Sandrine CARUSO

Théorème de Molien

Référence : Exercices corrigés posés aux oraux de Polytechnique et des ENS, solutions proposées par Leichtnam, tome algèbre et géométrie p 95

Soit n un entier et soit G un sous-groupe fini de $\mathrm{GL}(\mathbb{C}^n)$. On note $A = \mathbb{C}[X_1, \dots, X_n]$. Soit

$$\begin{array}{rcrcl} \sigma & : & G & \to & \mathfrak{S}(A) \\ & & g & \mapsto & (P \mapsto P(g^*(X_1, \dots, X_n))) \end{array}$$

où l'on a abusivement identifié g^*, l'adjoint de g, avec le n-uplet de polynômes de degré 1 de A dont les composantes de g^* sont les fonctions polynomiales associées. Enfin, on note A_k le sous-espace vectoriel de A formé des polynômes homogènes de degré k, et

$$A_k^G = \{P \in A_k, \forall g \in G, \sigma(g)(P) = P\}.$$

Lemme 1. *L'application σ est une action de G sur A, à valeurs dans* $\mathrm{GL}(A)$. *De plus, pour tout $g \in G$, le sous espace vectoriel A_k est stable par $\sigma(g)$.*

Pour tout g, on notera $\sigma_k(g)$ l'application induite par $\sigma(g)$ sur A_k.

Démonstration. Montrons que σ est un morphisme de groupes. Soient $g, h \in G$. Pour tout $P \in A$, on a $\sigma(g \circ h)(P) = P((g \circ h)^*(X_1, \dots, X_n)) = P(h^* \circ g^*(X_1, \dots, X_n) = \sigma(g)(P(h^*(X_1, \dots, X_n)) = \sigma(g) \circ \sigma(h)(P)$, et donc σ est bien un morphisme de groupes.

Prouvons maintenant qu'il est à valeurs dans $\mathrm{GL}(A)$. Soient $g \in G$, $P, Q \in A$ et $\lambda \in \mathbb{C}$. Alors $\sigma(g)(\lambda P + Q) = (\lambda P + Q)(g(X_1, \dots, X_n)) = \lambda\sigma(g)(P) + \sigma(g)(Q)$, et ainsi, $\sigma(g)$ est linéaire.

Enfin, soient $g \in G$ et $P \in A_k$, et montrons que $\sigma(g)(P) \in A_k$. Comme g^* est inversible, ses composantes sont des fonctions polynomiales homogènes (de degré 1), et donc la composée $P \circ g^* = \sigma(g)(P)$ reste homogène, de degré $k \times 1 = k$. $\square$

Ainsi, A_k^G est l'espace vectoriels des invariants de A_k sous l'action de G. On note $a_k(G)$ sa dimension.

Théorème 2 (Molien). *La série génératrice des $a_k(G)$ s'exprime de la manière suivante :*

$$\sum_{k=0}^{\infty} a_k(G) X^k = \frac{1}{\# G} \sum_{g \in G} \frac{1}{\det(id_E - Xg)}.$$

Pour établir ce résultat, on montre d'abord le lemme suivant :

Lemme 3. *Soient V un espace vectoriel de dimension finie, G un groupe fini, et φ un morphisme de groupes de G dans $\mathrm{GL}(V)$. On note*

$$V^G = \{x \in V, \forall g \in G, \varphi(g)(x) = x\} = \bigcap_{g \in G} \ker(id - \varphi(g)).$$

Alors

$$\dim V^G = \frac{1}{\# G} \sum_{g \in G} \operatorname{Tr} \varphi(g).$$

Démonstration. Considérons l'application linéaire $p_G = \frac{1}{\# G} \sum_{g \in G} \varphi(g)$. Montrons que $p_G(V) = V^G$.

Soit $x \in V^G$. Alors pour tout g, $\varphi(g)(x) = x$. Donc

$$p_G(x) = \frac{1}{\# G} \sum_{g \in G} \varphi(g)(x) = \frac{1}{\# G} \sum_{g \in G} x = x.$$

Ainsi, $x \in p_G(V)$ et même, x est un de ses propres antécédents par p_G.

Soit $x \in p_G(V)$. Il existe y tel que $x = p_G(y)$. Soit $g \in G$;

$$\varphi(g)(x) = \varphi(g)(p_G(y)) = \frac{1}{\# G} \sum_{h \in G} \varphi(g) \circ \varphi(h)(y) = \frac{1}{\# G} \sum_{h \in G} \varphi(gh)(y),$$

et comme l'application $h \mapsto gh$ est une bijection de G, on a encore

$$\varphi(g)(x) = \frac{1}{\# G} \sum_{h \in G} \varphi(h)(y) = p_G(y) = x.$$

Donc $x \in V^G$.

On a bien $p_G(V) = V^G$.

Montrons à présent que p_G est un projecteur. Soit $x \in V$. Alors $p_G(x) \in V^G$ d'après ce qui précède. Or, on a vu que tout élément de V^G était un de ses antécédents par p_G, donc $p_G \circ p_G(x) = p_G(x)$. Par conséquent, le rang de p_G est également égal à sa trace. Ainsi,

$$\dim V^G = \operatorname{rg} p_G = \operatorname{Tr} p_G = \frac{1}{\# G} \sum_{g \in G} \operatorname{Tr} \varphi(g),$$

ce que l'on voulait. □

Démonstration du théorème 2. Remarquons tout d'abord que tout élément de G est diagonalisable. En effet, les éléments de G sont tous annulés par le polynôme $X^{\# G} - 1$ qui est scindé à racines simples. Soit $g \in G$, et notons $\lambda_1, \ldots, \lambda_n$ ses valeurs propres, et u

l'endomorphisme envoyant une base de vecteurs propres associés sur la base canonique. Alors $\det(id - Xg) = \prod_{i=1}^n (1 - X\lambda_i)$. Ainsi,

$$\frac{1}{\det(id - Xg)} = \prod_{i=1}^n \sum_{k=0}^\infty \lambda_i^k X^k.$$

En développant le produit, on obtient

$$\frac{1}{\det(id - Xg)} = \sum_{k=0}^\infty \left(\sum_{k_1+\cdots+k_n=k} \lambda_1^{k_1} \cdots \lambda_n^{k_n} \right) X^k.$$

Fixons $k \in \mathbb{N}$. Soit $P = X_1^{k_1} \cdots X_n^{k_n}$ avec $k_1 + \cdots + k_n = k$ un monôme de A_k. Par définition de u, on a $\sigma_k(ugu^{-1})(P) = \lambda_1^{k_1} X_1^{k_1} \cdots \lambda_n^{k_n} X_n^{k_n} = \lambda_1^{k_1} \cdots \lambda_n^{k_n} P$. Ainsi, P est un vecteur propre de $\sigma_k(ugu^{-1})$ de valeur propre $\lambda_1^{k_1} \cdots \lambda_n^{k_n}$. Or, les monômes de la forme $X_1^{k_1} \cdots X_n^{k_n}$ avec $k_1 + \cdots + k_n = k$ formant une base de A_k, les $\lambda_1^{k_1} \cdots \lambda_n^{k_n}$ sont exactement les valeurs propres de $\sigma_k(ugu^{-1})$. En particulier,

$$\begin{aligned}\sum_{k_1+\cdots+k_n=k} \lambda_1^{k_1} \cdots \lambda_n^{k_n} &= \mathrm{Tr}(\sigma_k(ugu^{-1})) = \mathrm{Tr}(\sigma_k(u)\sigma_k(g)\sigma_k(u)^{-1}) \\ &= \mathrm{Tr}(\sigma_k(u)^{-1}\sigma_k(u)\sigma_k(g)) = \mathrm{Tr}(\sigma_k(g))\end{aligned}$$

et donc

$$\frac{1}{\det(id - Xg)} = \sum_{k=0}^\infty \mathrm{Tr}(\sigma_k(g)) X^k.$$

Maintenant, appliquons le lemme 3 avec $V = A_k$ et $\phi = \sigma_k$. On obtient

$$\dim A_k^G = a_k(G) = \frac{1}{\# G} \sum_{g \in G} \mathrm{Tr}(\sigma_k(g))$$

et par conséquent

$$\begin{aligned}\sum_{k=0}^\infty a_k(G) X^k &= \sum_{k=0}^\infty \frac{1}{\# G} \sum_{g \in G} \mathrm{Tr}(\sigma_k(g)) X^k \\ &= \frac{1}{\# G} \sum_{g \in G} \sum_{k=0}^\infty \mathrm{Tr}(\sigma_k(g)) X^k \\ &= \frac{1}{\# G} \sum_{g \in G} \frac{1}{\det(id - Xg)}\end{aligned}$$

ce que l'on voulait. $\square$