Université Claude Bernard Lyon 1
M2 de Mathématiques : Groupes algébriques
Année 2013–2014

III Formule de Molien et applications

1° Série de Poincaré

Si $R = \bigoplus_{n\in\mathbb{N}} R_n$ est une algèbre graduée ($R_n R_p \subset R_{n+p}$) ou plus généralement un espace vectoriel gradué, on définit sa série de Poincaré [1] par :

$$P_R(t) = \sum_{n\geqslant 0} \dim_{\mathbb{C}}(R_n)\, t^n \quad \text{(où } t \text{ est une indéterminée).}$$

a) Pour l'algèbre symétrique $S(V)$ d'un espace V de dimension d, on a : $P_{S(V)} = \frac{1}{(1-t)^d}$.
b) On suppose que R est intègre et engendrée par r éléments homogènes de degrés $d_1, \ldots, d_r$. On veut montrer qu'existe un polynôme $F \in \mathbb{Z}[t]$ tel que

$$P_R(t) = \frac{F(t)}{(1-t^{d_1})\cdots(1-t^{d_r})}.$$

L'indication proposée suivait la « preuve » de la proposition 1.9 de [1] (c'est pas beau de dénoncer). Comme vous l'avez justement remarqué, elle est fausse et même irratrapable : le pas de récurrence repose sur l'idée fausse que $R/(f_r)$ est intègre, ce qui permet de montrer que $F = 1$. Aucune de ces deux assertions n'est vraie en général.

Exemple. On prend $R = \mathbb{C}[x, y, z]/(xy - z^2)$, où $x = f_1$, $y = f_2$, $z = f_3$ sont trois générateurs de degré 1 : aucun des quotients $R/(f_i)$ n'est intègre !

Voici une version plus générale – elle parle de modules et ne comporte pas d'hypothèse parasite d'intégrité – et plus juste.

Théorème (Hilbert-Serre). *Soit $R = \bigoplus_{n\geqslant 0} R_n$ une algèbre graduée engendrée par un nombre fini d'éléments homogènes $f_1, \ldots, f_r$ de degrés respectifs $d_1, \ldots, d_r$ et soit $M = \bigoplus_{n\geqslant 0} M_n$ un R-module gradué [2] engendré par un nombre fini de générateurs homogènes [3]. Alors la série de Poincaré de M est de la forme*

$$P_M(t) = \frac{F(t)}{\prod_{i=1}^r (1 - t^{d_i})}$$

pour $F \in \mathbb{Z}[t]$ convenable.

Démonstration. On procède par récurrence sur r. Si $r = 0$, M est un espace vectoriel gradué de dimension finie et sa série de Poincaré est un polynôme $F \in \mathbb{N}[t]$. Pour $r \geqslant 1$, on introduit comme dans l'indication initiale l'application $\varphi : M \to M$, $m \mapsto f_r m$. Il n'y a aucune raison pour que φ soit injective, soit K son noyau ; comme φ est homogène, le R-module K est gradué : $K = \bigoplus_{n\geqslant 0} K_n$ où $K_n = K \cap M_n$. De même, l'image $f_r M$ est graduée : $(f_r M)_{n+d_r} = f_r M_n$ pour $n \geqslant 0$ et les composantes de degré $< d_r$ sont nulles.
On a deux suites exactes :

$$0 \to K \longrightarrow M \xrightarrow{\varphi} f_r M \to 0,$$
$$0 \to f_r M \xrightarrow{\iota} M \longrightarrow M/f_r M \to 0.$$

1. On l'appelle aussi série de Hilbert, voire série de Hilbert-Poincaré.
2. Cela signifie que $R_n M_p \subset M_{n+p}$ pour tous $n, p \in \mathbb{N}$.
3. Cela entraîne que les espaces M_n sont de dimension finie. Pourquoi ?

En observant les dimensions [4] degré par degré, on trouve pour tout $n \in \mathbb{Z}$ (si $n < 0$, $M_n = 0$) :

$$\dim M_n = \dim K_n + \dim(f_r M)_{n+d_r} \text{ et } \dim M_{n+d_r} = \dim(f_r M)_{n+d_r} + \dim(M/f_r M)_{n+d_r}.$$

On multiplie ces égalités par t^{n+d_r} et on somme sur n, il vient :

$$t^{d_r} P_M(t) = t^{d_r} P_K(t) + P_{f_r M}(t) \text{ et } P_M(t) = P_{f_r M}(t) + P_{M/f_r M}(t),$$

d'où en simplifiant :

$$(1 - t^{d_r}) P_M(t) = P_{M/f_r M}(t) - t^{d_r} P_K(t).$$

Variante : on a une suite exacte

$$0 \to K \longrightarrow M \xrightarrow{\varphi} M \longrightarrow M/f_r M \to 0,$$

où φ est de degré d_r et les autres applications préservent le degré. Cela signifie que l'on a des suites exactes pour tout $n \in \mathbb{Z}$:

$$0 \to K_n \longrightarrow M_n \xrightarrow{\varphi} M_{n+d_r} \longrightarrow (M/f_r M)_{n+d_r} \to 0,$$

d'où des égalités :

$$\dim(K_n) - \dim M_n + \dim M_{n+d_r} - \dim(M/f_r M)_{n+d_r} = 0.$$

En multipliant par t^{n+d_r} et en sommant, on retrouve :

$$t^{d_r} P_K(t) - t^{d_r} P_M(t) + P_M(t) - P_{M/f_r M}(t) = 0.$$

Il ne reste plus qu'à remarquer que K et $M/f_r M$ sont des modules de type fini sur l'algèbre $R' = R/(f_r)$, qui est engendrée par $r-1$ éléments de degrés respectifs $d_1, \ldots, d_{r-1}$ – les classes de $f_1, \ldots, f_{r-1}$ modulo l'idéal engendré par f_r. Par hypothèse de récurrence, il existe F_1 et F_2 dans $\mathbb{Z}[t]$ tels que $P_K(t) = F_1(t)/\prod_{i=1}^{r-1}(1 - t^{d_i})$ et $P_{M/f_r M}(t) = F_2(t)/\prod_{i=1}^{r-1}(1 - t^{d_i})$, ce qui permet de conclure.

Corollaire. *Soit $R = \bigoplus_{n \geqslant 0} R_n$ une algèbre graduée engendrée par des éléments homogènes $f_1, \ldots, f_r$ de degrés respectifs $d_1, \ldots, d_r$. Alors la série de Poincaré de R est de la forme*

$$P_R(t) = \frac{F(t)}{\prod_{i=1}^{r}(1 - t^{d_i})}$$

pour $F \in \mathbb{Z}[t]$ convenable.

Démonstration. Bien sûr, R est un R-module noethérien !

4. Rappelons que si $0 \to A \to B \to C \to 0$ est une suite exacte d'espaces vectoriels de dimension finie, on a : $B/A \simeq C$ d'où : $\dim B = \dim A + \dim C$.

c) Soit $R = \mathbb{C}[x_1, \dots, x_r]^{\mathfrak{S}_r}$. On sait que R est l'algèbre de polynômes $\mathbb{C}[e_1, \dots, e_r]$ où les e_i sont les fonctions symétriques élémentaires. Si on développe en série

$$\prod_{i=1}^{r} \frac{1}{(1-t^i)} = \prod_{i=1}^{r} \sum_{k_i \geqslant 0} \frac{1}{t^{ik_i}},$$

le coefficient de t^n est le nombre de multi-indices $(k_1, \dots, k_r) \in \mathbb{N}^r$ tels que $\sum_{i=1} ik_i = n$; c'est aussi le nombre de monômes $e_1^{k_1} \cdots e_r^{k_r}$ de degré n. Ainsi : $P_R = \prod_{i=1}^{r}(1-t^i)^{-1}$.
Soit $S = \mathbb{C}[x_1, \dots, x_r]^{\mathfrak{A}_r}$. On a vu que S est un R-module libre de rang 2, puisque $S = R \oplus vR$ où $v(x_1, \dots, x_r) = \prod_{i<j}(x_i - x_j)$. On a donc, puisque v est de degré $n(n-1)/2$:

$$P_S(t) = P_R(t) + t^{\frac{n(n-1)}{2}} P_R(t) = \frac{1 + t^{\frac{n(n-1)}{2}}}{\prod_{i=1}^{r}(1-t^i)} = \frac{1 - t^{n(n-1)}}{(1 - t^{\frac{n(n-1)}{2}}) \prod_{i=1}^{r}(1-t^i)}.$$

On va en déduire une présentation de S. Plus précisément, on montre grâce à la forme de la série qu'il y a une relation de degré $n(n-1)$ entre les générateurs et qu'il n'y a pas d'autre relation. ≪ Trouver ≫ la relation est très facile. On sait que v^2 est invariant par $\mathfrak{S}_n$: c'est à une constante près le discriminant de $\prod_{i=1}^{r}(X - x_i)$. Il existe donc un unique polynôme F tel que $v^2 = F(e_1, \dots, e_r)$ dans R. Par exemple, si $n = 2$, on a : $v^2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = e_1^2 - 4e_2$. Il est homogène[5] de degré $n(n-1)$ en les e_i puisque v est homogène de degré $n(n-1)/2$.
Soient $E_1, \dots, E_r, V$ des indéterminées et $T = \mathbb{C}[V, E_1, \dots, E_r]$. On gradue T en donnant à V le degré $n(n-1)/2$ et à E_i le degré i. Le morphisme surjectif $T \to S$, $V \mapsto v$, $E_i \mapsto e_i$ $(1 \leqslant i \leqslant r)$ se factorise à travers le quotient $\mathbf{S} = T/\big(V^2 - F(E_1, \dots, E_r)\big)$. De plus, la multiplication $T \to T$, $H \mapsto (V^2 - F)H$ est une injection dont le conoyau est le quotient $\mathbf{S}$. Aussi, il vient :

$$P_{\mathbf{S}}(t) = P_T(t) - t^{n(n-1)} P_T(t) = \frac{1 - t^{n(n-1)}}{(1 - t^{\frac{n(n-1)}{2}}) \prod_{i=1}^{r}(1-t^i)}.$$

Ainsi, S est un quotient de $\mathbf{S}$ et a la même série de Poincaré. Autrement dit : $S \simeq \mathbf{S}$.

2° Énoncé et preuve de la formule de Molien

a) D'abord, $\operatorname{Im}\theta$ est inclus dans W^G : si $w = \theta(v)$, on a pour $g \in G$ (en posant $h' = gh$) :

$$gw = \frac{1}{|G|} \sum_{h \in G} ghv = \frac{1}{|G|} \sum_{h' \in G} h'v = \theta v = w.$$

Inversement, si w est G-invariant, on a :

$$\theta(w) = \frac{1}{|G|} \sum_{h \in G} hw = \frac{1}{|G|} \sum_{h \in G} w = w.$$

En particulier, W^G est égal à $\operatorname{Im}(\theta)$ et la restriction de θ à $\operatorname{Im}(\theta)$ est l'identité. Cela signifie que $\theta \circ \theta = \theta$, c'est-à-dire que θ est un projecteur sur $\operatorname{Im}(\theta) = W^G$. Vérifions qu'il est équivariant. Soit $g \in G$, on a dans $\operatorname{End}_{\mathbb{C}}(W)$, par le changement de variable $h' = ghg^{-1}$:

$$g\theta = \frac{1}{|G|} \sum_{h \in G} gh = \frac{1}{|G|} \sum_{h' \in G} h'g = \theta g.$$

5. Vérifiez-le !

b) Le rang d'un projecteur est sa trace : $\dim W^G = \operatorname{rg}\theta = \operatorname{tr}\theta$.
c) On a, avec $\theta = \frac{1}{|G|}\sum_{g\in G} g$ l'élément de l'algèbre de groupe et par linéarité de la trace :

$$P_{G,V}(t) = \sum_{k\geqslant 0} \dim S^k(V)^G t^k = \sum_{k\geqslant 0} \operatorname{tr}(\theta|_{S^k(V)})t^k = \frac{1}{|G|}\sum_{g\in G}\sum_{k\geqslant 0} \operatorname{tr}(g|_{S^k(V)})t^k.$$

Fixons $g \in G$. Comme G est fini, g est d'ordre fini et comme on est sur $\mathbb{C}$, $g|_V$ est diagonalisable. Soient $(v_1, \ldots, v_n)$ une base de vecteurs propres et $(\lambda_1, \ldots, \lambda_n)$ les valeurs propres associées. Pour tout k, les monômes de degré k, c'est-à-dire la famille $\left(v_1^{m_1}\cdots v_n^{m_n}\right)_{(m_1,\ldots,m_n)\in\mathbb{N}^n,\ m_1+\cdots+m_n=k}$, forment une base de vecteurs propres de g. D'où :

$$\operatorname{tr}(g|_{S^k(V)}) = \sum_{m_1+\cdots+m_n=k} \lambda_1^{m_1}\cdots\lambda_n^{m_n}.$$

En sommant sur k, il vient :

$$\begin{aligned}\sum_{k\geqslant 0}\operatorname{tr}(g|_{S^k(V)})t^k &= \sum_{(m_1,\ldots,m_n)\in\mathbb{N}^n} \lambda_1^{m_1}\cdots\lambda_n^{m_n} t^{m_1+\cdots+m_n}\\ &= \prod_{i=1}^n \sum_{m_i\geqslant 0}(t\lambda_i)^{m_i} = \prod_{i=1}^n \frac{1}{1-t\lambda_i} = \frac{1}{\det(\mathrm{I}_n - tg)}.\end{aligned}$$

En moyennant sur G, il vient :

$$P_{G,V}(t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{I}_n - tg)}.$$

3° **Cône (singularité de type A_1)**

On fait agir l'élément non trivial de $G = \mathbb{Z}/2\mathbb{Z}$ sur $V = \mathbb{C}^2 = \mathbb{C}x \oplus \mathbb{C}y$ comme $-\mathrm{Id}$.
a) Bien sûr, $\mathbb{C}[x^2, xy, y^2]$ est inclus dans l'algèbre des invariants $\mathbb{C}[x,y]^{\mathbb{Z}/2\mathbb{Z}}$.
Pour l'inclusion inverse, on diagonalise l'action de G : les monômes en x et y de degré pair (resp. impair) sont invariants (resp. transformés en leur opposé par Id). Par suite, les polynômes invariants sont les combinaisons linéaires des monômes $x^a y^b$ avec $a+b$, c'est-à-dire que a et b ont la même parité. Mais alors, $a - \min(a,b)$ et $b - \min(a,b)$ sont pairs et on peut par exemple écrire :

$$x^a y^b = x^{a-\min(a,b)}(xy)^{\min(a,b)}y^{b-\min(a,b)} \in \mathbb{C}[x^2, xy, y^2].$$

De plus, par la formule de Molien, on a :

$$P_{S(V)^G}(t) = \frac{1}{2}\left(\frac{1}{\det(\mathrm{I}_2 - t\mathrm{I}_2)} + \frac{1}{\det(\mathrm{I}_2 - t\mathrm{I}_2)}\right) = \frac{1}{2}\left(\frac{1}{(1-t)^2} + \frac{1}{(1+t)^2}\right) = \frac{1+t^2}{(1-t^2)^2}.$$

b) On donne à u, v et w le degré 2 ; alors, $f = uv - w^2$ est homogène de degré 4 et $T = \mathbb{C}[u,v,w]/(uv-w^2)$ est graduée. Comme on l'a déjà fait ci-dessus, on réalise T comme quotient de $\mathbb{C}[u,v,w]$ par l'image de l'application injective $\varphi : \mathbb{C}[u,v,w] \to \mathbb{C}[u,v,w]$, $h \mapsto fh$. L'algèbre $\mathbb{C}[u,v,w]$ a pour série de Poincaré $1/(1-t^2)^3$ et l'image de φ, $t^4/(1-t^2)^3$. D'où : $P_T(t) = (1-t^4)/(1-t^2)^3 = (1+t^2)/(1-t^2)^2$.
c) Comme $x^2y^2 - (xy)^2 = 0$, on a un morphisme $T \simeq S(V)^G$, $u \mapsto x^2$, $v \mapsto y^2$, $w \mapsto xy$. Ce morphisme préserve la graduation, il est surjectif et T et $S(V)^G$ ont la même série de Poincaré : c'est donc un isomorphisme.

4° Singularités de type A

Mise en garde (Erreur d'énoncé !). *On fixe un générateur g de $\mathbb{Z}/n\mathbb{Z}$ et on le fait agir comme la matrice diagonale dont les valeurs propres sont $\zeta = e^{2i\pi/n}$ et ζ^{-1}.*
Si on fait agir g comme $\zeta\mathrm{Id}$, l'algèbre est engendrée par les monômes $x^a y^b$ avec $a+b \equiv 0\,[n]$, c'est beaucoup plus compliqué : les invariants sont engendrés par $(n+1)$ monômes $u_i = x^{n-i}y^i$ $(0 \leqslant i \leqslant n)$ et on a $(n-1)$ relations : $u_{i-1}u_{i+1} = u_i^2$ $(1 \leqslant i \leqslant n-1)$.

a) On veut montrer que $S(V)^G = \mathbb{C}[x^n, xy, y^n]$. On constate que les monômes en x et y sont une base de vecteurs propres de G dans $S(V)$; la valeur propre de $x^a y^b$ est ζ^{a-b}. L'algèbre des invariants est donc engendrée par les monômes invariants : $x^a y^b$ avec $a - b \equiv 0\,[n]$. Si cette condition est remplie et $a > b$, on a : $x^a y^b = (x^n)^{(a-b)/n}(xy)^{a-b}$; si $a < b$, on a : $x^a y^b = (xy)^{b-a}(y^n)^{(b-a)/n}$. On en déduit que $S(V)^G \subset \mathbb{C}[x^n, xy, y^n]$, l'inclusion réciproque étant évidente.
Appliquons la formule de Molien. Pour $k \in \mathbb{Z}/n\mathbb{Z}$, le déterminant de $\mathrm{Id}-tg^k$ est $(1-t\zeta^k)(1-t\zeta^{-k})$. Pour autant que $\zeta^k \neq \zeta^{-k}$, c'est-à-dire $2k \neq 0\,[n]$, on a :

$$\frac{1}{(1-t\zeta^k)(1-t\zeta^{-k})} = \frac{\frac{1}{\zeta^k-\zeta^{-k}}}{t-\zeta^k} - \frac{\frac{1}{\zeta^k-\zeta^{-k}}}{t-\zeta^{-k}}.$$

Il vient en sommant :

$$P_{G,V}(t) = \frac{1}{n}\sum_{k\in\mathbb{Z}/n\mathbb{Z}} \frac{1}{(1-t\zeta^k)(1-t\zeta^{-k})} = \sum_{2k\not\equiv 0[n]} \frac{\frac{2}{n(\zeta^k-\zeta^{-k})}}{t-\zeta^k} + \frac{1}{n(t-1)^2} + \frac{1}{n(t+1)^2},$$

où le dernier terme n'apparaît que si n est pair.
Inspiré par la suite, on peut écrire cette fraction sous forme irréductible en remarquant que ζ^k est un pôle simple si $2k \not\equiv 0\,[n]$, que 1 est un pôle double et que -1 est un pôle simple si n est impair et double si n est pair. Autrement dit, il existe un polynôme $F \in \mathbb{C}[t]$ tel que

$$P_{G,V}(t) = \frac{F(t)}{(1-t^n)(1-t^2)},$$

où -1 est un zéro simple de F si n est impair et pas un zéro si n est pair. On peut jouer à chercher F à partir de la décomposition en éléments simples ci-dessus...
b) Dans l'algèbre $\mathbb{C}[u,v,w]$, on donne le degré n à u et v et 2 à w. Alors, $uv - w^n$ est homogène de degré $2n$ et le quotient $T = \mathbb{C}[u,v,w]/(uv-w^n)$ est gradué. Sa série de Poincaré se calcule comme ci-dessus avec $n = 2$: d'une part, $\mathbb{C}[u,v,w]$ a pour série de Poincaré est $1/(1-t^n)^2(1-t^2)$; d'autre part, l'application $h \mapsto (uv-w^n)h$ préserve le degré et est injective donc son image a pour série $t^{2n}/(1-t^n)^2(1-t^2)$. Le quotient T a donc pour série de Poincaré :

$$P_T(t) = \frac{1-t^{2n}}{(1-t^n)^2(1-t^2)} = \frac{1+t^n}{(1-t^n)(1-t^2)}.$$

c) Montrons que l'on a : $T \simeq S(V)^G$. Le morphisme $\mathbb{C}[u,v,w] \to S(V)^G$, $u \mapsto x^n$, $v \mapsto y^n$, $w \mapsto xy$ préserve les degré et est surjectif. Comme $x^n y^n = (xy)^n$, il se factorise à travers l'idéal engendré par $uv - w^n$, d'où une surjection graduée $T = \mathbb{C}[u,v,w]/(uv-w^n) \to S(V)^G$. Pour montrer c'est un isomorphisme, il suffit de montrer l'égalité des séries de Poincaré, ce qui revient à décomposer $P_T(t)$ en éléments simples.
Les pôles de P_T sont les ζ^k (simples si $2k \not\equiv 0\,[n]$), 1 (double) et, si n est pair, -1 (double). Soit k tel que $2k \not\equiv 0\,[n]$. Le polynôme $t^n - 1$ a pour dérivée nt^{n-1} ; le résidu en ζ^k est donc :

$$\left.\frac{1+t^n}{nt^{n-1}(t^2-1)}\right|_{t=\zeta^k} = \frac{2}{\zeta^{(n-1)k}(\zeta^{2k}-1)} = \frac{2}{\zeta^k-\zeta^{-k}}.$$

Pour le pôle en 1, on pose $H(t) = (t-1)^2 P_T(t) = (t^n+1)/(t+1)(t^{n-1}+\cdots+1)$, qui est régulière en 1. On a donc :

$$P_T(t) = \frac{H(1) + (t-1)H'(1)}{(t-1)^2} + (\text{régulier en } 1).$$

On vérifie que $H(1) = 1/n$ et $H'(1) = 0$.
Reste à traiter le pôle en -1 lorsque n est pair. Mais alors, $P_T(t)$ est une fraction paire et donc :

$$P_T(t) = \frac{1}{(t+1)^2} + (\text{régulier en } -1).$$

Au bilan, on a bien : $P_T(t) = P_{S(V)^G}$, ce qui entraîne que $S(V)^G \simeq \mathbb{C}[u,v,w]/(uv - w^n)$.

5° **Groupe quaternionique**

Les calculs sont analogues, les faire ou voir le premier chapitre de [1].

Bibliographie

[1] Shigeru Mukai : *An introduction to invariants and moduli*, volume 81 de *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2003. Translated from the 1998 and 2000 Japanese editions by W. M. Oxbury.