Théorème de Molien.

Année 2014-2015

Arnaud STOCKER

ENS Rennes

Université de Rennes 1

Table des matières

1 Théorème de Molien

Théorème 1

Soit $u \in GL_n(\mathbb{C})$. Pour $P \in A = \mathbb{C}[X_1, ..., X_n]$ on pose $\sigma(u)(P) = P(u^{-1}(X_1, ..., X_n)^t)$. Alors :

1. *L'application $\sigma : GL_n(\mathbb{C}) \to \mathrm{Aut}(A)$ est bien définie et est un morphisme de groupes. $\forall k \in \mathbb{N}$, ce morphisme induit, par restriction, un morphisme $\sigma_k : GL_n(\mathbb{C}) \to \mathrm{Aut}(A_k)$ où A_k désigne l'ensemble des polynômes homogènes de degré k.*
2. *Si G est un sous-groupe fini de $GL_n(\mathbb{C})$, G agit aussi sur A_k et on a :*

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - gX)} = \sum_{k=0}^{\infty} \dim(A_k^G) X^k,$$

où $A_k^G = \{P \in A_k \mid \forall g \in G \ \sigma_k(g)(P) = P\}$.

Démonstration : 1. Soient $u, v \in GL_n(\mathbb{C})$ et $P \in A = \mathbb{C}[X_1, ..., X_n]$, alors :

$$\sigma(u \circ v)(P) = P(v^{-1} \circ u^{-1}(X_1, ..., X_n)^t) = \sigma(u)(P(v^{-1}(X_1, ..., X_n)^t)) = \sigma(u) \circ \sigma(v)(P).$$

Comme $\sigma(id) = id$, on en déduit que $\forall u \in GL_n(\mathbb{C})$, $\sigma(u)$ est inversible, d'inverse $\sigma(u^{-1})$. Les $\sigma(u)$ étant linéaires, $\sigma : GL_n(\mathbb{C}) \to \mathrm{Aut}(A)$ est bien définie et est un morphisme de groupes.
Notons $u^{-1} = (u^{-1}_{i,j})_{1 \leqslant i,j \leqslant n}$. Alors, en écrivant

$$\sigma(u)(P) = P(\sum_{i=1}^{n} u^{-1}_{1,i} X_i, ..., \sum_{i=1}^{n} u^{-1}_{n,i} X_i),$$

on remarque que le degré de P est invariant sous l'action de $GL_n(\mathbb{C})$. En particulier, $\forall k \in \mathbb{N}$ et $\forall u \in GL_n(\mathbb{C})$, on a $\sigma(u)(A_k) \subset A_k$. On obtient donc un morphisme

$$\begin{aligned} \sigma_k : GL_n(\mathbb{C}) &\longrightarrow Aut(A_k) \\ u &\longmapsto \sigma(u)_{|A_k} \end{aligned}$$

2. Considérons désormais G un sous-groupe fini de $GL_n(\mathbb{C})$, agissant sur A_k via le morphisme $\sigma_{k|G}$ (que je noterai σ_k aussi, par commodité).
D'après le théorème de Lagrange, le polynôme $X^{|G|} - 1$, qui est scindé à racines simples sur $\mathbb{C}$, est un polynôme annulateur de g, $\forall g \in G$. Par conséquent, les éléments de G sont diagonalisables.
Soit $g \in G$. Il existe donc une matrice $u \in GL_n(\mathbb{C})$ et des complexes $\lambda_1, ..., \lambda_n$ tels que $ugu^{-1} = \mathrm{diag}(\lambda_1, ..., \lambda_n)$.
Par suite,

$$\frac{1}{\det(I_n - gX)} = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i X} = \prod_{i=1}^{n} \left(\sum_{l=0}^{\infty} \lambda_i^l X^l \right) = \sum_{k=0}^{\infty} v_k X^k,$$

où $v_k = \sum_{k_1 + ... + k_n = k} \lambda_1^{k_1} ... \lambda_n^{k_n}$.
D'autre part, $\mathrm{Tr}(\sigma_k(g^{-1})) = \mathrm{Tr}(\sigma_k(ug^{-1}u^{-1}))$ car $\sigma_k(g^{-1})$ et $\sigma_k(ug^{-1}u^{-1})$ sont conjugués dans $\mathrm{Aut}(A_k)$.
Or, $\sigma_k(ug^{-1}u^{-1})(X_1^{k_1} ... X_n^{k_n}) = \lambda_1^{k_1} ... \lambda_n^{k_n} X_1^{k_1} ... X_n^{k_n}$ et $\{X_1^{k_1} ... X_n^{k_n} \mid k_1 + ... + k_n = k\}$ est une base de A_k. Il s'ensuit que,

$$\mathrm{Tr}(\sigma_k(g^{-1})) = \sum_{k_1 + ... + k_n = k} \lambda_1^{k_1} ... \lambda_n^{k_n} = v_k,$$

et donc,

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

La conclusion est alors une conséquence du lemme suivant, qui sera démontré à la fin :

Lemme 2

Sous les hypothèses du théorème, $\dim(A_k^G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\sigma_k(g))$.

En effet, on a alors :

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I_n-gX)} &= \frac{1}{|G|}\sum_{g\in G}\sum_{k=0}^{\infty}\mathrm{Tr}(\sigma_k(g^{-1}))X^k\\ &= \sum_{k=0}^{\infty}\left(\frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\sigma_k(g^{-1}))\right)X^k\\ &= \sum_{k=0}^{\infty}\dim(A_k^G)X^k.\end{aligned}$$

■

Démonstration du lemme :

Posons $f=\frac{1}{|G|}\sum_{g\in G}\sigma_k(g)$, dont la trace est exactement $\frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\sigma_k(g))$. On va montrer que f est une projecteur sur A_k^G ce qui suffira pour conclure.

- Soit $P\in A_k^G$. Alors, $\forall g\in G, \sigma_k(g)(P)=P$ et donc $f(P)=P$. Cela montre que $A_k^G\subset \mathrm{Im}(f)$,
- Soit $P\in\mathrm{Im}(f)$. Alors, $P=f(Q)$ pour un certain Q dans A_k. Par suite, $\forall h\in G$,

$$\sigma_k(h)(P)=\frac{1}{|G|}\sum_{g\in G}\sigma_k(hg)(Q)=f(Q)=P.$$

En conséquence, $\mathrm{Im}(f)=A_k^G$ et $f^2=f$. ■

2 Application en théorie des invariants

C'EST INFORMEL, CE SOT JUSTE DES NOTES SUR CE QUE JE PENSE AVOIR COMPRIS DES REFERENCE FOURNIT PAR IVORRA

2.1 Introduction

Le théorème de Molien ne permet pas seulement de calculer les dimensions des sous-espaces d'invariants, il apporte aussi des renseignements plus profonds sur la structure de l'algèbre d'invariants $\mathbb{C}[X_1,\dots,X_n]^G$.

Deux exemples :

1. Considérons l'action du groupe symétrique $\mathfrak{S}_n$. Le théorème de structure des polynômes symétriques affirme que $\mathbb{C}[X_1,\dots,X_n]^{\mathfrak{S}_n}=\mathbb{C}[\sigma_1,\dots,\sigma_n]$ où les σ_i, $i=1\dots n$, désignent les polynômes symétriques élémentaires.
2. Si l'on s'intéresse maintenant à l'action du groupe alterné $\mathfrak{A}_n$, on peut montrer que tout polynôme invariant par cette action s'écrit sous la forme $A+\Delta B$ avec A,B des polynômes symétriques et $\Delta=\prod_{1\leqslant i<j\leqslant n}(X_i-X_j)$. Cela peut encore s'exprimer de la façon suivante :

$$\mathbb{C}[X_1,\dots,X_n]^{\mathfrak{A}_n}=\mathbb{C}[\sigma_1,\dots,\sigma_n]\oplus\Delta\mathbb{C}[\sigma_1,\dots,\sigma_n]$$

De manière générale, dès que G est fini, l'algèbre admet une décomposition dite d'Hironaka, c'est-à-dire de la forme

$$\mathbb{C}[X_1,\dots,X_n]^G=\oplus_{i=1}^t\eta_i\mathbb{C}[\theta_1,\dots,\theta_n],$$

avec $\eta_1,\dots,\eta_r,\theta_1,\dots,\theta_n$ des polynômes. Les η_i sont appelés les invariants secondaires et les θ_i les invariants primaires.

2.2 Séries de Molien [Muk03]

Définition 3

Un anneau R muni d'une décomposition en somme direct $R = \oplus_{n\in\mathbb{Z}} R_n$ vérifiant $R_n R_m \subset R_{n+m}$ est appelé un anneau gradué. Les R_n sont appelés les composantes homogènes de R.

En reprenant les notations du théorème de Molien, l'anneau A des polynômes à plusieurs indéterminées est naturellement gradué : $A = \oplus_{d\in\mathbb{N}} A_d$. Il en est de même de l'algèbre des invariants de A sous l'action d'un groupe G. En effet on a :

$$A^G = \oplus_{d\in\mathbb{N}} A^G \cap A_d.$$

La série de Molien (ou de Hilbert ou de Poincaré) d'un groupe G est la série génératrice des dimensions des composantes homogènes de A^G (où l'action de G est celle définie dans le théorème de Molien).

Définition 4

La série de Molien d'un groupe G (fini) est la série formelle :

$$M_G(T) = \sum_{d\geqslant 0} (\dim(A^G \cap A_d))T^d.$$

Exemples : Reprenons les deux exemples précédents :

1. Si $G = \mathfrak{S}_n$, un élément de $A^G \cap A_d$, ie un polynôme symétrique homogène de degré d, est combinaison linéaire de monômes $\sigma_1^{k_1} \dots \sigma_n^{k_n}$ de degré totale d. On en déduit donc que :

$$M_G(T) = \sum_{d\geqslant 0} \left(\sum_{k_1+\dots+nk_n=d} 1 \right) T^d = \frac{1}{(1-T)\dots(1-T^n)}.$$

2. Si $G = \mathfrak{A}_n$, un raisonnement similaire conduit à

$$M_G(T) = \frac{1+T^{\frac{n(n-1)}{2}}}{(1-T)\dots(1-T^n)}.$$

Il est important de noter que, dans ces deux exemples, les puissances de T présentes au dénominateur coïncident avec les degrés des polynômes symétriques élémentaires (invariants primaires de G dans les deux cas)[1].
Ce fait, qui n'est pas anodin, illustre l'importance des séries de Molien dans l'étude de l'algèbre des invariants ("The Molien series *measures its size and shape*" [Muk03], page 12.) :

Théorème 5

Si A^G est engendré par des polynômes homogènes $f_1, \dots, f_r$ de degrés $d_1, \dots, d_r$, alors la série de Molien de G est le développement en série formelle d'une fraction rationnelle de la forme

$$\frac{F(T)}{(1-T^{d_1})\dots(1-T^{d_n})},$$

où $F(T) \in \mathbb{Z}[T]$.

Démonstration : Voir [Muk03] page 12[2]. ■

1. On constate aussi qu'au numérateur les puissances correspondent aux degrés des invariants secondaires :$\{1\}$ ou $\{1, \Delta\}$ selon l'exemple.
2. Je crois qu'une erreur de frappe s'est glissée dans le livre : lors de l'hérédité je pense qu'il faut lire $h \mapsto f_r h$ et non $h \mapsto f - rh$.

C'est là qu'intervient le théorème de Molien : en donnant une formule explicite de la série de Molien sous forme d'une fraction rationnelle, il permet de savoir où chercher les invariants (dans quelles composantes homogènes) ! [3]

2.3 Quelques exemples simples [Muk03], [CLO04]

Exemple 1 : Considérons le sous-groupe de $GL_n(\mathbb{C})$ le plus simple, à savoir $G = \{-I_n, I_n\}$.
Par le théorème de Molien, on a :

$$M_G(T) = \frac{1}{2}\left(\frac{1}{(1-T)^n} + \frac{1}{(1+T)^n}\right).$$

Par définition de l'action de G, un polynôme P est G-invariant si et seulement si $P(X_1, \ldots, X_n) = P(-X_1, \ldots, -X_n)$.
On en déduit immédiatement que A^G est engendré par les polynômes homogènes de degré pair.

Plaçons nous dans le cas $n = 2$, de sorte que A^G est engendré par X_1^2, X_2^2 et X_1X_2. Essayons de retrouver cela par la formule de Molien.
La formule ci-dessus, pour $n = 2$, donne

$$M_G(T) = \frac{1+T^2}{(1-T^2)^2} = \frac{1-T^4}{(1-T^2)^3}.$$

Le dénominateur suggère donc la présence des trois générateurs de degré 2.

A première vue il y a escroquerie, puisque dans la dernière égalité, on s'est arrangé pour faire apparaître au dénominateur les trois facteurs $(1-T^2)^3$ que l'on attendait. Cependant, si on raisonne par analogie avec ce que l'on a vu sur l'exemple du groupe alterné, on peut se dire, à la vue de l'expression $\frac{1+T^2}{(1-T^2)^2}$, que A^G possède deux invariants primaires de degré 2 (dénominateur) et un invariant secondaire de degré 2 (numérateur).
En fait on a [4] :

$$A^G = \mathbb{C}[X_1^2, X_2^2] \oplus X_1X_2\mathbb{C}[X_1^2, X_2^2].$$

On remarque alors que :

1. $A^G \cap A_d = (\mathbb{C}[X_1^2, X_2^2]) \cap A_d \oplus (X_1X_2\mathbb{C}[X_1^2, X_2^2]) \cap A_d$
2. $(\mathbb{C}[X_1^2, X_2^2]) \cap A_d$ est trivial si d est impair.

Soit $S = \mathbb{C}[X, Y]$ un anneau de polynôme en deux variables que l'on munit d'une nouvelle graduation en posant $\deg(X) = \deg(Y) = 2$ [5]. On dispose alors d'un isomorphisme d'algèbre graduée (ie un morphisme d'algèbre qui préserve les degrés) :

$$\begin{aligned} \psi : S &\longrightarrow \mathbb{C}[X_1^2, X_2^2] \\ X &\longmapsto X_1^2 \\ Y &\longmapsto X_2^2 \end{aligned}$$

En particulier, S_{2d} est isomorphe (comme espace vectoriel) à $(\mathbb{C}[X_1^2, X_2^2])_{2d} = (\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d}$ pour tout d. Ce dernier est donc de même dimension que l'espace des polynômes homogènes de degré d en deux variables (voir la note 5), c'est-à-dire $\binom{d+1}{d}$.
Maintenant, la multiplication par X_1X_2 est un isomorphisme de $(\mathbb{C}[X_1^2, X_2^2]) \cap A_d$ dans $(X_1X_2\mathbb{C}[X_1^2, X_2^2]) \cap$

3. Voilà... deux paragraphes de trucs inutiles pour l'agreg avec, comme ultime conclusion, une application finalement assez vague du théorème de Molien...
4. cela se déduit du fait que A^G est engendré par les polynômes homogènes de degré pair
5. On a S_d réduit à zéro pour d impair et S_{2d} qui est l'ensemble des polynômes homogènes de degré d pour la graduation "classique".

A_{d+2}, leurs dimensions sont donc égales. Au final, on obtient :

$$\begin{aligned}
M_G(T) &= \sum_{d\in\mathbb{N}} \dim((\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d} \oplus (X_1X_2\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d})T^{2d} \\
&= \sum_{d\in\mathbb{N}} \left(\dim((\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d}) + \dim((X_1X_2\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d})\right) T^{2d} \\
&= \sum_{d\in\mathbb{N}} \binom{d+1}{d} T^{2d} + \sum_{d\geqslant 2} \dim((\mathbb{C}[X_1^2, X_2^2]) \cap A_{2d-2})T^{2d} \\
&= \frac{1}{(1-T^2)^2} + T^2 \sum_{d\in\mathbb{N}} \binom{d+1}{d} T^{2d} \\
&= \frac{1+T^2}{(1-T^2)^2}
\end{aligned}$$

Je pense que cet argument s'adapte pour montrer le résultat suivant.

Théorème 6 (*[Vac]*)

Si la décomposition d'Hironaka de $\mathbb{C}[X_1, \ldots, X_n]^G$ est :

$$\mathbb{C}[X_1, \ldots, X_n]^G = \oplus_{i=1}^t \eta_i \mathbb{C}[\theta_1, \ldots, \theta_n],$$

avec les θ_i de degré d_i et les η_j de degré e_j alors,

$$M_G(T) = \frac{\sum_j T^{e_j}}{\prod_i (1-T^{d_j})}.$$

Références

[CLO04] D. A. COX, J. LITTLE et D. O'SHEA – *Using algebraic geometry*, Springer, 2004.

[Muk03] S. MUKAI – *An introduction to invariants and moduli*, Cambridge University, 2003.

[Vac] T. VACCON – *Polycopié du complément sur la théorie des invariants*.