INVARIANTS ET COVARIANTS DES GROUPES ALGÉBRIQUES RÉDUCTIFS

Notes d'un cours à l'école d'été de Monastir (juillet-août 1996)

Michel Brion

La théorie des invariants étudie les opérations des groupes algébriques dans les variétés algébriques. Son objectif principal est de construire et de décrire des variétés quotients, dans un sens en général plus faible que celui d'espace des orbites.

Dans les notes qui suivent, on trouvera une introduction à quelques aspects de la théorie des invariants, sur le corps des nombres complexes. La première partie commence par des propriétés générales des actions des groupes algébriques affines ; puis on étudie successivement les actions des groupes finis, des groupes unipotents, et des tores. On termine par un théorème de Rosenlicht qui affirme qu'un quotient par un groupe algébrique affine existe toujours sur un ouvert convenable.

Dans la seconde partie, on introduit les groupes (linéairement) réductifs : ce sont les groupes algébriques affines dont toutes les représentations rationnelles sont semi-simples. On montre que les groupes classiques sont réductifs, puis on étudie les représentations et les caractères des groupes réductifs, le cas de SL_2 étant traité en détail, avec une introduction à l'algèbre des covariants. On montre enfin le théorème de finitude pour les invariants et covariants des groupes réductifs.

Ce théorème est le point de départ de la construction de quotients par les groupes réductifs ; ceux-ci font l'objet de la troisième partie. On obtient une caractérisation des morphismes quotients, ainsi que le critère de Hilbert-Mumford qui permet de décrire leurs fibres. Puis on démontre le théorème de Hochster-Roberts : l'algèbre des invariants pour une action linéaire d'un groupe réductif est un module libre sur une sous-algèbre de polynômes. Ceci amène à l'étude des systèmes de paramètres pour les algèbres d'invariants.

Dans la quatrième partie, on applique le théorème de Hochster-Roberts et des techniques d'algèbre commutative (séries de Hilbert, résolutions libres) à la détermination des invariants pour les actions linéaires des groupes réductifs. On conclut par un aperçu des invariants des formes binaires ; leur étude a été le point de départ de la théorie des invariants au siècle dernier, mais leur structure algébrique reste mal comprise. Par contre, l'approche géométrique aboutit à des résultats plus satisfaisants.

Les prérequis de ces notes sont des notions de base d'algèbre commutative et de géométrie algébrique affine (des notions plus élaborés sont introduites dans les troisième et quatrième parties). Pour celles-ci, une bonne référence récente est [Ei]. Par contre, la structure et la classification des groupes réductifs ne sont pas abordées ; ce n'est pas nécessaire pour la plupart des exemples traités ici, qui concernent des groupes finis ou classiques, en particulier SL_2. Ces exemples constituent d'ailleurs une source d'exercices, de problèmes et de conjectures.

On renvoie aux notes du cours de Schwarz pour une approche analytique de la théorie des invariants, avec un traitement du théorème du slice étale, et à [Fu] et [Ho3] pour les représentations et invariants des groupes classiques. D'autres introductions à la théorie des invariants sont le classique [Hi] et les modernes [Sp2] et [Sta]. Pour aller plus loin, le lecteur pourra consulter [Kr] et [Kr-Sl-Sp], ainsi que l'exposé d'ensemble [Po-Vi].

Remerciements. Je remercie chaleureusement Ivan Arjantsev, Dimitri Chmelkine et Thierry Vust pour leurs commentaires sur ce texte et pour leurs corrections.

Table des matières

1. Opérations de groupes algébriques

1.1. *Opérations de groupes*

Rappelons qu'une *opération* (ou action) d'un groupe G dans un ensemble X est une application $\alpha : G \times X \to X$ telle que :

(i) $\alpha(gh, x) = \alpha(g, \alpha(h, x))$ pour tous g, h dans G, et tout $x \in X$.

(ii) $\alpha(e, x) = x$ pour tout $x \in X$, où e désigne l'élément neutre de G.

Pour une opération α de G dans X, on notera $\alpha(g, x) = g \cdot x$. L'*orbite* de $x \in X$ est alors l'ensemble

$$G \cdot x := \{g \cdot x \mid g \in G\}$$

et le *groupe d'isotropie* de x est

$$G_x := \{g \in G \mid g \cdot x = x\} \ .$$

On note X/G l'espace des orbites, et $\pi : X \to X/G$ le quotient.

Lorsque G opère dans X et dans Y, une application $f : X \to Y$ est *G-équivariante* si $f(g \cdot x) = g \cdot f(x)$ pour tous $g \in G$ et $x \in X$. En particulier, f est *invariante* si $f(g \cdot x) = f(x)$ pour tous $g \in G$ et $x \in X$, c'est-à-dire si f est constante sur les orbites de G dans X. Toute application invariante se factorise par le quotient $\pi : X \to X/G$.

Dans le cadre des opérations de groupes topologiques ou algébriques (définis plus précisément en 1.2), le passage au quotient soulève des problèmes, comme le montrent les exemples suivants.

(i) Soit $G = \mathbf{C}^*$ opérant dans $X = \mathbf{C}^2$ par multiplication :

$$t \cdot (x, y) = (tx, ty) \ .$$

Les orbites sont l'origine et les droites vectorielles privées de l'origine. Ainsi, l'adhérence de toute orbite contient l'origine ; donc le quotient X/G ne peut être muni d'une structure d'espace topologique séparé pour lequel l'application quotient $\pi : X \to X/G$ est continue. Par contre, le quotient $(X \setminus \{0\})/G$ existe ; c'est la droite projective complexe.

(ii) Soit $G = \mathbf{C}$ opérant dans $X = \mathbf{C}^2$ par

$$t \cdot (x, y) = (x + ty, y) \ .$$

La droite $y = 0$ est formée de points fixes ; les orbites sont ces points, ainsi que les droites $y = y_0$ où y_0 est une constante non nulle. Toutes les orbites sont fermées, mais X/G n'a pas de structure d'espace topologique séparé pour lequel le quotient $\pi : X \to X/G$ est continu. Sinon, deux orbites distinctes auraient des voisinages invariants disjoints ; mais ce n'est pas le cas pour les points fixes (vérifier).

De même, X/G n'a pas de structure de variété algébrique pour laquelle $\pi : X \to X/G$ est un morphisme. Sinon, on pourrait séparer les points de X/G par des fonctions rationnelles, et donc on pourrait séparer les orbites par des fonctions rationnelles invariantes sur X. Mais une telle fonction est fonction rationnelle de y (exercice) ; de plus, une fonction rationnelle de y ne peut séparer deux points fixes distincts. Par contre, la restriction de y à l'ouvert invariant $X \setminus \{y = 0\}$ est le quotient de cet ouvert par G.

(iii) Soit $G = \mathbf{C}^*$ opérant dans $X = \mathbf{C}^2 \setminus \{0\}$ par

$$t(x, y) = (tx, t^{-1}y) \ .$$

Toutes les orbites sont fermées, et tous les groupes d'isotropie sont triviaux, mais les orbites de $(1, 0)$ et de $(0, 1)$ n'admettent pas de voisinages invariants disjoints. Ainsi, X n'admet pas de quotient par G ; mais l'application donnée par $(x, y) \mapsto xy$ se restreint en un quotient algébrique sur les ouverts $X \setminus \{x = 0\}$ et $X \setminus \{y = 0\}$.

Plus généralement, pour toute opération algébrique, il existe un ouvert invariant non vide qui admet un quotient (théorème de Rosenlicht, voir 1.6). Pour une opération d'un groupe algébrique réductif G dans une variété algébrique affine X, on définira une variété algébrique affine $X//G$ qui est le quotient dans un sens affaibli : les fonctions régulières sur $X//G$ sont les fonctions régulières invariantes sur X, et les points de $X//G$ sont les orbites fermées de G dans X (voir 3.1).

1.2. *Opérations de groupes algébriques : généralités et exemples*

Dans tout ce qui suit, on considérera des espaces vectoriels et des variétés algébriques sur le corps $\mathbf{C}$ des nombres complexes. L'algèbre des fonctions régulières sur une variété algébrique X sera notée $\mathbf{C}[X]$. Si de plus X est irréductible, le corps des fonctions rationnelles sur X sera noté $\mathbf{C}(X)$. Lorsque X est affine, $\mathbf{C}(X)$ est le corps des fractions de $\mathbf{C}[X]$.

Définitions. Un *groupe algébrique* (affine) est un groupe G muni d'une structure de variété algébrique affine, telle que la multiplication $G \times G \to G : (g, h) \mapsto gh$ et l'inverse $G \to G : g \mapsto g^{-1}$ soient des morphismes de variétés algébriques.

Une opération

$$\begin{array}{rccc} \alpha : & G \times X & \to & X \\ & (g, x) & \mapsto & g \cdot x \end{array}$$

d'un groupe algébrique G dans une variété algébrique X, est dite *algébrique* si α est un morphisme de variétés algébriques. On dit alors que X est une *G-variété*.

Exemple 1 : les groupes classiques. Soit n un entier positif. Alors le *groupe linéaire* GL_n, formé des matrices $n \times n$ inversibles, est algébrique. En effet, GL_n est l'ouvert de l'espace des matrices $n \times n$ où le déterminant ne s'annule pas. Ainsi, GL_n est une variété algébrique affine, dont l'algèbre des fonctions régulières est engendrée par les coefficients matriciels et par l'inverse du déterminant. De plus, les formules pour la multiplication et l'inverse des matrices sont polynomiales en ces fonctions.

Il en résulte que tout sous-groupe de GL_n qui est défini par des équations polynomiales est algébrique, par exemple :

• le groupe B_n formé des matrices $n \times n$ triangulaires supérieures inversibles,

• le groupe U_n formé des matrices $n \times n$ triangulaires supérieures dont tous les coefficients diagonaux sont égaux à 1 (en particulier,

$$U_2 = \{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbf{C} \}$$

est isomorphe au groupe additif $\mathbf{C}$),

• le groupe T_n formé des matrices diagonales inversibles (alors $T_n \simeq (\mathbf{C}^*)^n$ est appelé *tore* de dimension n ; en particulier, $T_1 = \mathbf{C}^*$ est le groupe multiplicatif de $\mathbf{C}$),

• le *groupe spécial linéaire* SL_n, formé des matrices $n \times n$ de déterminant 1,

• le *groupe orthogonal* O_n formé des matrices qui laissent invariante une forme quadratique non dégénérée,

• le *groupe spécial orthogonal* $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$,

• le *groupe symplectique* Sp_n formé des matrices qui laissent invariante une forme bilinéaire alternée non dégénérée (une telle forme existe si et seulement si n est pair).

Tous ces groupes opèrent dans $\mathbf{C}^n$ par restriction de l'opération naturelle de GL_n dans $\mathbf{C}^n$; ces opérations sont algébriques. Les groupes GL_n, SL_n, O_n, SO_n et Sp_n sont appelés *groupes classiques.*

Exemple 2. Un groupe algébrique G opère dans lui-même par multiplication à gauche, via

$$\lambda(g) \cdot h := gh \ .$$

On a aussi l'opération par multiplication à droite, définie par

$$\rho(g) \cdot h = hg^{-1}$$

et l'opération par conjugaison, définie par

$$h^g := ghg^{-1} \ .$$

Ces trois opérations sont algébriques.

Exemple 3. Soit G un groupe algébrique, et soit G^0 la composante connexe de G qui contient l'élément neutre. Alors G^0 est un sous-groupe algébrique distingué de G, le quotient G/G^0 est fini, et la variété G^0 est irréductible (exercice).

Définition. Soit G un groupe. Un *G-module* est un espace vectoriel muni d'une opération linéaire de G. Si de plus G est algébrique, un G-module V est *rationnel* si tout $v \in V$ est contenu dans un sous-espace vectoriel $W \subseteq V$ (dépendant de v) tel que W est stable par G, et que l'action induite de G dans W est algébrique. Un *invariant* de G dans un G-module V est un point fixe de G ; l'ensemble des invariants de G dans V est un sous-espace vectoriel noté V^G.

Si V et W sont de G-modules rationnels, leur somme directe $V \oplus W$ et leur produit tensoriel $V \otimes W$ le sont aussi. Les puissances tensorielles $V^{\otimes d}$ sont donc des G-modules rationnels, ainsi que les puissance symétriques $S^d V$ et alternées $\wedge^d V$.

Exemple. L'opération naturelle de GL_n dans $\mathbf{C}^n$ fait de $\mathbf{C}^n$ un GL_n-module rationnel. Il en est de même du dual $(\mathbf{C}^n)^*$ où GL_n opère par

$$(g \cdot f)(v) := f(g^{-1}v) \qquad\qquad (g \in \mathrm{GL}_n,\ v \in \mathbf{C}^n,\ f \in (\mathbf{C}^n)^*)\ .$$

Plus généralement, la formule ci-dessus définit une opération de GL_n dans $\mathbf{C}[x_1, \ldots, x_n]$ (l'algèbre des fonctions polynomiales en n variables) ; cette opération préserve le degré. On en déduit que $\mathbf{C}[x_1, \ldots, x_n]$ est un GL_n-module rationnel, somme directe des modules rationnels de dimension finie

$$\mathbf{C}[x_1, \ldots, x_n]_d \simeq S^d(\mathbf{C}^n)^*$$

formés des fonctions polynomiales homogènes de degré d.

On utilisera uniquement des modules rationnels qui sont réunions croissantes d'une famille dénombrable de G-modules rationnels de dimension finie. Des exemples de tels modules sont donnés par la

Proposition 1. *Soient G un groupe algébrique et X une G-variété affine.*
(i) L'algèbre $\mathbf{C}[X]$ des fonctions régulières sur X est munie d'une structure de G-module rationnel par

$$(g \cdot f)(x) := f(g^{-1}x)\ .$$

(ii) Il existe un G-module V, rationnel et de dimension finie, et un morphisme G-équivariant $\iota : X \to V$ qui est un isomorphisme de X sur une sous-variété fermée de V, stable par G.

Démonstration. (i) Le morphisme α induit un homomorphisme d'algèbres

$$\alpha^* : \mathbf{C}[X] \to \mathbf{C}[G \times X] = \mathbf{C}[G] \otimes \mathbf{C}[X]$$

tel que $(\alpha^* f)(g,x) = f(g\cdot x)$. Soit $f \in \mathbf{C}[X]$; soient $u_1,\dots,u_n \in \mathbf{C}[G]$ et $f_1,\dots,f_n \in \mathbf{C}[X]$ tels que $f(g\cdot x) = \sum_{i=1}^n u_i(g) f_i(x)$. Alors on a :

$$g\cdot f = \sum_{i=1}^n u_i(g^{-1}) f_i \ .$$

Ainsi, l'espace vectoriel $\langle G\cdot f\rangle$ engendré par les $g\cdot f$ ($g \in G$), est contenu dans l'espace vectoriel $\langle f_1,\dots,f_n\rangle$. De plus, si l est une forme linéaire sur $\langle G\cdot f\rangle$, alors l s'étend en une forme linéaire (notée aussi l) sur $\langle f_1,\dots,f_n\rangle$, et on a

$$l(g\cdot f) = \sum_{i=1}^n u_i(g^{-1}) l(f_i) \ .$$

L'application $g \mapsto l(g\cdot f)$ est donc régulière. Il en résulte que le G-module $\langle G\cdot f\rangle$ est rationnel.

(ii) Soient $f_1,\dots,f_n$ des générateurs de l'algèbre $\mathbf{C}[X]$. On peut trouver un sous-G-module W de $\mathbf{C}[X]$ qui est de dimension finie et qui contient $f_1,\dots,f_n$. On considère alors l'application

$$\begin{array}{cccc} \iota : & X & \to & W^* \\ & x & \to & (w \to w(x) \ . \end{array}$$

Celle-ci est un morphisme G-équivariant, qui induit une surjection de $\mathbf{C}[W^*]$ sur $\mathbf{C}[X]$ (en effet, l'algèbre $\mathbf{C}[X]$ est engendrée par $W \subseteq \mathbf{C}[W^*]$). Par conséquent, ι identifie X à une sous-variété fermée de W^*.

On va maintenant donner des propriétés générales des orbites pour une opération algébrique d'un groupe algébrique G. Observons que les groupes d'isotropie sont alors fermés dans G ; ce sont donc des groupes algébriques.

Proposition 2. *Soient G un groupe algébrique, et X une G-variété.*

(i) Toute orbite de G dans X est ouverte dans son adhérence.

(ii) L'adhérence de toute orbite est formée de cette orbite et d'orbites de dimension strictement plus petite ; elle contient au moins une orbite fermée.

(iii) Pour tout $x \in X$, on a : $\dim(G\cdot x) = \dim(G) - \dim(G_x)$.

(iv) Pour tout $n \geq 0$, l'ensemble des $x \in X$ tels que $\dim(G\cdot x) \leq n$ *est fermé dans X.*

Démonstration. On va supposer que G est connexe ; le cas général est laissé au lecteur.

(i) L'application

$$\begin{array}{ccc} G & \to & \overline{G\cdot x} \\ g & \mapsto & g\cdot x \end{array}$$

est dominante, donc son image contient un ouvert non vide de $\overline{G\cdot x}$. Mais puisque G opère transitivement dans $G\cdot x$, ce dernier est ouvert dans $\overline{G\cdot x}$.

(ii) On peut supposer que $G \cdot x$ est ouvert dans X. On observe alors que $X \setminus G \cdot x$ est un fermé G-stable de X, et de dimension strictement plus petite. On conclut par récurrence sur la dimension de X.

(iii) Les fibres du morphisme $G \to G \cdot x$ sont les translatés gG_x, donc toutes ces fibres ont la même dimension, égale à celle de G_x. On conclut grâce au théorème sur la dimension des fibres d'un morphisme, voir [Ei] §14.3.

(iv) Considérons l'application

$$\begin{array}{ccc} G \times X & \to & X \times X \\ (g,x) & \mapsto & (x, g \cdot x) \end{array}$$

C'est un morphisme, dont la fibre en (g,x) est isomorphe à G_x. D'après le théorème de semi-continuité de la dimension des fibres d'un morphisme (voir [Ei] §14.3), l'ensemble des $(g,x) \in G \times X$ tels que $\dim(G_x) \geq n$ est fermé dans $G \times X$ pour tout entier n. Par suite, l'ensemble des $x \in X$ tels que $\dim(G_x) \geq n$ est fermé dans X. On conclut grâce à (iii).

Exemple 1 (les formes binaires). Soit $G = SL_2$. Pour tout entier $d \geq 0$, on note V_d l'espace des *formes binaires de degré* d, c'est-à-dire des polynômes homogènes de degré d en deux variables x et y. Alors G opère dans V_d par

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot f(x,y) = f(dx - cy, -bx + ay)$$

et V_d est un G-module rationnel de dimension $d+1$. En particulier, V_1 est le dual du G-module naturel $\mathbf{C}^2$. En fait, V_1 est isomorphe à $\mathbf{C}^2$ car on a une forme bilinéaire alternée non dégénérée et G-invariante sur $\mathbf{C}^2$, donnée par $(v,w) \mapsto \det(v,w)$. Plus généralement, on a :

$$V_d = S^d(\mathbf{C}^2)^* \simeq S^d\mathbf{C}^2 \ .$$

Tout $f \in V_d$ s'écrit sous la forme

$$f(x,y) = \prod_{i=1}^{d} (b_i x - a_i y) \ .$$

Si f est non nulle, les points $[a_i : b_i]$ de la droite projective complexe sont uniquement déterminés par f : ce sont les *racines* de f. Le groupe d'isotropie G_f permute ces racines ; si de plus f a au moins trois racines distinctes, alors le sous-groupe de G_f qui fixe les racines est contenu dans $\{1, -1\}$. Par suite, si f a toutes ses racines distinctes et si $d \geq 3$, alors G_f est fini, et donc l'orbite $G \cdot f$ est de dimension $\dim(\mathrm{SL}_2) = 3$.

Pour $f \in V_d$, on définit le *discriminant* de f par

$$\Delta(f) := \prod_{1 \leq i < j \leq d} (a_i b_j - a_j b_i)^2 \ .$$

Alors $\Delta(f)$ est bien défini, et l'application $\Delta : V_d \to \mathbf{C}$ est polynomiale et G-invariante (exercice). De plus, $\Delta(f) = 0$ si et seulement si f a deux racines confondues.

Si $f \in V_d$ a toutes ses racines distinctes et si $d \geq 2$, alors l'orbite $G \cdot f$ est fermée dans V_d. En effet, on a

$$\overline{G \cdot f} \subseteq \{\varphi \in V_d \mid \Delta(\varphi) = \Delta(f)\} .$$

Ce dernier ensemble est fermé dans V_d et ne contient que des orbites de dimension maximale, d'où l'assertion grâce à la proposition 2 (ii).

Par contre, si f a toutes ses racines confondues, c'est-à-dire si f est une puissance d'une forme linéaire, alors l'orbite $G \cdot f$ est de dimension 2, et l'adhérence de cette orbite contient l'origine (exercice).

Plus généralement, les orbites dont l'adhérence contient l'origine sont celles des formes qui ont une racine de multiplicité $> d/2$, voir 3.3 ci-dessous.

Exemple 2. Soit $G = \mathrm{GL}_n$ opérant dans $X := \mathbf{C}^n \times \mathbf{C}^n$ par $g \cdot (v, w) = (g \cdot v, g \cdot w)$. Si $n \geq 2$, alors G a une orbite ouverte dans X, formée des (v, w) tels que v et w sont linéairement indépendants. Le complémentaire de cette orbite consiste en l'origine, qui est l'unique orbite fermée, et en les orbites

$$\mathcal{O}_{a,b} := \{(av, bv) \mid v \in \mathbf{C}^n\}$$

où $(a, b) \in \mathbf{C}^2$ n'est pas nul. De plus, $\mathcal{O}_{a,b} = \mathcal{O}_{a',b'}$ si et seulement si les vecteurs (a, b) et (a', b') sont proportionnels. Ainsi, les orbites de G dans X sont indexées par la réunion de la droite projective complexe et de deux points.

En particulier, l'adhérence d'une orbite peut contenir une infinité d'orbites. On verra cependant que si G est un tore, alors l'adhérence de toute orbite de G ne contient qu'un nombre fini d'orbites, qu'on décrira de façon combinatoire (proposition 1.5.2 ci-dessous).

Corollaire 1. *Tout groupe algébrique (affine) est isomorphe à un sous-groupe d'un* GL_n*, défini par des équations polynomiales.*

Démonstration. On peut trouver un G-module V, rationnel de dimension finie, et qui contient G comme sous-variété fermée et stable par G (ici G opère dans lui-même par multiplication à gauche). L'opération de G dans V définit un homomorphisme de G dans $\mathrm{GL}(V) = \mathrm{GL}_n$, qui est injectif car V contient G. Par suite, si G opère dans GL_n par multiplication à gauche, alors tous ses groupes d'isotropie sont triviaux. Ainsi, toutes les orbites sont fermées, et en particulier l'image de G dans GL_n est fermée.

On démontre de même le

Corollaire 2. *Pour tout homomorphisme de groupes algébriques $u : G \to H$, l'image $u(G)$ est fermée dans H.*

Exemple. On fait opérer le groupe GL_n dans l'espace M_n des matrices $n \times n$, par conjugaison. On obtient ainsi un homomorphisme de groupes algébriques $u : \mathrm{GL}_n \to \mathrm{GL}_{n^2}$ dont le noyau est formé des homothéties, et dont l'image est PGL_n (le groupe projectif linéaire).

1.3. *Opérations des groupes finis*

Pour une opération d'un groupe fini dans une variété affine, l'espace des orbites est une variété affine, comme le montre la

Proposition 1. *Soit G un groupe fini d'automorphismes d'une variété algébrique affine X.*

(i) L'algèbre des invariants $\mathbf{C}[X]^G$ est de type fini. Si de plus X est irréductible, alors le corps des fractions de $\mathbf{C}[X]^G$ est le corps des invariants $\mathbf{C}(X)^G$.

On note Y la variété algébrique telle que $\mathbf{C}[X]^G = \mathbf{C}[Y]$, et $\pi : X \to Y$ le morphisme défini par l'inclusion de $\mathbf{C}[Y]$ dans $\mathbf{C}[X]$.

(ii) Le morphisme $\pi : X \to Y$ est surjectif, et ses fibres sont les orbites.

Démonstration. (i) Soient $f_1, \ldots, f_n$ des générateurs de l'algèbre $\mathbf{C}[X]$. Soit t une indéterminée. Pour $1 \leq i \leq n$, considérons le polynôme

$$P_i(t) := \prod_{g \in G} (t - g \cdot f_i) \ .$$

Alors les coefficients de P_i sont des invariants de G, car G permute les racines de P_i. Soit $A \subseteq \mathbf{C}[X]$ la sous-algèbre engendrée par les coefficients de $P_1, \ldots, P_n$. Alors chaque f_i est entier sur A, car $P_i(f_i) = 0$. Il en résulte que l'algèbre $\mathbf{C}[X]$ est entière sur A (voir [Ei] §4.1). Puisque l'algèbre A est de type fini, le A-module $\mathbf{C}[X]$ est de type fini (voir [Ei] §13.3). Enfin, comme

$$A \subseteq \mathbf{C}[X]^G \subseteq \mathbf{C}[X],$$

le A-module $\mathbf{C}[X]^G$ est de type fini, donc l'algèbre $\mathbf{C}[X]^G$ l'est aussi.

Il est clair que le corps des fractions de $\mathbf{C}[X]^G$ est contenu dans $\mathbf{C}(X)^G$. Réciproquement, soit $f \in \mathbf{C}(X)^G$. Écrivons $f = uv^{-1}$ avec u et v dans $\mathbf{C}[X]$. Posons $v' := \prod_{g \in G} g \cdot v$ et $u' := u \prod_{g \in G, g \neq e} g \cdot v$. Alors $v' \in \mathbf{C}[X]^G$ et $f = u'v'^{-1}$, donc $u' \in \mathbf{C}[X]^G$.

(ii) On a vu que $\mathbf{C}[X]$ est entier sur $\mathbf{C}[Y]$. Par suite, pour tout idéal premier $Q \subseteq \mathbf{C}[Y]$, il existe un idéal premier $P \subseteq \mathbf{C}[X]$ tel que $Q = P \cap \mathbf{C}[Y]$ (voir [Ei] §4.4). Il en résulte que $\pi : X \to Y$ est surjective.

Soit $x \in X$. Puisque π est G-invariante, on a $G \cdot x \subseteq \pi^{-1}(\pi(x))$. Si cette inclusion est stricte, choisissons $x' \in X$ tel que $\pi(x') = \pi(x)$ et $x' \notin G \cdot x$. Les orbites $G \cdot x$ et $G \cdot x'$ sont des sous-ensembles finis disjoints de X, donc il existe $f \in \mathbf{C}[X]$ telle que $f|_{G \cdot x} = 1$ et que $f|_{G \cdot x'} = 0$. Posons

$$F := \prod_{g \in G} g \cdot f \ .$$

Alors F est invariante, $F|_{G\cdot x} = 1$ et $F|_{G\cdot x'} = 0$ ce qui contredit le fait que $\pi(x') = \pi(x)$.

Cette démonstration reste valable lorsqu'on remplace $\mathbf{C}$ par un corps algébriquement clos arbitraire. Pour une opération linéaire d'un groupe fini dans un espace vectoriel complexe, on a le résultat plus précis suivant.

Proposition 2. *Soit G un sous-groupe fini de $\mathrm{GL}(V)$ où V est un espace vectoriel de dimension finie, et soit N l'ordre de G. Alors l'algèbre des invariants $\mathbf{C}[V]^G$ est engendrée par les invariants homogènes de degré au plus N.*

Démonstration. Soit A la sous-algèbre de $\mathbf{C}[V]^G$ engendrée par les invariants homogènes de degré au plus N. Soit $\mathbf{C}[V]_{<N}$ le sous-espace vectoriel de $\mathbf{C}[V]$ formé des fonctions polynomiales de degré au plus $N-1$. Montrons que le produit $A \cdot \mathbf{C}[V]_{<N}$ est égal à $\mathbf{C}[V]$.

Puisque l'espace vectoriel $\mathbf{C}[V]$ est engendré par les puissances des formes linéaires (exercice), il suffit de montrer que $l^n \in A \cdot \mathbf{C}[V]_{<N}$ pour toute forme linéaire l sur V, et pour tout entier $n \geq 0$. C'est clair si $n < N$. Si $n = N$, alors on a

$$\prod_{g\in G} (t - g \cdot l) = t^N + a_1 t^{N-1} + \cdots + a_N$$

où les a_i sont dans A. On a donc

$$l^N \in A + Al + \cdots + Al^{N-1}$$

et par récurrence sur $n \geq N$:

$$l^n \in A + Al + \cdots + Al^{N-1} \subseteq A\mathbf{C}[V]_{<N} \ .$$

Montrons maintenant que $A = \mathbf{C}[V]^G$. Soit $f \in \mathbf{C}[V]^G$. On peut écrire

$$f = \sum a_i \, f_i$$

avec des a_i dans A et des f_i dans $\mathbf{C}[V]_{<N}$. Soit $p : \mathbf{C}[V] \to \mathbf{C}[V]$ l'application telle que

$$p(u) = \frac{1}{N} \sum_{g\in G} g \cdot u \ .$$

Alors p est $\mathbf{C}[V]^G$-linéaire et envoie $\mathbf{C}[V]$ sur $\mathbf{C}[V]^G$ en préservant le degré. De plus, on a

$$f = p(f) = \sum a_i \, p(f_i)$$

avec des a_i dans A et des f_i dans $\mathbf{C}[V]^G_{<N} \subseteq A$.

Exemple 1 (les groupes cycliques). Soit $G \subset \mathbf{C}^*$ le groupe des racines N-ièmes de l'unité. On fait opérer G dans $V := \mathbf{C}^n$ par multiplication :

$$g \cdot (x_1, \ldots, x_n) = (gx_1, \ldots, gx_n) \ .$$

Alors l'algèbre $\mathbf{C}[V]^G$ est engendrée par les monômes de degré N en $x_1, \ldots, x_n$ (exercice). La borne de la proposition 2 est donc optimale dans ce cas (on peut montrer que c'est le seul cas où cette borne est atteinte, voir [Sc]).

Pour décrire le quotient, introduisons des indéterminées $t_1, \ldots, t_n$ et observons que les monômes de degré N en $x_1, \ldots, x_n$ sont des multiples contants des coefficients de $(t_1x_1+\cdots+t_nx_n)^N$ vu comme polynôme en $t_1, \ldots, t_n$. Autrement dit, on peut identifier V/G à l'ensemble des polynômes en $t_1, \ldots, t_n$ qui sont des puissances N-ièmes de formes linéaires. Cet ensemble est une sous-variété fermée de l'espace des polynômes homogènes de degré N (exercice), et le morphisme quotient est donné par

$$t_1x_1 + \cdots + t_nx_n = u \mapsto u^N \ .$$

Exemple 2 (les fonctions symétriques). Soit $G = S_n$ le groupe symétrique sur n lettres, opérant dans $V = \mathbf{C}^n$ par permutations des coordonnées. Alors l'algèbre $\mathbf{C}[V]^G$ est formée des polynômes symétriques en $x_1, \ldots, x_n$; elle est donc engendrée par les fonctions symétriques élémentaires $e_1, \ldots, e_n$ où

$$e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \ldots, x_{i_k} \ .$$

Autrement dit, le morphisme quotient $\pi : V \to V/G$ est donné par

$$\begin{array}{ccc} \mathbf{C}^n & \to & \mathbf{C}^n \\ (x_1, \ldots, x_n) & \mapsto & (e_1, \ldots, e_n). \end{array}$$

On peut reformuler ce résultat en introduisant une indéterminée t et en observant que

$$\sum_{k=0}^{n} e_k(x_1, \ldots, x_n)t^k = \prod_{i=1}^{n}(1 + tx_i) \ .$$

Ainsi, on peut identifier V/G à l'espace des polynômes en une indéterminée t, de degré au plus n et de terme constant 1. Le morphisme π s'identifie alors à

$$(x_1, \ldots, x_n) \mapsto \prod_{i=1}^{n} (1 + tx_i) \ .$$

Exemple 3 (les fonctions multisymétriques). Plus généralement, on considère l'opération du groupe symétrique $G = S_n$ dans $V = (\mathbf{C}^m)^n$ (produit de n copies de $\mathbf{C}^m$) par permutations de ces copies. L'algèbre $\mathbf{C}[V]$ est alors engendrée par les variables $x_i^{(j)}$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$ dans lesquelles S_n opère par permutation des indices i. L'algèbre des invariants $\mathbf{C}[V]^G$ est formée des *fonctions multisymétriques*.

Soient $t_1 \dots, t_m$ des indéterminées. On peut montrer que le morphisme quotient est donné par

$$(x_i^{(j)})_{1\leq i\leq n, 1\leq j\leq m} \mapsto \prod_{i=1}^{n} (1 + t_1 x_i^{(1)} + \cdots + t_m x_i^{(m)})$$

(voir [Ge-Ka-Ze] Chapter 4, Theorem 2.4). Ainsi, l'algèbre des fonctions multisymétriques est engendrée par les coefficients des monômes en $t_1, \dots, t_m$ dans le produit ci-dessus ; ces coefficients sont les *fonctions multisymétriques élémentaires.* Pour $m \geq 2$, on voit facilement que ces fonctions sont algébriquement dépendantes, mais on ne sait pas expliciter toutes les relations.

Exemple 4 (les groupes alternés). Soit $G = A_n$ le groupe alterné sur n lettres, opérant dans $V = \mathbf{C}^n$ par permutations des coordonnées. Alors (exercice) l'algèbre $\mathbf{C}[V]^G$ est engendrée par $e_1, \dots, e_n$ et par

$$d := \prod_{1\leq i<j\leq n} (x_j - x_i) \ .$$

De plus, d^2 est un polynôme en $e_1, \dots, e_n$.

Pour $n \geq 6$, on ignore si le corps $\mathbf{C}(V)^G = \mathbf{C}(e_1, \dots, e_n, d)$ peut être engendré par n éléments algébriquement indépendants. C'est vrai dans les cas où $n = 2$ (trivial), $n = 3$ (exercice), $n = 4$ (voir [Ke-Vu]) et $n = 5$ (voir [Mae]).

1.4. *Opérations des groupes unipotents.*

Définition. Un groupe algébrique G est *unipotent* s'il est isomorphe à un sous-groupe fermé d'un U_n (on rappelle que U_n désigne le groupe des matrices $n \times n$ triangulaires supérieures, dont tous les coefficients diagonaux sont égaux à 1).

Théorème. *Soit G un groupe unipotent.*

(i) Il existe une suite

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_N = G$$

telle que chaque G_i est un sous-groupe fermé distingué de G_{i+1}, et que chaque G_{i+1}/G_i est isomorphe à $\mathbf{C}$.

(ii) Tout G-module rationnel non trivial contient un invariant non nul de G.

(iii) Toute orbite de G dans une G-variété affine est fermée.

Démonstration. (i) On considère G comme un sous-groupe de U_n. Pour $0 \leq p \leq n$, on pose

$$U_n^p := \{g = (g_{ij}) \in U_n \mid g_{ij} = 0 \text{ si } 1 \leq j - i \leq p\} \ .$$

Alors (U_n^p) est une suite décroissante de sous-groupes fermés distingués de U_n, avec quotients successifs

$$U_n^p / U_n^{p+1} \simeq \mathbf{C}^{n-p} \ .$$

On en déduit qu'il existe une suite croissante

$$\{1\} = V_0 \subset V_1 \subset \cdots \subset V_N = U_n$$

(avec $N = n(n-1)/2$) qui vérifie (i) pour U_n.

On pose $G_i := G \cap V_i$; alors G_i est un sous-groupe fermé de G, distingué dans G_{i+1}, et le quotient G_{i+1}/G_i est un sous-groupe fermé de $V_{i+1}/V_i \simeq \mathbf{C}$. Puisque toute sous-variété fermée de $\mathbf{C}$ est $\mathbf{C}$ ou un nombre fini de points, on en déduit que G_{i+1}/G_i est trivial ou isomorphe à $\mathbf{C}$.

(ii) Soit M un G-module rationnel de dimension finie non nulle. Montrons par récurrence sur $\dim(G)$ que M contient un point fixe non nul.

Si G est de dimension 1, alors G est isomorphe à $\mathbf{C}$ d'après (i). En particulier, G est commutatif, donc tous les éléments de G ont un vecteur propre commun m dans M. On a : $g \cdot m = \chi(g)m$ où $\chi : G \to \mathbf{C}$ est une fonction régulière qui ne s'annule pas. Puisque G est isomorphe à $\mathbf{C}$, la fonction χ est constante, égale à 1 : le point m est fixé par G.

Dans le cas général, on peut trouver un sous-groupe fermé distingué $H \subset G$ tel que G/H est isomorphe à $\mathbf{C}$. D'après l'hypothèse de récurrence, l'ensemble M^H n'est pas réduit à 0. De plus, M^H est stable par G ; c'est donc un G-module rationnel, dans lequel G opère via le quotient $G \to G/H \simeq \mathbf{C}$. On conclut grâce à la première partie de la preuve.

(iii) Soit X une G-variété affine, et soit $x \in X$. Si $G \cdot x$ n'est pas fermé dans X, alors l'idéal I de $\overline{G \cdot x} \setminus G \cdot x$ dans $\overline{G \cdot x}$ n'est pas réduit à 0. D'après (ii), I contient un point fixe $f \neq 0$. Puisque f est invariante par G, elle est constante sur $G \cdot x$ donc sur son adhérence, contradiction.

Corollaire 1. *(i) Tout groupe unipotent est connexe.*

(ii) L'image d'un groupe unipotent par un homomorphisme de groupes algébriques est un groupe unipotent.

(iii) Dans un groupe algébrique, le produit de deux sous-groupes unipotents distingués est un sous-groupe unipotent distingué.

Démonstration. (i) résulte de l'assertion (i) du théorème, par récurrence sur la dimension de G.

(ii) Soit $u : G \to H$ un homomorphisme, où G est unipotent. On peut supposer que $H = \mathrm{GL}_n$; alors $\mathbf{C}^n$ est un G-module rationnel de dimension finie. Si $n \geq 1$, soit v_1 un point fixe de G dans $\mathbf{C}^n$. Alors le quotient $\mathbf{C}^n/\mathbf{C}e_1$ est un G-module rationnel. Par suite, si $n \geq 2$, on peut trouver v_2 dans $\mathbf{C}^n$ non proportionnel à v_1, tel que $g \cdot v_2 - v_2 \in \mathbf{C}v_1$ pour tout $g \in G$. On construit ainsi une base de $\mathbf{C}^n$ dans laquelle toutes les matrices de G sont triangulaires supérieures, avec des coefficients diagonaux égaux à 1.

(iii) Si U et V sont deux sous-groupes fermés distingués d'un groupe algébrique G, alors le produit UV est un sous-groupe fermé distingué de G (exercice). Supposons de plus U et V unipotents ; alors UV vérifie l'assertion

(i) du théorème, car $UV/V \simeq U/U \cap V$. Comme dans la preuve de (ii), on en déduit que UV est unipotent.

Il résulte de (iii) que tout groupe algébrique G contient un plus grand sous-groupe unipotent distingué : le *radical unipotent* de G, noté $R_u(G)$. On a par exemple $R_u(B_n) = U_n$ et $R_u(\mathrm{GL}_n) = \{1\}$ (exercices).

Corollaire 2. *Soit G un groupe algébrique unipotent opérant dans une variété affine irréductible X. Alors le corps des invariants $\mathbf{C}(X)^G$ est le corps des fractions de l'algèbre $\mathbf{C}[X]^G$.*

Démonstration. Soit $f \in \mathbf{C}(X)^G$. Notons M l'ensemble des $\varphi \in \mathbf{C}[X]$ telles que $f\varphi \in \mathbf{C}[X]$. Alors M est un sous-G-module de $\mathbf{C}[X]$, et de plus M est non trivial car f est dans le corps des fractions de $\mathbf{C}[X]$. Par suite, M contient un point fixe non nul de G. Ainsi, on peut écrire $f = \psi\varphi^{-1}$ avec $\varphi \in \mathbf{C}[X]^G$ et $\psi \in \mathbf{C}[X]$. Mais f est invariante, donc $\psi \in \mathbf{C}[X]^G$.

Pour une opération linéaire d'un groupe unipotent, on va voir que le corps des invariants est une extension transcendante pure de $\mathbf{C}$. Plus généralement, on a le résultat suivant, dû à Miyata (voir [Mi] et aussi [Ke-Vu]).

Proposition. *Soit G un sous-groupe du groupe B_n des matrices triangulaires supérieures inversibles. Pour l'action linéaire de G dans $\mathbf{C}^n$, le corps des fonctions rationnelles invariantes est une extension transcendante pure de $\mathbf{C}$.*

La démonstration repose sur le

Lemme. *Soient K un corps et t une indéterminée. Soit G un groupe d'automorphismes de l'anneau $K[t]$, qui laisse stable K. Il existe alors $p \in K[t]^G$ tel que $K(t)^G = K^G(p)$.*

Démonstration du lemme. Montrons que le corps des fractions de $K[t]^G$ est $K(t)^G$. En effet, pour $f \in K(t)^G$, écrivons $f = uv^{-1}$ avec u, $v \in K[t]$ premiers entre eux. Si $\deg(u) \geq \deg(v) > 0$, on écrit $u = qv + r$ avec q, $r \in K[t]$ et $\deg(r) < \deg(v)$; alors q et r sont uniques. Puisque f est invariante par G, les polynômes u et v sont vecteurs propres de G de même poids χ. Par unicité, r est vecteur propre de G de poids χ, et q est invariant par G. On a $uv^{-1} = q + rv^{-1}$ avec $rv^{-1} \in K(t)^G$. On conclut par récurrence sur $\deg(u) + \deg(v)$.

Montrons maintenant l'assertion du lemme. Si $K[t]^G$ est contenu dans K, on peut prendre $p = 1$. Sinon, soit $p \in K[t]^G \setminus K$ de degré minimal. Soit $f \in K[t]^G$. Ecrivons $f = pq + r$ avec $\deg(r) < \deg(p)$. Comme précédemment, on voit que q, $r \in K[t]^G$; d'où $r \in K^G$ et $\deg(q) < \deg(f)$. Par récurrence sur $\deg(f)$, on en déduit que $f \in K^G[p]$. D'où $K[t]^G = K^G[p]$, et $K(t)^G = K^G(p)$ d'après la première partie de la preuve.

La proposition résulte du lemme par récurrence sur n. En effet, soient $x_1,\ldots,x_n$ les coordonnées sur $\mathbf{C}^n$. Posons $K = \mathbf{C}(x_1, \ldots, x_{n-1})$ et $t = x_n$. Alors G est un groupe d'automorphismes de $K[t]$ qui laisse stable K.

Remarque. En particulier, pour une opération linéaire d'un groupe fini abélien, le corps des invariants est une extension transcendante pure de $\mathbf{C}$. Mais ce résultat n'est plus valable pour un groupe fini quelconque, voir [Sa] et aussi [Ke-Vu]. Lorsque G est un groupe algébrique connexe, la question est ouverte (problème de rationalité des corps d'invariants ; voir [Do]).

Exemple. On fait opérer le groupe additif $\mathbf{C}$ sur l'espace V_d des formes binaires de degré d par

$$(t \cdot f)(x,y) = f(x - ty, y) \ .$$

Pour $f \in V_d$, écrivons

$$f(x,y) = \sum_{i=0}^{d} \binom{d}{i} a_i x^{d-i} y^i \ .$$

Alors la coordonnée a_0 est invariante. Notons $\mathcal{U} \subset V_d$ l'ouvert où $a_0 \neq 0$; alors $\mathcal{U}$ est invariant. Soit $S \subset \mathcal{U}$ le fermé où $a_1 = 0$. Montrons que l'application

$$\begin{array}{ccc} \mathbf{C} \times S & \to & \mathcal{U} \\ (t,f) & \mapsto t \cdot f & \end{array}$$

est un isomorphisme. En effet, si $a_0 \neq 0$, il existe un unique $t \in \mathbf{C}$ tel que $t \cdot f \in S$; on a $t = -a_1 a_0^{-1}$ et

$$(t \cdot f)(x,y) = a_0 x^d + \sum_{i=2}^{d} (-1)^i \binom{d}{i} b_i x^{d-i} y^i$$

avec

$$b_i = (i-1) a_1^i + \sum_{j=2}^{i} (-1)^{j-1} \binom{i}{j} a_0^{j-1} a_1^{i-j} a_j$$

(vérifier).

Il en résulte que les fonctions polynomiales $b_2, \ldots, b_d$ sont invariantes, et que pour toute fonction polynomiale invariante P sur V_d, il existe un entier $n \geq 0$ tel que $a_0^n P$ est un polynôme en $a_0, b_2, \ldots, b_d$. En particulier, le corps des invariants est engendré par les éléments algébriquement indépendants a_0 et $b_2, \ldots, b_d$.

La structure de l'algèbre des invariants est plus compliquée. Cette algèbre est engendrée par a_0 pour $d = 1$, et par a_0 et $b_2 = a_1^2 - a_0 a_2$ pour $d = 2$ (exercice). Mais pour $d = 3$, l'algèbre des invariants n'est pas engendrée par a_0, b_2 et b_3, car le discriminant Δ n'est pas fonction polynomiale de ces invariants (exercice) ; en fait, l'algèbre des invariants est engendrée par a_0, b_2, b_3 et Δ, voir 2.4. Plus généralement, l'algèbre des invariants pour une opération linéaire du groupe additif est de type fini (théorème de Weitzenböck, voir le corollaire 2.5.2 ci-dessous).

Cependant, il existe des variétés affines X avec une action du groupe additif $G = \mathbf{C}$, telles que l'algèbre $\mathbf{C}[X]^G$ n'est pas de type fini. En effet, Nagata a construit un exemple d'un sous-groupe unipotent N de $\mathrm{GL}(V)$ tel que l'algèbre des invariants $\mathbf{C}[V]^N$ n'est pas de type fini ; voir [Na], et aussi [A], [Ste2] pour des développements récents. Soit (N_i) une suite de sous-groupes de N comme dans le théorème ci-dessus, et soit i maximal tel que l'algèbre $\mathbf{C}[V]^{N_i}$ est de type fini. Il existe alors une variété algébrique affine X telle que $\mathbf{C}[X] = \mathbf{C}[V]^{N_i}$. De plus, le groupe N_{i+1}/N_i (isomorphe à $\mathbf{C}$) opère dans $\mathbf{C}[X]$ et donc dans X, avec une algèbre d'invariants qui n'est pas de type fini.

1.5. *Opérations des tores.*

Définitions. Un *caractère multiplicatif* d'un groupe algébrique G est un homomorphisme de groupes algébriques $\chi : G \to \mathbf{C}^*$. L'ensemble des caractères multiplicatifs de G forme un groupe pour la multiplication des fonctions ; on le note $X^*(G)$.

Un *sous-groupe à un paramètre* (multiplicatif) de G est un homomorphisme de groupes algébriques $\lambda : \mathbf{C}^* \to G$. L'ensemble des sous-groupes à un paramètre est noté $X_*(G)$; c'est un groupe (pour la multiplication des fonctions à valeurs dans G) lorsque G est abélien.

Proposition 1. *Soit $T \simeq (\mathbf{C}^*)^n$ un tore de dimension n.*
(i) Tout caractère multiplicatif de T est de la forme

$$\chi_{a_1,\ldots,a_n}(t_1, \ldots, t_n) := t_1^{a_1} \cdots t_n^{a_n}$$

pour un unique $(a_1, \ldots, a_n) \in \mathbf{Z}^n$. Ceci identifie le groupe $X^*(T)$ à $\mathbf{Z}^n$.
(ii) Tout sous-groupe à un paramètre de T est de la forme

$$\lambda_{b_1,\ldots,b_n}(t) := (t^{b_1}, \ldots, t^{b_n})$$

pour un unique $(b_1, \ldots, b_n) \in \mathbf{Z}^n$. Ceci identifie le groupe $X_*(T)$ à $\mathbf{Z}^n$.
(iii) Pour tous $\chi \in X^*(T)$ et $\lambda \in X_*(T)$, il existe un unique entier $\langle \chi, \lambda \rangle$ tel que

$$\chi(\lambda(t)) = t^{\langle \chi, \lambda \rangle}$$

pour tout $t \in \mathbf{C}^*$. De plus, l'application

$$\begin{array}{ccc} X^*(T) \times X_*(T) & \to & \mathbf{Z} \\ (\chi, \lambda) & \mapsto & \langle \chi, \lambda \rangle \end{array}$$

est bilinéaire et non dégénérée.
(iv) Tout T-module rationnel V est somme directe de ses espaces propres

$$V_\chi := \{v \in V \mid t \cdot v = \chi(t)v \ \forall t \in T\}$$

où χ décrit les caractères multiplicatifs de T.

Démonstration. On commence par observer que

$$\mathbf{C}[T] = \mathbf{C}[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}] = \bigoplus_{(a_1,\ldots,a_n)\in\mathbf{Z}^n} \mathbf{C}t_1^{a_1}\cdots t_n^{a_n} \ .$$

(i) Soit $\chi : T \to \mathbf{C}^*$ un caractère multiplicatif. Alors χ est une fonction régulière inversible sur $(\mathbf{C}^*)^n$ donc χ est le produit d'un monôme de Laurent $\chi_{a_1,\ldots,a_n}$ par une constante. Puisque $\chi(1) = 1$, on a bien $\chi = \chi_{a_1,\ldots,a_n}$.

(ii) De même, un homomorphisme $\lambda : \mathbf{C}^* \to T$ est donné par n fonctions régulières inversibles sur $\mathbf{C}^*$, qui prennent la valeur 1 en 1. Chacune de ces fonctions est donc un monôme de Laurent.

(iii) résulte aussitôt de la formule

$$\chi_{a_1,\ldots,a_n}(\lambda_{b_1,\ldots,b_n}(t)) = t^{a_1b_1+\cdots+a_nb_n} \ .$$

(iv) On peut supposer V de dimension finie. Alors l'opération linéaire $T \times V \to V$ définit un morphisme

$$\begin{array}{ccc} V & \to & \mathbf{C}[T] \otimes V \\ v & \to & (t \mapsto t \cdot v). \end{array}$$

Grâce à la décomposition ci-dessus de $\mathbf{C}[T]$, il existe une famille $(v_{a_1,\ldots,a_n})$ dans V telle que

$$t \cdot v = \sum_{(a_1,\ldots,a_n)\in\mathbf{Z}^n} t_1^{a_1}\cdots t_n^{a_n} v_{a_1,\ldots,a_n} \ .$$

Il en résulte que $v = \sum v_{a_1,\ldots,a_n}$ est la décomposition de v en vecteurs propres de T.

Pour tout sous-groupe fermé D d'un tore T, le quotient T/D est un tore, ainsi que la composante neutre D^0 (exercice). Par suite, toutes les orbites d'un tore sont des tores. On va étudier les adhérences des orbites de T dans une variété affine X ; pour cela, d'après la proposition 1.2.1, on peut supposer que $X = V$ est un T-module rationnel de dimension finie.

Soit

$$V = \oplus_{\chi\in X^*(T)} V_\chi$$

la décomposition en sous-espaces propres. Pour $v \in V$, écrivons

$$v = \sum_{\chi\in X^*(T)} v_\chi$$

et notons $\chi(v)$ l'ensemble des χ tels que $v_\chi \neq 0$. Alors $\chi(v)$ est un sous-ensemble fini du groupe $X^*(T) \simeq \mathbf{Z}^n$. On note $C(v)$ le cône convexe engendré par $\chi(v)$ dans l'espace vectoriel réel $X^*(T)_\mathbf{R} \simeq \mathbf{R}^n$.

Rappelons qu'une *face* d'un convexe fermé $C \subseteq \mathbf{R}^n$ est un sous-ensemble de la forme $C \cap (f=0)$ où f est une forme linéaire sur $\mathbf{R}^n$ telle que $f(x) \geq 0$ pour tout $x \in C$. Pour chaque face F de $C(v)$, on note $\mathcal{O}_F$ l'orbite par T du vecteur

$$v_F := \sum_{\chi \in \chi(v) \cap F} v_\chi \ .$$

Proposition 2. *Avec les notations précédentes, l'application $F \to \mathcal{O}_F$ est une bijection de l'ensemble des faces du cône $C(v)$, sur l'ensemble des orbites de T dans $\overline{T \cdot v}$. De plus, pour deux faces F et F' arbitraires, on a $F \subseteq F'$ si et seulement si $\mathcal{O}_F \subseteq \overline{\mathcal{O}_{F'}}$.*

Démonstration. Posons $X = \overline{T \cdot v}$, et notons A l'algèbre des fonctions régulières sur X. L'application dominante $T \to X : t \mapsto t \cdot v$ induit un homomorphisme injectif $A \to \mathbf{C}[T]$ que l'on considérera comme une inclusion. On a

$$\mathbf{C}[T] = \bigoplus_{\chi \in X^*(T)} \mathbf{C}\chi$$

et de plus, A est stable par l'opération de T dans $\mathbf{C}[T]$ induite par la multiplication à gauche. On en déduit que

$$A = \bigoplus_{\chi \in S} \mathbf{C}\chi$$

où S est un semi-groupe contenu dans $X^*(T)$. Puisque l'algèbre A est engendrée par les fonctions coordonnées sur V, on en déduit que S est engendré par les $-\chi$, $\chi \in \chi(v)$.

Soit $Y \subseteq X$ une sous-variété irréductible fermée et stable par T ; soit $I \subseteq A$ l'idéal de Y. Alors I est un idéal premier de A, stable par T. On peut donc écrire

$$I = \bigoplus_{\chi \in S_I} \mathbf{C}\chi$$

où S_I est un sous-ensemble de S tel que, pour tous α et β dans S, on ait : $\alpha + \beta \notin S_I$ si et seulement si $\alpha \notin S_I$ et $\beta \notin S_I$. On en déduit qu'il existe une unique face F de $C(v)$ telle que : $\chi \in S_I$ si et seulement si $-\chi \in S \setminus F$.

Montrons que $Y = \overline{\mathcal{O}_F}$. Puisque F est une face de $C(v)$, il existe une forme linéaire sur $X^*(T)_\mathbf{R}$ qui est nulle sur F et négative sur $C(v) \setminus F$. Puisque le cône $C(v)$ est engendré par des points de $X^*(T)$, on peut trouver une telle forme linéaire λ dans le réseau dual $X_*(T)$. Alors, pour toute $f \in A$ et pour tout $x \in X$, la fonction $t \mapsto f(\lambda(t)x)$ a une limite quand $t \to 0$. De plus, l'idéal engendré par les fonctions $x \mapsto f(\lambda(t)x) - f(x)$ $(f \in A)$ est égal à I. Cela signifie que $\lambda(t)x$ a une limite en 0 pour tout $x \in X$, que cette limite est dans Y, et que l'application

$$\begin{array}{ccc} X = \overline{T \cdot v} & \to & Y \\ x & \mapsto & \lim_{t \to 0} \lambda(t)x \end{array}$$

est un morphisme surjectif et T-équivariant. Mais ce morphisme envoie v sur v_F, d'où l'assertion.

On a démontré que toute sous-variété irréductible fermée et stable par T est de la forme $\overline{\mathcal{O}_F}$ pour une unique face F. Il en résulte que toute orbite de T dans X est de la forme $\mathcal{O}_F$ pour une unique face F. Si de plus $F \subseteq F'$, alors on a pour les idéaux premiers correspondants : $I' \subseteq I$, d'où $\mathcal{O}_F \subseteq \overline{\mathcal{O}_{F'}}$.

Corollaire. *Le tore T n'a qu'un nombre fini d'orbites dans $\overline{T \cdot v}$. Pour une telle orbite $\mathcal{O}$, il existe un sous-groupe à un paramètre λ de T tel que la limite en 0 de la fonction $t \mapsto \lambda(t)v$ existe et appartient à $\mathcal{O}$.*

En particulier, on voit que l'adhérence d'une orbite d'un tore dans une variété affine contient une unique orbite fermée (car tout cône convexe a une unique face minimale). Ce résultat sera généralisé en 3.1.

On va maintenant décrire les algèbres d'invariants pour les opérations linéaires des tores, ou plus généralement pour l'opération d'un sous-groupe fermé $D \subseteq T_n$ dans $V = \mathbf{C}^n$. On note $x_1, \ldots, x_n$ les coordonnées sur $\mathbf{C}^n$, et $\chi_1, \ldots, \chi_n$ leurs poids par rapport à D. Chaque monôme

$$x^a := x_1^{a_1} \cdots x_n^{a_n}$$

est un vecteur propre de D, de poids $a_1\chi_1 + \cdots + a_n\chi_n$. Par suite, l'algèbre $\mathbf{C}[V]^D$ a pour base les monômes x^a tels que $\sum_{i=1}^n a_i\chi_i = 0$.

Soit S l'ensemble des n-uplets d'entiers non négatifs $(a_1, \ldots, a_n)$ tels que $\sum_{i=1}^n a_i\chi_i = 0$. Alors S est un semi-groupe pour l'addition. Un élément a de S est *indécomposable* si $a \neq 0$ et si a ne peut s'écrire comme somme de deux éléments non nuls de S. Notons $\mathcal{I}(S)$ l'ensemble des éléments indécomposables de S. On peut maintenant énoncer le résultat suivant dû à Gordan.

Proposition 3. *Avec les notations précédentes, l'ensemble $\mathcal{I}(S)$ est fini, et c'est un système générateur minimal du semi-groupe S. De plus, l'ensemble des monômes x^a $(a \in \mathcal{I}(S))$ est un système générateur minimal de l'algèbre $\mathbf{C}[V]^D$.*

Démonstration. Pour $a \in \mathbf{R}^n$, on pose

$$|a| := a_1 + \cdots + a_n \ .$$

Si $a \in S$ est décomposable, alors $a = a' + a''$ avec a', a'' dans S et $|a'| < |a|$, $|a''| < |a|$. On en déduit que $\mathcal{I}(S)$ est un système générateur minimal de S, puis que l'ensemble des x^a $(a \in \mathcal{I}(S))$ est un système générateur minimal de l'algèbre $\mathbf{C}[V]^D$.

Pour montrer que $\mathcal{I}(S)$ est fini, on introduit le cône convexe fermé $C \subseteq \mathbf{R}^n$ engendré par S. Alors $S = C \cap \mathbf{Z}^n$ et de plus

$$C = \{(x_1, \ldots, x_n) \in (\mathbf{R}_{\geq 0})^n \ ; | \ ; \sum_{i=1}^n x_i\chi_i = 0\} \ .$$

Il en résulte que le cône C est engendré par un nombre fini de demi-droites $d_1, \ldots, d_N$, telles que chaque d_i rencontre $\mathbf{Z}^n \setminus \{0\}$. On note γ_i l'unique générateur du semigroupe $d_i \cap \mathbf{Z}^n$.

D'après un théorème de Carathéodory, le cône C est réunion des cônes engendrés par les familles linéairement indépendantes des γ_i. Pour une telle famille $(\gamma_i)_{i\in I}$, on note C_I le cône engendré, et on pose $S_I = C_I \cap \mathbf{Z}^n$. Alors le semigroupe S_I est engendré par l'ensemble fini

$$\{x = \sum_{i \in I} x_i\gamma_i \;;|\;; 0 \leq x_i \leq 1\} \cap \mathbf{Z}^n$$

(exercice). Par suite, le semigroupe $S = \cup_I S_I$ est engendré par la réunion de ces ensembles finis.

Remarque 1. L'approche précédente conduit à des bornes effectives sur les degrés des générateurs de l'algèbre $\mathbf{C}[V]^D$, voir [We].

Remarque 2. Soit $V//D$ la variété algébrique affine dont l'algèbre des fonctions régulières est $\mathbf{C}[V]^D$. Le groupe T_n (qui contient D) opère dans l'algèbre $\mathbf{C}[V]^D$ par automorphismes ; il opère donc dans $V//D$. En fait, T_n a une orbite ouverte dans $V//D$, et le cône convexe associé n'est autre que C (exercice).

Réciproquement, si un tore opère dans une variété affine X avec une orbite ouverte, et si de plus X est normale (voir [Ei] §4.2 ou 3.2 ci-dessous), alors il existe un groupe diagonalisable D et un D-module V tels que $X = V//D$ (exercice).

Exemple 1. Soit m un entier positif. Soit $D \subset T_2$ le groupe cyclique d'ordre m, formé des matrices diagonales (ζ, ζ) où $\zeta^m = 1$. En notant x, y les coordonnées, l'algèbre $\mathbf{C}[V]^T$ est engendrée par les monômes en x et y de degré m.

Exemple 2. Soit $D \subset T_4$ le tore formé des matrices diagonales (u, u^{-1}, u^{-1}, u). En notant x, y, z, t les coordonnées, l'algèbre $\mathbf{C}[V]^T$ est engendrée par les monômes xy, xz, yt et zt. On en déduit que

$$\mathbf{C}[V]^D = \mathbf{C}[X, Y, Z, T]/(XT - YZ)\ .$$

Exemple 3. Soit T le tore de dimension 3 défini par

$$T = \{(t_1, t_2, t_3, t_4) \in (\mathbf{C}^*)^4 \;;|\; t_1t_2t_3t_4 = 1\}\ .$$

Pour $1 \leq i \leq 4$, notons χ_i le caractère de T tel que $\chi_i(t_1, t_2, t_3, t_4) = t_i$. Soit V le T-module rationnel dont les poids sont les $\chi_i + \chi_j$ $(1 \leq i < j \leq 4)$ de multiplicité un. Alors l'algèbre $\mathbf{C}[V]^G$ est engendrée par les monômes $x_{12}x_{34}$, $x_{13}x_{24}$, $x_{23}x_{14}$ avec des notations évidentes.

Enfin, toute opération d'un tore est "birationnellement triviale" dans le sens suivant :

Proposition 4. *Soit T un tore opérant dans une variété affine irréductible X, et soit $T_X \subseteq T$ le noyau de cette opération. Il existe alors un ouvert $X_0 \subseteq X$ non vide, affine et stable par T, ainsi qu'une sous-variété fermée $Y \subseteq X_0$ tels que l'application*

$$\begin{array}{ccc} (T/T_X) \times Y & \to & X_0 \\ (tT_X, y) & \to & t \cdot y \end{array}$$

est un isomorphisme.

Démonstration. Quitte à remplacer T par T/T_X, on peut supposer l'opération fidèle. Observons que l'ensemble des groupes d'isotropie T_x $(x \in X)$ est fini (pour le vérifier, on peut supposer que X est un T-module, et on utilise alors la proposition 1). De plus, pour tout sous-groupe non trivial T' de T, l'ensemble $X^{T'}$ de ses points fixes est distinct de X, car T opère fidèlement. Il existe donc $x \in X$ tel que T_x est trivial.

Soit $F := \overline{T \cdot x} \setminus T \cdot x$. Puisque F est fermé dans $\overline{T \cdot x}$, on peut trouver $\varphi \in \mathbf{C}[X]$ vecteur propre de T, tel que $\varphi(x) \neq 0$ et que $\varphi|_F = 0$. Alors l'ensemble

$$X_\varphi = \{z \in X \mid \varphi(z) \neq 0\}$$

est un ouvert affine de X, stable par T, et contenant $T \cdot x$ comme orbite fermée de T.

On a

$$\mathbf{C}[T \cdot x] = \mathbf{C}[T] = \bigoplus_{\chi \in X^*(T)} \mathbf{C}\chi \ .$$

On choisit une base $(\chi_1, \ldots, \chi_n)$ du groupe abélien libre $X^*(T)$, ce qui identifie T à $(\mathbf{C}^*)^n$. On étend chaque $\chi_i : T \cdot x \to \mathbf{C}^*$ en une fonction régulière f_i sur X_φ qui est vecteur propre de T de poids χ_i. Soit X_0 l'ouvert de X_φ où aucun des f_i ne s'annule. Alors l'application

$$f := (f_1, \ldots, f_n) : X_0 \to (\mathbf{C}^*)^n$$

est T-équivariante ; soit Y sa fibre au point $(1, \ldots, 1)$ de $(\mathbf{C}^*)^n$. Les applications

$$\begin{array}{ccc} T \times Y & \to & X_0 \\ (t, y) & \mapsto & t \cdot y \end{array}$$

et

$$\begin{array}{ccc} X_0 & \to & T \times Y \\ z & \to & (f(z), f(z)^{-1} \cdot z) \end{array}$$

sont des isomorphismes inverses l'un de l'autre.

Remarque. L'opération d'un groupe algébrique G dans une variété algébrique X n'est pas toujours birationnellement triviale. Par exemple, soit X l'ensemble des matrices $n \times n$ ayant toutes leurs valeurs propres distinctes. Alors $X \subset M_n$ est un ouvert affine, stable par l'opération de GL_n par conjugaison. De plus, tout groupe d'isotropie de GL_n dans X est conjugué au groupe T_n des matrices diagonales inversibles. Mais aucun ouvert GL_n-stable $X_0 \subseteq X$ n'est de la forme $(\mathrm{GL}_n/T_n) \times Y$. Sinon, puisque T_n fixe $n!$ points dans GL_n/T_n, l'ensemble $X_0^{T_n}$ aurait $n!$ composantes connexes. Mais $X_0^{T_n}$ est un ouvert de l'espace des matrices diagonales ; il est donc irréductible, contradiction.

1.6. *Un théorème de Rosenlicht*

On a vu en 1.1 que le quotient d'une variété algébrique X par l'opération d'un groupe algébrique n'existe pas toujours (comme variété algébrique). Mais un théorème fondamental, dû à M. Rosenlicht, affirme qu'un tel quotient existe si on remplace X par un ouvert convenable (voir [Ro]). Pour énoncer ce théorème, on doit d'abord préciser la notion de quotient.

Définition. Un *quotient géométrique* d'une variété irréductible X par l'action d'un groupe algébrique G est la donnée d'une variété Y et d'un morphisme $\pi : X \to Y$ tels que :

(i) π est surjectif et les fibres de π sont les orbites de G (en particulier, π est invariant, et toutes les orbites sont fermées).

(ii) π induit un isomorphisme $\mathbf{C}(Y) \to \mathbf{C}(X)^G$.

Pour l'opération d'un groupe fini G dans une variété affine X, le quotient géométrique existe d'après 1.3. Mais en général, le quotient géométrique peut ne pas exister, même si toutes les orbites sont fermées ; voir les exemples en 1.1.

Théorème. *Soit G un groupe algébrique opérant dans une variété affine irréductible X. Il existe alors un ouvert $X_0 \subseteq X$ non vide et stable par G, avec un quotient géométrique $\pi : X_0 \to Y_0$.*

Démonstration. On considère d'abord le cas où le groupe G est connexe. Puisque le corps $\mathbf{C}(X)$ est une extension de type fini de $\mathbf{C}$, il en est de même du sous-corps $\mathbf{C}(X)^G$. On choisit des générateurs $f_1, \ldots, f_n$ de ce sous-corps. Quitte à remplacer X par un ouvert stable par G, on peut supposer que les fonctions rationnelles $f_1, \ldots, f_n$ sont régulières sur X, et que le morphisme $\pi = (f_1, \ldots, f_n) : X \to \mathbf{C}^n$ a pour image une variété algébrique affine Y (mais X n'est pas nécessairement affine). D'après le théorème de platitude générique (voir [Ei] §14.2), on peut aussi supposer que le morphisme π est plat ; alors toutes ses fibres ont la même dimension. Puisque G est connexe, le corps $\mathbf{C}(X)^G$ est algébriquement clos dans $\mathbf{C}(X)$ (vérifier). On peut donc aussi supposer que toutes les fibres de π sont irréductibles.

On considère le morphisme

$$\begin{array}{rccc} \varphi & : G \times X & \to & X \times X \\ & (g, x) & \mapsto & (x, g \cdot x) \end{array}$$

et on note Γ son image ; alors

$$\Gamma = \{(x, x') \in X \times X \mid x' \in G \cdot x\} .$$

Puisque π est G-invariant, Γ est contenu dans la sous-variété fermée

$$X \times_Y X = \{(x, x') \in X \times X \mid \pi(x) = \pi(x')\}$$

de $X \times X$. En notant $pr_1 : X \times X \to X$ la première projection, on observe que les fibres de la restriction de pr_1 à Γ sont les orbites ; d'autre part, la restriction de pr_1 à $X \times_Y X$ est plate, et ses fibres sont les fibres de π. Il en résulte que la variété (quasi-affine) $X \times_Y X$ est irréductible.

On va montrer que Γ est dense dans $X \times_Y X$. Il en résultera qu'au-dessus d'un ouvert non vide de Y, chaque fibre de π contient une orbite dense de G. En remplaçant X par un ouvert formé d'orbites de dimension maximale, on peut supposer de plus que toutes les orbites sont fermées ; alors les fibres de π sont les orbites.

Si Γ n'est pas dense dans $X \times_Y X$, on peut trouver une fonction rationnelle sur $X \times_Y X$, définie et nulle sur Γ. Puisque $\mathbf{C}(X \times_Y X)$ est le corps des fractions (d'un quotient) de l'anneau $\mathbf{C}[X] \otimes_{\mathbf{C}[Y]} \mathbf{C}[X]$, et donc de $\mathbf{C}(X) \otimes_{\mathbf{C}(Y)} \mathbf{C}(X)$, on peut trouver $u_1, \ldots, u_r, v_1, \ldots, v_r \in \mathbf{C}(X)$ tels que $\sum_{i=1}^r u_i \otimes v_i$ est non nul dans $\mathbf{C}(X) \otimes_{\mathbf{C}(Y)} \mathbf{C}(X)$, mais nul sur Γ. Alors

$$\sum_{i=1}^r u_i(gv_i) = 0$$

pour tout $g \in G$. En décomposant les v_i dans une base du $\mathbf{C}(Y)$-espace vectoriel $\mathbf{C}(X)$, on peut supposer que $v_1, \ldots, v_r$ sont linéairement indépendants sur $\mathbf{C}(Y)$.

Montrons par récurrence sur r que $u_1 = \cdots = u_r = 0$, ce qui contredira l'hypothèse $\sum_{i=1}^r u_i \otimes v_i \neq 0$. Si $r = 1$, c'est clair. Dans le cas général, si $u_1 \neq 0$ alors

$$\sum_{i=1}^r h(u_i u_1^{-1})(gv_i) = 0$$

pour tous $g, h \in G$. D'où

$$\sum_{i=2}^r (h(u_i u_1^{-1}) - u_i u_1^{-1})(gv_i) = 0$$

et par hypothèse de récurrence : $h(u_i u_1^{-1}) = u_i u_1^{-1}$ pour tout $h \in G$, c'est-à-dire $u_i = u_1 w_i$ avec $w_i \in \mathbf{C}(Y)$. Mais alors $\sum_{i=1}^r v_i w_i = 0$ avec $w_1 = 1$, ce qui contredit l'indépendance linéaire de $v_1, \ldots, v_r$.

Dans le cas d'un groupe G non nécessairement connexe, l'argument ci-dessus fournit un ouvert $X_0 \subseteq X$ non vide et stable par G^0, admettant un quotient géométrique par G^0. Puisque le groupe G/G^0 est fini, l'intersection des gX_0 $(g \in G)$ est un ouvert non vide et stable par G^0. Quitte à remplaçer X par cet ouvert, on peut supposer que le quotient géométrique $X \to X/G^0$

existe, où X/G^0 est une variété quasi-affine dans laquelle opère le groupe fini G/G^0 (vérifier). Mais alors le quotient géométrique $X/G^0 \to X/G$ par G/G^0 existe, ce qui termine la preuve.

Corollaire. *Le degré de transcendance sur* $\mathbf{C}$ *du corps* $\mathbf{C}(X)^G$ *est égal à*

$$\dim(X) - \max_{x \in X} \dim(G \cdot x) \ .$$

En particulier, X *contient une orbite dense de* G *si et seulement si toute fonction rationnelle invariante sur* X *est constante.*

Démonstration. On peut remplacer X par un ouvert non vide et stable par G ; on peut donc supposer que le quotient géométrique $\pi : X \to Y$ existe. Alors les assertions résultent du théorème sur la dimension des fibres d'un morphisme (voir [Ei] §14.3).

Proposition 5. *Soient* G *un groupe algébrique affine, et* H *un sous-groupe fermé de* G*. Alors le quotient géométrique* $\pi : G \to G/H$ *existe.*

Démonstration. Soit $I \subset \mathbf{C}[G]$ l'idéal de la sous-variété fermée $H \subseteq G$. Alors

$$H = \{g \in G \mid Hg \subseteq H\} = \{g \in G \mid \rho(g)I(H) \subseteq I(H)\} \ .$$

Puisque le G-module $\mathbf{C}[G]$ est réunion croissante de sous-modules de dimension finie, et que l'idéal I est de type fini, il existe un G-module V (rationnel, de dimension finie), et un sous-espace vectoriel $W \subseteq V$ tels que

$$H = \{g \in G \mid g \cdot W \subseteq W\} \ .$$

Soit n la dimension de W, et soit $\wedge^n V$ la puissance extérieure n-ième de V. Alors $\wedge^n V$ est un G-module qui contient la droite $\wedge^n W$, et

$$H = \{g \in G \mid g \cdot \wedge^n W = \wedge^n W\} \ .$$

Autrement dit, H est le groupe d'isotropie du point $x = [\wedge^n W]$ de l'espace projectif $\mathbf{P}(\wedge^n V)$ dans lequel opère G. On définit $\pi : G \to G{\cdot}x$ par $\pi(g) = g{\cdot}x$. Alors les fibres de π sont les orbites de H. De plus, l'application $\pi^* : \mathbf{C}(G{\cdot}x) \to \mathbf{C}(G)^H$ est un isomorphisme d'après le lemme ci-dessous, donc π est un quotient géométrique.

Lemme. *Soient* X, Y *des variétés irréductibles, et* $\pi : X \to Y$ *un morphisme dominant. Soit* $f \in \mathbf{C}(X)$ *constante sur les fibres de* π*. Alors* f *est dans* $\pi^*\mathbf{C}(Y)$*.*

Démonstration. On peut supposer que X est affine et que $f \in \mathbf{C}[X]$. Considérons l'application

$$\begin{array}{rccc} \varphi : & X & \to & Y \times \mathbf{C} \\ & x & \to & (\pi(x), f(x)) \end{array}$$

Alors π se factorise par

$$\varphi : X \to \overline{\varphi(X)}$$

suivi de

$$\begin{array}{rccc} \psi : & \overline{\varphi(X)} & \to & Y \\ & (y,z) & \to & y \end{array}$$

De plus la restriction de ψ à $\varphi(X)$ est injective, donc ψ^* identifie le corps $\mathbf{C}(Y)$ à $\mathbf{C}(\overline{\varphi(X)})$. Mais ce dernier corps contient f.

Remarque. On montre de façon analogue que pour tout ouvert affine $U \subseteq G/H$, son image réciproque $\pi^{-1}(U) \subseteq G$ est affine, et que l'application $\pi^* : \mathbf{C}[U] \to \mathbf{C}[\pi^{-1}(U)]^H$ est un isomorphisme.

2. Représentations et invariants des groupes linéairement réductifs

2.1. *Groupes algébriques linéairement réductifs*

Définitions. Soient G un groupe algébrique et V un G-module rationnel. Alors V est *simple* si les seuls sous-modules rationnels de V sont $\{0\}$ et V.

On dit que V est *semi-simple* (ou encore *complètement réductible*) s'il vérifie l'une des conditions équivalentes suivantes :

(i) V est somme de sous-modules simples.

(ii) V est somme directe de sous-modules simples.

(iii) Tout sous-module de V admet un supplémentaire stable par G.

Enfin, le groupe G est *linéairement réductif* si tout G-module rationnel de dimension finie est semi-simple.

Voici plusieurs caractérisations des groupes linéairement réductifs.

Théorème. *Pour un groupe algébrique affine G, les conditions suivantes sont équivalentes :*

(i) G est linéairement réductif.

(ii) Tout G-module rationnel est semi-simple.

(iii) Dans le G-module $\mathbf{C}[G]$ où G opère par multiplication à droite, le sous-module $\mathbf{C}$ formé des fonctions constantes admet un supplémentaire stable par G.

(iv) Pour tout G-module rationnel V, le sous-module V^G formé des invariants de G dans V, admet un supplémentaire stable par G ; soit $p_V : V \to V^G$ la projection correspondante. De plus, si $u : V \to W$ est un morphisme de G-modules, alors $u|_{V^G} \circ p_V = p_W \circ u$.

Démonstration. (i)⇒(ii) : Soit W un sous-G-module de V. Montrons que W a un supplémentaire stable par G. Soit $(V_n)_{n\geq 0}$ une suite croissante de sous-modules de V, dont la réunion est V. Par hypothèse, on peut écrire $W \cap V_n = (W \cap V_{n-1}) \oplus W_n$ avec W_n stable par G, et aussi $V_n = V_{n-1} \oplus W_n \oplus S_n$ avec S_n stable par G. Alors $W = \oplus_{n\geq 0} W_n$ et $V = \oplus_{n\geq 0} (W_n \oplus S_n)$, donc $S = \oplus_{n\geq 0} S_n$ convient.

(ii)⇒(iii) : Décomposons $\mathbf{C}[G]$ en somme directe de sous-modules simples M_n ; alors le G-module trivial apparaît une seule fois, car les invariants de G dans $\mathbf{C}[G]$ sont formés des fonctions constantes. La somme directe des M_n qui sont non triviaux est donc le supplémentaire cherché.

(iii)⇒(iv) : Notons $I : \mathbf{C}[G] \to \mathbf{C}$ la projection définie par le choix d'un supplémentaire stable G de $\mathbf{C}$ dans $\mathbf{C}[G]$; alors I est invariante par G.

Soit V un G-module rationnel de dimension finie. A tous $v \in V$ et $l \in V^*$, associons l'élément $f_{v,l}$ de $\mathbf{C}[G]$ défini par

$$f_{v,l}(g) = l(g \cdot v) \ .$$

Si (e_i) est une base de V, et (e_j^*) est la base duale, alors on a

$$g \cdot e_i = \sum_j f_{ij}(g) e_i$$

avec $f_{ij} = f_{e_i, e_j^*}$. Les $f_{i,j}$ sont donc les coefficients matriciels du G-module V. On définit $p_V : V \to V$ par

$$p_V(e_i) = \sum_j I(f_{ij}) e_j,$$

c'est-à-dire :

$$l(p_V(v)) = I(f_{v,l})$$

pour tous $v \in V$ et $l \in V^*$. Vérifions que p_V a les propriétés requises.

Si $g \in G$, alors $l(p_V(g \cdot v)) = I(f_{gv,l}) = I(\rho(g) f_{v,l}) = I(f_{v,l}) = l(p_V(v))$ donc p_V est invariante par G. De plus, pour $v \in V^G$, on a $f_{v,l} = l(v)$ d'où $l(p_V(v)) = I(f_{v,l}) = l(v)$ et $p_V(v) = v$. Il en résulte que p_V est une projection de V sur V^G.

Si $u : V \to W$ est un G-morphisme, et si $m \in W^*$, alors $m((p_W \circ u)(v)) = I(f_{m,u(v)}) = I(f_{m \circ u, v}) = (m \circ u)(p_V(v))$ d'où $p_W \circ u = u \circ p_V$.

Enfin, lorsque V est un G-module rationnel arbitraire, on écrit V comme réunion croissante de sous-modules rationnels V_n de dimension finie. Puisque les p_{V_n} sont compatibles avec l'inclusion, elles s'assemblent en $p_V : V \to V^G$.

(iv)$\Rightarrow$(i) : Soit W un sous-G-module de V. La donnée d'un supplémentaire stable par G de W dans V équivaut à celle d'un G-morphisme $u : V/W \to V$ tel que $u(v + W) \in v + W$ pour tout $v \in V$.

On fait opérer G dans $\mathrm{Hom}(V/W, V)$ par $(g \cdot u)(x) = g \cdot u(g^{-1} \cdot x)$. Alors $\mathrm{Hom}(V/W, V)$ est un G-module rationnel, dont les invariants sont formés des G-morphismes de V/W dans V. On considère

$$M = \{u \in \mathrm{Hom}(V/W, V) \mid u(v + W) \in \lambda(u)(v + W) \text{ pour un } \lambda(u) \in \mathbf{C}\}\ .$$

Alors M est un sous-G-module de $\mathrm{Hom}(V/W, V)$ et de plus, l'application

$$\begin{array}{rccc} \lambda : & M & \to & \mathbf{C} \\ & u & \to & \lambda(u) \end{array}$$

est un G-morphisme de M vers le G-module trivial. Ce G-morphisme est non nul, car W admet un supplémentaire dans V. Puisque $\lambda|_{M^G} \circ p_M = \lambda$, il en résulte qu'on peut trouver $u \in M^G$ tel que $\lambda(u) \neq 0$. En divisant u par $\lambda(u)$, on a bien un G-morphisme $u : V/W \to V$ tel que $u(v + W) \in v + W$ pour tout $v \in V$.

De ce théorème résulte une caractérisation des groupes linéairement réductifs, par l'existence d'un analogue algébrique de la mesure de Haar pour les groupes compacts.

Proposition. *Un groupe algébrique G est linéairement réductif si et seulement s'il existe un morphisme G-invariant $I : \mathbf{C}[G] \to \mathbf{C}$ tel que $I(1) = 1$ (ici G opère dans $\mathbf{C}[G]$ par multiplication à droite). De plus, I est unique, et invariant par l'opération de G par multiplication à gauche.*

Démonstration. Supposons G linéairement réductif. Soit $\mathbf{C}[G] = \oplus_{n \geq 0} M_n$ une décomposition en sous-modules simples avec $M_0 = \mathbf{C}$. Alors M_n est non trivial pour tout $n > 0$, donc $I(M_n) = 0$ dans ce cas. L'unicité de I en résulte.

Si $g \in G$ alors $\lambda(g)I$ vérifie les propriétés de I, car $\lambda(g)$ commute aux multiplications à droite. Par unicité de I, on a donc $\lambda(g)I = I$.

Réciproquement, l'existence de I implique la condition (iii) du théorème ci-dessus.

On montre de même que pour tout G-module rationnel V, la projection

$$p_V : V \to V^G$$

est unique. Cette projection est appelée *l'opérateur de Reynolds* associé à V.

Exemples. (i) Tout groupe fini est linéairement réductif. En effet, si G est d'ordre N, alors

$$\begin{array}{rccc} I : & \mathbf{C}[G] & \to & \mathbf{C}[G]^G = \mathbf{C} \\ & f & \to & \frac{1}{N} \sum_{g \in G} \rho(g) f \end{array}$$

est invariante par multiplication à droite et envoie 1 sur 1.

(ii) Soit $T \simeq (\mathbf{C}^*)^n$ un tore. Alors T est linéairement réductif ; en effet, d'après la proposition 1.5.1, tout T-module rationnel est somme directe de modules de dimension 1, donc simples. On peut retrouver ce résultat en définissant $I : \mathbf{C}[T] \to \mathbf{C}$ par $I(1) = 1$ et $I(\chi) = 0$ pour tout caractère multiplicatif non trivial χ ; alors I vérifie les hypothèses de la proposition.

(iii) Le produit de deux groupes linéairement réductifs est linéairement réductif (exercice).

(iv) Le groupe additif $G = \mathbf{C}$ n'est pas linéairement réductif. En effet, $\mathbf{C}^2$ est un G-module rationnel pour l'opération $t \cdot (x, y) = (x, y + tx)$. Tout vecteur propre commun à tous les éléments de G est multiple de (1,0), donc la droite $\mathbf{C} \times \{0\}$ est stable par G mais n'admet pas de supplémentaire stable par G.

(v) Plus généralement, si le radical unipotent $R_u(G)$ (défini en 1.4) est non trivial, alors G n'est pas linéairement réductif. En effet, soit V un G-module dans lequel $R_u(G)$ opère non trivialement, et soit W l'ensemble des invariants de $R_u(G)$ dans V. Alors W est un sous-G-module de V, distinct de V ; de plus, W est non trivial d'après le théorème 3. Si W admet un supplémentaire S stable par G, alors S contient un invariant non trivial de $R_u(G)$, ce qui contredit le fait que $W = V^{R_u(G)}$.

Définition. Un groupe algébrique affine G est *réductif* si son radical unipotent est trivial. Si de plus G est connexe et de centre fini, on dit que G est *semi-simple.*

On vient de voir que les groupes linéairement réductifs sont réductifs. La réciproque est vraie, voir [Hu] : on montre d'abord que tout groupe réductif connexe est le quotient par un sous-groupe fini central d'un produit $T \times S$ où T est un tore et S est semi-simple. Puis on utilise la correspondance entre les représentations d'un groupe de Lie et celles de son algèbre de Lie, ainsi que la complète réductibilité des représentations de dimension finie des algèbres de Lie semi-simples complexes.

Exemples (les groupes classiques). Les groupes SL_n et Sp_n sont semi-simples, ainsi que SO_n pour $n \geq 3$. Les groupes GL_n et O_2 sont réductifs mais non semi-simples ; enfin, SO_2 est un tore de dimension 1 (exercice).

2.2. *Une caractérisation des groupes linéairement réductifs*

On va obtenir un critère pour qu'un sous-groupe algébrique du groupe linéaire soit linéairement réductif, et on en déduira que les groupes classiques sont linéairement réductifs. On aura besoin du résultat préliminaire suivant.

Soit G un sous-groupe de $\mathrm{GL}(V)$ où V est un espace vectoriel de dimension finie. Alors chaque puissance tensorielle $V^{\otimes m}$ (où m est un entier positif) est un G-module rationnel ; il en est de même des puissances extérieures $\wedge^m V$. On pose

$$\det(V) := \wedge^{\dim(V)} V \ .$$

C'est un G-module de dimension 1, où chaque $g \in G$ opère par multiplication par $\det(g)$. On peut donc définir les puissances tensorielles $\det(V)^{\otimes n}$ pour tout entier relatif n. Si G est fermé dans $\mathrm{GL}(V)$, alors les G-modules $V^{\otimes m}$ et $\det(V)^{\otimes n}$ sont rationnels.

Lemme. *Soit G un sous-groupe fermé de $\mathrm{GL}(V)$. Alors tout G-module rationnel de dimension finie est isomorphe à un sous-module d'un quotient d'une somme directe de G-modules de la forme $V^{\otimes m} \otimes (\det(V)^{\otimes n}$.*

Démonstration. Soit M un G-module rationnel de dimension d ; choisissons une base $(e_1^*, \ldots, e_d^*)$ de M^*. Alors l'application linéaire

$$\begin{array}{ccc} M & \to & \mathbf{C}[G]^d \\ m & \to & (g \to e_i^*(g \cdot m))_{1 \leq i \leq d} \end{array}$$

est injective et équivariante pour l'opération de G dans M, et pour l'opération par multiplication à droite dans $\mathbf{C}[G]^d$. De plus, le G-module $\mathbf{C}[G]$ est quotient de

$$\mathbf{C}[\mathrm{GL}(V)] = \mathbf{C}[End(V)][1/\det(V)] = \sum_{n \in \mathbf{Z}} \mathbf{C}[End(V)] \otimes \det(V)^{\otimes n}$$

où $End(V)$ désigne l'espace des endomorphismes de V. L'opération de G dans $End(V)$ est donnée par la composition à droite.

Observons que l'application

$$\begin{array}{ccc} V^* \otimes V & \to & End(V) \\ l \otimes v & \to & (x \to l(x)v) \end{array}$$

est un G-isomorphisme, où G opère dans $V^* \otimes V$ via son action dans V^*. L'algèbre $\mathbf{C}[End(V)]$ est quotient de l'algèbre tensorielle du dual de $End(V)$, qu'on peut écrire d'après ce qui précède :

$$T(End(V)^*) = \bigoplus_{m=0}^{\infty} (V \otimes V^*)^{\otimes m} = \bigoplus_{m=0}^{\infty} V^{\otimes m} \otimes (V^*)^{\otimes m} .$$

De plus, G opère dans cette algèbre via son action dans les puissances tensorielles $V^{\otimes m}$, et l'action triviale dans $(V^*)^{\otimes m}$.

Théorème. *Soit G un sous-groupe fermé de* $\mathrm{GL}(V)$ *où V est un espace vectoriel de dimension finie.*

(i) G est linéairement réductif si et seulement si le G-module $V^{\otimes m}$ est semi-simple pour tout entier positif m.

(ii) S'il existe une structure hermitienne sur V telle que l'adjoint de tout élément de G est dans G, alors G est linéairement réductif.

Démonstration. (i) Si G est linéairement réductif, alors les puissances tensorielles de V sont semi-simples, comme tous les G-modules rationnels. Réciproquement, si toute puissance tensorielle de V est semi-simple, alors d'après le lemme, tout G-module M (rationnel, de dimension finie) est quotient d'un sous-module d'un module semi-simple. Par suite, M est semi-simple, et on conclut grâce au théorème 2.1.

(ii) Soit $(- \cdot -)$ le produit scalaire hermitien donné sur V. Soit $W \subseteq V$ un sous-espace stable par G ; soit $W^\perp$ son orthogonal. Si $g \in G$, $x \in W^\perp$ et $y \in W$, alors $(gx \cdot y) = (x \cdot g^* y) = 0$, donc $W^\perp$ est stable par G. Puisque $V = W \oplus W^\perp$, on en déduit que le G-module V est semi-simple.

Pour tout entier positif m, on définit une structure hermitienne sur $V^{\otimes m}$ par

$$(x_1 \otimes \cdots \otimes x_m \cdot y_1 \otimes \cdots \otimes y_m) := \prod_{i=1}^{m} (x_i \cdot y_i) .$$

Si $u_1, \ldots, u_m$ sont dans $\mathrm{GL}(V)$, alors $u_1 \otimes \cdots \otimes u_m$ est dans $GL(V^{\otimes m})$ et on a :

$$(u_1 \otimes \cdots \otimes u_m)^* = u_1^* \otimes \cdots \otimes u_m^* .$$

On en déduit que l'image de G dans $\mathrm{GL}(V^{\otimes m})$ est stable par passage à l'adjoint. D'après la première partie de la démonstration, le G-module $V^{\otimes m}$ est donc complètement réductible, et on conclut grâce à (i).

Corollaire 1. *Les groupes classiques* GL_n, SL_n, Sp_n, O_n *et* SO_n *sont linéairement réductifs.*

Démonstration. La condition (ii) du théorème est évidente pour $G = \mathrm{GL}_n$ ou SL_n et pour $V = \mathbf{C}^n$. Elle est vérifiée pour $G = \mathrm{O}_n$ ou SO_n (avec la forme quadratique standard sur $\mathbf{C}^n$) et pour $V = \mathbf{C}^n$ (avec sa structure hermitienne standard), car alors G est stable par transposition et conjugaison. Le cas du groupe symplectique est laissé en exercice.

Corollaire 2. *Soit G un groupe algébrique affine qui contient un sous-groupe K, compact et dense dans G pour la topologie de Zariski. Alors G est linéairement réductif.*

Démonstration. On considère G plongé dans un $\mathrm{GL}(V)$. Montrons d'abord que V possède une structure hermitienne invariante par K. Soit $\mathcal{H}$ l'ensemble des formes sesquilinéaires sur V ; c'est un G-module (non rationnel!) de dimension finie. Soit $\mathcal{H}_{>0} \subset \mathcal{H}$ le sous-ensemble des formes définies positives ; c'est un cône convexe ouvert et stable par G. Si $q \in \mathcal{H}_{>0}$, alors l'orbite $K \cdot q$ est compacte et contenue dans $\mathcal{H}_{>0}$. Le centre de gravité de cette orbite est donc un point fixe de K dans $\mathcal{H}_{>0}$, autrement dit, une structure hermitienne invariante par K.

Comme dans la démonstration du théorème, on en déduit que $V^{\otimes m}$ possède une structure hermitienne invariante par K, et donc que le K-module $V^{\otimes m}$ est semi-simple. Puisque K est dense dans G, il en résulte que tout K-sous-module de $V^{\otimes m}$ est stable par G, et donc que le G-module $V^{\otimes m}$ est semi-simple.

Le corollaire 2 se déduit aussi de l'existence de la mesure de Haar sur K, voir [Br-tD]. Cette mesure $d\mu$ est l'unique mesure sur K qui est invariante par multiplication, et de masse totale 1. Pour toute $f \in \mathbf{C}[G]$, posons

$$I(f) := \int_K ; f(g) d\mu(g) \ .$$

Ceci définit une application linéaire $I : \mathbf{C}[G] \to \mathbf{C}$ telle que $I(1) = 1$. De plus, I est invariante par multiplication par K, et donc par G.

D'autre part, on peut montrer que tout groupe réductif est le complexifié d'un groupe de Lie compact, voir [He] Chapter 6. En conclusion, les notions de groupe réductif, linéairement réductif, et de complexifié d'un groupe de Lie compact, sont les mêmes. Pour simplifier, on écrira par la suite "réductif" pour "linéairement réductif".

2.3. *Représentations des groupes réductifs*

Soit G un groupe algébrique réductif. On note $\hat{G}$ l'ensemble des classes d'isomorphisme des G-modules rationnels simples. Pour $\omega \in \hat{G}$, on note V_ω un représentant de ω. Enfin, pour tout G-module rationnel M, on note $M_{(\omega)}$ la somme des sous-modules simples de M qui sont isomorphes à V_ω. On appelle $M_{(\omega)}$ la *composante isotypique* de M de type ω.

Avec ces notations, on peut décrire la structure des G-modules rationnels, comme suit.

Proposition 1. *(i) Si G est un groupe réductif et M est un G-module rationnel, alors*

$$M = \bigoplus_{\omega \in \hat{G}} M_{(\omega)}$$

et de plus l'application

$$\begin{array}{ccc} \mathrm{Hom}^G(V_\omega, M) \otimes V_\omega & \to & M_{(\omega)} \\ f \otimes v & \mapsto & f(v) \end{array}$$

est un isomorphisme de G-modules, où G opère dans le produit tensoriel via son action dans V_ω.
(ii) Si de plus $M = \mathbf{C}[X]$ où X est une G-variété, alors $\mathrm{Hom}^G(V_\omega, M)$ s'identifie à l'ensemble $\mathrm{Mor}^G(X, V_\omega^*)$ des G-morphismes de X vers V_ω^*.
(iii) On a un isomorphisme de $G \times G$-modules

$$\begin{array}{ccc} \bigoplus_{\omega \in \hat{G}} V_\omega^* \otimes V_\omega & \to & \mathbf{C}[G] \\ \ell \otimes v & \mapsto & (g \mapsto \ell(g^{-1}v) \end{array}$$

où $G \times G$ opère dans $\mathbf{C}[G]$ par multiplication à gauche et à droite, et dans les produits tensoriels par

$$(g, h) \cdot (l \otimes v) = (g \cdot l) \otimes (h \cdot v) \ .$$

Démonstration. (i) On décompose M en somme directe de G-modules simples et on regroupe les termes isomorphes, pour obtenir la première assertion. Pour la seconde assertion, on peut supposer que M est simple, et on applique alors le lemme de Schur.

(ii) L'ensemble des G-morphismes de X vers V_ω est

$$(\mathbf{C}[X] \otimes V_\omega)^G = \mathrm{Hom}^G(V_\omega^*, \mathbf{C}[X]) \ .$$

(iii) On considère l'action de G dans lui-même par multiplication à droite. D'après (ii), on a un isomorphisme

$$\bigoplus_{\omega \in \hat{G}} \mathrm{Mor}^G(G, V_\omega^*) \otimes V_\omega \to \mathbf{C}[G] \ .$$

Cet isomorphisme est équivariant pour l'action de G à droite, et aussi pour l'action à gauche, en faisant opérer G dans $\mathrm{Mor}^G(G, V)$ par multiplication à gauche dans la source G. De plus, pour tout G-module rationnel V, on a un isomorphisme de G-modules

$$\mathrm{Mor}^G(G, V) \to V : f \mapsto f(e)$$

d'où le résultat.

Définitions. La *multiplicité* d'un G-module simple V_ω dans un G-module rationnel V est la dimension de l'espace vectoriel $\mathrm{Hom}^G(V_\omega, V)$. Cette multiplicité est notée $mult(\omega, V)$. On a donc :

$$V \simeq \bigoplus_{\omega \in \hat{G}} mult(\omega, V) V_\omega \ .$$

Pour une G-variété X et un G-module V, un G-morphisme de X vers V est appelé un *G-covariant de X à valeurs dans V*. Le produit d'un tel covariant par un invariant de $\mathbf{C}[X]$ est encore un covariant : l'ensemble $\mathrm{Mor}^G(X, V)$ des G-covariants de X à valeurs dans V est donc un $\mathbf{C}[X]^G$-module.

Exemple. Soit $G = \mathrm{SL}(V)$ opérant dans l'espace V^k des k-uplets de points de V. Pour $1 \leq i \leq k$, soit $p_i : V^k \to V$ la i-ième projection ; c'est un covariant à valeurs dans le G-module V. D'après la théorie classique des invariants (voir [Ho3]), l'espace des covariants $\mathrm{Mor}^G(V^k, V)$ est engendré par $p_1, \ldots, p_k$ comme module sur l'algèbre des invariants.

Plus généralement, on verra en 2.5 que les modules de covariants sont de type fini. D'autres exemples de covariants seront donnés dans la section suivante.

On va maintenant étendre aux groupes linéairement réductifs des résultats classiques sur les caractères des groupes finis (ou compacts).

Définitions. Soient G un groupe réductif et V un G-module rationnel de dimension finie. Le *caractère* de V est l'application

$$\chi_V : \begin{array}{ccc} G & \to & \mathbf{C} \\ g & \mapsto & \mathrm{Tr}_V(g) \end{array}$$

où $\mathrm{Tr}_V(u)$ désigne la trace de l'endomorphisme u de V.

Une fonction $f \in \mathbf{C}[G]$ est *centrale* si f est invariante par conjugaison. Les fonctions centrales forment une sous-algèbre de $\mathbf{C}[G]$, notée $C(G)$.

Pour V comme ci-dessus, il est clair que $\chi_V \in C(G)$. De plus, on a $\chi_{V \oplus V'} = \chi_V \oplus \chi_{V'}$ et $\chi_{V \otimes V'} = \chi_V \times \chi_{V'}$ quels que soient les G-modules V et V'. Enfin, χ_V ne dépend que de la classe d'isomorphisme de V. Pour $\omega \in \hat{G}$, on note χ_ω le caractère de V_ω.

On munit $\mathbf{C}[G]$ de l'involution $*$ définie par

$$f^*(g) := f(g^{-1})$$

ainsi que du produit scalaire $\langle , \rangle$ tel que

$$\langle u, v \rangle = I(uv^*)$$

(où I est définie en 2.1). Alors $\langle,\rangle$ est symétrique, car $I(f^*) = I(f)$ (par unicité de I).

Proposition 2. *(i) La décomposition*

$$\mathbf{C}[G] = \bigoplus_{\omega \in \hat{G}} V_\omega^* \otimes V_\omega$$

est orthogonale. De plus, la restriction de $\langle,\rangle$ à chaque $V_\omega^* \otimes V_\omega$ est non dégénérée.

(ii) Les caractères χ_ω ($\omega \in \hat{G}$) forment une base orthonormée de l'espace $C(G)$ des fonctions centrales.

(iii) Pour tout G-module V, et pour tout $\omega \in \hat{G}$, on a

$$mult(\omega, V) = \langle \chi_\omega, \chi_V \rangle \ .$$

(iv) Tout G-module rationnel de dimension finie est déterminé à isomorphisme près par son caractère.

Démonstration. (i) Soient V et V' deux G-modules simples non isomorphes. Alors $M := V^* \otimes V'$ est un G-module, et $M^G = \{0\}$ d'après le lemme de Schur. Pour tous $l \in V^*$ et $v' \in V'$, on a donc $p_M(l \otimes v') = 0$ où p_M désigne l'opérateur de Reynolds. On en déduit que pour tous $v \in V$ et $l' \in V'^*$, on a

$$I(f_{v',l'} f_{v,l}^*) = 0$$

(voir la preuve du théorème 2.1). Autrement dit, les sous-espaces $V'^* \otimes V'$ et $V^* \otimes V$ de $\mathbf{C}[G]$ sont orthogonaux.

De même, pour tout $u \in End(V) \simeq V^* \otimes V$, on a

$$p_{End(V)}(u) = \lambda(u) id_V$$

pour un $\lambda(u) \in \mathbf{C}$. En prenant la trace, on en déduit

$$\lambda(u) \dim(V) = \mathrm{Tr}_V p_{End(V)}(u) = \mathrm{Tr}_V(u)$$

(puisque la trace est invariante, elle commute avec l'opérateur de Reynolds). D'où

$$p_{End(V)}(u) = \frac{\mathrm{Tr}_V(u)}{\dim(V)} id_V \ .$$

On en déduit que pour tous $v, v' \in V$ et $l, l' \in V^*$, on a

$$\langle f_{v,l}, f_{v',l'} \rangle = I(f_{v,l} f_{v',l'}^*) = \frac{l'(v) l(v')}{\dim(V)} \ .$$

Il en résulte que la restriction de $\langle,\rangle$ à $V^* \otimes V$ est non dégénérée (vérifier).

(ii) Soit (e_i) une base de V_ω, et soit (e_i^*) la base duale. Alors $\chi_\omega = \sum_i f^*_{e_i,e_i^*}$. En particulier, χ_ω est dans $V_\omega^* \otimes V_\omega$ donc il est orthogonal à χ_π pour tout $\pi \neq \omega$. De plus,

$$\langle \chi_\omega, \chi_\omega \rangle = \sum_{i,j} I(f^*_{e_i,e_i^*} f_{e_j,e_j^*}) = \frac{1}{\dim(V)} \sum_i 1 = 1 \ .$$

Enfin, d'après le lemme de Schur, χ_ω engendre l'espace des invariants par conjugaison dans $V_\omega^* \otimes V_\omega$. Il résulte alors de (i) que les χ_ω forment une base de $C(G)$.

(iii) La formule est conséquence immédiate de (ii) et de la décomposition

$$V = \bigoplus_{\omega \in \hat{G}} mult(\omega, V) V_\omega \ .$$

(iv) résulte de (iii) et de la décomposition ci-dessus.

Remarque. Soit T un tore maximal de G, et soit N son normalisateur. L'action de N dans T par conjugaison se factorise en une action du groupe quotient $N/T = W$, le *groupe de Weyl*. De plus, la restriction à T des fonctions centrales définit un homomorphisme d'algèbres

$$Res : C(G) \to \mathbf{C}[T]^W \ .$$

On verra en 3.2 que Res est un isomorphisme lorsque G est connexe. Les images par Res des caractères irréductibles χ_ω sont donnés alors par la formule des caractères de Weyl (voir [Hu], où on trouvera aussi une description des modules simples).

2.4. *Le cas de* SL_2.

Dans cette section, on considère le groupe $G = \mathrm{SL}_2$ et ses sous-groupes

$$U = U_2 = \{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbf{C}\}, \ T = \{\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mid t \in \mathbf{C}^*\} \ .$$

Alors T est un tore maximal de G. Le normalisateur N de T est engendré par T et $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Le groupe de Weyl $W = N/T$ est d'ordre 2 ; il opère dans T par $g \mapsto g^{-1}$. On en déduit que l'algèbre $\mathbf{C}[T]^W$ est formée des polynômes symétriques en t et t^{-1}.

On commence par décrire les G-modules simples et leurs caractères.

Proposition 1. *(i) Le G-module V_d est simple, et tout G-module simple est isomorphe à V_d pour un unique d.*

(ii) La restriction à T induit un isomorphisme

$$Res : C(G) \to \mathbf{C}[T]^W$$

qui envoie le caractère de V_d sur

$$\chi_d = t^d + t^{d-2} + \cdots + t^{-d+2} + t^{-d} = \frac{t^{d+1} - t^{-d-1}}{t - t^{-1}} \ .$$

Démonstration. Montrons que le G-module V_d est simple. Soit M un sous-G-module non nul de V_d. D'après le théorème 1.4, le sous-groupe U a un point fixe $f \neq 0$ dans M. On a donc $f(x,y) = f(x+ty,y)$ pour tout $t \in \mathbf{C}$. Il en résulte que f est un multiple non nul de y^d. Ainsi, M contient toutes les puissances des formes linéaires, donc $M = V_d$.

L'espace vectoriel V_d a pour base les $x^i y^{d-i}$ $(0 \leq i \leq d)$ qui sont vecteurs propres de T de poids t^{d-2i}. On en déduit que la valeur du caractère de V_d en $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ est donnée par les formules ci-dessus. Puisque tout polynôme symétrique en t et t^{-1} est combinaison linéaire des χ_d, l'application Res est surjective. D'autre part, la réunion des conjugués de T est dense dans G, donc Res est injective.

Ainsi, Res est un isomorphisme ; par suite, l'espace vectoriel $C(G)$ est engendré par les caractères irréductibles des V_d. Grâce à la proposition 2.3.2, il en résulte que tout G-module simple est isomorphe à un unique V_d.

Étudions maintenant les modules de covariants. Soit X une G-variété. Un élément de $\mathrm{Mor}^G(X, V_d)$ est appelé un *covariant d'ordre d*. La somme directe

$$\mathcal{C}(X) := \bigoplus_{d=0}^{\infty} \mathrm{Mor}^G(X, V_d)$$

est un $\mathbf{C}[X]^G$-module gradué par l'ordre, qu'on appelle *l'algèbre des covariants de X*. Cette terminologie est justifiée par l'énoncé suivant.

Proposition 2. *On a des isomorphismes*

$$\mathcal{C}(X) \simeq \mathbf{C}[X \times \mathbf{C}^2]^G \simeq \mathbf{C}[X]^U \ .$$

Démonstration. On a

$$\mathcal{C}(X) = (\mathbf{C}[X] \otimes \bigoplus_{n=0}^{\infty} V_n)^G = (\mathbf{C}[X] \otimes \mathbf{C}[x,y])^G$$

d'où le premier isomorphisme. Pour le second, on considère plus généralement un G-module M. Alors

$$(M \otimes \mathbf{C}[x,y])^G \simeq \mathrm{Mor}^G(\mathbf{C}^2, M) .$$

Observons que la restriction

$$\mathrm{Mor}^G(\mathbf{C}^2, M) \to \mathrm{Mor}^G(\mathbf{C}^2 \setminus \{0\}, M)$$

est un isomorphisme ; en effet, toute fonction régulière sur $\mathbf{C}^2 \setminus \{0\}$ s'étend en une fonction polynomiale sur $\mathbf{C}^2$ (exercice). Soit e le premier vecteur de base de $\mathbf{C}^2$, alors $U = G_e$ et l'orbite $G \cdot e$ est égale à $\mathbf{C}^2 \setminus \{0\}$. On en déduit que l'application

$$\begin{array}{ccc} \mathrm{Mor}^G(\mathbf{C}^2 \setminus \{0\}, M) & \to & M^U \\ \varphi & \mapsto & \varphi(e) \end{array}$$

est un isomorphisme, ce qui termine la démonstration.

En particulier, l'algèbre des covariants $\mathcal{C}(X)$ contient l'algèbre des invariants $\mathbf{C}[X]^G$. Un intérêt de la construction de $\mathcal{C}(X)$ est que cette algèbre est munie d'opérations ("transvections") qui permettent de construire beaucoup de covariants ; en voici une définition.

Soient d, e, n des entiers tels que $0 \le n \le \min(d,e)$. Pour $f \in V_d$ et $g \in V_e$, on pose

$$(f,g)_n := \frac{(d-n)!}{d!}\frac{(e-n)!}{e!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}\frac{\partial^n f}{\partial x^{n-i}\partial y^i}\frac{\partial^n g}{\partial x^i \partial y^{n-i}} .$$

En particulier, $(f,g)_0 = fg$ et $de(f,g)_1$ est le déterminant jacobien de f et g. L'élément $(f,g)_n$ de V_{d+e-2n} s'appelle le *n-ième transvectant* de f et de g.

Proposition 3. *L'application $(f,g) \mapsto (f,g)_n$ définit une application linéaire et G-équivariante de $V_d \otimes V_e$ sur V_{d+e-2n}. De plus, l'application*

$$\begin{array}{cccc} \tau : & V_d \otimes V_e & \to & \bigoplus_{n=0}^{\min(d,e)} V_{d+e-2n} \\ & f \otimes g & \mapsto & \sum_{n=0}^{\min(d,e)} (f,g)_n \end{array}$$

est un isomorphisme de G-modules ("formule de Clebsch-Gordan").

Démonstration. L'application $(f,g) \mapsto (f,g)_n$ est clairement bilinéaire. Si $f = u^d$ et $g = v^e$ où u et v sont des formes linéaires, alors on a

$$(f,g)_n = u^{d-n}v^{e-n}(\det(u,v))^n$$

(vérifier). Il en résulte que τ est G-équivariante, car les puissances des formes linéaires engendrent V_d et V_e. De plus, $(,)_n$ est non nulle et les V_{d+e-2n} sont deux à deux non isomorphes, donc τ est surjective. Pour des raisons de dimensions, c'est un isomorphisme.

Si maintenant u et v sont deux covariants sur X, d'ordres respectifs d et e, on peut définir des covariants $(u,v)_n$ d'ordre $d+e-2n$ pour $0 \leq n \leq \min(d,e)$. En particulier, lorsque $X = V_d$, on a un covariant évident, d'ordre d : l'application identique de V_d, notée f. De plus, il résulte de la formule de Clebsch-Gordan que l'espace vectoriel $\mathcal{C}(V_d)$ est engendré par les transvectants itérés

$$f,\ (f,f)_n,\ (f,(f,f)_n))_p,\ \ldots$$

D'après un théorème dû à Gordan (voir [Go] et aussi [Gr-Yo]), l'algèbre $\mathcal{C}(V_d)$ est engendrée par un nombre fini de ces transvectants itérés. La preuve de Gordan est constructive ; on verra en 2.5 un théorème de finitude beaucoup plus général, mais non effectif.

On donne ci-dessous les résultats de l'algorithme de Gordan pour les premières valeurs de d ; ces résultats seront retrouvés dans l'exemple 3 en 3.2, et aussi en 4.5. On observe que l'algèbre $\mathcal{C}(V_d)$ a une double graduation, par le degré et par l'ordre, et que les transvectants itérés de f sont bi-homogènes. De plus, l'isomorphisme

$$\mathcal{C}(V_d) \simeq \mathbf{C}[V_d][x,y]^G \simeq \mathbf{C}[V_d]^U$$

envoie chaque $g(x,y)$ sur $g(1,0)$ (voir la preuve de la proposition 2). L'algèbre des invariants $\mathcal{I}(V_d)$ s'identifie à la sous-algèbre de $\mathcal{C}(V_d)$ formée des covariants d'ordre 0.

Exemples. Si $d=1$, on a $(f,f)_n = 0$ pour $n \neq 0$. L'algèbre $\mathcal{C}(V_1)$ est engendrée par f, et l'algèbre $\mathcal{I}(V_1)$ est réduite aux constantes.

Si $d=2$, l'algèbre $\mathcal{C}(V_2)$ est engendrée par f et $(f,f)_2$; ce dernier engendre l'algèbre $\mathcal{I}(V_2)$. Si $f(x,y) = a_0x^2 + 2a_1xy + a_2y^2$ alors $(f,f)_2 = a_0a_2 - a_1^2$.

Si $d=3$, l'algèbre $\mathcal{C}(V_3)$ est engendrée par les quatre covariants

$$f,\ H := (f,f)_2, T :=\ (f,H)_1,\ \Delta := (H,H)_2$$

de degrés et ordres respectifs : $(1,3)$, $(2,2)$, $(3,3)$, $(4,0)$. En écrivant

$$f(x,y) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$$

on obtient, à des facteurs numériques près :

$$H = (a_0a_2 - a_1^2)x^2 + (a_0a_3 - a_1a_2)xy + (a_1a_3 - a_2^2)y^2,$$

$$\begin{aligned} T = {} & (a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3)x^3 + 3(a_0a_1a_3 - 2a_0a_2^2 + a_1^2a_2)x^2y \\ & -3(a_0a_2a_3 - 2a_1^2a_3 + a_1a_2^2)xy^2 - (a_0a_3^2 - 3a_1a_2a_3 + 2a_2^3)y^3, \end{aligned}$$

$$\Delta = (a_0a_3 - a_1a_2)^2 - 4(a_0a_2 - a_1^2)(a_1a_3 - a_2^2) \ .$$

Par l'isomorphisme $\mathcal{C}(V_3) \simeq \mathbf{C}[V_3]^U$, ces covariants sont envoyés sur a_0, b_2, b_3, Δ avec les notations de l'exemple en 1.4. En particulier, Δ est le discriminant de f ; il engendre l'algèbre $\mathcal{I}(V_3)$. De plus, on a une relation

$$T^2 + 4H^3 - f^2\Delta = 0$$

qui engendre l'idéal des relations entre les générateurs f, H, T et Δ.

Si $d = 4$, l'algèbre $\mathcal{C}(V_4)$ a pour générateurs les cinq covariants

$$f, \ H := (f,f)_2, \ I := (f,f)_4, T := \ (f,H)_1, J := \ (f,H)_4$$

de degrés et ordres respectifs $(1,4)$, $(2,4)$, $(2,0)$, $(3,6)$, $(3,0)$; de plus, l'idéal des relations est engendré par une combinaison linéaire de T^2, H^3, IHf^2 et Jf^3 . Il en résulte que I et J sont algébriquement indépendants et engendrent l'algèbre $\mathcal{I}(V_4)$. En écrivant

$$f(x,y) = a_0x^4 + 4a_1x^3y + 6a_2x^2y^2 + 4a_3xy^3 + a_4y^4$$

on trouve, à des facteurs numériques près :

$$I = a_0a_4 - 4a_1a_3 + 3a_2^2 \ , \ J = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix} \ .$$

La situation se complique très vite pour les degrés supérieurs : il faut 23 éléments pour engendrer $\mathcal{C}(V_5)$, et 26 pour $\mathcal{C}(V_6)$; les relations entre ces générateurs ne sont que très partiellement connues. Pour $d \geq 7$, le nombre minimal de générateurs de $\mathcal{C}(V_d)$ est inconnu.

Cependant, il est facile de décrire l'algèbre $\mathcal{C}(V_d)[f^{-1}]$ pour tout d. En effet, soient $g_2, \ldots, g_d$ les covariants définis inductivement par $g_2 = (f,f)_2$ et $g_i = (f, g_{i-1})_2$. Alors chaque g_i est de degré i et d'ordre $i(d-2)$. De plus, chaque $g_i(1,0)$ est un multiple non nul du polynôme b_i construit dans l'exemple 1.4 (vérifier). On en déduit que l'algèbre $\mathcal{C}(V_d)[f^{-1}]$ est engendrée sur $\mathbf{C}[f, f^{-1}]$ par $g_2, \ldots, g_d$, et que ceux-ci sont algébriquement indépendants.

2.5. *Invariants et covariants des groupes réductifs : propriétés de finitude.*

On revient au cas d'un groupe réductif arbitraire, pour établir le résultat fondamental suivant, dû à Hilbert et Nagata.

Théorème *Soient G un groupe réductif et R une algèbre de type fini dans laquelle G opère par automorphismes, et qui est un G-module rationnel. Alors l'algèbre des invariants $A := R^G$ est de type fini, et c'est un facteur direct du A-module R. De plus, pour tout idéal I de A, on a : $IR \cap A = I$.*

Démonstration. Soit $p : R \to A$ l'opérateur de Reynolds défini en 2.1. Soit $f \in A$, alors l'idéal fR engendré par f est stable par G, et on a $(fR)^G = fA$. D'après le théorème 2.1, la restriction de p à fR est la projection pour ce G-module. D'autre part, l'application $\varphi \to f\varphi$ est G-équivariante et envoie R sur fR, donc l'opérateur de Reynolds pour fR est donnée par $\varphi \to fp(\varphi)$. On en déduit que $p(f\varphi) = fp(\varphi)$ pour tout $\varphi \in R$. Autrement dit, l'opérateur de Reynolds $p : R \to A$ est un morphisme de A-modules. Par suite, A est facteur direct du A-module R.

Soit I un idéal de A. Montrons que $IR \cap A = I$. Il est clair que I est contenu dans $IR \cap A$. Réciproquement, si $f \in IR \cap A$, on peut écrire $f = \sum_{i=1}^n f_i\varphi_i$ avec $f_i \in I$ et $\varphi_i \in R$. Puisque $f \in A$, on a

$$f = p(f) = \sum_{i=1}^n f_i p(\varphi_i)$$

d'où $f \in I$.

Puisque l'algèbre R est noethérienne, il en résulte aussitôt que A est noethérienne. Il est moins facile de montrer que A est de type fini ; on va se ramener au cas où R est une algèbre graduée, comme suit.

On choisit des générateurs $x_1, \ldots, x_n$ de l'algèbre R ; on choisit ensuite un sous-G-module rationnel W de R qui contient $x_1, \ldots, x_n$, et on note V le dual de W. Alors l'application $V^* = W \to R$ s'étend en un homomorphisme d'algèbres $\mathbf{C}[V] \to R$ qui est surjectif et G-équivariant. Il induit donc un homomorphisme surjectif d'algèbres $\mathbf{C}[V]^G \to A$. Ainsi, il suffit de démontrer que l'algèbre $\mathbf{C}[V]^G$ est de type fini. On utilisera la graduation

$$\mathbf{C}[V] = \bigoplus_{n=0}^{\infty} \mathbf{C}[V]_n$$

où $\mathbf{C}[V]_n$ désigne l'espace vectoriel des fonctions polynomiales de degré n sur V. Cette graduation est stable par G, d'où

$$\mathbf{C}[V]^G = \bigoplus_{n=0}^{\infty} \mathbf{C}[V]_n^G \ .$$

Notons I l'idéal de $\mathbf{C}[V]$ engendré par les invariants homogènes et non constants. Puisque l'anneau $\mathbf{C}[V]$ est noethérien, on peut engendrer I par des invariants $f_1, \ldots, f_r$ en nombre fini ; de plus, on peut supposer que les f_i sont homogènes. Si $f \in \mathbf{C}[V]^G$ est homogène et non constante, alors $f = \sum_{i=1}^r f_i\varphi_i$ avec des $\varphi_i \in \mathbf{C}[V]$ homogènes. On en déduit que $f = p(f) = \sum_{i=1}^r f_i p(\varphi_i)$ avec des $p(\varphi_i) \in \mathbf{C}[V]^G$ homogènes tels que $\deg p(\varphi_i) < \deg \varphi_i$. Par récurrence sur le degré de f, on conclut que f est un polynôme en $f_1, \ldots, f_r$. L'algèbre $\mathbf{C}[V]^G$ est donc engendrée par $f_1, \ldots, f_r$.

Proposition. *Soit R une algèbre qui vérifie les hypothèses du théorème ; soit M un G-module rationnel de dimension finie. Alors l'espace* $\mathrm{Hom}^G(M,R)$ *est un module de type fini sur $R^G = A$.*

Démonstration. Dans le R-module $\mathrm{Hom}(M,R) = R \otimes M^*$, le sous-espace des invariants $\mathrm{Hom}^G(M,R)$ est stable par multiplication par les éléments de A, c'est donc un A-module. Pour la finitude, on se ramène comme au théorème précédent, au cas où $R = \mathbf{C}[V]$ avec V un G-module rationnel de dimension finie. On considère alors l'algèbre

$$\mathbf{C}[V \times M] = R \otimes \mathbf{C}[M]$$

graduée par le degré partiel par rapport à M. Alors $\mathbf{C}[V \times M]_1 = R \otimes M^*$. Si $\mathcal{M} \subseteq \mathrm{Hom}^G(M,R)$ est un sous-A-module, alors

$$I(\mathcal{M}) = \mathcal{M} \oplus \bigoplus_{n \geq 2} (R \otimes \mathbf{C}[M]_n)^G$$

est un idéal de $(R \otimes \mathbf{C}[M])^G$, car il est stable par multiplication par tout élément homogène de cette algèbre. De plus, $\mathcal{M}$ est l'ensemble des éléments homogènes de degré 1 dans $I(\mathcal{M})$. Puisque l'application $\mathcal{M} \to I(\mathcal{M})$ est croissante et que l'algèbre $(R \otimes \mathbf{C}[M])^G$ est noethérienne, le A-module $\mathrm{Hom}^G(M,R)$ est noethérien, donc de type fini.

Corollaire 1. *Soit R une algèbre qui vérifie les hypothèses du théorème. Alors on a un isomorphisme*

$$R \simeq \bigoplus_{\omega \in \hat{G}} \mathrm{Hom}^G(V_\omega, R) \otimes V_\omega$$

compatible avec les structures de G-module et de A-module. De plus, chaque A-module $\mathrm{Hom}^G(V_\omega, R)$ *est de type fini.*

En particulier, pour toute G-variété affine X, l'algèbre des invariants $\mathbf{C}[X]^G$ est de type fini, et tout module de covariants $\mathrm{Mor}^G(X, V_\omega)$ est de type fini.

Le théorème de Hilbert et Nagata permet aussi de démontrer le résultat de finitude suivant, dû à Weitzenböck.

Corollaire 2. *Soit V un module (rationnel et de dimension finie) pour le groupe additif $U = \mathbf{C}$. Alors l'algèbre $\mathbf{C}[V]^U$ est de type fini.*

Démonstration. On identifie V à $\mathbf{C}^n$, d'où une application polynomiale $\rho : \mathbf{C} \to \mathrm{GL}_n$ telle que $\rho(x+y) = \rho(x)\rho(y)$ pour tous x et y dans $\mathbf{C}$. On en déduit que $d\rho(x) = \rho(x)d\rho(0)$ où $d\rho(x)$ désigne la diférentielle de ρ à l'origine. On a donc : $\rho(x) = \exp(xA)$ avec $A = d\rho(0)$. Puisque ρ est polynomiale, la matrice A est nilpotente. En la ramenant à sa forme de Jordan, on obtient une décomposition

$$V = \bigoplus_{d\geq 0} ; V_{(d)}^{m_d}$$

où chaque $V_{(d)}$ est muni d'une base $(e_0, e_1, \ldots, e_d)$ telle que $Ae_0 = 0$ et que $Ae_i = e_{i-1}$ pour $1 \leq i \leq d$. En envoyant chaque e_i sur $x^{d-i}y^i/i!$, on définit un isomorphisme de $V_{(d)}$ sur V_d qui est U-équivariant. On en déduit que l'action de U dans V se prolonge en une action de SL_2 et on conclut grâce au théorème ci-dessus, combiné avec l'isomorphisme obtenu en 2.4.2 :

$$\mathbf{C}[V]^U \simeq \mathbf{C}[V \times \mathbf{C}^2]^{\mathrm{SL}_2} \ .$$

3. Quotients par les groupes réductifs

3.1. *Le quotient d'une variété affine par un groupe réductif*

Soit G un groupe algébrique réductif opérant dans une variété algébrique affine X. D'après le théorème 2.5, la sous-algèbre $\mathbf{C}[X]^G \subseteq \mathbf{C}[X]$ est de type fini. De plus, $\mathbf{C}[X]^G$ ne contient pas d'élément nilpotent non nul ; c'est donc l'algèbre des fonctions régulières sur une variété algébrique affine $X//G$, munie d'un morphisme

$$\pi : X \to X//G$$

appelé *quotient de X par G.*

Il est clair que π est invariante par G, et universelle pour cette propriété : si $p : X \to Y$ est un morphisme G-invariant vers une variété affine, alors il existe un unique morphisme $q : X//G \to Y$ tel que $p = q \circ \pi$. On va établir d'autres propriétés de π qui justifient son nom de "quotient".

Théorème. *Soit G un groupe réductif opérant dans une variété affine X.*

(i) Le morphisme $\pi : X \to X//G$ est surjectif.

(ii) Si $Z \subseteq X$ est un fermé stable par G, alors $\pi(Z)$ est fermé dans $X//G$, et la restriction $\pi|_Z : Z \to \pi(Z)$ est le quotient de Z par G. Si de plus $Z' \subseteq X$ est fermé et stable par G, alors $\pi(Z \cap Z') = \pi(Z) \cap \pi(Z')$.

(iii) Si $x \in X$, alors la fibre $\pi^{-1}(\pi(x))$ contient une unique orbite fermée ; notons-la $\mathcal{O}_x$. De plus, $\pi^{-1}(\pi(x))$ est l'ensemble des $p \in X$ tels que $\overline{G \cdot p}$ contient $\mathcal{O}_x$.

Démonstration. (i) Soit p un point de $X//G$, et soit $I_p \subset \mathbf{C}[X]^G$ l'idéal maximal correspondant. D'après le théorème 2.5, on a : $I_p\mathbf{C}[X] \cap \mathbf{C}[X]^G = I_p$. En particulier, $I_p\mathbf{C}[X]$ est strictement contenu dans $\mathbf{C}[X]$. Il existe donc un idéal maximal I_x de $\mathbf{C}[X]$ qui contient $I_p\mathbf{C}[X]$; alors $\pi(x) = p$.

(ii) L'application $\mathbf{C}[X]^G \to \mathbf{C}[Z]^G$ est surjective, puisque $\mathbf{C}[X] \to \mathbf{C}[Z]$ est surjective. Cela entraîne que la restriction $\pi|_Z$ est le quotient de Z par G, et que $\pi(Z) = Z//G$ est fermée dans $X//G$. De plus, on a $I_{\pi(Z)} = I_Z^G$ en notant I_Z (resp. $I_{\pi(Z)}$) l'idéal de Z dans $\mathbf{C}[X]$ (resp. de $\pi(Z)$ dans $X//G$). D'où

$$I_{\pi(Z\cap Z')} = I_{Z\cap Z'}^G = (I_Z + I_{Z'})^G = I_Z^G + I_{Z'}^G = I_{\pi(Z)} + I_{\pi(Z')} = I_{\pi(Z)\cap\pi(Z')}$$

où la seule égalité non évidente est $(I_Z + I_{Z'})^G = I_Z^G + I_{Z'}^G$ qui résulte par exemple du théorème 2.1.

(iii) Puisque $\pi^{-1}(\pi(x))$ est fermé et stable par G, il contient une orbite fermée $\mathcal{O}_x$. Si $\mathcal{O}$ est une autre orbite fermée dans $\pi^{-1}(\pi(x))$, alors $\mathcal{O} \cap \mathcal{O}_x$ est vide, donc $\pi(\mathcal{O})$ ne rencontre pas $\pi(\mathcal{O}_x)$ d'après (ii), ce qui est absurde. Ainsi, $\mathcal{O}_x$ est unique.

Soit $p \in \pi^{-1}(\pi(x))$, alors $\overline{G \cdot p}$ contient une orbite fermée, qui doit être égale à $\mathcal{O}_x$. Réciproquement, si $\overline{G \cdot p}$ contient $\mathcal{O}_x$, alors $\pi(p) = \pi(x)$ car π est constante sur les adhérences des orbites.

D'après le théorème, on peut voir le quotient $X//G$ comme l'espace des orbites fermées de G dans X. Ce quotient peut être réduit à un point (par exemple, lorsque $G = \mathbf{C}^*$ opère dans $\mathbf{C}^n$ par multiplication). Dans le cas où X est un G-module, on va donner un critère pour que les fibres générales du quotient contiennent une orbite dense.

Proposition 1. *Pour un groupe réductif G opérant dans une variété affine irréductible X, les conditions suivantes sont équivalentes :*

(i) Il existe un ouvert non vide de $X//G$ tel que toute fibre de $\pi : X \to X//G$ au-dessus de cet ouvert contient une orbite dense.

(ii) Le corps des fractions de l'algèbre $\mathbf{C}[X]^G$ est $\mathbf{C}(X)^G$.

Si de plus X est un G-module et si tout caractère multiplicatif de G est d'ordre fini, alors ces conditions sont vérifiées.

Démonstration. D'après le théorème 1.6, il existe un ouvert invariant non vide $X_0 \subseteq X$ tel que le quotient géométrique $p : X_0 \to X_0/G$ existe. De plus, $\mathbf{C}(X_0/G) = \mathbf{C}(X)^G$. L'image $\pi(X_0) \subseteq X//G$ contient un ouvert de $X//G$. Il existe donc $f \in \mathbf{C}[X]^G$ non nul tel que $\pi(X_0 \cap X_f) = X_f//G$ (on note X_f le complémentaire dans X de l'ensemble des zéros de f). D'après la propriété universelle du quotient, on peut supposer de plus que la restriction de p à $X_0 \cap X_f$ se factorise par $q : X_f//G \to (X_0 \cap X_f)/G$. La condition (i) équivaut alors au fait que q est birationnelle, c'est-à-dire que le corps des fractions de $\mathbf{C}[X_f//G]$ est égal à $\mathbf{C}(X_0 \cap X_f)^G = \mathbf{C}(X)^G$. Mais l'algèbre $\mathbf{C}[X_f//G] = \mathbf{C}[X]^G[1/f]$ a le même corps des fractions que l'algèbre $\mathbf{C}[X]^G$.

Supposons maintenant que X est un G-module et que tout caractère multiplicatif de G est d'ordre fini ; montrons que (ii) est vérifiée. Soit $f \in \mathbf{C}(V)^G$. Ecrivons $f = u/v$ avec u, v dans $\mathbf{C}[V]$ premiers entre eux. Alors on a $f = (g \cdot u)/(g \cdot v)$ pour tout $g \in G$. Il en résulte que $g \cdot u$ est divisible par u. Les fonctions polynomiales u et $g \cdot u$ ayant le même degré, il existe $\chi(g) \in \mathbf{C}^*$ tel que $g \cdot u = \chi(g)u$. On voit facilement que χ est un caractère multiplicatif de G, et que $g \cdot v = \chi(g)v$. Par hypothèse, il existe un entier $n > 0$ tel que $\chi^n = 1$. Alors uv^{n-1} et v^n sont invariantes par G, et de plus $f = (uv^{n-1})/v^n$ est dans le corps des fractions de $\mathbf{C}[V]^G$.

Corollaire. *Sous les hypothèses de la proposition, on a :*

$$\dim(V//G) = \dim(V) - \max_{v \in V} \dim(G \cdot v) \ .$$

Enfin, on va montrer que les groupes d'isotropie des orbites fermées sont réductifs, comme conséquence du résultat suivant, dû à Matsushima (voir [Mat]).

Proposition 2. *Pour un groupe réductif G et un sous-groupe fermé $H \subseteq G$, les conditions suivantes sont équivalentes :*

(i) Le groupe H est réductif.

(ii) La variété G/H est affine.

Démonstration. (i)$\Rightarrow$(ii) Pour l'action de H dans G par multiplication à gauche, toutes les orbites sont fermées. L'assertion résulte donc du théorème.

(ii)$\Rightarrow$(i) D'après la proposition 1.2.1, il existe un G-module V et un $v \in V$ tels que $G \cdot v$ est fermée dans V et que $G_v = H$. Si H n'est pas réductif, alors son radical unipotent $R_u(G)$ contient un sous-groupe U isomorphe à $\mathbf{C}$. Il résulte alors du théorème de Jacobson-Morozov (voir [Bo] VIII.11.2 Proposition 3) qu'il existe un sous-groupe $S \subseteq G$ qui contient U et qui est isomorphe à SL_2 ou à PSL_2. Par suite, S contient un tore T isomorphe à $\mathbf{C}^*$ et qui normalise U.

Puisque v est fixé par U, on peut écrire

$$v = \sum_{d \in \mathbf{Z}} ; v_d$$

avec $v_d \in V^U$ et $t \cdot v_d = t^d v_d$ pour tout $t \in T$. De la description des représentations de SL_2 (voir 2.4), on déduit que $v_d = 0$ pour tout $d < 0$, et que v_0 est fixé par S. Par suite, $v_0 = \lim_{t \to 0} t \cdot v$ est dans $\overline{G \cdot v}$. Puisque l'orbite $G \cdot v$ est fermée, elle contient v_0. D'autre part, G_{v_0} contient S, donc $S \cap R_u(G_{v_0}) = \{e\}$. Par suite, l'ensemble

$$\{g \in G ; | ; S \cap g R_u(G_{v_0}) g^{-1} = \{e\}\}$$

est un voisinage de e dans G. Ainsi, l'ensemble des $g \cdot v_0$ tels que $S \cap R_u(G_{g \cdot v_0})$ est trivial, est un voisinage de v_0 dans son orbite par G. Puisque $v_0 \in \overline{T \cdot v}$, il existe $t \in T$ tel que $S \cap R_u(G_{t \cdot v})$ est trivial. Mais $R_u(G_{tv}) = tR_u(G)t^{-1}$ contient $tUt^{-1} = U$, contradiction.

Exemple 1 (les formes binaires). Soit $G = \mathrm{SL}_2$ opérant dans $V = V_d$. Alors tout caractère multiplicatif de G est trivial. De plus, le groupe d'isotropie d'un $f \in V_d$ ayant toutes ses racines distinctes est fini si $d \geq 3$, et de dimension 1 si $d = 2$. On en déduit que

$$\dim(V//G) = \begin{cases} 0 & \text{si } d \leq 1 \\ 1 & \text{si } d = 2 \\ d-2 & \text{si } d \geq 3. \end{cases}$$

Les fibres du quotient seront décrites en 3.3 ci-dessous.

Exemple 2 (l'action adjointe). Soit G un groupe réductif connexe. On fait opérer G dans lui-même par conjugaison ; alors le groupe d'isotropie de tout $g \in G$ est le centralisateur de g dans G. On va décrire les orbites fermées, ainsi que les fibres du quotient.

Pour $g \in G$, notons $g = g_s g_u$ sa décomposition de Jordan (c'est-à-dire : g_s est semi-simple, g_u est unipotent, et $g_s g_u = g_u g_s$; une telle décomposition existe et est unique, voir par exemple [Ste1]). On va montrer que $G \cdot g_s$ est l'unique orbite fermée de G dans $\overline{G \cdot g}$.

Il en résultera que l'orbite $G \cdot g$ est fermée si et seulement si g est semi-simple. En outre, pour tous g et h dans G, on a : $\pi(g) = \pi(h)$ si et seulement si $G \cdot g_s = G \cdot h_s$. En particulier, si g est semi-simple régulier (c'est-à-dire si le centralisateur de g est un tore maximal de G), alors $\pi^{-1}(\pi(g)) = G \cdot g$.

En effet, soit H le centralisateur de g_s dans G. Il existe un tore maximal de G qui contient g_s, et un tel tore est contenu dans H. D'après le lemme ci-dessous, l'orbite $G \cdot g_s$ est fermée dans G. Pour montrer que $g_s \in \overline{G \cdot g}$, on observe d'abord que H est réductif et contient g_u. Comme dans la preuve de la proposition 2 ci-dessus, on utilise ensuite le théorème de Jacobson-Morozov : il existe un sous-groupe S de H qui contient g_u et qui est isomorphe à SL_2 ou à PSL_2. Il en résulte qu'il existe un sous-groupe à un paramètre λ de S tel que $\lim_{t \to 0} \lambda(t) g_u \lambda(t)^{-1} = e$ (en effet, si g_u est représenté par $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on peut prendre pour $\lambda(t)$ l'image de $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$). Alors $\lim_{t \to 0} \lambda(t) g \lambda(t)^{-1} = g_s$ d'où l'assertion.

En fait, dans tout groupe réductif H, l'ensemble des éléments unipotents contient une orbite dense pour l'action par conjugaison, voir [Ste1] 3.6 Theorem 3. On en déduit que toute fibre du quotient $\pi : G \to G//G$ contient une orbite dense. On a des résultats analogues pour l'action adjointe de G dans son algèbre de Lie.

Lemme. *Soit G un groupe algébrique affine opérant dans une variété affine X, et soit $x \in X$ un point fixé par un tore maximal de G. Alors l'orbite $G \cdot x$ est fermée dans X.*

Démonstration. Soit T un tore maximal de G qui fixe x, et soit $U \subset G$ un sous-groupe unipotent normalisé par T et maximal pour cette propriété. Posons $B = UT$; c'est un sous-groupe résoluble connexe de G, qui est maximal pour ces propriétés d'après [Ste1] 2.12 Theorem 1. De plus, l'orbite $B \cdot x = U \cdot x$ est fermée dans X d'après le corollaire 1.4. Il en résulte que le sous-ensemble

$$\{(g, y) \mid g^{-1} \cdot y \in B \cdot x\}$$

de $G \times X$ est fermé. Ce sous-ensemble est stable par l'action de B dans $G \times X$ via $b \cdot (g, y) = (gb^{-1}, y)$, donc le sous-ensemble

$$\{gB, y) \mid g^{-1} \cdot y \in B \cdot x\}$$

de $G/B \times X$ est fermé. De plus, l'image de ce sous-ensemble par la projection $G/B \times X \to X$ est l'orbite $G \cdot x$, qui est donc fermée car la variété G/B est complète (voir [Ste1] 2.12 Theorem 1).

3.2. *Un critère pour le quotient*

Comme précédemment, on considère un groupe algébrique réductif G et une G-variété affine X. On va donner une caractérisation du quotient $\pi : X \to X//G$ parmi les morphismes G-invariants $p : X \to Y$. Pour cela, on rappelle quelques notions de géométrie algébrique.

Définitions. Une variété affine irréductible X est *normale* si l'algèbre $\mathbf{C}[X]$ est intégralement close dans son corps des fractions $\mathbf{C}(X)$. Par exemple, si l'algèbre $\mathbf{C}[X]$ est factorielle, alors X est normale (exercice) ; en particulier, l'espace affine est normal.

Un *diviseur irréductible* d'une variété X est une sous-variété $D \subset X$ qui est irréductible et de codimension un. On note $\mathcal{O}_{X,D}$ l'ensemble des fonctions rationnelles sur X qui sont définies en au moins un point de D. Alors $\mathcal{O}_{X,D}$ est un sous-anneau local du corps $\mathbf{C}(X)$. Si de plus X est normale, alors $\mathcal{O}_{X,D}$ est un anneau de valuation discrète, et on a

$$\mathbf{C}[X] = \bigcap_D ; \mathcal{O}_{X,D}$$

(intersection sur tous les diviseurs irréductibles $D \subset X$; voir [Ei] §11.2).

Théorème. *Soit X une G-variété affine normale.*

(i) La variété quotient $X//G$ est normale.

(ii) Si Y est une variété affine normale et si $p : X \to Y$ est un morphisme G-invariant tel que les fibres générales de p contiennent une unique orbite fermée, et que l'image de p rencontre tout diviseur de Y, alors p est le quotient.

Démonstration. (i) Soit f dans le corps des fractions de $\mathbf{C}[X//G] = \mathbf{C}[X]^G$. Si f est entier sur $\mathbf{C}[X]^G$ alors f est entier sur $\mathbf{C}[X]$, donc $f \in \mathbf{C}[X]$ car X est normale. Mais f est invariant, donc $f \in \mathbf{C}[X]^G$.

(ii) Il existe un unique morphisme $q : X//G \to Y$ tel que $p = q \circ \pi$. Puisque l'image de p rencontre tout diviseur de Y, il en est de même pour l'image de q. Soit $y \in Y$ tel que $p^{-1}(y)$ contient une unique orbite fermée. Alors $q^{-1}(y) = \pi(p^{-1}(y))$ donc $q^{-1}(y)$ est un point. On en déduit que p est birationnelle ; on conclut alors grâce au

Lemme. *Soient Y et Z deux variétés affines avec Y normale, et soit $q : Z \to Y$ un morphisme birationnel dont l'image contient un sous-ensemble dense de tout diviseur irréductible. Alors q est un isomorphisme.*

Démonstration du lemme. Soit $D \subset Y$ un diviseur irréductible. Puisque Y est normale, $\mathcal{O}_{Y,D}$ est un sous-anneau maximal du corps $\mathbf{C}(Y)$. Ce dernier s'identifie à $\mathbf{C}(Z)$ via q^*. Puisque l'image de q contient un sous-ensemble dense de D, on peut trouver un diviseur irréductible $E \subset Z$ tel que $q(E)$ est dense dans D. Alors

$$\mathcal{O}_{Y,D} \subseteq \mathcal{O}_{Z,E} \subset \mathbf{C}(Z) = \mathbf{C}(Y)$$

donc $\mathcal{O}_{Y,D} = \mathcal{O}_{Z,E}$. D'où

$$\mathbf{C}[Z] \subseteq \bigcap_E \mathcal{O}_{Z,E} \subseteq \bigcap_D \mathcal{O}_{Y,D}$$

et ce dernier est égal à $\mathbf{C}[Y]$. Mais d'autre part $\mathbf{C}[Y] \subseteq \mathbf{C}[Z]$ via q^*, d'où $\mathbf{C}[Y] = \mathbf{C}[Z]$ et l'assertion.

Exemple 1 (l'action adjointe). On considère l'action du groupe réductif connexe G dans lui-même par conjugaison. Soit $T \subseteq G$ un tore maximal. Notons $N \subseteq G$ le normalisateur de T, et $W = N/T$ le groupe de Weyl ; c'est un groupe fini. L'action de N dans G laisse stable T, dans lequel T opère trivialement ; d'où une action de W dans T. La composition $T \to G \to G//G$ est invariante par W, et passe au quotient en $q : T/W \to G//G$.

Montrons que q est un isomorphisme. En effet, on a vu en 3.1 que toute orbite fermée de G dans lui-même est formée d'éléments semi-simples. Une telle orbite rencontre T, donc q est surjective. Soit $g \in G$ un élément semisimple régulier. Alors la fibre de $\pi : G \to G//G$ en g est l'orbite $G \cdot g$, qui coupe T suivant une unique orbite de W (vérifier). Par suite, la fibre de q en g est cette orbite de W, et le critère s'applique.

Autrement dit, la restriction à T définit un isomorphisme

$$Res : C(G) \to \mathbf{C}[T]^W \ .$$

De même, si g (resp. t) désigne l'algèbre de Lie de G (resp. T), on a un isomorphisme $p : t/W \to g//G$. Autrement dit, la restriction à t induit un isomorphisme

$$Res : \mathbf{C}[g]^G \to \mathbf{C}[t]^W$$

("théorème de Chevalley").

Exemple 2 (la loi de réciprocité de Hermite). Soit $X = V_1^d$ l'espace des d-uples de formes linéaires sur $\mathbf{C}^2$. On a une application naturelle

$$\begin{array}{cccc} p : & V_1^d & \to & V_d \\ & (f_1, \ldots, f_d) & \mapsto & \prod_{i=1}^d f_i. \end{array}$$

Soit T_d le sous-groupe de $(\mathbf{C}^*)^d$ formé des $(t_1, \ldots, t_d)$ tels que $\prod_{i=1}^d t_i = 1$. Le groupe T_d opère dans V_1^d par

$$(t_1, \ldots, t_d) \cdot (f_1, \ldots, f_d) = (t_1 f_1, \ldots, t_d f_d) \ .$$

Observons que p est invariante par cette action, et aussi par l'action du groupe symétrique S_d par permutation des copies de V_1. De plus, S_d normalise T_d ; soit Γ_d le produit semi-direct de T_d par S_d. Alors la fibre de p en tout $f \in V_d \setminus \{0\}$ est une orbite de Γ_d (factorisation unique des polynômes!). Puisque p est surjective, c'est le quotient par Γ_d.

On a donc un isomorphisme

$$p^* : \mathbf{C}[V_d] \simeq \mathbf{C}[V_1^d]^{\Gamma_d}$$

qui est SL_2-équivariant (on fait opérer SL_2 dans V_1^d de façon naturelle ; cette action commute à celle de Γ_d) et homogène de degré d. Par suite, pour tout entier n, on a un isomorphisme de SL_2-modules :

$$\mathbf{C}[V_d]_n \simeq \mathbf{C}[V_1^d]_{nd}^{\Gamma_d} \ .$$

D'autre part, l'espace $\mathbf{C}[V_1^d]_{nd}^{T_d}$ est formé des fonctions polynomiales sur $V_1^d = V_1 \times \cdots \times V_1$ qui sont homogènes de degré n par rapport à chaque facteur V_1. D'où un isomorphisme

$$\mathbf{C}[V_1^d]_{nd}^{T_d} \simeq (V_n^*)^{\otimes d}$$

ce qui entraîne que

$$\mathbf{C}[V_1^d]_{nd}^{\Gamma_d} = S^d(V_n^*) = \mathbf{C}[V_n]_d \ .$$

En conclusion, on a un isomorphisme canonique de SL_2-modules

$$\mathbf{C}[V_d]_n \simeq \mathbf{C}[V_n]_d$$

("loi de réciprocité de Hermite").

La loi de réciprocité permet de démontrer l'existence d'invariants ou de covariants de formes binaires. Par exemple, puisque l'algèbre $\mathbf{C}[V_3]^{\mathrm{SL}_2}$ est engendrée par un élément de degré 4, l'espace $\mathbf{C}[V_3]_n^{\mathrm{SL}_2}$ est de dimension 1 si n est divisible par 4. On en déduit que toute forme binaire de degré divisible par 4 admet un "unique" invariant de degré 3. D'autres applications de l'isomorphisme p^* seront données dans l'exemple ci-dessous.

Une reformulation de la loi de réciprocité est l'existence d'un isomorphisme GL_2-équivariant de $S^n(S^d\mathbf{C}^2)$ sur $S^d(S^n\mathbf{C}^2)$. Plus généralement, on peut construire une application $\mathrm{GL}(V)$-équivariante canonique

$$S^n(S^dV) \to S^d(S^nV)$$

où V est un espace vectoriel de dimension finie quelconque, et on conjecture que cette application est injective pour $n \leq d$ et surjective pour $n \geq d$ (voir [Ho1]). Cette conjecture impliquerait une classique conjecture de Foulkes : la multiplicité de tout $\mathrm{GL}(V)$-module simple dans $S^n(S^dV)$ est au moins égale à sa multiplicité dans $S^d(S^nV)$ si $n \geq d$.

Exemple 3 (la méthode symbolique). L'isomorphisme équivariant

$$p^* : \mathbf{C}[V_d] \to \mathbf{C}[V_1^d]^{\Gamma_d}$$

de l'exemple précédent, induit un isomorphisme

$$\mathcal{I}(V_d) = \mathbf{C}[V_d]^{\mathrm{SL}_2} \simeq (\mathbf{C}[V_1^d]^{\mathrm{SL}_2})^{\Gamma_d} = ((\mathbf{C}[V_1^d]^{\mathrm{SL}_2})^{T_d})^{S_d} \ .$$

De plus, l'algèbre $\mathbf{C}[V_1^d]^{\mathrm{SL}_2}$ a une description très explicite, grâce à la théorie classique des invariants. En effet, cette algèbre est engendrée par des symboles

$$[ij] := \det(f_i, f_j) \qquad (1 \leq i < j \leq d)$$

et les relations entre ces symboles sont engendrées par les "relations de Plücker"

$$[ij][kl] - [ik][jl] + [il][jk] = 0 \qquad (1 \leq i < j < k < l \leq d).$$

Par exemple, si $d = 2$, l'algèbre $\mathbf{C}[V_1^2]^{\mathrm{SL}_2}$ est engendrée par le symbole [12]. De plus, $\Gamma_2 = \{1, -1\}$ et $(-1)[12] = -[12]$ donc l'algèbre $\mathcal{I}(V_2)$ est engendrée par $[12]^2$. Ce dernier est le carré de la différence des racines, c'est-à-dire le discriminant.

Pour $d = 3$, l'algèbre $\mathbf{C}[V_1^3]^{\mathrm{SL}_2}$ est engendrée par les symboles [12], [13] et [23], et ceux-ci sont algébriquement indépendants. De plus, les invariants de T_3 dans cette algèbre sont engendrés par le produit [12][13][23]. Ce dernier est un vecteur propre de S_3 pour le caractère signature, donc l'algèbre $\mathcal{I}(V_3)$ est engendrée par $[12]^2[13]^2[23]^2$, c'est-à-dire par le discriminant.

Pour $d = 4$, l'algèbre $\mathbf{C}[V_1^4]^{\mathrm{SL}_2 \times T_4}$ est engendrée par les produits

$$x := [12][34], \; y := -[13][24], \; z := [14][23]$$

avec la relation $x + y + z = 0$ (voir l'exemple 3 en 1.5). On en déduit (exercice) que l'algèbre $\mathcal{I}(V_4)$ est engendrée par un invariant de degré 2,

$$I := x^2 + y^2 + z^2$$

et par un invariant de degré 3,

$$J := x^3 + y^3 + z^3 \; .$$

De plus, I et J sont uniques à des constantes multiplicatives près, et ils sont algébriquement indépendants.

Cette approche de l'algèbre des invariants des formes binaires a été développée au siècle dernier, sous le nom de "méthode symbolique" ; voir [Ho2] pour un exposé contemporain. La méthode symbolique s'adapte aux covariants, en considérant l'application

$$\begin{array}{cccc} q: & V_1^d \times V_1 & \to & V_d \times V_1 \\ & (f_1, \ldots, f_d, f_0) & \mapsto & (\prod_{i=1}^d f_i, f_0) \end{array} .$$

L'algèbre $\mathcal{C}(V_d)$ est donc formée des invariants de Γ_d dans l'algèbre définie par générateurs $[ij]$ $(0 \leq i < j \leq d)$ et relations ci-dessus pour $0 \leq i < j < k < l \leq d$. Le degré d'un covariant est le degré partiel par rapport à f_i (où $1 \leq i \leq d$) d'un représentant de ce covariant, tandis que son ordre est le degré partiel par rapport à f_0. Le covariant identité est représenté par le produit $[01][02]\ldots[0d]$. Ceci permet de décrire $\mathcal{C}[V_d]$ pour $d \leq 3$.

Si $d = 1$, l'algèbre $\mathcal{C}(V_1)$ est engendrée par $f = [01]$.

Si $d = 2$, l'algèbre $\mathbf{C}[V_1^2 \times V_1]^{\mathrm{SL}_2 \times T_2}$ est engendrée par $[01][02]$ et $[12]$. L'algèbre $\mathcal{C}(V_2)$ est donc engendrée par $f = [01][02]$ et $\Delta = [12]^2$.

Si $d = 3$, l'algèbre $\mathbf{C}[V_1^3 \times V_1]^{\mathrm{SL}_2 \times T_3}$ est engendrée par

$$[01][02][03],\ [12][23][13],\ x := [01][23],\ y := -[02][13],\ z := [03][12]\ .$$

De plus, on a $x + y + z = 0$. On en déduit (exercice) que l'algèbre $\mathcal{C}(V_3)$ est engendrée par

$$f = [01][02][03],\ H = x^2 + y^2 + z^2,\ \Delta = [12]^2[23]^2[13]^2,$$
$$T = x^2y + y^2z + z^2x - xy^2 - yz^2 - zx^2\ .$$

On revient au cas d'un groupe algébrique arbitraire G ; on va décrire le quotient dans un cas très particulier mais utile.

Proposition. *Soient G un groupe algébrique, et V un G-module rationnel de dimension finie. On suppose qu'il existe un groupe algébrique $\tilde{G} \supseteq G$ tel que :*

(i) G est le groupe dérivé de $\tilde{G}$,

(ii) le quotient $\tilde{G}/G$ est un tore, et

(iii) l'action linéaire de G dans V s'étend en une action linéaire de $\tilde{G}$, avec une orbite ouverte Ω.

Alors l'algèbre $\mathbf{C}[V]^G$ est engendrée par les équations $f_1, \ldots, f_n$ des composantes irréductibles de codimension un de $V \setminus \Omega$. De plus, $f_1, \ldots, f_n$ sont algébriquement indépendantes.

Démonstration. Observons d'abord que $f_1, \ldots, f_n$ sont des vecteurs propres de $\tilde{G}$, et donc des invariants de G grâce à l'hypothèse (i). De plus, d'après les hypothèses (i) et (ii), l'algèbre $\mathbf{C}[V]^G$ est somme directe de sous-espaces propres de $\tilde{G}$. Soit $f \in \mathbf{C}[V]^G$ un vecteur propre de $\tilde{G}$. L'ensemble des zéros de f est stable par $\tilde{G}$; c'est donc une réunion de composantes irréductibles de codimension un de $V \setminus \Omega$. Par suite, il existe une constante non nulle c et des entiers non négatifs $a_1, \ldots, a_n$ tels que

$$f = c \prod_{i=1}^{n} f_i^{a_i}\ .$$

Ainsi, l'algèbre $\mathbf{C}[V]^G$ est engendrée par $f_1, \ldots, f_n$.

Notons χ_i le poids de f_i. Montrons que les caractères $\chi_1, \ldots, \chi_n$ de $\tilde{G}$ sont linéairement indépendants. Sinon, on aurait des entiers $b_1, \ldots, b_n$ non tous nuls, tels que la fonction rationnelle

$$F := \prod_{i=1}^{n} f_i^{b_i}$$

soit invariante par $\tilde{G}$. Mais F n'est pas constante, ce qui contredit le fait que $\tilde{G}$ a une orbite ouverte dans V.

Montrons enfin que $f_1, \ldots, f_n$ sont algébriquement indépendantes. Sinon, soit

$$P(f_1, \ldots, f_n) = \sum ; p_{a_1 \ldots a_n} f_1^{a_1} \cdots f_n^{a_n} = 0$$

une relation non triviale, telle que les nombre N des $(a_1, \ldots, a_n)$ qui vérifient $p_{a_1 \ldots a_n} \neq 0$ est minimal. Alors, pour tout $g \in \tilde{G}$, on a

$$\sum ; p_{i_1 \ldots i_n} \chi_1(g)^{a_1} \cdots \chi_n(g)^{a_n} f_1^{a_1} \cdots f_n^{a_n} = 0 \ .$$

Puisque les caractères $\chi_1^{a_1} \cdots \chi_n^{a_n}$ sont deux à deux distincts, on en déduit une relation non triviale entre $f_1, \ldots, f_n$ avec moins de N coefficients, contradiction.

Exemple 1. Si $G = \mathrm{SL}_2$ et si $V = V_2$ ou V_3, alors $\tilde{G} := \mathrm{GL}_2$ a une orbite dense dans V, formée des polynômes ayant toutes leurs racines distinctes. On retrouve ainsi le fait que l'algèbre $\mathbf{C}[V]^G$ est engendrée par le discriminant.

Exemple 2. Si $G = \mathrm{SL}_n$ et si V est l'espace des formes quadratiques en n variables, alors $\tilde{G} := \mathrm{GL}_n$ a une orbite dense dans V, qui consiste en les formes quadratiques non dégénérées. L'algèbre $\mathbf{C}[V]^G$ est donc engendrée par le discriminant.

Exemple 3. Soient p et q deux entiers positifs, et soit $M_{p,q}$ l'espace des matrices $p \times q$. Le groupe $\mathrm{GL}_p \times \mathrm{GL}_q$ opère dans $M_{p,q}$ par

$$(A, B) \cdot X := AXB^{-1} \ .$$

On considère l'action du sous-groupe $G := U_p^- \times U_q$ où U_p^- désigne le sous-groupe de GL_p formé des matrices triangulaires inférieures avec coefficients diagonaux égaux à 1. Soit $\tilde{G} := B_p^- \times B_q$. Alors les hypothèses (i) et (ii) sont satisfaites. Pour $1 \leq k \leq \min(p, q)$, et pour $X = (x_{i,j}) \in M_{p,q}$, posons

$$\Delta_k(X) := \det(x_{i,j})_{1 \leq i,j \leq k} \ .$$

Alors $\tilde{G}$ a une orbite ouverte dans $M_{p,q}$, et son complémentaire est réunion des zéros des Δ_k (exercice). On en déduit que l'algèbre $\mathbf{C}[M_{p,q}]^G$ est engendrée par les Δ_k. Ceci conduit à une preuve géométrique de la “formule de Cauchy” (voir [Ho3]).

3.3. *Le critère de Hilbert-Mumford*

Lorsqu'un tore opère dans une variété affine avec une orbite ouverte, on peut atteindre toutes les autres orbites par des limites de sous-groupes à un paramètre, d'après le corollaire à la proposition 1.5.2. Ce résultat n'est plus valable lorsqu'on remplace le tore par un groupe réductif arbitraire ; voir l'exemple ci-dessous. Mais on va voir que l'orbite fermée peut être atteinte par un sous-groupe à un paramètre ("critère de Hilbert-Mumford"). On en déduira une caractérisation des orbites fermées, ainsi qu'une description des fibres du quotient.

Exemple. Considérons le groupe $G = \mathrm{SL}_2$ opérant dans l'espace V_d des formes binaires de degré $d \geq 3$. Alors l'adhérence de l'orbite de $x^{d-1}y$ contient x^d (exercice). Mais il n'existe aucun sous-groupe à un paramètre λ de G tel que $\lim_{t\to 0} \lambda(t) \cdot x^{d-1}y$ existe et appartient à $G \cdot x^d$. Sinon, l'image de λ fixerait cette limite ; mais le groupe d'isotropie de tout point de $G \cdot x^d$ n'admet pas de sous-groupe à un paramètre non trivial (exercice).

Théorème. *Soit G un groupe réductif opérant dans une variété affine X, et soit $x \in X$. Notons $\mathcal{O}$ l'orbite fermée de G dans $\overline{G \cdot x}$. Il existe alors un sous-groupe à un paramètre λ de G tel que* $\lim_{t\to 0} \lambda(t) \cdot x$ *existe et est dans $\mathcal{O}$.*

Démonstration (d'après [Kr] III.2.4). Grâce au corollaire à la proposition 1.5.2, il suffit de montrer qu'il existe $g \in G$ et un tore $T \subseteq G$ tels que $\overline{T \cdot gx}$ rencontre $\mathcal{O}$. Pour cela, on utilise la décomposition de Cartan $G = KTK$ où K est un sous-groupe compact maximal de G, et T est le complexifié d'un tore maximal de K (voir [He] Chapter 9). Si $\overline{T \cdot y}$ ne rencontre pas $\mathcal{O}$ pour tout $y \in G \cdot x$, alors il existe $f_y \in \mathbf{C}[X]^T$ telle que $f_y(y) = 1$ et que $f_y|_{\mathcal{O}} = 0$ (théorème 3.1). Posons

$$U_y := \{z \in X \; ;| \; ; f_y(z) \neq 0\} \; .$$

Alors le compact $K \cdot x$ est recouvert par les ouverts U_y ($y \in G \cdot x$) donc il existe $y_1, \ldots, y_n$ dans $G \cdot x$ tels que

$$K \cdot x \subseteq U_{y_1} \cup \cdots \cup U_{y_n} \; .$$

Définissons une application $f : X \to \mathbf{R}$ par

$$f(z) := \sum_{i=1}^{n} \; ; |f_{y_i}(z)| \; .$$

Alors f est continue, invariante par T, nulle sur $\mathcal{O}$, et strictement positive sur $K \cdot x$. Il existe donc $\varepsilon > 0$ tel que $f \geq \varepsilon$ sur $K \cdot x$. D'où $f \geq \varepsilon$ sur $\overline{TK \cdot x}$. Ainsi, $\overline{TK \cdot x}$ ne rencontre pas $\mathcal{O}$. Mais $\overline{G \cdot x} = K \cdot \overline{TK \cdot x}$ car K est compact, et car l'adhérence de $G \cdot x$ pour la topologie de Zariski est la même que pour la topologie transcendante. Il en résulte que $\overline{G \cdot x}$ ne rencontre pas $\mathcal{O}$, ce qui est absurde.

Corollaire 1. *Soit G un groupe réductif opérant dans une variété affine X, et soit $x \in X$. Les conditions suivantes sont équivalentes :*

(i) L'orbite $G \cdot x$ est fermée et le groupe d'isotropie G_x est fini.

(ii) Pour tout sous-groupe à un paramètre λ de G, l'application $t \mapsto \lambda(t) \cdot x$ n'a pas de limite en 0.

De plus, sous l'une de ces hypothèses, la fibre du quotient en x est réduite à $G \cdot x$.

Démonstration. (i)⇒(ii) Si $\lambda(t) \cdot x$ a une limite y quand $t \to 0$, alors $y \in G \cdot x$ et le groupe d'isotropie de y contient l'image de λ. Puisque G_y est fini, λ est trivial.

(ii)⇒(i) D'après le critère de Hilbert-Mumford, l'orbite $G \cdot x$ est fermée dans X, donc affine. D'après la propopsition 2 en 3.1, le groupe d'isotropie G_x est réductif. Mais l'hypothèse implique que tout sous-groupe à un paramètre de G_x est trivial, et donc G_x est fini.

Enfin, sous l'hypothèse (i), l'orbite $G \cdot x$ est fermée et de dimension maximale ; ainsi, elle ne peut être contenue dans l'adhérence d'une autre orbite. D'après le théorème 3.1, la fibre du quotient en x est donc $G \cdot x$.

Considérons maintenant un G-module V (rationnel, de dimension finie).

Définitions. Le *nilcône* de V est la fibre du quotient $\pi : V \to V//G$ à l'origine, notée $\mathcal{N}(V)$. D'après le théorème 3.1, on a :

$$\mathcal{N}(V) = \{v \in V \ ;| \ ;0 \in \overline{G \cdot v}\} \ .$$

Un point $v \in V$ est dit *instable* si $v \in \mathcal{N}(V)$, et *semi-stable* sinon. Enfin, v est dit *stable* si l'orbite $G \cdot v$ est fermée dans V, et si de plus le groupe d'isotropie G_v est fini.

Une conséquence immédiate du critère de Hilbert-Mumford est le

Corollaire 2. *Le nilcône de V est l'ensemble des v tels qu'il existe un sous-groupe à un paramètre λ de G avec $\lim_{t \to 0} \lambda(t) \cdot v = 0$.*

Exemple 1 (les formes binaires). Soit $G = \mathrm{SL}_2$ opérant dans V_d. Alors les points stables sont les formes dont toutes les racines ont une multiplicité $< d/2$.

En effet, pour tout sous-groupe à un paramètre non trivial λ de G, il existe $g \in G$ et un entier $n > 0$ tels que

$$\lambda(t) = g \lambda_0(t^n) g^{-1}$$

où λ_0 est le sous-groupe à un paramètre standard, donné par

$$\lambda_0(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \ .$$

On a donc
$$\lambda_0(t) \cdot x^i y^{d-i} = t^{d-2i} x^i y^{d-i} \ .$$
Par suite, pour $\varphi \in V_d$ non nulle, l'application
$$t \to \lambda_0(t^n) \cdot \varphi$$
a une limite en 0 si et seulement si $i \leq d/2$ pour tout monôme $x^i y^{d-i}$ figurant dans f, c'est-à-dire si $y = 0$ est racine de φ de multiplicité $\geq d/2$. On conclut grâce au corollaire 1.

On montre de même que les points instables sont les formes qui admettent une racine de multiplicité $> d/2$; on en déduit que la dimension du nilcône est $1 + \frac{d}{2}$ si d est pair, et $1 + \frac{d+1}{2}$ si d est impair.

Ceci conduit à une description complète des fibres du quotient. Lorsque d est impair, si f a toutes ses racines de multiplicité $\leq (d-1)/2$, alors la fibre de f est son orbite ; sinon, f est dans le nilcône. Lorsque d est pair, les fibres du quotient sont les orbites des formes dont toutes les racines sont de multiplicité $< d/2$, le nilcône, et aussi les ensembles
$$G \cdot (cx^{d/2} y^{d/2} + x^{(d/2)+1} V_{(d/2)-1})$$
où c est une constante non nulle (exercice).

Exemple 2 (les formes cubiques ternaires). On considère l'opération de $G = \mathrm{SL}_3$ dans l'espace $V = \mathbf{C}[x, y, z]_3$ des polynômes homogènes de degré 3 en 3 variables ("formes cubiques ternaires" dans la terminologie du siècle dernier). On peut voir chaque $f \in V \setminus \{0\}$ comme une équation d'une courbe $C(f) \subset \mathbf{P}^2(\mathbf{C})$ de degré 3 (une cubique plane).

Soit λ un sous-groupe à un paramètre de G. Dans des coordonnées convenables, on peut écrire
$$\lambda(t) = \begin{pmatrix} t^a & 0 & 0 \\ 0 & t^b & 0 \\ 0 & 0 & t^c \end{pmatrix}$$
où a, b, c sont des entiers tels que $a \geq b \geq c$ et que $a + b + c = 0$. On en déduit que l'espace vectoriel formé des f tels que $\lim_{t\to 0} \lambda(t) \cdot f = 0$, est contenu dans l'espace vectoriel engendré par x^3, x^2y, xy^2, y^3 et x^2z. De plus, ces espaces sont égaux lorsque (par exemple) $(a, b, c) = (2, 1, -3)$. Ainsi, tout $f \in \mathcal{N}(V)$ s'écrit dans des coordonnées convenables :
$$f(x, y, z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z \ .$$
Cela conduit aux possibilités suivantes pour $C(f)$:
- Si $de \neq 0$, alors $C(f)$ a un point de rebroussement, de coordonnées homogènes $[0 : 0 : 1]$, et de tangente $(x = 0)$.

• Si $d = 0$ et $ce \neq 0$, alors $C(f)$ est réunion de la conique $(ax^2+bxy+cy^2+exz = 0)$ et de sa tangente $(x = 0)$.
• Si $c = d = 0$ ou si $e = 0$, alors $C(f)$ est réunion de trois droites concourantes, éventuellement confondues.

On conclut que $\mathcal{N}(V)$ est formé des équations des cubiques à point de rebroussement, ainsi que de leurs dégénerescences. On vérifie de même que les points stables sont les équations des cubiques non singulières. En fait, chaque fibre du quotient est, soit une orbite $G \cdot f$ où $C(f)$ est non singulière, soit l'ensemble des f tels que $C(f)$ a un point double ordinaire, soit le nilcône.

Exemple 3. Plus généralement, considérons l'opération de $G = \mathrm{SL}_n$ dans l'espace $V = \mathbf{C}[x_1, \ldots, x_n]_d$ où $n \geq 2$ et $d \geq 3$. Chaque $f \in V \setminus \{0\}$ est l'équation d'une hypersurface $H(f) \subset \mathbf{P}^{n-1}(\mathbf{C})$ de degré d. Montrons que f est stable si $H(f)$ est non singulière.

Observons que $H(f)$ est non singulière si et seulement si l'origine est l'unique zéro commun aux dérivées partielles $f_1, \ldots, f_n$ de f. Cette condition se traduit par la non-annulation en f d'un invariant homogène Δ sur V, le discriminant. Comme dans l'exemple 1.2.1, il suffit donc de vérifier que G_f est fini lorsque $H(f)$ est non singulière (ce résultat est dû à Jordan).

Le groupe G_f est infini si et seulement si son algèbre de Lie est non nulle. L'algèbre de Lie de G est formée des matrices $n \times n$ de trace nulle ; elle opère dans V par

$$(A \cdot f)(x) = \frac{d}{dt} f(exp(-tA)x)|_{t=0} = -df_x(Ax) \ .$$

Si G_f est infini, alors il existe $A = (a_{ij})$ non nulle, telle que

$$\sum_{i=1}^{n} ; (\sum_{j=1}^{n} ; a_{ij}x_j) \ ; f_i = 0 \ .$$

D'autre part, puisque l'unique zéro commun à $f_1, \ldots, f_n$ est l'origine, la suite $(f_1, \ldots, f_n)$ est régulière, c'est-à-dire : pour $1 \leq i \leq n$, la multiplication par f_i est injective dans le quotient de $\mathbf{C}[V]$ par l'idéal engendré par les f_j $(j \neq i)$; voir [Ei] §18.2 ou la section suivante. Il en résulte que $\sum_{j=1}^n ; a_{ij}x_j$ est dans l'idéal engendré par les f_j $(j \neq i)$. Mais comme le degré de chaque f_j est au moins 2, on a $\sum_{j=1}^n ; a_{ij}x_j = 0$ pour tout i, ce qui est absurde.

3.4. *Le théorème de Hochster-Roberts*

Pour énoncer ce théorème, on a besoin de quelques préliminaires d'algèbre commutative. Soient k un corps, $A = \oplus_{n=0}^\infty ; A_n$ une k-algèbre graduée de type fini, $A_+ = \oplus_{n=1}^\infty A_n$ son idéal maximal homogène, et $M = \oplus_{n=-\infty}^\infty ; M_n$ un A-module gradué de type fini.

Définition. Une suite $(a_1, \ldots, a_r)$ d'éléments homogènes de A_+ est un *système de paramètres homogènes* si le quotient $M/a_1M + \cdots + a_rM$ est de dimension finie sur k, et si r est minimal pour cette propriété.

Notons $Ann(M) := \{a \in A \;|\; aM = 0\}$ l'annulateur de M dans A. On déduit du lemme de normalisation de Noether que $(a_1, \ldots, a_r)$ est un système de paramètres homogènes si et seulement si : les images $\overline{a_1}, \ldots, \overline{a_r}$ dans $A/Ann(M)$ sont algébriquement indépendantes, et de plus M est un module de type fini sur $k[\overline{a_1}, \ldots \overline{a_r}]$. Il en résulte que tous les systèmes de paramètres homogènes de A ont la même longueur : la dimension de M, notée $\dim(M)$ (voir [Ei] §10.1).

Définition. Une suite $(a_1, \ldots, a_r)$ d'éléments homogènes de A_+ est *régulière dans* M si pour $1 \leq s \leq r$, la multiplication par a_s est injective dans le quotient $M/a_1M + \cdots + a_{s-1}M$.

On montre que la suite $(a_1, \ldots, a_r)$ est régulière dans M si et seulement si : $a_1, \ldots, a_r$ sont algébriquement indépendants, et de plus M est un module libre sur $k[a_1, \ldots, a_r]$ (voir [Ei] §18.4). Il en résulte que toute suite régulière peut se compléter en un système de paramètres. En particulier, la longueur de toute suite régulière est au plus $\dim(M)$; on montre que toutes les suites régulières maximales ont la même longueur, appelée la *profondeur* de M (voir [Ei] §17.2).

Définition. Le A-module M est *de Cohen-Macaulay* s'il admet une suite régulière qui est un système de paramètres.

Autrement dit, M est de Cohen-Macaulay si et seulement si M est un module libre et de type fini sur une sous-algèbre graduée de A, engendrée par des éléments algébriquement indépendants. De plus, dans un module de Cohen-Macaulay, toutes les suites régulières maximales sont des systèmes de paramètres.

Exemple 1 (les algèbres de polynômes). Soit $A = k[x_1, \ldots, x_n]$ une k-algèbre graduée de polynômes. Alors la suite $(x_1, \ldots, x_n)$ est régulière dans A, et donc A est de Cohen-Macaulay. Plus généralement, une suite $(a_1, \ldots, a_n)$ d'éléments homogènes est régulière si et seulement si l'origine est le seul zéro commun à $a_1, \ldots, a_n$. En effet, d'après le théorème des zéros de Hilbert, cette dernière condition équivaut au fait que le quotient de A par l'idéal engendré par $a_1, \ldots, a_n$ est de dimension finie comme espace vectoriel sur k.

Exemple 2 (les invariants des groupes finis). Soit G un sous-groupe fini de GL_n. Montrons que tout module de covariants de $\mathbf{C}^n$ est de Cohen-Macaulay. Soit $(a_1, \ldots, a_r)$ un système de paramètres homogènes de l'algèbre $\mathbf{C}[x_1, \ldots, x_n]^G$. Alors $\mathbf{C}[x_1, \ldots, x_n]$ est entière sur la sous-algèbre de polynômes $\mathbf{C}[a_1, \ldots, a_r]$, donc $r = n$ et $\mathbf{C}[x_1, \ldots, x_n]$ est un module libre sur $\mathbf{C}[a_1, \ldots, a_n]$. Grâce au corollaire 2.5.1, tout module de covariants M est facteur direct de ce module libre ; puisque M est gradué, il est libre.

Plus généralement, on va montrer que les algèbres d'invariants pour les actions linéaires des groupes réductifs sont de Cohen-Macaulay. En fait, on va démontrer l'énoncé suivant, dû à Hochster et Roberts (voir [Ho-Ro]).

Théorème. *Soit $R = k[x_1, \dots, x_n]$ une algèbre graduée de polynômes sur un corps k, et soit $A \subseteq R$ une sous-algèbre graduée, telle que A est facteur direct du A-module R. Alors l'algèbre A est de type fini, et de Cohen-Macaulay.*

Démonstration (d'après F. Knop, voir [Br-He] 6.5.4)). Par hypothèse, il existe une application A-linéaire $p : R \to A$ qui préserve le degré, et telle que $p(1) = 1$. Comme dans la preuve du théorème 2.5, on montre alors que l'algèbre A est noethérienne. Puisque A est graduée, on en déduit que c'est une algèbre de type fini sur k.

Soit $(a_1, \dots, a_r)$ un système de paramètres homogènes de A. Montrons que $(a_1, \dots, a_r)$ est une suite régulière dans A. Il suffit de montrer que si $f \in A$ et si $fa_s \in Aa_1 + \dots + Aa_{s-1}$, alors $f \in Ra_1 + \dots + Ra_{s-1}$ (en effet, ceci entraîne que $f = p(f) \in Aa_1 + \dots + Aa_{s-1}$). Ce résultat est conséquence de la

Proposition. *Soit k un corps, et soient $a_1, \dots, a_r$ des éléments homogènes et algébriquement indépendants de l'algèbre de polynômes $R = k[x_1, \dots, x_n]$. Soit A une k-algèbre graduée qui est un module fini sur $k[a_1, \dots, a_r]$ et qui est munie d'un $k[a_1, \dots, a_r]$-morphisme $\psi : A \to R$ préservant le degré. Si $f \in A$ et $fa_s \in Aa_1 + \dots + Aa_{s-1}$ alors $\psi(f) \in Ra_1 + \dots + Ra_{s-1}$.*

Démonstration de la proposition. On peut supposer que f est homogène, et on écrit $fa_s = f_1a_1 + \dots + f_{s-1}a_{s-1}$ avec des $f_i \in A$ homogènes.

On pose $B := k[a_1, \dots, a_r]$, et on choisit des générateurs homogènes $h_1, \dots, h_m$ du B-module A. On peut trouver un sous-anneau $k_0 \subseteq k$, de type fini sur $\mathbf{Z}$ et qui contient tous les coefficients des polynômes $a_1, \dots, a_r$, $\psi(f_1) \dots, \psi(f_{s-1})$ et $\psi(h_1), \dots, \psi(h_m)$, ainsi que des polynômes h_{ijl} tels que

$$h_ih_j = \sum_l h_{ijl}(a_1, \dots, a_r)h_l$$

et que des polynômes f_{ij} tels que

$$f_i = \sum_j f_{ij}(a_1, \dots, a_r)h_j.$$

En posant $R_0 := k_0[x_1, \dots, x_n]$, $B_0 := k_0[a_1, \dots, a_r]$ et $A_0 := B_0[h_1, \dots, h_m]$, on a alors : $\psi(A_0) \subseteq R_0$, $A_0 = B_0h_1 + \dots B_0h_m$, et $f, f_1, \dots, f_{s-1} \in A_0$.

Il suffit de montrer que

$$\psi(f) \in R_0a_1 + \dots + R_0a_{s-1}.$$

On raisonne par l'absurde, et on suppose que $\psi(f) \notin R_0a_1 + \dots + R_0a_{s-1}$. Puisque f et les a_i sont homogènes, cela signifie qu'un système linéaire (S) à coefficients dans k_0 n'a pas de solution dans k_0. Si ce système a des solutions dans le corps des fractions de k_0, alors on rajoute les dénominateurs de ces solutions à k_0.

On peut donc supposer que (S) n'a pas de solutions dans le corps des fractions de k_0, c'est-à-dire qu'un certain déterminant d n'est pas nul. Quitte à agrandir k_0, on peut supposer que $d^{-1} \in k_0$. Alors la réduction de (S) modulo tout idéal maximal $M \subset k_0$ n'a pas de solution.

Pour un tel M, on pose $\overline{k} := k_0/M$, $\overline{R} := R_0/MR_0$, $\overline{A} := A_0/MA_0$ et $\overline{B} := B_0/MB_0$. D'après le lemme ci-dessous, $\overline{k}$ est un corps fini ; soit p sa caractéristique. De plus, $\overline{R}$ et $\overline{B}$ sont des $\overline{k}$-algèbres de polynômes. Enfin, $\psi(\overline{f}) \notin \overline{R}\,\overline{a}_1 + \cdots + \overline{R}\,\overline{a}_{s-1}$. On peut aussi supposer que l'application $\overline{B} \to \overline{R}$ est injective, grâce à l'argument suivant : d'après le théorème de platitude générique (voir [Ei] §14.2), il existe $t \in B_0$ non nul, tel que $R_0[t^{-1}]$ est un module libre sur $B_0[t^{-1}]$. On choisit M tel que $t \notin MB_0$; alors les applications $B_0/MB_0 \to B_0[t^{-1}]/MB_0[t^{-1}]$ et $B_0[t^{-1}]/MB_0[t^{-1}] \to R_0[t^{-1}]/MR_0[t^{-1}]$ sont injectives, d'où l'assertion.

Comme $\overline{A}$ est un module fini sur $\overline{B}$, on peut trouver un sous-module libre $L \subseteq \overline{A}$ et $b \in \overline{B}$ tels que $b\overline{A} \subseteq L$. De plus, on a

$$\overline{f}\,\overline{a_s} = \sum_{i=1}^{s-1} \overline{f_i}\,\overline{a_i}$$

avec des $\overline{f_i}$ dans $\overline{A}$. On élève cette équation à la puissance $q = p^N$ et on multiplie par b : on obtient

$$(b\overline{f}^q)\,\overline{a_s}^q = \sum_{i=1}^{s-1} (b\overline{f_i}^q)\,\overline{a_i}^q \ ,$$

une équation dans le $\overline{B}$-module libre L, où $\overline{B}$ est une algèbre de polynômes en $\overline{a_1}, \ldots, \overline{a_r}$. Puisque la suite $(\overline{a_1}^q, \ldots, \overline{a_r}^q)$ est régulière dans L, il existe des $h_{iq} \in L$ $(1 \leq i \leq s-1)$ tels que $b\overline{f}^q = \sum_{i=1}^{s-1} h_{iq}\overline{a_i}^q$. D'où

$$b\psi(\overline{f})^q = \sum_{i=1}^{s-1} \psi(h_{iq})\overline{a_i}^q \ ,$$

une équation dans $\overline{R} = \overline{k}[\overline{x}_1, \ldots, \overline{x}_n]$.

Pour tout multi-indice $\alpha = (\alpha_1, \ldots, \alpha_n)$, on pose $|\alpha| := \max_{1 \leq i \leq n}(\alpha_i)$. Les monômes $\overline{x}^\alpha$, $|\alpha| < q$, forment une base du module $\overline{R}$ sur $\overline{k}[\overline{x_1}^q, \ldots, \overline{x_n}^q]$. On choisit q assez grand pour que $b = \sum_{|\alpha|<q} b_\alpha \overline{x}^\alpha$ avec des b_α dans $\overline{k}$ non tous nuls. On écrit aussi $\psi(h_{iq}) = \sum_{|\alpha|<q} (h_{iq\alpha})^q \overline{x}^\alpha$ avec des $h_{iq\alpha} \in \overline{R}$. On a donc

$$\sum_{|\alpha|<q} b_\alpha \psi(\overline{f})^q \overline{x}^\alpha = \sum_{|\alpha|<q} (h_{iq\alpha})^q \overline{x}^\alpha \overline{a}_i^q \ .$$

D'où, en prenant un coefficient non nul :

$$b_\alpha \psi(\overline{f})^q \in (\overline{R}\,\overline{a}_1 + \cdots + \overline{R}\,\overline{a}_{s-1})^q$$

et donc $\psi(\overline{f}) \in \overline{R}\,\overline{a}_1 + \cdots + \overline{R}\,\overline{a}_{s-1}$ ce qui est absurde.

Lemme. *Soit K un anneau de type fini sur $\mathbf{Z}$. Si K est un corps, alors K est fini.*

Démonstration. Notons K_0 le sous-corps de K engendré par 1. D'après une version du théorème des zéros de Hilbert (voir [Ei] §13.2), le corps K est de dimension finie sur K_0. Il suffit donc de montrer que K_0 est fini. Sinon, K_0 est le corps des rationnels. Par hypothèse, il existe $x_1, \ldots, x_n \in K$ qui engendrent K comme anneau. On peut écrire $x_i = a_i b^{-1}$ où $a_1, \ldots, a_n$ sont des entiers de K, et où b est un entier non nul. Alors la trace $\mathrm{Tr}_{K/\mathbf{Q}}$ est à valeurs dans $\mathbf{Z}[b^{-1}]$ ce qui est absurde.

3.5. *Systèmes de paramètres homogènes des algèbres d'invariants*

Soit G un groupe réductif et soit V un G-module (rationnel, de dimension finie). Le théorème de Hochster-Roberts ramène en partie la description de l'algèbre des invariants $\mathbf{C}[V]^G$ à la construction d'un système de paramètres homogènes pour cette algèbre. On va démontrer un résultat dû à Hilbert, qui caractérise les systèmes de paramètres de $\mathbf{C}[V]^G$ en termes du nilcône $\mathcal{N}(V)$ (défini en 3.3).

Proposition 1. *Pour des invariants $a_1, \ldots, a_n$ homogènes et non constants avec $n = \dim(V//G)$, les conditions suivantes sont équivalentes :*

(i) $(a_1, \ldots, a_n)$ est un système de paramètres homogènes de $\mathbf{C}[V]^G$.

(ii) L'ensemble des zéros communs à $a_1, \ldots, a_n$ est le nilcône.

Démonstration. (i)$\Rightarrow$(ii) Il est clair que $\mathcal{N}(V)$ est contenu dans l'ensemble des zéros communs à $a_1, \ldots, a_n$. Réciproquement, si $v \notin \mathcal{N}(V)$, on peut trouver un invariant f homogène et non constant, tel que $f(v) \neq 0$. Puisque $(a_1, \ldots, a_n)$ est un système de paramètres homogènes, f est entier sur $\mathbf{C}[a_1, \ldots, a_n]$. On a donc une équation de la forme

$$f^N + h_1 f^{N-1} + \cdots + h_N = 0$$

où les h_i sont des polynômes homogènes et non constants en $a_1, \ldots, a_n$. Ainsi, il existe i tel que $h_i(v) \neq 0$, donc $a_1, \ldots, a_n$ ne s'annulent pas tous en v.

(ii)$\Rightarrow$(i) Soit f un invariant homogène et non constant. Par hypothèse, f s'annule sur les zéros communs à $a_1, \ldots, a_n$. D'après le théorème des zéros de Hilbert, il existe un entier $N \geq 1$ tel que f^N est dans l'idéal de $\mathbf{C}[V]$ engendré par $a_1, \ldots, a_n$. A l'aide du théorème 2.5, on en déduit que f^N est dans l'idéal I de $\mathbf{C}[V]^G$ engendré par $a_1, \ldots, a_n$. L'idéal maximal homogène du quotient $\mathbf{C}[V]^G/I$ est donc formé d'éléments nilpotents. Mais cet idéal est de type fini, donc l'algèbre $\mathbf{C}[V]^G/I$ est de dimension finie. D'après le lemme de Nakayama gradué, l'algèbre $\mathbf{C}[V]^G$ est entière sur $\mathbf{C}[a_1, \ldots, a_n]$.

Exemple 1 (les groupes finis). On suppose que G est fini, et on note n la dimension de V. Alors, pour des invariants $a_1, \ldots, a_n$ homogènes et non constants, les conditions suivantes sont équivalentes :

(i) $(a_1, \ldots, a_n)$ est un système de paramètres de $\mathbf{C}[V]^G$.

(ii) $a_1, \ldots, a_n$ n'ont que le zéro trivial en commun.

On en déduit une construction d'un système de paramètres homogènes de $\mathbf{C}[V]^G$. On commence par construire inductivement des formes linéaires $\ell_1, \ldots, \ell_n$ sur V, telles que ℓ_i ne s'annule identiquement sur aucun des sous-espaces vectoriels

$$(g_1 \cdot \ell_1 = 0) \cap \cdots \cap (g_{i-1} \cdot \ell_{i-1} = 0)$$

pour $1 \leq i \leq n$ et pour $g_1, \ldots, g_{i-1}$ dans G. On pose $a_i := \prod_{g \in G} g \cdot \ell_i$ pour $1 \leq i \leq n$. Alors $(a_1, \ldots, a_n)$ est un système de paramètres pour l'algèbre des invariants, formé d'éléments homogènes de degré égal à l'ordre de G.

Exemple 2 (les fonctions multisymétriques). Soit $G = S_n$ opérant dans $V = (\mathbf{C}^m)^n$ comme dans l'exemple 3 en 1.3. Alors un système de paramètres homogènes est formé des fonctions symétriques élémentaires

$$e_k(x_1^{(j)}, \ldots, x_n^{(j)}) \qquad\qquad (1 \leq j \leq m,\ 1 \leq k \leq n)$$

Exemple 3 (groupes diagonalisables). Avec les notations de 1.5, soit D un sous-groupe fermé de T_n ; soit $S \subseteq \mathbf{Z}^n$ le semi-groupe associé, et soit $C \subseteq \mathbf{R}^n$ le cône convexe fermé engendré par S. On suppose que C est simplicial, c'est-à-dire engendré par des demi-droites $d_1, \ldots, d_N$ dont les directions sont linéairement indépendantes ; cette hypothèse est vérifiée si D est fini (exercice). On note alors γ_i l'unique générateur du semi-groupe $d_i \cap \mathbf{Z}^n$, et a_i le monôme de $\mathbf{C}[x_1, \ldots, x_n]$ d'exposant γ_i. Alors les monômes $a_1, \ldots, a_N$ forment un système de paramètres homogènes de l'algèbre $\mathbf{C}[V]^D$ (exercice).

Exemple 4 (invariants des formes binaires). Considérons l'action de $G = \mathrm{SL}_2$ dans V_d où d est un entier positif, divisible par 4. L'application

$$\begin{array}{ccc} V_d \times V_{d-2} & \to & V_{d-2} \\ (u, v) & \to & (u, v)_{d/2} \end{array}$$

(voir 2.4 pour la définition de $(u, v)_n$) identifie V_d à un sous-G-module de $End(V_{d-2})$ dans lequel G opère par conjugaison. Chaque $u \in V_d$ définit un endomorphisme de V_{d-2} ; notons $a_1(u), \ldots, a_{d-1}(u)$ les coefficients du polynôme caractéristique de cet endomorphisme. Alors $a_1, \ldots, a_{d-1}$ sont des invariants de V_d de degré égal à leur indice, donc la trace a_1 est nulle sur V_d.

On conjecture (voir [Di] et [Li-Pr]) que $(a_2, \ldots, a_{d-1})$ est un système de paramètres homogènes de l'algèbre $\mathbf{C}[V_d]^G$. Cette conjecture est démontrée pour $d = 4$ et pour $d = 8$; vérifions-la pour $d = 4$.

Observons que V_2 est muni d'une forme quadratique non dégénérée et invariante par G : le discriminant. De plus, l'image de V_4 dans $End(V_2)$ consiste en les endomorphismes symétriques pour cette forme, et de trace nulle (exercice). Il existe de tels endomorphismes u pour lesquels $a_2(u)$ et $a_3(u)$ ne sont pas nuls. D'après l'exemple 2 en 3.2, on conclut que a_2 et a_3 engendrent l'algèbre $\mathbf{C}[V_4]^G$.

On revient au cas d'un groupe réductif quelconque G ; on va caractériser les G-modules dont tous les modules de covariants sont de Cohen-Macaulay.

Proposition 2. *Pour un groupe réductif G et un G-module V, les conditions suivantes sont équivalentes :*

(i) Toutes les fibres du quotient $\pi : V \to V//G$ ont la même dimension.

(ii) La codimension de $\mathcal{N}(V)$ dans V est la dimension de $V//G$.

(iii) Tout module de covariants de V est de Cohen-Macaulay.

Démonstration. (i)⇒(ii) Puisque π est dominante, la codimension de la fibre générale de π est la dimension de $V//G$.

(ii)⇒(iii) Soit $(a_1, \ldots, a_n)$ un système de paramètres homogènes de $\mathbf{C}[V]^G$; alors $n = \dim(V//G)$. D'après la proposition 1 ci-dessus, l'ensemble des zéros communs à $a_1, \ldots, a_n$ est le nilcône ; d'après l'hypothèse, ce dernier est de codimension n dans V. Il en résulte que la suite $(a_1, \ldots, a_n)$ est régulière dans $\mathbf{C}[V]$ (voir [Ei] §18.2), donc le $\mathbf{C}[a_1, \ldots, a_n]$-module gradué $\mathbf{C}[V]$ est libre.

Soit V_ω un G-module rationnel simple. D'après 2.3, le $\mathbf{C}[V]^G$ module $\mathbf{C}[V]$ contient un facteur direct isomorphe à $\mathrm{Mor}^G(V, V_\omega) \otimes V_\omega$. En particulier, le $\mathbf{C}[a_1, \ldots, a_n]$-module $\mathrm{Mor}^G(V, V_\omega)$ est facteur direct du module libre gradué $\mathbf{C}[V]$, d'où l'assertion.

(iii)⇒(ii) s'obtient en renversant les arguments précédents.

(ii)⇒(i) Pour $v \in V$ non dans le nilcône, notons C l'image par $\pi : V \to V//G$ de la droite vectorielle engendrée par v. Alors toutes les fibres de π au-dessus de $C \setminus \pi(0)$ sont isomorphes à la fibre de π en v. D'après le théorème de semi-continuité de la dimension des fibres d'un morphisme, on a donc

$$\dim \pi^{-1}(\pi(v)) \leq \dim \pi^{-1}(\pi(0)) .$$

D'autre part, on a aussi

$$\dim \pi^{-1}(\pi(v)) \geq \dim(V) - \dim(V//G) = \dim \mathcal{N}(V)$$

d'où le résultat.

Cette proposition conduit à une caractérisation des G-modules pour lesquels tous les modules de covariants sont libres.

Corollaire. *Pour un groupe réductif G et un G-module V (rationnel et de dimension finie), les conditions suivantes sont équivalentes :*

(i) La codimension du nilcône dans V est la dimension de $V//G$, et de plus $\mathbf{C}[V]^G$ est une algèbre de polynômes.

(ii) Le $\mathbf{C}[V]^G$-module $\mathbf{C}[V]$ est libre.

(iii) Tout module de covariants de V est libre.

Démonstration. (i)$\Rightarrow$(ii) résulte de la proposition ci-dessus et du fait qu'un module gradué de Cohen-Macaulay sur une algèbre graduée de polynômes est libre.

(ii)$\Leftrightarrow$(iii) se démontre comme pour la proposition ci-dessus.

(iii)$\Rightarrow$(i) Le $\mathbf{C}[V]$-module trivial (quotient de $\mathbf{C}[V]$ par son idéal maximal homogène) admet une résolution libre finie, donnée par le complexe de Koszul (voir [Ei] §17.2, ou 4.3 ci-dessous). Puisque $\mathbf{C}[V]$ est libre sur $\mathbf{C}[V]^G$, ce complexe est aussi une résolution libre finie du $\mathbf{C}[V]^G$-module trivial. D'après [Ei] §19.3, il en résulte que l'algèbre $\mathbf{C}[V]^G$ est engendrée par des éléments $a_1, \ldots, a_n$ homogènes et algébriquement indépendants. Alors $\mathbf{C}[V]$ est libre sur $\mathbf{C}[a_1, \ldots, a_n]$ donc la suite $(a_1, \ldots, a_n)$ est régulière dans $\mathbf{C}[V]$. Ceci entraîne que la codimension de $\mathcal{N}(V)$ (qui est l'ensemble des zéros communs à $a_1, \ldots, a_n$) est égale à n.

Définitions. Le G-module V est dit

- *équidimensionnel* si toutes les fibres du quotient ont la même dimension,
- *corégulier* si $\mathbf{C}[V]^G$ est une algèbre de polynômes,
- *colibre* si le $\mathbf{C}[V]^G$-module $\mathbf{C}[V]$ est libre.

D'après le corollaire, colibre équivaut à équidimensionnel et corégulier. En fait, on conjecture qu'équidimensionnel implique colibre lorsque G est semi-simple (voir [Po-Vi] §8.7 et ses références). Une conjecture plus forte affirme que soit tous les modules de covariants sont de Cohen-Macaulay, soit un nombre fini seulement de ces modules sont de Cohen-Macaulay. On renvoie à [VdB] pour des résultats sur les modules de covariants liés à cette dernière conjecture.

Exemple 1 (les groupes finis). Pour un groupe fini G, tous les modules sont équidimensionnels. De plus, un G-module V est corégulier si et seulement s'il est colibre. Comme on verra en 4.2, ceci revient à dire que l'image de G dans $\mathrm{GL}(V)$ est engendrée par des pseudo-réflexions.

Exemple 2 (les formes binaires). On considère $G = \mathrm{SL}_2$ et $V = V_d$. La dimension du nilcône a été calculée dans l'exemple 1 en 3.3. On en déduit que V_d est équidimensionnel si et seulement si $d \leq 4$. Dans ce cas, on a vu que V_d est corégulier ; il est donc colibre. En fait, V_d n'est pas corégulier lorsque $d \geq 5$ (voir 4.5).

Exemple 3. Soit $G = \mathrm{SL}_n$ opérant dans la somme directe V de $n+1$ copies de $\mathbf{C}^n$. D'après la théorie classique des invariants, l'algèbre $\mathbf{C}[V]^G$ est engendrée par les $n+1$ éléments

$$(u_1, \ldots, u_{n+1}) \mapsto \det(u_1, \ldots, \hat{u_i}, \ldots, u_{n+1})$$

qui sont algébriquement indépendants. En identifiant V à l'espace des matrices $n \times (n+1)$, le nilcône est donc formé des matrices de rang $< n$. Par suite, $\mathcal{N}(V)$ est de codimension deux dans V, et le $\mathbf{C}[V]^G$-module $\mathbf{C}[V]$ n'est pas libre.

Dans cet exemple, on peut montrer qu'aucun module de covariants non trivial n'est libre. Vérifions-le pour le module $\mathrm{Mor}^G(V, \mathbf{C}^n)$. En effet, un ensemble minimal de générateurs pour ce module est formé des $n+1$ projections $a_i : V \to \mathbf{C}^n$. Mais ces dernières sont linéairement dépendantes sur l'algèbre des invariants, car

$$\sum_{i=1}^{n+1} ;(-1)^{i-1} ;\det(u_1, \ldots, \hat{u}_i, \ldots, u_{n+1}) u_i = 0 \ .$$

4. Séries de Hilbert et résolutions libres des algèbres d'invariants

4.1. *Séries de Hilbert ; la formule de Molien-Weyl*

Soit

$$A = \bigoplus_{n=0}^{\infty} A_n$$

une algèbre graduée de type fini sur $\mathbf{C}$, et soit

$$M = \bigoplus_{n=-\infty}^{\infty} M_n$$

un A-module gradué de type fini. Alors chaque M_n est un espace vectoriel de dimension finie sur $\mathbf{C}$. De plus, la série formelle

$$\sum_{n=-\infty}^{\infty} \dim(M_n)\, z^n$$

est le développement de Taylor à l'origine d'une fraction rationnelle $F_M(z)$: la *série de Hilbert* de M.

Par exemple, si A est une algèbre de polynômes en r indéterminées de degrés $d_1, \ldots, d_r$, alors

$$F_A(z) = \frac{1}{\prod_{i=1}^{r} (1 - z^{d_i})} \ .$$

Plus généralement, si $(a_1, \ldots, a_r)$ est un système de paramètres homogènes de M de degrés $d_1, \ldots, d_r$, alors il existe un polynôme $P(z)$ à coefficients entiers, tel que

$$F_M(z) = \frac{P(z)}{\prod_{i=1}^{r} (1 - z^{d_i})} \ .$$

De plus, $P(1)$ est le rang du $\mathbf{C}[a_1, \ldots, a_r]$-module M ; en particulier, $P(1) \neq 0$. Il en résulte que F_M a un pôle en $z = 1$ d'ordre égal à la dimension de M. Le "résidu"

$$e(M) := \lim_{z \to 1} (1-z)^r F_M(z) = \frac{P(1)}{\prod_{i=1}^{r} d_i}$$

est un invariant numérique de M, appelé sa *multiplicité*. Le rang du A-module M est égal à $e(M)/e(A)$ (exercice). Un autre invariant numérique de M est le degré de F_M, défini par

$$\deg(F_M) := \deg(P) - \sum_{i=1}^{r} d_i \ .$$

Si M et N sont des A-modules gradués de type fini, on a immédiatement

$$F_{M\oplus N}(z) = F_M(z) + F_N(z),\ F_{M\otimes N}(z) = F_M(z)F_N(z)$$

et aussi, pour tout entier q

$$F_{M(q)}(z) = z^{-q}F_M(z)$$

où $M(q)$ désigne le A-module M, gradué par $M(q)_n := M(n+q)$.

Lorsque le A-module M est de Cohen-Macaulay, il admet une base homogène comme module sur $\mathbf{C}[a_1,\ldots,a_r] := B$; soit $(e_1,\ldots,e_s)$ la suite ordonnée des degrés des éléments de cette base. Puisque $M = \oplus_{j=1}^s B(-e_j)$, on a :

$$(*) \qquad F_M(z) = \frac{\sum_{j=1}^s z^{e_j}}{\prod_{i=1}^r (1-z^{d_i})}$$

d'où

$$e(M) = \frac{s}{\prod_{i=}^r d_i} \text{ et } \deg(F_M) = e_s - \sum_{i=1}^r d_i\ .$$

Une écriture de F_M sous la forme $(*)$ est *représentative* si M admet un système de paramètres homogènes de degrés $d_1,\ldots,d_r$. Une telle écriture permet par exemple de majorer par e_s les degrés des générateurs du A-module M. Mais une écriture $(*)$ de F_M peut ne pas être représentative. En effet, soit

$$A = \mathbf{C}[X,Y,Z,T]/(XZ-Y^2)$$

où X, Y, Z sont de degré 1 et où T est de degré 2. Alors $F_A(z) = (1-z)^{-3}$ mais A n'est pas une algèbre de polynômes en 3 indéterminées de degré 1 (vérifier). Cette algèbre est isomorphe à l'algèbre des invariants du groupe $G \subset \mathrm{GL}_3$ engendré par les matrices diagonales $diag(-1,-1,1)$ et $diag(1,1,i)$. En effet, pour l'action naturelle de G dans $\mathbf{C}[x,y,z]$, l'algèbre des invariants est engendrée par $X = x^2$, $Y = xy$, $Z = y^2$, $T = z^4$ et toute relation entre ces générateurs est multiple de $XZ - Y^2$ (exercice).

Exemple. Si $F_A(z)$ admet une écriture représentative de la forme

$$\frac{1+z^e}{\prod_{i=1}^r (1-z^{d_i})}$$

alors il existe $b \in A_e$ tel que

$$A = \mathbf{C}[a_1,\ldots,a_r] \oplus \mathbf{C}[a_1,\ldots,a_r]b\ .$$

On a donc $b^2 = ub + v$ pour des éléments homogènes u, v de $\mathbf{C}[a_1,\ldots,a_r]$. Il en résulte aussitôt que

$$A = \mathbf{C}[a_1,\ldots,a_r,x]/(x^2-ux-v)\ .$$

Ceci permet de décrire les algèbres des invariants des formes binaires de degrés 5 et 6 (voir 4.5).

On considère maintenant l'algèbre des invariants pour une action linéaire d'un groupe réductif. La série de Hilbert de tout module de covariants est alors donnée par une formule, due à Molien (pour les groupes finis) et à Weyl (pour les groupes compacts).

Théorème. *Soient G un groupe réductif, U et V des G-modules rationnels de dimension finie, et $M = \mathrm{Mor}^G(V,U)$ le module des covariants de V à valeurs dans U. Alors*

$$F_M(z) = I(\chi_{M,z})$$

où $\chi_{M,z} \in \mathbf{C}[G](z)$ est défini par

$$\chi_{M,z}(g) = \frac{\chi_U(g)}{\det_V(1 - zg^{-1})} \ .$$

En particulier, lorsque G est fini d'ordre N, on a

$$F_M(z) = \frac{1}{N} \sum_{g \in G} \frac{\chi_U(g)}{\det_V(1 - zg^{-1})} \ .$$

Démonstration. On a

$$M = \bigoplus_{n=0}^{\infty} M_n$$

avec

$$M_n = (\mathbf{C}[V]_n \otimes U)^G \ .$$

Mais pour tout G-module E, la dimension de E^G est égale à

$$\langle 1, \chi_E \rangle = I(\chi_E)$$

d'après la proposition 2.3.2. D'où

$$\dim(M_n) = I(\chi_{\mathbf{C}[V]_n \otimes U}) = I(\chi_{\mathbf{C}[V]_n} \chi_U) \ .$$

Pour terminer la preuve de la première assertion, il suffit de vérifier que

$$\sum_{n=0}^{\infty} \chi_{\mathbf{C}[V]_n}(g) \, z^n = \frac{1}{\det_V(1 - zg^{-1})}$$

ou encore que, pour tout $g \in \mathrm{GL}(V)$, on a

$$\sum_{n=0}^{\infty} \mathrm{Tr}_{\mathbf{C}[V]_n}(g) \, z^n = \frac{1}{\det_V(1 - zg^{-1})} \ .$$

Soient $\lambda_1, \ldots, \lambda_d$ les valeurs propres de g (avec leurs multiplicités). Alors les valeurs propres de g opérant dans $\mathbf{C}[V]_n$ sont les monômes de degré n en $\lambda_1^{-1}, \ldots, \lambda_d^{-1}$ (exercice). On a donc

$$\sum_{n=0}^{\infty} \mathrm{Tr}_{\mathbf{C}[V]_n}(g) z^n = \sum_n z^n \sum_{n_1+\cdots+n_d=n} \lambda_1^{-n_1} \cdots \lambda_d^{-n_d}$$
$$= \prod_{i=1}^{d} \frac{1}{1 - z\lambda_i^{-1}} = \prod_{i=1}^{d} \frac{1}{\det_V(1 - zg^{-1})} \ .$$

Si de plus G est fini, alors $I = \frac{1}{N} \sum_{g \in G} g$ d'où la seconde assertion.

On va donner deux applications de la formule de Molien aux modules de covariants pour les groupes finis.

Proposition 1. *Soit $G \subset \mathrm{GL}(V)$ un sous-groupe fini.*
(i) Pour tout G-module U, le rang du module de covariants $\mathrm{Mor}^G(V, U)$ est égal à la dimension de U.
(ii) Tout G-module simple apparaît dans une puissance symétrique de V.

Démonstration. (i) Posons $A := \mathbf{C}[V]^G$ et $M := \mathrm{Mor}^G(V, U)$. D'après le théorème, on a :

$$e(A) = \lim_{z \to 1} (1 - z)^{\dim(V)} F_A(z) = 1/N$$

et de même $e(M) = \chi_U(1)/N = \dim(U)/N$. De plus, le rang du A-module M est $e(M)/e(A)$, d'où l'assertion.

(ii) Si U est simple, alors U^* apparaît dans $\mathbf{C}[V]$; en effet, $\mathrm{Mor}^G(V, U) \neq 0$ puisque sa multiplicité est non nulle. Ainsi, le G-module U apparaît dans l'algèbre symétrique de V.

Dans l'étude de la série de Hilbert au voisinage de $z = 1$, on est amené à considérer les éléments de G qui ont une valeur propre de multiplicité égale à $\dim(V) - 1$, d'où la

Définition. Un endomorphisme g d'un espace vectoriel V de dimension finie est une *pseudo-réflexion* si g est diagonalisable et si $g - id_V$ est de rang 1.

Autrement dit, on a $V = H \oplus \ell$ où H est l'hyperplan formé des points fixes de g, et où ℓ est une droite propre de g pour une valeur propre $\lambda(g) \neq 1$. Si de plus $\lambda(g) = -1$, on dit que g et une *réflexion*.

Proposition 2. *Soit V un espace vectoriel de dimension finie n ; soient $G \subset \mathrm{GL}(V)$ un groupe fini d'ordre N, et U un G-module.*
(i) La série de Hilbert du module de covariants $M = \mathrm{Mor}^G(V, U)$ admet un développement de Laurent en $z = 1$, de la forme

$$F_M(z) = \frac{\dim(U)}{N} \frac{1}{(1 - z)^n} + \frac{1}{N} \Big(\sum_{g \in \mathcal{PR}(G)} \frac{\chi_U(g)}{1 - \lambda(g)} \Big) \frac{1}{(1 - z)^{n-1}} + \cdots$$

où $\mathcal{PR}(G)$ désigne l'ensemble des pseudo-réflexions de G.
(ii) Pour $A = \mathbf{C}[V]^G$, on a

$$F_A(z) = \frac{1}{N}\frac{1}{(1-z)^n} + \frac{r}{2N}\frac{1}{(1-z)^{n-1}} + \cdots$$

où r désigne le nombre de pseudo-réflexions de G.
(iii) Si le A-module M est libre, et si G ne contient aucune pseudo-réflexion, alors G opère trivialement dans U.

Démonstration. (i) résulte aussitôt du théorème.

(ii) Observons que l'inverse d'une pseudo-réflexion est encore une pseudo-réflexion ; d'où

$$\sum_{g\in\mathcal{PR}(G)} \frac{1}{1-\lambda(g)} = \frac{1}{2}\sum_{g\in\mathcal{PR}(G)} \frac{1}{1-\lambda(g)} + \frac{1}{1-\lambda(g)^{-1}} = \frac{r}{2}\ .$$

(iii) Si le A-module M est libre, il admet une base formée d'éléments homogènes ; soient $e_1,\ldots,e_s$ leurs degrés. Puique s est le rang du A-module M, on a $s = \dim(U)$. De plus, on a

$$F_M(z) = (\sum_{i=1}^{s} z^{e_i})\, F_A(z) = \frac{s}{N}\frac{1}{(1-z)^n} + \frac{rs - 2(e_1+\cdots+e_s)}{2N}\frac{1}{(1-z)^{n-1}} + \cdots$$

Si de plus G ne contient aucune pseudo-réflexion, alors en comparant avec (i), on obtient $e_1+\cdots+e_s = 0$. Comme les e_i sont non négatifs, il en résulte que $e_1 = \ldots = e_s = 0$, et donc que G opère trivialement dans U.

Remarque. Revenons au cas d'un groupe réductif G. Lorsque G est connexe, la formule de Molien-Weyl, combinée avec la formule d'intégration de Weyl (voir [Br-tD]), exprime F_M par une intégrale sur un sous-tore compact maximal de G. Mais en rang au moins 2, cette intégrale est difficile à calculer ; voir [Br] pour une autre méthode de calcul de F_M. Lorsque $G = \mathrm{SL}_2$ et $V = V_d$, on donnera une formule explicite pour F_M en 4.5.

4.2. *Le cas des groupes finis engendrés par des pseudo-réflexions*

On va démontrer le résultat fondamental suivant, dû à Shephard-Todd et Chevalley.

Théorème. *Pour un sous-groupe fini G de* $\mathrm{GL}(V)$, *les conditions suivantes sont équivalentes :*
(i) G est engendré par des pseudo-réflexions.
(ii) Le $\mathbf{C}[V]^G$-module $\mathbf{C}[V]$ est libre.
(iii) L'algèbre $\mathbf{C}[V]^G$ est engendrée par des éléments homogènes algébriquement indépendants.

Démonstration. On pose $A := \mathbf{C}[V]^G$.

(i)$\Rightarrow$(ii) Soit I l'idéal de $\mathbf{C}[V]$ engendré par les invariants homogènes non constants. Montrons d'abord que si $\sum_{i=1}^m a_i f_i = 0$ avec des $a_i \in A_+$ et des $f_i \in \mathbf{C}[V]$ homogènes, alors $a_1 \in Aa_2 + \cdots + Aa_m$ ou $f_1 \in I$. On raisonne par récurrence sur le degré d de f_1. Si $d = 0$, alors $a_1 \in \mathbf{C}[V]a_2 + \cdots + \mathbf{C}[V]a_m$ d'où en appliquant l'opérateur de Reynolds : $a_1 \in Aa_2 + \cdots + Aa_m$. Si $d > 0$, soit $g \in G$ une pseudo-réflexion, et soit $\ell_g \in V^*$ une équation de l'hyperplan des points fixes de g. Pour tout $f \in \mathbf{C}[V]$, la différence $f - g \cdot f$ est divisible par ℓ_g. On peut donc définir un endomorphisme D_g de l'espace vectoriel $\mathbf{C}[V]$ par

$$D_g(f) = \frac{f - g \cdot f}{\ell_g} \ .$$

Cet endomorphisme est A-linéaire et de degré -1. On a :

$$\sum_{i=1}^m a_i D_g(f_i) = D_g(\sum_{i=1}^m a_i f_i) = 0$$

d'où, par hypothèse de récurrence : $a_1 \in Aa_2 + \cdots Aa_m$ ou $D_g(f_1) \in I$. Dans ce dernier cas, $g \cdot f_1 - f_1 \in I$. Si ce cas se produit pour toutes les pseudo-réflexions g, alors, comme celles-ci engendrent le groupe G, l'image de f_1 dans $\mathbf{C}[V]/I$ est un invariant de G. Mais l'espace vectoriel $(\mathbf{C}[V]/I)^G = \mathbf{C}[V]^G/I^G$ est engendré par l'image de 1, et f_1 est homogène de degré $d > 0$, donc $f_1 \in I$.

Soient maintenant $f_1, \ldots, f_m$ une partie d'un système générateur minimal du A-module $\mathbf{C}[V]$, formé d'éléments homogènes. Montrons par récurrence sur m que $f_1, \ldots, f_m$ sont linéairement indépendants sur A. En effet, soient $a_1, \ldots, a_m \in A$ tels que $a_1 f_1 + \cdots + a_m f_m = 0$. Puisque les f_i sont homogènes, on peut supposer que les a_i le sont aussi. Comme $f_1 \notin I$, on a $a_1 \in Aa_2 + \cdots + Aa_m$. Écrivons $a_1 = u_2 a_2 + \cdots + u_m a_m$ avec des u_i dans A homogènes. Alors

$$a_2(f_2 + u_2 f_1) + \cdots + a_m(f_m + u_m f_1) = 0$$

et $f_2 + u_2 f_1, \ldots, f_m + u_m f_1$ font partie d'un système minimal de générateurs homogènes du A-module $\mathbf{C}[V]$. On conclut par l'hypothèse de récurrence.

(ii)$\Rightarrow$(iii) résulte du corollaire 3.5.

(iii)$\Rightarrow$(i) Soient $a_1, \ldots, a_n$ des générateurs homogènes et algébriquement indépendants de l'algèbre A, de degrés respectifs $d_1, \ldots, d_n$. La série de Hilbert de A est alors

$$F_A(z) = \prod_{i=1}^n \frac{1}{1 - z^{d_i}} \ .$$

D'après la proposition 4.1 (ii), on a $N = d_1 \cdots d_n$ et $r = d_1 + \cdots + d_n - n$. Puisque G opère fidèlement dans V, l'un des d_i est au moins 2 ; il en résulte que G contient des pseudo-réflexions. Soit G' le sous-groupe de G engendré par ses pseudo-réflexions, et soit $A' = \mathbf{C}[V]^{G'}$. Par l'implication (i)$\Rightarrow$(iii), l'algèbre

A' est engendrée par des éléments homogènes et algébriquement indépendants $a'_1, \cdots, a'_n$; notons $d'_1, \ldots, d'_n$ leurs degrés. On peut supposer $d_1 \leq \cdots \leq d_n$ et $d'_1 \leq \cdots \leq d'_n$. Puisque $A \subseteq A'$ on peut écrire $a_i = P_i(a'_1, \ldots, a'_n)$ pour un unique $P_i \in \mathbf{C}[X_1, \ldots, X_n]$; alors P_i est homogène pour la graduation où chaque X_i est de degré d'_i. Puisque $a_1, \ldots, a_i$ sont algébriquement indépendants, P_i n'est pas dans $\mathbf{C}[X_1, \ldots, X_{i-1}]$ et donc $d_i \geq d'_i$. Mais le nombre de pseudo-réflexions de G et de G' est

$$d_1 + \cdots + d_n - n = d'_1 + \cdots + d'_n - n \ .$$

On en déduit que $d_i = d'_i$ pour tout i, puis que $F_A(z) = F_{A'}(z)$. Mais comme $A \subseteq A'$, ceci entraîne que $A = A'$.

Définition. Un sous-groupe fini $G \subset \mathrm{GL}_n$ engendré par des pseudo-réflexions est appelé *groupe de pseudo-réflexions*.

La suite croissante $(d_1, \ldots, d_n)$ des degrés d'un système génerateur minimal, formé d'éléments homogènes, de l'algèbre $\mathbf{C}[x_1, \ldots, x_n]^G$ est la suite des *degrés caractéristiques*.

D'après le lemme 4.1, on a alors

$$d_1 + \cdots + d_n = n + r, \ \ d_1 \ldots d_n = N$$

où r est le nombre de pseudo-réflexions dans G, et où N est son ordre.

Exemple 1 (le groupe symétrique). Soit $G = S_n$ opérant dans $\mathbf{C}^n$ par permutations des coordonnées. Chaque transposition (ij) a pour point fixe l'hyperplan $(x_i = x_j)$, et sa valeur propre non triviale est -1 ; c'est donc une réflexion. Puisque G est engendré par les transpositions, c'est un groupe de réflexions. L'algèbre $\mathbf{C}[x_1, \ldots, x_n]^G$ est engendrée par les fonctions symétriques élémentaires, donc les degrés caractéristiques sont $1, 2, \ldots, n$. On en déduit que $r = n(n-1)/2$, puis que les pseudo-réflexions de G sont exactement les transpositions (le vérifier directement).

Exemple 2 (la représentation adjointe). Soient G un groupe réductif connexe, $T \subseteq G$ un tore maximal, N son normalisateur dans G, et $W = N/T$ le groupe de Weyl. Celui-ci opère dans T et dans son algèbre de Lie t. Pour cette action, le groupe W est engendré par des réflexions (voir [Hu]). Ainsi, $\mathbf{C}[t]^W$ est engendrée par r éléments homogènes et algébriquement indépendants, où $r = \dim(t) = \dim(T)$ est le *rang* de G. D'après l'exemple 1 en 3.2, l'algèbre $\mathbf{C}[g]^G$ est isomorphe à $\mathbf{C}[t]^W$ où g désigne l'algèbre de Lie de G. De plus, le nilcône de g est formé de ses éléments nilpotents ; il est de codimension r dans g (voir [Ste1] 3.6). Grâce au corollaire 3.6, on en déduit que le G-module g est colibre.

On va maintenant étudier de plus près la structure du $\mathbf{C}[V]^G$-module $\mathbf{C}[V]$ lorsque $G \subset \mathrm{GL}(V)$ est un groupe de pseudo-réflexions. Plus généralement, on a le résultat suivant, dû à Stanley.

Proposition. *Soit $G \subset GL(V)$ un sous-groupe fini ; soit $(a_1, \ldots, a_n)$ un système de paramètres homogènes de l'algèbre $\mathbf{C}[V]^G$ et soient $d_1, \ldots, d_n$ leurs degrés respectifs.*

(i) Il existe un sous-G-module gradué $\mathcal{H} \subseteq \mathbf{C}[V]$ tel que l'application

$$\begin{array}{ccc} \mathbf{C}[a_1, \ldots, a_n] \otimes \mathcal{H} & \to & \mathbf{C}[V] \\ p \otimes q & \to & pq \end{array}$$

est un isomorphisme.

(ii) Le rang du $\mathbf{C}[a_1, \ldots, a_n]$-module $\mathbf{C}[V]^G$ est égal à

$$\mu := \frac{d_1 \cdots d_n}{N}$$

où N désigne l'ordre de G.

(iii) La représentation de G dans $\mathcal{H}$ est isomorphe à la somme directe de μ copies de la représentation régulière de G.

Démonstration. (i) Puisque $\mathbf{C}[V]$ est complètement réductible, il existe un sous-G-module gradué $\mathcal{H} \subseteq \mathbf{C}[V]$ tel que la restriction à $\mathcal{H}$ de l'application quotient

$$\mathbf{C}[V] \to \mathbf{C}[V]/(\mathbf{C}[V]a_1 + \cdots + \mathbf{C}[V]a_m)$$

est un isomorphisme. D'après le lemme de Nakayama, l'application

$$\mathbf{C}[a_1, \ldots, a_n] \otimes \mathcal{H} \to \mathbf{C}[V]$$

est alors surjective. Mais comme le $\mathbf{C}[a_1, \ldots, a_n]$-module $\mathbf{C}[V]$ est libre, cette application est un isomorphisme.

(ii) On a

$$\begin{aligned} d_1 \cdots d_n = \dim(\mathcal{H}) &= \mathrm{rg}_{\mathbf{C}[a_1,\ldots,a_n]} \mathbf{C}[V] \\ &= \mathrm{rg}_{\mathbf{C}[V]^G} \mathbf{C}[V] \, \mathrm{rg}_{\mathbf{C}[a_1,\ldots,a_n]} \mathbf{C}[V]^G = N \, \mathrm{rg}_{\mathbf{C}[a_1,\ldots,a_n]} \mathbf{C}[V]^G \ . \end{aligned}$$

(iii) Soit U un G-module simple. Le module de covariants $\mathrm{Mor}^G(V, U)$ est de rang $\dim(U)$ sur $\mathbf{C}[V]^G$, donc de rang $\mu \dim(U)$ sur $\mathbf{C}[a_1, \ldots, a_n]$. Mais on a :

$$\mathrm{Mor}^G(V, U) = (\mathbf{C}[V] \otimes U)^G = \mathbf{C}[a_1, \ldots, a_n] \otimes (\mathcal{H} \otimes U)^G \ .$$

Ainsi, la multiplicité de U^* dans $\mathcal{H}$ est égale à $\mu \dim(U)$, d'où le résultat.

Corollaire. *Soit $G \subset \mathrm{GL}(V)$ un groupe de pseudo-réflexions. Il existe un sous-G-module gradué $\mathcal{H} \subseteq \mathbf{C}[V]$, isomorphe à la représentation régulière de G, tel que la multiplication dans V induit un isomorphisme*

$$\mathbf{C}[V]^G \otimes \mathcal{H} \to \mathbf{C}[V] \ .$$

4.3. *Résolutions libres*

Pour décrire une algèbre A (graduée et de type fini) par générateurs et relations, on en choisit un système générateur minimal formé d'éléments homogènes de degrés respectifs $d_1, \ldots, d_r$. Soit $R = \mathbf{C}[x_1, \ldots, x_r]$ l'algèbre graduée des polynômes en r variables de degrés $d_1, \ldots, d_r$. L'algèbre A est le quotient de R par un idéal homogène I (l'idéal des relations). Soient $f_1, \ldots, f_s$ des générateurs homogènes de I, en nombre minimal ; alors

$$A = \mathbf{C}[x_1, \ldots, x_r]/(f_1, \ldots, f_s)$$

est la description cherchée.

Mais si $s \geq 1$, les relations $f_1, \ldots, f_s$ vérifient d'autres relations. Plus précisément, I est le quotient du R-module libre gradué $L_1 = \oplus_{i=1}^s Re_i$ (où chaque e_i est homogène de même degré que f_i) par un sous-module gradué N_1. De plus, N_1 contient les éléments

$$e_{ij} := f_j e_i - f_j e_i$$

pour $1 \leq i < j \leq s$. On a donc une suite exacte de R-modules gradués

$$0 \to N_1 \to L_1 \to R \to A \to 0.$$

En présentant N_1 comme quotient d'un R-module libre gradué L_2, on obtient une suite exacte

$$0 \to N_2 \to L_2 \to L_1 \to R \to A \to 0$$

et on peut itérer cette construction.

Si de plus la suite $(f_1, \ldots, f_s)$ est régulière dans R, alors les e_{ij} forment un système générateur minimal du R-module N_1 (exercice). De plus, on a les relations

$$f_i e_{jk} - f_j e_{ik} + f_k e_{ij} = 0$$

pour $1 \leq i < j < k \leq s$ (vérifier) qui définissent donc des éléments e_{ijk} de N_2. Ces constructions conduisent aux

Définitions. Soient

$$R = \bigoplus_{n=0}^{\infty} R_n$$

une algèbre graduée et de type fini sur $\mathbf{C}$, et

$$M = \bigoplus_{n=-\infty}^{\infty} M_n$$

un R-module gradué. Une *résolution libre graduée* de M est une suite exacte de R-modules

$$\cdots \to L_m \to L_{m-1} \to \cdots \to L_1 \to L_0 \to M \to 0$$

où les L_m sont des R-modules libres gradués, et où chaque application $u_m : L_m \to L_{m-1}$ préserve le degré.

La *longueur* de la résolution est le plus petit m_0 tel que $L_m = 0$ pour tout $m > m_0$ si un tel m_0 existe, et l'infini sinon.

Une résolution est *minimale* si chaque base de L_m relève un système générateur minimal du R-module $\mathrm{Im}(u_m) = \mathrm{Ker}(u_{m-1})$.

Si $f_1, \ldots, f_s$ sont des éléments homogènes de R, le *complexe de Koszul* $K(f_1, \ldots, f_s)$ est le complexe

$$0 \to R^{(s)} \to \cdots \to R^{(m)} \to R^{(m-1)} \to \cdots \to R^{(1)} \to R^{(0)} \to 0$$

où chaque $R^{(m)}$ est un R-module libre gradué admettant pour base $(e_{i_1 \ldots i_m})$ $(1 \leq i_1 < \cdots < i_m \leq s)$ tels que $\deg(e_{i_1 \ldots i_m}) = \deg(e_{i_1}) + \cdots + \deg(e_{i_m})$, et où la différentielle

$$d_m : R^{(m)} \to R^{(m-1)}$$

est l'application R-linéaire telle que

$$d_m(e_{i_1 \cdots i_m}) = \sum_{j=1}^{m} (-1)^{j-1} f_j e_{i_1 \cdots \hat{i}_j \cdots i_m} \; .$$

En particulier, on a $R^{(1)} = \oplus_{i=1}^{s} R(\deg(f_j))$, $R^{(0)} = R$ et l'image de la différentielle $d_1 : R^{(1)} \to R^{(0)}$ est l'idéal engendré par $f_1, \ldots, f_s$.

On montre facilement que tout R-module M, gradué et de type fini, admet une résolution minimale. De plus, tous les modules libres gradués L_m qui y figurent sont de rang fini, et la suite des degrés d'une base homogène de L_m ne dépend que de m et de M (mais les applications u_m ne sont pas uniques en général). Par abus de langage, on parlera désormais de la résolution minimale de M.

Dans le cas d'une algèbre A, quotient de R par l'idéal engendré par $f_1, \ldots, f_s$, on montre que le complexe de Koszul $K(f_1, \ldots, f_s)$ est une résolution de A si et seulement si la suite $(f_1, \ldots, f_s)$ est régulière dans R ; alors ce complexe de Koszul est la résolution minimale (voir [Ei] §19.1). On dit alors que A est une *intersection complète*. Si de plus $s = 1$ (c'est-à-dire A vérifie une "unique" relation), on dit que A est une *hypersurface*.

Soit R une algèbre graduée de polynômes, et soit M un R-module gradué et de type fini. D'après des théorèmes de Hilbert et d'Auslander-Buchsbaum (voir [Ei] §§19.2 et 19.3), la longueur de la résolution minimale de M est finie, et égale à $\dim(R) - \mathrm{prof}(M)$ où $\mathrm{prof}(M)$ désigne la profondeur de M.

Réciproquement, si R est une algèbre graduée de type fini telle que le module trivial $\mathbf{C} = R/R_+$ admet une résolution libre de longueur finie, alors R est une algèbre de polynômes (voir [Ei] §19.3).

Observons que la série de Hilbert de M se lit sur sa résolution minimale. Plus précisément, écrivons $R = \mathbf{C}[x_1, \ldots, x_r]$ où chaque x_i est homogène de degré d_i. Pour tout $m \geq 0$, notons $(d_{i,m})_{i \in I_m}$ la suite des degrés d'une base homogène du R-module L_m. On a immédiatement :

$$F_M(z) = \frac{\sum_{m \geq 0} (-1)^m \sum_{i \in I_m} z^{d_{i,m}}}{\prod_{i=1}^r (1 - z^{d_i})} .$$

Lorsque $A = \mathbf{C}[x_1, \ldots, x_r]/(f_1, \ldots, f_s)$ est une intersection complète, on a

$$F_A(z) = \frac{\prod_{j=1}^s (1 - z^{\delta_j})}{\prod_{i=1}^r (1 - z^{d_i})}$$

où d_i (resp. δ_j) désigne le degré de x_i (resp. f_j).

Les résultats ci-dessus et le théorème de Hochster-Roberts impliquent aussitôt le

Théorème. *Soient G un groupe réductif et V un G-module rationnel de dimension finie ; soit r le nombre minimal de générateurs homogènes de l'algèbre $\mathbf{C}[V]^G$. Alors la résolution minimale du $\mathbf{C}[x_1, \ldots, x_r]$-module $\mathbf{C}[V]^G$ est de longueur $r - \dim(V//G)$.*

Exemple 1. Soit $G \subset \mathrm{GL}(3)$ le sous-groupe engendré par les matrices diagonales $diag(-1, 1, -1)$ et $diag(-1, \zeta, \zeta^2)$ où ζ est une racine de l'unité d'ordre 6. Alors G est d'ordre 12 et l'algèbre $A = \mathbf{C}[x, y, z]^G$ est engendrée minimalement par $X = x^2$, $Y = xyz$, $Z = y^6$, $T = y^2 z^2$, $U = z^6$. De plus, les relations sont engendrées minimalement par $XT - Y^2$ et $ZU - T^3$ (exercice). Par suite, A est intersection complète et sa résolution minimale est de la forme

$$0 \to R(14) \to R(8) \oplus R(6) \to R \to A \to 0$$

où $R = \mathbf{C}[X, Y, Z, T, U]$.

Exemple 2. Soit G le groupe des racines N-ièmes de l'unité, opérant dans $V = \mathbf{C}^2$ par multiplication. Le monômes $x^N, x^{N-1}y, \ldots, y^N$ forment un système générateur minimal de l'algèbre $A = \mathbf{C}[V]^G$. On a donc $r = N + 1$ et $\dim(V//G) = 2$: la résolution minimale de A est de longueur $N - 1$.

En écrivant $A = R/I$ où $R = \mathbf{C}[x_1, \ldots, x_{N+1}]$, l'idéal I a pour système minimal de générateurs l'ensemble des mineurs 2×2 de la matrice

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_N \\ x_2 & x_3 & \cdots & x_{N+1} \end{pmatrix}$$

(exercice). Le nombre de ces générateurs est $N(N-1)/2$ donc ils ne forment pas une suite régulière pour $N \geq 3$. D'autre part, lorsque $N = 2$, on a

$$A = \mathbf{C}[x_1, x_2, x_3]/(x_1x_3 - x_2^2).$$

Ainsi, A est une intersection complète si et seulement si $N = 2$.

Lorsque $N = 3$, l'idéal I est engendré par

$$\Delta_1 = x_2x_4 - x_3^2,\ \Delta_2 = x_1x_4 - x_2x_3,\ \Delta_3 = x_1x_3 - x_2^2$$

et ceux-ci vérifient les relations

$$x_1\Delta_1 - x_2\Delta_2 + x_3\Delta_3 = 0,\ x_2\Delta_1 - x_3\Delta_2 + x_4\Delta_4 = 0\ .$$

On obtient donc un complexe

$$(*) \qquad 0 \to R(9)^2 \to R(6)^3 \to R \to A \to 0$$

où $u : R(9)^2 \to R(6)^3$ est donnée par la matrice

$$\begin{pmatrix} x_1 & x_2 \\ -x_2 & -x_3 \\ x_3 & x_4 \end{pmatrix}$$

De plus, le complexe $(*)$ est exact, sauf peut-être en $R(6)^3$. Mais la série de Hilbert de A est donnée par

$$F_A(z) = \frac{1 + 2z^3}{(1 - z^3)^2} = \frac{1 - 3z^6 + 2z^{12}}{(1 - z^3)^4}\ .$$

Il en résulte que l'homologie de $(*)$ a une série de Hilbert nulle, et donc que $(*)$ est la résolution minimale de A.

4.4. *Module canonique et propriété de Gorenstein*

Soit A une algèbre graduée et de type fini. Le choix d'un système minimal de générateurs homogènes de A permet d'écrire $A = R/I$ où R est une algèbre graduée de polynômes. Soit alors

$$0 \to L_c \to L_{c-1} \to \cdots \to L_1 \to L_0 = R \to A \to 0$$

la résolution minimale du R-module A. Considérons le complexe dual

$$(*) \qquad 0 \to L_0^* \to L_1^* \to \cdots \to L_{c-1}^* \to L_c^* \to 0$$

où chaque $L_m^* = \mathrm{Hom}_R(L_m, R)$ est un R-module libre gradué. Lorsque A est de Cohen-Macaulay, on a vu que $c = r - \dim(A)$. On montre que le complexe

$(*)$ est exact sauf en L_c^* et que le R-module $L_c^*/\mathrm{Im}(L_{c-1}^*)$ est annulé par I ; c'est donc un A-module, gradué et de type fini.

Définition. Le *module canonique* de A est le A-module

$$\omega_A = (L_c^*/\mathrm{Im}(L_{c-1}^*))(-d_1 - \cdots - d_r)$$

(rappelons que pour tout A-module gradué M, on désigne par $M(q)$ le A-module M gradué par $M(q)_n = M(n+q)$).

Observons que la série de Hilbert de ω_A est donnée par

$$F_{\omega_A}(t) = (-1)^{\dim(A)} F_A(t^{-1}) \ .$$

En effet, puisque $(*)$ est exact, on a

$$\begin{aligned} F_{L_c^*/\mathrm{Im}(L_{c-1}^*)}(t) &= \sum_{m=0}^{c} (-1)^m \, F_{L_{c-m}^*}(t) \\ &= \frac{\sum_{m=0}^{c} (-1)^{c-m} \, \sum_{i \in I_m} \, t^{-d_{i,m}}}{\prod_{i=1}^{r} (1-t^{d_i})} = (-1)^{r-c} \, t^{-d_1 - \cdots - d_r} \, F_A(t) \ . \end{aligned}$$

Définition. Une algèbre graduée A, de type fini et de Cohen-Macaulay, est *de Gorenstein* s'il existe un entier q tel que $\omega_A \simeq A(-q)$ comme A-module gradué.

Si A est de Gorenstein, alors

$$F_A(z^{-1}) = (-1)^{\dim(A)} \, z^q \, F_A(z)$$

d'où $q = -\deg(F_A)$. Réciproquement, on montre que toute algèbre de Cohen-Macaulay dont la série de Hilbert vérifie une telle équation, est de Gorenstein ; voir [Ei] §21.12. De plus, la résolution minimale d'une algèbre de Gorenstein est auto-duale, c'est-à-dire :

$$L_m^* \simeq L_{c-m}(q)$$

comme R-modules gradués.

Exemple 1. Soit $A = \mathbf{C}[x_1, \ldots, x_r]/(f_1, \ldots, f_s)$ une intersection complète. Le complexe de Koszul donne alors un isomorphisme

$$\omega_A \simeq A(-d_1 - \cdots - d_r + \delta_1 + \cdots + \delta_s)$$

où d_i (resp. δ_j) est le degré de x_i (resp. f_j). Il en résulte que toute intersection complète est de Gorenstein (l'auto-dualité de la résolution minimale se voit alors sur le complexe de Koszul). La réciproque est fausse en général ; des exemples seront donnés ci-dessous.

Exemple 2. Soit A l'algèbre des invariants du groupe des racines cubiques de l'unité, opérant par multiplication dans $\mathbf{C}^2$. Alors A n'est pas de Gorenstein, d'après la forme de sa résolution minimale donnée en 4.3 (exercice : décrire ω_A). Ceci résulte aussi du

Théorème. *Soient G un groupe réductif et V un G-module rationnel de dimension finie. L'algèbre $\mathbf{C}[V]^G$ est de Gorenstein si tout caractère multiplicatif de G est trivial, ou si G est fini et si $\det_V(g) = 1$ pour tout $g \in G$. Réciproquement, si $\mathbf{C}[V]^G$ est de Gorenstein et si $G \subset \mathrm{GL}(V)$ est fini et ne contient aucune pseudo-réflexion, alors $\det_V(g) = 1$ pour tout $g \in G$.*

Démonstration. Si tout caractère multiplicatif de G est trivial, alors l'algèbre $A = \mathbf{C}[V]^G$ est factorielle (exercice). Comme elle est de Cohen-Macaulay, elle est de Gorenstein d'après [Ei] §21.12.

Soit $G \subset \mathrm{GL}(V)$ un sous-groupe fini d'ordre N ; notons n la dimension de V. Si $\det_V(g) = 1$ pour tout $g \in G$, alors on a d'après le théorème 4.1 :

$$F_A(z^{-1}) = \frac{1}{N} \sum_{g \in G} \frac{1}{\det_V(1 - z^{-1}g^{-1})} = (-z)^n F_A(z)$$

donc A est de Gorenstein. Réciproquement, si A est de Gorenstein, alors il existe $q \in \mathbf{Z}$ tel que

$$\sum_{g \in G} \frac{1}{\det_V(1 - z^{-1}g^{-1})} = (-1)^n \, z^q \sum_{g \in G} \frac{1}{\det_V(1 - zg^{-1})} \ .$$

Si de plus G ne contient aucune pseudo-réflexion, alors en considérant le coefficient de $(1 - z)^{-n+1}$ dans le développement de Laurent en $z = 1$ des deux membres, on obtient $q = n$. Puis, en faisant tendre z vers l'infini, on obtient

$$N = (-1)^n \sum_{g \in G} \frac{1}{\det_V(-g^{-1})} = \sum_{g \in G} \det_V(g) \ .$$

Puisque chaque $\det_V(g)$ est une racine de l'unité, ceci entraîne que $\det_V(g) = 1$ pour tout $g \in G$.

La propriété de Gorenstein pour une algèbre d'invariants est très utile pour décrire sa résolution minimale : grâce à l'auto-dualité de cette résolution, il suffit d'en calculer la moitié.

Exemple 3. Soit $G = \mathrm{SL}_2$ opérant diagonalement dans le produit V_1^d de d copies de V_1. Rappelons que les

$$[ij] = \det(f_i, f_j) \qquad (1 \le i < j \le d)$$

forment un système générateur minimal de l'algèbre $A = \mathbf{C}[V]^G$, et que les "relations de Plücker"

$$f_{ijkl} := [ij][kl] - [ik][jl] + [il][jk] \qquad (1 \le i < j < k < l \le d)$$

forment un système générateur minimal de l'idéal des relations. De plus, la dimension de $V_1^d//G$ est égale à $2d-3$ d'après le corollaire 3.1. On en déduit que la longueur de la résolution minimale de A est $(d-2)(d-3)/2$; en outre, cette résolution est auto-duale d'après la proposition ci-dessus.

Si $d \leq 3$ alors A est une algèbre de polynômes ; si $d = 4$, l'idéal des relations est engendré par l'unique relation de Plücker, et donc A est une hypersurface. Pour $d \geq 5$, l'algèbre A n'est pas une intersection complète ; pour $d = 5$, sa résolution minimale est de la forme

$$0 \to R(-q) \to R(-q+4)^5 \to R(-4)^5 \to R \to A \to 0$$

où R est l'algèbre des polynômes en 10 indéterminées de degré 2, et où q est un entier. D'autre part, les f_{ijkl} satisfont des relations de degré 6, par exemple

$$[15]f_{1234} - [14]f_{1235} + [13]f_{1245} - [12]f_{1345} = 0$$

(vérifier). Il en résulte que $q = 10$ et que les relations entre les f_{ijkl} sont engendrées par les 5 relations de la forme ci-dessus.

Énonçons enfin une autre conséquence de la propriété de Gorenstein. Soit A une algèbre graduée et de type fini ; soit $\overline{A}$ le quotient de A par l'idéal engendré par un système de paramètres homogènes $(a_1, \ldots, a_n)$. Alors $\overline{A}$ est une algèbre graduée, de dimension finie comme espace vectoriel complexe ; il existe donc un plus grand entier N tel que $\overline{A}_N \neq 0$. Lorsque A est de Gorenstein, on montre que l'espace vectoriel $\overline{A}_N$ est de dimension 1, et que la multiplication

$$\overline{A}_n \times \overline{A}_{N-n} \to \overline{A}_N$$

définit une forme bilinéaire non dégénérée pour $0 \leq n \leq N$ (voir [Ei] §21.12). En notant d_i le degré de a_i et $(0 = e_1, e_2 \ldots, e_s)$ la suite ordonnée des degrés d'une base homogène du $\mathbf{C}[a_1, \ldots, a_n]$-module A, on a $F_{\overline{A}}(z) = \sum_{j=1}^{s} z^{e_j}$ et ce polynôme est symétrique, c'est-à-dire : $e_j = e_{s-j}$ pour tout j. L'entier q tel que $\omega_A = A(-q)$ est alors $-\deg(F_A) = -e_s + d_1 + \cdots + d_r$.

On peut utiliser cette symétrie pour trouver les relations de certaines algèbres d'invariants :

Exemple 4. Soit G le groupe symétrique S_3 opérant dans $V = (\mathbf{C}^2)^3$ par permutation des copies de $\mathbf{C}^2$. Alors $A = \mathbf{C}[V]^G$ est formée des fonctions multisymétriques en les variables $x_i^{(j)}$ où $i = 1, 2, 3$ et $j = 1, 2$. Rappelons qu'un système de paramètres homogènes de A est formé des fonctions symétriques élémentaires $e_k(x_1^{(j)}, x_2^{(j)}, x_3^{(j)})$ où $j = 1, 2$ et $k = 1, 2, 3$, et aussi que A est engendrée par les fonctions multisymétriques élémentaires (voir l'exemple 3 en 1.3). Il en résulte que l'algèbre $\overline{A}$ est engendrée par des éléments homogènes b de degré 2 et c_1, c_2 de degré 3. D'autre part, la formule de Molien conduit à

$$F_A(z) = \frac{1 + z^2 + 2z^3 + z^4 + z^6}{(1-z)^2(1-z^2)^2(1-z^3)^3}$$

d'où $F_{\overline{A}}(z) = 1 + z^2 + 2z^3 + z^4 + z^6$. Puisque $dim\overline{A}_5 = 0$, on a $bc_1 = bc_2 = 0$. Puisque $\dim \overline{A}_6 = 1$, les monômes b^3, c_1^2, $c_1 c_2$, c_2^2 sont linéairement dépendants. Puisque la multiplication $\overline{A}_2 \times \overline{A}_4 \to \overline{A}_6$ est non dégénérée, on a $b^3 = 0$, et donc c_1^2, $c_1 c_2$, c_2^2 sont des multiples de b^3. On en déduit (exercice) que A est le quotient de l'algèbre R des polynômes en 2 générateurs de degré 1, 3 générateurs de degré 2 et 4 générateurs de degré 3, par l'idéal engendré par 2 relations de degré 5 et 3 relations de degré 6. En particulier, A n'est pas intersection complète. Puisque la résolution minimale de A est auto-duale et que $q = -\deg(F_A) = 14$, cette résolution est de la forme

$$0 \to R(-14) \to R(-8)^3 \oplus R(-9)^2 \to R(-5)^2 \oplus R(-6)^3 \to R \to A \to 0 .$$

Remarque. Soient G un groupe réductif et V un G-module ; soit q le degré minimal d'un élément du module canonique de $A = \mathbf{C}[V]^G$, c'est-à-dire : $q = -\deg(F_A)$. On peut montrer que $q \geq 1$ si $A \neq \mathbf{C}$ (voir [Ke] ; lorsque G est fini, on voit sur la formule de Molien que $q \geq \dim(V)$). On en déduit que l'algèbre A est engendrée par ses éléments de degré $\leq \dim(V) + d_1 + \cdots + d_r$ où $d_1, \ldots, d_r$ sont les degrés d'un système de paramètres homogènes ; c'est une motivation supplémentaire pour la recherche de systèmes de paramètres. Le module canonique d'une algèbre d'invariants est décrit dans [Kn].

4.5. *Séries de Hilbert des invariants et covariants des formes binaires*

Lorsque $G = \mathrm{SL}_2$ opère dans l'espace V_d des formes binaires de degré d, la série de Hilbert de tout module de covariants est donnée par une formule due à Springer, voir [Sp2]. Pour énoncer cette formule, on introduit la notation suivante.

Pour tout entier $j \geq 0$, soit $\Phi_j : \mathbf{C}[z] \to \mathbf{C}[z]$ l'application linéaire telle que

$$\Phi_j(z^n) = \begin{cases} z^{n/j} & \text{si } j \text{ divise } n \\ 0 & \text{sinon.} \end{cases}$$

Alors Φ_j est $\mathbf{C}[z^j]$-linéaire, et elle s'étend en une unique application $\mathbf{C}(z^j)$-linéaire

$$\Phi_j : \mathbf{C}(z) \to \mathbf{C}(z) .$$

Théorème. *Pour le module de covariants $M = \mathrm{Mor}^G(V_d, V_e)$, on a*

$$F_M(z) = \sum_{0 \leq j < d/2} (-1)^j \Phi_{d-2j}((1 - z^2) z^e \gamma_{dj}(z))$$

où

$$\gamma_{dj}(z) = \frac{z^{j(j+1)}}{\prod_{k=1}^{j}(1 - z^{2k}) \prod_{l=1}^{d-j}(1 - z^{2l})} .$$

Démonstration. D'après la formule de Molien-Weyl et 2.4, on a $F_M(z) = I(\chi_{M,z})$ où

$$\chi_{M,z}\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} = \frac{\chi_e(t)}{\prod_{j=0}^{d}(1-zt^{-d+2j})} \ .$$

En décomposant en éléments simples, on obtient

$$\frac{1}{\prod_{j=0}^{d}(1-zt^{-d+2j})} = \sum_{j=0}^{d}(-1)^j \frac{\gamma_{dj}(t)}{1-zt^{-d+2j}} \ .$$

De plus, pour toute fonction centrale χ sur G, on a d'après 2.4 :

$$\chi\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} = \sum_{e} I(\chi_e\chi)\frac{t^{e+1}-t^{-e-1}}{t-t^{-1}} \ .$$

Par suite, $I(\chi_e\chi)$ est le coeficient de t^{-e} dans

$$(1-t^2)\chi\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \ .$$

On obtient donc

$$F_M(z) = \sum_{j=0}^{d}(-1)^j\sum_{n=0}^{\infty} a_{n,j}z^n$$

où $a_{n,j}$ est le coefficient de $t^{n(d-2j)}$ dans $t^e(1-t^2)\gamma_{dj}(t)$. Ceci équivaut à la formule annoncée.

L'algèbre des covariants

$$\mathcal{C}(V_d) = \bigoplus_{e=0}^{\infty}\mathrm{Mor}^G(V_d, V_e) = \mathbf{C}[V_d\times\mathbf{C}^2]^G$$

est bi-graduée par le degré et l'ordre ; on peut donc définir sa série de Hilbert en deux variables

$$F_d(z,w) = \sum_{n,e\geq 0}\dim\mathcal{C}(V_d)_{n,e}\, z^n w^e \ .$$

On obtient aussitôt le

Corollaire. *Avec les notations précédentes, on a*

$$F_d(z,w) = \sum_{0\leq j<d/2}(-1)^j\Phi_{d-2j}\Big(\frac{1-z^2}{1-zw}\gamma_{dj}(z)\Big) \ .$$

Exemples. Pour $d \leq 4$, on trouve :

$$F_1(z,w) = \frac{1}{1-zw},$$

$$F_2(z,w) = \frac{1}{(1-z^2)(1-zw^2)},$$

$$F_3(z,w) = \frac{1+z^3w^3}{(1-z^4)(1-zw^3)((1-z^2w^2)},$$

$$F_4(z,w) = \frac{1+z^3w^6}{(1-z^2)(1-z^3)(1-zw^4)(1-z^2w^4)} .$$

Ces écritures sont représentatives : si par exemple $d = 4$, on vérifie à l'aide du critère de Hilbert-Mumford que I, J, f, H forment un système de paramètres bi-homogènes de $\mathcal{C}(V_4)$, de bi-degrés respectifs $(2,0)$, $(3,0)$, $(1,4)$, $(2,4)$ (exercice). Comme dans l'exemple en 4.1, on conclut que l'algèbre $\mathcal{C}(V_4)$ est une hypersurface.

En notant $F_d(z) = F_d(z,0)$ la série de Hilbert de l'algèbre des invariants $\mathcal{I}(V_d)$, on obtient

$$F_5(z) = \frac{1+z^{18}}{(1-z^4)(1-z^8)(1-z^{12})},$$

$$F_6(z) = \frac{1+z^{15}}{(1-z^2)(1-z^4)(1-z^6)(1-z^{10})},$$

$$F_8(z) = \frac{1+z^8+z^9+z^{10}+z^{18}}{(1-z^2)(1-z^3)(1-z^4)(1-z^5)(1-z^6)(1-z^7)}$$

et aussi

$$F_7(z) = \frac{P(z)}{(1-z^4)(1-z^8)(1-z^{12})^2(1-z^{20})}$$

avec

$$\begin{aligned} P(z) = 1 &+ 2z^8 + 4z^{12} + 4z^{14} + 5z^{16} + 9z^{18} + 6z^{20} + 9z^{22} + 8z^{24} \\ &+ 9z^{26} + 6z^{28} + 9z^{30} + 5z^{32} + 4z^{34} + 4z^{36} + 2z^{40} + z^{48} . \end{aligned}$$

On peut montrer que toutes ces écritures sont représentatives ; d'après l'exemple en 4.1, il en résulte que les algèbres $\mathcal{I}(V_5)$ et $\mathcal{I}(V_6)$ sont des hypersurfaces. Pour $d \geq 7$, la structure de $\mathcal{I}(V_d)$ est bien plus compliquée. Le seul cas entièrement décrit est celui de $d = 8$ (voir [Sh]) : l'algèbre $\mathcal{I}(V_8)$ est engendrée minimalement par 9 éléments homogènes de degrés 2, 3, 4, 5, 6, 7, 8, 9 et 10, et sa résolution minimale est de la forme

$$\begin{aligned} 0 \to R(-45) &\to R(-25) \oplus R(-26) \oplus R(-27) \oplus R(-28) \oplus R(-29) \\ &\to R(-16) \oplus R(-17) \oplus R(-18) \oplus R(-19) \oplus R(-20) \to R \to A \to 0 . \end{aligned}$$

On peut montrer que le nombre minimal de générateurs pour $\mathcal{I}(V_d)$ est 30 pour $d = 7$ (voir [Di-La]) et que ce nombre tend vers l'infini rapidement avec d (voir [Di-Er-Ni]).

Références.

[A] A. A'Campo-Neuen : *Note on a counterexample to Hilbert's fourteenth problem given by P. Roberts*, Indag. Matem., N.S., **5** (1994), 253-257.

[Bo] N. Bourbaki : *Groupes et algèbres de Lie, chapitres 7 et 8*, C.C.L.S., Paris 1975.

[Br-tD] T. Bröcker et T. tom Dieck : *Representations of compact Lie groups*, Springer-Verlag, Berlin 1985.

[Br] B. Broer : *A new method for calculating Hilbert series*, J. Algebra **168** (1994), 43-70.

[Br-He] W. Bruns et J. Herzog : *Cohen-Macaulay rings*, Cambridge University Press, Cambridge 1993.

[Di] J. Dixmier : *Quelques résultats et conjectures concernant les invariants des formes binaires*, dans : Séminaire d'algèbre P. Dubreil et M. P. Malliavin, 127-160, Lecture Notes in Math. **146**, Springer, Berlin 1985.

[Di-Er-Ni] J. Dixmier, P. Erdös et J-L. Nicolas : *Sur le nombre d'invariants fondamentaux des formes binaires*, C. R. Acad. Sci. Paris Série I Math. **305** (1987), 319-322.

[Di-La] J. Dixmier et D. Lazard : *Le nombre minimum d'invariants fondamentaux pour les formes binaires de degré 7*, Portugal. Math. **43** (1985-86), 377-392.

[Do] I. Dolgachev : *Rationality of fields of invariants*, in : Proc. Symp. Pure Math. **46** (1987), 3-16.

[Ei] D. Eisenbud : *Commutative Algebra with a View Towards Algebraic Geometry*, Graduate Text in Math. **150**, Springer-Verlag, New York, 1995.

[Fo] H. O. Foulkes : *Concomitants of the quintic and of the sextic up to degree four in the coefficients of the ground form*, J. London Math. Soc. **25** (1950), 205-209.

[Fu] W. Fulton : *Young Tableaux*, Cambridge University Press, Cambridge 1997.

[Ge-Ka-Ze] I. M. Gelfand, M. M. Kapranov et A. V. Zelevinsky : *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston 1994.

[Go] P. Gordan : *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Form ist*, J. Crelle **69** (1868), 323-354.

[Gr-Yo] J. Grace et A. Young : *The Algebra of Invariants*, Cambridge University Press 1903.

[He] S. Helgason : *Differential Geometry, Lie Groups, and Symmetric Spaces*, Academic Press, New York 1978.

[Hi] D. Hilbert : *Theory of Algebraic Invariants*, Cambridge University Press, Cambridge, 1993.

[Ho-Ro] M. Hochster et J. L Roberts : *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. Math. **13** (1974), 115-175.

[Ho1] R. Howe : *$(\mathrm{GL}_n, \mathrm{GL}_m)$-duality and symmetric plethysm*, Proc. Indian Acad. Sci. (Math. Sci.) **97** (1987), 85-109.

[Ho2] R. Howe : *"The Classical Groups" and invariants of binary forms*, dans : Proc. Symp. Pure Math. **48**, p. 133-166, AMS, Providence, 1988.

[Ho3] R. Howe : *Perspectives on invariant theory : Schur duality, multiplicity-free actions and beyond*, dans : Isr. Math. Conf. Proc. **8**, p. 1-182, Bar-Ilan University, 1995.

[Hu] J. Humphreys : *Linear Algebraic Groups*, Springer, New York 1975.

[Ke] G. Kempf : *The Hochster-Roberts theorem in invariant theory*, Michigan Math. J. **26** (1979), 19-32.

[Ke-Vu] M. Kervaire et Th. Vust : *Fractions rationnelles invariantes par un groupe fini : quelques exemples*, dans [Kr-Sl-Sp].

[Kn] F. Knop : *Der kanonische Modul eines Invariantenrings*, J. Algebra **127** (1989), 40-54.

[Kr] H. Kraft : *Geometrische Methoden in der Invariantentheorie,* Fried. Vieweg and Sohn, Braunschweig-Wiesbaden, 1985.

[Kr-Sl-Sp] H. Kraft, P. Slodowy, T. Springer (éd.), *Algebraic Transformation Groups and Invariant Theory,* DMV Seminar Band 13, Birkhäuser, Basel, 1989.

[Li-Pr] P. Littelmann et C. Procesi : *On the Poincaré series of the invariants of binary forms*, J. Algebra **133** (1990), 490-499.

[Mae] T. Maeda : *Noether's problem for A_5*, J. Algebra **125** (1989), 418-430.

[Mat] Y. Matsushima : *Espaces homogènes de Stein des groupes de Lie complexes*, Nagoya Math. J. **16** (1960), 205-218.

[Mi] T. Miyata : *Invariants of certain groups, I*, Nagoya Math. J. **41** (1971), 69-73.

[Na] M. Nagata : *On the fourteenth problem of Hilbert*, dans : Proc. Int. Congress Math., p. 459-462 (1958), Cambridge University Press, 1960.

[Po] V. Popov : *Groups, Generators, Syzygies, and Orbits in Invariant Theory*, Transl. Math. Monographs, vol. **100**, AMS, Providence 1993.

[Po-Vi] V. Popov et E. Vinberg : *Linear Algebraic Groups and Invariant Theory,* Encyclopaedia of Mathematical Sciences, Springer-Verlag 1995.

[Ro] M. Rosenlicht : *A remark on quotient spaces*, An. Acad. Brasil. Cienc. **35** (1963), 487-489.

[Sa] D. J. Saltman : *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71-84.

[Sc] B. Schmidt : *Finite groups and invariant theory*, dans : Topics in Invariant Theory, Lecture Note in Math. **1478**, Springer-Verlag, Berlin 1991.

[Sh] T. Shioda : *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022-1046.

[Sp1] T. A. Springer : *Invariant Theory*, Lecture Note in Math. **585**, Springer-Verlag, Berlin 1977.

[Sp2] T. A. Springer : *On the invariant theory of* SU_2, Indag. Math. **42** (1980), 339-345.

[Sta] R. Stanley : *Invariants of finite groups and their applications to combinatorics*, Bull. A. M. S. (New Series) **1** (1979), 475-511.

[Ste1] R. Steinberg : *Conjugacy Classes in Algebraic Groups*, Lecture Note in Math. **366**, Springer-Verlag, Berlin 1974.

[Ste2] R. Steinberg : *Nagata's Example*, dans : Algebraic Groups and Lie Groups, Australian Mathematical Society Lecture Series **9**, p. 375-384, Cambridge University Press 1997.

[VdB] M. Van den Bergh : *Modules of Covariants*, dans : Proc. Int. Congress Math., p. 352-362 (1994), Birkhäuser, Basel 1995.

[We] D. Wehlau : *Constructive Invariant Theory for Tori*, Ann. Inst. Fourier (Grenoble) **43** (1993), 1055-1066.