

Sur un théorème de Chevalley

Benoît CLAUDON

9 novembre 2010

Résumé

Nous revenons sur un théorème de Claude Chevalley décrivant les invariants d'un groupe fini engendré par des réflexions complexes. Une conséquence intéressante de cette description est la lissité du quotient correspondant.

1 Invariants d'un groupe fini

Soient V un \mathbb{C} -espace vectoriel de dimension n et G un sous-groupe fini de $GL(V)$ d'ordre N . L'action de G sur V induit naturellement une action sur $A = \text{Sym}(V^*)$ l'algèbre des fonctions polynômiales sur V . En toute généralité, la structure de la sous-algèbre des invariants est décrite par le résultat suivant [Noe15].

Théorème 1.1 (E. Noether, 1915)

Soit G un groupe fini agissant sur une \mathbb{C} -algèbre A de type fini¹. La sous-algèbre A^G des éléments G -invariants est alors elle aussi de type fini et A est de type fini comme A^G -module.

Démonstration :

Remarquons tout d'abord que l'anneau A est entier² sur A^G : en effet, pour $a \in A$ le développement du produit (évidemment nul)

$$\prod_{g \in G} (a - g(a))$$

fournit l'identité (relations coefficients-racines) :

$$a^N + \sum_{k=1}^N (-1)^k \left(\prod_{(g_1, \dots, g_k) \in G^k} g_1(a) \dots g_k(a) \right) a^{N-k} = 0.$$

Les coefficients de cette relation polynômiale sont visiblement invariants par G et ceci montre que A est entier sur A^G . Appelons alors B la sous-algèbre de A engendrée par les coefficients apparaissant dans la relation ci-dessus lorsque a décrit un système fini (a_1, \dots, a_m) de générateurs de A . Comme toute \mathbb{C} -algèbre

1. ici \mathbb{C} pourrait être remplacé par n'importe quel anneau noethérien.

2. rappelons qu'un anneau A est dit entier sur un sous-anneau B si tout élément de A est racine d'un polynôme unitaire à coefficients dans B ; de manière équivalente, $B[a]$ est de type fini sur B pour tout élément $a \in A$.

de type fini, B est noethérienne et vérifie $B \subset A^G \subset A$. Comme A est engendrée par un nombre fini d'éléments qui sont entiers sur B , A est un B -module de type fini. Les invariants constituent donc un sous- B -module du B -module A et A^G est donc également un B -module de type fini (noethérianité de B). Il est alors immédiat d'en déduire que l'algèbre A^G est de type fini sur \mathbb{C} et que A est de type fini sur A^G . \square

Bien entendu, dans le cas général, les générateurs de l'algèbre des invariants vérifient des relations non triviales. Ainsi, si $G = \mathbb{Z}_2$ agit sur \mathbb{C}^2 par multiplication par $(x, y) \mapsto (-x, -y)$, l'algèbre des polynômes invariants est dans ce cas engendrée par $p = x^2$, $q = xy$ et $r = y^2$ et ces trois polynômes vérifient évidemment $pr = q^2$.

2 Cas des groupes de réflexions

Nous allons voir que, pour certains sous-groupes de $GL(V)$, l'algèbre des invariants est une algèbre libre.

Définition 2.1

Une réflexion (complexe) est une application linéaire qui fixe un hyperplan et qui est diagonalisable. Un groupe fini $G \subset GL(V)$ est appelé groupe de réflexions si il est engendré par des réflexions.

Le résultat de C. Chevalley [Che55] précise le théorème 1.1 dans les cas des groupes de réflexions.

Théorème 2.1 (C. Chevalley, 1955)

Si $G \subset GL(V)$ est un groupe de réflexions, l'algèbre des polynômes invariants $\text{Sym}(V^)^G$ est elle-même une algèbre de polynômes : il existe n polynômes homogènes invariants algébriquement indépendants (f_1, \dots, f_n) tels que*

$$\text{Sym}(V^*)^G = \mathbb{C}[f_1, \dots, f_n].$$

De plus, si d_i désigne le degré de f_i , l'ordre de G vérifie $N = \prod_{i=1}^n d_i$ et le nombre de réflexions de G est exactement $\sum_{i=1}^n (d_i - 1)$.

Ce résultat est une (vaste) généralisation du théorème classique sur les polynômes symétriques : tout polynôme symétrique s'écrit de manière unique comme un polynôme en les fonctions symétriques élémentaires (ici le résultat est toute fois plus précis puisque le système de générateurs est explicite). En effet, ceci correspond au théorème 2.1 appliqué au groupe symétrique S_n agissant par permutation sur \mathbb{C}^n : S_n étant engendré par les transpositions, il s'agit bien d'un groupe de réflexions. Les générateurs étant donnés par les fonctions symétriques élémentaires Σ_i (qui sont bien homogènes) de degré $d_i = i$, les relations sur l'ordre du groupe et le nombre de réflexions sont aisément vérifiées (S_n contient $n(n-1)/2$ transpositions).

Avant de procéder à la démonstration du théorème 2.1, mentionnons une propriété particulière de l'action d'un groupe de réflexion sur $A = \text{Sym}(V^*)$, propriété essentielle dans la suite. Soient g est une réflexion par rapport à l'hyperplan H et l une forme linéaire définissant H . Quitte à multiplier l par une

constante non nulle, on peut écrire l'action de g sous la forme :

$$g(v) = v + l(v)v_0$$

où v_0 est un vecteur propre de g pour la valeur propre différente de 1. Il est alors très facile de constater que tout polynôme f de degré d vérifie une identité du type :

$$g \cdot f - f = l\Delta_g(f)$$

pour un certain polynôme $\Delta_g(f)$ de degré $d - 1$ (cette remarque va nous permettre de "dévisser" l'action de G par récurrence sur le degré).

Démonstration du théorème 2.1 (première partie) :

Commençons par fixer quelques notations : comme ci-dessus, nous noterons A l'algèbre des fonctions polynômiales sur V et A^G la sous-algèbre (graduée) des invariants ; enfin, I désignera l'idéal homogène engendré par les éléments homogènes de degré strictement positif de A^G . D'après le théorème 1.1, nous savons que A^G est de type fini ; en particulier, nous pouvons choisir une base de I (comme idéal de A) formée d'un nombre fini de polynômes homogènes. Fixons donc dans la suite une telle base (f_1, \dots, f_m) que nous supposons de plus minimale.

Remarquons tout de suite la chose suivante : si nous savons montrer que les f_i sont algébriquement indépendants, nous aurons nécessairement $m = n$. En effet, supposons que A^G soit une algèbre de polynôme en m variables et considérons les corps

$$K = \text{Frac}(A^G) \quad \text{et} \quad L = \text{Frac}(A).$$

Le groupe agit naturellement sur L et un procédé de moyennisation classique montre que le corps K s'identifie aux invariants de L sous l'action de G : une fraction rationnelle G -invariante est le quotient de deux polynômes eux-mêmes G -invariants. L'extension $K \subset L$ est donc finie (galoisienne, de groupe de Galois G) et les corps L et K ont en particulier même degré de transcendance sur \mathbb{C} , c'est-à-dire $m = n$.

Il nous faut donc pour conclure montrer que les polynômes f_1, \dots, f_m sont algébriquement indépendants. Pour cela, considérons une relation de la forme :

$$F(f_1, \dots, f_m) = 0 \tag{1}$$

où F est un polynôme de degré minimal avec cette propriété. Comme les f_i sont homogènes, nous pouvons de plus supposer que tous les monômes $y_1^{a_1} \dots y_m^{a_m}$ sont de degré pondéré constant :

$$\sum_{j=1}^m a_j d_j = \text{cste}$$

(rappelons que d_j désigne le degré de f_j). Pour $j = 1..m$, considérons les polynômes :

$$F_j = \frac{\partial F}{\partial y_j}(f_1, \dots, f_m).$$

L'hypothèse faite sur les monômes de F assure que les F_j sont des polynômes *homogènes*; par minimalité de F , ils sont bien évidemment non tous nuls et engendrent donc un idéal non trivial J de A^G . Nous pouvons alors (quitte à les réordonner) supposer que F_1, \dots, F_r engendrent l'idéal J et ce de manière minimale : pour tout $j = 1..r$, F_j n'est pas dans l'idéal (de A^G) engendré par les autres F_i . Pour $j = r + 1..m$, nous pouvons cependant écrire :

$$F_j = \sum_{i=1}^r a_{i,j} F_i$$

(avec $a_{i,j}$ homogènes car les F_i le sont tous). En dérivant la relation (1) par rapport à x_k , nous obtenons :

$$\sum_{j=1}^m F_j \frac{\partial f_j}{\partial x_k} = \sum_{j=1}^r F_j \left(\frac{\partial f_j}{\partial x_k} + \sum_{i=r+1}^m a_{j,i} \frac{\partial f_i}{\partial x_k} \right) = 0.$$

Comme nous avons convenablement ré-ordonné les F_j , nous pouvons appliquer le lemme 2.1 ci-dessous (qui constitue le point crucial de la démonstration) et en déduire que

$$\forall j = 1 \dots r, \forall k = 1 \dots n, \frac{\partial f_j}{\partial x_k} + \sum_{i=r+1}^m a_{j,i} \frac{\partial f_i}{\partial x_k} \in I$$

(rappelons que I est l'idéal homogène de A engendré par les polynômes homogènes G -invariants). Signalons au passage que l'emploi du lemme 2.1 est légitime puisque les polynômes

$$\frac{\partial f_j}{\partial x_k} + \sum_{i=r+1}^m a_{j,i} \frac{\partial f_i}{\partial x_k}$$

sont bien homogènes (suite à nos considérations sur les monômes de F). En multipliant ces relations par x_k et en les ajoutant, la relation d'Euler³ montre que⁴ :

$$\forall j = 1 \dots r, d_j f_j + \sum_{i=r+1}^m a_{j,i} d_i f_i = \sum_{l=1}^m b_l^j f_l$$

où les b_l^j sont des polynômes homogènes vérifiant $b_l^j(0) = 0$ (car dans l'idéal maximal (x_1, \dots, x_n)). En spécifiant par exemple la relation précédente pour $j = 1$, nous en déduisons que :

$$d_1 f_1 + \sum_{i=r+1}^m a_{1,i} d_i f_i = \sum_{l=1}^m b_l^1 f_l$$

et, pour des raisons de degré, le coefficient b_1^1 doit être constant donc nul. L'égalité ci-dessus montre que f_1 est dans l'idéal de A engendré par f_2, \dots, f_m ;

3. un polynôme P homogène de degré d en les variables x_1, \dots, x_n vérifie :

$$dP = \sum_{i=1}^n x_i \frac{\partial P}{\partial x_i}.$$

4. puisque f_1, \dots, f_m engendrent l'idéal I .

ceci constitue la contradiction cherchée puisque nous avons supposée la famille (f_1, \dots, f_m) minimale. \square

Comme nous pouvons le constater, la démonstration ci-dessus est une somme de considération de pure algèbre commutative (graduée) et nous n'avons pas fait usage du fait que G est une groupe de réflexion. C'est à travers le lemme suivant que cette propriété apparaît de manière déterminante.

Lemme 2.1

Soit $y_1, \dots, y_m \in A^G$ tel que y_1 n'appartienne pas à l'idéal de A^G engendré par y_2, \dots, y_m . Si z_1, \dots, z_m sont des polynômes homogènes vérifiant

$$\sum_{i=1}^m z_i y_i = 0,$$

alors z_1 est dans l'idéal I .

Démonstration :

Procédons par récurrence sur le degré d de z_1 (le cas $d = 0$ étant trivial). Considérons pour cela une réflexion g de G et écrivons

$$g(z_i) = z_i + l\Delta_g(z_i)$$

pour tout i . Les polynômes y_i étant invariants, la relation de dépendance devient :

$$\sum_{i=1}^m \Delta_g(z_i) y_i = 0$$

d'où l'on tire (le degré de $\Delta_g(z_1)$ est strictement inférieur à celui de z_1) que $\Delta_g(z_1) \in I$. Comme $g(z_1) - z_1 \in I$ pour toute réflexion de G et comme G est un groupe de réflexion, on en déduit que $g(z_1) - z_1 \in I$ pour tout $g \in G$ (I est stable sous l'action de G) ; l'addition de toutes ces relations montre que $z_1 \in I$ (la moyenne d'un polynôme homogène est bien un polynôme *homogène* invariant car l'action de G est linéaire). \square

Démonstration du théorème 2.1 (deuxième partie) :

Concernant la deuxième partie du théorème 2.1, commençons par remarquer que A/I est de dimension finie (sur \mathbb{C}). En effet, d'après le théorème 1.1, A est un A^G -module de type fini et, pour les polynômes invariants, l'opération de passage au quotient consiste à ne garder que le terme constant : une famille génératrice de A comme A^G -module engendre donc A/I sur \mathbb{C} . Considérons donc une famille de polynômes *homogènes* (a_1, \dots, a_m) dont les classes forment une base de A/I (conformément à la remarque que nous venons de faire, nous pouvons également supposer que cette famille engendre le A^G -module A) ; nous allons montrer qu'elle forme une base de A comme A^G -module (et donc de L comme K -espace vectoriel⁵).

Pour ce faire, donnons nous une relation de dépendance linéaire :

$$\sum_{i=1}^m \lambda_i a_i = 0$$

5. rappelons que L et K désignent respectivement les corps de fractions de A et A^G .

où les λ_i sont dans A^G (et même dans I). Comme les a_i sont homogènes, on peut supposer que les λ_i le sont aussi et nous sommes donc en mesure d'appliquer le lemme 2.1 (ou plutôt sa contraposition) : comme en particulier $a_1 \notin I$, on en déduit que λ_1 est dans l'idéal (de A^G) engendré par les autres λ_i

$$\lambda_1 = \sum_{j=2}^m z_j \lambda_j \quad (z_j \in I)$$

En remplaçant dans la relation de dépendance, nous obtenons :

$$\sum_{i=2}^m \lambda_i (a_i + z_i a_1) = 0$$

et, comme la classes dans A/I de $a_i + z_i a_1$ coïncide avec celle de a_i , une récurrence immédiate montre que la famille (a_1, \dots, a_m) est libre. La dimension de A/I sur \mathbb{C} est donc aussi le rang de A sur A^G ou encore la dimension de L sur K , c'est-à-dire

$$\dim_{\mathbb{C}}(A/I) = m = |G|.$$

Pour conclure que l'ordre de G est bien donnée par le produit des degrés des générateurs de A^G , une manière élégante est d'introduire les séries de Hilbert-Poincaré des algèbres graduées A , A^G et A/I . Rappelons que la série de Hilbert-Poincaré d'une \mathbb{C} -algèbre graduée B de type fini est par définition la série formelle :

$$HP_B(t) := \sum_{d \geq 0} \dim_{\mathbb{C}}(B_d) t^d$$

où B_d désigne le sous-espace des éléments homogènes de degré d . Le fait que les a_i forment une base de A comme A^G -module et que leurs classes forment une \mathbb{C} -base de A/I s'écrit alors :

$$HP_A(t) = HP_{A^G}(t) HP_{A/I}(t).$$

Or, comme $A = \mathbb{C}[x_1, \dots, x_n]$ et $A^G = \mathbb{C}[f_1, \dots, f_n]$ avec f_i de degré d_i , un rapide calcul donne :

$$HP_A(t) = (1-t)^{-n} \quad \text{et} \quad HP_{A^G}(t) = \prod_{i=1}^n (1-t^{d_i})^{-1},$$

ou encore :

$$HP_{A/I}(t) = \frac{\prod_{i=1}^n (1-t^{d_i})}{(1-t)^n} = \prod_{i=1}^n \left(\sum_{j=0}^{d_i} t^j \right).$$

La valeur en $t = 1$ donne l'identité recherchée :

$$|G| = \dim_{\mathbb{C}}(A/I) = HP_{A/I}(1) = \prod_{i=1}^n d_i.$$

□

Pour démontrer la relation donnant le nombre de réflexion de G , il nous faut tout d'abord calculer une autre expression de la série de Hilbert-Poincaré de A^G .

Proposition 2.1

Soit G un sous-groupe fini de $GL_n(\mathbb{C})$ et A^G l'algèbre des polynômes invariants ; la série de Hilbert-Poincaré de A^G est donnée par :

$$HP_{A^G}(t) = \frac{1}{|G|} \sum_{g \in G} \det(1 - gt)^{-1}.$$

Démonstration :

Il est bien connu que, si un groupe fini G opère sur un espace vectoriel de dimension finie W , la dimension du sous-espace invariant est donnée⁶ par :

$$\dim(W^G) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}_W(g).$$

En appliquant cela aux polynômes homogènes de degré d , nous obtenons :

$$\dim(A_d^G) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}_{A_d}(g).$$

Pour un élément g fixé, choisissons des coordonnées pour lesquelles l'action de g est diagonale de valeurs propres ξ_1, \dots, ξ_n . Un calcul direct montre que :

$$\text{Tr}_{A_d}(g) = \sum_{p_1 + \dots + p_n = d} \xi_1^{-p_1} \dots \xi_n^{-p_n}$$

et par suite :

$$\begin{aligned} \sum_{d \geq 0} \text{Tr}_{A_d}(g) t^d &= \sum_{p_1 + \dots + p_n = d} \xi_1^{-p_1} \dots \xi_n^{-p_n} t^{p_1 + \dots + p_n} \\ &= \prod_{i=1}^n (1 - \xi_i^{-1} t)^{-1} = \det(1 - g^{-1} t)^{-1}. \end{aligned}$$

En reportant cette égalité dans l'expression de la série de Hilbert-Poincaré de A^G (et en remplaçant g par g^{-1}), nous obtenons l'identité recherchée. \square

Cette fois, nous pouvons conclure sur le dernier point.

Démonstration du théorème 2.1 (fin) :

Pour montrer que le nombre de réflexions de G est bien donnée par le nombre $\sum_i d_i - 1$, nous allons évaluer de deux façons différentes la limite en $t = 1$ de l'expression

$$2|G|(1-t)^{n-1} P_{A^G}(t) - \frac{2}{1-t}. \quad (2)$$

En utilisant l'identité

$$HP_{A^G}(t) = \prod_{i=1}^n (1 - t^{d_i})^{-1},$$

6. en effet, l'application

$$\frac{1}{|G|} \sum_{g \in G} g$$

est une projection sur W^G

nous constatons que l'expression (2) vaut en $t = 1$:

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

D'autre part, en utilisant la proposition précédente et en isolant l'élément $g = 1$ (qui compense le terme en $\frac{1}{1-t}$), l'expression (2) devient :

$$\begin{aligned} 2|G|(1-t)^{n-1}P_{AG}(t) - \frac{2}{1-t} &= 2(1-t)^{n-1} \sum_{g \in R} \det(1-gt)^{-1} \\ &+ 2(1-t)^{n-1} \sum_{g \notin R, g \neq 1} \det(1-gt)^{-1}, \end{aligned}$$

où R désigne l'ensemble des réflexions de G . Si g n'est pas une réflexion et $g \neq 1$, g a au moins deux valeurs propres différentes de 1 et $\det(1-gt)$ est d'ordre au plus $n-2$. La valeur en $t = 1$ de l'expression ci-dessus ne dépend donc que de la somme portant sur les réflexions. Pour un tel élément g de G , notons ξ la valeur propre différente de 1 ; nous avons alors :

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

Cette dernière quantité prenant la valeur 1 en $t = 1$, nous pouvons conclure quant à l'égalité :

$$|R| = \left(2|G|(1-t)^{n-1}P_{AG}(t) - \frac{2}{1-t} \right)_{|t=1} = \sum_{i=1}^n (d_i - 1).$$

□

Remarque 2.1

Il n'est pas très difficile de montrer que le théorème de Chevalley constitue en fait une caractérisation de groupes de réflexions complexes : un sous-groupe fini G de $GL_n(\mathbb{C})$ est un groupe de réflexions si et seulement si l'algèbre de ses invariants est engendrée par n polynômes homogènes algébriquement indépendants. Pour plus de précisions, nous renvoyons au livre [Spr77].

3 Le quotient \mathbb{C}^n/G comme espace complexe

Le théorème 2.1 a une conséquence assez surprenante sur la structure de l'espace complexe \mathbb{C}^n/G . Rappelons tout d'abord le théorème de H. Cartan [Car57] sur la structure de ce dernier.

Théorème 3.1 (H. Cartan, 1953)

Soit G un sous-groupe fini de $GL_n(\mathbb{C})$ et (f_1, \dots, f_p) des polynômes homogènes qui engendrent la sous-algèbre des invariants de G . L'application

$$\varphi : \begin{cases} \mathbb{C}^n & \longrightarrow & \mathbb{C}^p \\ (x_1, \dots, x_n) & \longmapsto & (f_1(x), \dots, f_p(x)) \end{cases}$$

induit alors par passage au quotient un isomorphisme entre \mathbb{C}^n/G et le sous-ensemble algébrique (normal) de \mathbb{C}^p dont les équations sont données par les relations existantes entre les polynômes (f_1, \dots, f_p) .

Illustrons ce résultat en reprenant l'exemple mentionné dans la section 1. $G = \mathbb{Z}_2$ agit sur \mathbb{C}^2 par multiplication par -1 , les invariants sont $X = x^2$, $Y = xy$ et $Z = y^2$ avec comme relation $XZ = Y^2$; le quotient $\mathbb{C}^2/\mathbb{Z}_2$ est donc un cône quadratique.

Remarque 3.1

Le théorème 3.1 est souvent employé sous la forme suivante : si un groupe G agit (par biholomorphismes) proprement discontinûment sur une variété complexe X , le quotient X/G est un espace normal.

Comme dans le cas d'un groupe de réflexions les générateurs ne vérifient pas de relations (ils sont algébriquement indépendants), la structure du quotient est la plus simple possible.

Corollaire 3.1

Si G est un groupe de réflexions agissant sur \mathbb{C}^n , le quotient \mathbb{C}^n/G est une variété lisse.

Le cas d'un groupe de réflexions cyclique illustre (s'il en est besoin) ce corollaire; en effet, un tel groupe est engendré (à conjugaison près) par une transformation qui laisse fixe les $n - 1$ premières coordonnées et qui agit par multiplication par une racine de l'unité sur la dernière. Nous sommes donc ramené au cas d'une seule variable et, dans ce cas, le corollaire 3.1 est bien connu.

Remarque 3.2

Comme ci-dessus, le corollaire 3.1 admet une réciproque : le quotient \mathbb{C}^n/G est lisse si et seulement si G est un groupe de réflexions (voir par exemple [Pri67]).

Références

[Car57] Henri Cartan, *Quotient d'un espace analytique par un groupe d'automorphismes*, Algebraic geometry and topology, Princeton University Press, Princeton, N. J., 1957, A symposium in honor of S. Lefschetz,, pp. 90–102.

[Che55] Claude Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.

[Noe15] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1915), no. 1, 89–92.

[Pri67] David Prill, *Local classification of quotients of complex manifolds by discontinuous groups*, Duke Math. J. **34** (1967), 375–386.

[Spr77] T. A. Springer, *Invariant theory*, Lecture Notes in Mathematics, Vol. 585, Springer-Verlag, Berlin, 1977.