ANNALES DE L'INSTITUT FOURIER

MUSTAPHA RAIS

Le théorème fondamental des invariants pour les groupes finis

Annales de l'institut Fourier, tome 27, nº 4 (1977), p. 247-256

<http://www.numdam.org/item?id=AIF_1977__27_4_247_0>

Ann. Inst. Fourier, Grenoble
27, 4 (1977), 247-256.

LE THÉORÈME FONDAMENTAL DES INVARIANTS POUR LES GROUPES FINIS

par Mustapha RAIS

1. Le procédé de la polarisation et le premier problème de la théorie classique des invariants.

1.1. Soit V un espace vectoriel de dimension finie sur un corps K de caractéristique zéro. Soit G un groupe (pour le moment quelconque) et soit $r : G \to GL(V)$ une représentation linéaire de G dans V. On désignera par r^* la représentation contragrédiente de r. Le groupe G opère alors naturellement dans les algèbres symétriques S(V) et S(V*) (où V* est le dual de V), qu'on identifiera (presque systématiquement) aux algèbres des fonctions polynomiales définies dans V* et V (respectivement) et à valeurs dans K. Au moyen de cette identification, l'action de G dans S(V) et S(V*) s'explicite facilement. Par exemple, si x est dans G et $f : V \to K$ est dans S(V*), la fonction $x.f$ transformée de f par x est telle que : $(x.f)(v) = f(r(x)^{-1}.v)$ pour tout v dans V.

1.2. Dès que la représentation r de G dans V est donnée, on peut considérer pour chaque entier $p \geqslant 1$ la représentation linéaire r_p de G dans V^p définie de la manière suivante :

$$r_p(x)(v_1, v_2, \ldots, v_p) = (r(x)v_1, r(x)v_2, \ldots, r(x)v_p)$$

pour tous x dans G et $v_1, \ldots, v_p$ dans V. Pour chaque tel p, on désignera par J_p l'algèbre des fonctions polynômes définies dans V^p qui sont invariantes par G. Le premier problème fondamental de la théorie des invariants est celui de trouver « explicitement » un système de générateurs de l'algèbre J_p pour chaque p. Par exemple, lorsque V est $\mathbf{C}^n$, le problème correspondant à divers sous-groupes intéressants de $GL(n, \mathbf{C})$ (opérant naturellement dans $\mathbf{C}^n$) (en particulier les groupes classiques) est résolu dans [6]. Un exposé moderne des résultats de H. Weyl se trouve dans [5].

1.3. Soit $f: V \to K$ une fonction polynôme homogène de degré m, invariante par G. On va lui associer pour chaque entier $p \geqslant 1$ une famille f_α de fonctions polynômes G-invariantes sur V^p, de la manière suivante : Soient $t_1, \ldots, t_p$ des éléments variables dans K et $v_1, \ldots, v_p$ des éléments variables dans V. Alors $f(t_1v_1 + \cdots + t_pv_p)$ est une fonction polynomiale en $t_1, \ldots, t_p$, à coefficients dans l'algèbre des fonctions polynômes définies dans V^p. En utilisant la notation habituelle des multi-indices, on a donc :

$$f(t_1v_1 + \cdots + t_pv_p) = \sum_{|\alpha|=m} (t^\alpha/\alpha\,!)f_\alpha(v_1, \ldots, v_p)$$

de sorte que :

$$f_\alpha(v_1, \ldots, v_p) = (\partial/\partial t)^\alpha f(t_1v_1 + \cdots + t_mv_m).$$

Il est immédiat que chaque fonction f_α est homogène de degré m et G-invariante. Parmi ces fonctions f_α définies dans les divers espaces V^p, il en est une qui joue un rôle particulier, à savoir celle $Pf: V^m \to K$ correspondant au cas où $p = m$ et $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ avec

$$\alpha_1 = \alpha_2 = \cdots = \alpha_m = 1.$$

Il est bien connu que Pf, qu'on appelle la polarisée complète de f, est une forme multilinéaire symétrique sur V^m et que l'on a : $m\,!\, f(v) = (Pf)(v, \ldots, v)$ (formule d'Euler), de sorte que :

$$m\,!\, f(t_1v_1 + \cdots + t_pv_p) = \Sigma t_{i_1} \ldots t_{i_m} Pf(v_{i_1}, \ldots, v_{i_m})$$

Ceci montre qu'à un coefficient de proportionnalité près, chaque $f_\alpha(v_1, \ldots, v_p)$ s'obtient à partir de $Pf(w_1, \ldots, w_m)$ en faisant $w_1 = \cdots = w_{\alpha_1} = v_1$,

$$w_{\alpha_1+1} = \cdots = w_{\alpha_1+\alpha_2} = v_2, \ldots, w_{\alpha_1+\cdots+\alpha_{m-1}+1} = \cdots = w_m = v_p.$$

Autrement dit, pour un entier p donné, les diverses fonctions $f_\alpha(v_1, \ldots, v_p)$ s'obtiennent à partir de la seule fonction $\mathrm{P}f(w_1, \ldots, w_m)$ en donnant de toutes les manières possibles aux « variables » $w_1, \ldots, w_m$ des « valeurs » prises parmi $v_1, \ldots, v_p$.

1.4. Ce qui précède donne un procédé pour obtenir des fonctions invariantes sur V^p en partant des fonctions invariantes sur V. Ce procédé peut être explicité d'une autre manière qui fait intervenir les opérations de dérivations successives. Supposons que le groupe G opère linéairement dans un autre espace W (de dimension finie). Soit $\mathrm{F} : \mathrm{V} \to \mathrm{W}$ une fonction polynomiale (ou plus généralement dérivable si $\mathrm{K} = \mathbf{R}$ ou $\mathbf{C}$) invariante par G, ce qui signifie : $\mathrm{F}(x.v) = x.\mathrm{F}(v)$ pour tout x dans V. Alors la dérivée $d\mathrm{F} : \mathrm{V} \to \mathrm{Hom}\,(\mathrm{V}, \mathrm{W})$ est aussi invariante (ce qui a un sens puisque G opère linéairement dans Hom (V, W) dès qu'il opère dans V et dans W). De plus $d\mathrm{F}$ est homogène de degré $m - 1$ si F est homogène de degré m. Soit maintenant $f : \mathrm{V} \to \mathrm{K}$ une fonction invariante. Alors sa dérivée p-ième $d^pf : \mathrm{V} \to \overset{p}{\otimes}\, \mathrm{V}^*$ est une fonction polynômiale définie dans V et à valeurs dans la puissance tensorielle p-ième de V^*. Autrement dit, chaque fois que v est dans V, la valeur $(d^pf)(v)$ de d^pf au point v est une forme multilinéaire symétrique sur V^p et la fonction

$$(v_1, v_2, \ldots, v_{p+1}) \longmapsto (d^pf)(v_1)(v_2, \ldots, v_{p+1})$$

est une fonction polynômiale invariante sur V^{p+1}. En particulier, si f est homogène de degré m, la fonction d^mf est homogène de degré 0 et sa valeur en n'importe quel point de V est la polarisée complète $\mathrm{P}f$ de f.

1.5. Fixons un entier $p \geqslant 2$, et désignons par A_p la *sous-algèbre* de J_p *engendrée* par les fonctions invariantes f_α obtenues par le procédé indiqué dans 1.3. à partir de *toutes* les fonctions f homogènes invariantes sur V. Si f et g sont deux fonctions invariantes sur V, on a :

$$f(t_1v_1 + \cdots + t_pv_p)g(t_1v_1 + \cdots + t_pv_p) = \sum_{\alpha,\beta} (t^{\alpha+\beta}/\alpha\,!\,\beta\,!)f_\alpha(v_1, \ldots, v_p)g_\beta(v_1, \ldots, v_p).$$

Ceci montre que l'algèbre A_p est de type fini dès que l'algèbre J des fonctions polynômes invariantes sur V est elle-même de type fini. Une autre remarque concernant l'algèbre A_p est la suivante : Faisons opérer linéairement le groupe G^p dans V^p au moyen de r^p (autrement dit :

$$r^p(x_1, \ldots, x_p)(v_1, \ldots, v_p) = (x_1 v_1, \ldots, x_p v_p)$$

pour tous $v_1, \ldots, v_p$ dans V et $x_1, \ldots, x_p$ dans G). Alors l'algèbre des fonctions polynômes définies dans V^p et invariantes sous cette action de G^p s'identifie naturellement à $\overset{p}{\otimes}$ J. C'est donc une sous-algèbre de A_p.

2. Le théorème fondamental des invariants pour les groupes finis.

2.1. Supposons désormais que G soit un sous-groupe *fini* de GL(V), la représentation r étant la représentation naturelle de G dans V. Dans ces conditions, il est immédiat que l'algèbre $S((V^*)^p)$ est entière sur l'algèbre des invariants du groupe fini G^p opérant dans V^p, laquelle algèbre est une sous-algèbre de A_p. Il en résulte que J_p est entière sur A_p. Si K est algébriquement clos, ce qu'on supposera désormais, on voit que tout caractère de l'algèbre A_p est la restriction à A_p d'un caractère de J_p, ce qui exprime qu'une certaine application est surjective. A l'opposé, on va montrer que cette application est « génériquement » injective. On sait en effet qu'il existe un ouvert de Zariski non vide U dans V, qui est G-invariant et qui a la propriété suivante : L'application de passage au quotient $V \to V/G$ est localement injective dans U. Soient maintenant $v_1, \ldots, v_p$ et $w_1, \ldots, w_p$ dans V tels que $F(v_1, \ldots, v_p) = F(w_1, \ldots, w_p)$ pour tout F dans A_p. Comme A_p contient les fonctions G^p-invariantes, il existe $x_1, \ldots, x_p$ dans G tels que

$$w_1 = x_1 . v_1, \ \ldots, \ w_p = x_p . v_p.$$

On a donc :

$$\begin{aligned} f(t_1 v_1 + \cdots + t_p v_p) &= f(t_1 x_1 . v_1 + \cdots + t_p x_p . v_p) \\ &= f(t_1 v_1 + t_2 x_1^{-1} x_2 . v_2 + \cdots + t_p x_1^{-1} x_p . v_p) \end{aligned}$$

pour tous $t_1, \ldots, t_p$ dans K et pour toute fonction f, G-invariante sur V. Supposons que v_1 soit dans U et appelons M un voisinage ouvert de v_1 dans U dans lequel l'application $V \to V/G$ est injective. Il existe un voisinage ouvert L de $(1, 0, \ldots, 0)$ dans K^p tel que $t_1v_1 + \cdots + t_pv_p$ aussi bien que $t_1v_1 + t_2x_1^{-1}x_2.v_2 + \cdots + t_px_1^{-1}x_p.v_p$ soit dans M pour tout $(t_1, \ldots, t_p)$ dans L. Mais

$$t_1v_1 + \cdots + t_pv_p \quad \text{et} \quad t_1v_1 + t_2x_1^{-1}x_2.v_2 + \cdots + t_px_1^{-1}x_p.v_p$$

sont G-conjugués d'après l'hypothèse faite plus haut. On a donc

$$t_1v_1 + \cdots + t_pv_p = t_1v_1 + t_2x_1^{-1}x_2.v_2 + \cdots + t_px_1^{-1}x_p.v_p$$

pour tout $(t_1, \ldots, t_p)$ dans L, ce qui donne :

$$x_1.v_2 = x_2.v_2 = w_2, \ \ldots, \ x_1.v_p = x_p.v_p = w_p.$$

Autrement dit : $(v_1, \ldots, v_p)$ et $(w_1, \ldots, w_p)$ sont G-conjugués dans V^p. Il est clair maintenant qu'on peut énoncer : Il existe un ouvert de Zariski non vide U_p de V^p qui est G-invariant et dans lequel l'algèbre A_p sépare les orbites de G.

2.2. Théorème. — *Sous les hypothèses faites dans* 2.1, *on peut affirmer que* A_p *et* J_p *ont même corps de fractions.*

Ceci est un résultat qui paraîtra sûrement évident aux spécialistes de géométrie algébrique « élémentaire ». La situation est en tout cas la suivante : Soient X et Y les variétés irréductibles définies respectivement par les algèbres J_p et A_p. Du fait que J_p est entière sur A_p, il existe un morphisme dominant $u : X \to Y$ et le corps des fonctions K(X) est une extension finie du corps des fonctions K(Y). Remarquons maintenant que X est la variété quotient V^p/G, et que c'est une variété normale ([4], [1]). On sait alors que le degré de K(X) sur K(Y) est le nombre d'éléments qui se trouvent dans une fibre « générique » de u ([2] § 5, Corollaire 1 du théorème 1). Le fait que A_p sépare les orbites de G dans un ouvert de V^p montre alors que ce degré est exactement 1, ou encore que X et Y ont même corps des fonctions rationnelles.

2.3. C'est ce théorème qu'on peut appeler le théorème fondamental des invariants des groupes finis. Il donne un procédé pour trouver les fonctions rationnelles invariantes sur V^p à partir des fonctions rationnelles invariantes sur V.

3. Relation entre les invariants du groupe adjoint d'une algèbre de Lie semi-simple et ceux d'un groupe de Weyl.

3.1. Voici une application de ce qui précède à la relation entre les invariants du groupe adjoint d'une algèbre de Lie semi-simple complexe et ceux du groupe de Weyl. Soit $\mathscr{G}$ une algèbre de Lie semi-simple complexe. On désignera par G son groupe adjoint et par $Ad : G \to GL(\mathscr{G})$ la représentation adjointe de G. La représentation Ad_p, définie comme dans 1.2, est une représentation linéaire de G dans $\mathscr{G}^p$. Soit maintenant $\mathscr{H}$ une sous-algèbre de Cartan de $\mathscr{G}$ et soit W le groupe de Weyl de $(\mathscr{G}, \mathscr{H})$. On désignera par r la représentation naturelle de W dans $\mathscr{H}$ et par r_p celle de W dans $\mathscr{H}^p$, définie dans 1.2. Il est immédiat que la restriction à $\mathscr{H}^p$ d'une fonction polynôme définie dans $\mathscr{G}^p$ et invariante par G est une fonction polynôme W-invariante sur $\mathscr{H}^p$. On dispose donc d'un homomorphisme d'algèbres R_p de l'algèbre des invariants de G dans l'algèbre des invariants de W. Lorsque $p = 1$, il s'agit d'un *isomorphisme* d'algèbres, d'après un théorème classique de Chevalley ([3], théorème 7.3.5). Les exemples qui suivent montrent qu'il n'en est plus ainsi pour $p > 1$.

3.2. Soit f une fonction polynôme sur $\mathscr{G}$, invariante par G. Alors la fonction $F : \mathscr{G} \times \mathscr{G} \to \mathbf{C}$ définie par $F(X, Y) = f([X, Y])$ (pour tous X et Y dans $\mathscr{G}$) est G-invariante, et $F(X, Y) = 0$ si X et Y sont dans $\mathscr{H}$ et si $f(0) = 0$. Par exemple, la fonction

$$F(X, Y) = K([X, Y], [X, Y])$$

où K est la forme de Killing de $\mathscr{G}$ est G-invariante et non nulle : Si α est une racine de $\mathscr{G}$ par rapport à $\mathscr{H}$, il existe un vecteur radiciel non nul X_α associé à α, un vecteur radiciel non nul Y_α associé à $-\alpha$, tels que (en posant $H_\alpha = [X_\alpha, Y_\alpha]$) on ait $[H_\alpha, X_\alpha] = 2X_\alpha$ ([3], théorème 1.10.2). On a alors : $F(X_\alpha, Y_\alpha) = K(H_\alpha, H_\alpha) = K([H_\alpha, X_\alpha], Y_\alpha)$ du fait de l'invariance de K. On a donc :

$$F(X_\alpha, Y_\alpha) = 2K(X_\alpha, Y_\alpha) \neq 0,$$

car $K(X_\alpha, Y_\alpha)$ ne peut être nul ([3], théorème 1.10.2). L'homomorphisme R_2 n'est donc pas injectif. De même la fonction $F_p : \mathscr{G}^p \to \mathbf{C}$ définie pour $p \geqslant 3$ par

$$\begin{aligned} F_p(X_1, \ldots, X_p) &= K(X_1, \operatorname{ad} X_2 \operatorname{ad} X_3 \ldots \operatorname{ad} X_{p-1}(X_p)) \\ &= K(X_1, [X_2, [\ldots, [X_{p-1}, X_p] \ldots])) \end{aligned}$$

est G-invariante non nulle sur $\mathscr{G}^p$ tandis que sa restriction à $\mathscr{H}^p$ est nulle. L'homomorphisme R_p n'est donc jamais injectif dès que p est supérieur à 1.

3.3. Je ne sais pas pour le moment si R_p est toujours surjectif. Toutefois, on peut faire les remarques suivantes : Désignons par J_p l'algèbre des invariants de W dans $\mathscr{H}^p$ et par A_p la sous-algèbre de J_p construite comme dans 1.5 à partir des invariants de W dans $S(\mathscr{H}^*)$. Il est immédiat que l'image de R_p contient A_p : Soient $f : \mathscr{H} \to \mathbf{C}$ et $F : \mathscr{G} \to \mathbf{C}$ des fonctions polynômes invariantes respectivement par W (opérant dans $\mathscr{H}$) et par G (opérant dans $\mathscr{G}$) et telles que f soit la restriction de F à $\mathscr{H}$. Soient $t_1, \ldots, t_p$ dans $\mathbf{C}$, $X_1, \ldots, X_p$ dans $\mathscr{G}$ et $H_1, \ldots, H_p$ dans $\mathscr{H}$. On a alors :

$$\begin{aligned} F(t_1X_1 + \cdots + t_pX_p) &= \Sigma(t^\alpha/\alpha\,!)F_\alpha(X_1, \ldots, X_p) \\ f(t_1H_1 + \cdots + t_pH_p) &= \Sigma(t^\alpha/\alpha\,!)f_\alpha(H_1, \ldots, H_p) \end{aligned}$$

ce qui montre que f_α est la restriction à $\mathscr{H}^p$ de F_α. Ainsi l'image de R_p a même corps de fractions que J_p. Intuitivement, on peut dire qu'une fonction rationnelle W-invariante sur $\mathscr{H}^p$ est la « restriction » à $\mathscr{H}^p$ d'une fonction rationnelle G-invariante sur $\mathscr{G}^p$. En tout cas, l'homomorphisme R_p sera surjectif chaque fois que $A_p = J_p$. C'est le cas lorsque $\mathscr{G}$ est l'algèbre de Lie $sl(n, \mathbf{C})$ des matrices $n \times n$ complexes de trace nulle ([6], chapitre II, paragraphe 3).

4. Des exemples et une conjecture.

4.1. Revenons à la situation générale d'un groupe G opérant linéairement dans un espace vectoriel V (paragraphe 1). La discussion précédente montre que la question importante est la suivante : Est-ce que $A_p = J_p$? Comme je l'ai signalé plus haut, la réponse est oui si G est le groupe de Weyl de $sl(n, \mathbf{C})$ et je *conjecture* qu'il en est toujours ainsi si G est un sous-groupe de V engendré par des pseudo-réflexions. En tout cas, lorsque G est fini, l'égalité $A_p = J_p$ équivaut au fait que l'algèbre A_p soit intégralement close. Les exemples qui suivent montrent qu'en général la réponse à la question posée est négative.

4.2. Ici $V = \mathbf{C}^2$ et G est le groupe engendré par la symétrie $(x_1, x_2) \longmapsto (-x_1, -x_2)$ par rapport à l'origine, qui n'est pas une pseudo-réflexion. L'algèbre J des fonctions G-invariantes sur $\mathbf{C}^2$ est engendrée par les fonctions x_1^2, x_2^2 et x_1x_2, dont les polarisées respectives sont les fonctions bilinéaires $2x_1y_1$, $2x_2y_2$ et $y_1x_2 + y_2x_1$. Il en résulte que l'algèbre A_2 est engendrée par les fonctions suivantes définies dans V^2 :

$$x_1^2,\ x_2^2,\ x_1x_2,\ x_1y_1,\ x_2y_2,\ x_1y_2 + x_2y_1,\ y_1^2,\ y_2^2 \quad \text{et} \quad y_1y_2.$$

Il est par ailleurs facile de constater que l'algèbre J_2 des invariants de G opérant dans V^2 est engendrée par les fonctions précédentes *et par* la fonction x_1y_2. *En tout cas*, des considérations de degré montrent que cette dernière fonction n'est pas dans A_2 de sorte que $A_2 \neq J_2$. (Bien entendu, on a : $x_1y_2 = (x_1x_2/x_2y_2)y_2^2$ ou encore : x_1y_2 est dans le corps des fractions de A_2, ce qu'on savait d'avance.)

4.3. Ici $V = sl(2, \mathbf{C})$ et G est le groupe adjoint de $sl(2, \mathbf{C})$. L'algèbre J des fonctions invariantes sur V est engendrée par la forme quadratique $K(X, X)$. Il en résulte que A_p est l'algèbre engendrée par les fonctions f_{ij} :

$$(X_1, \ldots, X_p) \to K(X_i, X_j) \quad (1 \leqslant i \leqslant j \leqslant p)$$

en nombre $p(p+1)/2$. Lorsque $p = 2$, on constate que $A_2 = J_2$ (générateurs : $K(X_1, X_1)$, $K(X_1, X_2)$ et $K(X_2, X_2)$). Par contre dans J_3 se trouve la fonction

$$F(X_1, X_2, X_3) = K(X_1, [X_2, X_3])$$

qui ne peut pas se trouver dans A_3 puisque

$$F(-X_1, -X_2, -X_3) = -F(X_1, X_2, X_3)$$

alors que toutes les fonctions f_{ij} sont invariantes par la transformation $(X_1, X_2, X_3) \longmapsto (-X_1, -X_2, -X_3)$. On a donc en fait : $A_p \neq J_p$ pour tout $p \geqslant 3$, et même les corps de fractions sont distincts. Pour voir cela, on peut dire ce qui suit : L'algèbre A_p est intégralement close parce que c'est l'algèbre des invariants du groupe orthogonal de la forme de Killing. Si $\mathrm{Fr}(A_p) = \mathrm{Fr}(J_p)$, cela entraînerait $J_p = A_p$ puisque J_p est entière sur A_p. Une autre façon de voir les choses est que l'algèbre A_p ne sépare les orbites de G dans aucun ouvert non vide. Incidemment, on peut énoncer le théorème fondamental des invariants de la représentation adjointe du groupe $SL(2, \mathbf{C})$: Les deux invariants $K(X, X)$ et $F(X_1, X_2, X_3)$ forment un système *basique* d'invariants (au sens de [6]).

4.4. Ici $V = \mathbf{C}^3$ et G est le groupe des matrices de la forme

$$(x, y, z) = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

où x, y et z sont des nombres complexes. La représentation r est la représentation coadjointe du groupe de Heisenberg (complexifiée) :

$$r(x, y, z)(a, b, c) = (a + cy, b - cx, c)$$

pour tous (x, y, z) dans G et (a, b, c) dans $\mathbf{C}^3$. L'algèbre J des invariants de G est engendrée par l'unique fonction c. L'algèbre J_2 des fonctions polynômes définies dans $\mathbf{C}^3 \times \mathbf{C}^3$ et invariantes par r_2 est l'algèbre de *polynômes* engendrée par c_1, c_2, $a_1c_2 - a_2c_1$ et $b_1c_2 - b_2c_1$, tandis que l'algèbre A_2 est celle engendrée par c_1 et c_2. Il y a donc loin dans ce cas entre A_2 et J_2 (l'une est de degré de transcendance 2 tandis que l'autre est de degré de transcendance 4).

Note. — Je remercie bien sincèrement MM. D. Luna et Th. Vust qui m'ont fait parvenir des remarques intéressantes après lecture de la première version de ce texte.

BIBLIOGRAPHIE

[1] H. Cartan, Quotients of complex spaces, Intern. Colloq. on Function Theory, Tata Institute Bombay, 1960 (pp. 1-15).
[2] J. Dieudonné, Cours de géométrie algébrique 2, PUF., 1974.
[3] J. Dixmier, Algèbres enveloppantes, *Cahiers Scientifiques*, Fascicule 37, Gauthier-Villars, 1974.
[4] J. Fogarty, Invariant Theory, Benjamin 1969.
[5] Th. Vust, Sur la théorie des invariants des groupes classiques, *Ann. Inst. Fourier*, 26, 1 (1976), 1-31.
[6] H. Weyl, The Classical Groups, Princeton University Press, 1946.

Manuscrit reçu le 16 novembre 1976
Proposé par J. Dieudonné.

Mustapha Rais,
Département de Mathématiques
Université de Poitiers
40, avenue du Recteur Pineau
86022 Poitiers.