Université de Montréal

COEFFICIENTS DE LAURENT DE LA SÉRIE DE HILBERT

par

Aziz Raymond Elmahdaoui

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

Orientation mathématiques fondamentales

novembre 2006

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

COEFFICIENTS DE LAURENT DE LA SÉRIE DE HILBERT

présenté par

Aziz Raymond Elmahdaoui

a été évalué par un jury composé des personnes suivantes :

Prof. Pavel Winternitz

(président-rapporteur)

Prof. Abraham Broer

(directeur de recherche)

Prof. Jiri Patera

(membre du jury)

Mémoire accepté le:

8 novembre 2006

SOMMAIRE

Si un groupe agit linéairement sur un espace vectoriel V de dimension finie sur le corps K, cela induit une action sur l'anneau $K[V]$ des fonctions polynomiales sur V en préservant le degré de ces fonctions.

Il est en général difficile de trouver les polynômes invariants pour une telle action. Ces polynômes forment une K-algèbre graduée notée $K[V]^G$. De plus, si on fixe un entier i et que nous considérons seulement les invariants homogènes de degré i, ceux-ci forment un espace vectoriel de dimension finie sur K, noté $K[V]_i^G$. Ainsi, un outils largement utilisé dans l'analyse de ces invariants est la série de Hilbert :

$$\mathcal{H}(K[V]^G, t) = \sum_{i=0}^{\infty} dim_K(K[V]_i^G)t^i.$$

Une approche récemment étudiée consiste à considérer l'expansion de Laurent de la série de Hilbert autour de $t = 1$. Nous pouvons ainsi réécrire la série de Hilbert comme

$$\mathcal{H}(K[V]^G, t) = \sum_{i=0}^{\infty} \frac{\psi_i(K[V]^G)}{(1-t)^{n-i}}$$

pour un certain entier n. Dans ce mémoire, nous discutons des coefficients $\psi_i(K[V]^G)$.

Nous montrons quelques résultats qui ne sont pas dans la littérature. Par exemple, au corollaire 2.5.3, nous donnons une formule pour $\psi_2(\mathbb{C}[V]^G)$ lorsque G est un sous-groupe fini de $SL(V)$. Nous montrons également au corollaire 3.3.1 que $\psi_1(K[V]^G) = \psi_2(K[V]^G) = 0$ lorsque G ne possède ni réflexions ni 2-réflexions, à condition que $K[V]^G$ soit un domaine de factorisation unique (et ce, peu importe la caractéristique de K). Dans la proposition 3.4.1, nous réussissons à annuler plusieurs $\psi_i(K[V]^G)$ lorsque G est un p-groupe. Finalement, le théorème 3.2.11

est une généralisation de la conjecture de Carlisle-Kropholler (cette conjecture avait été démontrée par Benson et Crawley-Boevey dans [**Ben2**]).

Mots clés : Théorie des invariants, série de Hilbert, coefficients de Laurent, formule de Molien, cas modulaire, ramification, différent.

SUMMARY

A linear action of a group on a finite dimensional vector space V over a field K induces an action of the group on the ring $K[V]$ of polynomial functions on V. This action preserves the degree of the functions.

In general, it is difficult to find the polynomial invariants for such an action. Those invariants form a graded K-algebra denoted by $K[V]^G$. Furthermore, for a fixed integer i, the set $K[V]_i^G$ of homogeneous invariants of degree i is a finite dimensional vector space over K. Thus, we can define the Hilbert series :

$$\mathcal{H}(K[V]^G, t) = \sum_{i=0}^{\infty} dim_K(K[V]_i^G)t^i.$$

Some recent research is dedicated to the Laurent expansion of the Hilbert series centered at $t = 1$. We can indeed rewrite the Hilbert series :

$$\mathcal{H}(K[V]^G, t) = \sum_{i=0}^{\infty} \frac{\psi_i(K[V]^G)}{(1-t)^{n-i}}$$

for some integer n. In this master's thesis, we discuss the coefficients $\psi_i(K[V]^G)$.

Some results in this thesis cannot be found in the literature. For example, corollary 2.5.3 gives a formula for $\psi_2(\mathbb{C}[V]^G)$ whenever G is a finite subgroup of $SL(V)$. We also show in corollary 3.3.1 that $\psi_1(K[V]^G) = \psi_2(K[V]^G) = 0$ if G has no reflections and no 2-reflections, given that $K[V]^G$ is a UFD (with no condition on the characteristic of K). In proposition 3.4.1, we give conditions on i for which $\psi_i(K[V]^G) = 0$ when G is a p-group. Finally, theorem 3.2.11 is a generalisation of the Carlisle-Kropholler conjecture (the conjecture was proved by Benson and Crawley-Boevey in [**Ben2**]).

Keywords : Invariant theory, Hilbert series, Laurent coefficients, Molien formula, modular case, ramification, different.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

REMERCIEMENTS

Je tiens à remercier, d'abord et avant tout, mon directeur M. Abraham Broer pour sa grande patience et sa disponibilité, ainsi que pour ses judicieux conseils. Il a également réussi à me trouver un sujet qui a pu me passionner (et m'occuper) pour toute la durée de ma maîtrise. Malgré l'intérêt suscité par ce sujet, une maîtrise ne serait pas une maîtrise sans ses moments difficiles. Pour cette raison, je remercie M. Broer également pour son support moral et ses encouragements durant ces moments.

Je tiens également à remercier les organismes gouvernementaux du CRSNG (Conseil de recherches en sciences naturelles et en génie du Canada) et du FQRNT (Fonds québecois de la recherche sur la nature et les technologies) pour m'avoir permis, par leur support financier considérable, de me concentrer pleinement sur mes études sans aucun soucis provenant de l'extérieur.

PRÉLIMINAIRES

Nous prenons pour acquis que le lecteur est familier avec les définitions et les théorèmes de base en théorie des groupes, anneaux et modules, incluant la définition de groupe de Galois. Nous rappelons dans cette section certaines définitions dont nous nous servirons tout au long du mémoire. Par exemple, les notions d'anneaux et de modules gradués. Prenez note que, pour nous, le terme «anneau» désigne un anneau commutatif possédant un neutre pour la multiplication.

Définition 0.0.1. *Un anneau R est dit un* **anneau gradué** *si on peut écrire $R = \bigoplus_{i=-\infty}^{\infty} R_i$ de telle sorte que $R_i R_j \subseteq R_{i+j}$. On dit que R est une K-**algèbre graduée** (pour un corps K) si, de plus, chacun des R_i est un K-espace vectoriel. R est* **positivement gradué** *si $R_i = 0$ pour $i < 0$.*

*Pour un anneau gradué R, on définit un R-**module gradué** comme étant un R-module $M = \bigoplus_{i=-\infty}^{\infty} M_i$ tel que $R_i M_j \subseteq M_{i+j}$.*

Les éléments de M_j sont appelés les éléments de degré j.

Si M est un R-module gradué, nous écrivons $M[d]$ pour le module qui a tous les degrés décalés de d, c'est-à-dire que $M[d]_j = M_{d+j}$ pour tous les entiers j.

Par exemple, l'ensemble $R = K[x_1, \ldots, x_n]$ des polynômes en $x_1, \ldots, x_n$ est un exemple de K-algèbre positivement graduée où R_i est l'ensemble des polynômes homogènes de degré i. R est aussi un R-module gradué.

De plus, nous verrons que l'ensemble des polynômes invariants est lui aussi un exemple d'algèbre graduée en graduant par le degré comme dans le cas de $K[x_1, \ldots, x_n]$.

Puisque nous travaillons généralement avec des polynômes, nous introduisons certaines notations spécifiques aux polynômes. $K[x_1, \ldots, x_n]$ est l'anneau des polynômes en $x_1, \ldots, x_n$. Le degré d'un monôme $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ est $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Le degré d'un polynôme f (noté $deg(f)$) est le maximum des degrés des monômes de f. Le polynôme f est dit **homogène** de degré d si tous les monômes de f sont de degré d. L'ensemble de tous les polynômes homogènes de degré d est noté $K[x_1, \ldots, x_n]_d$. Finalement, si R est un sous-anneau de $K[x_1, \ldots, x_n]$, un idéal de R est appelé homogène si on peut choisir ses générateurs de telle sorte qu'ils soient tous homogènes.

Soit R un anneau. Un R-module M est dit **noethérien** si tous les sous-modules de M sont finiment engendrés ou, de manière équivalente, si toute suite croissante

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$$

de sous-modules de M est stationnaire (c'est-à-dire qu'il existe un nombre k tel que $N_k = N_{k+1} = N_{k+2} = \cdots$).

Un anneau R est dit **noethérien** s'il est noethérien comme R-module. Autrement dit, tout idéal de R est finiment engendré ou encore toute suite croissante d'idéaux de R est stationnaire.

Exemple 0.1. *Quelques exemples classiques d'anneaux noethériens :*

(1) Les corps sont noethériens puisque leurs seuls idéaux sont (0) *et* (1).

(2) $\mathbb{Z}$ est noethérien car c'est un anneau principal, c'est-à-dire que chaque idéal de $\mathbb{Z}$ est engendré par un seul élément.

(3) $K[x_1, \ldots, x_n]$ est noethérien. Voir théorème 1.3.3.

(4) Si R est noethérien, $R \oplus R$ l'est également. Donc, toute somme directe d'un nombre fini de copies de R est un anneau noethérien.

Finalement, nous utilisons dans ce mémoire le vocabulaire de la théorie des représentations. Il faut donc savoir que, pour un groupe G et un espace vectoriel V sur un corps K, un homomorphisme de groupes $\rho : G \longrightarrow GL(V)$ est appelé une **représentation** de G sur V. Cette représentation est dite **fidèle** si ρ est injectif. On dit alors que G agit fidèlement sur V. Lorsque la représentation est claire par le contexte, il arrive parfois d'écrire g au lieu de $\rho(g)$, si $g \in G$. Par exemple, il est évident que $det(g)$ désigne le déterminant de $\rho(g)$.

Nous appelons **action linéaire** de G sur V le fait de munir G d'une action sur V de telle sorte que pour tout $g \in G$, $v, w \in V$ et $k \in K$

(1) $g \cdot (v + w) = g \cdot v + g \cdot w$,

(2) $k(g \cdot v) = g \cdot (kv)$.

En fait, il y a correspondance biunivoque entre les représentations du groupe G sur V et les actions linéaires de G sur V. En effet, si ρ est une représentation, $g \cdot v = \rho(g)v$ détermine une action linéaire. De plus, pour une action linéaire donnée, chaque $g \in G$ agit comme une application linéaire de V, ce qui donne un homomorphisme entre G et $GL(V)$.

Si le groupe G est fini (et muni d'une représentation), nous distinguons deux cas. Le cas **modulaire** est le cas où la caractéristique du corps K divise l'ordre du groupe. Sinon, nous disons que nous sommes dans le cas **non modulaire** (qui comprend par exemple le cas où la caractéristique est 0).

INTRODUCTION

La théorie des invariants étudie les propriétés de l'anneau des polynômes invariants pour une action de groupe linéaire donnée. Dans ce mémoire, nous considérons seulement le cas où G est un groupe fini muni d'une représentation sur un espace vectoriel V de dimension finie sur le corps K. G agit également sur l'anneau $K[V]$ des fonctions poynomiales définies sur V. Nous dénoterons les invariants d'une telle action par $K[V]^G$.

Par exemple, si nous considérons le groupe $\mathbb{S}_n$ des permutations qui agit sur les polynômes à n variables en permutant les variables, les invariants sont alors appelés les polynômes symétriques. Un résultat classique d'algèbre stipule que les polynômes symétriques forment une algèbre polynomiale. Autrement dit, les polynômes symétriques sont engendrés, comme K-algèbre, par n générateurs algébriquement indépendants (nous les donnons explicitement dans l'exemple 1.1).

Cependant, les polynômes invariants ne forment pas toujours une algèbre polynomiale. Autrement dit, en général, les générateurs possèdent des relations algébriques entre eux. La structure de l'algèbre des invariants est alors plus complexe. Il existe par contre certains outils permettant de trouver des informations sur cette structure. Un de ces outils est la série de Hilbert :

$$\mathcal{H}(K[V]^G, t) = \sum_{i=0}^{\infty} dim_K(K[V]_i^G)t^i,$$

où $K[V]_i^G$ désigne l'ensemble des invariants homogènes de degré i. En particulier, l'expansion de Laurent de cette série autour de $t = 1$ s'est avérée très informative. Nous montrerons que les termes de cette expansion ont une signification particulière qui nous permettra de déduire des propriétés spécifiques de l'anneau des invariants. Nous nous intéresserons également à trouver des méthodes permettant

de calculer certains de ces termes sans devoir calculer la série de Hilbert, ce qui nous permettra d'obtenir des résultats partiels dans des cas où le calcul de la série de Hilbert est trop difficile.

Avant de continuer, notons que dans ce mémoire, nous ne faisons qu'un survol des résultats pertinents au problème de l'expansion de Laurent autour de $t = 1$. Il existe cependant une littérature beaucoup plus large au sujet de la série de Hilbert en général. En particulier, il existe de nombreux textes en physique traitant de séries de Hilbert pour des groupes (finis et infinis) qui interviennent souvent dans des problèmes physiques. Si le lecteur est intéressé à ce type de problème, il pourra se référer aux textes [**Jar**], [**Jar2**] et [**Pat**], entre autres. De plus, on retrouve une classification des sous-groupes de $O(2)$ et $O(3)$ dans [**Jar3**].

Chapitre 1

FAITS GÉNÉRAUX

1.1. DÉFINITIONS

Soit V un espace vectoriel de dimension finie sur un corps K et soit G un groupe fini muni d'une représentation $\rho : G \to GL(V)$. G agit alors linéairement sur V par $g \cdot v = \rho(g)v$ pour tout $g \in G$ et $v \in V$. De plus, notons par $K[V]$ l'anneau des fonctions polynomiales sur V. Autrement dit, soit $\{x_1, x_2, \ldots, x_n\}$ une base de V^*, alors $K[V] = K[x_1, x_2, \ldots, x_n]$ est l'anneau des polynômes en n variables.

Alors, G (munie de la représentation ρ) agit sur $K[V]$ par $(g \cdot f)(v) = f(g^{-1} \cdot v)$ pour tout $g \in G$ et $f \in K[V]$. Ainsi, nous définissons simplement l'anneau des invariants (qui est également une K-algèbre)

$$K[V]^G = \{f \in K[V] \mid g \cdot f = f, \forall g \in G\}.$$

Remarquons avant de continuer que l'action de G préserve le degré des polynômes, c'est-à-dire que $deg(g \cdot f) = deg(f)$ pour tous les $g \in G$ et $f \in K[V]$.

Un exemple classique d'invariants est celui des polynômes symétriques, qui sont définis comme les polynômes pour lesquels on peut permuter les variables sans changer leur valeur.

Exemple 1.1 (Polynômes symétriques). *Soit $G = \mathbb{S}_n$ le groupe des permutations de n objets. Soit V un espace vectoriel de dimension n avec une base fixée. Pour chaque permutation de $\mathbb{S}_n$, il existe une matrice de permutation et il est immédiat que cette correspondance est en fait un homomorphisme (et donc une représentation) entre G et $GL_n(K) \cong GL(V)$. Soit $\{x_1, x_2, \ldots, x_n\}$ une base fixée de V^*.*

$\mathbb{S}_n$ agit sur $K[V]$ en permutant les variables. Donc, $K[V]^{\mathbb{S}_n}$ est l'ensemble des polynômes symétriques.

Par le théorème fondamental des polynômes symétriques (voir par exemple **[Rot]***),*

$$K[V]^{\mathbb{S}_n} = K[f_1, f_2, \ldots, f_n],$$

où $f_i = \sum x_{j_1} x_{j_2} \cdots x_{j_i}$, la somme étant prise sur tous les $1 \leq j_1 < \cdots < j_i \leq n$.

À titre d'exemple, pour $n = 3$, $K[V]^{\mathbb{S}_3} = K[f_1, f_2, f_3]$, où

$$f_1 = x_1 + x_2 + x_3,$$
$$f_2 = x_1x_2 + x_1x_3 + x_2x_3,$$
$$f_3 = x_1x_2x_3.$$

Dans cet exemple, nous voyons que l'anneau des polynômes symétriques est polynomial , c'est-à-dire que les générateurs $f_1, \ldots, f_n$ sont algébriquement indépendants (donc, $K[f_1, \ldots, f_n]$ est isomorphe à $K[x_1, \ldots, x_n]$).

Par contre, un anneau d'invariants n'est pas toujours polynomial. En fait, c'est rarement le cas. Autrement dit, il peut exister des relations entre les générateurs (comme K-algèbre), comme nous le verrons dans certains exemples (voir, entre autres, l'exemple 2.1).

1.1.1. Algèbres graduées

Puisque l'action de G sur $K[V]$ préserve le degré des polynômes, il est évident que G agit également sur chacun des $K[V]_d$, c'est-à-dire l'ensemble des polynômes homogènes de degré d. On peut donc trouver les invariants de cette action, que nous appelons $K[V]_d^G$. Ainsi, puisque $K[V] = \bigoplus_{d=0}^{\infty} K[V]_d$ est une algèbre positivement graduée, cela implique une graduation $K[V]^G = \bigoplus_{d=0}^{\infty} K[V]_d^G$.

Non seulement cette graduation nous permettra-t-elle de définir l'objet principal de ce mémoire (la série de Hilbert) dans le cas des invariants (voir section 1.2), mais elle permet également de simplifier l'analyse des invariants en transformant un espace vectoriel de dimension infinie en une somme directe de plusieurs parcelles de dimension finie. Un exemple d'algorithme (bien que peu efficace en pratique) se servant de cette construction est tiré du livre **[Der]** :

Exemple 1.2. *Soient $\sigma_1, \sigma_2, \ldots, \sigma_r$ des générateurs du groupe G. Considérons l'application linéaire*

$$\begin{aligned} \phi : K[V]_d &\longrightarrow (K[V]_d)^r \\ f &\longmapsto (\sigma_1 \cdot f - f, \sigma_2 \cdot f - f, \ldots, \sigma_r \cdot f - f) \end{aligned}$$

Ainsi, $K[V]_d^G = ker(\phi)$ peut être trouvé simplement par les méthodes classiques d'algèbre linéaire.

Dans cet exemple, on voit qu'il pourrait être utile de savoir s'il existe une borne sur les degrés des générateurs de $K[V]^G$, ainsi il suffirait d'utiliser cette méthode pour un nombre fini de d pour trouver tous les générateurs. Plusieurs théorèmes bornent le degré des générateurs sous certaines hypothèses. Pour une discussion de ces bornes, se référer au livre [**Der**].

1.2. Série de Hilbert

La série de Hilbert est en quelque sorte une généralisation du concept de dimension d'algèbre linéaire adaptée pour les K-algèbres. C'est une série qui encode la dimension, comme espace vectoriel, de chaque étage de la graduation. Elle nous permettra entre autres de «deviner» les degrés des générateurs de l'anneau des invariants.

Définition 1.2.1. *Soit $A = \bigoplus_{i=0}^{\infty} A_i$ une K-algèbre positivement graduée telle que $A_0 \cong K$ et $M = \bigoplus_{j=-\infty}^{\infty} M_j$ un A-module gradué tel que pour tout j, $dim_K(M_j) < \infty$. Alors, la série de Hilbert de M est*

$$\mathcal{H}(M,t) = \sum_{j=-\infty}^{\infty} dim_K(M_j)t^j.$$

Nous savons que pour deux espaces vectoriels V_1 et V_2, nous avons que

$$dim_K(V_1 \oplus V_2) = dim_K(V_1) + dim_K(V_2)$$

et

$$dim_K(V_1 \otimes V_2) = dim_K(V_1) \cdot dim_K(V_2).$$

Si nous utilisons ces propriétés pour chaque coefficient de la série de Hilbert, nous pouvons déduire les propriétés suivantes pour des modules gradués M et N :

(1) $\mathcal{H}(M \oplus N, t) = \mathcal{H}(M, t) + \mathcal{H}(N, t)$

(2) $\mathcal{H}(M \otimes_K N, t) = \mathcal{H}(M, t) \cdot \mathcal{H}(N, t)$.

Nous pouvons donc calculer la série de Hilbert des exemples suivants :

Exemple 1.3. *Soit K un corps.*

(1) Soit z un élément de degré d. Alors,

$$\mathcal{H}(K[z], t) = 1 + t^d + t^{2d} + t^{3d} + \cdots = \frac{1}{1 - t^d}.$$

En effet, l'ensemble $\{1, z, z^2, z^3, z^4, \ldots\}$ est une base de $K[z]$ comme espace vectoriel.

(2) Soit $z_1, z_2, \ldots, z_n$ des éléments pour lesquels $deg(z_i) = d_i$, alors, puisque $K[z_1, z_2, \ldots, z_n] \cong K[z_1] \otimes_K K[z_2] \otimes_K \cdots \otimes_K K[z_n]$,

$$\mathcal{H}(K[z_1, z_2, \ldots, z_n], t) = \frac{1}{\prod_{i=1}^{n}(1 - t^{d_i})}.$$

(3) Soit A un anneau contenant $K[z_1, z_2, \ldots, z_n]$ comme sous-anneau et tel que

$$A = \eta_1 K[z_1, z_2, \ldots, z_n] \oplus \eta_2 K[z_1, z_2, \ldots, z_n] \oplus \cdots \oplus \eta_t K[z_1, z_2, \ldots, z_n]$$

comme $K[z_1, z_2, \ldots, z_n]$-module gradué.

Alors,

$$\mathcal{H}(A, t) = \frac{t^{s_1} + t^{s_2} + \cdots + t^{s_k}}{\prod_{i=1}^{n}(1 - t^{d_i})}$$

où $s_i = deg(\eta_i)$.

En pratique, il n'est pas très intéressant de calculer la série de Hilbert à partir des générateurs (comme dans l'exemple précédent) puisque nous voulons nous servir de cette série comme outil pour trouver ces générateurs. Il nous faudrait donc une formule nous permettant de calculer cette série sans connaître les générateurs. Nous discuterons de ce sujet au chapitre 2.

1.3. Propriétés de $K[V]^G$

Comme mentionné au début du chapitre, l'anneau des invariants n'est pas, en général, polynomial. Il possède cependant plusieurs propriétés que nous déduisons dans cette section.

1.3.1. Anneaux noethériens

Nous voulons montrer que $K[V]^G$ est un anneau noethérien. Nous montrons d'abord que toute K-algèbre finiment engendrée est un anneau noethérien. Ensuite, nous obtiendrons que $K[V]^G$ est une K-algèbre finiment engendrée.

Lemme 1.3.1. *Soit M un R-module noethérien et soit N un sous-module de M. Alors, le quotient M/N est également un R-module noethérien.*

Démonstration. Les sous-modules de M/N sont en correspondance avec les sous-modules de M contenant N, et ceux-ci sont finiment engendrés. Donc, un sous-module de M/N est engendré par les classes d'équivalence des générateurs du sous-module de M correspondant. □

Donc, un quotient d'un module noethérien est noethérien. Si R est noethérien, nous avons la caractérisation suivante pour les R-modules noethériens :

Proposition 1.3.2. *Soit R un anneau noethérien. Un R-module M est noethérien si et seulement si M est finiment engendré.*

Démonstration. Si M est finiment engendré, alors il est un quotient d'une somme directe d'un nombre fini de copies de R. M est donc noethérien.

Si M est noethérien, construisons une suite $x_1, x_2, x_3, \ldots$ de telle sorte que x_i ne soit pas dans le sous-module engendré par $x_1, x_2, \ldots, x_{i-1}$. Puisque M est noethérien, cette suite doit se terminer. Donc, M est finiment engendré. □

Les anneaux polynomiaux sont des exemples d'anneaux noethériens. Plus généralement :

Théorème 1.3.3 (Théorème de base de Hilbert). *Si R est noethérien, $R[x]$ l'est aussi.*

Démonstration. Supposons que I est un idéal de $R[x]$. Il suffit de montrer que I est finiment engendré. Soit I_0 l'idéal de R engendré par tous les coefficients dominants des polynômes de I. R étant noethérien par hypothèse, I_0 est finiment engendré, disons par $\{a_1, a_2, \ldots, a_k\}$. Choisissons alors des polynômes $f_1, f_2, \ldots, f_k$ dans I tels que le coefficient dominant de f_i est a_i. Notons par t_i le degré de f_i.

Soit maintenant $f \in I$ quelconque de degré $m > max\{t_i\}$. Le coefficient dominant de f est dans I_0, disons qu'il est $\sum_{i=0}^{k} c_i a_i$ pour certains c_i dans R.

Ainsi, le degré du polynôme f est strictement plus grand que le degré de $f - \sum_{i=0}^{k} c_i f_i x^{m-t_i}$.

Nous pouvons réitérer ce processus jusqu'à ce qu'on puisse écrire $f = g + h$ où $g \in (f_1, \ldots, f_k)$ et $deg(h) < max\{t_i\}$.

Autrement dit, $h \in I \cap (1, x, x^2, \ldots, x^{max\{t_i\}-1})$. Or, par la proposition 1.3.2, $(1, x, x^2, \ldots, x^{max\{t_i\}-1})$ est noethérien comme R-module et, donc, le sous-module $I \cap (1, x, x^2, \ldots, x^{max\{t_i\}-1})$ est finiment engendré. Or, il est évident que

$$I = (f_1, \ldots, f_k) + I \cap (1, x, x^2, \ldots, x^{max\{t_i\}-1}).$$

Donc, I est finiment engendré. □

Remarquons que cela implique que $R[x_1, \ldots, x_n]$ est noethérien si R est noethérien, par récurrence. En particulier, si K est un corps, $K[x_1, \ldots, x_n]$ est noethérien.

En fait, n'importe quelle K-algèbre finiment engendrée est noethérienne. En effet, si A est une algèbre engendrée par $f_1, \ldots, f_n$, alors on peut construire l'homomorphisme d'anneaux

$$\phi : K[x_1, \ldots, x_n] \longrightarrow A$$
$$x_i \longmapsto f_i$$

Nous voyons alors que $A \simeq K[x_1, \ldots, x_n]/\ker(\phi)$ est noethérien. Nous montrons maintenant que l'anneau des invariants est finiment engendré comme K-algèbre. Ainsi, il est toujours noethérien.

1.3.2. Nombre fini de générateurs

Notre prochain résultat est un théorème dû à Hilbert (dans le cas non modulaire), puis généralisé par Noether. Il faut cependant aborder le concept d'extension entière.

Soit $A \subseteq B$ une extension d'anneau. Un élément $x \in B$ est dit **entier** sur A s'il existe un polynôme unitaire f avec coefficients dans A tel que $f(x) = 0$ (rappelons qu'un polynôme est dit unitaire si son coefficient dominant est 1). L'extension est appelée une **extension entière** si tous les éléments de B sont entiers sur A.

Un résultat classique en algèbre commutative nous dit que si x est un élément de B, alors $A[x]$ est un A-module finiment engendré si et seulement si x est entier sur A. Par récurrence, $A[x_1, \ldots, x_n]$ est un A-module finiment engendré si et seulement si l'extension $A \subseteq A[x_1, \ldots, x_n]$ est entière.

Par exemple, dans le prochain théorème, nous verrons que l'extension $A^G \subseteq A$ est une extension entière, où A^G désigne les invariants de A pour une action du groupe fini G. En fait, A est un A^G-module finiment engendré.

De plus, nous montrerons que si A est une K-algèbre finiment engendrée, alors A^G l'est également.

Théorème 1.3.4 (Hilbert-Noether). *Soit K un corps et G un groupe fini agissant comme groupe d'automorphismes sur une K-algèbre A commutative et finiment engendrée. Alors, A^G est aussi une K-algèbre commutative et finiment engendrée. De plus, A est finiment engendré comme A^G-module.*

Démonstration. Soit $a \in A$. Alors a est un zéro du polynôme unitaire

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

et, donc, A est une extension entière de A^G. Puisque A est finiment engendrée par hypothèse, nous pouvons choisir un ensemble fini de générateurs. À chacun de ces générateurs correspond le polynôme unitaire définit ci-haut. Soit A' la sous-algèbre de A^G engendrée par les coefficients de ces polynômes. Alors, A' est une K-algèbre finiment engendrée et, donc, noethérienne. A est un A'-module finiment engendré, ce qui implique que A^G l'est également (proposition 1.3.2). Donc, A^G est une K-algèbre finiment engendrée. □

Le fait que l'anneau des invariants soit finiment engendré est reflété dans sa série de Hilbert. En effet, dans ce cas, le théorème suivant montre que la série de Hilbert est une fonction rationnelle qui a une forme particulière.

Théorème 1.3.5 (Hilbert-Serre). *Supposons que* $A = \bigoplus_{j=0}^{\infty} A_j$ *est un anneau gradué avec* $A_0 = K$. *Supposons de plus que* A *soit finiment engendré par des éléments homogènes* $x_1, x_2, \ldots, x_s$ *de degrés* $k_1, k_2, \ldots, k_s$, *respectivement. Soit* $M = \bigoplus_{j=-\infty}^{\infty} M_j$ *un* A*-module finiment engendré. Alors,*

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

où $f(t)$ *est un polynôme de Laurent en* t *avec coefficients entiers.*

Démonstration. Par récurrence sur s. Pour $s = 0$, $\mathcal{H}(M,t)$ est un polynôme de Laurent. Supposons maintenant $s > 0$. Notons M' le noyau et M'' le conoyau de la multiplication par x_s (le conoyau est le codomaine quotienté par l'image). Cela donne une suite exacte pour chaque $r \in \mathbb{Z}$:

$$0 \longrightarrow M'_r \longrightarrow M_r \xrightarrow{x_s} M_{r+k_s} \longrightarrow M''_{r+k_s} \longrightarrow 0.$$

Or, M' et M'' sont des $K[x_1, \ldots, x_{s-1}]$-modules finiment engendrés et ont donc une série de Hilbert de la forme voulue, par l'hypothèse de récurrence.

En utilisant la suite exacte ci-haut et en remarquant que pour une suite exacte d'espaces vectoriels, la somme alternées des dimensions est nulle, on obtient :

$$t^{k_s}\mathcal{H}(M',t) - t^{k_s}\mathcal{H}(M,t) + \mathcal{H}(M,t) - \mathcal{H}(M'',t) = 0.$$

Donc,

$$\mathcal{H}(M,t) = \frac{\mathcal{H}(M'',t) - t^{k_s}\mathcal{H}(M',t)}{1-t^{k_s}}$$

a bien la forme voulue. □

1.3.3. Normalisation de Noether

Bien que l'anneau des invariants n'est pas toujours polynomial, nous verrons qu'il est «presque» polynomial dans le sens qu'il existe toujours un sous-anneau B polynomial pour lequel l'anneau des invariants est un B-module finiment engendré. Nous verrons également que dans le cas non modulaire, il est en outre un B-module libre.

Introduisons tout d'abord la notion de système homogène de paramètres. Soit A une K-algèbre positivement graduée telle que $A_0 \cong K$. Un ensemble

$\{\theta_1, \theta_2, \ldots, \theta_m\}$ d'éléments homogènes de A de degrés strictement positifs est appelé un **système homogène de paramètres** si

(1) $\theta_1, \theta_2, \ldots, \theta_m$ sont algébriquement indépendants sur K.

(2) A est un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module gradué finiment engendré.

Similairement, si M est un A-module gradué, l'ensemble $\{\theta_1, \theta_2, \ldots, \theta_m\}$ d'éléments homogènes de A est un **système homogène de paramètres** pour M si

(1) $\theta_1, \theta_2, \ldots, \theta_m$ sont algébriquement indépendants sur K.

(2) $K[\theta_1, \theta_2, \ldots, \theta_m] \cap Ann_A(M) = 0$.

(3) M est un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module gradué finiment engendré.

Le théorème de normalisation de Noether (que nous énonçons ci-après) garantit l'existence d'un tel système sous certaines conditions. De plus, la cardinalité d'un tel système est unique et correspond en fait à la **dimension de Krull** du module M.

Nous définissons la dimension de Krull d'un anneau R, notée $dim(R)$, comme la longueur n de la plus longue suite $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \cdots \subset \mathcal{P}_n$ d'idéaux premiers de R. On pose $dim(R) = \infty$ si ces longueurs ne sont pas bornées.

D'autre part la dimension de Krull d'un R-module M finiment engendré, notée $dim_R(M)$ (ou $dim(M)$ si l'anneau R est clair par le contexte), est égale à $dim(R/Ann(M))$.

Théorème 1.3.6 (Normalisation de Noether). *Soit $A = \bigoplus_{j=0}^{\infty} A_j$ une K-algèbre graduée finiment engendrée avec $A_0 \cong K$. Soit maintenant $M = \bigoplus_{j=-\infty}^{\infty} M_j$ un A-module finiment engendré. Alors, il existe toujours un système homogène de paramètres $\{\theta_1, \theta_2, \ldots, \theta_m\}$ pour M.*

De plus, $m = dim(M)$.

Démonstration. Voir **[Ben]**, théorème 2.2.7. □

Comme nous l'avons mentionné, dans ce mémoire, nous nous intéressons à l'expansion de Laurent de la série de Hilbert des invariants autour de $t = 1$.

Soit M un R-module. Nous noterons par $\gamma(M)$ l'ordre du pôle en $t = 1$ de $\mathcal{H}(M, t)$. Nous voulons montrer que $\gamma(M) = dim(M)$. Une conséquence de cela est que $\gamma(K[V]^G) = dim(K[V]^G) = dim_K(V)$.

Théorème 1.3.7. *Soit $A = \bigoplus_{j=0}^{\infty} A_j$ une K-algèbre graduée finiment engendrée avec $A_0 \cong K$. Soit maintenant $M = \bigoplus_{j=-\infty}^{\infty} M_j$ un A-module finiment engendré. Alors, $\gamma(M) = dim(M)$.*

Démonstration. Par le théorème de normalisation de Noether, il existe un anneau polynomial $R = K[\theta_1, \ldots, \theta_r]$ tel que M est un R-module finiment engendré et $Ann_R(M) = 0$.

Nous voulons montrer qu'il existe une copie de R incluse dans M. Autrement dit, il existe un $m \in M$ tel que $Ann_R(m) = 0$. Ainsi, pour ce m, $R \cdot m \subseteq M$ est une copie de R.

Nous démontrons cela par récurrence sur le nombre de générateurs de M comme R-module. Si M a un seul générateur, disons m, alors $M = R \cdot m$ et $Ann_R(m) = Ann_R(M) = 0$.

Maintenant, supposons qu'il existe un $s > 1$ tel que $\{m_1, \ldots, m_s\}$ est un ensemble minimal de générateurs pour M. Si $Ann_R\langle m_1, \ldots, m_{s-1}\rangle = 0$ ou si $Ann_R(m_s) = 0$, alors, la preuve est terminée puisque nous pouvons prendre un $m \in M$ tel que $Ann_R(m) = 0$, par l'hypothèse de récurrence. Donc, supposons que ce n'est pas le cas et posons

$$\alpha = Ann_R\langle m_1, \ldots, m_s\rangle \neq 0$$

$$\beta = Ann_R(m_s) \neq 0$$

Ainsi, le produit $\alpha \cdot \beta$ est non nul car R est un domaine intègre. Mais alors, nous avons que

$$0 \neq \alpha \cdot \beta \subseteq Ann_R\langle m_1, \ldots, m_s\rangle = Ann_R(M) = 0,$$

une contradiction.

Ainsi, nous avons montré qu'il existe un $m \in M$ tel que $R \cdot m$ est isomorphe à R. Autrement dit, si d est le degré de m, alors $\mathcal{H}(R \cdot m, t) = t^d \mathcal{H}(R, t)$. De plus, puisque $R \cdot m \subseteq M$, nous avons que

$$\mathcal{H}(R \cdot m) = t^d \mathcal{H}(R, t) \leq \mathcal{H}(M, t),$$

dans le sens que l'inégalité est vraie pour tous les coefficients.

Finalement, puisque M est finiment engendré, il existe un R-module libre L et un homomorphisme surjectif $L \longrightarrow M$. En effet, si M est engendré par $m_1, \ldots, m_s$, on peut considérer L comme le module libre de dimension s, avec des générateurs $e_1, \ldots, e_s$. Pour que l'homomorphisme surjectif préserve la graduation, on peut définir le degré des générateurs de L comme $d_i = deg(e_i) = deg(m_i)$.

Ainsi, la série de Hilbert de L est

$$\mathcal{H}(L,t) = \left(\sum_{i=1}^{s} t^{d_i}\right) \mathcal{H}(R,t).$$

De plus, puisque nous avons un homomoprhisme surjectif, cela implique l'inégalité

$$\mathcal{H}(M,t) \leq \mathcal{H}(L,t).$$

Autrement dit, nous avons

$$t^d \mathcal{H}(R,t) \leq \mathcal{H}(M,t) \leq \left(\sum_{i=1}^{s} t^{d_i}\right) \mathcal{H}(R,t).$$

Or, les deux séries aux extrémités ont un pôle d'ordre r puisque

$$\mathcal{H}(R,t) = \frac{1}{\prod_{i=1}^{r}(1-t^{k_i})}$$

où $k_i = deg(\theta_i)$.

Nous pouvons donc montrer que l'ordre de $\mathcal{H}(M,t)$ a aussi un pôle d'ordre r. Il suffit tout d'abord de remarquer que dans notre cas, nous pouvons multiplier chaque terme par $(t-1)^r$ et préserver les inégalités. Ensuite, lorsque nous prenons les limites lorsque t tend vers 1, la convergence des deux séries aux extrémités implique la convergence de la série du milieu.

Donc, $\gamma(M) = r = dim(M)$ par le théorème de normalisation de Noether. □

Donc, si nous considérons le cas $A = M = K[V]^G$, nous obtenons $\gamma(K[V]^G) = dim(K[V]^G)$. De plus, un système homogène de paramètres pour $K[V]^G$ est également un système homogène de paramètres pour $K[V]$ puique $K[V]$ est un $K[V]^G$-module finiment engendré. Donc, $dim(K[V]) = dim(K[V]^G)$, ce qui veut dire que $\gamma(K[V]^G) = dim(K[V]) = dim_K(V)$.

Remarque 1.1. *En fait, pour un A-module M satisfaisant aux hypothèses du théorème 1.3.7, nous aurions pu définir directement la dimension de Krull de M*

comme étant $dim(M) = \gamma(M)$. Cette définition simplifie en général les démonstrations. À titre d'exemple, il est maintenant aisé de démontrer que la dimension de Krull de $K[x_1, \ldots, x_n]$ est n. En effet, il suffit de remarquer que la série de Hilbert

$$\mathcal{H}(K[x_1, \ldots, x_n], t) = \prod_{i=1}^{n} \frac{1}{(1 - t^{d_i})},$$

où $d_i = deg(x_i)$, a un pôle d'ordre n.

1.3.4. Modules Cohen-Macaulay

$K[V]^G$ est donc un module finiment engendré sur un anneau polynomial. Cela ne veut pas dire, cependant, qu'il est libre sur cet anneau. Un anneau R est dit **Cohen-Macaulay** s'il est libre sur l'anneau polynomial engendré par un système homogène de paramètres. Similairement, nous avons défini un système homogène de paramètres pour un module M et nous disons que ce module est Cohen-Macaulay s'il est un module libre sur l'anneau polynomial engendré par ce système.

Remarque 1.2. *On peut montrer que la propriété Cohen-Macaulay ne dépend pas du choix du système homogène de paramètres (voir* [**Ser**]*, théorème 2, p.IV-20).*

Remarque 1.3. *La définition que nous avons donnée pour un module (ou un anneau) Cohen-Macaulay n'est pas celle que nous rencontrons usuellement dans la littérature. Un module est dit Cohen-Macaulay si sa profondeur (que nous n'avons pas définie ici) est égale à sa dimension de Krull. Cependant, notre définition est équivalente. Une preuve de cette équivalence est présentée dans* [**Ben**]*, théorème 4.3.5.*

Comme nous l'avons vu à la section 1.3.2, pour un module M finiment engendré, il est toujours possible d'écrire la série de Hilbert comme une fonction rationnelle de la forme

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

où $f(t)$ est un polynôme de Laurent en t avec coefficients entiers.

Si, de plus, M est Cohen-Macaulay, alors nous avons une information supplémentaire sur la série de Hilbert. En effet, dans ce cas, M est libre sur un anneau

polynomial, disons $K[f_1, \ldots, f_s]$, tel que $deg(f_i) = k_i$. Ainsi, nous pouvons toujours écrire

$$M = \eta_1 K[f_1, f_2, \ldots, f_s] \oplus \eta_2 K[f_1, f_2, \ldots, f_s] \oplus \cdots \oplus \eta_t K[f_1, f_2, \ldots, f_s].$$

Supposons que $deg(\eta_i) = d_i$. Donc,

$$\mathcal{H}(M, t) = \frac{t^{d_1} + t^{d_2} + \cdots + t^{d_t}}{\prod_{j=1}^{s}(1 - t^{k_j})}$$

Il arrive parfois que $K[V]^G$ soit Cohen-Macaulay. En fait, nous verrons au chapitre 2 qu'il est toujours Cohen-Macaulay dans le cas non modulaire.

Dans ce cas, nous pouvons toujours écrire

$$K[x_1, \ldots, x_n]^G = K[f_1, f_2, \ldots, f_n] \oplus \eta_1 K[f_1, f_2, \ldots, f_n] \oplus \cdots \oplus \eta_t K[f_1, f_2, \ldots, f_n]$$

pour des polynômes $f_1, f_2, \ldots, f_n, \eta_1, \eta_2, \ldots, \eta_k$ invariants.

L'ensemble $\{f_1, f_2, \ldots, f_n\}$ est alors appelé un ensemble d'**invariants primaires**, tandis que l'ensemble $\{\eta_1, \eta_2, \ldots, \eta_k\}$, un ensemble d'**invariants secondaires**. Bien que le choix de ces ensembles ne soit pas unique, le nombre et le degré de ces polynômes le sont.

1.3.5. Anneaux Gorenstein

Soit R un anneau Cohen-Macaulay et soit A un anneau polynomial sur lequel R est libre. Nous pouvons définir le **module canonique** de R comme étant le module

$$\omega_A(R) = Hom_A(R, A).$$

Ainsi, le module canonique est en quelque sorte le dual de R. Si R est isomorphe à $\omega_A(R)$ (comme R-module), nous disons que R est **Gorenstein**. En d'autres termes, un anneau Gorenstein est « auto-dual ». Si l'isomorphisme préserve la graduation, on dit que R est **Gorenstein gradué**. Nous verrons que les anneaux Gorenstein peuvent être caractérisés par leur série de Hilbert.

Remarque 1.4. *Nous montrons à l'annexe C que $\omega_A(R)$ ne dépend pas du choix de A, à isomorphisme près. Nous écrirons par la suite simplement $\omega(R)$ pour le module canonique. Une conséquence de cela est bien sûr que la propriété Gorenstein ne dépend pas non plus du choix de A.*

Nous avons une équation fonctionnelle pour la série de Hilbert du module canonique :

$$\mathcal{H}(R, t^{-1}) = (-1)^n t^{n+r} \mathcal{H}(\omega(R), t)$$

pour un nombre entier r (n est la dimension de Krull de R).

En effet, soit $\{\phi_i\}$ une base de R comme A-module libre. Soit maintenant $\{\phi_i^*\}$ la base duale (donc une base pour $\omega(R)$). Autrement dit, $\phi_i^*(\sum a_j \phi_j) = a_i$. Si e_i est le degré de ϕ_i, alors le degré de ϕ_i^* est $-e_i$ puisque ϕ_i^* fait diminuer le degré d'un élément de e_i. Ainsi, nous avons que la série de Hilbert de R est

$$\mathcal{H}(R, t) = \frac{\sum t^{e_i}}{\prod_{j=1}^{n}(1 - t^{deg(f_j)})}$$

tandis que la série de Hilbert de $\omega(R)$ est

$$\mathcal{H}(\omega(R), t) = \frac{\sum t^{-e_i}}{\prod_{j=1}^{n}(1 - t^{deg(f_j)})}.$$

D'où nous avons l'équation fonctionnelle si nous posons $n + r = \sum deg(f_j)$.

Nous nous intéressons donc aux anneaux **Gorenstein**, c'est-à-dire aux anneaux R tels que $R \cong \omega(R)$ (comme R-module). Dans ce cas, nous avons l'équation fonctionnelle

$$\mathcal{H}(R, t^{-1}) = (-1)^n t^{n+q} \mathcal{H}(R, t) \tag{1.3.1}$$

pour un entier q.

Remarque 1.5. *Nous pouvons voir $\omega(R) \cong Hom_A(R, A)$ comme un R-module en définissant, pour $r, r' \in R$ et $f \in Hom_A(R, A)$, un produit $(r \cdot f)(r') := f(rr')$.*

Cette relation peut également être énoncée de la manière suivante. Puisque R est Cohen-Macaulay, nous avons vu que sa série de Hilbert est de la forme

$$\mathcal{H}(R, t) = \frac{f(t)}{\prod_{i=0}^{n}(1 - t^{d_i})},$$

où $f(t)$ est un polynôme à coefficients entiers positifs ou nuls et les d_i sont des nombres naturels. Posons $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_m t^m$. Alors, la relation (1.3.1) implique que $a_i = a_{m-i}$ pour $i = 0, 1, \ldots, m$.

En effet, supposons que les e_i sont ordonnés de sorte que $e_1 \leq e_2 \leq \cdots \leq e_s$. Alors, par l'équation 1.3.1, nous avons qu'il existe un entier $\tilde{q}$ tel que

$$\sum t^{e_i} = t^{\tilde{q}} \sum t^{-e_i}.$$

En comparant les deux côtés en en regroupant les termes qui ont même exposant, nous avons que bien que $a_i = a_{m-i}$ pour $i = 0, 1, \ldots, m$.

En fait, il est intéressant de noter que R.P. Stanley a déjà démontré qu'un anneau gradué Cohen-Macaulay R intègre est Gorenstein si et seulement si sa série de Hilbert satisfait à l'équation 1.3.1.

Théorème 1.3.8. *Soit R un anneau intègre gradué et Cohen-Macaulay. R est Gorenstein si et seulement si sa série de Hilbert satisfait à l'équation 1.3.1.*

Démonstration. Nous avons déjà montré un côté de l'équivalence. Maintenant, supposons que R est un anneau gradué intègre tel que sa série de Hilbert satisfait à 1.3.1. Supposons également que les e_i sont ordonnés comme précédemment et que les ϕ_i forment une base de R sur A. ϕ_s est l'unique élément de la base qui est de degré maximal. En effet, le fait que $A \subseteq R$ implique qu'un (et un seul) des ϕ_i soit une constante. En fait, c'est ϕ_1 étant donné que les e_i sont ordonnés. Autrement dit, nous avons que $e_1 = 0$ et que $e_i > 0$ pour $i > 1$. Donc, $a_1 = 1$. Or, par la relation 1.3.1, $a_m = a_1 = 1$, ce qui montre bien que ϕ_s est l'unique élément de la base de degré maximal. Ainsi, ϕ_s^* est l'unique ϕ_i^* de degré minimal.

Définissons alors le morphisme

$$\begin{aligned} \zeta : R &\longrightarrow \omega(R) \cong Hom_A(R, A) \\ r &\longmapsto \zeta_r \end{aligned}$$

où $\zeta_r(r') = \phi_s^*(rr')$.

Nous voulons montrer que ζ est en fait un isomorphisme. Tout d'abord, si nous passons aux corps de fractions, nous avons un morphisme

$$\tilde{\zeta} : Q(R) \longrightarrow Hom_{Q(A)}(Q(R), Q(A))$$

Remarquons avant de continuer que $z \in Q(R)$ peut s'écrire comme $\frac{r}{a}$ où $r \in R$ et $0 \neq a \in A$ (voir remarque 1.6). De plus, $\tilde{\zeta}(\frac{r}{a}) = \zeta_{\frac{r}{a}}$ où $\zeta_{\frac{r}{a}}(\frac{r'}{a'}) = \frac{1}{aa'}\phi_s^*(rr')$. Or, puisque $Q(R)$ est un corps, le noyau de $\tilde{\zeta}$ est soit 0 où $Q(R)$. Le noyau n'est pas $Q(R)$ puisque $\tilde{\zeta}(\phi_s) = \zeta_{\phi_s}$ et $\zeta_{\phi_s}(1) = \phi_s^*(\phi_s) = 1 \neq 0$. Donc, ζ est injectif.

Finalement, R et $\omega(R)$ ont la même série de Hilbert (il faut peut-être multiplier la série de $\omega(R)$ par un facteur de t^q), ce qui implique que $R[q]$ et $\omega(R)$ sont isomorphes. □

Remarque 1.6. *En fait, plus généralement, si $R \subset S$ est une extension finie d'anneaux intègres, alors les éléments du corps de fractions de S sont de la forme s/r où $s \in S$ et $0 \neq r \in R$. Si on note par $Q(S)$ le corps de fractions de S et par T l'ensemble des éléments s/r où $s \in S$ et $0 \neq r \in R$, alors nous voulons montrer que $Q(S) = T$. Or, puisque l'extension $R \subset S$ est finie, alors l'extension $Q(R) \subseteq Q(S)$ est finie. Or, $T \subseteq Q(S)$ implique que $Q(R) \subseteq T$ est également finie. Donc, T est un corps. Ainsi, pour chaque $s \in S$, $s/1 \in T$. Puisque T est un corps, on a également que l'inverse $1/s \in T$. Donc, T est le corps de fractions de S et ainsi $T = Q(S)$.*

Exemple 1.4. *Soit G le groupe de matrices engendré par $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ agissant sur $\mathbb{C}[x, y]$. Le groupe G est un sous-groupe de $SL(V)$ (donc $\mathbb{C}[V]^G$ est Gorenstein, comme nous verrons dans le théorème 2.5.1). Nous calculons la série de Hilbert de $\mathbb{C}[V]^G$ dans l'exemple 2.1 :*

$$\mathcal{H}(\mathbb{C}[x,y]^G, t) = \frac{1}{4}\left[\frac{1}{(1-t)^2} + \frac{2}{1+t^2} + \frac{1}{(1+t)^2}\right] = \frac{1+t^4}{(1-t^2)(1-t^4)}$$

qui est bien de la forme prédite (ici $m = 4$).

1.4. Expansion de Laurent autour de $t = 1$

Nous allons utiliser la notation suivante pour les termes de l'expansion de Laurent :

$$\mathcal{H}(M,t) = \frac{\psi_0(M)}{(1-t)^n} + \frac{\psi_1(M)}{(1-t)^{n-1}} + \cdots + \frac{\psi_k(M)}{(1-t)^{n-k}} + \cdots$$

où $n = dim(A)$. Puisque la dimension de Krull de A n'est pas nécéssairement égale à celle de M, il est possible que les premiers termes soient nuls. Remarquons également que les $\psi_i(M)$ sont des nombres rationnels.

Nous énonçons maintenant plusieurs résultats concernant les coefficients de Laurent $\psi_i(M)$. Nous ne supposons pas, pour l'instant, que M correspond aux invariants d'une action de groupe. Nous traiterons ce cas particulier dans les prochains chapitres.

Remarque 1.7. *Dans la littérature, les deux premiers termes sont habituellement notés $deg(M)$ et $\psi(M)$. Cependant, cette notation est difficile à généraliser pour les autres termes de l'expansion. Pour cette raison, nous utiliserons tout au long de ce texte la notation $\psi_i(M)$ pour le i^e terme de cette expansion. Donc, $deg(M) = \psi_0(M)$ et $\psi(M) = \psi_1(M)$.*

Nous présentons tout de suite notre premier lemme (tiré de [**Ben**]) sur les deux premiers termes de cette expansion. Rappelons que nous notons $M[d]$ le module gradué tel que $M[d]_i = M_{i+d}$. De plus, si A est un anneau intègre, nous définissons le rang d'un A-module M, noté $rang_A(M)$, comme la dimension de $Q(A) \otimes_A M$ sur $Q(A)$.

Lemme 1.4.1. *Nous avons que :*

(1) $\psi_0(M[d]) = \psi_0(M)$

(2) $\psi_1(M[d]) = \psi_1(M) - d\psi_0(M)$

(3) Si A est intègre, $\psi_0(M) = rang_A(M)\,\psi_0(A)$

Démonstration. *(1)* et *(2)* peuvent être démontrés par calcul direct. En effet, on a que

$$\mathcal{H}(M,t) = t^d \mathcal{H}(M[d],t).$$

Or, on peut réécrire cela comme

$$\mathcal{H}(M,t) = \left(\sum_{i=0}^{d}(t-1)^i\right)\mathcal{H}(M[d],t)$$

puisque $t^d = ((t-1)+1)^d$ et nous utilisons la formule du binôme. En prenant l'expansion de Laurent des deux côtés, nous obtenons les deux premiers points du théorème.

(3) Voir le lemme 1.4.2 (3). □

Définition 1.4.1. *Soit M un A-module. Nous définissons la* ***longueur*** *de M (notée $long_A(M)$) comme la longueur h de la plus longue suite $0 \subset M_1 \subset M_2 \subset \cdots \subset M_h = M$ de A-modules, si les longueurs de telles suites sont bornées.*

Similairement, nous définissons la **hauteur** ou la **codimension** d'un idéal premier $\mathcal{P}$, notée $haut(\mathcal{P})$ ou $codim(\mathcal{P})$, comme la longueur h de la plus longue chaîne d'idéaux premiers

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \cdots \subset \mathcal{P}_h = \mathcal{P}.$$

En fait, si nous comparons la définition de hauteur avec celle de dimension nous voyons que $dim(\mathcal{P}) = n - h$ si $\mathcal{P}$ est un idéal premier de hauteur h dans un anneau de dimension n. C'est pour cette raison que certains auteurs écrivent codimension plutôt que hauteur. Dans ce texte, nous utiliserons toujours le mot hauteur.

Nous avons une formule très utile pour le premier terme non nul de l'expansion de Laurent provenant de l'article [**Avr**] :

Lemme 1.4.2. *Soit $M \neq 0$ un A-module gradué finiment engendré avec*

$$h = dim(A) - dim(M).$$

Alors,

(1) $\psi_j(M) = \psi_j(M') + \psi_j(M'')$ *pour tout* $j \in \mathbb{Z}$ *si on a une suite exacte*

$$0 \to M' \to M \to M'' \to 0.$$

(2) $\psi_j(M) = 0$ *pour* $j < h$.

(3) $\psi_h(M) = \sum_{\mathcal{P}} long_{A_{\mathcal{P}}}(M_{\mathcal{P}})\psi_h(A/\mathcal{P})$, *où la somme est prise sur les idéaux premiers $\mathcal{P}$ homogènes de hauteur h.*

Démonstration. *(1)* est une conséquence de l'additivité de la série de Hilbert et de l'unicité des coefficients de l'expansion de Laurent.

(2) est évident puisque $dim(M) = dim(A) - h$ et que nous avons déjà montré que le premier terme non nul de l'expansion de Laurent d'un module M est le coefficient de $(1-t)^{-dim(M)}$.

(3) Voir l'article [**Avr**]. □

Dans la section 1.3.5, nous avons donné une équation fonctionnelle satisfaite par la série de Hilbert d'un anneau Gorenstein. En fait, cette équation donne beaucoup d'information sur les coefficients de Laurent.

En effet, considérons une série rationnelle de la forme

$$\mathcal{H}(t) = \frac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})},$$

où $f(t)$ est une série à coefficients entiers et les d_i sont des nombres naturels. Il n'est même pas nécessaire de voir $\mathcal{H}(t)$ comme la série de Hilbert des invariants pour le moment. Il suffit de remarquer que l'ordre du pôle de $\mathcal{H}(t)$ en $t = 1$ est n et que $\mathcal{H}(t)$ admet donc une expansion de Laurent

$$\mathcal{H}(t) = \frac{\psi_0}{(1-t)^n} + \frac{\psi_1}{(1-t)^{n-1}} + \cdots + \frac{\psi_k}{(1-t)^k} + \cdots$$

où les ψ_i sont des nombres rationnels. Nous pouvons également définir la série $\widetilde{\mathcal{H}}(t)$ par l'équation fonctionnelle

$$\mathcal{H}(t^{-1}) = (-1)^n t^{n+q}\widetilde{\mathcal{H}}(t).$$

Ainsi, nous pourrons éventuellement considérer $\widetilde{\mathcal{H}}$ comme la série de Hilbert du module canonique. Pour l'instant, remarquons que cette série aura, elle aussi, une expansion de Laurent

$$\widetilde{\mathcal{H}}(t) = \frac{\tilde{\psi}_0}{(1-t)^n} + \frac{\tilde{\psi}_1}{(1-t)^{n-1}} + \cdots + \frac{\tilde{\psi}_k}{(1-t)^k} + \cdots$$

où les $\tilde{\psi}_i$ sont des nombres rationnels.

Nous avons alors le théorème suivant tiré de l'article [**Bro2**] qui met en relation les coefficients des deux expansions :

Théorème 1.4.3. *Avec les notations précédentes :*

(1) Soit $\mathcal{F} = \frac{f(1)}{d_1 d_2 \cdots d_n}$, *les coefficients* ψ_i *et* $\tilde{\psi}_j$ *sont reliés comme suit :*

$$\begin{aligned} \tilde{\psi}_0 &= \psi_0 = \mathcal{F}; \\ \tilde{\psi}_1 + \psi_1 &= q\mathcal{F}; \\ \tilde{\psi}_2 - \psi_2 &= (q+1)(\psi_1 - \frac{q}{2}\mathcal{F}); \\ &\vdots \\ \sum_{i=1}^{m} \binom{m-1}{i-1} (-1)^i \psi_i &= \sum_{i=0}^{m} \binom{q}{m-i} (-1)^{m-i} \tilde{\psi}_i \end{aligned}$$

pour $m \geq 1$. *En particulier, quand* $q = 0$, *nous avons que*

$$\tilde{\psi_m} = \sum_{i=1}^{m} \binom{m-1}{i-1} (-1)^i \psi_i.$$

(2) Si on suppose que $\mathcal{H}(t)$ *satisfait lui-même à l'équation fonctionnelle*

$$\mathcal{H}(t^{-1}) = (-1)^n t^{n+q} \mathcal{H}(t)$$

pour un entier q, *alors* $\mathcal{F}q = 2\psi_1$. *Donc, si* $\psi_1 = 0$, *alors* $q = 0$ *et pour tout* $m > 1$,

$$(1 - (-1)^m)\psi_m = \sum_{i=2}^{m-1} \binom{m-1}{i-1} (-1)^i \psi_i.$$

Ainsi, si $m \geq 2$ *est minimal tel que* $\psi_m \neq 0$, *alors* m *est pair et*

$$m\psi_m = 2\psi_{m+1}.$$

En particulier, $\psi_2 = \psi_3$ *si* $\psi_1 = 0$.

Démonstration. (1) Tout d'abord, si $\mathcal{H} = \frac{f(t)}{\prod(1-t^{d_i})}$, alors

$$\psi_0 = \lim_{t \to 1} \mathcal{H}(t)(1-t)^n = \lim_{t \to 1} \frac{f(t)}{\prod_{i=1}^{n}(1 + t + t^2 + \cdots + t^{d_i - 1})} = \frac{f(1)}{d_1 d_2 \cdots d_n} = \mathcal{F}.$$

Nous pouvons utiliser le même type d'argument pour $\tilde{\psi}_0$ puisque, explicitement

$$\widetilde{\mathcal{H}}(t) = \frac{t^{\sum_i (d_i - 1) - q}}{\prod_{i=1}^{n}(1 - t^{d_i})}.$$

Si nous substituons t par t^{-1} dans l'expansion de Laurent de $\mathcal{H}(t)$, nous obtenons

$$\frac{1}{(1-t^{-1})^n}\left(\mathcal{F}+\sum_{i\geq 1}\psi_i(1-t^{-1})^i\right)=\frac{(-t)^n}{(1-t)^n}\left(\mathcal{F}+\sum_{i\geq 1}\psi_i\frac{(1-t)^i}{(-t)^i}\right).$$

Puisque $\mathcal{H}$ et $\widetilde{\mathcal{H}}$ sont reliés par l'équation fonctionnelle, alors l'expansion de $\mathcal{H}(t^{-1})$ ci-dessus est égale à

$$\frac{(-t)^n t^q}{(1-t)^n}\left(\mathcal{F}+\sum_{i\geq 1}\tilde{\psi}_i(1-t)^i\right),$$

ce qui implique que

$$\left(\mathcal{F}+\sum_{i\geq 1}\psi_i\frac{(1-t)^i}{(-t)^i}\right)=t^q\left(\mathcal{F}+\sum_{i\geq 1}\tilde{\psi}_i(1-t)^i\right). \tag{1.4.1}$$

En se servant de l'égalité

$$\frac{1}{t^i}=\left(\frac{1}{1-(1-t)}\right)^i=\sum_{j\geq 0}\binom{i+j-1}{j}(1-t)^j,$$

nous pouvons déduire que le côté gauche de l'équation 1.4.1 est égal à

$$\mathcal{F}+\sum_{m\geq 1}\left(\sum_{i=1}^{m}\binom{m-1}{i-1}(-1)^i\psi_i\right)(1-t)^m.$$

D'autre part, nous pouvons nous servir du fait que

$$t^q=(1-(1-t))^q=\sum_{i\geq 0}\binom{q}{i}(-1)^i(1-t)^i$$

pour développer le côté droit de l'équation 1.4.1 et ainsi obtenir que celui-ci est égal à

$$\mathcal{F}+\sum_{m\geq 1}\left(\sum_{i=0}^{m}\binom{q}{m-i}(-1)^{m-i}\tilde{\psi}_i\right)(1-t)^m.$$

Donc, en comparant les coefficients des deux côtés de l'équation 1.4.1, nous obtenons tout de suite l'égalité voulue pour $m\geq 1$:

$$\sum_{i=1}^{m}\binom{m-1}{i-1}(-1)^i\psi_i=\sum_{i=0}^{m}\binom{q}{m-i}(-1)^{m-i}\tilde{\psi}_i.$$

(2) Supposons que l'équation fonctionnelle soit vérifiée pour $\mathcal{H}$. Ainsi, nous avons $\mathcal{H}=\widetilde{\mathcal{H}}$ et $\psi_i=\tilde{\psi}_i$ pour tout i. Nous obtenons donc automatiquement que $2\psi_1=\mathcal{F}q$ et donc que $q=0$ si $\psi_1=0$.

Par (1), lorsque $q = 0$, nous avons que pour tout $m \geq 1$

$$\psi_m = \sum_{i=1}^{m} \binom{m-1}{i-1} (-1)^i \psi_i.$$

Nous pouvons alors soustraire à chacun des côtés $(-1)^m \psi_m$ pour obtenir

$$(1 + (-1)^m)\psi_m = \sum_{i=2}^{m-1} \binom{m-1}{i-1} (-1)^i \psi_i.$$

□

Corollaire 1.4.4. *Soit G un groupe fini muni d'une représentation sur un espace vectoriel V de dimension finie. Si $K[V]^G$ est Gorenstein et qu'il existe un $k > 1$ pour lequel*

$$\psi_1(K[V]^G) = \psi_2(K[V]^G) = \cdots = \psi_{k-1}(K[V]^G) = 0, \textit{ mais } \psi_k(K[V]^G) \neq 0$$

alors, k est pair et

$$k\psi_k(K[V]^G) = 2\psi_{k+1}(K[V]^G).$$

L'exemple 2.3 contient quelques exemples d'anneaux d'invariants Gorenstein ainsi que leur série de Hilbert. Nous pouvons voir dans ces exemples les relations énoncées ci-haut entre les deux premiers termes non nuls.

1.5. Interprétation géométrique des invariants

Dans la présente section nous donnons une interprétation géométrique des invariants. Pour un bref survol des notions de base de géométrie algébrique, nous référons le lecteur à l'annexe B.

Posons d'abord $V//G$ la variété algébrique affine correspondant à l'anneau $K[V]^G$. Autrement dit, supposons que $K[V]^G$ soit engendré par $f_1, \ldots, f_m$ comme K-algèbre et que ces générateurs satisfont aux relations

$$r_1(f_1, \ldots, f_m) = 0, \ldots, r_k(f_1, \ldots, f_m) = 0.$$

Ainsi, $K[V]^G \cong K[y_1, \ldots, y_m]/(r_1, \ldots, r_k)$ et nous définissons $V//G$ comme la sous-variété de K^m correspondant à l'idéal $(r_1, \ldots, r_k)$. Si K est un corps algébriquement clos, nous voulons montrer qu'il y a bijection entre $V//G$ et l'ensemble

V/G des orbites de G dans V. Cela nous permet donc de considérer V/G comme une variété algébrique affine.

Pour démontrer cette bijection, nous utilisons le morphisme $\phi : V \longrightarrow V//G$, appelé le **quotient catégorique**, qui correspond à l'inclusion $K[V]^G \hookrightarrow K[V]$. Plus précisément, si $v \in V$, on définit $\phi(v) = (f_1(v), \ldots, f_m(v))$.

Théorème 1.5.1. *Si K est algébriquement clos, il y a bijection entre les orbites dans V et les éléments de $V//G$.*

Démonstration. Par définition de ϕ, il est évident que si deux éléments v et w de V se trouvent sur une même orbite, alors $\phi(v) = \phi(w)$.

Il reste à montrer la surjectivité de ϕ. Soit $z = (z_1, \ldots, z_m) \in V//G \subseteq K^m$. Considérons l'idéal $\mathcal{I} = (f_1 - z_1, \ldots, f_m - z_m)$ de $K[V]$. Puisque K est algébriquement clos, l'ensemble des zéros $\mathcal{V}(\mathcal{I})$ n'est pas vide. Donc, il existe $v \in V$ tel que $f_1(v) = z_1, \ldots, f_m(v) = z_m$. Alors, ϕ est surjectif. □

Nous pouvons nous servir des propriétés gométriques de $V//G$ (ou V/G) pour comprendre $K[V]^G$. Par exemple, il est clair que $K[V]^G$ est polynomial si et seulement si $V//G$ est un espace vectoriel. Un espace vectoriel ne possède jamais de singularités (pour la définition d'une singularité dans un contexte algébrique, référez-vous à l'annexe B). Cependant, $V//G$ peut en posséder. Le théorème 1.5.5 montre que $V//G$ est toujours un espace vectoriel s'il ne possède pas de singularités. Auparavant, nous devons énoncer le fameux lemme de Nakayama et quelques corollaires.

Lemme 1.5.2 (Nakayama). *Soient $R = \bigoplus_{i \geq 0} R_i$ un anneau positivement gradué tel que $R_0 = K$ est un corps et μ l'idéal maximal $\bigoplus_{i>0} R_i$. Soit $M = \bigoplus_{d \geq d_0} M_d$ un R-module finiment engendré.*

Si $I \subseteq \mu$ est un idéal homogène tel que $I \cdot M = M$, alors $M = 0$.

Démonstration. Soit $I = \bigoplus_{d \geq d_1} I_d$ pour un $d_1 > 0$ et supposons que $M \neq 0$. On peut alors supposer que $M_{d_0} \neq 0$. Alors, le degré minimal d'un élément sera $d_1 + d_0 > d_0$, ce qui contredit que $M_{d_0} \subseteq I \cdot M$. □

Corollaire 1.5.3. *Soit $N \subseteq M$ un sous-module gradué tel que $M \subseteq N + \mu \cdot M$, alors $M = N$.*

Démonstration. Par hypothèse, nous avons que

$$\mu \cdot (M/N) \subseteq (\mu \cdot M + N)/N = M/N.$$

Donc, par Nakayama, $M/N = 0$. □

Corollaire 1.5.4. *Soient $m_1, m_2, \ldots, m_r \in M$ des éléments homogènes tels que $\overline{m_1}, \overline{m_2}, \ldots, \overline{m_r}$ forment une base de $M/(\mu \cdot M)$ comme K-espace vectoriel, alors $m_1, m_2, \ldots, m_r$ sont un système de générateurs minimal de M comme R-module.*

Démonstration. Soit $N = \langle m_1, m_2, \ldots, m_r \rangle$. Alors, par hypothèse, N est un sous-module de M tel que $M = N + \mu \cdot M$. Donc, par le corollaire précédent, $M = N$. De plus, s'il existait un système de générateurs plus petit pour M, leurs classes d'équivalences engendreraient $M/(\mu \cdot M)$, ce qui contredirait le fait que c'est un espace de dimension r. □

Nous sommes maintenant prêts pour démontrer :

Théorème 1.5.5. *Soit G un groupe agissant linéairement sur un espace vectoriel V de dimension finie sur un corps K algébriquement clos. La variété $V//G$ est un espace vectoriel si et seulement si elle ne possède pas de singularités.*

Démonstration. Il suffit de montrer que si $V//G$ ne possède pas de singularités, alors c'est un espace vectoriel. $K[V]^G$ est un anneau gradué positivement tel que $K[V]_0^G = K$. Soit μ l'idéal maximal comme dans le lemme de Nakayama. $V//G$ sans singularité implique que $dim_K(\mu/\mu^2) = dim(K[V]^G) = n$. Par le lemme de Nakayama (ou plutôt par le corollaire 1.5.4), l'idéal μ peut être engedré par n éléments. Or, puisque μ contient tous les éléments de degré strictement positif dans $K[V]^G$, cela implique que $K[V]^G$ est lui-même engendré, comme K-algèbre, par ces mêmes n éléments. Puisque nous avons supposé que $dim(K[V]^G) = n$, cela veut dire que ces n éléments sont algébriquement indépendants. Donc, $K[V]^G$ est polynomial. □

Chapitre 2

CAS NON MODULAIRE

Dans ce chapitre, nous nous attardons seulement au cas non modulaire. Tout au long du chapitre, nous étudions $K[V]^G$ en supposant que la caractéristique du corps K n'est pas un diviseur de l'ordre du groupe G. Comme nous le verrons, cette supposition aide grandement à l'analyse de $K[V]^G$. De plus, le cas non modulaire est important puisqu'il comprend le cas «classique» du corps de caractéristique 0.

2.1. Théorème de Molien

Dans le cas non modulaire, il est possible de calculer la série de Hilbert de $K[V]^G$ à partir d'aucune autre information que l'action du groupe (i.e. la représentation de G). Le principe est simple : si nous pouvons construire une projection dont l'image est $K[V]_j^G$, alors la trace de cette projection est égale à la dimension de $K[V]_j^G$. Il faut cependant faire attention puisque la trace est un élément de K tandis que la dimension est un nombre naturel. Cela ne pose évidemment pas problème en caractéristique 0. Heureusement, il existe une manière de donner un sens à cette interprétation en caractéristique p.

Supposons que $|G| = p^a m$ avec m non divisible par p. Alors, on peut toujours trouver un isomorphisme entre les racines m-ième de l'unité de $\bar{K}$ et les racines m-ième de l'unité dans $\mathbb{C}$. Soit maintenant $g \in G$ d'ordre non divisible par p. Alors, par l'isomorphisme précédent, les valeurs propres de g correspondent à des nombres complexes $\lambda_1, \lambda_2, \ldots, \lambda_n$. On définit alors

$$trace^0(g) := \lambda_1 + \lambda_2 + \cdots + \lambda_n \in \mathbb{C}$$

ainsi que

$$det^0(g) := \lambda_1\lambda_2\cdots\lambda_n \in \mathbb{C}.$$

Cette méthode, consistant à «relever» les traces et les déterminants dans un corps de caractéristique 0 est appelée le **relevé de Brauer** (pour plus de détails, voir **[Neu]** pp. 47-49). Ainsi, lorsque nous sommes en caractéristique p, il suffit de remplacer *trace* par $trace^0$ et *det* par det^0 dans l'argument qui suit.

Dans le cas non modulaire, on peut définir la projection $\pi^G = \frac{1}{|G|}\sum_{g\in G} g$, dont l'image est $K[V]^G$. Donc, $dim_K(K[V]_j^G) = trace(\pi^G, K[V]_j)$, c'est-à-dire la trace de π^G sur $K[V]_j$.

On obtient donc que

$$\mathcal{H}(K[V]^G, t) = \sum_{j=0}^{\infty} trace(\pi^G, K[V]_j)t^j = \frac{1}{|G|}\sum_{g\in G}\sum_{j=0}^{\infty} trace(g, K[V]_j)t^j.$$

De plus,

$$\sum_{j=0}^{\infty} trace(g, K[V]_j)t^j = \frac{1}{det(1-g^{-1}t)}.$$

En effet, pour montrer cette égalité, nous pouvons supposer que K est algébriquement clos, puisque travailler dans une extension de corps ne change aucun des deux côtés de l'égalité. Donc, il existe une base de V pour laquelle g est triangulaire supérieure (si K est de caractéristique nulle, g est diagonalisable). Supposons que les valeurs propres de g sont $\lambda_1, \ldots, \lambda_n$. Alors, les valeurs propres de g sur V^* sont $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. Donc, les valeurs propres de g sur $K[V]_j$ sont les produits de j des λ_i (avec possiblement des répétitions).

Autrement dit,

$$\sum_{j=0}^{\infty} trace(g, K[V]_j)t^j = \left(\sum_{j=0}^{\infty}\lambda_1^{-j}t^j\right)\cdots\left(\sum_{j=0}^{\infty}\lambda_n^{-j}t^j\right) = \prod_{i=1}^{n}\frac{1}{1-\lambda_i^{-1}t} = \frac{1}{det(1-g^{-1}t)}.$$

Nous venons donc de montrer :

Théorème 2.1.1 (T. Molien). *Soit G un groupe fini agissant linéairement sur un K-espace vectoriel V. Supposons que la caractéristique de K ne divise pas l'ordre de G (cas non modulaire).*

Alors,

$$\mathcal{H}(K[V]^G, t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{det(1-gt)}.$$

Ce théorème sert entre autres à suggérer le degré des générateurs des invariants, comme le démontre l'exemple suivant.

Exemple 2.1. *Soit G le groupe engendré par la matrice* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *agissant sur* $\mathbb{C}[x,y]$. *Alors* $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \}$ *et*

$$\mathcal{H}(\mathbb{C}[x,y]^G, t) = \frac{1}{4}\left[\frac{1}{(1-t)^2} + \frac{2}{1+t^2} + \frac{1}{(1+t)^2}\right] = \frac{1+t^4}{(1-t^2)(1-t^4)}.$$

Cette série suggère que $\mathbb{C}[x,y]^G = \mathbb{C}[f_1, f_2] \oplus f_3\mathbb{C}[f_1, f_2]$ *où les* f_i *sont de degré* 2, 4 *et* 4, *respectivement. Or, on peut trouver trois invariants avec les bons degrés :*

$$f_1 = x^2 + y^2$$

$$f_2 = x^2y^2$$

$$f_3 = x^3y - xy^3,$$

Avec ces valeurs pour f_1, f_2 *et* f_3, $\mathbb{C}[f_1, f_2] \oplus f_3\mathbb{C}[f_1, f_2]$ *est une sous-algèbre de* $\mathbb{C}[x,y]^G$ *qui a la même série de Hilbert que* $\mathbb{C}[x,y]^G$. *On conclut alors l'égalité.*

Remarque 2.1. *Il existe également une version plus générale du théorème de Molien qui permet de calculer, sous les mêmes hypothèses, la série de Hilbert de* $K[V]^G_\chi = \{f \in K[V] \mid g \cdot f = \chi(g)f\}$ *pour un caractère* χ *(c'est-à-dire que* χ *est un homomorphisme entre* G *et* $K^\times$*).*

La formule est

$$\mathcal{H}(K[V]^G_\chi, t) = \frac{1}{|G|}\sum_{g \in G} \frac{\chi(g)}{det(1-gt)}.$$

En particulier, le cas $\chi = det$ *joue un rôle important pour la théorie des anneaux Gorenstein puisque, dans le cas non modulaire, l'anneau* $K[V]^G_{det}$ *est isomorphe au module canonique. Cela est en fait le résultat du théorème de Watanabe dont nous rediscuterons (voir le théorème 2.5.1).*

2.2. Les deux premiers termes

Nous voulons maintenant nous servir du théorème de Molien pour trouver des formules pour les deux premiers termes de l'expansion de Laurent : $\psi_0(K[V]^G)$ et $\psi_1(K[V]^G)$.

Supposons que V est une représentation fidèle de G. Remarquons alors que, dans le cas non modulaire, il est facile de déduire $\psi_0(K[V]^G)$ par le théorème de Molien. En effet, soit $\{\lambda_i\}$ l'ensemble des valeurs propres de $g \in G$, un terme de la formule de Molien est de la forme

$$\frac{1}{|G|}\frac{1}{det(1-tg)} = \frac{1}{|G|}\frac{1}{\prod_{i=1}^{n}(1-t\lambda_i)}$$

et contribue au pôle d'ordre n pour $t = 1$ si et seulement si $\lambda_i = 1$ pour tous les i. Or, puisque nous sommes dans le cas non modulaire, la caractéristique de K ne divise pas l'ordre de g. Donc, g doit être l'identité de G pour contribuer au terme $\psi_0(K[V]^G)$. Donc,

$$\psi_0(K[V]^G) = \frac{1}{|G|}.$$

Nous verrons dans le théorème 3.1.2 que ce résultat demeure vrai dans le cas modulaire.

Nous pouvons utiliser la même technique pour calculer $\psi_1(K[V]^G)$. Auparavant, nous devons définir :

Définition 2.2.1. *Soit G un groupe muni d'une représentation sur un espace vectoriel V de dimension n. Un élément $g \neq 1$ de G d'ordre fini est appelé une* **réflexion** *s'il existe un hyperplan (donc un sous espace de V de dimension $n-1$) qui est laissé fixe point par point par g. Le groupe G est un* **groupe de réflexion** *s'il est engendré par des réflexions.*

Plus généralement, un élément ($\neq 1$) d'ordre fini est appelé une k-réflexion s'il fixe point par point un sous-espace de V de dimension $n-k$. Donc, les réflexions sont des 1-réflexions.

Par exemple, le groupe $\mathbb{S}_n$ (muni de l'action linéaire qui consiste à permuter les éléments de la base de V^*) est un groupe de réflexion puisqu'il est engendré par les couples (i,j), $i \neq j$. Chaque élément (i,j) fixe l'hyperplan qui correspond à l'équation $x_i - x_j = 0$.

Un terme de la formule de Molien contribue au pôle d'ordre $n-1$ si et seulement si $n-1$ des λ_i sont égaux à 1 et que la valeur propre restante n'est pas 1. Autrement dit, $g \in G$ contribue au deuxième terme si et seulement si g est une réflexion.

De plus, la contribution d'une réflexion g, si la valeur propre différente de 1 est λ, est

$$\lim_{t\to 1}\left((1-t)^{n-1}\frac{1}{|G|}\frac{1}{det(1-tg)}\right) = \frac{1}{|G|}\frac{1}{(1-\lambda)}.$$

Finalement, remarquons que

$$\frac{1}{1-\lambda}+\frac{1}{1-\lambda^{-1}} = \frac{(1-\lambda)+(1-\lambda^{-1})}{1-\lambda^{-1}-\lambda+1} = 1.$$

Autrement dit, si nous regroupons les réflexions avec leurs inverses, nous voyons que la contribution de chacune est $\frac{1}{2|G|}$. Si une réflexion est son propre inverse, elle a comme valeur propre $\lambda = -1$ et sa contribution est également $\frac{1}{|G|}\frac{1}{1-(-1)} = \frac{1}{2|G|}$.

Notez que cette valeur propre λ peut être vue comme un nombre complexe en utilisant le relevé de Brauer. Donc, cette analyse a un sens même dans le cas où la caractéristique de K n'est pas 0.

On conclut alors que dans le cas non modulaire

$$\psi_1(K[V]^G) = \frac{r}{2|G|},$$

où r est le nombre de réflexions de G.

L'exemple suivant nous montre comment cette analyse est particulièrement utile lorsque G est un groupe de réflexion.

Exemple 2.2. *Supposons que G est un groupe de réflexion. Nous verrons alors au théorème 2.3.1 que $K[V]^G$ est polynomial et donc que $K[V]^G = K[f_1,\ldots,f_n]$ pour certains $f_i \in K[V]$. Posons $d_i = deg(f_i)$. Nous avons alors la série de Hilbert*

$$\mathcal{H}(K[V]^G,t) = \frac{1}{\prod_{i=1}^{n}(1-t^{d_i})}.$$

Nous pouvons facilement calculer les premiers termes de l'expansion de Laurent de cette série et obtenir :

$$\mathcal{H}(K[V]^G,t) = \frac{1}{d_1d_2\cdots d_n}\frac{1}{(1-t)^n} + \frac{2(d_1+d_2+\cdots+d_n-n)}{d_1d_2\cdots d_n}\frac{1}{(1-t)^{n-1}} + \cdots$$

Or, cela nous donne beaucoup d'information en comparant avec les valeurs de ψ_0 *et* ψ_1 *que nous avons trouvées. Nous avons donc automatiquement que*

$$|G| = d_1 d_2 \cdots d_n$$

et le nombre de réflexions de G *est*

$$r = (d_1 - 1) + (d_2 - 1) + \cdots + (d_n - 1).$$

Nous voyons donc que ce sont les réflexions qui contribuent au terme $\psi_1(K[V]^G)$. Toujours en utilisant le théorème de Molien, il est facile de déduire que si G ne possède aucune réflexion, alors ce sont seulement les 2-réflexions qui contribuent au terme $\psi_2(K[V]^G)$. Par contre, dans ce cas, il est difficile de trouver une formule permettant de calculer la contribution de ces 2-réflexions. De même, s'il existe un nombre $1 \leq k \leq n$ pour lequel G ne possède pas de l-réflexions pour $l < k$, alors, ce sont seulement les k-réflexions qui contribuent au terme $\psi_k(K[V]^G)$.

Dans les prochaines sections, nous discutons des propriétés de l'anneau des invariants dans le cas non modulaire.

2.3. Anneau polynomial

Dans le cas non modulaire, il existe un critère pour savoir si $K[V]^G$ est polynomial ou non. Nous avons le résultat suivant énoncé sans preuve (voir **[Ben]**, théorème 7.2.1) :

Théorème 2.3.1 (Shephard-Todd, Chevalley). *Supposons que* G *est un groupe fini agissant fidèlement sur un espace* V *de dimension finie. Alors,*

$$K[V]^G \text{ polynomial} \Longrightarrow G \text{ est un groupe de réflexion.}$$

De plus, dans le cas non modulaire, nous avons l'équivalence

$$K[V]^G \text{ polynomial} \Longleftrightarrow G \text{ est un groupe de réflexion.}$$

En caractéristique 0, il existe une classification des groupes de réflexion irréductibles. Cette classification est donnée dans le tableau 7.1.1 de **[Neu]** et dans le tableau 7.1 de **[Ben]**.

2.4. Anneau Cohen-Macaulay

Théorème 2.4.1. *Dans le cas non modulaire,* $K[V]^G$ *est Cohen-Macaulay.*

Démonstration. $K[V] \cong K[x_1, \ldots, x_n]$ est un anneau Cohen-Macaulay puisque $\{x_1, \ldots, x_n\}$ est un système homogène de paramètres. Soit $\{\theta_1, \theta_2, \ldots, \theta_m\}$ un système homogène de paramètres pour $K[V]^G$ (l'existence d'un tel système est garantie par le théorème 1.3.6). Ainsi, $K[V]^G$ est un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module finiment engendré.

Or, $K[V]$, étant un $K[V]^G$-module finiment engendré par le théorème 1.3.6, est également un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module finiment engendré. Donc, $\{\theta_1, \theta_2, \ldots, \theta_m\}$ est un système homogène de paramètres pour $K[V]$, ce qui implique que $K[V]$ est un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module libre puisque $K[V]$ est Cohen-Macaulay.

Pour terminer la preuve, il suffit de montrer que $K[V]^G$ est un sommand direct de $K[V]$, c'est-à-dire qu'il existe un $K[V]^G$-module U tel que $K[V] = K[V]^G \oplus U$. Si c'est le cas, nous avons alors que $K[V]^G$ est également un $K[\theta_1, \theta_2, \ldots, \theta_m]$-module libre. Considérons l'homomorphisme π^G sur $K[V]$ défini par

$$\pi^G(f) = \frac{1}{|G|} \sum_{g \in G} g \cdot f.$$

Cet homomorphisme est en fait une projection dont l'image est exactement $K[V]^G$, ce qui termine la démonstration. □

2.5. Anneau Gorenstein

Dans le cas non modulaire, il est facile de savoir si $K[V]^G$ est Gorenstein gradué pour une action linéaire donnée du groupe G sur l'espace vectoriel V grâce au théorème de Watanabe.

Théorème 2.5.1 (Watanabe). *Soit G un groupe fini muni d'une représentation sur un espace vectoriel V de dimension finie sur le corps K. Si la caractéristique de K n'est pas un diviseur de $|G|$, alors*

$$\omega(K[V]^G) \cong K[V]^G_{det} := \{f \in K[V] \mid g \cdot f = \det(g) f, \ \ \forall g \in G\}.$$

En particulier, $K[V]^G$ est Gorenstein gradué $\iff G < SL(V)$.

Démonstration. Soit $A = K[f_1, \ldots, f_n]$ un anneau polynomial sur lequel $K[V]^G$ est libre (on se souvient que $K[V]^G$ est Cohen-Macaulay). Posons $k_i = deg(f_i)$ et

supposons que $k_i > 0$ pour tout i. Nous avons

$$\begin{aligned}\omega(K[V]^G) &\cong Hom_A(K[V]^G, A)[\sum_i (k_i - 1)] \\ &\cong (Hom_A(K[V], A)[\sum_i (k_i - 1)])^G \\ &\cong (K[V] \otimes det^{-1})^G \cong K[V]^G_{\text{det}}\end{aligned}$$

□

2.5.1. Classification des sous-groupes de $SL_n(\mathbb{C})$

Dans le cas où $K = \mathbb{C}$, nous avons par le théorème 2.5 que $\mathbb{C}[V]^G$ est Gorenstein si et $G < SL(V) \cong SL_n(\mathbb{C})$ où n est la dimension de V. Bien sûr, $\psi_0(K[V]^G) = 1/|G|$, comme c'est toujours le cas. Le fait que $G < SL_n(\mathbb{C})$ implique de plus que $\psi_1(K[V]^G) = 0$ puisque G ne contient aucune réflexion.

De plus, nous pouvons déduire du théorème de Molien :

Théorème 2.5.2. *Supposons que nous sommes dans le cas non modulaire et soit $k \geq 1$ tel que $codim(V^\sigma) \geq k$ pour tout $\sigma \neq 1$ (V^σ est le sous-espace fixé par σ). Alors,*

$$|G|\psi_k(K[V]^G) = \sum_W |G_W|\psi_k(K[V]^{G_W})$$

où la somme est prise sur les sous-espaces $W \subset V$ de codimension k et G_W est le sous-groupe de G qui fixe point par point W.

Nous montrerons au corollaire 3.2.9 que le théorème, pour $k = 1$, demeure vrai dans le cas modulaire. Pour $k > 1$, nous ne savons pas, à ce jour, si nous pouvons laisser tomber l'hypothèse du cas non modulaire.

Démonstration. Remarquons d'abord que si W et W' sont des espaces distincts de codimension k, alors $G_W \cap G_{W'} = \{1\}$. En effet, si $\sigma \in G_W \cap G_{W'}$, alors σ fixe point par point le sous-espace de V engendré par $W \cup W'$ qui est un espace de codimension $< k$, ce qui contredit l'hypothèse.

D'autre part, par le théorème de Molien, nous avons que

$$\begin{aligned}\mathcal{H}(K[V]^G,t) &= \frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{det(1-t\sigma)} \\ &= \frac{1}{|G|}\left(\frac{1}{(1-t)^n}+\sum_{W}\sum_{\substack{\sigma\in G_W\\ \sigma\neq 1}}\frac{1}{det(1-t\sigma)}+\sum_{\sigma\in G\setminus H}\frac{1}{det(1-t\sigma)}\right),\end{aligned}$$

où la somme est prise sur les W de codimension k et H est la réunion des G_W.

Or, nous pouvons réécrire

$$\begin{aligned}\sum_{W}\sum_{\substack{\sigma\in G_W\\ \sigma\neq 1}}\frac{1}{det(1-t\sigma)} &= \sum_{W}\frac{|G_W|}{|G_W|}\left(\sum_{\sigma\in G_W}\frac{1}{det(1-t\sigma)}-\frac{1}{(1-t)^n}\right) \\ &= \sum_{W}\left(|G_W|\mathcal{H}(K[V]^{G_W},t)-\frac{1}{(1-t)^n}\right).\end{aligned}$$

En remplaçant dans l'égalité précédente et en prenant l'expansion de Laurent autour de $t=1$ de chaque côté, nous obtenons, en remarquant que les éléments qui ne sont pas dans H ne contribuent pas au terme $\psi_k(K[V]^G)$,

$$\begin{aligned}\frac{\psi_0(K[V]^G)}{(1-t)^n} &+ \frac{\psi_k(K[V]^G)}{(1-t)^{n-k}}+O\left(\frac{1}{(1-t)^{n-k-1}}\right) \\ &= \frac{1}{|G|}\left(\frac{1}{(1-t)^n}+\sum_{W}|G_W|\frac{\psi_k(K[V]^{G_W})}{(1-t)^{n-k}}+O\left(\frac{1}{(1-t)^{n-k-1}}\right)\right).\end{aligned}$$

On obtient le résultat voulu en comparant les coefficients des deux expansions.

□

En particulier, pour $G<SL(V)$,

$$|G|\psi_2(\mathbb{C}[V]^G)=\sum_{W}|G_W|\psi_2(\mathbb{C}[V]^{G_W})$$

où la somme est prise sur les sous-espaces $W\subset V$ de codimension 2. Or, G_W est isomorphe à un sous-groupe fini de $SL_2(\mathbb{C})$ puisque tous les éléments de G_W sont diagonalisables et ont tous des valeurs propres égales à 1 pour les $n-2$ vecteurs propres se trouvant dans W.

Les valeurs de $\psi_2(\mathbb{C}[V]^{G_W})$ sont donc faciles à trouver puisqu'il existe une classification des sous-groupes finis de $SL_2(\mathbb{C})$. En effet, selon **[Spr]**, G_W est isomorphe à un des groupes énumérés dans le tableau 2.1.

Type	Description	$\lvert X_r\rvert$	$\mathcal{H}(\mathbb{C}[V]^{X_r}, t)$	$\lvert X_r\rvert\psi_2(\mathbb{C}[V]^{X_r})$
A_r	Groupe cyclique	r	$\frac{1-t^{2r}}{(1-t^2)(1-t^r)^2}$	$(r^2-1)/12$
D_r	Groupe dihédral	$4r$	$\frac{1-t^{4r+4}}{(1-t^4)(1-t^{2r})(1-t^{2r+2})}$	$(4r(r+3)-1)/12$
E_6	Groupe tétraédral	24	$\frac{1-t^{24}}{(1-t^6)(1-t^8)(1-t^{12})}$	14
E_7	Groupe octaédral	48	$\frac{1-t^{36}}{(1-t^8)(1-t^{12})(1-t^{18})}$	32
E_8	Groupe icosaédral	120	$\frac{1-t^{60}}{(1-t^{12})(1-t^{20})(1-t^{30})}$	90

TAB. 2.1. Classification des sous-groupes finis de $SL_2(\mathbb{C})$

On peut résumer les résultats du tableau 2.1 par la formule

$$|X_r|\psi_2(\mathbb{C}[V]^{X_r}) = (c(X_r)|X_r| - 1)/12,$$

où $c(A_r) = r$, $c(D_r) = r+3$, $c(E_6) = 7$, $c(E_7) = 8$, $c(E_8) = 9$. Remarquons que si nous nous restreignons au cas $K = \mathbb{R}$, seul le type A_r apparaît.

Nous venons de montrer :

Corollaire 2.5.3. *Soit G un sous-groupe fini de $SL(V)$, où V est un espace vectoriel de dimension finie sur $\mathbb{C}$. Alors,*

$$\psi_2(\mathbb{C}[V]^G) = \frac{1}{12|G|}\sum_W (c(G_W)|G_W| - 1)$$

où la somme est prise sur les sous-espaces W de codimension 2.

Nous pouvons réutiliser la même astuce en supposant cette fois que $\psi_1(\mathbb{C}[V]^G) = \psi_2(\mathbb{C}[V]^G) = 0$. Ainsi, pour calculer $\psi_3(\mathbb{C}[V]^G)$, nous serions intéressé à une classification complète des sous-groupes finis de $SL_3(\mathbb{C})$ qui peut être trouvée dans **[Yau]**. Cependant, il n'est pas nécessaire d'utiliser une telle classification pour trouver $\psi_3(\mathbb{C}[V]^G)$ puisque nous avons mentionné que la série de Hilbert d'un anneau Gorenstein satisfaisait à une équation fonctionnelle de la même forme que celle du théorème 1.4.3. Nous pouvons donc déduire du corollaire 1.4.4 que $\psi_3(\mathbb{C}[V]^G) = 0$.

Évidemment, il serait facile de généraliser cette méthode dans le sens que nous pouvons calculer $\psi_k(\mathbb{C}[V]^G)$ si $G < SL(V)$ et que G ne possède pas de r-réflexions pour $r < k$. En effet, dans ce cas,

$$\psi_1(\mathbb{C}[V]^G) = \psi_2(\mathbb{C}[V]^G) = \cdots = \psi_{k-1}(\mathbb{C}[V]^G) = 0.$$

Si k est impair, alors nous savons que $\psi_k(\mathbb{C}[V]^G) = 0$. Si k est pair, nous pourrions considérer une classification des sous-groupes de $SL_k(\mathbb{C})$. En fait, il n'est pas nécessaire de considérer tous les types de sous-groupes finis de $SL_k(\mathbb{C})$, mais seulement ceux qui ne possèdent aucun élément ayant des valeurs propres égales à 1 (sauf l'identité). En effet, un tel élément fixerait un sous-espace de codimension $< k$. De tels groupes sont appelés des groupes sans points fixes et nous en rediscuterons dans la section 2.6.

Exemple 2.3. *Voici quelques exemples d'anneaux d'invariants Gorenstein :*

(1) Soit G le sous-groupe de $SL_2(\mathbb{C})$ engendré par les matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^5 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

où $\omega = e^{2\pi i/6}$. $\mathbb{C}[V]^G$ est donc Gorenstein.

De plus, nous pouvons calculer (puisque nous sommes dans le cas non modulaire) la série de Hilbert avec le théorème de Molien et ensuite trouver son expansion de Laurent autour de $t = 1$. Ce calcul nous donne :

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{1}{12(1-t)^2} + \frac{71}{144} + \frac{71}{144}(1-t) + \cdots$$

Nous avons bel et bien que $\psi_1(\mathbb{C}[V]^G) = 0$ et que $\psi_2(\mathbb{C}[V]^G) = \psi_3(\mathbb{C}[V]^G)$.

(2) Posons cette fois $\omega = e^{2\pi i/10}$ et soit G le sous-groupe de $SL_4(\mathbb{C})$ engendré par les matrices

$$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^3 & 0 & 0 \\ 0 & 0 & \omega^9 & 0 \\ 0 & 0 & 0 & \omega^{27} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \omega^5 & 0 & 0 & 0 \end{pmatrix}.$$

Toujours en utilisant le théorème de Molien pour ensuite trouver l'expansion de Laurent autour de $t = 1$,

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{1}{40(1-t)^4} + \frac{1389}{3200} + \frac{1389}{1600}(1-t) + \cdots$$

Nous avons encore une fois $\psi_1(\mathbb{C}[V]^G) = 0$ *et les premiers termes non nuls sont reliés par* $4\psi_4(\mathbb{C}[V]^G) = 2\psi_5(\mathbb{C}[V]^G)$.

(3) Prenons cette fois $\omega = e^{2\pi i/34}$ *et soit* G *le sous-groupe de* $SL_8(\mathbb{C})$ *engendré par le matrices*

$$\begin{pmatrix} \omega & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^15 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^{15^2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^{15^3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^{15^4} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^{15^5} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega^{15^6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^{15^7} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Cette fois,

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{1}{272(1-t)^8} + \frac{30497}{69632} + \frac{30497}{17408}(1-t) + \cdots$$

Nous avons encore une fois $\psi_1(\mathbb{C}[V]^G) = 0$ *et les premiers termes non nuls sont reliés par* $8\psi_8(\mathbb{C}[V]^G) = 2\psi_9(\mathbb{C}[V]^G)$.

2.6. Groupes sans points fixes

Comme nous en avons discuté brièvement dans la section 2.5.1, les groupes sans points fixes jouent un rôle important dans l'analyse des termes de l'expansion de Laurent. Nous précisons ici la définition :

Définition 2.6.1. *Pour un groupe fini* G, *une représentation sur un espace vectoriel* V *de dimension finie sur un corps* K *est appelée une* ***représentation sans points fixes*** *si pour tout* $1 \neq \sigma \in G$, σ *ne possède pas de valeur propre égale à* 1.

Un groupe G muni d'une telle représentation est appelé un ***groupe sans points fixes****.*

Autrement dit, G ne possède aucune k-réflexion pour $k < dim_K(V)$.

Dans le cas $K = \mathbb{C}$, ces groupes jouent également un rôle dans la théorie du codage pour des réseaux d'antennes à haut débit, ce qui a mené les auteurs de l'article **[Sho]** à donner une classification complète de ces groupes (et de leurs représentations). En fait, cette classification avait déjà été démontrée dans le livre **[Wol]**.

Remarquons que puisque nous sommes dans le cas non modulaire, nous pouvons nous servir du théorème de Molien pour déduire que si $n = dim_K(V)$ et que G est sans points fixes, alors

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{\psi_0(\mathbb{C}[V]^G)}{(1-t)^n} + \psi_n(\mathbb{C}[V]^G) + \psi_{n+1}(\mathbb{C}[V]^G)(1-t) + \cdots$$

Autrement dit, $\psi_i(\mathbb{C}[V]^G) = 0$ pour $0 < i < n$. Ainsi, si $G < SL(V)$ et $n > 1$, on a, par le corollaire 1.4.4,

$$n\psi_n(\mathbb{C}[V]^G) = 2\psi_{n+1}(\mathbb{C}[V]^G).$$

Les groupes de l'exemple 2.3 sont des exemples de groupes sans points fixes qui sont également des sous-groupes de $SL(V)$. Nous donnons ici quelques exemples de groupes sans points fixes qui ne sont pas des sous-groupes de $SL(V)$.

Exemple 2.4. *(1) Posons $\omega = e^{2\pi i/20}$ et soit G le sous-groupe de $GL_4(\mathbb{C})$ engendré par les matrices*

$$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{13} & 0 & 0 \\ 0 & 0 & \omega^{13^2} & 0 \\ 0 & 0 & 0 & \omega^{13^3} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \omega^5 & 0 & 0 & 0 \end{pmatrix}.$$

En utilisant le théorème de Molien et en calculant l'expansion de Laurent autour de $t = 1$, nous trouvons

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{1}{80(1-t)^4} + \frac{2589}{6400} + \frac{4989}{3200}(1-t) + \cdots$$

(2) Posons $\omega = e^{2\pi i/30}$ *et soit* G *le sous-groupe de* $GL_4(\mathbb{C})$ *engendré par les matrices*

$$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{11} & 0 & 0 \\ 0 & 0 & \omega^{11} & 0 \\ 0 & 0 & 0 & \omega^{11^2} \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ \omega^3 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -\omega^3 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Toujours en utilisant le théorème de Molien et en calculant l'expansion de Laurent autour de $t = 1$, *nous trouvons*

$$\mathcal{H}(\mathbb{C}[V]^G, t) = \frac{1}{120(1-t)^4} + \frac{48251}{86400} + \frac{51973}{43200}(1-t) + \cdots$$

Comme nous pouvons le voir dans les exemples 2.3 et 2.4, il semble y avoir une régularité dans les $\psi_n(\mathbb{C}[V]^G)$, c'est-à-dire dans le premier terme non nul suivant $\psi_0(\mathbb{C}[V]^G)$. En effet, il semble que le dénominateur de $\psi_n(\mathbb{C}[V]^G)$ soit toujours un diviseur de

$$|G|2^{dim_K(V)}(dim_K(V)+1)(\frac{1}{2}dim_K(V)+1)^2.$$

Bien qu'une explication pour une telle formule nous soit inconnue, plusieurs calculs tendent à la confirmer. Nous l'énonçons donc comme conjecture.

Conjecture. *Soit* G *un groupe fini muni d'une représentation sans points fixes et soit* $n = dimV$, *alors*

$$|G|2^{dim_K(V)}(dim_K(V)+1)(\frac{1}{2}dim_K(V)+1)^2\psi_n(\mathbb{C}[V]^G)$$

est un entier.

Chapitre 3

CAS MODULAIRE

Dans ce chapitre, nous tentons de généraliser les résultats obtenus au chapitre précédent dans un contexte modulaire. Puisqu'il n'est plus possible d'utiliser le théorème de Molien en général, nous devons trouver de nouveaux outils nous permettant d'obtenir tout de même des résultats partiels. Pour cette raison, le cas modulaire s'avère beaucoup plus complexe que le cas non modulaire. La théorie présentée dans ce chapitre utilise des notions très diverses telles que le différent et la ramification d'idéaux premiers.

3.1. $\psi_0(K[V]^G)$

Commençons d'abord par le premier terme : $\psi_0(K[V]^G)$. Pour ce, nous aurons besoin du théorème suivant provenant de la théorie de Galois :

Théorème 3.1.1. *Supposons que V est une représentation fidèle du groupe fini G sur le corps K. Alors, $K(V)$ est une extension normale et séparable de $K(V)^G$ pour laquelle G est le groupe de Galois. $K[V]^G$ est intégralement clos dans son corps de fractions $K(V)^G$.*

Démonstration. Puisque G agit comme groupe d'automorphismes sur $K(V)$, il est évident que G est le groupe de Galois de l'extension.

Tout élément de $K(V)$ peut s'écrire comme f_1/f_2 où $f_2 \in K[V]^G$ en multipliant le numérateur et le dénominateur par les éléments de l'orbite de f_2. Cela implique que $K(V)^G$ est bien le corps de fractions de $K[V]^G$.

Finalement, un élément f de $K(V)^G$ qui est intègre sur $K[V]^G$ l'est aussi sur $K[V]$. Or, $K[V]$ étant intégralement clos dans $K(V)$, cela implique que $f \in K[V]$. Or, f étant G-invariant, nous avons que $f \in K[V]^G$. □

Nous pouvons maintenant montrer la même formule que dans le cas non modulaire.

Théorème 3.1.2. *Soient G un groupe fini et V une représentation fidèle de G de dimension finie sur un corps K, alors*

$$\psi_0(K[V]^G) = \frac{1}{|G|}$$

Il est important de noter qu'ici, aucune assomption n'est faite sur la caractéristique de K.

Démonstration. Par le théorème 3.1.1, nous pouvons conclure que

$$rang_{K[V]^G}(K[V]) = |G|.$$

Donc, par le lemme 1.4.1,

$$\psi_0(K[V]) = |G|\psi_0(K[V]^G).$$

Or, $\psi_0(K[V]) = 1$ puisque

$$\mathcal{H}(K[V], t) = \frac{1}{(1-t)^n}.$$

□

3.2. $\psi_1(K[V]^G)$

Dans le cas non modulaire, nous avions une formule pour $\psi_1(K[V]^G)$ que nous avons donné au théorème 2.5.2 (en posant $k = 1$) :

$$|G|\psi_1(K[V]^G) = \sum_W |G_W|\psi_1(K[V]^{G_W}),$$

où les W sont les hyperplans de V (c'est-à-dire des sous-espaces de codimension 1). Cette section vise à montrer que cette formule tient également dans le cas modulaire. Ensuite, nous nous servirons de ce résultat pour déduire quelques formules.

Pour y arriver, nous aurons besoins des notions de diviseurs premiers, de ramification et de différent que nous introduisons maintenant.

Remarque 3.1. *En fait, le théorème 2.5.2 est plus général puisqu'il donne cette formule pour un k quelconque, à condition que les ψ_i sont nuls pour $1 \leq i < k$. Dans le cas modulaire, nous ne démontrons que le cas $k = 1$. Le fait que le cas $k = 1$ demeure vraie dans le cas modulaire incite évidemment à se demander si nous pouvons également généraliser pour $k > 1$. La réponse à cette question n'est pas encore connue.*

Avant de continuer, nous devons cependant définir la notion d'anneau normal. Un anneau A est dit **normal** s'il est commutatif, noethérien et intégralement clos.

3.2.1. Diviseurs premiers

Nous verrons dans cette section que les idéaux premiers de hauteur 1 jouent un rôle important pour calculer le terme $\psi_1(K[V]^G)$ puisque certains d'entre eux correspondent à des hyperplans de réflexions.

Tout d'abord, nous aurons besoin de la définition d'idéal fractionnaire qui généralise le concept d'idéal.

Définition 3.2.1. *Soit A un anneau normal et L son corps de fractions. Un* **idéal fractionnaire** *α est un sous-A-module de L qui a la propriété qu'il existe $x \in A$ tel que $x\alpha \subseteq A$.*

En particulier, les idéaux sont des idéaux fractionnaires en prenant $x = 1$.

Un idéal fractionnaire est dit **principal** s'il est engendré par un seul élément $y \in L$ (comme A-module) et est noté (y).On dit qu'il est **divisoriel** s'il est une intersection d'idéaux fractionnaires principaux.

On écrit $\alpha^{-1} = \{b \in L \mid b\alpha \subseteq A\} = \bigcap_{a \in \alpha}(a^{-1})$, qui est un idéal fractionnaire divisoriel. Ainsi, $(\alpha^{-1})^{-1}$ est le plus petit idéal fractionnaire divisoriel qui contient α. On introduit alors la notation $\bar{\alpha} = (\alpha^{-1})^{-1}$.

Nous pouvons maintenant classer les idéaux fractionnaires par classes d'équivalence en posant que deux tels idéaux α et β sont **Artin-équivalents** (noté $\alpha \sim \beta$) si et seulement si $\bar{\alpha} = \bar{\beta}$ (i.e. $\alpha^{-1} = \beta^{-1}$). La classe d'équivalence de l'idéal α est noté $d(\alpha)$.

On dénote par $D(A)$ l'ensemble des classes d'équivalence des idéaux fractionnaires de A.

Cette équivalence est compatible pour la multiplication d'idéaux dans le sens que si $\alpha \sim \beta$, alors $\alpha\gamma \sim \beta\gamma$ pour γ un idéal fractionnaire. En effet, si $\alpha \sim \beta$, alors $\alpha^{-1} = \beta^{-1}$. Donc,

$$(\alpha\gamma)^{-1} = \{x \in L \mid x\gamma \subseteq \alpha^{-1}\} = \{x \in L \mid x\gamma \subseteq \beta^{-1}\} = (\beta\gamma)^{-1}.$$

Cela nous permet de faire de $D(A)$ un groupe abélien en définissant une opération entre les classes d'équivalence (notée additivement) comme suit :

$$d(\alpha) + d(\beta) := d(\alpha\beta).$$

Le neutre est donc $0 = d(A)$.

De plus, $D(A)$ est un **groupe abélien ordonné** si on introduit l'ordre

$$d(\alpha) \geq d(\beta) \iff \alpha \subseteq \beta.$$

Pour cet ordre, deux éléments de $D(A)$ ont toujours un infimum et un supremum. On peut montrer qu'un groupe abélien ordonné muni d'infimums et de supremums est toujours isomorphe au groupe abélien libre sur les éléments minimaux strictement positifs (voir par exemple la proposition 3.1.4 dans [**Ben**]).

Appelons ces éléments minimaux les **diviseurs premiers** de $D(A)$. Ainsi, $D(A)$ est le groupe abélien libre sur ses diviseurs premiers.

Or, ces diviseurs premiers correspondent exactement aux idéaux premiers de hauteur 1. En d'autres termes, si $\mathcal{P}$ est un idéal fractionnaire, alors $d(\mathcal{P})$ est un diviseur premier $\iff$ $\mathcal{P}$ est un idéal premier de hauteur 1.

Commençons d'abord par montrer les deux lemmes suivants.

Lemme 3.2.1. *Si $\mathcal{P}$ est un idéal divisoriel, alors $d(\mathcal{P})$ est un diviseur premier si et seulement si $\mathcal{P}$ est un idéal premier dans A.*

Démonstration. Supposons que $d(\mathcal{P})$ est un diviseur premier. Puisque nous avons que $d(\mathcal{P}) \geq 0$, alors $\mathcal{P} \subseteq A$. Si $x, y \in A$ et $xy \in \mathcal{P}$, alors $d(x) + d(y) = d(xy) \geq d(\mathcal{P})$. Or, puisque $D(A)$ possède des supremums et des infimums pour tous ses éléments, cela implique que $d(x) \geq d(\mathcal{P})$ ou $d(y) \geq d(\mathcal{P})$. Autrement dit, $x \in \mathcal{P}$ ou $y \in \mathcal{P}$.

Inversement, supposons que $\mathcal{P}$ est un idéal premier de A. Nous pouvons alors écrire $d(\mathcal{P}) = \sum n_i d(\mathcal{P}_i)$ où les $d(\mathcal{P}_i)$ sont des diviseurs premiers et, donc, des idéaux premiers. Ainsi, nous pouvons écrire $\mathcal{P} = \prod \mathcal{P}_i^{n_i}$, ce qui veut dire qu'il existe un i pour lequel $\mathcal{P} = \mathcal{P}_i$. □

Lemme 3.2.2. *Tout idéal premier non nul contient un idéal premier non nul qui est divisoriel. De plus, un idéal premier divisoriel ne peut être strictement contenu dans un autre.*

Démonstration. Soit $\mathcal{P}$ un idéal premier non nul et soit $0 \neq x \in \mathcal{P}$. Nous pouvons alors écrire $0 \neq d(x) = \sum n_i d(\mathcal{P}_i)$ de telle sorte que $n_i \geq 0$, que les $\mathcal{P}_i$ soient divisoriels et que les $d(\mathcal{P}_i)$ soient des diviseurs premiers. Par le lemme précédent, les $\mathcal{P}_i$ sont des idéaux premiers. Si $y \in \prod \mathcal{P}_i^{n_i}$, alors $d(y) \geq d(x)$ et donc $(y) \subseteq (x)$. Ainsi, $\prod \mathcal{P}_i^{n_i} \subseteq (x) \subseteq \mathcal{P}$. Or, $\mathcal{P}$ est premier, ce qui implique qu'il existe un i pour lequel $\mathcal{P}_i \subseteq \mathcal{P}$. □

Nous pouvons ainsi démontrer que les diviseurs premiers correspondent en effet aux idéaux premiers de hauteur 1.

Proposition 3.2.3. *Un idéal premier est divisoriel si et seulement s'il est de hauteur* 1.

Démonstration. Si $\mathcal{P}$ est un idéal premier de hauteur 1, il doit être divisoriel par le lemme 3.2.2. Inversement, supposons que $\mathcal{P}$ est divisoriel. S'il contient strictement un idéal premier, celui-ci doit contenir un idéal fractionnaire. Or, cela est impossible par le lemme 3.2.2. □

Notation. Soit A un anneau normal et L son corps de fractions. Pour chaque élément $0 \neq x \in L$, l'idéal fractionnaire principal (x) est divisoriel. Donc, il existe des uniques coefficients $v_{\mathcal{P}}(x) \in \mathbb{Z}$ tels que

$$d(x) = \sum_{\mathcal{P}} v_{\mathcal{P}}(x) d(\mathcal{P}),$$

où la somme est prise sur les idéaux premiers de hauteur 1. Cette somme est finie puisque $v_{\mathcal{P}}(x)$ est 0 sauf pour un nombre fini de $\mathcal{P}$.

3.2.2. Ramification

À la fin de ce chapitre, nous verrons que, comme dans le cas non modulaire, ce sont les réflexions qui contribuent au terme $\psi_1(K[V]^G)$, ce qui motive la compréhension du lien entre certains idéaux premiers de hauteur 1 et les hyperplans de réflexions. La notion de ramification permet, entre autres, de savoir quels sont les idéaux premiers de hauteur 1 qui correspondent à ces hyperplans.

Supposons que $A \subseteq B$ est une extension finie d'anneaux normaux dont les corps de fractions sont $L \subseteq L'$. Si β est un idéal premier de B, alors $\mathcal{P} = \beta \cap A$ est un idéal premier de A. Nous disons alors que β est **au-dessus** de $\mathcal{P}$. Dans ce cas, un résultat classique d'algèbre commutative est que β est de hauteur 1 si et seulement si $\mathcal{P}$ est de hauteur 1.

Donc, si β est de hauteur 1, nous pouvons comparer $v_{\mathcal{P}}$ et la restriction de v_β à L. En fait, par la discussion dans [**Ben**] juste avant le corollaire 3.2.6, nous avons que la restriction de v_β sur L est un multiple entier de $v_{\mathcal{P}}$. Définissons alors

$$v_\beta = e(\beta, \mathcal{P}) v_{\mathcal{P}}.$$

Le nombre $e = e(\beta, \mathcal{P})$ est appelé l'**index de ramification** de β sur $\mathcal{P}$. Nous disons que l'extension $A \subseteq B$ est **non ramifiée** en β si $e(\beta, \mathcal{P}) = 1$. Sinon, elle est **ramifiée**.

Dans le cas où $L \subseteq L'$ est une extension de Galois (c'est la cas qui nous intéresse) il existe une manière de mesurer la ramification à l'aide de la théorie des groupes. En effet, notons G le groupe d'automorphismes associé à l'extension. Notons $G_d(\beta)$ le sous-groupe de G défini par

$$G_d(\beta) = \{\sigma \in G \mid \sigma\beta\sigma^{-1} = \beta\}.$$

C'est le **groupe de décomposition** de β.

On s'intéresse alors au sous-groupe normal de $G_d(\beta)$ (appelé **groupe d'inertie** et noté G_β) composé des éléments qui agissent trivialement sur $B_\beta/\beta B_\beta$. Nous verrons que dans le cas de $K[V]^G$, les idéaux premiers β de hauteur 1 sont en

fait engendrés par des formes linéaires et correspondent à des hyperplans de réflexion. De plus, le lemme 3.2.4 nous donnera que $G_\beta = G_W$ si W est l'hyperplan correspondant à la forme linéaire qui engendre β.

Remarque 3.2. *Par le théorème 1.4.4 (iii) dans* [**Ben**], *G agit transitivement sur l'ensemble $\{\beta = \beta_1, \beta_2, \ldots, \beta_r\}$ des idéaux premiers au-dessus de $\mathcal{P}$. Donc, $e(\beta, \mathcal{P})$ ne dépend pas de β et est souvent noté $e(\mathcal{P})$.*

Le prochain lemme montre clairement, dans le cas des invariants, le lien étroit qui existe entre les notions de ramification, de groupes d'inertie et de réflexions. Pour W un hyperplan, nous notons β_W l'idéal premier de $K[V]$ engendré par une forme linéaire qui s'annule en W. Un hyperplan W est appelé un hyperplan de réflexion du groupe G si G_W n'est pas trivial.

Lemme 3.2.4. *Supposons que G agit fidèlement sur V. Si β est un idéal premier homogène de hauteur 1 de $K[V]$ avec un groupe d'inertie non trivial, alors $\beta = \beta_W$ pour un certain hyperplan de réflexion $W \subset V$. Le groupe d'inertie de β est alors G_W. Posons $\mathcal{P} = \beta \cap K[V]^G$. Si $char(K) = 0$, l'index de ramification $e(\mathcal{P})$ est égal à $|G_W|$. Si $char(K) = p$ et que $|G_W| = p^\alpha h$ où h n'est pas divisible par p, alors $e(\mathcal{P}) = h$.*

Démonstration. L'idéal β est engendré par un élément homogène (disons de degré d) puisque $K[V]$ est un domaine de factorisation unique. Supposons que $d \geq 2$. Alors, tout élément du groupe d'inertie fixe les éléments de degré 1, mais cela implique que le groupe d'inertie est trivial puisque l'action est fidèle, ce qui contredit l'hypothèse. Donc, β est engendré par un élément homogène de degré 1. Le groupe d'inertie de $\mathcal{P}$ est donc le groupe qui fixe point par point l'hyperplan W correspondant au générateur de β (i.e. G_W).

Pour trouver l'index de ramification, nous devons séparer la preuve en deux cas. Premièrement, supposons que $char(K) = 0$. Dans ce cas, G_W est cyclique, engendré par un élément g d'ordre h diagonalisable avec une seule valeur propre différente de 1. Donc, il existe une base $\{v_1, v_2, \ldots, v_n\}$ pour laquelle $g(v_i) = v_i$, $1 \leq i < n$ et $g(v_n) = \lambda v_n$, où $\lambda^h = 1$. Notons $\{x_1, x_2, \ldots, x_n\}$ la base duale, alors $K[V]^{G_W} = K[x_1, \ldots, x_{n-1}, x_n^h]$. Dans ce cas, $\beta = (x_n)$ et $\mathcal{P} = (x_n^h)$. Donc, $e(\mathcal{P}) = h$.

Finalement, supposons que $char(K) = p$. On peut alors écrire $|G_W| = p^a h$ où h n'est pas divisible par p. Puisque les éléments de G_W agissent trivialement sur W, on peut choisir une base $\{v_1, v_2, \ldots, v_n\}$ pour laquelle les éléments de G_W sont de la forme

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \rho_{1g} \\ 0 & 1 & \cdots & 0 & \rho_{2g} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \rho_{ng} \\ 0 & 0 & \cdots & 0 & \rho_{ng} \end{pmatrix}.$$

On peut donc choisir des générateurs g et $g_1, g_2, \ldots, g_a$ tels que $g_i(v_j) = v_j$ pour $1 \leq j < n$ et $g_i(v_n) = v_n + \sum_{j=1}^{n-1} \lambda_{ij} v_j$ pour certains coefficients $\lambda_{ij} \in K$. De plus, $g(v_j) = v_j$ pour $1 \leq j < n$ et $g(v_n) = \lambda v_n$ où $\lambda^h = 1$.

Pour la base duale $\{x_1, x_2, \ldots, x_n\}$ l'action est comme suit : $g(x_j) = x_j$ pour $1 \leq j < n$ et $g(x_n) = \lambda^{-1} x_n$. Ensuite, $g_i(x_j) = x_j - \lambda_{ij} x_n$ pour $1 \leq j < n$ et $g_i(x_n) = x_n$. Encore une fois, nous avons $\mathcal{P} = (x_n^h)$ et $e(\mathcal{P}) = h$. □

Comme mentionné précédemment, nous verrons plus tard que les réflexions sont les seuls éléments qui contribue à la valeur de $\psi_1(K[V]^G)$. Donc, il est important de bien comprendre la ramification des idéaux premiers de hauteur 1. Un outil nous permettant de tester s'il y a ramification ou non en un idéal premier de hauteur 1 est le différent (parfois appelé le différent de Dedekind). C'est à cette notion qu'est dédiée la prochaine section.

3.2.3. Différent

Supposons que $A \subseteq B$ est une extension finie d'anneaux normaux dont les corps de fractions sont $L \subseteq L'$. On peut alors voir L' comme un espace vectoriel sur L et, pour chaque $x \in L'$, la multiplication par x peut être vue comme la multiplication par une matrice avec coefficients dans L. On écrit alors $Tr_{L'/L}(x)$ pour la trace de cette matrice.

Les propriétés de base de cet objet sont que si on a $L \subseteq L' \subseteq L''$, alors $Tr_{L'/L} \circ Tr_{L''/L'} = Tr_{L''/L}$. De plus, dans le cas où $L \subseteq L'$ est une extension

séparable, alors la forme bilinéaire $(x, y) \longmapsto Tr_{L'/L}(xy)$ est un pairage non-dégénéré $L' \bigotimes_L L' \longrightarrow L$ (c'est-à-dire que si $Tr_{L'/L}(xy) = 0$ pour tout y, alors $x = 0$).

Nous supposons maintenant que $L \subseteq L'$ est une extension séparable. On définit alors

$$\mathcal{D}_{B/A}^{-1} = \{x \in L' \mid \forall y \in B,\ Tr_{L'/L}(xy) \in A\},$$

appelé le **différent inverse**.

Nous avons alors que l'application $\mathcal{D}_{B/A}^{-1} \longrightarrow B^*$ qui envoit x à l'application $y \longmapsto Tr_{L'/L}(xy)$ est un isomorphisme. De plus, $\mathcal{D}_{B/A}^{-1}$ est un idéal fractionnaire divisoriel et nous définissons son inverse

$$\mathcal{D}_{B/A} = (\mathcal{D}_{B/A}^{-1})^{-1}$$

que nous appelons le **différent**.

Comme il a été dit à la fin de la section précédente, ce différent sert, entre autres, à tester la ramification. En effet, nous avons le théorème :

Théorème 3.2.5. *Soit A un anneau normal, noethérien et intègre dont le corps de fractions est L. Soit $L \subseteq L'$ une extension de corps finie et séparable et soit B la fermeture intègre de A dans L'. Soit maintenant β un idéal premier de hauteur 1 dans B. Alors, $A \subseteq B$ est ramifiée en β si et seulement si $\beta \supseteq \mathcal{D}_{B/A}$.*

Démonstration. Voir [**Ben**], p.40. □

Il est donc très utile de trouver un test permettant de savoir si $\beta \supseteq \mathcal{D}_{B/A}$. Une manière d'y arriver est en calculant $v_\beta(\mathcal{D}_{B/A})$ puisque il est non nul seulement lorsque $\beta \supseteq \mathcal{D}_{B/A}$.

On peut d'ailleurs calculer la valeur de $v_\beta(\mathcal{D}_{B/A})$ localement dans le sens que

$$v_\beta(\mathcal{D}_{B/A}) = v_\beta(\mathcal{D}_{B/B^{G_\beta}}).$$

3.2.4. Formules homologiques

Il existe des méthodes homologiques nous permettant de trouver des relations entre les termes de l'expansion de Laurent. Ces méthodes consistent généralement à utiliser le module Ext. Nous référons le lecteur à l'annexe A pour plus de détails sur ce module.

L'approche utilisée par Luchezar L. Avramov, Ragnar-Olaf Buchweitz et Judith D. Sally dans [**Avr**] consiste à comparer les coefficients de l'expansion de Laurent en $t = 1$ des fonctions rationnelles

$$\sum_{i=0}^{j}(-1)^j\mathcal{H}(Ext_A^i(M,N),t) \quad \text{et} \quad \frac{\mathcal{H}(M,t^{-1})\mathcal{H}(N,t)}{\mathcal{H}(A,t^{-1})}$$

En fait, nous avons :

Théorème 3.2.6. *Si M et N sont des A-modules finiment engendrés tels que $Ext_A^i(M,N) = 0$ pour $i \gg 0$, alors il y a égalité des fonctions rationnelles*

$$\sum_i(-1)^i\mathcal{H}(Ext_A^i(M,N),t) = \frac{\mathcal{H}(M,t^{-1})\mathcal{H}(N,t)}{\mathcal{H}(A,t^{-1})}.$$

La 0-ième relation obtenue (i.e. la relation entre les coefficients de $(1-t)^0$ dans l'expansion de Laurent) est :

$$\psi_0(A)\psi_0(Hom_A(M,N)) = \psi_0(M)\psi_0(N).$$

La première relation (entre les coefficients de $(1-t)^1$) est :

$$\psi_0(A)(\psi_1(Hom_A(M,N)) - \psi_1(Ext_A^1(M,N))) =$$
$$\psi_1(A)\psi_0(Hom_A(M,N)) + \psi_0(M)\psi_1(N) - \psi_0(N)\psi_1(M).$$

On peut continuer ainsi pour obtenir d'autres relations de ce type. À titre d'exemple, si on utilise la notation

$$\epsilon_j(M,N) = \sum_{i=0}^{j}(-1)^i\psi_j(Ext_A^i(M,N))$$

la deuxième relation donne :

$$\psi_0(A)\epsilon_2(M,N) - \psi_1(A)\epsilon_1(M,N) + (\psi_2(A) - \psi_1(A))\epsilon_0(M,N) =$$
$$\psi_0(M)\psi_2(N) - \psi_1(M)\psi_1(N) + (\psi_2(M) - \psi_1(M))\psi_0(N).$$

Bien que nous avons besoin de la condition $Ext_A^i(M,N) = 0$ pour $i \gg 0$ dans le théorème 3.2.6, cette condition n'est pas nécessaire pour chacune des relations précédentes. Nous devons d'abord définir la notion d'anneau régulier.

Définition 3.2.2. *Un anneau A de dimension de Krull n est dit* ***régulier en codimension*** *k si A ne possède aucune singularité* ***ou*** *si les singularités sont toutes de codimension $> k$.*

Théorème 3.2.7. *Soient M et N des A-modules gradués où A est un anneau gradué.*

Si A possède un unique idéal premier $\mathcal{P}$ de hauteur 0 et $A_{\mathcal{P}}$ est un corps, alors la 0-ième relation est vérifiée.

Si A est un domaine intègre régulier en codimension 1, alors la première relation est vérifiée.

Si A est un domaine de factorisation unique régulier en codimension 2, alors la deuxième relation est vérifiée.

Pour les démonstrations de ces résultats et pour plus de détails, nous vous référons à [**Avr**].

3.2.5. Formule de ramification

Avec les mêmes hypothèses que dans le théorème 3.2.5, Benson et Crawley-Boevey (voir [**Ben2**]) ont démontré une formule de ramification :

Théorème 3.2.8.

$$|L' : L|\psi_1(A) - \psi_1(B) = \frac{1}{2}\sum_{\beta} v_\beta(\mathcal{D}_{B/A})\psi_1(B/\beta),$$

où la somme est prise sur les idéaux premiers homogènes β de hauteur 1.

Démonstration. Par le lemme 1.4.2, nous avons que

$$\begin{aligned}\psi_1(\mathcal{D}_{B/A}^{-1}) - \psi_1(B) = \psi_1(\mathcal{D}_{B/A}^{-1}/B) &= \sum_{\beta} long_{B_\beta}((\mathcal{D}_{B/A}^{-1}/B)_\beta)\psi_1(B/\beta) \\ &= \sum_{\beta} v_\beta(\mathcal{D}_{B/A})\psi_1(B/\beta)\end{aligned}$$

D'un autre côté, $\mathcal{D}_{B/A}^{-1} \cong B^*$ comme A-modules. Donc, il suffit d'utiliser la première relation du théorème 3.2.7 en posant $M = B$ et $N = A$ pour obtenir

$$\psi_1(\mathcal{D}_{B/A}^{-1}) + \psi_1(B) = 2|L' : L|\psi_1(A).$$

Nous obtenons le résultat voulu en combinant les deux égalités. □

Bien sûr, nous voulons appliquer ce résultat dans le cas des invariants d'un groupe fini.

Corollaire 3.2.9. *Nous avons la formule*

$$|G|\psi_1(K[V]^G) = \sum_W |G_W|\psi_1(K[V]^{G_W}),$$

où la somme est prise sur les hyperplans de V.

Démonstration. Dans notre cas, $G_W \cap G_{W'} = \{1\}$ pour des hyperplans W et W' distincts. Autrement dit, β_W est le seul idéal premier homogène de hauteur 1 sur lequel l'extension $K[V]^{G_W} \subseteq K[V]$ est ramifiée. Donc, par le théorème 3.2.8,

$$\begin{aligned} |G_W|\psi_1(K[V]^{G_W}) &= \frac{1}{2}v_{\beta_W}(\mathcal{D}_{K[V]/K[V]^{G_W}})\psi_1(K[V]/\beta_W) \\ &= \frac{1}{2}v_{\beta_W}(\mathcal{D}_{K[V]/K[V]^{G}})\psi_1(K[V]/\beta_W) \end{aligned}$$

Donc, en prenant la somme de chaque côté sur tous les hyperplans et en réutilisant le théorème 3.2.8,

$$\begin{aligned} \sum_W |G_W|\psi_1(K[V]^{G_W}) &= \frac{1}{2}\sum_W v_{\beta_W}(\mathcal{D}_{K[V]/K[V]^{G}})\psi_1(K[V]/\beta_W) \\ &= |G|\psi_1(K[V]^G) \end{aligned}$$

□

Cette formule est en fait très utile puisque les $\psi_1(K[V]^{G_W})$ sont plus faciles à obtenir. En effet, le prochain théorème montre que $K[V]^{G_W}$ est polynomial.

Théorème 3.2.10. *Soit G un groupe fini agissant fidèlement sur un espace vectoriel de dimension finie et supposons qu'il existe un hyperplan W de V qui est laissé fixe point par point par les éléments de G.*

Alors, $K[V]^G$ est polynomial, disons

$$K[V]^G = K[h_1, h_2, \ldots, h_n],$$

où $\deg(h_i) = d_i$.

En particulier,

$$\mathcal{H}(K[V]^G, t) = \frac{1}{\prod_{i=1}^n (1 - t^{d_i})}$$

et donc,

$$\psi_1(K[V]^G) = \frac{1}{2|G|}((d_1 - 1) + (d_2 - 1) + \cdots + (d_n - 1)).$$

Démonstration. Tout d'abord, remarquons que nous pouvons supposer que K est algébriquement clos. En effet, prendre une extension du corps ne change pas les générateurs des invariants et, donc, ne change pas le fait que $K[V]^G$ soit polynomial ou non.

Supposons, par l'absurde, qu'il existe une singularité $x \in V//G$. Considérons l'ensemble des translations par W : $T = \{\tau_w \mid w \in W\}$, où $\tau_w(v) = v+w$. Puisque W est invariant pour l'action de G, ces deux actions commutent, c'est-à-dire que $\sigma(v + w) = \sigma(v) + w$ pour chaque $\sigma \in G$. Cela induit donc une action de T sur $K[V]^G$ et, ainsi, sur $V//G$.

Or, cette action préserve les singularités, c'est-à-dire que pour tout $w \in W$, $\tau_w(x)$ est aussi une singularité. W étant de codimension 1, cela implique que l'ensemble des singularités est aussi de codimension 1. Cependant cela est impossible pour un anneau normal (comme $K[V]^G$) par le critère de Serre (voir **[Eis]**, théorème 11.5). □

Il existe également d'autres preuves (ou variations de cette preuve) pour ce résultat ne passant pas par la géométrie algébrique. Voir, par exemple, **[Har]** et **[Chu]**.

Nous n'avons qu'à substituer ce résultat dans le corollaire 3.2.9 pour démontrer :

Théorème 3.2.11. *Soit G un groupe fini agissant fidèlement sur V, alors pour chaque hyperplan W de V, $K[V]^{G_W}$ est polynomial, disons*

$$K[V]^{G_W} = K[h_1^W, h_2^W, \ldots, h_n^W]$$

où chaque h_i^W est de degré d_i^W.

Alors,

$$\psi_1(K[V]^G) = \frac{1}{2|G|} \sum_W ((d_1^W - 1) + (d_2^W - 1) + \cdots + (d_n^W - 1)).$$

Remarque 3.3. *Le résultat obtenu précédemment pour $\psi_1(K[V]^G)$ dans le cas non modulaire n'est évidemment qu'un cas particulier du dernier théorème. En effet, dans le cas non modulaire, le nombre de réflexions peut s'écrire $r = \sum_W r_W$*

où r_W est le nombre de réflexions qui fixent l'hyperplan W. Or, nous avons vu dans l'exemple 2.2 que $r_W = \sum_{i=1}^{n}(d_i^W - 1)$.

Exemple 3.1. *Supposons que $K = \mathbb{F}_{25}$ et $V = K^3$. Considérons le groupe $G < GL_n(K)$ d'ordre 20 engendré par les matrices*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nous pouvons calculer $\psi_1(K[V]^G) = \psi_1(K[x,y,z]^G)$ en nous servant du théorème 3.2.11 (remarquons qu'il ne serait pas possible de tout simplement se servir du théorème de Molien puisque $|G| = 20$ est un multiple de la caractéristique de K). Puisque le groupe est fini, il est possible d'énumérer tous les éléments de G et de calculer pour chaque élément l'espace propre associé à la valeur propre 1 (i.e. le sous-espace fixé par cet élément). Nous pouvons ensuite retenir seulement les éléments fixant un hyperplan.

Dans notre cas, nous trouvons 6 hyperplans de réflexion :

$$\begin{aligned} W_1 &= \langle (1,0,0), (0,0,1) \rangle \\ W_2 &= \langle (1,0,0), (0,1,0) \rangle \\ W_3 &= \langle (1,0,0), (0,1,-1) \rangle \\ W_4 &= \langle (1,0,0), (0,1,1) \rangle \\ W_5 &= \langle (1,0,0), (0,1,2) \rangle \\ W_6 &= \langle (1,0,0), (0,1,3) \rangle \end{aligned}$$

où la notation $\langle X \rangle$ désigne le sous-espace de V engendré par la liste de vecteurs X. Parmi les réflexions que nous avons retenues, seule la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

fixe l'hyperplan W_1. Donc, $K[V]^{G_{W_1}} = K[x, y^2, z]$ et $\sum(d_i^{W_1} - 1) = 1$.

L'hyperplan W_2, cependant, est fixé par 9 réflexions. Il est cependant facile de constater, par la définition de W_2 que x et y sont des invariants. Il ne reste plus qu'à trouver le troisième générateur. Une technique souvent utilisée est de prendre une des variables et de la multiplier par tous les éléments de son orbite. Si nous faisons cela avec z, nous obtenons

$$\omega = (z(z+y)(z+2y)(z+3y)(z+4y)(-z)(-z-y)(-z-2y)(-z-3y)(-z-4y))$$

et $K[V]^{Gw_2} = K[x, y, \omega]$. Donc, cette fois-ci, $\sum(d_i^{W_2} - 1) = 9$.

Nous pouvons continuer ainsi pour les autres hyperplans pour obtenir :

$$\begin{aligned}
\sum(d_i^{W_1} - 1) &= 1 \\
\sum(d_i^{W_2} - 1) &= 9 \\
\sum(d_i^{W_3} - 1) &= 2 \\
\sum(d_i^{W_4} - 1) &= 2 \\
\sum(d_i^{W_5} - 1) &= 2 \\
\sum(d_i^{W_6} - 1) &= 2
\end{aligned}$$

Donc, nous pouvons déduire en nous servant du théorème 3.2.11 que

$$\psi_1(K[V]^G) = \frac{1}{2|G|}(1 + 9 + 2 + 2 + 2 + 2) = \frac{9}{20}.$$

Autrement dit,

$$\mathcal{H}(K[V]^G, t) = \frac{1/20}{(1-t)^n} + \frac{9/20}{(1-t)^{n-1}} + O\left(\frac{1}{(1-t)^{n-2}}\right).$$

Nous pouvons par exemple donner une formule explicite pour le cas spécial $K = \mathbb{F}_p$ où p est premier (à condition que l'action du groupe G soit fidèle). Cette formule était une conjecture de Carlisle-Kropholler qui a été démontrée par Benson et Crawley-Boevey dans [**Ben2**]. Nous déduisons ici ce résultat du théorème 3.2.11.

Pour un hyperplan W, on peut toujours choisir une base $\{v_1, \ldots, v_n\}$ de V telle que W est engendré par $\{v_2, \ldots, v_n\}$. Sur cette base, la représentation matricielle

d'un élément de G_W est de la forme

$$\begin{pmatrix} \rho_{1g} & 0 & \cdots & 0 \\ \rho_{2g} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{ng} & 0 & \cdots & 1 \end{pmatrix}$$

Soit alors h_W l'ordre du groupe formé des ρ_{1g} tels que $g \in G_W$. Posons également a_W comme étant le nombre de i entre 2 et n pour lesquels les ρ_{ig} ne sont pas tous 1.

On voit alors que G_W est en fait un produit direct entre le groupe $(\mathbb{Z}/(p))^{a_W}$ ($a_W \leq n-1$) et le groupe cyclique $\mathbb{Z}/(h_W)$ où h_W est un diviseur de $p-1$. En réajustant la base de V comme il faut, on peut écrire que G_W est engendré par les éléments g et $g_2, \ldots, g_{a_W+1}$ tels que

$$g(v_1) = \lambda v_1 \quad g_i(v_1) = v_1 + v_i$$
$$g(v_j) = v_j \quad g_i(v_j) = v_j \qquad (j > 1)$$

où λ est un racine primitive de l'unité d'ordre h_W dans $\mathbb{F}_p$.

L'action de ces générateurs sur la base duale $\{x_1, \ldots, x_n\}$ est alors donnée par

$$g(x_1) = \lambda^{-1} x_1 \quad g_i(x_1) = x_1$$
$$g(x_j) = x_j \qquad g_i(x_j) = x_j - \delta_{ij} x_1 \qquad (j > 1)$$

où δ_{ij} est le delta de Kronecker.

En sachant cela, nous pouvons facilement déduire les invariants du groupe G_W qui sont donnés dans le lemme suivant.

Lemme 3.2.12. *Les invariants $B^{G_W} = \mathbb{F}_p[x_1, \ldots, x_n]^{G_W}$ forment un anneau polynomial*

$$\mathbb{F}_p[x_1^{h_W}, x_2^p - x_2 x_1^{p-1}, \ldots, x_{a_W+1}^p - x_{a_W+1} x_1^{p-1}, x_{a_W+2}, \ldots, x_n].$$

Démonstration. Les générateurs donnés sont définitivement des invariants puisqu'ils sont des produits d'orbites des x_i. Il est également clair que $B \supseteq B^{G_W}$ est une extension finie de degré $h_W p^{a_W}$. Or, ce nombre est également l'ordre du groupe G_W et donc, si on passe aux corps de fractions, l'extension est du degré prédit par la théorie de Galois. Il ne reste plus qu'à remarquer que cet anneau est intègralement clos pour conclure l'égalité avec les invariants. □

Il ne nous reste qu'à utiliser ce résultat dans le théorème 3.2.11 pour démontrer la conjecture de Carlisle-Kropholler :

Théorème 3.2.13 (Conjecture de Carlisle-Kropholler). *Soit G comme précédemment, alors*

$$\psi_1(\mathbb{F}_p[V]^G) = \frac{1}{2|G|}\sum_W((p-1)a_W + h_W - 1),$$

où la somme est prise sur tous les hyperplans de réflexions de G.

3.3. $\psi_2(K[V]^G)$ ET 2-RÉFLEXIONS

Nous pouvons nous servir du théorème 3.2.7 pour déduire un résultat intéressant au sujet du terme $\psi_2(K[V]^G)$.

Corollaire 3.3.1. *Soit G un groupe fini agissant linéairement sur un espace vectoriel V de dimension finie sur un corps K. Si $K[V]^G$ est un domaine de factorisation unique et que G ne possède ni réflexions ni 2-réflexions, alors*

$$\psi_1(K[V]^G) = \psi_2(K[V]^G) = 0.$$

Ce résultat est clair dans le cas non modulaire. Cependant, ici, nous ne faisons aucune hypothèse sur la caractéristique du corps.

Démonstration. Il suffit d'appliquer le théorème 3.2.7 dans le cas $A = K[V]^G$ et $M = N = K[V]$. Le fait qu'il n'y ait pas de réflexions et de 2-réflexions implique que $K[V]^G$ soit régulier en codimension 2. Les hypothèses du théomrème 3.2.7 sont donc bien vérifiée. En utilisant la première relation de ce théorème, nous obtenons facilement que $\psi_1(K[V]^G) = 0$ puisque

$$\psi_1(Ext^1_{K[V]^G}(K[V], K[V])) = \psi_1(Hom_{K[V]^G}(K[V], K[V])) = 0.$$

En effet, les $Ext^i_{K[V]^G}(K[V], K[V])$ sont de codimension > 2 à cause de la régularité de $K[V]^G$ en codimension 2 et $Hom_{K[V]^G}(K[V], K[V]) \cong K[V] \cdot G$.

Ensuite, nous pouvons utiliser ce résultat dans la deuxième relation pour obtenir que $\psi_2(K[V]^G) = 0$. Encore une fois, beaucoup des termes de cette relation s'annulent pour les mêmes raisons que celle mentionnées ci-haut. □

Ce corollaire nous montre à quel point il est important de savoir si $K[V]^G$ est un domaine de factorisation unique ou non. Il existe en fait un théorème qui permet de tester s'il en est un. Nous l'énonçons ici sans preuve (voir [**Ben**]) :

Théorème 3.3.2 (Nakajima). *$K[V]^G$ est un domaine de factorisation unique si et seulement s'il n'existe pas d'homomorphismes de groupes $G \longrightarrow K^\times$ non triviaux prenant la valeur 1 sur toutes les réflexions.*

3.4. p-GROUPES EN CARACTÉRISTIQUE p

Le corollaire 3.3.1 nous donne des conditions pour annuler les deux premiers termes de l'expansion (après $\psi_0(K[V]^G)$. Dans cette section nous nous intéressons à savoir quels termes peuvent être annulés ainsi dans un cas particulier : les p-groupes en caractéristique p.

Par définition, un groupe G est appelé un p-groupe si $|G| = p^\alpha$ pour un entier $\alpha \geq 1$.

Supposons que R est un anneau polynomial sur un corps K de caractéristique p et que G est un p-groupe agissant sur R comme un groupe d'automorphismes de K-algèbres. Nous verrons qu'il est possible de déduire que quelques-uns des $\psi_i(R^G)$ seront nuls et de borner la valeur du premier $\psi_i(R^G)$ potentiellement non nul (nous excluons évidemment $\psi_0(R^G)$ qui est déjà connu).

Plus précisément, définissons l' **application transfert** (parfois appelé l' **application trace**) comme suit :

$$\begin{aligned} Tr^G : R &\longrightarrow R^G \\ r &\longmapsto \sum_{\sigma \in G} \sigma(r) \end{aligned}$$

Notons l'image de ce transfert par $I_G = Tr^G(R)$. Il est possible de vérifier que I_G est un idéal de R^G. Nous verrons que $\psi_i(R^G) = 0$ pour $1 \leq i < haut(I_G)$. Autrement dit, c'est la hauteur de I_G qui détermine quel sera le premier terme après $\psi_0(R^G)$ qui pourra être non nul. En fait, nous avons seulement défini la hauteur d'un idéal premier. Pour un idéal quelconque I, la hauteur de I est le minimum des hauteurs des idéaux premiers qui contiennent I.

Bien qu'il existe une infinité de KG-modules (c'est-à-dire des K-espaces vectoriels munis de l'action linéaire du groupe G) indécomposables non isomorphes entre eux, seul un nombre fini de ceux-ci interviennent dans la décomposition de R^G (voir **[Kar]**). Soit alors D le maximum des dimensions des KG-modules indécomposables de la décomposition de R^G, excluant ceux isomorphes à KG. Alors, nous avons le résultat suivant tiré de **[Bro2]** :

Proposition 3.4.1. *En utilisant les notations de la discussion qui précède,*

(1) Pour tout $i \geq 0$,

$$\frac{|G|-D}{|G|}dim(R^G/I_G)_i \leq dim(R_i^G) - \frac{1}{|G|}dim(R)_i \leq \frac{|G|-1}{|G|}dim(R^G/I_G)_i.$$

(2) Pour $0 \leq i < haut(I_G)$, *nous avons que* $\psi_i(R^G/I_G) = 0$ *et donc*

$$\psi_0(R^G) = \frac{1}{|G|}, \psi_i(R^G) = 0 \text{ pour } 1 \leq i < haut(I_G)$$

et

$$\frac{|G|-D}{|G|}\psi_{haut(I_G)}(R^G/I_G) \leq \psi_{haut(I_G)}(R^G) \leq \frac{|G|-1}{|G|}\psi_{haut(I_G)}(R^G/I_G).$$

Démonstration. *(1)* N'importe quel KG-module indécomposable qui intervient dans la décomposition de R_i contient un invariant puisque nous avons supposé que G est un p-groupe. Donc, $dim(R_i^G)$ est le nombre de KG-modules indécomposables dans la décomposition de R_i. Le seul sous-KG-module de R sur lequel l'application Tr^G ne s'annule pas est la représentation régulière de dimension $|G|$ pour laquelle l'image est unidimensionnelle. Donc, $dim(I_G)_i$ est le nombre de copies de la représentation régulière dans la décomposition de R_i et $dim(R^G/I_G)_i$ est le nombre de copies des autres KG-modules indécomposables. En particulier,

$$|G|dim(I_G)_i \leq dim R_i$$

et

$$dim(R^G/I_G)_i \leq dim R_i - |G|dim(I_G)_i \leq D\, dim(R^G/I_G)_i$$

puisque tout autre KG-module indécomposable dans la décomposition a dimension entre 1 et D.

En soustrayant $|G|dim(R^G/I_G)_i$ de toutes parts de l'inégalité et en divisant par $-|G|$, nous obtenons l'inégalité du lemme.

(2) Nous avons

$$\mathcal{H}(R^G/I_G, t) = \frac{\psi_{haut(I_G)}(R^G/I_G)}{(1-t)^{n-haut(I_G)}} + O\left(\frac{1}{(1-t)^{n-haut(I_G)-1}}\right).$$

Il suffit alors d'utiliser *(1)*.

□

CONCLUSION

La série de Hilbert est un outil très utile en théorie des invariants puisque ses propriétés réflètent souvent des propriétés de l'anneau des invariants. Entre autres, il s'est avéré très informatif de comprendre l'expansion de Laurent de cette série autour de $t = 1$. Par exemple, nous avons vu qu'un des termes nous donne de l'information sur les réflexions dans le groupe. Cependant, il est en général difficile de calculer ces termes. Heureusement, dans le cas non modulaire, il existe une formule, donnée par le théorème de Molien, qui nous permet de trouver la série de Hilbert (il suffit ensuite de trouver son expansion de Laurent). De plus, dans ce cas, nous savons que nous pouvons calculer le nombre de réflexions à partir du deuxième terme de l'expansion. Par contre, dans le cas modulaire, nous n'avons pas de formules nous donnant directement la série de Hilbert. Nous avons cependant vu que le deuxième terme de l'expansion donne, encore une fois, une information au sujet des réflexions du groupe. Par contre, cette information est un peu plus subtile que dans le cas non modulaire.

Un des buts visés de ce mémoire est de montrer qu'il reste encore énormément de chemin à faire dans cette étude et que, finalement, nous ne connaissons que très peu de choses au sujet des termes de l'expansion. Pourtant, l'étude de ces termes semble intéressante dans le contexte de la théorie des invariants.

BIBLIOGRAPHIE

[Ati] M.F. ATIYAH ET I.G. MACDONALD, *Introduction to Commutative Algebra*, Adison-Wesley Series in Mathematics, Reading, Massachussets, 1969.

[Avr] LUCHEZAR L. AVRAMOV, RAGNAR-OLAF BUCHWEITZ, JUDITH D. SALLY, *Laurent Coefficients and Ext of Finite Graded Modules*, Mathematische Annalen 307, pp. 401-415, 1997.

[Ben] D.J. BENSON, *Polynomial Invariants of Finite Groups*, Cambridge University Press, London, 1993.

[Ben2] D.J. BENSON ET W.W. CRAWLEY-BOEVEY, *A ramification formula for Poincaré series, and a hyperplane formula in modular invariant theory.*, Bulletin of the London Mathematical Society, 1995.

[Bro] ABRAHAM BROER, *The Direct Summand Property in Modular Invariant Theory*, Transformation Groups 10 :1, pp. 5-27, 2005.

[Bro2] ABRAHAM BROER, *Hilbert Series Expansion*, correspondance privée, 2006.

[Bum] DANIEL BUMP, *Algebraic Geometry*, World Scientific, London, 1998.

[Chu] JIANJUN CHUAI, *On the Invariants of Modular Groups*, preprint, 2006.

[Der] HARM DERKSEN ET GREGOR KEMPER, *Computational Invariant Theory*, Springer-Verlag, New York, 2002.

[Eis] DAVID EISENBUD, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 2002.

[Har] JULIA HARTMANN ET ANNE SHEPLER, *Jacobians of Reflection Groups*, Transactions of the American Mathematical Society, 2004.

[Jar] MARCO V. JARIĆ ET JOSEPH L. BIRMAN, *New algorithms for the Molien function*, J. of Mathematical Physics 18, pp. 1456-1458, 1977.

[Jar2] MARCO V. JARIĆ ET JOSEPH L. BIRMAN, *Calculation of the Molien generating function for invariants of space groups*, J. of Mathematical Physics 18, pp. 1459-1465, 1977.

[Jar3] M. V. JARIĆ, L. MICHEL ET R.T. SHARP, *Zeros of covariant vector fields for the point groups : invariant formulation*, Journal de physique 45, pp. 1-27, 1984.

[Kar] D.B. KARAGUEUZEIAN ET P. SYMONDS, *The Module Structure of a Group Action on a Polynomial Ring : A Finiteness Theorem*, J. Algebra 218, pp. 672-692, 1999.

[Lan] SERGE LANG, *Algebra, Third edition*, Springer-Verlag, New York, 2002.

[Neu] MARA D. NEUSEL ET LARRY SMITH, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs, American Mathematical Society, Providence, 2002.

[Osb] M. SCOTT OSBORNE, *Basic Homological Algebra*, Springer-Verlag, New York, 2000.

[Pat] J. PATERA, R. T. SHARP ET P. WINTERNITZ, *Polynomial irreducible tensors for point groups*, J. of Mathematical Physics 19, pp. 2362-2376, 1978.

[Rot] JOSEPH ROTMAN, *Galois Theory, 2nd edition*, Springer-Verlag, Berlin, 1998.

[Ser] J.-P. SERRE, *Algèbre locale-multiplicités*, Lecture Notes in Mathematics, vol. 11, Springer-Verlag, 1965.

[Sha] R.Y. SHARP, *Steps in Commutative Algebra.*, Second Edition, London Mathematical Society Student Texts 51, Cambridge University Press, Cambridge, 2000.

[Sho] AMIN SHOKROLLAHI, BABAK HASSIBI, BERTRAND M. HOCHWALD ET WIM SWELDENS, *Representation Theory for High-Rate Multiple-Antenna Code Design.*, IEEE Transactions on Information Theory, vol.47, no. 6, 2001.

[Spr] T.A. SPRINGER, *Invariant Theory*, Springer-Verlag, Berlin, 1977.

[Sta] RICHARD P. STANLEY, *Invariants of Finite Groups and their Applications to Combinatorics*, Bulletin of the American Mathematical Society, 1 (new series), 475-511, 1979.

[Wol] J.A. WOLF, *Spaces of constant curvature*, McGraw-Hill, New York, 1967.

[Yau] STEPHEN S.-T. YAU AND YUNG YU, *Gorenstein Quotient Singularities in Dimension Three*, Memoirs of the American Mathematical Society no. 505, American Mathematical Society, 1993.

Annexe A

MODULES EXT

Si L,M et N sont des R-modules. La suite d'homomorphismes

$$L \xrightarrow{d} M \xrightarrow{\partial} N$$

est appelée **exacte** si $im(d) = ker(\partial)$. Elle est appelée un **complexe** si $im(d) \subseteq ker(\partial)$. L'**homologie** du complexe est alors définie comme étant le quotient $ker(\partial)/im(d)$. L'homologie sert donc à mesurer à quel point la suite n'est pas exacte.

Plus généralement, une suite

$$\cdots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \longrightarrow \cdots$$

est appelée une suite exacte si $ker(d_i) = im(d_{i+1})$ pour tout i. Cette suite est un complexe si on a seulement que $im(d_{i+1}) \subseteq ker(d_i)$. La i-ème homologie du complexe est le quotient $ker(d_i)/im(d_{i+1})$.

Soit P un R-module. On dit que P est **projectif** si pour toute suite exacte

$$L \xrightarrow{d} M \xrightarrow{\partial} N$$

la suite

$$Hom(P,L) \xleftarrow{Hom(P,d)} Hom(P,M) \xleftarrow{Hom(P,\partial)} Hom(P,N)$$

obtenue en appliquant le foncteur $Hom(P,-)$ est également exacte.

On appelle alors **résolution projective** de M une suite exacte

$$\cdots \longrightarrow P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \cdots \longrightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \longrightarrow 0$$

telle que tous les P_i sont projectifs. Une telle résolution est possible pour tout R-module M (voir [**Osb**]).

Supposons maintenant que N est aussi un R-module. On peut appliquer le foncteur $Hom(-, N)$ à la suite précédente et enlever le terme $Hom(M, N)$ ce qui donne le complexe suivant :

$$\cdots \longleftarrow Hom(P_1, N) \xleftarrow{Hom(d_1,N)} Hom(P_0, N) \xleftarrow{Hom(d_0,N)} 0$$

$$\cdots \longleftarrow Hom(P_{n+1}, N) \xleftarrow{Hom(d_{n+1},N)} Hom(P_n, N) \xleftarrow{Hom(d_n,N)} \cdots$$

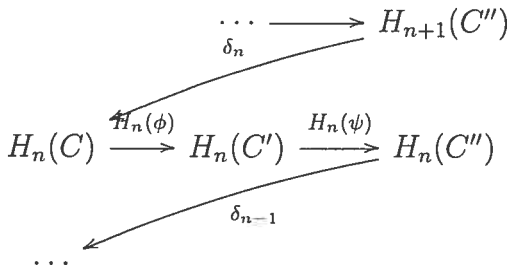
On dénote alors par $Ext^n_R(M, N)$ la n-ième homologie de cette suite. Par exemple, $Ext^0_R(M, N) \cong Hom_R(M, N)$. Les modules Ext servent à «mesurer» à quel point N n'est pas projectif dans le sens que si N est projectif, alors $Ext^n_R(M, N) = 0$ pour $n > 0$ puisque la suite ci-haut est exacte. Remarquons également que la définition que nous avons donnée dépend du choix de la résolution prejective de M (qui n'est pas unique). Or, il est possible de montrer que cela ne fait aucune différence sur les modules Ext à isomorphisme près.

Un résultat classique d'algèbre homologique sur les modules Ext est le théorème d'existence d'une longue suite exacte. Tout d'abord nous avons besoin de :

Théorème A.0.2. *Supposons que nous avons le diagramme commutatif*

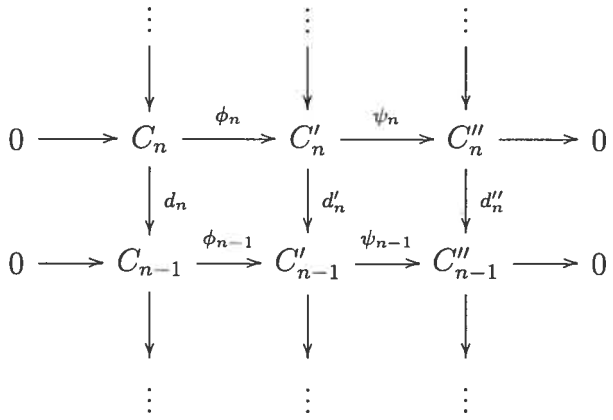
$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_n & \xrightarrow{\phi_n} & C'_n & \xrightarrow{\psi_n} & C''_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle d''_n} & & \\
0 & \longrightarrow & C_{n-1} & \xrightarrow{\phi_{n-1}} & C'_{n-1} & \xrightarrow{\psi_{n-1}} & C''_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

dans lequel toutes les lignes sont des suites exactes et toutes les colonnes sont des complexes. Dénotons par $H_n(C)$ la n-ième homologie du complexe $\{C_i\}$. Alors il existe une suite d'applications $\delta_n : H_n(C'') \to H_{n-1}(C)$ telle que



est exacte.

Démonstration. Nous devons d'abord définir δ_n. Considérons le diagramme commutatif



et suposons $x \in C''_n$ avec $d''_n(x) = 0$. ψ_n est surjectif, donc, $\exists\ y \in C'_n$ tel que $\psi_n(y) = x$. Par ailleurs, $0 = d''_n(x) = d''_n\psi_n(y) = \psi_{n-1}d'_n(y)$, donc $d'_n(y) \in ker(\psi_{n-1}) = im(\phi_{n-1})$. Nous définissons $\delta_n(x + im(d''_{n+1}))$ comme étant la classe correspondant à ce $z \in C_{n-1}$ pour lequel $\phi_{n-1}(z) = d'_n(y)$. Il nous reste à vérifier :

(1) $z+im(d_n)$ est indépendant du choix de y : Si $\phi_n(y') = x$, alors $\phi_n(y-y') = 0$, donc $y - y' \in ker(\psi_n) = im(\phi_n)$). Donc, $y - y' = \phi_n(t)$ pour un certain $t \in C_n$. Ainsi, $d'_n(y) - d'_n(y') = d'_n(y - y') = d'_n\phi_n(t) = \phi_{n-1}d_n(t)$. Donc, si $d'_n(y) = \phi_{n-1}(z)$ et $d'_n(y') = \phi_{n-1}(z')$, alors (puisque ϕ_{n-1} est injectif) $z - z' = d_n(t) \in im(d_n)$, d'où $z + im(d_n) = z' + im(d_n)$.

(2) $z + im(d_n) \in H_{n-1}(C)$, c'est-à-dire que $d_{n-1}(z) = 0$: $\phi_{n-2}d_{n-1}(z) = d'_{n-1}\phi_{n-1}(z) = d'_{n-1}d'_n(y) = 0$. Donc, $d_{n-1}(z) = 0$ car ϕ_{n-2} est injectif.

(3) Si $x \in im(d''_{n+1})$, alors $z \in im(d_n)$: Si $x = d''_{n+1}(s)$, alors nous choisissons $u \in C'_{n+1}$ tel que $\psi_{n+1}(u) = s$ (cela est possible puisque ψ_{n+1} est surjectif). Alors, $x = d''_{n+1}\psi_{n+1}(u) = \psi_n d'_{n+1}(u)$, donc nous pouvons prendre $y = d'_{n+1}(u)$. Mais alors, $d'_n(y) = 0$ et nous prenons donc $z = 0$. Par (1), tout autre choix de y donne un $z \in 0 + im(d_n) = im(d_n)$.

Maintenant, nous savons que δ_n est bien défini (nous pouvons également vérifier que c'est un homomorphisme). Il nous reste maintenant à montrer l'exactitude de la suite aux endroits où les δ_n sont utilisés :

(4) $ker(\delta_n) \supseteq im(H_n(\psi))$: Si $x+im(d''_{n+1}) \in im(H_n(\psi))$, alors on peut choisir y tel que $H_n(\psi)(y+im(d'_{n+1})) = x+im(H_n(\psi))$, puisque la seule restriction est que $\psi_n(y) = x$. C'est-à-dire que nous pouvons remplacer x par $\psi_n(y)$ sans changer la classe de $im(d''_{n+1})$ dans $H_n(C'')$. Cependant, pour ce x et ce y, $d'_n(y) = 0$ car cela représente une classe d'homologie dans $H_n(C')$. Ainsi, $z = 0$ et $\delta_n(x + im(d''_{n+1})) = 0$.

(5) $ker(\delta_n) \subseteq im(H_n(\psi))$: Si $\delta_n(x + im(d''_{n+1})) = 0$, alors $z \in im(d_n)$, c'est-à-dire que $z = d_n(t)$ pour un $t \in C_n$. Ainsi, $d'_n(y) = \phi_{n-1}(z) = \phi_{n-1}d_n(t) = d'_n\phi_n(t)$. Autrement dit, $d'_n(y - \phi_n(t)) = 0$. Or, $\psi_n(y - \phi_n(t)) = \psi_n(y) - \psi_n\phi_n(t) = x - 0$. Donc, $H_n(\psi)(y - \phi_n(t) + im(d'_{n+1})) = x + im(d''_n)$.

(6) $ker(H_{n-1}(\psi)) \supseteq im(\delta_n)$: Par définition, $H_{n-1}(\psi)\delta_n(x + im(d''_{n+1})) = \phi_{n-1}(z) + im(d'_n) = d'_n(y) + im(d'_n) = 0$.

(7) $ker(H_{n-1}(\psi)) \subseteq im(\delta_n)$: Si $z + im(d_n) \in ker(H_{n-1}(\psi))$, alors $\phi_{n-1}(z) \in im(d'_n)$, c'est-à-dire que $\phi_{n-1}(z) = d'_n(y)$ pour $y \in C_n$. Posons $x = \psi_n(y)$. Autrement dit, nous parcourons la définition de δ_n à l'envers, donc nous devons seulement nous assurer que $x + im(d''_{n+1}) \in H_n(C'')$, c'est-à-dire que $d''_n(x) = 0$ pour le x que nous avons défini. Or, $d''(x) = d''_n\psi_n(y) = \psi_{n-1}d'_n(y) = \psi_{n-1}\phi_{n-1}(z) = 0$.

Il ne nous reste plus qu'à vérifier que la suite est exacte aux autres endroits. Remarquons que $H_n(\psi)H_n(\phi) = H_n(\psi\phi) = H_n(0) = 0$. Donc, nous avons au moins que $ker(H_n(\psi)) \supseteq im(H_n(\phi))$.

(8) $ker(H_n(\psi)) \subseteq im(H_n(\phi))$: Supposons $H_n(\psi)(u + im(d'_{n+1})) = 0$. Alors, $\psi_n(u) \in im(d''_{n+1})$, alors $\psi_n(u) = d''_{n+1}(v)$ pour un $v \in C''_{n+1}$. Maintenant, ψ_{n+1} est surjectif, donc $v = \psi_{n+1}(w)$ pour un certain $w \in C'_{n+1}$. Ainsi,

$$\psi_n(u) = d''_{n+1}(v) = d''_{n+1}\psi_{n+1}(w) = \psi_n d'_{n+1}(w)$$

d'où $\psi_n(u - d'_{n+1}(w)) = 0$. C'est-à-dire que $u - d'_{n+1}(w) \in ker(\psi_n) = im(\phi_n)$, donc $u - d'_{n+1}(w) = \phi_n(t)$ pour un certain $t \in C_n$. Or, $\phi_{n-1}d_n(t) = d'_n\phi_n(t) = d'_n(u) - d'_n d'_{n+1}(w) = 0$, puisque u représente une classe d'homologie. Donc, $d_n(t) = 0$ car ϕ_{n-1} est injectif. Donc, nous pouvons conclure que $H_n(\psi)(t + im(d_{n+1})) = u + im(d'_{n+1})$.

□

Nous pouvons maintenant démontrer :

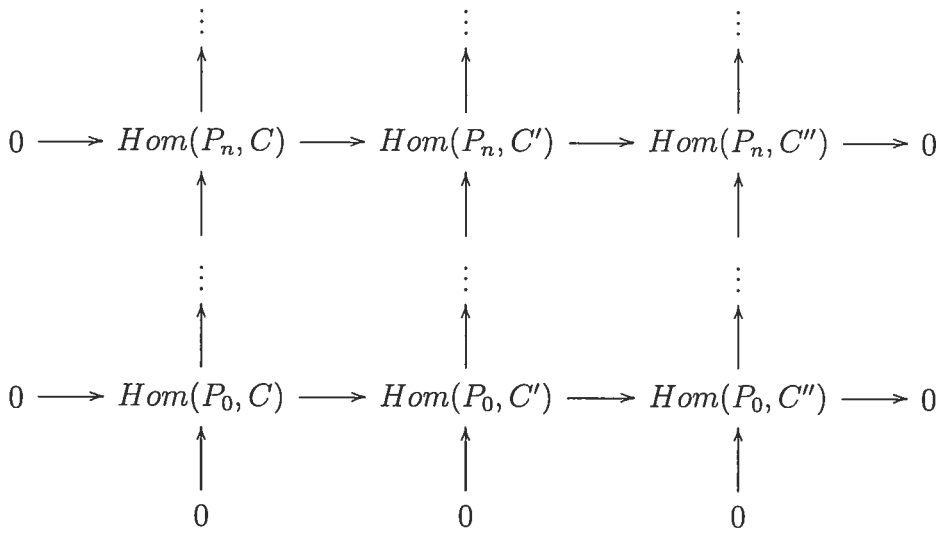
Théorème A.0.3 (Suite exacte longue pour Ext). *Supposons que*

$$0 \longrightarrow C \longrightarrow C' \longrightarrow C'' \longrightarrow 0$$

est une suite exacte courte de R-modules. Alors, pour tout R-module à droite B, il existe une suite exacte longue

$$\begin{array}{ccccccc}
Ext^{n+1}(B,C) & \longrightarrow & \cdots & & & & \\
 & \searrow & & & & & \\
Ext^n(B,C) & \longrightarrow & Ext^n(B,C') & \longrightarrow & Ext^n(B,C'') & & \\
 & \searrow & & \searrow & & & \\
 & & \cdots & & \cdots & & \\
 & & & \searrow & & & \\
Ext^1(B,C) & \longrightarrow & Ext^1(B,C') & \longrightarrow & \cdots & & \\
 & \searrow & & & & & \\
0 & \longrightarrow & Hom(B,C) & \longrightarrow & Hom(B,C') & \longrightarrow & Hom(B,C'')
\end{array}$$

Démonstration. Considérons le diagramme suivant :



Les rangées sont toutes exactes puisque les P_k sont projectifs. Il ne reste qu'à utiliser le théorème A.0.2. □

Annexe B

INTRODUCTION À LA GÉOMÉTRIE ALGÉBRIQUE

B.0.1. Variétés algébriques affines

Une variété algébrique est en fait l'ensemble des solutions d'un système d'équations polynomiales.

Soit V un espace vectoriel de dimension n sur un corps K et soit $K[V]$ l'algèbre des fonctions polynomiales sur V. Pour un ensemble $S \subseteq K[V]$, on note

$$\mathcal{V}(S) = \{v \in V \mid f(v) = 0, \forall f \in S\}.$$

On remarque que $\mathcal{V}(S) = \mathcal{V}(J)$ où J est l'idéal engendré par S.

Définition B.0.1. *Un sous-ensemble $X \subseteq V$ est appelé un* **ensemble algébrique** *si $X = \mathcal{V}(J)$ pour un idéal quelconque de $K[V]$. De plus X est appelé une* **variété algébrique affine** *si X peut s'écrire comme $\mathcal{V}(\mathcal{P})$ où $\mathcal{P}$ est un idéal premier.*

Autrement dit, un sous-ensemble $X \subseteq V$ est un ensemble algébrique s'il peut être vu comme un ensemble-solution d'un système d'équations polynomiales. Il est une variété algébrique affine s'il peut être vu comme ensemble-solution d'un système d'équations polynomiales tel que les polynômes du système engendrent un idéal premier. Nous verrons plus tard pourquoi il est important de distinguer le cas où l'idéal est premier.

Dans la prochaine section, nous verrons comment correspondent les notions d'algèbre et de géométrie.

B.0.2. Idéaux radicaux, premiers et maximaux

En général, pour un idéal propre I de $K[x_1, \ldots, x_n]$, rien ne nous garantit que $\mathcal{V}(I) \neq \emptyset$. Par exemple dans $\mathbb{R}^2$, $\mathcal{V}(x^2 + y^2 + 1) = \emptyset$. Cependant, il y aurait eu des solutions dans $\mathbb{C}^2$.

Le célèbre Nullstellensatz (théorème des zéros) de Hilbert, nous garantit l'existance de solutions (c'est-à-dire que si I est un idéal propre de $K[x_1, \ldots, x_n]$, alors $\mathcal{V}(I) \neq \emptyset$) à condition que K soit algébriquement clos. Notez que nous appelons ce résultat la version «faible» du Nullstellensatz, par opposition à la version «forte» énoncée au théorème B.0.4.

Par contre, même dans le cas algébriquement clos, la correspondance entre les idéaux et les ensembles algébriques n'est pas biunivoque. En effet, supposons que $X = \mathcal{V}(I)$ pour un idéal I. Alors, nous avons également que $X = \mathcal{V}(I^2)$. Par exemple, $\mathcal{V}(x^2 + y^2 - 1) = \mathcal{V}((x^2 + y^2 - 1)^2)$.

Pour contourner ce problème, nous définissons le **radical** de l'idéal I d'un anneau R comme étant

$$\sqrt{I} = \{r \in R \mid \exists_{n \in \mathbb{N}}\ r^n \in I\}.$$

L'idéal I est dit **radical** si $\sqrt{I} = I$.

Remarquons alors que $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$ et que, en particulier, $\sqrt{I} = \sqrt{I^2}$. Donc, si nous nous restreignons aux idéaux radicaux, il est possible que nous puissons obtenir cette fois-ci une correspondance biunivoque entre ces idéaux et les ensembles algébriques.

C'est en effet le cas (si K est algébriquement clos) et c'est exactement ce qu'affirme le prochain théorème qui est une version plus forte du Nullstellensatz :

Théorème B.0.4 (Nullstellensatz, version forte). *Soient K un corps algébriquement clos et I un idéal de $K[x_1, \ldots, x_n]$. Si $f \in K[x_1, \ldots, x_n]$ s'annule partout sur $\mathcal{V}(I)$, alors $f \in \sqrt{I}$.*

Donc, nous pouvons noter $\mathcal{I}(X)$ l'unique idéal radical qui correspond à l'ensemble algébrique X. Remarquons que cette correspondance inverse l'ordre dans le sens que $X \subseteq Y$ si et seulement si $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$.

Par la discussion de la section précédente, X est une variété algébrique affine si et seulement si $\mathcal{I}(X)$ est un idéal premier. Il y a donc non seulement une correspondance biunivoque entre les idéaux radicaux et les ensembles algébriques, mais également entre les idéaux premiers et les variétés algébriques affines.

En supposant toujours que K est algébriquement clos, nous avons également une correspondance biunivoque entre les points de V et les idéaux maximaux de $K[x_1, \ldots, x_n]$. En effet, pour un point $c = (c_1, c_2, \ldots, c_n) \in V$, nous avons que $\{c_1, c_2, \ldots, c_n\} = \mathcal{V}(x_1 - c_1, x_2 - c_2, \ldots, x_n - c_n)$ qui est un idéal maximal (noté μ_c). Il reste à montrer que tout idéal maximal est en fait un μ_c pour un $c \in V$. Soit alors μ un idéal maximal quelconque. Puisque μ est un idéal propre, $\mathcal{V}(\mu) \neq \emptyset$. Soit alors c un point de $\mathcal{V}(\mu)$. Cela se traduit par $\mu \subseteq \mu_c$. Nous obtenons l'égalité par la maximalité des deux idéaux.

La raison pour laquelle nous nous intéressons tant aux correspondances biunivoques est que nous pouvons maintenant nous détacher du concept d'espace vectoriel. En effet, au lieu de parler de points, de variétés et d'ensemble algébriques, nous pouvons parler, respectivement, d'idéaux maximaux, d'idéaux premiers et d'idéaux radicaux. Or, ces types d'idéaux sont présents dans tous les anneaux, pas seulement dans les anneaux de fonctions polynomiales sur des espaces vectoriels. Nous pouvons donc utiliser des arguments «géométriques» sur une classe beaucoup plus large d'anneaux.

En fait, nous avons déjà vu sans le savoir ce genre de généralisation. En effet, nous verrons plus loin que la définition de dimension de Krull correspond à la notion géométrique usuelle de dimension, quoique nous pouvons utiliser cette définition dans un contexte non géométrique (comme nous l'avons fait).

Nous résumons cette correspondance entre géométrie et algèbre dans le tableau B.1 qui nous servira dorénavant de «dictionnaire» pour passer de l'un à l'autre.

Dans la prochaine section, nous verrons plus précisément comment interpréter géométriquement un anneau intègre, dans le cas particulier où il peut être vu comme une K-algèbre finiment engendrée. Le but visé est évidemment d'utiliser ce procédé sur l'anneau des invariants.

Algèbre commutative		Géométrie algébrique
Idéal radical	$\longleftrightarrow$	Ensemble algébrique
Idéal premier	$\longleftrightarrow$	Variété algébrique affine
Idéal maximal	$\longleftrightarrow$	Point
Dimension de Krull	$\longleftrightarrow$	Dimension

TAB. B.1. Dictionnaire Algèbre-Géométrie

B.0.3. Anneau de fonctions polynomiales

Comme nous l'avons vu, l'anneau $K[V] = K[x_1, \ldots, x_n]$ peut être interprété comme l'anneau des fonctions polynomiales sur V. Soit maintenant $X \subseteq V$ une variété algébrique affine. Nous aimerions lui associer un anneau de fonctions polynomiales (noté $K[X]$). Une façon de faire est de prendre les restrictions des polynômes de $K[V]$ sur X. Cependant, pour que les éléments de $K[X]$ soient tous dinstinguables, nous devrons travailler sur des classes d'équivalences de telle sorte que deux polynômes $f, g \in K[V]$ sont identifiés s'ils ont les mêmes valeurs partout sur X.

Autrement dit, f et g sont équivalents si le polynôme $f - g$ est toujours 0 sur X, i.e. $f - g \in \mathcal{I}(X)$. Nous définissons donc

$$K[X] := K[V]/\mathcal{I}(X)$$

que nous appelons l'**anneau des fonctions polynomiales** sur X.

Nous voyons ici la raison pour laquelle nous donnons un nom différent aux ensembles algébriques dont l'idéal associé est premier. Cela correspond au fait que l'anneau des fonctions polynomiales soit intègre.

En fait, toute K-algèbre intègre finiment engendrée peut être vu comme un $K[X]$ pour une variété X. En effet, soit A un tel anneau et choisissons un ensemble de générateurs $\{f_1, f_2, \ldots, f_k\}$. Nous pouvons toujours construire un homomorphisme de K-algèbres

$$\phi : K[x_1, \ldots, x_k] \longrightarrow A$$
$$x_i \longmapsto f_i$$

Il est donc évident que $A \cong K[x_1, \ldots, x_k]/\ker(\phi)$ où $\ker \phi$ est un idéal premier puisque A est intègre. Ainsi, $A = K[\mathcal{V}(\ker(\phi))]$.

Donc, pour chaque K-algèbre intègre finiment engendrée, on peut lui associer une variété algébrique affine. Pour cette raison, on appelle une algèbre de ce type une **algèbre affine**.

Cependant, le choix de la variété n'est *a priori* pas unique. En effet, il dépend du choix des générateurs pour l'algèbre affine. Or, tout comme pour le cas polynomial, il est assez aisé de montrer que tous les idéaux maximaux de $K[X] = K[x_1, \ldots, x_n]/\mathcal{I}(X)$ sont de la forme $(x_1 - c_1, \ldots, x_n - c_n)/\mathcal{I}(X)$ et, donc, correspondent à des points de X. Il y a donc, en quelque sorte, unicité.

Autrement dit, pour une algèbre affine A donnée, les points de la variété algébrique affine associée sont en bijection avec les idéaux maximaux de A qui, eux, ne dépendent pas du choix des générateurs.

Plus précisément, si X et Y sont deux variétés algébriques affines telles que $K[X] \cong K[Y]$, alors X est isomorphe à Y. Nous n'avons pas encore défini la notion d'isomorphisme entre deux variétés :

Définition B.0.2. *Soient $X \subseteq K^n$ et $Y \subseteq K^m$ deux variétés algébriques affines. Une application $F : X \longrightarrow Y$ est appelée un* **morphisme** *s'il existe des polynômes en n variables $f_1, f_2, \ldots, f_m$ tels que*

$$F : (a_1, \ldots, a_n) \mapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)).$$

Un **isomorphisme** *est, bien sûr, un morphisme bijectif.*

Par conséquent, lorsque nous avons une algèbre affine (par exemple l'anneau des invariants), nous pouvons parler de **la** variété algébrique affine associée.

Comme cela a été mentionné auparavant, on peut également définir la notion de dimension d'une variété algébrique affine. Soit X une telle variété, on définit

sa **dimension** comme étant la longueur m de la plus longue chaîne

$$X_0 \subset X_1 \subset \cdots \subset X_n = X$$

de variétés algébriques affines. Si les longueurs de telles chaînes ne sont pas bornées, on dit que la dimension est infinie. En particulier, comme d'habitude, la dimension d'un point est 0, celle d'une courbe est 1, celle d'une surface, 2, etc.

Dans l'anneau des fonctions polynomiales, un telle chaîne de variétés correspond à une chaîne d'idéaux premiers. La dimension d'une variété algébrique affine est donc égale à la dimension de Krull de l'anneau correspondant (on comprend maintenant pourquoi la notion de dimension de Krull est en effet une dimension).

B.0.4. Localisation et singularités

Nous nous intéressons aux propriétés des variétés car celles-ci donnent de l'information sur l'algèbre affine.

Une notion qu'il est important d'étudier est la notion de singularité. Intuitivement, une singularité est un point sur une variété algébrique affine pour lequel l'espace tangent n'a pas la même dimension que la variété.

Ces singularités empêchent, par exemple, un isomorphisme entre la variété et un espace vectoriel puisque les isomorphismes conservent les singularités et que les espaces vectoriels n'en possèdent pas. Nous cherchons donc une méthode purement algébrique permettant de déceler la présence de singularités.

La première étape consiste à définir précisément ce que nous entendons par «espace tangent» en algèbre.

En analyse, si M est une variété différentiable et $x \in M$, nous définissons l'espace tangent $T_x(M)$ de la façon suivante. Nous commençons par une courbe paramétrée $\rho : (-\epsilon, \epsilon) \longrightarrow M$ telle que $\rho(0) = x$. Ensuite nous définissons une dérivée en x comme étant $d_x\rho(f) := \frac{d}{dt} f(\rho(t)) \mid_{t=0}$ pour une fonction f différentiable en x. L'espace tangent est alors l'espace vectoriel de toutes ces dérivations.

En algèbre, nous pouvons définir ce même genre d'idées sans se servir de dérivées et de fonctions différentiables. Plutôt que de s'intéresser aux fonctions différentiables en x, nous considérons les **fonctions régulières** en x.

Définition B.0.3. *Soit X une variété algébrique affine et $x \in X$. Notons par $K(X)$ le corps des fractions de $K[X]$. $f \in K(X)$ est dite* **régulière** *en x s'il existe $g, h \in K[X]$ telles que $f = g/h$ et que $h(x) \neq 0$.*

L'ensemble des fonctions régulières en x est noté $\mathcal{O}_x$. Par la définition précédente, il est évident que $\mathcal{O}_x = K[X]_{\mu_x}$, c'est-à-dire que $\mathcal{O}_x$ est l'ensemble des fractions $\frac{g}{h}$ telles que $g, h \in K[X]$ et que h n'est pas dans μ_x (on se souvient que μ_x est l'idéal maximal de tous les polynômes s'annulant en x). De plus, il est facile de montrer que $\mu_x\mathcal{O}_x$ est l'unique idéal maximal de $\mathcal{O}_x$. Un anneau ayant un unique idéal maximal est appelé un anneau local et $\mathcal{O}_x$ est appelé la localisation de $K[X]$ en l'idéal μ_x.

Plus généralement, pour un anneau R et un idéal premier $\mathcal{P}$, on peut localiser R en $\mathcal{P}$ en formant l'anneau $R_{\mathcal{P}}$ des fractions dont le dénominateur n'est pas dans $\mathcal{P}$. Encore une fois, $\mathcal{P}R_{\mathcal{P}}$ est l'unique idéal maximal de $R_{\mathcal{P}}$.

Il ne nous reste plus qu'à définir l'espace tangent en x comme étant l'espace vectoriel des dérivations en x (noté $T_x(X)$). Pour nous, une dérivation en x est une fonction $D : \mathcal{O}_x \longrightarrow K$ telle que :

(1) D est K-linéaire.

(2) $D(a) = 0$ si $A \in K$.

(3) $D(fg) = f(x)D(g) + g(x)D(f)$ si $f, g \in \mathcal{O}_x$.

Dans le cas d'une variété différentielle, les «dérivations» $d_x\rho$ que nous avions données sont exactement les fonctions ayant les propriétés ci-dessus. La seule différence est que cette fois-ci toutes les définitions sont purement algébriques.

Donc, nous pouvons définir une **singularité** d'une variété algébrique affine X comme étant un point $x \in X$ tel que $dim_K(T_x(X)) \neq dim(K[X])$.

Nous nous intéressons maintenant à trouver la dimension de $T_x(X)$. Soit D une dérivation en x. La valeur de D sur $\mathcal{O}_x$ est complètement déterminée si on connaît sa valeur sur un ensemble de générateurs de $\mu_x\mathcal{O}_x$ grâce aux propriétés énoncées ci-dessus. Donc, il va de soit que la dimension de $T_x(X)$ est tout simplement le nombre minimal de générateurs de $\mu_x\mathcal{O}_x$ qui correspond à la dimension, comme espace vectoriel, de $\mu_x\mathcal{O}_x/(\mu_x\mathcal{O}_x)^2$.

Annexe C

MODULE CANONIQUE

Dans l'annexe A, nous définissons les A-modules $Ext^i_A(M,N)$ comme étant les homologies du complexe

$$\cdots \longleftarrow Hom_A(P_2,N) \longleftarrow Hom_A(P_1,N) \longleftarrow Hom_A(P_0,N) \longleftarrow 0$$

pour une résolution projective

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

Nous définissons alors la **dimension homologique** de M, notée $hdim(M)$, comme la longueur d'une résolution projective minimale de M. Si A est polynomial, ce nombre est égal à la plus grande valeur de i pour laquelle $Ext^i_A(M,K) \neq 0$ puisque la dimension de cet espace est égal au nombre de générateurs de P_i comme module libre. En effet, il a été démontré que les A-modules projectifs sont libres lorsque A est polynomial (Quillen et Suslin 1976).

Similairement, nous définissons la **codimension homologique** de M, notée $hcodim(M)$, comme la plus petite valeur de $i \geq 0$ pour laquelle $Ext^i_A(K,M) \neq 0$.

Nous avons vu dans la section 1.3.4 que l'anneau des invariants est parfois Cohen-Macaulay. Un tel anneau possède toujours une série de Hilbert de la forme

$$\mathcal{H}(M,t) = \frac{f(t)}{\prod_{i=0}^{n}(1-t^{d_i})},$$

où $f(t)$ est un polynôme à coefficients entiers et les d_i sont des nombres naturels.

Nous verrons que si un A-module M est Cohen-Macaulay, presque tous les $Ext^i_A(M,A)$ sont triviaux. En particulier, si B est un anneau polynomial sur lequel M est libre, alors $Ext^i_B(M,B) = 0$ pour tous les $i > 0$. Donc, nous nous

intéressons uniquement à $Ext^0_B(M,B) \cong Hom_B(M,B)$ qui est en quelque sorte le «module dual» de M, que nous appelons le **module canonique**. En particulier, les anneaux Cohen-Macaulay qui sont isomorphes à leur module canonique sont appelés **Gorenstein**. Nous redéfinirons ces termes plus précisément plus tard et nous verrons que les anneaux Gorenstein ont une série de Hilbert qui a une forme très particulière.

Tout d'abord, citons le théorème suivant (voir [**Ben**], corollaire 4.5.2).

Théorème C.0.5. *Soit $A = K[y_1, \ldots, y_s]$ un anneau polynomial gradué dont les degrés des y_i sont strictement positifs. Si M est un A-module gradué Cohen-Macaulay de dimension de Krull n, alors $Ext^i_A(M,A) = 0$ pour $i \neq s-n$.*

Ainsi, par le théorème C.0.5, $Ext^{s-n}_A(M,A)$ est le seul module de cette forme qui est possiblement non nul. Cependant, il semblerait que ce module dépende de s qui est le nombre de générateurs de A. Nous aimerions trouver un module qui caractérise M et qui ne dépend d'aucun choix. Le prochain théorème nous expliquera comment passer d'un ensemble de générateurs à un autre.

Théorème C.0.6. *Soient $A = K[y_1, \ldots, y_s] \subseteq A' = K[y_1, \ldots, y_{s+1}]$ des anneaux polynomiaux gradués tels que les degrés des y_i sont strictement positifs. Si M est un A'-module gradué qui est finiment engendré et Cohen-Macaulay de dimension de Krull n comme A-module, alors M est aussi Cohen-Macaulay comme A'-module et il y a un isomorphisme de A-modules*

$$Ext^{s+1-n}_{A'}(M,A') \cong Ext^{s-n}_A(M,A).$$

Démonstration. Nous avons une suite exacte courte de A'-modules

$$0 \longrightarrow A' \otimes_A M \xrightarrow{1 \otimes y_{s+1} - y_{s+1} \otimes 1} A' \otimes_A M \longrightarrow M \longrightarrow 0$$

et donc une suite exacte longue

$$\cdots \longrightarrow Ext_{A'}^{s-n}(M, A') \longrightarrow Ext_{A'}^{s-n}(A' \otimes_A M, A')$$

$$\longrightarrow Ext_{A'}^{s-n}(A' \otimes_A M, A') \longrightarrow Ext_{A'}^{s+1-n}(M, A')$$

$$\longrightarrow Ext_{A'}^{s+1-n}(A' \otimes_A M, A') \longrightarrow \cdots$$

Par le corollaire C.0.5, le terme en haut à gauche de cette suite est nul. Maintenant, si

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

est une résolution projective de M comme A-module, alors

$$\cdots \longrightarrow A' \otimes_A P_1 \longrightarrow A' \otimes_A P_0 \longrightarrow A' \otimes_A M \longrightarrow 0$$

est une résolution projective de $A' \otimes_A M$ comme A'-module (c'est une suite exacte car A' est un A-module libre).

De plus,

$$Hom_{A'}(A' \otimes_A P_i, A') \cong Hom_A(P_i, A') \cong A' \otimes_A Hom_A(P_i, A)$$

comme A'-modules. Donc,

$$Ext_{A'}^i(A' \otimes_A M, A') \cong Ext_A^i(P_i, A') \cong A' \otimes_A Ext_A^i(M, A).$$

Cela implique que le terme en bas à droite de la suite exacte longue est également nul. Ainsi, $Ext_{A'}^{s+1-n}(M, A')$ est isomorphe au conoyau de $1 \otimes y_{s+1} - y_{s+1} \otimes 1$ sur $A' \otimes_A Ext_A^{s-n}(M, A)$ qui, comme A-module, est isomorphe à $Ext_A^{s-n}(M, A)$. □

En fait, l'isomorphisme du théorème précédent ne préserve pas la graduation. On devrait plutôt écrire $Ext_{A'}^{s+1-n}(M, A') \cong Ext_A^{s-n}(M, A)[deg(y_{s+1})]$ pour préciser que la graduation est décalée de $deg(y_{s+1})$.

Nous pouvons maintenant définir le module canonique. Soit R un anneau gradué Cohen-Macaulay finiment engendré sur le corps K par des éléments homogènes $y_1, \ldots, y_s$ de degrés strictement positifs. On peut voir R comme un A-module, où A est l'anneau polynomial $A = K[y_1, \ldots, y_s]$.

Supposons que la dimension de Krull de R soit n. On définit alors le **module canonique** de R comme le R-module

$$\omega_A(R) := Ext_A^{s-n}(R, A)[-(\sum_{i=0}^{s} deg(y_i)) + n].$$

En fait, en utilisant le théorème C.0.6, on peut toujours passer de l'ensemble de générateurs $y_1, \ldots, y_s$ à un autre ensemble de notre choix en ajoutant les générateurs voulus et en enlevant ceux que nous ne désirons pas. Donc, la définition du module canonique ne dépend pas réellement du choix de A (à isomorphisme près). C'est pourquoi nous pouvons simplement écrire $\omega(R)$ pour le module canonique.

En particulier, puisque R est Cohen-Macaulay de dimension de Krull n, on peut toujours choisir A de telle sorte que $s = n$ et que R soit finiment engendré sur A. Nous venons donc de montrer que si $A = K[f_1, \ldots, f_n]$ est choisi de cette façon, alors

$$\omega(R) \cong Ext_A^{n-n}(R, A)[-\sum_{i-0}^{n}(deg(f_i) - 1)] \cong Hom_A(R, A)[-\sum_{i-0}^{n}(deg(f_i) - 1)].$$