho_{g^{-1}}$ et $\rho_{g^{-1}} \in Aut(A)$.
$\rightsquigarrow$ Montrons que ρ_g induit un automorphisme de A_k.
Pour tout $k \in \mathbb{N}$, pour tout $g \in G$, on a $\rho_g(A_k) \subset A_k$ par définition de ρ_g et comme A_k est de dimension finie et ρ_g injective (car ρ_g est un automorphisme), alors ρ_g induit un isomorphisme sur A_k.

Étape 3 : démonstration du (2).
A_k admet pour base $\{X_1^{i_1}, \ldots, X_n^{i_n}; i_1, \ldots, i_n \in \mathbb{N} \quad \text{et} \quad i_1 + \ldots + i_n = k\}$. On a donc :

$$a_k = \dim A_k = \text{card}\{(i_1, \ldots, i_n) \in \mathbb{R}^n; i_1 + \ldots + i_n = k\}$$

Pour $z \in \mathbb{C}$ tel que $|z| < 1$, on a :

$$\left(\sum_{k=0}^{+\infty} z^k\right)^n = \left(\frac{1}{1-z}\right)^n = \frac{1}{(1-z)^n}$$

car on reconnaît la série géométrique qui est de rayon de convergence 1.
Le produit de ces n séries entières montre que a_k est le coefficient de z^k dans le développement de $\dfrac{1}{(1-z)^n}$, donc pour $z \in \mathbb{C}$ tel que $|z| < 1$, on a :

$$\sum_{k=0}^{+\infty} a_k z^k = \frac{1}{(1-z)^n}$$

Étape 4 : démonstration du (3).
On a $A_k^G = \{P \in A_k, \forall g \in G, \rho_g(P) = P\} \subset A_k$ et $a_k(G) = \dim A_k^G$.
Comme $0 \leq a_k(G) \leq a_k$ alors la série $\sum_k a_k(G) z^k$ converge pour $z \in \mathbb{C}$ tel que $|z| < 1$ par comparaison.
D'après le théorème de Lagrange, on sait que $g^{|G|} = id$ donc le polynôme $X^{|G|} - 1$ est un polynôme annulateur de g qui est scindé à racines simples, donc g est diagonalisable, il va donc exister $u \in \mathcal{L}(V)$ tel que ugu^{-1} soit une matrice diagonale, notons-la d dans la base $(e_1, \ldots, e_n)$. On a alors :

$$\rho_{|A_k}(ugu^{-1}) = \rho_{|A_k}(u)\rho_{|A_k}(g)\rho_{|A_k}(u^{-1}) = \rho_{|A_k}(g)$$

car $\rho_{|A_k} = \rho_{g_k}$ est un automorphisme d'après le (1) (en notant $\rho_{|A_k}(u) = \rho_u$ restreinte à A_k).
D'où :

$$trace(\rho_{|A_k}(g)) = trace(\rho_{g_k}(g)) = trace(\rho_{g_k}(d))$$

De plus comme $g^{|G|} = id$ alors $d^{|G|} = (ugu^{-1})^{|G|} = u^{|G|}g^{|G|}(u^{-1})^{|G|} = id$ donc les valeurs propres vérifient $\lambda_i^{|G|} = 1$, ie qu'elles sont de module 1, donc pour tout $z \in \mathbb{C}$ tel que $|z| < 1$, on a :

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

où :

$$v_p = \sum_{k_1, \ldots, k_n \in \mathbb{N}; k_1 + \ldots + k_n = p} \lambda_1^{k_1} \ldots \lambda_n^{k_n}$$

On a également $\rho_{g_p}(X_1^{k_1}, \ldots, X_n^{k_n}) = (\lambda_1^{k_1} \ldots \lambda_n^{k_n}) X_1^{k_1} \ldots X_n^{k_n}$, on en déduit alors que $v_p = trace(\rho_{g_p})$ (si on la calcule dans la base de A_k mentionnée ci-dessus) donc :

$$\frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} trace(\rho_{g_k}) z^k$$

Étape 5 : conclusion.
Posons pour tout $k \in \mathbb{N}$:

$$\begin{aligned} \phi : G &\longrightarrow GL(A_k) \\ g &\longmapsto \rho_{g_k} \end{aligned}$$

c'est une représentation linéaire et le lemme nous donne :

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

Donc pour tout $z \in \mathbb{C}$ tel que $|z| < 1$, on a :

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

Trucs utilisés
Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Soit G un sous-groupe fini de $GL(V)$. On fixe $(e_1, \ldots, e_n)$ une base de V.

Définition 0.1 (Projecteur) *Un endomorphisme $p \in \mathcal{L}(V)$ est appelé un projecteur si $p \circ p = p$.*

Proposition 0.2 *Soit $p \in \mathcal{L}(V)$. p est un projecteur si et seulement si p est la projection sur $Im(p)$ parallèlement à $\ker(p)$. On a alors $V = Im(p) \oplus \ker(p)$.*

Proposition 0.3 *Soit V un $\mathbb{K}$-espace vectoriel de dimension finie n. Soit $p \in \mathcal{L}(V)$. Alors $trace(p) = rang(p)1_{\mathbb{K}}$.*

Démonstration Comme p est un projecteur, on a $V = Im(p) \oplus \ker(p)$. Soit $r = rang(p)$. Soit $(e_, \ldots, e_r)$ une base de $Im(p)$ et $(e_{r+1}, \ldots, e_n)$ une base de $\ker(p)$, alors $(e_1, \ldots, e_n)$ est une base de V et la matrice de p dans cette base s'écrit :

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

Donc $trace(p) = rang(p)1_{\mathbb{K}}$.

Définition 0.2 (Degré d'un polynôme) *On appelle degré total d'un monôme non nul de $A[X_1, \ldots, X_n]$, la somme de ses degrés partiels en $X_1, \ldots, X_n$, ie le degré total de $\alpha X_1^{i_1} \ldots X_n^{i_n}$ est $i_1 + \ldots + i_n$.*
On appelle degré total d'un polynôme non nul de $A[X_1, \ldots, X_n]$, le maximum des degrés totaux des monômes dont il est la somme.

Définition 0.3 (Polynôme homogène) *Un polynôme f non nul dans $A[X_1, \ldots, X_n]$ est dit homogène de degré d s'il est somme de monômes de même degré total $d \geq 0$.*

Définition 0.4 (Représentation linéaire) *Une représentation linéaire de G dans V est un morphisme $\rho : G \longrightarrow GL(V)$, ie pour tout $s \in G$, $\rho(s) \in GL(V)$ et pour tous $s, t \in G$, $\rho(st) = \rho(s) \circ \rho(t)$.*

Définition 0.5 (Trace) *Soit $a \in \mathcal{L}(V)$ de matrice $(a_{i,j})_{1 \leq i,j \leq n}$. On appelle trace de a le scalaire :*

$$trace(a) = \sum_{i=1}^{n} a_{ii}$$

Remarque : La somme des valeurs propres de a (comptées avec leurs multiplicités) ne dépend pas de la base choisie (e_i).

Définition 0.6 (Caractère) *Soit $\rho : G \longrightarrow GL(V)$ une représentation linéaire du groupe G dans V. Pour tout $s \in G$, on pose :*

$$\chi_\rho(s) = trace(\rho(s))$$

On appelle $\chi_\rho : G \longrightarrow \mathbb{C}$ le caractère de la représentation linéaire ρ.

Références

[Cal06] Josette Calais. *Eléments de la théorie des anneaux.* Ellipses, 2006.

[Gou94] Xavier Gourdon. *Algèbre.* Ellipses, 1994.

[Lei] Eric Leichtnam. *Exercices corrigés de mathématiques.* Ellipses.

[Ser98] Jean-Pierre Serre. *Représentations linéaires des groupes finis.* Hermann, 1998.