Stage de L3 magistère effectué au laboratoire Jean Leray, Nantes

Université de Rennes 1, 2015-2016

Auteur : Harold Favereau Encadré par Vincent Franjou

Théorie des invariants

Le but de ce stage était d'étudier la théorie des invariants classiques, telle qu'introduite par Cayley en 1845 et à laquelle Hilbert a notamment contribué. La théorie des invariants consiste à étudier des fonctions polynômiales invariantes sous l'action d'un groupe donné G. Sujet de recherche important au dix-neuvième siècle, jusqu'à être le sujet du quatorzième problème de Hilbert, il fut délaissé un temps avant de regagner en popularité depuis le milieu du vingtième siècle. Plus récemment, le calcul explicite en théorie des invariants est un sujet gagnant en importance (voir DERKSEN, STURMFELS*).*

Table des matières

1 Introduction à la théorie des invariants

1.1 Cadre d'étude de la théorie des invariants

On introduit la situation classique d'étude de la théorie des invariants. Soit $\mathbb{K}$ un corps algébriquement clos, et V un espace vectoriel de dimension fini sur $\mathbb{K}$. On construit l'algèbre des fonctions polynômiales sur V de deux manières différentes.

Par une base de V : Soit $(e_i)_{1\leq i\leq n}$ une base de V, et $(e_i^*)_{1\leq i\leq n}$ la base duale dans V^* ; c'est à dire, pour tout $1 \leq j \leq n$:

$$e_j^*(\sum_{i=1}^{n} x_i e_i) = x_j$$

On pose alors $S(V)$ la sous-algèbre de l'espace des fonctions de V à valeurs dans $\mathbb{K}$ engendrée par les fonctions e_i^* : c'est l'algèbre des *fonctions polynômiales* sur V.

Par l'algèbre tensorielle de V : Soit $W = V^*$. On pose, pour $k \in \mathbb{N}$:

$$T^k(W) = \bigotimes_{i=1}^{k} W, \text{ (avec } T^0(W) = \mathbb{K}) \text{ et } T(W) = \bigoplus_{k\in\mathbb{N}} T^k(W)$$

On peut munir $T(W)$ d'une structure de $\mathbb{K}$-algèbre de la manière suivante. Soit $\varphi : W^p \times W^m = W^{p+m} \to T^{p+m}(W)$ l'application $(m+p)$-linéaire canonique. Par propriété universelle du produit tensoriel, on a une application $T^p(W) \times T^m(W) \to T^{p+m}(W)$. On définit ensuite le produit sur $T(W)$:

$$\sum_{n\in\mathbb{N}} X_n \times \sum_{m\in\mathbb{N}} Y_n = \sum_{(n,m)\in\mathbb{N}^2} X_n \times Y_n.$$

$T(W)$, muni de ce produit, est bien une $\mathbb{K}$-algèbre. Enfin, pour obtenir $S(W)$, on quotiente $T(W)$ par l'idéal engendré par les éléments de la forme $x_1 \otimes \ldots \otimes x_n - x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(n)}$, $\sigma \in \mathfrak{S}_n$ (Pour "rendre commutatif" le produit).
Les deux constructions donnent bien le même objet - on peut vérifier que le morphisme de $\mathbb{K}$-algèbres qui à f_i (dans la première construction) associe f_i ($\in T^1(W) = W$) est un isomorphisme.

La première construction donne une "bonne idée" sur la manière de travailler avec les fonctions polynômiales ; la deuxième construction montre que ces fonctions ne dépendent pas de la base de V choisie dans la première construction.

On peut remarquer que le morphisme de $\mathbb{K}$-algèbres qui à e_i^* associe T_i dans l'algèbre des polynômes $\mathbb{K}[T_1, \ldots, T_n]$ est un isomorphisme (ce n'est le cas que lorsque $\mathbb{K}$ est infini : ici, on a supposé $\mathbb{K}$ algébriquement clos, en particulier, il est infini). Dans la suite, on confondra parfois les fonctions de $S(V)$ avec les polynômes de $\mathbb{K}[T_1, \ldots, T_n]$.

Par la suite, on aura aussi besoin de la notion d'algèbre graduée :

Définition 1

Soit A une $\mathbb{K}$-algèbre. A est dite graduée s'il existe une famille de sous-espaces vectoriels de A, $\{A_i, i \in \mathbb{N}\}$ telle que :
- $A = \bigoplus_{i\in\mathbb{N}} A_i$
- $\forall i, j \in \mathbb{N}$, $A_i A_j \subseteq A_{i+j}$

Remarque 1. A_0 est alors un sous-anneau de A : il est stable par addition en tant que sous espace vectoriel, et stable par multiplication car $A_0 A_0 \subseteq A_{0+0} = A_0$.

Exemple 1. $A = \mathbb{K}[T_1, \ldots, T_n]$ est une algèbre graduée : on pose A_i le sous-espace des polynômes dont chaque monôme est de degré total i (le degré total de $T_1^{\alpha_1} \ldots T_n^{\alpha_n}$ est $\alpha_1 + \ldots + \alpha_n$). Cette graduation correspond à la graduation de $S(V)$ où $S(V)_i$ est le sous-espace des fonctions f vérifiant $f(\lambda v) = \lambda^i f(v)$, $v \in V, \lambda \in \mathbb{K}$. On appelle les éléments de A_i les éléments *homogènes* de degré i.

1.2 Théorie des invariants

Soit $G \subseteq GL(V)$ un groupe d'automorphismes linéaires de V. On définit une action de groupe de G sur $S(V)$ de la manière suivante : pour $f \in S(V), g \in G, g \cdot f$ est la fonction qui à tout $v \in V$, associe $g \cdot f(v) = f(g^{-1}v)$. On peut alors vérifier qu'on définit une action à gauche de G sur $S(V)$. On peut remarquer que $S(V)_i$ est stable sous l'action de G.

La théorie des invariants consiste alors à étudier l'ensemble $S(V)^G$ des polynômes invariants sous cette action, c'est à dire tels que $g \cdot f = f$ pour tout $g \in G$ (On dit alors que f est G-invariant). On vérifie facilement le résultat suivant :

Proposition 1

$S(V)^G$ est une sous-algèbre graduée de $S(V)$, pour la graduation $S(V)_i^G = S^G \cap S(V)_i$.

Démonstration : On voit clairement que $S(V)^G$ est une sous-algèbre de $S(V)$. Montrons qu'elle est graduée pour la graduation donnée. Soit $f \in S(V)^G, g \in G$. On a $f \in S(V)$ algèbre graduée, donc il existe une décomposition en éléments homogènes :

$$f = \sum_{i \in \mathbb{N}} f_i \text{ (somme finie).}$$

Par invariance de f, on a :

$$f = g \cdot f = \sum_{i \in \mathbb{N}} g \cdot f_i.$$

Les $S(V)_i$ sont stables par action de G : par la propriété de somme directe, on a alors, pour tout i, $g \cdot f_i = f_i$: les f_i sont G-invariants, d'où la décomposition recherchée. Les autres propriétés viennent directement du fait que les $S(V)_i$ forment une graduation de $S(V)$. ■

On peut donner la caractérisation suivante des polynômes invariants à partir des orbites de l'action de groupe :

Proposition 2

$f \in S(V)$ est G-invariante si et seulement si elle est constante sur les orbites de l'action

$$\mathcal{O}(v) = \{g \cdot v : g \in G\}$$

La question principale de ce mémoire sera la suivante : $S(V)^G$ est-elle une algèbre de type fini ? (C'est à dire, existent-ils $f_1, \ldots, f_n$ tels que $S(V)^G = \mathbb{K}[f_1, \ldots, f_n]$?).
Si le résultat est positif, d'autres questions classiques sont :

1. Déterminer des générateurs de cette algèbre
2. Déterminer leurs relations de dépendance algébrique
3. Donner un algorithme pour exprimer un invariant donné comme polynôme en les générateurs.

1.3 Exemples

La théorie des invariants est un sujet où les exemples jouent un rôle fondamental dans la compréhension. Ainsi, on peut donner quelques exemples de calcul de la sous-algèbre des invariants :

Exemple 2. On se place dans le cas où $\mathbb{K} = \mathbb{C}$ et $V = \mathbb{C}^2$. Soit $G = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \alpha \in \mathbb{C} \right\}$. On va montrer le résultat suivant :

Proposition 3

L'algèbre des invariants est de type fini et vérifie $S(V)^G = \mathbb{K}[T_2]$

Démonstration : On a $g \cdot T_1 = T_1 - \alpha T_2$ et $g \cdot T_2 = T_2$. La deuxième égalité montre directement que $\mathbb{K}[T_2] \subseteq S(V)^G$. Démontrons l'inclusion inverse. Soit f polynôme invariant sous l'action de G. $S(V)^G$ étant une algèbre graduée, on peut supposer sans perte de généralité f homogène de degré d. On peut alors écrire :

$$f = \sum_{i_1=0}^{d} \lambda_{i_1} T_1^{i_1} T_2^{d-i_1}.$$

Par invariance de f, on a alors, pour tout $\alpha \in \mathbb{C}$:

$$f = \sum_{i_1=0}^{d} \sum_{k=0}^{i_1} \lambda_{i_1} \binom{i_1}{k} \alpha^k T_1^{i_1-k} T_2^{d-i_1+k} = \sum_{k=0}^{d} \alpha^k \left(\sum_{i_1=k}^{d} \lambda_{i_1} \binom{i_1}{k} T_1^{i_1-k} T_2^{d-i_1+k} \right).$$

En considérant cette dernière expression comme un polynôme de $(\mathbb{C}[T_1, T_2])[\alpha]$, on voit que l'égalité ne peut être vraie que si, pour k différent de 0 :

$$\sum_{i_1=k}^{d} \lambda_{i_1} \binom{i_1}{k} T_1^{i_1-k} T_2^{d-i_1+k} = 0.$$

Ce qui n'est possible que si $\lambda_{i_1} = 0$ pour i_1 différent de 0, ce qui montre le résultat recherché. ■

Ce résultat sera particulièrement intéressant dans la deuxième partie : en effet, on pourra voir que ce groupe n'est pas réductif, et pourtant, l'algèbre des invariants étudiée ici est bien de type fini.

Exemple 3. On se place ici dans le cas d'un corps algébriquement clos quelconque. On choisit $V = \mathbb{K}^n$ et G le groupe des matrices de permutations, $G \cong \mathfrak{S}_n$. G agit de la manière suivante sur V :

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Dans ce cas classique, les invariants sont aussi appelés *polynômes symétriques*. On a alors :

Proposition 4

L'algèbre des invariants est de type fini et vérifie $S(V)^G = \mathbb{K}[F_1, \ldots, F_n]$, où les F_i sont les polynômes symétriques élémentaires définis par

$$F_i = \sum_{1 \leq j_1 < \ldots < j_i \leq n} T_{j_1} \ldots T_{j_i}.$$

De plus, les F_i sont algébriquement indépendants.

On fournit une preuve algorithmique du résultat, ce qui répondra aux trois questions de la théorie des invariants.

Démonstration : On définit un ordre sur les monômes de $\mathbb{K}[T_1, \ldots, T_n]$, noté $\prec$, de la manière suivante. $T_1^{\alpha_1} \ldots T_n^{\alpha_n} \prec T_1^{\beta_1} \ldots T_n^{\beta_n}$ si une des deux conditions suivantes est vérifiée :

1. $\sum_{i=1}^n \alpha_i \leq \sum_{i=1}^n \beta_i$.
2. $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ et, en posant i_0 le plus petit entier tel que $\alpha_{i_0} \neq \beta_{i_0}$, on a $\alpha_{i_0} < \beta_{i_0}$.

$\prec$ est un ordre total. On peut ainsi poser $init(f)$ le monôme maximal à coefficient non nul dans f. Soit S_0 un polynôme symétrique. Pour tout monôme $T_1^{\alpha_1} \ldots T_n^{\alpha_n}$ dans S_0, et toute permutation σ, le monôme $T_1^{\alpha_{\sigma(1)}} \ldots T_n^{\alpha_{\sigma(n)}}$ apparaît aussi dans S_0 (par symétrie de S_0). Nécessairement, le monôme maximal $init(S_0) = c\, T_1^{\gamma_1} \ldots T_n^{\gamma_n}$ vérifie donc $\gamma_1 \geq \ldots \geq \gamma_n$.

On pose $M_0 = c\, F_1^{\gamma_1 - \gamma_2} F_2^{\gamma_2 - \gamma_3} \ldots F_{n-1}^{\gamma_{n-1} - \gamma_n} F_n^{\gamma_n}$. Posons alors $\widetilde{S} = S_0 - M_0$. On répète ensuite la même opération avec S_1 jusqu'à obtenir un $n \in \mathbb{N}$ tel que $S_n = 0$.

Montrons que le processus s'arrête en un nombre fini d'étapes. Par construction, $init(S_0) = init(M_0)$, donc les monômes maximaux s'annulent dans $S_0 - M_0$ et on obtient $init(S_1) \prec init(S_0)$. Le nombre de monômes m qui vérifient $m \prec init(f)$ est fini (leur degré est majoré). Ainsi, l'algorithme se termine (sinon, il produirait une suite décroissante infinie de monômes) et les valeurs de M donnent la décomposition recherchée.

Démontrons maintenant l'indépendance algébrique des F_i. Soit $P \in \mathbb{K}[y_1, \cdots, y_n]$ non nul. Il suffit de montrer que $P(F_1, \ldots, F_n) \neq 0$. Pour tout monôme $y_1^{\alpha_1} \ldots y_n^{\alpha_n}$ de P, le monôme initial de $F_1^{\alpha_1} \ldots F_n^{\alpha_n}$ est $M := T_1^{\alpha_1+\ldots+\alpha_n} T_2^{\alpha_2+\ldots+\alpha_n} \ldots T_n^{\alpha_n}$. De plus, l'application

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (\alpha_1 + \ldots + \alpha_n, \alpha_2 + \ldots + \alpha_n, \ldots, \alpha_n)$$

est injective (application linéaire dont la matrice est triangulaire supérieure avec des 1 sur la diagonale, donc de déterminant 1). L'injectivité de cette application montre que tout autre monôme $F_1^{\beta_1} \ldots F_n^{\beta_n}$ a un monôme initial différent de M : ainsi M n'est annulé par aucun autre monôme dans l'expression, d'où $P(F_1, \ldots, F_n) \neq 0$. ■

On peut ainsi procéder à la décomposition d'un polynôme symétrique : soit $S_0 = T_1^3 T_2 + T_1 T_2^3$. En appliquant l'algorithme, on obtient $S_1 = S_0 - F_1^2 F_2 = -2T_1^2 T_2^2 = -2F_2^2$ d'où $S_0 = F_1^2 F_2 - 2F_2^2$.

Tout au long de ce mémoire, de nombreux exemples seront rajoutés aux deux précédents, certains nécessitant pour leur calcul de nouveaux outils qui seront abordés par la suite.

2 Quelques notions de géométrie algébrique

La théorie des invariants, dans son développement, est liée à la géométrie algébrique : ainsi, dans (Mumford, Fogarty et Kirwan 1994), la question est en lien avec la mise en place d'une "bonne" structure de variété algébrique sur les orbites de l'action d'un groupe sur une variété algébrique. Néanmoins, cela nécessiterait le développement de plusieurs autres notions. Nous aurons ici seulement besoin de quelques bases afin de démontrer le résultat principal concernant la question de la finitude de l'algèbre des invariants.

On se place toujours dans le cas d'un corps $\mathbb{K}$ algébriquement clos et d'une espace vectoriel V sur $\mathbb{K}$ de dimension finie. Lorsque le contexte est clair, on écrira S pour désigner $S(V)$ l'algèbre des fonctions polynômiales.

2.1 Anneau noethérien

Définition 2

Soit R un anneau commutatif. R est dit noethérien s'il vérifie l'une des trois propriétés équivalentes suivantes :

1. *Tout idéal I de R est de type fini : il existe $a_1, \ldots, a_n \in R$ tels que $I = Ra_1 + \ldots + Ra_n$ (On notera aussi $I = \langle a_1, \ldots, a_n \rangle$ lorsque, dans le contexte, on voit clairement quel est l'anneau R).*
2. *Toute famille $\mathcal{F}$ d'idéaux de R possède un élément maximal M, c'est à dire que M n'est contenu dans aucun autre idéal de $\mathcal{F}$*
3. *Toute suite croissante d'idéaux de R est stationnaire : pour $I_1 \subseteq I_2 \subseteq \ldots$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $I_n = I_N$*

On aura besoin du résultat suivant :

Théorème 1 (*Théorème de la base de Hilbert*)

Si R est noethérien, alors $R[T]$ est lui aussi noethérien.

Démonstration : Voir (Lang 2002, p. 186) ■

Corollaire 1

Si R est noethérien, alors $R[T_1, \ldots, T_n]$ aussi.

Démonstration : Par simple récurrence sur n, le résultat est immédiat. ■

Corollaire 2

$S(V)$ est noethérien.

Proposition 5

Si R est noethérien, alors, pour tout idéal I de R, R/I est noethérien.

Démonstration : Soit $\pi : R \to R/I$ l'application canonique, J un idéal de R/I. Il existe un idéal J' de R qui contient I tel que $\pi(J') = J$. R est noethérien donc il existe $a_1, \ldots, a_n \in R$ tels que $J' = \langle a_1, \ldots, a_n \rangle$. On voit alors que $J = \pi(J') = \langle \pi(a_1), \ldots, \pi(a_n) \rangle$. ■

Proposition 6

Si A est une $\mathbb{K}$-algèbre de type fini, alors A est noethérien.

Démonstration : A peut s'écrire sous la forme $A = \mathbb{K}[a_1, \ldots, a_n]$. A est alors l'image de $\mathbb{K}[T_1, \ldots, T_n]$ par le morphisme φ qui à T_i associe a_i. Alors A est isomorphe à $\mathbb{K}[T_1, \ldots, T_n]/\ker(\varphi)$ qui, par la proposition précédente, est noethérien. ■

Remarque 2. Plus simplement, on vient de donner une caractérisation des algèbres de type fini : ce sont les quotients des algèbres de polynômes.

2.2 Topologie de Zariski

Définition 3

Soit I un idéal de S. $v \in V$ est appelé ***zéro*** *de I si pour tout $f \in I$, $f(v) = 0$.*

On pose $\mathcal{V}(I)$ l'ensemble des zéros de l'idéal I. On peut facilement vérifier les propriétés suivantes :

Proposition 7

1. $\mathcal{V}(\{0\}) = V$, $\mathcal{V}(S) = \emptyset$.
2. $I \subseteq J \Rightarrow \mathcal{V}(J) \subseteq \mathcal{V}(I)$.
3. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.
4. *Soit $(I_a)_{a \in A}$ une famille d'idéaux. On note $\sum_{a \in A} I_a$ l'idéal composé des sommes finies d'éléments des I_a. Alors $\mathcal{V}(\sum_{a \in A} I_a) = \bigcap_{a \in A} \mathcal{V}(I_a)$.*

Ces quatre propriétés permettent de définir une topologie sur V où les fermés sont exactement les $\mathcal{V}(I)$ pour tout idéal I de S. On l'appelle *topologie de Zariski*. Démontrons quelques propriétés de la topologie de Zariski :

Proposition 8

1. *Les points sont fermés pour la topologie de Zariski.*
2. *Si $\dim V = 1$, la topologie de Zariski coïncide avec la topologie cofinie.*
3. *Si V et $\mathbb{K}$ sont munis de la topologie de Zariski, alors les fonctions de S sont continues.*

Démonstration : 1. On se place dans le cas de la construction 1 de $S(V)$. Soit $v = (v_1, \dots, v_n)$ dans la base $(e_i)_{1 \leq i \leq n}$. Alors $\{v\} = \mathcal{V}(\langle T_1 - v_1, \dots, T_n - v_n \rangle)$.

2. Si $\dim V = 1$, $S(V)$ est un anneau principal, et les zéros d'un idéal I sont exactement les racines d'un polynôme f tel que $I = \langle f \rangle$, qui sont en nombre fini.

3. D'après le résultat précédent, il suffit de montrer que pour tout $l \in \mathbb{K}$, $f^{-1}(\{l\})$ est un fermé dans V. Or, $v \in f^{-1}(\{l\}) \Leftrightarrow f(v) = l \Leftrightarrow v \in \mathcal{V}(\langle f - l \rangle)$ et ce dernier ensemble est fermé par définition. ■

Pour $X \subseteq V$, on pose $\mathcal{J}(X) = f \in S : f(X) = 0$. C'est un idéal de S.

Proposition 9

On a $\mathcal{V}(\mathcal{J}(X)) = \overline{X}$ (l'adhérence de X).

Démonstration : $\mathcal{V}(\mathcal{J}(X))$ est fermé et contient X, donc $\overline{X} \subseteq \mathcal{V}(\mathcal{J}(X))$. Réciproquement, soit I idéal de S tel que $\overline{X} = \mathcal{V}(I)$. Soit $f \in I$. Pour tout $x \in X$, $f(x) = 0$, donc $f \in \mathcal{J}(X)$. On a donc $I \subseteq \mathcal{J}(X)$ donc d'après la propriété 3 de la proposition 7, $\mathcal{V}(\mathcal{J}(X)) \subseteq \mathcal{V}(I) = \overline{X}$, d'où le résultat. ■

On va ensuite démontrer une propriété fondamentale de la topologie de Zariski : tous les ouverts non vides sont denses.

Définition 4

*Soit X un espace topologique. X est dit **réductible** s'il existe X_1, X_2 deux fermés non égaux à X tels que $X = X_1 \cup X_2$. Sinon, X est dit **irréductible**. De manière équivalente, X est irréductible si deux ouverts non vides ont toujours une intersection non vide.*

Remarque 3. La notion d'irréductibilité est très restrictive en comparaison aux espaces "habituels" de la topologie. En effet, dès qu'un espace topologique est séparé, alors nécessairement il ne peut pas être irréductible.

Proposition 10

Un ensemble fermé $X \subseteq V$ est irréductible si et seulement si $\mathcal{J}(X)$ est un idéal premier de S.

Démonstration :
- $\Rightarrow$: Supposons X irréductible. Soient $f_1, f_2 \in S$ tels que $f_1 f_2 \in \mathcal{J}(X)$. On pose $X_i = \mathcal{V}(\langle f_i \rangle)$. On a alors $X = X_1 \cup X_2$. L'hypothèse d'irréductibilité implique que l'un des X_i est égal à X : le f_i correspondant appartient alors à $\mathcal{J}(X)$, ce qui montre que $\mathcal{J}(X)$ un idéal premier.
- $\Leftarrow$: Supposons X réductible, et soit $X = X_1 \cup X_2$ une décomposition en fermés propres. D'après la proposition 9, $\mathcal{J}(X_i) \neq \mathcal{J}(X)$. Soient $f_i \in \mathcal{J}(X_i) \backslash \mathcal{J}(X)$. On a alors $f_1 f_2 \in \mathcal{J}(X)$ mais $f_1, f_2 \notin \mathcal{J}(X) : \mathcal{J}(X)$ n'est pas un idéal premier. ■

Corollaire 3

V est irréductible

Corollaire 4

Tout ouvert U non vide de V est dense.

Démonstration : U et $V \backslash \overline{U}$ sont deux ouverts non vides de V avec une intersection vide. L'irréductibilité de V implique que l'un des deux ensembles est vide : U est non vide donc $V \backslash \overline{U} = \emptyset$ ce qui démontre le résultat. ■

Remarque 4. Ce dernier résultat montre à quel point la topologie de Zariski diffère d'une topologie métrique usuelle : les ouverts non vides y sont "gros", leur adhérence valant l'espace tout entier. Si on place dans le cas où $\mathbb{K} = \mathbb{C}$, tous les fermés pour Zariski ont un intérieur vide pour la topologie métrique classique de $\mathbb{C}^n$: les fermés sont "petits".

2.3 Variété algébrique affine

Nous n'étudions pas ici en détail la notion de variété algébrique affine, fondamentale à la géométrie algébrique. Cette notion nous servira principalement à définir les groupes algébriques linéaires par la suite.

Définition 5

On appelle variété algébrique affine un sous ensemble fermé de V.

Les restrictions des fonctions de S à X forment une sous-algèbre de S qu'on note S_X, les fonctions polynômiales sur X.

Définition 6

Soient X, X' deux variétés algébriques affines d'espaces vectoriels V, V'. Soit $\phi : X \to X'$ une application quelconque. ϕ induit une application depuis les fonctions de X' à valeurs dans $\mathbb{K}$ dans les fonctions de X à valeurs dans $\mathbb{K}$ de la manière suivante :

$$\phi^* : f' \longmapsto (\phi^*(f') : v \longmapsto f'(\phi(v))$$

ϕ est appelé un morphisme de variétés algébriques affines si $\phi^*(S'_{X'}) \subseteq S_X$, c'est à dire si ϕ^* envoie les fonctions polynômiales de X' sur des fonctions polynômiales de X.

Remarque 5. Par la suite, on utilisera plutôt la caractérisation suivante, plus concrète, des morphismes : soient $(e_i)_{1\leq i\leq n}$ et $(e'_j)_{1\leq j\leq n'}$ deux bases respectives de V et V' ; soient f_i et f'_j des bases duales (telles que dans la construction 1) ; et soient g_i et g'_j leurs restrictions à X et X'. Alors

$$\phi(v) = \sum_{j=1}^{n'} \phi^*(g'_j)(v) e'_j$$

ϕ est un morphisme si et seulement si les $\phi^*(g'_j)$ sont des fonctions polynômiales : autrement dit, si et seulement si les coordonnées de $\phi(v)$ sont des polynômes en les coordonnées de v.

2.4 Groupe algébrique linéaire

On donne ici une définition plus simple que la définition classique de groupe algébrique linéaire. On ne rentre pas ici dans les détails de la théorie des groupes algébriques linéaires. On pourra cependant consulter (Borel 1991) à ce sujet.

Soit $E = \mathcal{L}(V)$ l'espace vectoriel des endomorphismes de V. Le groupe $\mathrm{GL}(V)$ est un ouvert pour la topologie de Zariski : en effet, $\mathrm{GL}(V) = \{X \in E : \det(X) \neq 0\}$, et le déterminant est bien un polynôme en les coefficients de la matrice X. Par la suite, on voudrait voir $\mathrm{GL}(V)$ comme une variété algébrique affine ; pour cela, on identifie $\mathrm{GL}(V)$ à son image par l'injection :

$$i : \begin{array}{ccc} \mathrm{GL}(V) & \longrightarrow & E \times \mathbb{K} \\ g & \longmapsto & \left(g, \det(g)^{-1}\right) \end{array}$$

$i(\mathrm{GL}(V))$ est alors bien un fermé : c'est l'ensemble des couples (g, x) qui annulent le polynôme $x \det(g) - 1$.

Définition 7

Un groupe linéaire algébrique est un sous groupe fermé d'un $\mathrm{GL}(V)$, pour la topologie induite par la topologie de Zariski sur $E \times \mathbb{K}$.

On peut alors donner l'exemple de nombreux groupes linéaires algébriques ; par isomorphisme, on peut considérer $V = \mathbb{K}^n$, et $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{K})$ le groupe des matrices inversibles :

– $\mathrm{SL}_n(\mathbb{K}) = \{(g,x) \in E \times \mathbb{K} : \det(g) - 1 = 0\}$.
– $\mathrm{O}_n(\mathbb{K}) = \{(g,x) \in E \times \mathbb{K} : g \times {}^t g - 1 = 0\}$. On peut vérifier que cette équation définit bien un polynôme en les coefficients de g.
– $T_n(\mathbb{K})$ le groupe des matrices diagonales : il suffit de prendre l'idéal engendré par les $x_{i,j}$ pour $i \neq j$.
– Tout sous-groupe fini : en tant qu'union de singletons fermés pour la topologie de Zariski.

Pour cette topologie, on dispose du résultat suivant :

Proposition 11

Soit $G \subseteq \mathrm{GL}(V)$ un groupe linéaire algébrique, muni de la topologie de $E \times \mathbb{K}$. Soit $a \in G$. Alors, les bijections de G dans lui même $g \longmapsto g^{-1}$, $g \mapsto ag$, $g \mapsto ga$ sont des homéomorphismes

Démonstration : Soit F sous-ensemble fermé de G. G est fermé dans $\mathrm{GL}(V)$ donc F est fermé dans $\mathrm{GL}(V)$: il existe $P_1, \ldots, P_n \in S(E \times \mathbb{K})$ tels que $F = \mathcal{V}(\langle P_1, \ldots, P_n \rangle)$. Montrons que F^{-1} est fermé. Pour tout g, $g^{-1} = \det(g)^{-1}\, {}^t\mathrm{com}\, g$ (la comatrice de g). Les coefficients de la comatrice de g sont des polynômes en les coefficients de g (déterminants de sous-matrices de g). On voit donc qu'il existe des polynômes $Q_1, \ldots, Q_n$ tels que $P_i(g) = 0 \Leftrightarrow Q_i(g) = 0$, et F^{-1} est bien fermé. Les deux autres cas se traitent de manière similaire. ■

Nous allons ensuite pouvoir considérablement réduire le nombre de groupes où il est nécessaire d'étudier l'algèbre des invariants grâce au résultat suivant :

Théorème 2

Soit G un sous-groupe de $\mathrm{GL}(V)$. Alors $\overline{G}$, l'adhérence de G, est un groupe et $S^G = S^{\overline{G}}$.

Démonstration : Démontrons tout d'abord que l'adhérence est bien un groupe. Soit $a \in G$. D'après la proposition 11, $a\overline{G}$ est un ensemble fermé contenant G, donc $\overline{G} \subseteq a\overline{G}$. En opérant de même avec a^{-1}, on montre que $a\overline{G} = \overline{G}$. Ceci étant vrai pour tout $a \in G$, on a $G\overline{G} = \overline{G}$. En opérant de même avec $a \in \overline{G}$, on obtient finalement que $\overline{G}\,\overline{G} = \overline{G}$. Il reste à montrer que $(\overline{G})^{-1} = \overline{G}$. $(\overline{G})^{-1}$ est un fermé contenant G^{-1}, donc $\overline{G} = (\overline{G^{-1}}) \subseteq (\overline{G})^{-1}$. On obtient l'autre inclusion en passant à l'inverse cette dernière inclusion, d'où le résultat.

Démontrons ensuite que $S^G = S^{\overline{G}}$. $G \subseteq \overline{G}$ donc $S^{\overline{G}} \subseteq S^G$. Réciproquement, soit $f \in S^G, v \in V$ fixés. Soit $\overline{g} \in \overline{G}$. Montrons que $(\overline{g} \cdot f)(v) = f(v)$, ce qui prouvera le résultat. Considérons l'application φ qui à g dans $\mathrm{GL}(V)$ associe $(g \cdot f)(v)$. Elle est continue (il suffit de vérifier que pour tout $l \in \mathbb{K}$, $\varphi^{-1}(\{l\})$ est un fermé de $\mathrm{GL}(V)$. Or, $(g \cdot f)$ et f étant continues en tant qu'applications de V dans $\mathbb{K}$, il est facile de voir que g appartient à $\varphi^{-1}(\{l\})$ si g vérifie des équations polynômiales en ses coefficients). Elle est constante égale à $f(v)$ sur G, donc elle est constante égale à $f(v)$ sur l'adhérence de G, ce qui montre la $\overline{G}$-invariance de f. ■

2.5 Exemples

En plus de réduire le nombre de groupes sur lesquels il est nécessaire d'étudier la théorie des invariants, la géométrie algébrique va nous permettre de déterminer la sous-algèbre des invariants dans un autre cas particulier :

Exemple 4. On se place sur un corps $\mathbb{K}$ algébriquement clos quelconque, et on choisit $V = \mathcal{M}_n(K)$. On choisit G le sous-groupe de $\mathrm{GL}(V)$ correspondant aux changements de base ; $G \cong \mathrm{GL}_n(\mathbb{K})$. On identifie les deux groupes. G agit sur V par conjugaison : $g \cdot a = gag^{-1}$.

Soient $s_1, \ldots, s_n$ les polynômes de S définis par :

$$\det(t.\,\mathrm{id} - a) = t^n - s_1 t^{n-1} + \ldots + (-1)^n s_n(a).$$

Les s_i sont invariants sous l'action de G : il est facile de voir que le polynôme caractéristique est invariant sous l'action, et le résultat en découle. On va démontrer le résultat suivant :

Proposition 12

La sous-algèbre S^G des invariants est de type fini et vérifie $S^G = \mathbb{K}[s_1, \ldots, s_n]$. De plus, les s_i sont algébriquement indépendants.

Pour cela, nous aurons besoin des deux lemmes suivants :

Lemme 1

L'ensemble U des matrices avec n valeurs propres distinctes est ouvert (et donc dense, car non vide) pour la topologie de Zariski.

Démonstration : Considérons le polynôme $\prod_{1\leq i<j\leq n}(T_i - T_j)^2$. Il est symétrique, donc d'après l'exemple 3, il existe un polynôme D à n variables tel que :

$$\prod_{1\leq i<j\leq n} (T_i - T_j)^2 = D(F_1, \ldots, F_n)$$

où les F_i sont les polynômes symétriques élémentaires. Soit $a \in \mathcal{M}_n(\mathbb{K})$. En évaluant cette expression en les $s_i(a)$:

$$\prod_{1\leq i<j\leq n} (\lambda_i - \lambda_j)^2 = D(s_1(a), \ldots, s_n(a))$$

et en comparant cette expression avec celle du polynôme caractéristique, les relations coefficients-racines nous donnent que les λ_i sont exactement les valeurs propres de a. Ainsi, a possède n valeurs propres distinctes si et seulement si $D(s_1(a), \ldots, s_n(a)) \neq 0$, ce qui montre que U est ouvert. ■

Lemme 2

Soit $c = (c_1, \ldots, c_n) \in \mathbb{K}^n$ et

$$A_c = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -c_0 \\ 1 & \ddots & \ddots & \vdots & -c_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -c_{n-2} \\ 0 & \cdots & 0 & 1 & -c_{n-1} \end{pmatrix}.$$

Alors le polynôme caractéristique de A_c est $P(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_0$ et si A_c a n valeurs propres distinctes alors A_c est diagonalisable.

Démonstration propriété : Soit A_c matrice compagnon définie comme dans le lemme précédent. Par le calcul du polynôme caractéristique, on a $s_i(A_c) = (-1)^i c_i$. Soit $f \in S(V)^G$ un polynôme invariant. Soit p le polynôme en n variables tel que $p(c_1, \ldots, c_n) = f(A_c)$. Soit $P \in S(V)$ tel que $P(A) = p(-s_1(A), s_2(A), \ldots, (-1)^n s_n(A))$. Par invariance des s_i, P est un polynôme G-invariant. De plus, P et f coïncident sur les matrices compagnons. P et f sont G-invariants donc ils coïncident sur les classes de conjugaisons des matrices compagnons $M := \{gA_cg^{-1} : g \in G, c \in \mathbb{K}^n\}$. Il suffit alors de montrer que U, l'ensemble des matrices à n valeurs propres distinctes, est un sous-ensemble de M : par densité de U, f et P coïncideront sur l'ensemble des matrices. Mais on sait que toutes les matrices de M et toutes les matrices de U sont diagonalisables : on en déduit le résultat.

Montrons l'indépendance algébrique des s_i. On a $s_i(A_c) = (-1)^i c_i$, donc l'ensemble $\{(s_1(A_c), \ldots, s_n(A_c) : c \in \mathbb{K}^n\}$ est égal à $\mathbb{K}$ tout entier. Soit p polynôme tel que $p(s_1, \ldots, s_n) = 0$. Alors $p(s_1, \ldots, s_n)(A_c) = p(s_1(A_c), \ldots, s_n(A_c)) = 0$ pour tout $c \in \mathbb{K}^n$, ce qui implique $p(c_1, \ldots, c_n) = 0$ pour tout $c \in \mathbb{K}^n$. D'où $p = 0$. ■

On peut aussi étudier l'exemple trivial suivant :

Exemple 5. On considère l'action de $\mathrm{GL}(V)$ sur V. Les orbites de l'action sont $\{0\}$ et $V\backslash\{0\}$. D'après la proposition 2, f est G-invariante si et seulement si elle est constante sur ces deux orbites. $V\backslash\{0\}$ est un ouvert pour la topologie de Zariski, son adhérence est donc V tout entier. Si f est constante sur $V\backslash\{0\}$, alors f est constante sur son adhérence V : c'est une fonction constante. L'algèbre des invariants est donc $\mathbb{K}$.

Dans la suite, nous allons chercher à déterminer une propriété d'un groupe $G \in \mathrm{GL}(V)$ qui permettrait d'assurer que l'algèbre des invariants soit de type fini. On utilisera l'approche historique : on démontrera d'abord le premier résultat, de Hilbert, puis le résultat plus fort, de Nagata.

3 Réductivité linéaire : l'approche de Hilbert

Nous aurons tout d'abord besoin de la notion suivante :

Définition 8

Soit $G \in \mathrm{GL}(V)$, et W un espace vectoriel de dimension finie sur $\mathbb{K}$. Une représentation de G sur W est un morphisme de groupes $\rho : G \longrightarrow \mathrm{GL}(W)$. ρ est une représentation polynômiale si ρ est aussi un morphisme de variétés algébriques, c'est à dire que pour g dans G, $\rho(g)$ est une matrice dont les coordonnées sont des polynômes en les n^2+1 coordonnées de g (On voit G comme sous-ensemble de $E \times \mathbb{K}$: la n^2+1 coordonnée correspond à l'inverse du déterminant).

Exemple 6. On présente ici un exemple classique, celui de l'action de $SL_2(\mathbb{K})$ sur les formes binaires de degré fixé, tel qu'étudié par Gordan dans (Gordan 1987). $G = SL_2(\mathbb{K})$ agit sur $A := \mathbb{K}[X,Y]$ de la manière suivante :

$$\rho\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}(X) = aX + bY \qquad \rho\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}(Y) = cX + dY.$$

Pour tout g, $\rho(g)$ laisse invariant les sous-espaces homogènes A_d (engendré par $X^d, X^{d-1}Y, \ldots, XY^{d-1}, Y^d$) invariants : on peut ainsi définir une représentation ρ_d sur A_d : c'est une représentation polynômiale.

3.1 Réductivité linéaire

On peut désormais définir la réductivité linéaire pour un groupe linéairement algébrique :

Définition 9

Soit G un groupe linéairement algébrique. On dit que G est linéairement réductif si pour toute représentation polynômiale $\rho : G \longrightarrow \mathrm{GL}(W)$ et pour tout $w \in W\backslash\{0\}$ tel que pour tout g, $\rho(g)w = w$, il existe une fonction linéaire G-invariante telle que $f(w) \neq 0$.

On peut donner des exemples de groupes linéairement réductifs :

Proposition 13

1. *Si G est un groupe fini dont l'ordre est premier avec la caractéristique de $\mathbb{K}$, alors G est linéairement réductif.*
2. *Dans le cas $V = \mathbb{K}^n$, le sous-groupe T des matrices diagonales inversibles est linéairement réductif.*

Démonstration : 1. Soient ρ et w tels que dans la définition. Posons

$$P = |G|^{-1} \sum_{g \in G} \rho(g).$$

P est une application linéaire qui vérifie $P^2 = P$: c'est donc une projection. On a alors que W est la somme directe des sous-espaces propres $\ker P$ et $\operatorname{Im} P$. De plus, $P(w) = w$ donc $w \in \operatorname{Im} P$. Soit W' un supplémentaire de $\mathbb{K}w$ dans $\operatorname{Im} P$. Soit f une application linéaire dont le noyau est $\ker P + W'$. Montrons que f vérifie les propriétés demandées. $f(w) \neq 0$ par choix du noyau : w est dans le complémentaire de W' dans $\operatorname{Im} P$. f est G-invariante : on a la décomposition suivante de W

$$W = \ker P \oplus W' \oplus \mathbb{K}w = \ker f \oplus \mathbb{K}w$$

Soit $x = x_k + \lambda w$ une décomposition adaptée. Alors

$$(g \cdot f)(x) = f(g^{-1}x_k) + f(g^{-1}\lambda w) = 0 + f(\lambda w) = f(x_k) + f(\lambda w) = f(x)$$

d'où le résultat.

2. Soient ρ tel que dans la définition et $t = \operatorname{diag}(x_1, \ldots, x_n)$. ρ est une représentation polynômiale, donc les coordonnées de $\rho(t)$ dans une certaine base de W sont des combinaisons linéaires de monômes $x_1^{a_1} \ldots x_n^{a_n}$, avec $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Pour un tel $(a_1, \ldots, a_n)$ fixé, l'application $\chi : t \longmapsto \chi(t) = x_1^{a_1} \ldots x_n^{a_n}$ est une représentation polynômiale de T dans $GL_1(\mathbb{K})$. On l'appelle caractère polynômial de T. Il existe alors un ensemble fini S de caractères et des endomorphismes de W A_χ tels que

$$\rho(t) = \sum_{\chi \in S} \chi(t) A_\chi \tag{1}$$

ρ et les χ sont des morphismes donc $\rho(tt') = \rho(t)\rho(t')$ et $\chi(tt') = \chi(t)\chi(t')$ et en utilisant ces deux égalités dans l'égalité 1 on obtient l'égalité :

$$\sum_{\chi \in S} \chi(t)\chi(t') A_\chi = \sum_{\chi, \chi' \in S} \chi(t)\chi'(t') A_\chi A_{\chi'}$$

D'après (Lang 2002), les caractères sont linéairement indépendants. On en déduit :

$$\chi(t) A_\chi = \sum_{\chi' \in S} \chi'(t) A_{\chi'} A_\chi$$

En réutilisant à nouveau l'indépendance des caractères, on en déduit les trois résultats suivants :

$$A_\chi A_{\chi'} = 0 \quad (\chi \neq \chi') \tag{2}$$

$$A_\chi^2 = A_\chi \tag{3}$$

$$\sum_{\chi \in S} A_\chi = \mathrm{id} \tag{4}$$

(Pour la dernière égalité, il suffit de prendre l'égalité 1 avec $t = \mathrm{id}$). On pose ensuite $W_\chi = A_\chi W$. Montrons que W est somme directe des W_χ. L'égalité 4 donne directement que W est somme des W_χ. Montrons que la somme est directe. Soit $0 = \sum_{\chi \in S} w_\chi$ une décomposition dans cette somme de 0. En appliquant chaque A_χ et en utilisant les égalités 2 et 3, on voit que pour tout $\chi \in S, w_\chi = 0$, d'où la décomposition unique. De même, chaque W_χ est stable par $\rho(t)$ et la restriction à W_χ de $\rho(t)$ est la multiplication par $\chi(t)$: $\rho(t)$ est diagonale dans une base associée à la somme directe des W_χ.
Soit w tel que dans la définition 9. On a $w \in W_1$, où 1 désigne le caractère de T qui envoie t sur 1. Soit W_1' un supplémentaire de $\mathbb{K}w$ dans W_1. Soit f une fonction linéaire dont l'ensemble des zéros est $W_1' + \sum_{\chi \neq 1} W_\chi$. Par le même argument que dans la démonstration précédente, f vérifie les propriétés requises. ■

Remarque 6. L'opérateur P tel que défini dans la première démonstration n'est pas juste un objet quelconque de cette démonstration : il correspond à l'idée "d'effectuer la moyenne" sur les éléments de G. C'est cette idée fondamentale qui est à l'origine de l'opérateur de Reynolds que nous allons étendre à des groupes infinis et utiliser pour démontrer le résultat principal de cette partie.

3.2 Représentation semi-simple

Par la suite, nous aurons besoin de la notion de représentation semi-simple :

Définition 10

Soit G un groupe quelconque, et $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation de V. On dit que V est un G-module.

1. *ρ est dite réductible s'il existe un sous-espace W de V ni nul ni égal à V tel que W soit stable par ρ : c'est à dire que pour tout $g \in G, w \in W, \rho(g)W \in W$. Sinon, ρ est dite irréductible.*
2. *ρ est dite semi-simple si pour tout sous-espace W stable par $\rho(G)$, il existe un supplémentaire W' qui est lui aussi stable par $\rho(G)$.*

Nous faisons maintenant le lien entre cette notion et celle de réductivité linéaire :

Proposition 14

Un groupe linéaire algébrique $G \subseteq \mathrm{GL}(V)$ est linéairement réductif si et seulement si toute représentation polynômiale de G est semi-simple.

Démonstration : On montre d'abord la réciproque. Soit ρ une représentation de G semi-simple. Soit w tel que dans la définition 9. $\mathbb{K}w$ est un espace $\rho(G)$-stable de V, et ρ est semi-simple donc il existe W supplémentaire $\rho(G)$-stable de $\mathbb{K}w$. Soit f application linéaire dont l'ensemble des zéros est W. Alors f vérifie les propriétés demandées (même type d'argument que dans la démonstration de la proposition 13).

On montre ensuite le sens direct. Supposons désormais G linéairement réductif et soit W un sous-espace $\rho(G)$-stable de V différent de V et de $\{0\}$. Soit $\overline{\rho}$ la représentation induite sur V/W (si v_1, v_2 sont dans la même classe d'équivalence, $v_1 - v_2 \in W$ $\rho(G)$-stable donc $\rho(g)(v_1 - v_2) \in W$ et la représentation quotient est bien définie). C'est une représentation polynômiale. Soit $H = \hom(V/W, V)$ l'espace des applications linéaires de V/W dans V. ρ induit une représentation polynômiale σ sur H :

$$(\sigma(g)h)(x) = \rho(g)h(\overline{\rho}(g)^{-1}x).$$

Soient π le morphisme canonique de V dans V/W et $s : V/W \longrightarrow V$ linéaire ($s \in H$) telle que $\pi \circ s = \mathrm{id}$. On pose H_1 le sous-espace de H engendré par $\{\sigma(g)s : g \in G\}$ et H_1' le sous-espace de H engendré par $\{\sigma(g)s - s : g \in G\}$. On remarque que H_1' est un sous-espace de H_1. Montrons tout d'abord qu'ils ne sont pas égaux : pour cela, montrons que

$$\pi\left(\sigma(g)s - s\right)(V/W) \subseteq \{0\}.$$

Remarquons tout d'abord que par définition de la représentation quotient, pour tout $g \in G$, $\overline{\rho(g)}\pi(v) = \pi(\rho(g)v)$. Soit $\tilde{v} \in V/W$. On a

$$\begin{aligned}\pi(\sigma(g)s - s)(\tilde{v}) &= \pi\rho(g)s\overline{\rho}(g^{-1})(\tilde{v}) - \pi s(\tilde{v}) \\ &= \overline{\rho}(g)\pi s\overline{\rho}(g^{-1})(\tilde{v}) - \tilde{v} \\ &= \tilde{v} - \tilde{v} = 0\end{aligned}$$

et on déduit alors que pour tout $h' \in H_1', \pi(h'(V/W)) \subseteq \{0\}$. Or $\pi(s(V/W)) = V/W$ donc $s \notin H_1'$, d'où le résultat. Soit alors l une application linéaire de H_1 dont l'ensemble des zéros est H_1'.

H_1 est stable sous l'action σ de G, on peut donc considérer la représentation τ de G dans H_1^*, le dual de $H_1(\tau(g)$ est l'application qui à ϕ dans le dual associe $\phi \circ \sigma(g^{-1}))$. Cette représentation est bien polynômiale. Montrons que $\tau(g)l = l$ pour tout g. Il suffit de montrer que pour tout $\tilde{g} \in G$, $[\tau(g)l](\sigma(\tilde{g})s) = l(\sigma(\tilde{g})s)$. Or

$$\begin{aligned}[\tau(g)l - l](\sigma(\tilde{g})s) &= l(\sigma(g^{-1})\sigma(\tilde{g})s - \sigma(\tilde{g})s) \\ &= l(\sigma(g^{-1}\tilde{g})s - s + s - \sigma(\tilde{g})s) \\ &= l(\sigma(g^{-1}\tilde{g})s - s) + l(s - \sigma(\tilde{g})s)) = 0\end{aligned}$$

où la dernière égalité vient que fait que $\ker l = H_1'$. On en déduit, par réductivité linéaire de G, qu'il existe une fonction linéaire s' sur H_1^*, ou, par isomorphisme canonique entre un espace vectoriel de dimension finie et son bidual, un élément s' de H_1 tel que $\sigma(g)s' = s'$ et $l(s') \neq 0$. $W' = s'(V/W)$ est alors un supplémentaire $\rho(G)$-stable de W, ce qui est le résultat voulu. ■

3.3 Opérateur de Reynolds et premier théorème

Plaçons nous dans le cas où G est un groupe fini dont l'ordre est premier avec la caractéristique du corps $\mathbb{K}$. On peut alors définir sur l'algèbre des fonctions polynômiales $S(V)$ l'application suivante, qui consiste à "effectuer la moyenne" :

$$\mathcal{R}: \begin{array}{ccc} S(V) & \longrightarrow & S(V) \\ f & \longmapsto & |G|^{-1} \sum_{g \in G} g \cdot f \end{array}$$

$\mathcal{R}$ vérifie trois propriétés caractéristiques :

1. $\mathcal{R}$ est une application $\mathbb{K}$-linéaire à valeurs dans $S(V)^G$
2. $\mathcal{R}$ vaut l'identité sur $S(V)^G$
3. $\mathcal{R}$ est un morphisme de $S(V)^G$-modules, c'est à dire, pour $f \in S(V), m \in S(V)^G, \mathcal{R}(mf) = m\mathcal{R}(f)$

On définit alors :

Définition 11

*Soit $G \subseteq \mathrm{GL}(V)$. Tout fonction de $S(V)$ vérifiant les trois propriétés précédentes est appelé **opérateur de Reynolds** (pour G).*

Un des premiers grands résultats, dû à Hilbert, se base exclusivement sur l'existence d'un opérateur de Reynolds. Nous allons énoncer et démontrer ce résultat, puis, ensuite, nous montrerons que tout groupe linéairement réductif induit un opérateur de Reynolds, ce qui démontrera notre première caractérisation.

Théorème 3 (*Hilbert*)

Soit $G \subseteq \mathrm{GL}(V)$. Si G induit un opérateur de Reynolds sur $S(V)$ alors l'algèbre des invariants $S(V)^G$ est de type fini.

Démonstration : D'après la première propriété de l'opérateur de Reynolds, $S(V)^G$ est l'espace vectoriel engendré par les $\mathcal{R}(T_1^{e_1} \dots T_n^{e_n})$ avec $(e_1, \dots, e_n) \in \mathbb{N}^n$. Soit I_G l'idéal (de $S(V)$) engendré par les $\mathcal{R}(T_1^{e_1} \dots T_n^{e_n})$ pour $(e_1, \dots, e_n) \neq (0, \dots, 0)$. On a montré que $S(V)$ était noethérien donc I_G est un idéal de type fini : il existe $p_1, \dots, p_m$ tels que $I_G = \langle p_1, \dots, p_n \rangle$.

Montrons que $S(V)^G = \mathbb{K}[p_1, \dots, p_m]$. Supposons par l'absurde que ce ne soit pas le cas. Il existe $q \in S(V)^G \backslash \mathbb{K}[p_1, \dots, p_m]$. Quitte à décomposer q dans l'algèbre graduée $S(V)^G$, on peut supposer q homogène. Choisissons alors q homogène de degré minimal.

On a $q \in I_G$, donc il existe $f_1, \dots, f_m$ homogènes de degrés strictement inférieurs au degré de q tels que

$$q = f_1 p_1 + \dots + f_m p_m.$$

On applique l'opérateur de Reynolds à cette égalité et d'après les propriétés 2 et 3 :

$$q = \mathcal{R}(f_1) p_1 + \dots + \mathcal{R}(f_m) p_m.$$

Par minimalité du degré de q, les $\mathcal{R}(f_i)$ appartiennent à $\mathbb{K}[p_1, \dots, p_m]$, donc q aussi, ce qui conclut la preuve. ■

3.4 Opérateur de Reynolds pour les groupes linéairement réductifs

Proposition 15

Soit $G \subseteq \mathrm{GL}(V)$ un groupe linéairement réductif. Il existe un opérateur de Reynolds $\mathcal{R}$ pour $S(V)$.

Démonstration : Considérons la décomposition de $S(V)$ en algèbre graduée $S(V) = \bigoplus_{d\in\mathbb{N}} S_d$ Chaque sous-espace S_d est de dimension finie, et stable sous l'action de G. Soit ρ_d la représentation induite sur S_d. C'est une représentation polynômiale. Par la proposition 14, ρ_d est semi-simple. Il existe donc un supplémentaire T_d $\rho_d(G)$-stable au sous-espace S_d^G des polynômes homogènes de degré d invariants. On peut donc écrire :

$$S(V) = \bigoplus_{d\in\mathbb{N}} (S_d^G + T_d) = \bigoplus_{d\in\mathbb{N}} S_d^G \oplus \bigoplus_{d\in\mathbb{N}} T_d = S(V)^G \oplus T$$

où T est G-stable.

Montrons que P, la projection sur $S(V)^G$ parallèlement à T est un opérateur de Reynolds. Les deux premières propriétés découlent directement du fait que c'est une projection. Il reste à démontrer la propriété suivante :

$$\forall f \in S(V), \forall m \in S(V)^G, P(mf) = mP(f)$$

Décomposons $f = f_m + f_t$ et $m = m + 0$ dans la somme directe. On a $mf = mf_m + mf_t$, et si l'on montre que mf_t appartient à T, on aura $P(mf) = mf_m = mP(f)$ et le résultat sera obtenu. Montrons alors que $mf_t \in T$.

Soit V un espace vectoriel de dimension fini, irréductible, invariant sous l'action de G, inclus dans T et tel que $f_t \in T$. Par le lemme de Schur, soit $mV = 0$, soit V est isomorphe à mV un sous espace irréductible et invariant. Puisque m est invariant, les représentations de G sur V sont isomorphes et non-triviales, ce qui implique que $mV \subset T$, ce qui termine la démonstration. ■

4 Réductivité : l'approche de Nagata

Dans cette seconde approche, nous allons partir d'une hypothèse plus faible sur le groupe linéairement algébrique G : celle de réductivité (ou réductivité géométrique). Nous verrons par la suite que cette hypothèse n'est réellement utile que pour les corps dont la caractéristique est strictement positive.

4.1 Réductivité géométrique

Définition 12

Soit G un groupe linéairement algébrique. On dit que G est réductif (ou géométriquement réductif) si pour toute représentation polynômiale $\rho : G \longrightarrow \mathrm{GL}(W)$ et pour tout $w \in W\backslash\{0\}$ tel que pour tout g, $\rho(g)w = w$, il existe une fonction polynômiale G-invariante telle que $f(w) \neq 0$ et $f(0) = 0$.

Remarque 7.
- G est donc linéairement réductif si on peut choisir f linéaire dans la définition.
- Il est équivalent de demander qu'il existe une fonction f homogène G-invariante et non constante telle que $f(w) \neq 0$. Si un telle fonction existe, alors elle remplit les hypothèses de la définition. Dans l'autre sens, soit f telle que dans la définition. On peut écrire

$$f = \sum_{d\geq 0} f_d$$

la décomposition en fonctions homogènes de f. $f(w) \neq 0$ donc il existe au moins un $d \geq 0$ tel que $f_d(w) \neq 0$. De plus, f_d ne peut être constante ; sinon, $f(0) = f_d(0) = f_d(w) \neq 0$ et on aurait une contradiction.

La prochaine proposition fait le lien entre réductivité linéaire et géométrique dans le cas de la caractéristique 0 :

Proposition 16

Supposons que $\mathbb{K}$ soit un corps de caractéristique 0. Alors G est linéairement réductif si et seulement si G est géométriquement réductif.

Démonstration : L'implication est évidente. Pour la réciproque, soient f et w tels que dans la définition 12. D'après la remarque précédente, on peut supposer f homogène de degré d. Soient f_i les fonctions polynômiales définies par :

$$f(w + xv) = \sum_{i=0}^{d} x^i f_i(v),\ x \in \mathbb{K}.$$

Les f_i sont homogènes de degré i : soit $\lambda \in \mathbb{K}$. Pour tout $x \in \mathbb{K}$,

$$f(w + x\lambda v) = \sum_{i=0}^{d} x^i \lambda^i f_i(v) = \sum_{i=0}^{d} x^i f_i(\lambda v).$$

L'égalité étant vraie pour tout x, on a, pour tout i, $f_i(\lambda v) = \lambda^i f_i(v)$. Les f_i sont aussi G-invariantes

$$\begin{aligned} f(w + x(g \cdot v)) &= f(g \cdot (g^{-1} \cdot w + xv)) \\ &= f(g^{-1} \cdot w + xv) \text{ par } G\text{-invariance de } f \\ &= f(w + xv) \text{ par invariance de } w \end{aligned}$$

et le même type d'égalité qu'au dessus étend le résultat aux f_i. f_1 est linéaire et G-invariante : il suffit de montrer que $f_1(w) \neq 0$. Or

$$\begin{aligned} f(w + xw) &= \sum_{i=0}^{d} x^i f_i(w) \text{ par définition de } f \\ &= f((x+1)w) = (x+1)^d f(w) = \sum_{i=0}^{d} \binom{d}{i} x^i f(w) \end{aligned}$$

d'où $f_1(w) = \binom{d}{1} f(w) \neq 0$ car en caractéristique 0, $\binom{d}{i}$ est différent de 0. ■

Remarque 8. Une proposition additionnelle que l'on ne démontrera pas ici permet encore plus de renforcer l'idée que la réductivité géométrique est la bonne notion pour étudier le cas de la caractéristique strictement positive : les seuls groupes linéairement réductifs en caractéristique strictement positive sont les tori (groupes isomorphes à un groupe de matrices diagonales), les groupes finis dont l'ordre est premier avec la caractéristique du corps, et les produits de tels groupes (Derksen et Kemper 2015).

La proposition suivante nous donne un exemple de groupes réductifs :

Proposition 17

Soit $G \in \mathrm{GL}_n(\mathbb{K})$ un groupe fini. Alors G est réductif.

Démonstration : Soit ρ une représentation polynômiale et w tels que dans la définition. Soit l une application linéaire qui ne s'annule pas en w. On pose $f = \prod_{g \in G}(g \cdot l)$. f est polynômiale, G-invariante. De plus :

$$f(w) = \prod_{g \in G} (g \cdot l)(w) = \prod_{g \in G} l(\rho(g)^{-1}(w)) = l(w)^{|G|} \neq 0.$$

f vérifie bien les hypothèses demandées. ■

4.2 Second théorème

Nous allons désormais démontrer un second théorème qui permet, dans le cas d'un groupe géométriquement réductif, de montrer que l'algèbre des fonctions polynômiales invariantes sous l'action du groupe est de type fini.

Nous aurons tout d'abord besoin du lemme suivant, permettant de caractériser la réductivité géométrique :

Lemme 3

Soit G un groupe linéaire algébrique. Supposons que G agisse sur $\mathbb{K}[T_1, \ldots, T_m]$ par automorphismes linéaires, tel que

$$g \cdot T_i = \sum_{j=1}^{m} x_{j,i}(g) T_j$$

où l'application de G dans $\mathrm{GL}_m(\mathbb{K})$ qui à g associe la matrice $(x_{j,i})$ est une représentation polynômiale de G.

Supposons de plus que pour tout $g \in G$, on ait $x_{1,1}(g) = 1$ et $x_{1,i}(g) = 0$ pour $i > 1$ (en particulier, $\mathbb{K}T_2 + \ldots + \mathbb{K}T_m$ est stable sous l'action de G).

Sous ces hypothèses, G est géométriquement réductif si et seulement si il existe un invariant homogène de $\mathbb{K}[T_1, \ldots, T_m]^G$ qui contienne un terme de la forme T_1^d.

Démonstration : La preuve consiste à réduire le problème au cas de $W = (\mathbb{K}T_1 + \ldots \mathbb{K}T_m)^*$ le dual de l'espace vectoriel engendré par les indéterminées. Montrons tout d'abord l'implication.

Supposons G géométriquement réductif. Supposons que G agisse sur $\mathbb{K}[T_1, \ldots, T_m]$ avec les hypothèses du lemme. Montrons tout d'abord l'égalité suivante :

$$\forall i, j \in \{1, \ldots, m\}, \forall g \in G, (g \cdot T_i^*)(T_j) = x_{i,j}(g^{-1})$$

(où T_i^* est l'application duale de T_i dans la base $(T_1, \ldots, T_m)$ et g agit sur W par $(g \cdot f)(x) = f(g^{-1}x)$). On a

$$\begin{aligned}(g \cdot T_i^*)(T_j) &= T_i^*(g^{-1} \cdot T_j) \\ &= T_i^*\left(\sum_{k=1}^{m} x_{k,j}(g^{-1}) T_k\right) \\ &= x_{i,j}(g^{-1})\end{aligned}$$

d'où l'égalité recherchée. On a alors, pour tout g, $(g \cdot T_1^*)(T_1) = x_{1,1}(g^{-1}) = 1$ et pour $i > 1$, $(g \cdot T_1^*)(T_i) = x_{1,i}(g^{-1}) = 0$, ce qui revient exactement à dire que $g \cdot T_1^* = T_1^*$ et donc que T_1^* est invariant sous l'action de G. En utilisant l'hypothèse de réductivité sur G, on obtient l'existence d'un invariant polynômial homogène f non constant tel que $f(T_1^*) \neq 0$. Cette dernière inégalité revient à dire que f contient un terme de la forme T_1^d.

Réciproquement, supposons qu'il existe un invariant homogène qui contienne un terme de la forme T_1^d dès que G agit sur $\mathbb{K}[T_1, \ldots, T_m]$ sous les hypothèses du lemme. Soit w un élément non nul invariant sous l'action de G de $(\mathbb{K}T_1 + \ldots \mathbb{K}T_m)^*$. On peut compléter w en une base $(w, w_2, \ldots, w_m)$ de W. Soit $(v, v_2, \ldots, v_m)$ une base antéduale. On peut alors vérifier que pour tout $g \in G$, selon les notations du lemme,

$$x_{1,1} = 1 \quad x_{1,i} = 0,\ i > 1.$$

Ainsi, il existe un invariant homogène f contenant un terme de la forme v^d, ce qui revient exactement à dire que $f(w) \neq 0$, ce qui montre la réductivité de G. ■

La preuve du théorème reposera essentiellement sur la réduction au cas des algèbres graduées ; par conséquent, nous aurons besoin de quelques résultats les concernant :

Définition 13

Soit $A = \bigoplus_{d\geq 0} A_d$ une algèbre graduée. Un idéal I de A est dit homogène si $I = \bigoplus_{d\geq 0}(I \cap A_d)$: c'est à dire, si $a \in I$, tous les éléments homogènes a_d de sa décomposition en éléments homogènes $a = \sum_{d\geq 0} a_d$ appartiennent eux aussi à l'idéal.
On peut alors munir l'algèbre quotient d'une graduation en posant $(A/I)_d = (A_d + I)/I$.

Lemme 4

Soit $A = \bigoplus_{d\geq 0} A_d$ une algèbre graduée. Si l'idéal $A^+ = \bigoplus_{d>0} A_d$ est de type fini alors A est une algèbre de type fini sur l'anneau A_0 (c'est à dire qu'il existe $a_1, \ldots, a_n \in A$ tels que $A = A_0[a_1, \ldots, a_n]$).

Démonstration : Voir (Springer 1977, p.23) ■

Nous aurons aussi besoin d'un lemme concernant les algèbres de type finis :

Définition 14

Soit B un anneau commutatif unitaire et A un sous-anneau de B. B est dit entier sur A si pour tout élément b de B, il existe $P \in A[X]$ unitaire tel que $P(b) = 0$.

Lemme 5

Soit B une $\mathbb{K}$-algèbre et A une sous-algèbre de B. Supposons que B est de type fini (sur $\mathbb{K}$) et entière sur A. Alors A est de type fini (sur $\mathbb{K}$).

Démonstration : B est de type fini, donc il existe $b_1, \ldots, b_s \in B$ tels que $B = \mathbb{K}[b_1, \ldots, b_s]$. B est entière sur A, donc il existe des éléments $a_{i,j}$ de A tels que, pour tout $i \in \{1, \ldots, s\}$,

$$b_i^{n_i} + a_{i,1} b_i^{n_i - 1} + \ldots + a_{i,n_i} = 0.$$

Soit $a_1, \ldots, a_t$ l'ensemble des éléments de A apparaissant dans ces équations, et posons $A' = \mathbb{K}[a_1, \ldots, a_t]$. C'est un anneau noethérien, comme quotient de l'algèbre $\mathbb{K}[T_1, \ldots, T_t]$. B est entière sur A' donc B est engendré en tant que A'-module par un nombre fini de monômes $b_1^{h_1} \ldots b_s^{h_s}$: c'est un A'-module de type fini. Un sous-module d'un module de type fini sur un anneau noethérien est lui aussi de type fini : ce qui montre que A est un A'-module de type fini. Soient $a_{t+1}, \ldots, a_n$ des générateurs de A en tant que A'-module. Alors on a $A = \mathbb{K}[a_1, \ldots, a_t, a_{t+1}, \ldots, a_n]$, ce qui montre le résultat. ■

Remarque 9. Ce résultat permet de montrer le résultat plus élémentaire suivant : pour tout groupe G fini, l'algèbre des invariants est de type fini : en effet, on pose $A = S(V)^G$, $B = S(V)$. Il suffit de montrer que B est bien entière sur A. Soit $f \in B$. Soit $P \in B[X]$ défini par $P(X) = \prod_{g\in G}(X - g \cdot f)$. On peut vérifier que P est à coefficients dans A, ce qui montre l'assertion. Le lemme précédent affirme alors que A est de type fini.

Soit $G \subseteq \mathrm{GL}(V)$ un groupe linéaire algébrique. Soient I et J des idéaux G-stables de $S := S(V)$ l'algèbre des fonctions polynômiales sur V tels que $I \subseteq J$. Posons $A = S/I$, $B = S/J$: ce sont des $\mathbb{K}$-algèbres. Soit ϕ le morphisme canonique de A vers B.

$$\begin{array}{ccc} S & \xrightarrow{\pi_b} & B \\ {\scriptstyle \pi_a}\downarrow & \nearrow_{\phi} & \\ A & & \end{array} \qquad \ker \pi_a = I \subseteq J = \ker \pi_b$$

G agit sur A et B par automorphismes linéaires ($g \cdot \pi(x) = \pi(g \cdot x)$, bien défini car I et J sont G-stables). On peut alors vérifier que pour tout $g \in G$, g et ϕ commutent. Soit $a = \pi_a(x) \in A$.

$$g \cdot \phi(a) = g \cdot \phi(\pi_a(x)) = g \cdot \pi_b(x) = \pi_b(g \cdot x) = \phi(\pi_a(g \cdot x)) = \phi(g \cdot \pi_a(x)) = \phi(g \cdot a).$$

Si I est un idéal homogène, alors A est une algèbre graduée, G stabilise les espaces A_d et les représentations de G dans les espaces A_d sont des représentations polynômiales.

On bénéficie alors du résultat suivant :

Lemme 6

Soient A^G, B^G les algèbres graduées des éléments G-invariants de A et B. Supposons que G est réductif. Si $b \in B^G$, alors il existe $a \in A^G$ et un entier $d \geq 1$ tel que $\phi(a) = b^d$. En particulier, B^G est entière sur le sous-anneau $\phi(A^G)$.

Démonstration : Si b vaut 0, alors on peut choisir $a = 0$. Supposons désormais $b \neq 0$, et soit $a_1 \in A$ un antécédent de B par ϕ. Soit $W \in A$ le sous-espace vectoriel (de dimension finie) engendré par l'ensemble $\{g \cdot a_1 : g \in G\}$, et W' le sous espace de W engendré par $\{g \cdot a_1 - a_1 : g \in G\}$. Montrons que $W' \neq W$ et $W = \mathbb{K}a_1 \oplus W'$. Pour tout $g \in G$,

$$\phi(g \cdot a_1 - a_1) = \phi(g \cdot a_1) - \phi(a_1) = g \cdot b - b = 0 \quad (b \text{ est invariant}).$$

Ainsi $W' \subseteq \ker \phi$ alors que $a_1 \notin \ker \phi$, ce qui montre la non égalité. Soit $w \in W$. On peut écrire :

$$w = \sum_{i=1}^{m} \lambda_i (g_i \cdot a_1) = \sum_{i=1}^{m} \lambda_i (g_i \cdot a_1 - a_1) + a_1 \sum_{i=1}^{m} \lambda_i.$$

ce qui montre que W est bien somme des espaces W' et $\mathbb{K}a_1$. La somme est directe : si l'intersection était différente de $\{0\}$, par égalité de dimension, elle contiendrait a_1 ; absurde car $a_1 \notin W'$. On peut remarquer que l'on retrouve ici la même construction que dans la démonstration de la proposition 14.

La représentation de G dans W est polynômiale et est telle que W' est un espace G-stable. Soit $(a_2, \ldots, a_n)$ une base de W'. $(a_1, \ldots, a_n)$ est alors une base de W. La représentation de G est polynômiale, de telle manière que l'on puisse écrire :

$$g \cdot a_i = \sum_{j=1}^{n} x_{j,i}(g) a_j.$$

Faisons agir G de manière similaire sur $\mathbb{K}[T_1, \ldots, T_n]$, c'est à dire que :

$$g \cdot T_i = \sum_{j=1}^{n} x_{j,i}(g) T_j.$$

Il existe un morphisme de $\mathbb{K}$-algèbres ψ de $\mathbb{K}[T_1, \ldots, T_n]$ dans A tel que $\psi(T_i) = a_i$, et l'on a que g et ψ commutent pour tout $g \in G$ (du fait que l'action est définie de manière similaire). Montrons désormais que l'action de G sur $\mathbb{K}[T_1, \ldots, T_n]$ vérifient les hypothèses du lemme 3. W' est G-stable donc, pour $i > 1$, $g \cdot a_i$ appartient à W', ce qui revient à dire que la composante en a_1 est nulle : $x_{1,i} = 0$. De plus, on a :

$$g \cdot a_1 - a_1 = \left(\sum_{j=1}^{n} x_{j,1}(g) a_j \right) - a_1 = (x_{1,1}(g) - 1) a_1 + \sum_{j=2}^{n} x_{j,i}(g) a_j.$$

Or on sait que cet élément appartient à W', ce qui revient à dire que $x_{1,1}(g) - 1 = 0$, $x_{1,1}(g) = 1$. Les hypothèses du lemme 3 sont bien vérifiées : par réductivité de G, il existe un invariant $f \in \mathbb{K}[T_1, \ldots, T_n]$ contenant un terme de la forme T_1^d. Posons alors $a := \psi(f)$. a est bien G-invariant, et peut s'écrire sous la forme :

$$a = a_1^d + \sum_{i=1}^{n} b_i c_i.$$

avec $b_i \in A$, $c_i \in W'$. On a alors

$$\phi(a) = \phi(a_1)^d + \sum_{i=1}^{n} \phi(b_i)\phi(c_i) = b^d.$$

ce qui prouve le lemme. ■

Nous allons enfin pouvoir démontrer le théorème principal de cette partie :

Théorème 4

Supposons G réductif. Soit I un idéal homogène G-stable de $S(V)$. Alors $(S/I)^G$ est une $\mathbb{K}$-algèbre de type fini.

Démonstration : On va raisonner par l'absurde. Supposons qu'il existe un idéal I homogène G-stable tel que $(S/I)^G$ ne soit pas une algèbre de type fini. Soit $\mathcal{F}$ la famille des tels idéaux. S est noethérien donc d'après la deuxième caractérisation des anneaux noethériens (voir la définition 2), il existe un idéal I_0 maximal pour cette famille, c'est à dire que pour tout idéal J tel que $I_0 \subset J$ et $I_0 \neq J$, $(S/J)^G$ est de type fini. Posons $A := S/I_0$. La maximalité de I_0 entraîne que pour tout idéal J homogène G-stable et non nul de A, $(A/J)^G$ est de type fini. En effet, si on pose $\tilde{J}$ l'idéal réciproque de J par la projection canonique, on a $J = \tilde{J}/I$ et par troisième théorème d'isomorphisme, $A/J = (S/I)/(\tilde{J}/I)$ est isomorphe à $S/\tilde{J}$ donc $(A/J)^G$ est isomorphe à $(S/\tilde{J})^G$ qui est de type fini. Soit ψ le morphisme canonique de A^G sur $(A/J)^G$ (la restriction de la projection ψ de A sur A/J à A^G, il suffit de vérifier qu'elle est bien à valeurs dans $(A/J)^G$. Mais pour tout $g \in G$ et $a \in A^G$, $g \cdot \psi(a) = \psi(g \cdot a) = \psi(a)$). Par le lemme 6, $(A/J)^G$ est entier sur $\psi(A^G)$, et par le lemme 5, $\psi(A^G)$ est de type fini. De plus, par le premier théorème d'isomorphisme, $\psi(A^G)$ est isomorphe à $A^G/(A^G \cap J)$. On en déduit donc :

Pour tout idéal J homogène G-stable non nul de A, $A^G/(A^G \cap J)$ est une $\mathbb{K}$-algèbre de type fini (résultat 1).

Supposons désormais qu'il existe $a \in A^G$ homogène de degré positif et non diviseur de zéro dans A. Montrons que $aA \cap A^G = aA^G$. Si $x \in aA^G$, x s'écrit ay avec $y \in A^G$. On a clairement $x \in aA$. Pour tout g, $g \cdot x = g \cdot (ay) = (g \cdot a)(g \cdot y) = ay = x$, donc $x \in A^G$. Réciproquement, soit $x \in aA \cap A^G$. x est G-invariant et s'écrit ay avec $y \in A$. Il suffit alors de montrer que y est G-invariant. Or $a(g \cdot y - y) = g \cdot (ay) - ay = 0$, et comme a n'est pas diviseur de zéro, $g \cdot y - y = 0$ et y est bien G-invariant. En prenant J $= aA$, on déduit alors que A^G/aA^G est de type fini (par le résultat 1). On va alors utiliser le lemme 4 pour montrer que A^G est de type fini, une contradiction. Il faut donc montrer que l'idéal $(A^G)^+$ (c'est à dire $\bigoplus_{d>0}(A^G)_d$) est de type fini. A^G/aA^G est de type fini donc noethérienne. Soit π la projection de A^G sur A^G/aA^G. $\pi((A^G)^+)$ est un idéal de A^G/aA^G : par la définition 2, c'est donc un idéal de type fini : il existe $\pi(a_1), \ldots, \pi(a_n)$ tels que $\pi((A^G)^+) = \langle \pi(a_1), \ldots, \pi(a_n) \rangle$. On voit alors facilement que $(A^G)^+ = \langle a_1, \ldots, a_n, a \rangle$. D'après le lemme, A^G est alors de type fini sur $(A^G)_0$ isomorphe à $\mathbb{K}$: c'est une $\mathbb{K}$-algèbre de type fini, contradiction. Tous les éléments homogènes de degré positif de A^G sont donc diviseurs de zéro.

Soit alors un tel a. Posons I_a l'ensemble des $x \in A$ tels que $ax = 0$. I_a est un idéal homogène G-stable non nul de A. donc $(A/I_a)^G$ est de type fini. $(A/I_a)^G$ est entière sur $A^G/(I_a \cap A^G)$ (premier paragraphe). En réutilisant la preuve du lemme 5, on voit alors que $(A/I_a)^G$ est un $A^G/(I_a \cap A^G)$-module de type fini. En utilisant le fait que $(A/I_a)^G$ et $(aA)^G$ sont isomorphes en tant que $A^G/(I_a \cap A^G)$-modules (on le montrera à la fin de la démonstration), on a que $(aA)^G$ est un A^G-module de type fini, ce qui revient à dire que c'est un idéal de A^G de type fini. De plus, en utilisant l'égalité $(aA)^G = aA \cap A^G$ et le résultat 1 avec $J = aA$, on trouve que $A^G/(aA)^G$ est une algèbre de type fini. Par le même argument qu'au paragraphe précédent, on en déduit que $(A^G)^+$ est de type fini, et ainsi que A^G est une algèbre de type fini, ce qui est absurde.

Montrons désormais que $(A/I_a)^G$ et $(aA)^G$ sont isomorphes en tant que $A^G/(I_a \cap A^G)$-modules. Soient π_2 la projection de A sur A/I_a et π_3 la projection de A^G sur $A^G/(I_a \cap A^G)$. Soit φ l'application de $(aA)^G$ dans $(A/I_a)^G$ qui à af associe $\pi_2(f)$. Montrons que φ est un isomorphisme de $A^G/(I_a \cap A^G)$-modules.

- φ est bien à valeurs dans $(A/I_a)^G$. Soient $af \in (aA)^G, g \in G$. On a :

$$0 = g \cdot af - af = a(g \cdot f - f)$$

  donc $g \cdot f - f \in I_a = \ker \pi_2$, d'où $\pi_2(f) = g \cdot \pi_2(f)$, le résultat recherché.
- φ est bien un morphisme de $A^G/(I_a \cap A^G)$-modules : soient $af_1, af_2 \in (aA)^G$,

$$\varphi(af_1 + af_2) = \varphi(a(f_1 + f_2)) = \pi_2(f_1 + f_2) = \varphi(af_1) + \varphi(af_2).$$

  Soient $af \in (aA)^G, \pi_3(\lambda) \in A^G/(I_a \cap A^G)$:

$$\varphi(\pi_3(\lambda) \cdot af) = \varphi(a\lambda f) = \pi_2(\lambda f) = \pi_2(\lambda)\pi_2(f) = \pi_3(\lambda) \cdot \pi_2(f)$$

– φ est bien injective : $\varphi(af) = 0 \Leftrightarrow f \in \ker \pi_2 = I_a \Leftrightarrow af = 0$
– φ est bien surjective : soit $\pi_2(f) \in (A/I_a)^G$. Il suffit de montrer que af est bien G-invariant :

$$g \cdot (af) - af = a(g \cdot f - f) \quad \pi_2(g \cdot f - f) = 0$$

où la dernière égalité découle du fait que $\pi_2(f)$ est G-invariant. Ainsi $g \cdot f - f \in I_a$, ce qui revient exactement à dire que $a(g \cdot f - f) = 0$, l'égalité recherchée. ■

Corollaire 5

Si $G \subset \mathrm{GL}(V)$ est un groupe linéaire algébrique réductif, alors $S(V)^G$ est une $\mathbb{K}$-algèbre de typé fini.

Démonstration : Prendre I l'idéal nul dans le théorème précédent. ■

Ce dernier théorème permet de montrer que l'algèbre des invariants est de type fini dans de nombreux cas : Pour $\mathrm{SL}_n(\mathbb{K}), SO_n(\mathbb{K})$ par exemple, qui sont réductifs (voir Haboush 1975).

Remarque 10. Plus que l'hypothèse de réductivité géométrique, c'est la propriété du lemme 6, qui permet la démonstration du théorème ci-dessus. Bien que moins maniable, cette propriété permet d'étendre le résultat à plus de structures qu'à un corps algébriquement clos. On pourra notamment consulter Franjou et Van Der Kallen 2008 à ce sujet.

Ce dernier résultat n'est cependant pas une équivalence, comme nous allons le voir dans l'exemple suivant.

4.3 Exemple

On reprend l'exemple 2 : $\mathbb{K} = \mathbb{C}$ et $V = \mathbb{C}^2$. Soit $G = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \alpha \in \mathbb{C} \right\}$. On a montré que l'algèbre des invariants est de type fini : plus précisément $S(V)^G = \mathbb{K}[T_2]$. Nous désormais montrer le résultat suivant :

Proposition 18

G n'est pas un groupe réductif.

Démonstration : On utilise la caractérisation du lemme 3 : montrons que G vérifie les hypothèses du théorème. On pose $g_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. G agit par automorphisme linéaires sur $\mathbb{K}[T_1, T_2]$ par

$$g_\alpha \cdot T_1 = T_1 - \alpha T_2 \quad g_\alpha \cdot T_2 = T_2$$

ce qui montre que $x_{1,1} = 1$ et $x_{1,2} = 0$. Ainsi, d'après le lemme 3, si G était réductif, il existerait un invariant contenant un terme de la forme T_1^d, ce qui n'est pas le cas ici. G n'est donc pas réductif. ■

Remarque 11. On pourrait, en vue de tous les exemples considérés, se demander si l'algèbre des invariants n'est pas toujours de type fini quelque soit le groupe considéré. Cette question resta longuement sans réponse ; elle fit d'ailleurs l'objet du quatorzième problème de Hilbert. Ce n'est qu'en 1958 que Nagata fournit un contre-exemple pour $V = \mathbb{C}^{16}$ (voir Nagata 1959).

5 Théorie des invariants des groupes finis

Après avoir étudié la première question de la théorie des invariants dans un cadre général, nous nous intéressons désormais aux autres questions dans le cadre plus restreint des groupes finis :
– Déterminer des générateurs de l'algèbre des invariants
– Déterminer leurs relations de dépendance algébrique

– Donner un algorithme pour exprimer un invariant donné comme polynôme en les générateurs.

Dans cette partie, nous nous placerons dans le cas où le corps de base est $\mathbb{C}$, pour pouvoir entre autre utiliser l'opérateur de Reynolds

$$\mathcal{R}(f) = |G|^{-1} \sum_{g \in G} g \cdot f$$

quelque soit l'ordre du groupe G. Cependant, la plupart des résultats présentés ici s'étendent aux corps de caractéristiques strictement positives.

Les deux dernières questions, à savoir déterminer les relations de dépendance algébrique et donner un algorithme pour exprimer un invariant donné comme polynôme en les générateurs, portent plus sur les algorithmes de polynômes, notamment sur ceux utilisant les bases de Gröbner. Nous ne rentrerons donc pas dans le détail des bases, sujet qui mériterait un dossier à lui seul. On pourra cependant trouver une introduction aux bases de Gröbner en lien avec la théorie des invariants dans Derksen et Kemper 2015.

5.1 Premiers résultats

Dans la partie précédente, nous avons déjà démontré le résultat suivant :

Théorème 5

Si $G \in \mathrm{GL}(V)$ est un groupe fini, alors l'algèbre des invariants $S(V)^G$ est de type fini

Nous pouvons cependant déjà améliorer ce résultat dans le cas des groupes finis, grâce au théorème suivant :

Théorème 6 (*Majoration du degré de Noether*)

Soit $G \in GL(V)$ un groupe fini, n la dimension de V. L'algèbre des invariants $S(V)^G$ a une base d'algèbre avec au plus $\binom{n+|G|}{n}$ invariants dont le degré est majoré par l'ordre du groupe $|G|$.

Pour démontrer ce théorème, nous aurons besoin du lemme suivant portant sur les polynômes symétriques :

Lemme 7

L'algèbre des polynômes symétriques $\mathbb{K}[F_1, \ldots, F_n]$ est engendrée par les polynômes $P_1, \ldots, P_n$ définis par

$$P_k = \sum_{i=1}^{n} T_i^k$$

appelés sommes de puissances.

Démonstration : Voir Sturmfels 2008, p.4. ■

Démonstration Théorème : A tout vecteur d'entiers naturels $\Theta = (e_1, \ldots, e_n)$, on associe l'invariant homogène $J_\Theta = \mathcal{R}(T_1^{e_1} \ldots T_n^{e_n})$. On pose $\theta = e_1 + \ldots + e_n$. Soient $U_1, \ldots, U_n$ de nouvelles variables. Posons

$$\begin{aligned} S_\theta(U_1, \ldots, U_n, T_1, \ldots T_n) &= \mathcal{R}\left((U_1 T_1 + \ldots + U_n T_n)^\theta\right) \\ &= |G|^{-1} \sum_{g \in G} [U_1(T_1 \circ g) + \ldots + U_n(T_n \circ g)]^\theta \end{aligned}$$

le polynôme en les nouvelles variables dont les coefficients sont des polynômes en les anciennes variables. En développant l'expression ci-dessus, on trouve que le coefficient de $U_1^{e_1} \ldots U_n^{e_n}$ (qu'on appelle U-coefficient) dans S_θ est égal à J_Θ multiplié par un entier positif.

Les polynômes S_Θ sont les sommes de puissances en les $|G|$ variables $U_1(T_1 \circ g) + \ldots + U_n(T_n \circ g)$. Par le lemme précédent, chaque S_θ peut alors s'exprimer comme un polynôme en les $|G|$ sommes de puissances $S_1, \ldots, S_{|G|}$. Ainsi, tous les U-coefficients sont des polynômes en les U-coefficients de $S_1, \ldots, S_{|G|}$. Or les U-coefficients sont les J_Θ multipliés par un entier positif : ceci montre donc que chaque J_Θ s'exprime comme polynôme en les J_Θ tels que $\theta \leq |G|$. Or, les J_Θ engendre l'algèbre des invariants, d'où

$$S(V)^G = \mathbb{C}[\{J_\Theta : \theta \leq |G|\}.$$

De plus, l'ensemble des vecteurs d'entiers tels que $e_1 + \ldots + e_n \leq |G|$ vaut $\binom{n+|G|}{n}$, ce qui achève la démonstration. ■

Ce premier résultat donne déjà un moyen de déterminer un système de générateurs dans le cas d'un groupe fini. La construction de l'opérateur de Reynolds montre que celui-ci conserve le degré des éléments homogènes : ainsi, pour déterminer un système fini de générateurs, il suffit de calculer

$$\{\mathcal{R}(T_1^{e_1} \ldots T_n^{e_n}) : e_1 + \ldots e_n \leq |G|\}.$$

Néanmoins, la méthode est peu satisfaisante. Le système de générateurs n'est en général pas minimal : il existe des sous-ensembles stricts qui engendrent eux aussi l'algèbre des invariants.

Pour améliorer cette méthode, nous allons introduire un nouvel outil : les séries de Hilbert.

5.2 Séries de Hilbert et algèbre des invariants

On commence par introduire les séries de Hilbert :

Définition 15

Soit $A = \sum_{d \leq 0} A_d$ une $\mathbb{K}$-algèbre graduée. On suppose de plus que pour tout $d \in \mathbb{N}$, A_d est un $\mathbb{K}$-espace vectoriel de dimension finie. Alors la série de Hilbert de A est la série entière définie par :

$$H(A, z) = \sum_{d=0}^{\infty} \dim(A_d) z^d.$$

On dispose du résultat suivant, restreignant les formes possibles des séries de Hilbert :

Proposition 19

Si $A = \mathbb{K}[s_1, \ldots, s_n]$ où les s_i sont des éléments homogènes de degré d_i, alors il existe un polynôme $P \in \mathbb{Z}[T]$ tel que

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

Démonstration : Voir Springer 1977 ■

On démontre cependant le résultat suivant, précisant le résultat si les éléments sont algébriquement indépendants, qui nous servira lorsque l'on cherchera une décomposition en somme directe de l'algèbre des invariants :

Proposition 20

Si $A = \mathbb{K}[s_1, \ldots, s_n]$ où les s_i sont des éléments homogènes de degré d_i, algébriquement indépendants, alors

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

Démonstration : Les s_i sont algébriquement indépendants, ce qui revient à dire que tous les monômes $s_1^{a_1} \dots s_n^{a_n}$ sont linéairement indépendants. Ainsi,

$$\{s_1^{a_1} \dots s_n^{a_n} : a_1 d_1 + \dots + a_n d_n = d\}$$

est une base de l'espace vectoriel A_d. Ainsi, la dimension de A^d est égale au cardinal de

$$N_d := \{(a_1, \dots, a_n) \in N^n : a_1 d_1 + \dots + a_n d_n = d\}.$$

On a alors

$$\begin{aligned}
\frac{1}{\prod_{i=1}^n (1 - z^{d_i})} &= \prod_{i=1}^n \frac{1}{1 - z^{d_i}} \\
&= \prod_{i=1}^n \left(\sum_{j_i=0}^{\infty} z^{j_i d_i} \right) \\
&= \sum_{d=0}^{\infty} \sum_{j_1, \dots, j_n \in N_d} z^d \\
&= \sum_{d=0}^{\infty} |N_d| z^d
\end{aligned}$$

ce qui prouve le résultat. ■

L'utilité des séries de Hilbert dans le cas des invariants d'un groupe fini est qu'il est possible de calculer la série de Hilbert de l'algèbre des invariants sans connaître ses générateurs, grâce au résultat suivant :

Théorème 7 (*Molien*)

La série de Hilbert de l'algèbre des invariants $S(V)^G$ est égale à

$$\phi_G(z) = |G|^{-1} \sum_{g \in G} \frac{1}{\det(\mathrm{id} - zg)}.$$

Pour le démontrer, nous auront besoin du résultat intermédiaire suivant :

Lemme 8

Soit $G \subset \mathrm{GL}(V)$ un groupe fini. Alors la dimension du sous-espace invariant V^G des éléments $v \in V$ tels que pour tout $g \in G$, $g \cdot v = v$ vaut $|G|^{-1} \sum_{g \in G} \mathrm{Tr}(g)$.

Démonstration : Soit $P = |G|^{-1} \sum_{g \in G} g$. On vérifie que P est une projection sur l'espace V^G. Or, dans le cas d'une projection P, la dimension de l'image de P est égale à la trace de P, ce qui démontre le résultat. ■

Démonstration Théorème de Molien : On pose $S(V) = \sum_{d \geq 0} S_d$. S_d est de dimension $\binom{n+d-1}{d}$

Tout élément $g \in G$ induit un endomorphisme g_d sur chaque espace S_d, et dans ce cas, S_d^G est précisément l'espace des éléments invariants pour le groupe composé des g_d.

Pour calculer la trace de g_d, on identifie V avec son espace dual S_1. Soient $l_{g,1}, \dots, l_{g,n}$ les vecteurs propres de g et $\rho_{g,1}, \dots, \rho_{g,n}$ les valeurs propres associées.

On remarque ensuite que les éléments $l_{g,1}^{d_1} \dots l_{g,n}^{d_n}$ sont des vecteurs propres de S_d où $d = d_1 + \dots + d_n$, et qu'il y a exactement $\binom{n+d-1}{d}$ éléments de cette forme : ce sont donc précisément les vecteurs propres de S_d, de valeurs propres associées $\rho_{g,1}^{d_1} \dots \rho_{g,n}^{d_n}$. La trace de g_d vaut donc

$$\mathrm{Tr}(g_d) = \sum_{d_1 + \dots + d_n = d} \rho_{g,1}^{d_1} \dots \rho_{g,n}^{d_n}$$

et d'après le lemme précédent, ce nombre est égal à la dimension de S_d. On obtient donc

$$\begin{aligned}
\phi_G(z) &= \sum_{d=0}^{\infty} |G|^{-1} \sum_{g\in G} \left(\sum_{d_1+\ldots+d_n=d} \rho_{g,1}^{d_1} \ldots \rho_{g,n}^{d_n} \right) z^d \\
&= |G|^{-1} \sum_{g\in G} \sum_{(d_1,\ldots,d_n)\in\mathbb{N}^n} \rho_{g,1}^{d_1} \ldots \rho_{g,n}^{d_n} z^{d_1+\ldots+d_n} \\
&= |G|^{-1} \sum_{g\in G} \frac{1}{(1-z\rho_{g,1})\ldots(1-z\rho_{g,n})} \\
&= |G|^{-1} \sum_{g\in G} \frac{1}{\det(\mathrm{id}-zg)}.
\end{aligned}$$

■

Ces résultats nous fournissent directement un algorithme pour déterminer si un ensemble d'invariants $\{s_1, \ldots, s_n\}$ engendre l'algèbre des invariants. Soit $R = \mathbb{K}[s_1, \ldots, s_n]$. Si $H(R, z) = \phi_G(z)$, alors le système est une base d'algèbre. Sinon, on peut écrire

$$\phi_G(z) - H(R, z) = c_d z^d + \text{termes de plus haut degré.}$$

Il existe alors c_d invariants linéairement indépendants de degré d qui ne peuvent s'exprimer comme polynômes en $s_1, \ldots, s_n$: on les calcule grâce à l'opérateur de Reynolds, on les rajoute à notre ensemble et on recommence avec le nouvel ensemble obtenu.

Le problème se réduit alors à calculer $H(R, z)$. Soit I le noyau du morphisme de $\mathbb{K}[T_1, \ldots, T_n]$ dans $\mathbb{K}[s_1, \ldots, s_n]$ (qu'il est possible de calculer grâce aux bases de Gröbner, cela revient à déterminer les relations de dépendance algébriques entre $s_1, \ldots, s_n$). R est isomorphe à $\mathbb{K}[T_1, \ldots, T_n]/I$ en tant qu'algèbre graduée, où l'on pose que le degré de chaque variable T_i est égal au degré de s_i. Il est alors possible de calculer la série de Hilbert de cette dernière algèbre en calculant une base de Gröbner de I (voir Derksen et Kemper 2015, p.25).

Exemple 7 (Exemple d'application de l'algorithme)**.** On se place sur $\mathbb{K} = \mathbb{C}$, $V = \mathbb{C}^2$, et l'on considère le groupe à 4 éléments G engendré par la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On commence par calculer la série de Hilbert de $S(V)^G$ grâce au théorème de Molien :

$$\begin{aligned}
\phi_G(z) &= \frac{1}{4}\left[\frac{1}{\begin{vmatrix} 1-z & 0 \\ 0 & 1-z \end{vmatrix}} + \frac{1}{\begin{vmatrix} 1+z & 0 \\ 0 & 1+z \end{vmatrix}} + \frac{1}{\begin{vmatrix} 1 & z \\ -z & 1 \end{vmatrix}} + \frac{1}{\begin{vmatrix} 1 & -z \\ z & 1 \end{vmatrix}} \right] \\
&= \frac{1+z^4}{(1-z^2)(1-z^4)} \\
&= 1 + z^2 + 3z^4 + 3z^6 + \ldots
\end{aligned}$$

L'algorithme nous indique alors qu'il manque un invariant de degré 2. On applique l'opérateur de Reynolds aux monômes de degré 2 jusqu'à en trouver un non nul :

$$\mathcal{R}(T_1^2) = \frac{1}{4}(T_1^2 + T_1^2 + T_2^2 + T_2^2) = \frac{1}{2}(T_1^2 + T_2^2)$$

Quitte à multiplier par 2, on trouve comme premier invariant $s_1 = T_1^2 + T_2^2$. La série de Hilbert de $R_0 := \mathbb{C}[s_1]$ est, d'après la proposition 20 :

$$H(R_0, z) = \frac{1}{1-z^2} = 1 + z^2 + z^4 + \ldots$$

On a alors

$$\phi_G(z) - H(R_0, z) = 2z^4 + \dots$$

L'algorithme nous indique alors qu'il existe deux invariants linéairement indépendants de degré 4 qui n'appartiennent pas à R_0. On utilise l'opérateur de Reynolds jusqu'à les obtenir :

$$\mathcal{R}(T_1^2T_2^2) = (T_1^2T_2^2)$$
$$\mathcal{R}(T_1^3T_2) = \frac{1}{4}(T_1^3T_2 + T_1^3T_2 - T_1T_2^3 - T_1T_2^3) = \frac{1}{2}(T_1^3T_2 - T_1T_2^3)$$

Quitte à multiplier encore, on obtient $s_2 = T_1^2T_2^2$ et $s_3 = T_1^3T_2 - T_1T_2^3$. Calculons désormais la série de Hilbert de $R_1 = \mathbb{C}[s_1, s_2, s_3]$. Nous allons utiliser ici une méthode différente de celle présentée dans l'algorithme, n'ayant pas développé la théorie des bases de Gröbner. Le noyau du morphisme de $\mathbb{C}[U_1, U_2, U_3]$ dans R_1 est $\langle U_3^2 - U_2U_1^2 + 4I_2^2\rangle$. Ceci montre que tout polynôme $P \in H_1$ peut écrire de manière unique sous la forme

$$p(s_1, s_2, s_3) = q(I_1, I_2) + I_3 r(I_1, I_2)$$

ce qui revient à dire que l'on dispose de la décomposition en somme directe d'espaces vectoriels gradués :

$$\mathbb{C}[s_1, s_2, s_3] = \mathbb{C}[s_1, s_2] \oplus I_3\mathbb{C}[s_1, s_2].$$

La série de Hilbert de $R_2 := \mathbb{C}[s_1, s_2]$ est, d'après le lemme la proposition 20,

$$H(R_2, z) = \frac{1}{(1-z^2)(1-z^4)}.$$

Soit $R_3 := I_3R_2$. Les éléments de degré d de R_2 sont en bijection avec les éléments de degré $d+4$ de R_3, ce qui permet d'obtenir :

$$H(R_3, z) = \frac{z^4}{(1-z^2)(1-z^4)}.$$

Comme la somme directe est une somme directe d'espace gradués, on a

$$H(R_1, z) = H(R_2, z) + H(R_3, z) = \phi_G(z).$$

D'où $S(V)^G = \mathbb{C}[s_1, s_2, s_3]$.

5.3 Propriété de Cohen-Macaulay et décomposition d'Hironaka

Dans cette dernière partie, nous allons introduire la notion de propriété de Cohen-Macaulay pour une algèbre graduée, qui permet d'obtenir une décomposition en somme directe très pratique de l'algèbre en question (appelée décomposition d'Hironaka), et montrer que l'algèbre des invariants vérifie toujours cette propriété dans le cas d'un groupe fini. Nous donnerons ensuite un moyen de calculer la décomposition d'Hironaka

Remarque 12. Il est aussi possible de montrer que, plus généralement, l'algèbre des invariants vérifie la propriété de Cohen-Macaulay dans le cas où G est linéairement réductif. La preuve, hautement non triviale, ne sera pas faite ici. On pourra cependant consulter Derksen et Kemper 2015 à ce sujet.

Soit $R = \sum_{d\geq 0} R_d$ une $\mathbb{K}$-algèbre graduée de dimension n (le nombre maximal d'éléments algébriquement indépendants de R est n. Ce nombre est la dimension de Krull de R, $\dim(R)$).

Définition 16

Un système homogène de paramètres (s.h.d.p.) de R est un ensemble d'éléments homogènes de degré strictement positif $\{\theta_1 \dots, \theta_n\}$ tels que R est un module de type fini sur sa sous-algèbre $\mathbb{K}[\theta_1, \dots, \theta_n]$ (ce qui implique en particulier que $\theta_1, \dots, \theta_n$ sont algébriquement indépendants).

Lemme 9 (*Lemme de normalisation de Noether*)

Il existe toujours un s.h.d.p. pour R.

Démonstration : Voir Lang 2002. ■

Théorème 8

Soit R une $\mathbb{K}$-algèbre graduée, et $\theta_1, \dots, \theta_n$ un s.h.d.p de R. On a équivalence entre les deux propositions suivantes :

- *R est un module libre de type fini sur $\mathbb{K}[\theta_1, \dots, \theta_n]$: il existe $b_1, \dots, b_t \in R$ (que l'on peut choisir homogènes) tels que*
$$R = \bigoplus_{i=1}^{t} b_i \mathbb{K}[\theta_1, \dots, \theta_n].$$
- *Le résultat précédent est vrai pour tout s.h.d.p $\phi_1, \dots, \phi_n$ de R.*

Si les deux conditions sont vraies, alors $b_1, \dots, b_t$ forment une base de R si et seulement si leurs images forment une base du $\mathbb{K}$-espace vectoriel $R/\langle \theta_1, \dots, \theta_n \rangle$.

Si R vérifie les deux propositions équivalentes, alors on dit que R est de Cohen-Macaulay ou vérifie la propriété de Cohen-Macaulay. La décomposition en somme directe donnée dans la première équivalence est une décomposition d'Hironaka de R.

Démonstration : Voir Sturmfels 2008. ■

Remarque 13. L'anneau de polynômes $\mathbb{K}[T_1, \dots, T_n]$ vérifie la propriété de Cohen-Macaulay : il suffit de prendre $T_1, \dots, T_n$ comme s.h.d.p.

Théorème 9

Si G est un groupe fini, alors $S(V)^G$ vérifie la propriété de Cohen-Macaulay.

Démonstration : Rappelons le fait suivant : $S(V)$ est un module de type fini sur $S(V)^G$ (vu dans la remarque 9). De plus, on a la décomposition en somme directe de $S(V)^G$-modules $S(V) = S(V)^G \oplus T$ où T est le noyau de l'opérateur de Reynolds.

Le lemme de normalisation de Noether donne l'existence d'un s.h.d.p. $\theta_1, \dots, \theta_n$ de $S(V)^G$. $S(V)$ est fini sur $S(V)^G$ qui est fini sur $\mathbb{K}[\theta_1, \dots, \theta_n]$, donc $S(V)$ est fini sur $\mathbb{K}[\theta_1, \dots, \theta_n] : \theta_1, \dots, \theta_n$ forment un s.h.d.p. pour $S(V)$. Or $S(V)$ est de Cohen-Macaulay : ainsi, $S(V)$ est un $\mathbb{K}[\theta_1, \dots, \theta_n]$-module libre de type fini.

De la décomposition $S(V) = S(V)^G \oplus T$, on obtient la décomposition de $\mathbb{K}$-espaces vectoriels de dimensions finies :

$$S(V)/\langle \theta_1, \dots, \theta_n \rangle = S(V)^G/\langle \theta_1, \dots, \theta_n \rangle \oplus U/\langle \theta_1 U, \dots, \theta_n U \rangle$$
$$f + \sum h_i \theta_i \mapsto \mathcal{R}(f) + \sum \mathcal{R}(h_i)\theta_i + (f - \mathcal{R}(f)) + \sum (\mathcal{R}(h_i) - h_i)\theta_i$$

Soit une base homogène $\overline{b_1}, \dots, \overline{b_t}, \overline{b_{t+1}}, \dots, \overline{b_s}$ de $S(V)/\langle \theta_1, \dots, \theta_n \rangle$ telle que $\overline{b_1}, \dots, \overline{b_t}$ soit une base de $S(V)^G/\langle \theta_1, \dots, \theta_n \rangle$ et $\overline{b_{t+1}}, \dots, \overline{b_s}$ une base de $U/\langle \theta_1 U, \dots, \theta_n U \rangle$.

Soient $b_1, \dots, b_s \in S(V)^G$ tels que l'image de b_i soit $\overline{b_i}$. D'après le théorème 8, $b_1, \dots, b_s$ est alors une base de $S(V)^G$, ce qui donne la décomposition d'Hironaka recherchée et montre que $S(V)^G$ est de Cohen-Macaulay. ■

Nous allons voir maintenant comment obtenir une telle décomposition. Par la suite, les θ_i seront appelés invariants primaires de $S(V)^G$, et les b_j invariants secondaires. On notera $d_i := \deg(\theta_i)$ et $e_j := \deg(b_j)$.

On dispose du résultat suivant :

Proposition 21

Soient $\theta_1, \ldots, \theta_n$ une famille d'invariants primaires de G. Alors

1. *le nombre d'invariants secondaires vérifie $t = \frac{d_1 \ldots d_n}{|G|}$.*
2. *les degrés des invariants secondaires vérifient*

$$\phi_G(z) \times \prod_{i=1}^{n}(1 - z^{d_j}) = z^{e_1} + \ldots + z^{e_t}.$$

Démonstration : La décomposition d'Hironaka

$$S(V)^G = \bigoplus_{i=1}^{t} b_i \mathbb{K}[\theta_1, \ldots, \theta_n]$$

et la proposition 20 donne la formule suivante

$$\phi_G(z) = \left(\sum_{j=1}^{t} z^{e_j}\right) / \prod_{i=1}^{n}(1 - z^{d_i})$$

ce qui donne directement la seconde partie de la proposition. En utilisant le théorème de Molien, on a

$$|G|^{-1} \sum_{g \in G} \frac{1}{\det(\mathrm{id} - zg)} = \left(\sum_{j=1}^{t} z^{e_j}\right) / \prod_{i=1}^{n}(1 - z^{d_i}).$$

On multiplie de chaque côté par $(1 - z)^n$ pour obtenir

$$|G|^{-1} \sum_{g \in G} \frac{(1 - z)^n}{\det(\mathrm{id} - zg)} = \left(\sum_{j=1}^{t} z^{e_j}\right) / \prod_{i=1}^{n}(1 + z + \ldots + z^{d_j - 1})$$

. On prend la limite de cette expression quand z tend vers 1. $\frac{(1-z)^n}{\det(\mathrm{id} - zg)}$ converge vers 0 sauf pour la matrice identité, pour laquelle l'expression tend vers 1 : ainsi l'expression de gauche converge vers $\frac{1}{|G|}$. L'expression de droite converge vers $\frac{t}{d_1 \ldots d_n}$, ce qui donne la première partie de la proposition. ■

Remarque 14. La proposition donne une certaine forme d'unicité des invariants secondaires une fois que les invariants primaires sont fixés. Cependant, il n'y a pas unicité de la décomposition d'Hironaka : dans le cas trivial $G = \{1\}, V = \mathbb{K}$, on a

$$S(V)^G = \mathbb{K}[T] = \mathbb{K}[T^2] \oplus T\mathbb{K}[T^2].$$

Il ne reste finalement plus qu'à déterminer un moyen de calculer des invariants primaires pour un groupe donné. Nous donnons ici un algorithme dont nous ne ferons pas la preuve :

Entrée : L'opérateur de Reynolds d'un groupe fini G.
Sortie : Un s.h.d.p. $\theta_1, \ldots, \theta_n$ de $S(V)^G$
Pour i allant de 1 à n :
– Choisir une forme linéaire l_i sur V qui ne s'annule sur aucun des espaces $\langle l_1 \circ g_1, \ldots, l_{i-1} \circ g_{i-1}$ quelque soit le choix d'éléments de G
– Poser $\theta_i := \prod_{g \in G} l_i \circ g$.

Remarque 15. $\mathbb{K}$ est un corps infini, il est donc toujours possible de choisir une forme l_i telle que demandée dans l'algorithme.

Nous pouvons désormais fournir un algorithme donnant une décomposition d'Hironaka de l'algèbre des invariants.

Entrée : L'opérateur de Reynolds d'un groupe fini G.
Sortie : Une décomposition d'Hironaka de $S(V)^G$

1. Calculer $\phi_G(z)$, la série de Hilbert de $S(V)^G$ grâce au théorème de Molien
2. Calculer un ensemble d'invariants primaires grâce à l'algorithme précédent
3. Calculer le polynôme
$$\phi_G(z) \times \prod_{i=1}^{n}(1 - z^{d_j}) = c_1 z^{e_1} + \ldots + c_r z^{e_r}$$
4. En utilisant l'opérateur de Reynolds et la série de Hilbert, pour $i \in \{1, \ldots, r\}$, trouver c_i invariants linéairement indépendants dans $S(V)^G/\langle\theta_1, \ldots \theta_n\rangle$.

On termine en donnant un exemple de décomposition d'Hironaka d'une algèbre d'invariants :

Exemple 8. On se place sur $\mathbb{K} = \mathbb{C}$, $V = \mathbb{C}^2$. On pose $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.

La série de Hilbert de $S(V)^G$ vaut

$$\begin{aligned}
\phi_G(z) &= \frac{1}{2}\left(\frac{1}{\begin{vmatrix} 1-z & 0 \\ 0 & 1-z \end{vmatrix}} + \frac{1}{\begin{vmatrix} 1+z & 0 \\ 0 & 1+z \end{vmatrix}} \right) \\
&= \frac{1+z^2}{(1-z^2)^2} \\
&= 1 + 3z^2 + 5z^4 + \ldots
\end{aligned}$$

On cherche deux invariants primaires de degré 2. On trouve facilement que $s_1 = T_1^2$ et $s_2 = T_2^2$ conviennent. On cherche maintenant des invariants secondaires pour ces deux invariants. la proposition 21 nous donne qu'il y a $t = 2$ invariants secondaires et que leur degré vérifie $z^{e_1} + z^{e_2} = \phi_G(z) \times (1 - z^2)^2 = 1 + z^2$. On cherche donc un invariant secondaire de degré 1 (qui sera toujours 1) et un invariant secondaire de degré 2. En utilisant l'opérateur de Reynolds, on obtient

$$b_1 = 1 \quad b_2 = T_1 T_2.$$

On a donc la décomposition d'Hironaka suivante :

$$S(V)^G = \mathbb{C}[T_1^2, T_2^2] \oplus (T_1 T_2)\mathbb{C}[T_1^2, T_2^2].$$

Références

[1] Armand Borel. *Linear algebraic groups*. Second. T. 126. Graduate Texts in Mathematics. Springer-Verlag, New York, 1991, p. xii+288. ISBN : 0-387-97370-2. DOI : 10.1007/978-1-4612-0941-6. URL : http://dx.doi.org/10.1007/978-1-4612-0941-6.

[2] Harm Derksen et Gregor Kemper. *Computational invariant theory*. enlarged. T. 130. Encyclopaedia of Mathematical Sciences. With two appendices by Vladimir L. Popov, and an addendum by Norbert A. Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII. Springer, Heidelberg, 2015, p. xxii+366. ISBN : 978-3-662-48420-3 ; 978-3-662-48422-7. DOI : 10.1007/978-3-662-48422-7. URL : http://dx.doi.org/10.1007/978-3-662-48422-7.

[3] V. Franjou et W. Van Der Kallen. "Power reductivity over an arbitrary base". In : *ArXiv e-prints* (juin 2008). arXiv : 0806.0787 [math.RT].

[4] Paul Gordan. *Vorlesungen über Invariantentheorie*. Second. Erster Band : Determinanten. [Vol. I : Determinants], Zweiter Band : Binäre Formen. [Vol. II : Binary forms], Edited by Georg Kerschensteiner. Chelsea Publishing Co., New York, 1987, Vol. I : xii+201 pp., Vol. II : xii+360. ISBN : 0-8284-0328-7.

[5] W. J. Haboush. "Reductive groups are geometrically reductive". In : *Ann. of Math. (2)* 102.1 (1975), p. 67–83. ISSN : 0003-486X.

[6] Serge Lang. *Algebra*. third. T. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, p. xvi+914. ISBN : 0-387-95385-X. DOI : 10.1007/978-1-4613-0041-0. URL : http://dx.doi.org/10.1007/978-1-4613-0041-0.

[7] D. Mumford, J. Fogarty et F. Kirwan. *Geometric invariant theory*. Third. T. 34. Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]. Springer-Verlag, Berlin, 1994, p. xiv+292. ISBN : 3-540-56963-4. DOI : 10.1007/978-3-642-57916-5. URL : http://dx.doi.org/10.1007/978-3-642-57916-5.

[8] Masayoshi Nagata. "On the 14-th problem of Hilbert". In : *Amer. J. Math.* 81 (1959), p. 766–772. ISSN : 0002-9327.

[9] T. A. Springer. *Invariant theory*. Lecture Notes in Mathematics, Vol. 585. Springer-Verlag, Berlin-New York, 1977, p. iv+112.

[10] Bernd Sturmfels. *Algorithms in invariant theory*. Second. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, 2008, p. vi+197. ISBN : 978-3-211-77416-8.