M.M.F.A.I. Année 1999/2000

Polynômes Invariants

Jonathan Le Roux Julien Lévy

Exposé de maîtrise sous la direction de Yves Benoist

Jeudi 8 juin 2000

Table des matières

1 Introduction

Nous nous intéressons dans cet exposé aux polynômes sur un espace vectoriel invariants par l'action d'un groupe fini. *Hilbert* démontre dans un célèbre théorème que l'algèbre des polynômes invariants est de type fini. Nous souhaitons ici caractériser le fait que cette algèbre est une algèbre de polynômes. *Shephard*, *Todd* et *Chevalley* ont démontré que c'était le cas si et seulement si le groupe était engendré par des *pseudo-réflexions*, i.e. des automorphismes différents de l'identité, d'ordre fini, ayant un hyperplan de points fixes. Pour démontrer ce théorème, nous introduirons la notion de *série de Poincaré*, avec en particulier les théorèmes de *Hilbert-Serre* et de *Molien*, et des notions d'homologie algébrique, notamment le théorème des *sysygies* de *Hilbert*. Nous admettrons dans cet exposé le théorème de *Serre*, réciproque du théorème des *sysygies*.

2 Invariants et Théorème de Hilbert

2.1 Algèbre des invariants

Soit G un groupe fini, $\mathbb{F}$ un corps, V un $\mathbb{F}$-espace vectoriel de dimension finie, et $\rho : G \to Aut(V) = GL(V)$ une représentation de G sur V. G agit sur V via ρ par automorphismes.

Pour un espace vectoriel V sur $\mathbb{F}$, on note $\mathbb{F}[V]$ l'algèbre des fonctions polynômes sur V, définie comme étant l'algèbre symétrique sur V^*, dual de V. Si V est de dimension n sur $\mathbb{F}$, et $x_1, \ldots, x_n$ est une base de V^*, alors : $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$. On note $\mathbb{F}[V]_n$ la composante homogène de degré n de $\mathbb{F}[V]$. On considère aussi les éléments de $\mathbb{F}[V]$ comme des fonctions de V dans $\mathbb{F}$.

Une fois donnée une représentation $\rho : G \to GL(V)$, le groupe G agit sur $\mathbb{F}[V]$ via

$$(gf)(v) := f(\rho(g^{-1})v),$$

pour tout $g \in G$ et tout $v \in V$. L'objet fondamental de la théorie des invariants est l'ensemble des points fixes de l'action de G, l'**anneau des invariants** :

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \,|\, gf = f \,\forall g \in G\}.$$

Si ρ n'est pas injective, ρ induit une représentation injective $\tilde{\rho} : G/ker(\rho) \hookrightarrow GL_n(\mathbb{F})$. Il est clair que $\mathbb{F}[V]^G = \mathbb{F}[V]^{G/ker(\rho)}$, et on peut donc supposer sans perte de généralité que ρ est injective.

2.2 Hilbert's Basis Theorem

Définition 2.2.1. *Un module M sur un anneau commutatif A est dit* **noethérien** *si toute suite croissante de sous-modules est stationnaire. Un anneau A est dit* **noethérien** *s'il est noethérien comme A-module.*

On montre facilement que comme dans le cas des anneaux noethériens, cette définition est équivalente au fait que tout sous-module de M est de type fini, ou encore au fait que toute famille non vide de sous-modules admet un élément maximal. Il est clair qu'un sous-module et un quotient d'un module noethérien sont noethériens. Plus généralement, si M est noethérien et N est un autre module sur le même anneau, un morphisme surjectif de M sur N rend N noethérien. Réciproquement, si N et M/N sont noethériens, alors M est noethérien : en effet, si L est un sous-module de M, $L \cap N$ et $L/L \cap N \simeq (L+N)/N$ sont de type fini, donc L aussi. On en déduit qu'une somme directe finie de modules noethériens est un module noethérien, et en particulier que si A est un anneau noethérien, A^n est un A-module noethérien. Les quotients de A^n étant aussi noethériens, on en déduit la

Proposition 2.2.2. *Un module M sur un anneau noethérien A est noethérien si et seulement si il est de type fini.*

□

Corollaire 2.2.3. *Un sous-module d'un module de type fini sur un anneau noethérien est de type fini.*

□

Théorème 2.2.4. *(Théorème de la base de Hilbert) Si A est un anneau commutatif noethérien, alors $A[X]$ est aussi un anneau commutatif noethérien.*

Démonstration : Il suffit de montrer que tout idéal $\mathcal{I}$ de $A[X]$ est de type fini. Soit $\mathcal{I}'$ l'idéal de A engendré par les coefficients dominants des polynômes de $\mathcal{I}$. A étant noethérien, $\mathcal{I}'$ est de type fini, engendré par $a_1, \ldots, a_n$. Soient $f_1, \ldots, f_n \in \mathcal{I}$ des polynômes ayant ces coefficients dominants, soit t le maximum des degrés des f_i, et soit $\mathcal{I}_0$ l'idéal de $A[X]$ engendré par les f_i. Si f est un polynôme de $\mathcal{I}$ de degré au moins t, son coefficient dominant est dans $\mathcal{I}'$, et l'on peut soustraire une combinaison linéaire de produits de f_i et de puissances de x pour éliminer le coefficient dominant de f. On a alors $f = g + h$, avec $g \in \mathcal{I}_0, h \in \mathcal{I}$, et $deg(h) < deg(f)$. En répétant le procédé, on aboutit finalement à $f = \bar{g} + \bar{h}$, avec $\bar{g} \in \mathcal{I}_0, \bar{h} \in \mathcal{I}$, et $deg(\bar{h}) < t$.
D'où :

$$\mathcal{I} = \mathcal{I}_0 + (\mathcal{I} \cap (A \oplus Ax \oplus \cdots \oplus Ax^{t-1})).$$

$\mathcal{I} \cap (A \oplus Ax \oplus \cdots \oplus Ax^{t-1})$ est de type fini comme sous-module d'un module de type fini sur A noethérien. Donc $\mathcal{I}$ est de type fini.

□

Corollaire 2.2.5. *Par récurrence, on en déduit que si A est un anneau noethérien, alors $A[X_1, \ldots, X_n]$ est noethérien. Donc si A est une $\mathbb{F}$-algèbre commutative de type fini, A est un anneau noethérien.*

□

2.3 Théorème de finitude de Hilbert

Théorème 2.3.1. *(Hilbert)Soit G un groupe fini, $\mathbb{F}$ un corps de caractéristique nulle, $V = \mathbb{F}^n$ et $G \hookrightarrow GL(\mathbb{F}^n)$ une représentation de G. Alors $\mathbb{F}[V]^G$ est de type fini comme* *algèbre.*

Démonstration : On pose $B = \mathbb{F}[V]^G, B_+ = \{f \in B |\, deg(f) > 0\}, A = \mathbb{F}[V]$. Soit $\mathcal{I}$ l'idéal engendré par $B_+, \mathcal{I} = B_+A$. D'après le théorème 2.2.4, A est noethérien, donc $\mathcal{I}$ est de type fini. Soient $f_1, \ldots, f_d$ des éléments de $\mathcal{I}$ qui l'engendrent. Les f_i sont dans B_+A, donc on peut les supposer dans B_+, et même homogènes de degrés strictement positifs, quitte à prendre leurs composantes homogènes.

Montrons que les f_i engendrent B comme anneau : soit $f \in B\backslash\mathbb{F}[f_1, \ldots, f_d]$ homogène de degré minimal. $f \in \mathcal{I}$, donc $f = \sum_i f_i a_i, a_i \in A$. $d^o(f) = d^o(f_i) + d^o(a_i)$, $\forall i$, donc $d^o(a_i) < d^o(f)$.
On fait la moyenne sur les éléments du groupe :

$$f = \frac{1}{|G|}\sum_{g\in G} gf = \sum_i (f_i \frac{1}{|G|}\sum_{g\in G}(ga_i)).$$

Donc $f = \sum_i f_i\tilde{a_i}$, où les $\tilde{a_i}$ sont G-invariants, donc dans B. Or $d^o(\tilde{a_i}) < d^o(f)$, donc les a_i sont dans $\mathbb{F}[f_1, \ldots, f_d]$. On a alors $f \in \mathbb{F}[f_1, \ldots, f_d]$, absurde.

□

Le fait que l'anneau des invariants soit de type fini n'est pas un fait particulier à la caractéristique nulle. Noether a démontré que c'était vrai pour un corps de caractéristique quelconque ; elle a aussi montré que $\mathbb{F}[V]$ est une extension finie entière de $\mathbb{F}[V]^G$:

Théorème 2.3.2. *(Noether) Soit $\mathbb{F}$ un corps, G un groupe fini agissant par automorphismes sur une $\mathbb{F}$-algèbre commutative de type fini A. Alors A^G est aussi une $\mathbb{F}$-algèbre commutative de type fini, et A est de type fini en tant que module sur A^G.*

Démonstration : Si $a \in A$ alors a est racine du polynôme unitaire

$$\prod_{g\in G}(X - g(a)) \in A^G[X].$$

A est donc une extension entière de A^G; de plus A est de type fini sur A^G en tant qu'algèbre, car de type fini sur $\mathbb{F}$ et $\mathbb{F} \subset A^G$, donc A est de type fini sur A^G en tant que module. Soit B la sous-algèbre de A^G engendrée par les coefficients des polynômes unitaires introduits plus hauts et satisfaits par un ensemble fini de générateurs de la $\mathbb{F}$-algèbre A. B est une $\mathbb{F}$-algèbre de type fini, et B est donc noethérien. Les générateurs de A considérés sont entiers sur B par construction, donc A est entière sur B ; étant de type fini sur B comme algèbre, A est un B-module de type fini ; d'où A^G aussi car B noethérien. Donc A^G est une $\mathbb{F}$-algèbre de type fini. □

Corollaire 2.3.3. *Soit G un groupe fini, $\mathbb{F}$ un corps et V une représentation de G de dimension finie. Alors $\mathbb{F}[V]^G$ est une $\mathbb{F}$-algèbre de type fini, et $\mathbb{F}[V]$ est une extension finie entière de $\mathbb{F}[V]^G$.*

□

3 Séries de Poincaré

Soit $G \to GL(V)$ une représentation linéaire d'un groupe fini G. On remarque que l'action de G envoie les monômes sur les monômes de même degré ; on peut ainsi décomposer un polynôme invariant en somme de composantes homogènes invariantes. On s'intéresse donc à la dimension de la composante homogène $\mathbb{F}[V]_j^G$, constituée des polynômes invariants homogènes de degré j.

3.1 Modules gradués et Séries de Poincaré

Définition 3.1.1. *Un* **espace vectoriel gradué** *sur* $\mathbb{F}$ *est une somme directe d'espaces vectoriels* $M = \bigoplus_{i \in \mathbb{Z}} M_i$. M_i *est appelé* **composante homogène** *de degré* i. *Si* $M_i = 0$ *pour tout* $i < 0$, M *est dit espace vectoriel* **positivement gradué** *sur* $\mathbb{F}$. *Si* $\dim_{\mathbb{F}} M_i$ *est finie pour tout* i, *on dit que* M *est de type fini. Si* M *et* N *sont des espaces vectoriels gradués sur* $\mathbb{F}$, *un* **morphisme d'espaces vectoriels gradués de degré** d, $f : M \to N$, *est une suite d'applications linéaires* $\{f_i : M_i \to N_{i+d} \,|\, i \in \mathbb{Z}\}$. *On définit de même un* **module gradué** M *sur un anneau* A.

Définition 3.1.2. *Une* **algèbre graduée** A *sur un corps* $\mathbb{F}$ *est une* $\mathbb{F}$*-algèbre graduée comme* $\mathbb{F}$*-espace vectoriel,* $A = \bigoplus_{i \in \mathbb{Z}} A_i$, *telle que pour tout* i *et* j *dans* $\mathbb{Z}$, $A_i \cdot A_j \subset A_{i+j}$.

Si A *est positivement graduée et si l'inclusion de* $\mathbb{F}$ *dans* A_0 *est un isomorphisme, on dit que* A *est connexe.*

Remarque 3.1.3. $\mathbb{F}$ *s'injecte bien dans* A_0 *car* $1 \in A_0$.
En effet, si $1 \in A_i$, $1 = 1 \cdot 1 \in A_{2i}$, *et la somme étant directe,* $i = 0$.

Définition 3.1.4. *Soit* M *un espace vectoriel gradué de type fini sur* $\mathbb{F}$. *La série de Poincaré de* M *est la série formelle*

$$P(M, t) = \sum_{j=0}^{\infty} \dim_{\mathbb{F}}(M_j) t^j.$$

Pour des espaces vectoriels gradués M', M'', on définit leur somme directe composante par composante : $(M' \oplus M'')_i = M'_i \oplus M''_i$, et leur produit tensoriel comme l'espace vectoriel gradué de composante de degré n : $\bigoplus_{i+j=n} M'_i \otimes M''_j$.

Il est clair que la série de Poincaré d'un espace vectoriel gradué est *additive* et *multiplicative*, i.e. pour une suite exacte $0 \to M' \to M \to M'' \to 0$ d'espaces vectoriels gradués de type fini, les morphismes étant de degré 0, on a $P(M, t) = P(M', t) + P(M'', t)$, et pour M et M' positivement gradués et de type fini, on a $P(M' \otimes_{\mathbb{F}} M'', t) = P(M', t) \cdot P(M'', t)$.

3.2 Théorème de Hilbert-Serre

Théorème 3.2.1. *(Hilbert, Serre) Soit* A *une* $\mathbb{F}$*-algèbre graduée connexe de type fini, engendrée sur* $\mathbb{F}$ *par des éléments homogènes* $x_1, \ldots, x_s$ *de degrés strictement positifs*

$k_1, \ldots, k_s$. Soit M un A-module gradué de type fini. Alors la série de Poincaré $P(M,t)$ est de la forme

$$\frac{f(t)}{\prod_{j=1}^{s}(1-t^{k_j})}$$

où $f(t)$ est un polynôme en t à coefficients entiers.

Démonstration : On démontre le résultat par récurrence sur s. Si $s = 0$, M est un $\mathbb{F}$-espace vectoriel de dimension finie, et $P(M,t)$ est un polynôme. Soit $s > 0$. On suppose le résultat vrai pour tout $i < s$. Soit $\lambda : M \to M$ la multiplication à gauche par $x_s \in A$. On a les suites exactes

$$0 \to ker(\lambda) \to M \to M/ker(\lambda) \to 0$$

$$0 \to Im(\lambda) \to M \to coker(\lambda) \to 0,$$

d'où l'on tire

$$P(M,t) = P(ker(\lambda),t) + P(M/ker(\lambda),t)$$

$$P(M,t) = P(Im(\lambda),t) + P(coker(\lambda),t).$$

λ est un morphisme de degré $d^o(x_s)$, i.e. $\lambda = \{\lambda_j : M_j \to M_{j+d^o(x_s)}\}$, où l'on note M_i la composante homogène de degré i.
D'où

$$(M/ker(\lambda))_j \simeq (Im(\lambda))_{j+d^o(x_s)},$$

puis

$$P(M/ker(\lambda),t) = t^{-d^o(x_s)} P(Im(\lambda),t).$$

En substituant dans les relations précédentes, on trouve

$$P(M,t) = P(ker(\lambda),t) + t^{-d^o(x_s)} P(Im(\lambda),t)$$

$$P(M,t) = P(Im(\lambda),t) + P(M/Im(\lambda),t).$$

En multipliant par $t^{d^o(x_s)}$ la première équation et en soustrayant à la deuxième, on obtient

$$P(M,t) = \frac{-t^{d^o(x_s)}}{1-t^{d^o(x_s)}} P(ker(\lambda),t) + \frac{1}{1-t^{d^o(x_s)}} P(M/Im(\lambda),t).$$

A est noethérien d'après le corollaire 2.2.5, donc M est noethérien car de type fini sur A. On en déduit que les modules $ker(\lambda)$ et $M/Im(\lambda)$ sont noethériens, donc de type fini sur A. L'action de x_s sur ces modules est triviale, ils sont donc de type fini sur la sous-algèbre de A engendrée par $x_1, \ldots, x_{s-1}$. Par hypothèse de récurrence, le membre de droite de l'équation précédente est une fraction rationnelle de la forme voulue.

$\square$

Remarque 3.2.2. *Pour une algèbre de polynômes sur $\mathbb{F}$ engendrée par des éléments $x_1, \ldots, x_n$ de degrés $d_1, \ldots, d_n$ la série de Poincaré est donnée par*

$$P(A,t) = \prod_{i=1}^{n} \frac{1}{1-t^{d_i}}.$$

3.3 Étude du pôle en $t = 1$

L'ordre du pôle de $P(M,t)$ en $t = 1$ peut être mis en relation avec le taux de croissance de la dimension des composantes homogènes. C'est ce que traduit la proposition suivante

Proposition 3.3.1. *Soit $P(t) = \frac{f(t)}{\prod_{j=1}^{s}(1-t^{k_j})} = \sum_{r\geq 0} a_r t^r$, où $f(t)$ est un polynôme à coefficients entiers et les a_i sont des entiers positifs ou nuls. Soit $d(M)$ l'ordre du pôle de $P(t)$ en $t = 1$. Alors*

(i)il existe une constante $\kappa > 0$ telle que $a_n \leq \kappa \cdot n^{d(M)-1}$ pour tout $n > 0$,

mais

(ii)il n'existe aucune constante $\kappa > 0$ telle que $a_n \leq \kappa \cdot n^{d(M)-2}$ pour tout $n > 0$.

Démonstration : Le problème est inchangé si l'on remplace $\frac{1}{(1-t^{k_j})}$ par $\frac{1}{(1-t^{k_j})} \cdot (1 + t + \cdots + t^{k_j - 1})$. On peut donc supposer que chaque $k_j = 1$, et alors $P(t) = f(t)/(1-t)^{d(M)}$, avec $f(1) \neq 0$. On pose $f(t) = \alpha_m t^m + \cdots + \alpha_0$. On a

$$a_n = \alpha_0 \binom{n + d(M) - 1}{d(M) - 1} + \alpha_1 \binom{n + d(M) - 2}{d(M) - 1} + \cdots + \alpha_m \binom{n + d(M) - m - 1}{d(M) - 1}.$$

$f(1) \neq 0$ implique que $\alpha_0 + \cdots + \alpha_m \neq 0$, donc cette expression est un polynôme de degré exactement $d(M) - 1$ en n.

$\square$

On note $d(M)$ l'ordre du pôle en $t = 1$ de $P(M,t)$.

Lemme 3.3.2. *Soit $A \supseteq B$ une extension finie (en tant que B-module) d'algèbres graduées, A et B étant des algèbres de type fini sur $\mathbb{F}$ engendrées par des éléments homogènes de degrés strictement positifs. Alors $d(A) = d(B)$.*

Démonstration : A est un B-module de type fini, donc est un quotient d'un B-module libre de type fini M. Soit $x_1, \ldots, x_n$ une base de M sur B, de degrés $\alpha_1, \ldots, \alpha_n$. $M = Bx_1 \oplus \cdots \oplus Bx_n$, d'où

$$P(M,t) = \sum_i (t^{\alpha_i} P(B,t)) = (\sum_i t^{\alpha_i}) P(B,t).$$

Donc $P(M,t) = f(t)P(B,t)$ pour un certain polynôme $f(t)$ avec $f(1) > 0$. On a ainsi, coefficient par coefficient, $P(B,t) \leq P(A,t) \leq f(t)P(B,t)$, ce qui prouve le lemme.

$\square$

Proposition 3.3.3. $d(\mathbb{F}[V]^G) = \dim_{\mathbb{F}}(V)$.

Démonstration : $\mathbb{F}[V]$ est une extension finie de $\mathbb{F}[V]^G$, donc d'après le lemme 3.3.2, il suffit de regarder le pôle en $t = 1$ de $P(\mathbb{F}[V], t) = 1/(1-t)^n$, où $n = \dim_{\mathbb{F}}(V)$.

$\square$

3.4 Théorème de Molien

On se donne $\rho : G \hookrightarrow GL_n(\mathbb{F})$ une représentation d'un groupe fini G.

On appelle **transfert** l'application $Tr^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ définie par

$$Tr^G(f)(x) = \sum_{g \in G} g(f)(x) = \sum_{g \in G} f(g^{-1}(x)).$$

Pour $g' \in G$, on a

$$g' \cdot Tr^G(f) = \sum_{g'' \in G} g'g''(f) = \sum_{g'g'' \in G} g'g''(f) = Tr^G(f).$$

Donc on a bien $Tr^G(f) \in \mathbb{F}[V]^G$.

On remarque que la composée

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V] \xrightarrow{Tr^G} \mathbb{F}[V]^G$$

est la multiplication par $|G|$; on suppose que $\mathbb{F}$ est de caractéristique nulle, et on note $\pi^G = \frac{1}{|G|} Tr^G : \mathbb{F}[V] \to \mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$. π^G est l'identité sur $\mathbb{F}[V]^G$, et est donc une projection d'image $\mathbb{F}[V]^G$. On a ainsi : $\mathbb{F}[V] = \mathbb{F}[V]^G \oplus ker(\pi^G)$.

La dimension de $\mathbb{F}[V]_j^G$ est donc égale à la trace de la matrice de π^G sur $\mathbb{F}[V]_j$, d'où

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \sum_{j=0}^{\infty} tr(g, \mathbb{F}[V]_j) t^j.$$

La proposition suivante va nous permettre de simplifier cette dernière égalité.

Proposition 3.4.1. *Soit $\mathbb{F}$ un corps de caractéristique nulle, $\rho : G \hookrightarrow GL_n(\mathbb{F})$ une représentation d'un groupe fini G. Si $g \in G$, alors la trace de l'action de g sur $\mathbb{F}[V]$ est donnée par $\sum_{j=0}^{\infty} tr(g, \mathbb{F}[V]_j) t^j = \frac{1}{det(1 - g^{-1}t)}$.*

Démonstration : Étendre le corps ne change aucun des deux membres de l'égalité, donc on peut supposer $\mathbb{F}$ algèbriquement clos. $g \in G$ groupe fini, donc g annule le polynôme $X^{|G|} - 1$, scindé à racines simples car $\mathbb{F}$ est de caractéristique nulle. g est donc diagonalisable, soient $\lambda_1, \ldots, \lambda_n$ ses valeurs propres. Les valeurs propres sur V^* sont $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$, donc les valeurs propres sur $\mathbb{F}[V]_j$ sont les produits de j λ_i^{-1} non nécessairement distincts. On a ainsi en calculant dans une base où g est diagonale

$$\sum_{j=0}^{\infty} tr(g, \mathbb{F}[V]_j)t^j = (\sum_{j=0}^{\infty} \lambda_1^{-j} t^j) \cdots (\sum_{j=0}^{\infty} \lambda_n^{-j} t^j) = \prod_{i=1}^{n} \frac{1}{1-\lambda_i^{-1}t} = \frac{1}{det(1-g^{-1}t)},$$

ce qui prouve la proposition.

□

On en déduit le théorème

Théorème 3.4.2. *(Molien) Soit $\rho : G \hookrightarrow GL_n(\mathbb{F})$ une représentation d'un groupe fini G sur un corps $\mathbb{F}$ de caractéristique nulle. Alors la série de Poincaré de l'anneau des invariants est donnée par*

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{det(1-g^{-1}t)}.$$

□

3.5 Séries de Poincaré et pseudo-réflexions

Définition 3.5.1. *Soit V un espace vectoriel de dimension finie sur un corps $\mathbb{F}$. On dit qu'un automorphisme $s : V \to V$ est une* **pseudo-réflexion** *si $s \neq 1$, l'ordre de s est fini, et s est l'identité sur un hyperplan H_s fixe, appelé* **hyperplan de** *s. $\mathbb{F}$ étant de caractéristique nulle, s est diagonalisable car d'ordre fini. Soit λ_s la valeur propre de s différente de* 1, *appelée* **racine de** *s. λ_s est une racine de l'unité dans $\mathbb{F}$. Si $\lambda_s = -1$, on dit que s est une* **réflexion réelle**, *ou plus simplement une réflexion.*

Soit s une pseudo-réflexion d'hyperplan H_s. $Im(1-s) = vect(x_s)$ est la droite propre de s associée à λ_s. Donc on peut écrire $s(v) = v + l_s(v)x_s$, $\forall v \in V$, où $l_s : V \to \mathbb{F}$ est une forme linéaire de noyau H_s. Pour $f \in \mathbb{F}[V]$ et $u \in H_s$, on a

$$(sf - f)(u) = f(s^{-1}(u)) - f(u) = f(u) - f(u) = 0,$$

d'où l_s divise $sf - f \in \mathbb{F}[V]$.

Définition 3.5.2. *On appelle* **dérivation twistée** *ou* **Δ-opérateur** *associé à s, et on note Δ_s, l'application qui à $f \in \mathbb{F}[V]$ associe le quotient de $sf - f$ par l_s dans $\mathbb{F}[V]$:*

$$sf - f = \Delta_s(f) l_s.$$

$\Delta_s(f) \in \mathbb{F}[V]$ est de degré $d^o(f) - 1$.

Lemme 3.5.3. *Soit $s \in GL_n(\mathbb{F})$ une pseudo-réflexion, S le sous-groupe de $GL_n(\mathbb{F})$ engendré par s, $f \in \mathbb{F}[V]$. Alors $f \in \mathbb{F}[V]^S$ si et seulement si $\Delta_s(f) = 0$.*

□

Ainsi, si $\rho : G \hookrightarrow GL_n(\mathbb{F})$ est une représentation telle que $\rho(G)$ est engendré par des pseudo-réflexions, alors $f \in \mathbb{F}[V]^G$ si et seulement si $\Delta_s(f) = 0$ pour tout $s \in \rho(G)$ pseudo-réflexion.

De plus, Δ_s est $\mathbb{F}[V]^G$-linéaire.

D'après le théorème de Molien, on a

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|}\left\{\frac{1}{det(1-t)} + \sum_{g\neq 1 \in G} \frac{1}{det(1-g^{-1}t)}\right\}.$$

Les $g \neq 1 \in G$ ne peuvent avoir 1 comme valeur propre d'ordre n, donc

$$Q(t) = \sum_{g\neq 1\in G} \frac{1}{det(1-g^{-1}t)}$$

a un pôle en $t = 1$ d'ordre au plus $n-1$. Ainsi, la valeur en $t = 1$ de la fonction $(1-t)^n P(\mathbb{F}[V]^G, t)$ est $1/|G|$.

En introduisant les pseudo-réflexions de G, on peut obtenir plus d'informations sur le développement de Laurent de $P(\mathbb{F}[V]^G, t)$: les éléments de G qui contribuent au pôle d'ordre $n-1$ de $Q(t)$ sont ceux tels que $\dim_{\mathbb{F}}(V^g) = n-1$, c'est à dire exactement les pseudo-réflexions de G. Soit $s(G)$ l'ensemble des pseudo-réflexions de G. Pour $g \in s(G)$, on a

$$\frac{(1-t)^{n-1}}{det(1-g^{-1}t)} = \frac{1}{1-\lambda^{-1}t}.$$

On remarque que si g est une pseudo-réflexion, g^{-1} aussi, et $g = g^{-1}$ exactement quand g est une réflexion réelle. L'égalité $\frac{1}{1-\lambda^{-1}} + \frac{1}{1-\lambda} = 1$ montre que si l'on regroupe chaque pseudo-réflexion non réelle avec son inverse, la contribution au pôle d'ordre $n-1$ des pseudo-réflexions non réelles est exactement la moitié de leur nombre ; les réflexions réelles ayant leur λ égal à -1, elles contribuent aussi pour la moitié de leur nombre. On a ainsi démontré le résultat suivant :

Proposition 3.5.4. *Soient $\mathbb{F}$ un corps de caractéristique nulle et $\rho : G \hookrightarrow GL_n(\mathbb{F})$ une représentation injective de G sur $V = \mathbb{F}^n$, alors le développement de Laurent de la série de Poincaré $P(\mathbb{F}[V]^G, t)$ a pour premiers termes :*

$$P(\mathbb{F}[V]^G, t) = \frac{\frac{1}{|G|}}{(1-t)^n} + \frac{\frac{|s(G)|}{2\cdot|G|}}{(1-t)^{n-1}} + \cdots,$$

où $|s(G)|$ est le nombre de pseudo-réflexions de G dans la représentation ρ.

□

On a aussi le résultat suivant reliant les degrés des générateurs à des informations sur le groupe :

Proposition 3.5.5. *Soit $\rho : G \to GL_n(\mathbb{F})$ une représentation d'un groupe fini G sur un corps $\mathbb{F}$ de caractéristique nulle. On suppose qu'il existe*

$$f_1, \dots, f_n \in \mathbb{F}[V]^G,\ deg(f_i) = d_i,\ \forall i = 1, \dots, n,$$

tels que

$$\text{(i)} \prod_{i=1}^{n} d_i = |G|,$$

$$\text{(ii)} f_1, \dots, f_n \text{ sont algébriquement indépendants.}$$

Alors

$$|s(G)| \geq \sum_{i=1}^{n} (d_i - 1).$$

Démonstration : Les f_i étant algébriquement indépendants, d'après la remarque 3.2.2,

$$P(\mathbb{F}[f_1, \dots, f_n], t) = \frac{1}{\prod_{i=1}^{n} (1 - t^{d_i})}.$$

De $(1 - t^{d_i}) = (1 - t) \sum_{i=0}^{d_i - 1} t^j$, on déduit que

$$(1-t)^n P(\mathbb{F}[f_1, \dots, f_n], t) \underset{t \to 1}{\longrightarrow} \frac{1}{d_1 \cdots d_n}.$$

En vue de calculer le pôle d'ordre $n - 1$, on pose $P_i(t) = \sum_{i=0}^{d_i - 1} t^j$.
On a

$$(1-t)^{n-1} \left(P(\mathbb{F}[f_1, \dots, f_n], t) - \frac{\frac{1}{d_1 \cdots d_n}}{(1-t)^n} \right) = \frac{1}{1-t} \left(\frac{1}{\prod_{i=1}^{n} P_i(t)} - \frac{1}{d_1 \cdots d_n} \right).$$

Or $P_1 \cdots P_n(1) = d_1 \cdots d_n$, d'où

$$\frac{1}{(d_1 \cdots d_n) \prod_{i=1}^{n} P_i(t)} \cdot \left(\frac{d_1 \cdots d_n - \prod_{i=1}^{n} P_i(t)}{1 - t} \right) \underset{t \to 1}{\longrightarrow} \frac{(P_1 \cdots P_n)'(1)}{(d_1 \cdots d_n)^2}.$$

$(P_1 \cdots P_n)'(1) = \sum_{i=1}^{n} P_i' \cdot P_1 \cdots \widehat{P}_i \cdots P_n(1) = \sum_{i=1}^{n} \frac{d_i(d_i - 1)}{2} d_1 \cdots \widehat{d_i} \cdots d_n = (d_1 \cdots d_n) \frac{\sum_{i=1}^{n} d_i - 1}{2}.$
On a ainsi montré que

$$P(\mathbb{F}[f_1, \dots, f_n], t) = \frac{\frac{1}{d_1 \cdots d_n}}{(1-t)^n} + \frac{\frac{\sum_{i=1}^{n} (d_i - 1)}{2 \cdot d_1 \cdots d_n}}{(1-t)^{n-1}} + \cdots.$$

D'après la proposition 3.5.4 et l'hypothèse (i), $P(\mathbb{F}[f_1,\ldots,f_n],t)$ et $P(\mathbb{F}[V]^G,t)$ ont un pôle d'ordre n en $t=1$, et

$$\lim_{t\to 1}(1-t)^n P(\mathbb{F}[V]^G,t) = \frac{1}{|G|} = \frac{1}{d_1\cdots d_n} = \lim_{t\to 1}(1-t)^n P(\mathbb{F}[f_1,\ldots,f_n],t).$$

La différence $\Delta(t) = P(\mathbb{F}[V]^G,t) - P(\mathbb{F}[f_1,\ldots,f_n],t)$ a donc un pôle d'ordre $n-1$ en $t=1$. Puisque $\mathbb{F}[f_1,\ldots,f_n] \subseteq \mathbb{F}[V]^G$, on a, coefficient par coefficient,

$$P(\mathbb{F}[V]^G,t) \geq P(\mathbb{F}[f_1,\ldots,f_n],t).$$

Ainsi $\Delta(t)$ est une série à coefficients entiers positifs ou nuls, et prend par conséquent des valeurs positives pour t réel positif. Il en est de même pour $(1-t)^{n-1}\Delta(t)$ si $0 \leq t \leq 1$. On en déduit

$$0 \leq \lim_{t\to 1}[(1-t)^{n-1}\Delta(t)] = \frac{|s(G)|}{2|G|} - \frac{\sum\limits_{i=1}^{n}(d_i-1)}{2\cdot d_1\cdots d_n} = \frac{1}{2|G|}\left(|s(G)| - \sum_{i=1}^{n}(d_i-1)\right).$$

□

La proposition 3.5.4 donne aussi des informations importantes dans le cas d'une représentation injective pour laquelle l'anneau des invariants $\mathbb{F}[V]^G$ est une algèbre de polynômes :

Proposition 3.5.6. *Soit $\mathbb{F}$ un corps de caractéristique nulle, $G \hookrightarrow GL_n(\mathbb{F})$ une représentation injective d'un groupe fini G.*
Si $\mathbb{F}[V]^G \simeq \mathbb{F}[f_1,\ldots,f_n]$, $deg(f_i) = d_i$, $i=1,\ldots,n$, alors

$$|G| = d_1\cdots d_n,$$

$$|s(G)| = \sum_{i=1}^{n}(d_i-1),$$

où $|s(G)|$ est le nombre de pseudo-réflexions dans G.

Démonstration : On réutilise le calcul fait lors de la démonstration de la précédente proposition :

$$P(\mathbb{F}[V]^G,t) = P(\mathbb{F}[f_1,\ldots,f_n],t) = \frac{\frac{1}{d_1\cdots d_n}}{(1-t)^n} + \frac{\frac{\sum_{i=1}^{n}(d_i-1)}{2\cdot d_1\cdots d_n}}{(1-t)^{n-1}} + \cdots.$$

En identifiant les coefficients de cette expression avec celle donnée par la proposition 3.5.4 , on obtient $|G| = d_1\cdots d_n$, puis $|s(G)| = \sum\limits_{i=1}^{n}(d_i-1)$.

□

4 Homologie et algèbres graduées

4.1 Notions d'homologie algébrique

Dans cette section, on introduit quelques outils d'homologie algébrique. La présentation est trés largement inspirée de [Mat], Appendix B, auquel on se réfèrera pour plus de détails.

4.1.1 Modules projectifs

Définition 4.1.1. *Soit A un anneau commutatif et P un A-module. On dit que P est projectif s'il vérifie les trois propositions équivalentes :*

(i) Pour tout morphisme surjectif de A-modules $f : M \twoheadrightarrow N$ et pour tout morphisme $g : P \to N$, il existe un morphisme $h : P \to M$ tel que le diagramme suivant soit commutatif :

$$\begin{tikzcd} M \arrow[r, "f"] & N \\ P \arrow[u, "h"] \arrow[ur, "g"'] & \end{tikzcd}$$

(ii) Le foncteur $Hom_A(P, -)$ est exact, i.e. pour toute suite exacte de A-modules

$$0 \to L \to M \to N \to 0$$

la suite

$$0 \to Hom_A(P, L) \to Hom_A(P, M) \to Hom_A(P, N) \to 0$$

est aussi exacte.

(iii) Il existe un A-module libre F et un A-module M tel que $P \oplus M = F$.

Soit A un anneau commutatif et M un A-module. Alors il existe K_0 un A-module et P_0 un A-module projectif tels que la suite $0 \to K_0 \to P_0 \to M \to 0$ soit exacte. De même, on peut construire des A-modules K_i et des A-modules projectifs P_i tels que les suites $0 \to K_i \to P_i \to K_{i-1} \to 0$ soient exactes. On alors une suite exacte

$$\cdots \to P_i \to \cdots \to P_1 \to P_0 \to M \to 0.$$

Définition 4.1.2. *Une telle suite est appelée une résolution projective de M.*

Définition 4.1.3. *Soit A un anneau commutatif et M un A-module.*

- *On appelle dimension projective de M, $prdimM$, la longueur minimale d'une résolution de M :*

$$0 \to P_n \to \cdots \to P_i \to \cdots \to P_1 \to P_0 \to M \to 0.$$

- *On appelle dimension globale de A, $gldim(A) = sup_{M \in Mod(A)}(prdim(M))$.*

4.1.2 Foncteur de torsion

Soient M et N deux A-modules, P_* une résolution de M. On note

$$P_* \otimes N : \qquad \cdots \to P_i \otimes N \to \cdots \to P_1 \otimes N \to P_0 \otimes N \to M \otimes N \to 0.$$

On a alors l'homologie $H_n(P_* \otimes N) = \frac{\ker(P_n \otimes N \to P_{n-1} \otimes N)}{Im(P_{n+1} \otimes N \to P_n \otimes N)}$.

Définition 4.1.4. $Tor_n^A(M, N) = H_n(P_* \otimes N)$.

$Tor_n^A(M, N)$ est bien définie malgré la non unicité de P_*.

Proposition 4.1.5. *Soit A un anneau commutatif et M un A-module.*
- *si M est plat (i.e. le foncteur $M \otimes -$ est exact), alors $\forall n > 0$, $Tor_n^A(M, N) = 0$.*
- *$Tor^A(M, N) = Tor^A(N, M)$.*

□

4.1.3 Foncteur Ext

Soient M et N deux A-modules, P_* une résolution de M. On note $Hom(P_*, N)$:

$$0 \to Hom(M, N) \to Hom(P_0, N) \to Hom(P_1, N) \to \cdots \to Hom(P_i, N) \to \cdots.$$

On a alors l'homologie $H_n(Hom(P_*, N))$.

Définition 4.1.6. $Ext_n^A(M, N) = H_n(Hom(P_*, N))$.

$Ext_n^A(M, N)$ est bien définie malgré la non unicité de P_*.

4.2 Lemme de Nakayama

Définition 4.2.1. *Soit A une $\mathbb{F}$-algèbre graduée connexe. On définit son idéal d'augmentation par $\bar{A} = \{a \in A, val(a) > 0\}$. C'est d'ailleurs l'unique idéal gradué maximal de A.*

Définition 4.2.2. *Soit A une $\mathbb{F}$-algèbre graduée connexe et M un A-module gradué. On definit $QM = M/(\bar{A}M)$ le module des éléments indécomposables de M.*

Si A est une $\mathbb{F}$-algèbre graduée connexe, alors $A/\bar{A} \simeq \mathbb{F}$. Ainsi, si M est un A-module gradué, $QM = M/(\bar{A}M) \simeq \mathbb{F} \otimes_A M$.

Proposition 4.2.3 (lemme de Nakayama). *Soit A une $\mathbb{F}$-algèbre graduée connexe et M un A-module gradué positif. Alors $M = 0$ si et seulement si $QM = 0$.*

Démonstration : Si $M = 0$, alors $QM = 0$. Réciproquement, supposons $QM = 0$. Montrons par récurrence sur $s \geq 0$ que $\forall i < s$, $M_i = 0$.

C'est vrai pour $s = 0$. Pour $s \geq 0$, soit $x \in M_s$, comme $QM = 0$, i.e. $M = \bar{A}M$, on a $x = \sum a_i x_i$ avec $a_i \in A$ et $x_i \in M$ homogènes où $d^o(a_i) > 0$ et, par hypothèse de récurrence, $d^o(x_i) \geq s$. D'où $x \in M_s \cap \bigoplus_{j>s} M_j = 0$, et $x = 0$.

□

Corollaire 4.2.4. *Soit A une $\mathbb{F}$-algèbre graduée connexe, M et M' des A-modules positivement gradués et $f : M \to M'$. Alors f est surjective si et seulement si $Qf : QM \to QM'$ est surjective.*

Démonstration : La suite $M \to M' \to coker(f) \to 0$ est exacte. Donc, par application du foncteur $\mathbb{F} \otimes_A -$, la suite $QM \to QM' \to Qcoker(f) \to 0$ est aussi exacte. D'après le lemme de Nakayama, $Qcoker(f) = 0 \iff coker(f) = 0$.

□

4.3 Modules plats, modules projectifs et modules libres

Proposition 4.3.1. *Soit A une algèbre commutative graduée connexe sur un corps $\mathbb{F}$ et M un A-module gradué positif. Les propositions suivantes sont équivalentes :*
(i) M est un A-module libre.
(ii) M est un A-module projectif.
(iii) M est un A-module plat.
(iv) $Tor_1^A(\mathbb{F}, M) = 0$.

Démonstration : $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$ est vrai dans le cadre des anneaux commutatifs. Montrons donc $(iv) \Rightarrow (i)$. Soit $q : M \longrightarrow QM$ la projection canonique et $\sigma : QM \longrightarrow M$ une section de $\mathbb{F}$-espaces vectoriels gradués. Soit $\phi : A \otimes_{\mathbb{F}} QM \longrightarrow M$, le morphisme de A-modules défini par $\phi(a \otimes v) = a \cdot \sigma(v)$. Alors $Q(A \otimes_{\mathbb{F}} QM) \simeq QM$ par $Q\phi$. En effet, $Q\phi(\overline{1 \otimes v}) = q \circ \sigma(v) = v$, donc $Q\phi$ est surjective et si

$$\phi(\sum a \otimes v) = \sum a\sigma(v) \in \bar{A}M$$

alors

$$q \circ \phi(\sum a \otimes v) = 0 = \sum q(a\sigma(v)) = \sum_{a \in \mathbb{F}} av$$

et

$$\overline{\sum a \otimes v} = \sum_{a \in \mathbb{F}} \overline{a \otimes v} = \overline{\sum_{a \in \mathbb{F}} 1 \otimes av} = \overline{1 \otimes \sum_{a \in \mathbb{F}} av} = 0$$

et $Q\phi$ est injective.

D'après le corollaire du lemme de Nakayama ϕ est surjective et on a une suite exacte :

$$0 \to K \to A \otimes_{\mathbb{F}} QM \to M \to 0$$

que l'on peut prolonger en une résolution projective de QM :

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r] & P_1 \arrow[rr] \arrow[dr] & & A \otimes_{\mathbb{F}} QM \arrow[r] & QM \arrow[r] & 0 \\
& & & K \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

En appliquant le foncteur $\mathbb{F} \otimes_A -$ et comme $Tor_1^A(\mathbb{F}, M) = 0$, on voit aisément que la suite

$$0 \to QK \to Q(A \otimes_{\mathbb{F}} QM) \to QM \to 0$$

est aussi exacte et $QK = 0$ i.e. $K = 0$ par le lemme de Nakayama.

□

5 Algèbres graduées et dimension globale

5.1 Complexe de Koszul

Définition 5.1.1. *Soit A une $\mathbb{F}$-algèbre commutative et $a_1, \ldots, a_n \in A$. On définit le complexe de Koszul de A par rapport aux a_i comme l'algèbre commutative graduée différentielle*

$$\mathcal{K} = \mathcal{K}(a_1, \ldots, a_n) = A \otimes_{\mathbb{F}} \Lambda(\oplus_{i=1}^n \mathbb{F}\tilde{a}_i)$$

où $\Lambda(\oplus_{i=1}^n \mathbb{F}\tilde{a}_i)$ est l'algèbre extérieure de $\oplus_{i=1}^n \mathbb{F}\tilde{a}_i$ et où la différentielle d est définie par :

$$d(\tilde{a}_i) = a_i$$

$$d(x \wedge y) = d(x) \wedge y + (-1)^{deg(x)} x \wedge d(y).$$

Définition 5.1.2. *Soit A un anneau commutatif et $a_1, \ldots, a_n \in A$. La suite $a_1, \ldots, a_n$ est dite régulière si a_1 est régulier (i.e. la multiplication par a_1 est injective) et si les a_i sont réguliers dans $A/(a_1, \ldots, a_{i-1})$.*

Théorème 5.1.3. *Soit A une $\mathbb{F}$-algèbre commutative graduée connexe et $a_1, \ldots, a_n \in A$. Le complexe de Koszul $\mathcal{K}(a_1, \ldots, a_n)$ est acyclique si et seulement si la suite $(a_1, \ldots, a_n)$ est régulière.*

Démonstration : Notons $\mathcal{K}(i) = \mathcal{K}(a_1, \ldots, a_i)$ et $\mathcal{K}(0) = A$. On a la suite exacte de complexes

$$0 \to \mathcal{K}(i-1) \hookrightarrow \mathcal{K}(i) \to \mathcal{K}(i-1) \to 0$$

où la dernière flèche diminue le degré de un. On a alors la suite exacte longue

$$\cdots \to H_j(\mathcal{K}(i-1)) \to H_j(\mathcal{K}(i)) \to H_{j-1}(\mathcal{K}(i-1)) \to H_{j-1}(\mathcal{K}(i-1)) \to \cdots.$$

Il suffit donc de montrer que les $H_1(\mathcal{K}(i))$ sont nuls si et seulement si la suite (a_i) est régulière. Supposons donc la suite régulière. On a $H_1(\mathcal{K}(1)) = 0$. Soient $j \leq n$ et $\sum_{i \leq j} \alpha_i \tilde{a}_i$ de différentielle nulle. Si $\alpha_j = 0$, alors, par récurrence, $\sum \alpha_i \tilde{a}_i \in Im(d)$. Sinon, $\alpha_j a_j \in (a_1, \ldots, a_{j-1})$ i.e. $\alpha_j \in (a_1, \ldots, a_{j-1})$ et $\alpha_j = \sum_{i<j} \beta_i a_i$. Or $d(\sum_{i<j} \beta_i \tilde{a}_i \wedge \tilde{a}_j) = \alpha_j \tilde{a}_j + \sum_{i<j} \gamma_i \tilde{a}_i$ et par récurrence $\sum \gamma_i \tilde{a}_i \in Im(d)$ i.e. $H_1(\mathcal{K}(i)) = 0$. Réciproquement, si les $H_1(\mathcal{K}(i))$ sont nuls, alors

$$\sum_{i<j} -\alpha_i a_i = \alpha_j a_j \Rightarrow \sum \alpha_i \tilde{a}_i \in Im(d) \Rightarrow \alpha_j \in (a_1, \ldots, a_{j-1})$$

i.e. la suite est régulière.

□

Corollaire 5.1.4 (Théorème de Koszul). *Soit A une $\mathbb{F}$-algèbre commutative graduée connexe et $a_1, \ldots, a_n \in A$ une suite régulière. Alors $\mathcal{K}(a_1, \ldots, a_n)$ est une résolution de $A/(a_1, \ldots, a_n)$ comme A-module.*

□

5.2 Théorème de Hilbert des *syzygies*

Théorème 5.2.1 (Théorème de Hilbert des *syzygies*). *Soit M un module sur l'algèbre de polynômes $\mathbb{F}[z_1, \ldots, z_n]$. Alors la dimension projective de M est au plus n.*

Démonstration : Notons $A = \mathbb{F}[z_1, \ldots, z_n]$. Soit M un A-module et $N = A \otimes_{\mathbb{F}} M$ que l'on munit d'une structure de A-module par :

$$z_i \cdot (a \otimes m) = (z_i a) \otimes m + a \otimes (z_i m).$$

Alors N est un A-module libre car si $(m_i)_{i \in I}$ est une base de M comme $\mathbb{F}$-espace vectoriel, alors $(1 \otimes m_i)_{i \in I}$ est une base de N comme A-module.

Le complexe de Koszul

$$\mathcal{K} = \Lambda(\oplus_{i=1}^n \mathbb{F}\tilde{z}_i) \otimes_{\mathbb{F}} N$$

$$\partial(\tilde{z}_{i_1} \wedge \ldots \wedge \tilde{z}_{i_k} \otimes m) = \sum (-1)^j \tilde{z}_{i_1} \wedge \ldots \wedge \widehat{\tilde{z}_{i_j}} \wedge \ldots \wedge \tilde{z}_{i_k} \otimes z_{i_j} m$$

fournit alors une résolution libre de M comme A-module.

□

Proposition 5.2.2. *Soit A une $\mathbb{F}$-algèbre commutative graduée connexe, M un A-module et $n \in \mathbb{N}$. Alors les quatre propositions suivantes sont équivalentes :*

(i) $prdim M \leq n$.

(ii) $Ext_A^{n+1}(M, -) = 0$.

(iii) $Ext_A^n(M, -)$ est exact à droite.

(iv) Pour toute suite exacte

$$0 \to K_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

où les P_i sont projectifs, alors K_n est projectif.

Démonstration : Les implications $(iv) \Rightarrow (i) \Rightarrow (ii) \Rightarrow (iii)$ sont claires. Supposons (iii) et montrons que $Hom(K_n, -)$ est exact. Soit

$$0 \to N' \to N \to N'' \to 0$$

une suite exacte de A-modules.

On peut décomposer la longue suite exacte (iv) en suites exactes courtes :

$$
\begin{tikzcd}[column sep=small]
 & & & 0 \arrow[dr] & & 0 & & & 0 \arrow[dr] & & 0 & & \\
 & & & & K_{n-1} \arrow[ur] \arrow[dr] & & & \cdots & & K_1 \arrow[ur] \arrow[dr] & & & \\
0 \arrow[r] & K_n \arrow[rr] \arrow[dr, "\simeq"'] & & P_{n-1} \arrow[rr] \arrow[ur] & & P_{n-2} \arrow[rr] \arrow[dr] & & \cdots\cdots \arrow[r] & P_1 \arrow[rr] \arrow[ur] & & P_0 \arrow[r] & M \arrow[r] & 0 \\
 & & K_n \arrow[ur] \arrow[dr] & & & & K_{n-2} \arrow[dr] & & & & & & \\
 & 0 \arrow[ur] & & 0 & & 0 \arrow[ur] & & 0 & & & & &
\end{tikzcd}
$$

De plus, la suite

$$Hom_A(P_{n-1}, N) \to Hom_A(K_n, N) \to Ext_A^n(M, N) \to 0 \qquad (*)$$

est exacte. En effet, on a :

$$Ext_A^n(M, N) = \frac{\ker Hom_A(P_n, N) \to Hom_A(P_{n+1}, N)}{Im(Hom_A(P_{n-1}, N) \to Hom_A(P_n, N))}.$$

Soit $f : P_n \to N$ telle que

$$
\begin{tikzcd}
P_{n+1} \arrow[r] \arrow[dr, "0"'] & P_n \arrow[d, "f"'] \\
 & N
\end{tikzcd}
$$

alors $K_{n+1} \subset \ker f$ et on peut factoriser f :

$$
\begin{tikzcd}
\frac{P_n}{K_{n+1}} \arrow[r, "\simeq"] \arrow[d, "\tilde{f}"'] & K_n \arrow[dl] \\
N &
\end{tikzcd}
$$

D'où $Hom(K_n, N) \twoheadrightarrow Ext_A^n(M, N)$.

Soit $f : K_n \to N$ telle qu'il existe $g : P_{n-1} \to N$ factorisant $\tilde{f} : P_n \to K_n \xrightarrow{f} N$:

$$
\begin{tikzcd}
P_n \arrow[rr] \arrow[dr] \arrow[dd, "\tilde{f}"'] & & P_{n-1} \arrow[ddll, bend left, "g"] \\
 & K_n \arrow[ur] \arrow[dl, "f"'] & \\
N & &
\end{tikzcd}
$$

Alors g factorise aussi f et la suite $(*)$ est exacte.

On a alors le diagramme commutatif suivant :

$$\begin{tikzcd}
Hom_A(P_{n-1},N) \arrow[r] \arrow[d] & Hom_A(K_n,N) \arrow[r] \arrow[d] & Ext^n_A(M,N) \arrow[r] \arrow[d] & 0 \\
Hom_A(P_{n-1},N'') \arrow[r] & Hom_A(K_n,N'') \arrow[r] & Ext^n_A(M,N'') \arrow[r] & 0
\end{tikzcd}$$

Les première et troisième flèches verticales sont surjectives car P_{n-1} est projectif et $Ext^n_A(M,-)$ est exact à droite ; on voit alors aisement que la flèche du milieu est surjective.

□

5.3 Théorème de Serre

Théorème 5.3.1 (Théorème de Serre). *Soit A une algèbre commutative graduée connexe sur un corps $\mathbb{F}$. Alors si $gldim\, A = d < \infty$, on a $A \simeq \mathbb{F}[z_1, \ldots, z_d]$.*

Démonstration : voir [Smi] 6.4.3.

□

Corollaire 5.3.2. *Soit $A \subset \mathbb{F}[z_1, \ldots, z_d]$ une sous-algèbre graduée de l'algèbre graduée polynomiale $\mathbb{F}[z_1, \ldots, z_d]$. Si $\mathbb{F}[z_1, \ldots, z_d]$ est un A-module libre, alors $A = \mathbb{F}[f_1, \ldots, f_k]$.*

Démonstration : D'après le théorème de Serre, il suffit de montrer que $gldim\, A < \infty$. Notons $S = \mathbb{F}[z_1, \ldots, z_d]$. Soit M un A-module et

$$0 \to K_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0$$

une résolution projective partielle de M, i.e. les P_i sont projectifs. Comme S est un A-module libre, le foncteur $- \otimes_A S$ est exact et envoie les modules projectifs sur les modules projectifs. Ainsi la suite

$$0 \to K_n \otimes_A S \to P_{n-1} \otimes_A S \to \ldots \to P_0 \otimes_A S \to M \otimes_A S \to 0$$

est exacte et les $P_i \otimes_A S$ sont projectifs. D'après 5.2.2, $K_n \otimes_A S$ est un S-module projectif, car d'après le théorème de Hilbert des *syzygies*, $gldim\, S \leq n$. De plus, S est un A-module libre, donc $K_n \otimes_A S$ est un A-module projectif, et $S = A \oplus_A L$ d'où $K_n = K_n \otimes_A A$ est un facteur direct du A-module projectif $K_n \otimes_A S$. On en conclut que K_n est un A-module projectif.

□

6 Théorème de Shephard-Todd

6.1 Choix de polynômes homogènes

Lemme 6.1.1. *Soit $\mathbb{F}$ un corps de caractéristique nulle, A une $\mathbb{F}$-algèbre graduée. On suppose que A est isomorphe à une algèbre de polynômes. Alors il existe $g_1, \ldots, g_n$ polynômes homogènes générateurs de A, algébriquement indépendants.*

Démonstration : Soient $f_1, \ldots, f_n$ algébriquement indépendants engendrant A : $A = \mathbb{F}[f_1, \ldots, f_n]$. On peut supposer $val(f_i) = n_i > 0\ \forall i$, car les constantes sont dans le corps. $A = \bigoplus_{m \geq 0} A_m$. Soit $\bar{A} = \bigoplus_{m>0} A_m = (f_1, \ldots, f_n)$ l'idéal d'augmentation de A. $\bar{A}$ et $\bar{A}\bar{A}$ sont gradués. Comme on le voit composante homogène par composante homogène, $\bar{A}\bar{A}$ admet un supplémentaire gradué dans $\bar{A}$, de dimension $\dim_{\mathbb{F}}(\bar{A}_{/\bar{A}\bar{A}}) = n$. Soit $g_1, \ldots, g_n$ une base graduée d'un supplémentaire V de $\bar{A}\bar{A}$ dans $\bar{A}$, i.e. une base constituée de polynômes homogènes (on peut par exemple l'extraire de la famille des composantes homogènes d'une base quelconque).

Montrons que A est engendrée par V : $\bar{A} = V \oplus \bar{A}\bar{A}$; or

$$\bar{A}\bar{A} \supset VV + \bar{A}\bar{A}\bar{A},$$

$$\bar{A}\bar{A} \subset \bar{A}V + \bar{A}\bar{A}\bar{A} \subset (V + \bar{A}\bar{A})V + \bar{A}\bar{A}\bar{A} = VV + \bar{A}\bar{A}\bar{A},$$

d'où

$$\bar{A}\bar{A} = VV + \bar{A}\bar{A}\bar{A}.$$

Ainsi

$$\bar{A} = V + V^2 + V^3 + \cdots + V^n + (\bar{A})^{n+1}$$

par récurrence.

Si un polynôme est de degré $m > 0$, il est dans $V + V^2 + V^3 + \cdots + V^m$, car $A_m = V_m + (V^2)_m + \cdots + (V^m)_m + ((\bar{A})^{m+1})_m$, et $((\bar{A})^{m+1})_m = 0$. Donc A est engendré par V.

De même que pour $k = 2$, $\dim_{\mathbb{F}}(\bar{A}_{/(\bar{A})^k})$ est le nombre de monômes unitaires en n variables parmi les f_i de degré entre 1 et $k-1$. Or les monômes en n variables parmi les g_i engendrent aussi $\bar{A}_{/(\bar{A})^k}$. $A = \mathbb{F}[g_1, \ldots, g_n], \bar{A} = (g_1, \ldots, g_n) = \sum_{i=1}^{n} g_i A$; de même $(\bar{A})^2 = \sum_{i,j} g_i g_j A$, et ainsi de suite. Il y a le même nombre de monômes que la dimension de $\bar{A}_{/(\bar{A})^k}$, et ils engendrent, donc ils sont libres, et ce pour tout k, ce qui équivaut au fait que les g_i sont algébriquement indépendants.

$\square$

6.2 Théorème de Shephard-Todd

Théorème 6.2.1. *(Shephard-Todd, Chevalley) Soit $\mathbb{F}$ un corps de caractéristique nulle, V un $\mathbb{F}$-espace vectoriel de dimension finie et $\rho : G \hookrightarrow GL(V)$ une représentation d'un groupe G fini. Alors les assertions suivantes sont équivalentes :*

(i) G est engendré par des pseudo-réflexions,

(ii) $\mathbb{F}[V]^G$ est une algèbre de polynômes.

Démonstration : $(i) \Rightarrow (ii)$ On suppose que G est engendré par des pseudo-réflexions dans la représentation ρ. D'après le corollaire 5.3.2, il suffit de montrer que $\mathbb{F}[V]$ est un $\mathbb{F}[V]^G$-module libre pour conclure que $\mathbb{F}[V]^G$ est une algèbre de polynômes. Cela revient à montrer, d'après la proposition 4.3.1, que $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]) = 0$.

L'action de G sur $\mathbb{F}[V]$ induit une action sur $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V])$. Par définition de Δ_s, on a

$$s(f) - f = l_s \Delta_s(f) \qquad \forall f \in \mathbb{F}[V].$$

Δ_s est un endomorphisme $\mathbb{F}[V]^G$-linéaire de $\mathbb{F}[V]$, ainsi

$$s(\zeta) - \zeta = l_s \cdot Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \Delta_s)(\zeta) \qquad \forall \zeta \in Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]).$$

Supposons $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V])$ non nul. Soit ζ un élément non nul de degré minimal dans $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V])$; Δ_s diminue le degré de 1, donc $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \Delta_s)(\zeta) = 0$. On en déduit que $s(\zeta) = \zeta$ pour toute pseudo-réflexion $s \in G$. G étant engendré par les pseudo-réflexions, ζ est G-invariant.

Si M est un G-module, l'action de G sur M induit une action de G sur $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, M)$. On note $i : \mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$, morphisme de G-modules, où G agit trivialement sur $\mathbb{F}[V]^G$. L'application π^G introduite en 3.4 est un morphisme de $\mathbb{F}[V]^G$-module de $\mathbb{F}[V]$ dans $\mathbb{F}[V]^G$. On a donc les morphismes induits

$$\begin{tikzcd}
Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]) \arrow[dr, "Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \pi^G)"] & & \\
& Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]^G) \arrow[dr, "Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, i)"] & \\
& & Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]).
\end{tikzcd}$$

La composée $i \cdot \pi^G$ est l'identité sur $\mathbb{F}[V]^G$. Donc

$$\zeta = Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, i) \cdot Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \pi^G)(\zeta) = 0,$$

car

$$Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]^G) = 0$$

puisque $\mathbb{F}[V]^G$ est un module libre sur lui-même. On a ainsi une contradiction, et $Tor_1^{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]^G) = 0$.

$(ii) \Rightarrow (i)$ On suppose que $\mathbb{F}[V]^G$ est une algèbre de polynômes, et on choisit $f_1, \ldots, f_n$ polynômes homogènes de degrés $d_1 \leq \cdots \leq d_n$ algébriquement indépendants engendrant $\mathbb{F}[V]^G$. Soit $H < G$ le sous-groupe de G engendré par $s(G)$, l'ensemble des pseudo-réflexions de G. D'après la première implication du théorème, $\mathbb{F}[V]^H$ est aussi une algèbre de polynômes. Soient $h_1, \ldots, h_m$ polynômes homogènes de degrés $e_1 \leq \cdots \leq e_m$ algébriquement indépendants engendrant $\mathbb{F}[V]^H$. En fait $m = n$, car d'après la proposition 3.3.3, $n = d(\mathbb{F}[V]^G) = \dim_{\mathbb{F}}(V) = d(\mathbb{F}[V]^H) = m$. On a pour $i = 1, \ldots, n$, $f_i \in \mathbb{F}[h_1, \ldots, h_n]$. De plus, grâce à la proposition 3.5.6, on a

$$\begin{array}{ll} |G| = d_1 \cdots d_n & s(G) = \sum_{i=1}^n (d_i - 1) \\ |H| = e_1 \cdots e_n & s(H) = \sum_{i=1}^n (e_i - 1). \end{array}$$

Montrons que $d_i \geq e_i$ pour $i = 1, \ldots, n$. Cest clair pour $i = 1$. On suppose que $d_i \geq e_i$ pour $i = 1, \ldots, m$; si $d_{m+1} < e_{m+1}$, alors f_{m+1} est un polynôme en $h_1, \ldots, h_m$. De même, puisque $d_i \leq d_{m+1} < e_{m+1}$ pour $i = 1, \ldots, m$, $f_1, \ldots, f_m$ sont dans $\mathbb{F}[h_1, \ldots, h_m]$.
On pose

$$\frac{1}{\prod_{i=1}^{m} (1 - t^{e_i})} = \sum_{i=1}^{\infty} a_i t^i,$$

$$\frac{1}{\prod_{i=1}^{m} (1 - t^{d_i})} = \sum_{i=1}^{\infty} b_i t^i.$$

Les f_i, $i = 1, \ldots, m+1$ sont algébriquement indépendants et sont dans $\mathbb{F}[h_1, \ldots, h_m]$; on en déduit : $a_n \geq b_n$, $\forall n \geq 0$. D'après la proposition 3.3.1, il existe $\kappa > 0$ tel que $b_n \leq a_n \leq \kappa \cdot n^{m-1}$, $\forall n > 0$, car $m = d(\mathbb{F}[h_1, \ldots, h_m])$. Or $m + 1 = d(\mathbb{F}[f_1, \ldots, f_{m+1}])$, ce qui aboutit à une contradiction par la proposition 3.3.1. Donc $d_i \geq e_i$, $\forall i$.

G et H ayant les mêmes pseudo-réflexions, on a

$$\sum_{i=1}^{n} (d_i - 1) = \sum_{i=1}^{n} (e_i - 1),$$

d'où $d_i = e_i$, $\forall i$. Ainsi $|G| = d_1 \cdots d_n = e_1 \cdots e_n = |H|$, d'où $G = H$ et G est engendré par des pseudo-réflexions.

$\square$

Références

[Lan] **S. Lang**
Algebra Addison Wesley 3^{rd} ed. (1994).

[Mac] **S. Mac Lane**
Homology Springer (1966).

[Mat] **H. Matsumura**
Commutative Ring Theory Cambridge University Press (1986).

[Smi] **L. Smith**
Polynomial Invariants of Finite Groups Research Notes In Math. (1995).