SÉMINAIRE N. BOURBAKI

MICHEL DEMAZURE

Démonstration de la conjecture de Mumford

Séminaire N. Bourbaki, 1976, exp. n° 462, p. 138-144

<http://www.numdam.org/item?id=SB_1974-1975__17__138_0>

Séminaire BOURBAKI 462-01
27e année, 1974/75, n° 462 Février 1975

DÉMONSTRATION DE LA CONJECTURE DE MUMFORD

[d'après W. HABOUSH]

par Michel DEMAZURE

1. Le problème

Soient k un corps et G un k-groupe algébrique réductif. Si k est de caractéristique 0 , toute représentation linéaire de G dans un k-espace vectoriel V est semi-simple, et il existe un unique projecteur G-invariant $v \longmapsto v^{\natural}$ de V sur le sous-espace V^G des invariants de G dans V (projecteur de Reynolds). Cela s'applique notamment lorsque G opère sur un k-schéma algébrique affine X et qu'on prend pour V l'algèbre affine A de X ; l'application π est alors l'analogue algébrique d'une intégration sur G :

$$a^{\natural}(x) = \int_G a(gx)\, dx .$$

Considérons alors le schéma affine Y d'algèbre affine A^G et le morphisme canonique $\pi : X \to Y$; de l'existence du projecteur de Reynolds découlent aisément les propriétés suivantes :

a) la k-algèbre A^G est de type fini, i.e. Y est algébrique,

b) deux fermés de X stables par G et disjoints ont des images (fermées et) disjointes dans Y ,

c) π est surjectif et Y a la topologie quotient.

Cela signifie que Y , qui est le quotient de X par l'action de G dans la catégorie des schémas, a les propriétés que l'on doit attendre d'un quotient raisonnable. Ces remarques, étendues aux actions linéarisables sur des schémas quasi-projectifs, sont à la base de la théorie créée par Mumford dans son livre "Geometric Invariant Theory". De nombreux espaces de modules apparaissant naturellement comme quotient de schémas convenables par des groupes réductifs (groupes linéaire et projectif notamment), on en déduit ainsi, en caractéristique zéro, l'existence de nombreux schémas de modules.

Lorsque k est de caractéristique $\neq 0$, les représentations linéaires d'un groupe réductif ne sont plus nécessairement semi-simples, et il n'y a plus d' "intégration sur le groupe". Cependant, comme le remarque Mumford dans l'introduction du livre cité, la condition suivante sur G (qui exprime en gros l'existence d'un procédé non linéaire d'intégration) est suffisante pour faire fonctionner la théorie du passage au quotient :

(CM) *Pour toute représentation linéaire de G dans un k-espace vectoriel V de dimension finie et tout élément $v_o \neq 0$ de V^G, il existe un polynôme P sur V, invariant par G, et tel que $P(v_o) \neq 0$ et $P(0) = 0$.*

Cette condition, vérifiée d'abord pour SL_2 en caractéristique 2 (Oda), puis pour SL_2 en général (Seshadri), vient d'être démontrée en général par W. Haboush ; c'est cette démonstration que l'on va exposer ci-dessous. Pour un exposé général de la théorie du passage au quotient, on renvoie au rapport de Seshadri à l'Ecole d'été d'Arcata qui contient une bibliographie importante.

2. Quelques remarques

a) *Exemples.*- 1) Supposons que G soit un groupe fini au sens usuel, et soit π une forme linéaire sur V telle que $\pi(v_o) \neq 0$. Alors le polynôme $P(v) = \prod_{g \in G} \pi(gv)$ convient ; notons qu'un projecteur invariant de V sur le sous-espace kv_o est $\frac{1}{|G|} \sum_{g \in G} \pi(gv)$, lorsque $|G|$ n'est pas nul dans k.

2) Supposons que $G = GL_{nk}$, que $V = M_n(k)$, avec $g(v) = gvg^{-1}$, et $v_o = id_V$. Alors $P(v) = \det(v)$ convient (le projecteur de Reynolds de V sur $V^G = k.id_V$ est $\pi(v) = \frac{1}{n} \mathrm{Tr}(v)$). Plus généralement, si m est un entier tel que $\binom{n}{m} \neq 0$ dans k, on peut prendre $P(v) = \binom{n}{m}^{-1} \mathrm{Tr}(\Lambda^m v)$.

b) Dans (CM), on peut évidemment supposer P *homogène* ; soit alors n son degré. Considérons les polaires Q_i de v_o relativement à P définies par

$$P(v_o + \lambda v) = \Sigma \lambda^i Q_i(v) .$$

Alors chaque Q_i est invariant et on a $\Sigma \lambda^i Q_i(v_o) = P(v_o + \lambda v_o) = (1+\lambda)^n P(v_o)$, donc $Q_i(v_o) = \binom{n}{i} P(v_o)$.

Si k est de caractéristique 0 , on peut donc remplacer P par Q_1 , donc supposer P linéaire ; la propriété (CM) équivaut donc, dans ce cas là, à la complète réductibilité.

Si k est de caractéristique $p \neq 0$, posons $n = p^r m$ avec $(p,m) = 1$; alors $\binom{n}{p^r} \not\equiv 0 \ (p)$, donc $Q_{p^r}(v_o) \neq 0$ et on peut supposer que le degré de P est une puissance de la caractéristique.

c) La condition (CM) équivaut à la suivante :

(CM*) Soit $f : E \to F$ un G-morphisme surjectif de représentations de G ; si $y \in F^G$, il existe $k \in \mathbb{N}$ et $x \in S^k(E)^G$ tels que $S^k f(x) = y^k$.

On se réduit en effet aussitôt au cas où E est de dimension finie et F de dimension 1 ; (CM*) équivaut alors à (CM) par dualité.

d) Nagata a démontré qu'inversement (CM) implique que G est réductif.

3. Le théorème d'Haboush

THÉORÈME (W. Haboush).- Tout groupe réductif satisfait à la condition (CM).

Cela va résulter de la proposition suivante :

PROPOSITION 1.- Soient k un corps algébriquement clos, G un k-groupe algébrique semi-simple et simplement connexe, T un tore maximal de G , et A(G) l'algèbre affine de G sur laquelle G opère par translations à gauche et T par translations à droite. Alors le G-module $A(G)^T$ est réunion filtrante croissante de sous-G-modules isomorphes à des modules End(E) , où E est un G-module de dimension finie.

Montrons d'abord comment la proposition 1 implique le théorème. Puisque toute représentation d'un tore est semi-simple et que les groupes finis n'occasionnent pas de difficultés (cf. exemple 2), on peut supposer que G est semi-simple et simplement connexe ; on peut aussi supposer le corps de base algébri-

ment clos. Soient alors V et v_o comme dans (CM) ; soit v_o^* un élément du dual V^* de V tel que $\langle v_o^*, v_o \rangle = 1$; considérons l'application $\varphi : V \to A(G)$ telle que $\varphi(v)(g) = \langle v_o^*, gv \rangle$. Alors φ est un G-homomorphisme et $\varphi(v_o) = 1$. Par ailleurs, la représentation de T dans $A(G)$ est semi-simple et le projecteur de Reynolds $\pi : A(G) \to A(G)^T$ est évidemment G-linéaire. D'après la proposition, il existe un sous-G-module V' de $A(G)^T$ contenant $\pi \circ \varphi(V)$ et un isomorphisme $\sigma : V' \to \mathrm{End}(E)$ où E est un G-module de dimension finie. Comme $A(G)^G$ est réduit aux scalaires, donc $V'^G \simeq \mathrm{End}(E)^G$ est de dimension 1 , on a nécessairement $\sigma(1) = \lambda\, \mathrm{id}_E$ avec $\lambda \neq 0$. Mais alors le polynôme $P = \det \circ \sigma \circ \pi \circ \varphi$ sur V est invariant par G et on a $P(v_o) = \det(\lambda\, \mathrm{id}_E) \neq 0$, C.Q.F.D.

Pour démontrer la proposition 1, choisissons deux sous-groupes de Borel B et B' de G tels que $B \cap B' = T$ et notons U et U' les parties unipotentes de B et B' . Considérons le morphisme G-équivariant :

$$\theta : G \times T \to G/U \times G/U'$$

tel que $\theta(g,t) = (gtU, gU')$. Il induit un isomorphisme de $G \times T$ sur un ouvert de $G/U \times G/U'$ et, si g , g' sont deux points de G , on a

$$((gU, g'U') \in \mathrm{Im}\, \theta) \Leftrightarrow (g'^{-1}g \in UTU') .$$

Soit par ailleurs ρ la demi-somme des racines de T dans B', considérée comme un caractère de T , de B et de B' . Il existe une fonction unique $\Phi_o \in A(G)$ telle que

$$\Phi_o(bgb') = \rho(b)\, \Phi_o(g)\, \rho(b') , \quad b \in B , g \in G , b' \in B' ,$$

$$\Phi_o(1) = 1 ,$$

et UTU' est l'ouvert de G défini par la condition $\Phi_o \neq 0$. (En fait, le diviseur de Φ_o est la somme, avec multiplicité 1 , des composantes du complémentaire de UTU' .)

Il s'ensuit que l'on a

$$((gU, g'U') \in \mathrm{Im}\, \lambda) \Leftrightarrow (\Phi(g,g') \neq 0)$$

où $\Phi(g,g') = \Phi_o(g'^{-1}g)$.

Par conséquent l'application $f \longmapsto f \circ \theta$ induit un isomorphisme de G-modules

$$\theta^* : (A(G)^U \otimes A(G)^{U'})[\Phi^{-1}] \to A(G) \otimes A(T) .$$

Pour chaque T-module à droite E , et chaque caractère λ de T , notons E^λ le sous-espace propre de E associé à λ , $((x \in E^\lambda) \Leftrightarrow xt = \lambda(t)x)$. Si $f \in A(G)^{U,\lambda} \otimes A(G)^{U',\mu}$, alors

$\theta^*(f\Phi^{-n})(g,t) = f(gt,g)\ \Phi_o^{-n}(t) = f(gt,g)\ \rho(t)^{-n}$, tandis que

$\theta^*(f\Phi^{-n})(gt_1,tt_2) = f(gt_1tt_2,gt_1)\ \rho(tt_2)^{-n} = \lambda(t_1t_2)\mu(t_1)\rho(t_2)^{-n} f(gt,g)\ \rho(t)^{-n}$.

Donc $\theta^*(f\Phi^{-n}) \in A(G)^T = A(G)^T \otimes A(T)^T$ si et seulement si $\lambda = n\rho = -\mu$. On en conclut que le G-module $A(G)^T$ est la limite inductive du système de G-modules

$$\xrightarrow{\Phi^*} A(G)^{U,n\rho} \otimes A(G)^{U',-n\rho} \xrightarrow{\Phi^*} A(G)^{U,(n+1)\rho} \otimes A(G)^{U',-(n+1)\rho} \xrightarrow{\Phi^*}$$

où Φ^* est la multiplication par Φ .

Soit w_o un élément de G(k) tel que $w_oTw_o^{-1} = T$, $w_o^{-1}Bw_o = B'$; l'application $f(g) \longmapsto f(gw_o)$ est un isomorphisme de $A(G)^{U,\lambda}$ sur $A(G)^{U',w_o(\lambda)}$. Comme $w_o(\rho) = -\rho$, on en déduit que $A(G)^T$ est <u>réunion filtrante croissante de sous-modules isomorphes aux</u> $E_{n\rho} \otimes E_{n\rho}$, où on note

$$E_\lambda = \{f \in A(G) \mid f(gb) = f(g)\lambda(b) \ , \ g \in G \ , \ b \in B\} .$$

L'élément 1 de $A(G)^T$ correspond à un élément invariant de $E_{n\rho} \otimes E_{n\rho}$, c'est-à-dire un G-homomorphisme $\varphi_n : E_{n\rho}^* \to E_{n\rho}$. L'image de φ_n est le sous-G-module (irréductible) $E'_{n\rho}$ de $E_{n\rho}$ engendré par le vecteur dominant Φ_o^n . Si $E'_{n\rho} = E_{n\rho}$, alors $E_{n\rho}$ est isomorphe à son dual ($E_{n\rho}$ est de dimension finie, comme espace des sections d'un fibré en droites sur la variété projective G/B) et $E_{n\rho} \otimes E_{n\rho}$ isomorphe à $\mathrm{End}(E_{n\rho})$ de façon que l'élément 1 corresponde à l'application identique de $E_{n\rho}$. Pour achever la démonstration de la prop. 1, il suffit donc de prouver :

PROPOSITION 2.- <u>Il existe une infinité de</u> $n > 0$ <u>tel que</u> $E_{n\rho}$ <u>soit égal à</u> $E'_{n\rho}$ (<u>i.e. engendré par ses vecteurs dominants, i.e. irréductible</u>).

Si k est de caractéristique 0, $E_{n\rho}$ est irréductible (par exemple par complète réductibilité) et c'est terminé. Supposons k de caractéristique $p \neq 0$, et notons $\overline{E}_{n\rho}$ le G-module obtenu par réduction à partir du module correspondant en caractéristique 0. On a $E'_{n\rho} \subset E_{n\rho} \subset \overline{E}_{n\rho}$.

a) Si L est le fibré en droites sur G/B correspondant à ρ, on a $E_{n\rho} = H^0(G/B, L^n)$. Comme L est ample, on a $H^1(G/B, L^n) = 0$ pour n assez grand (Serre), donc $\overline{E}_{n\rho} = E_{n\rho}$ pour n assez grand.

b) D'après la formule de H. Weyl, on a

$$\dim \overline{E}_{n\rho} = \prod_{\alpha > 0} \frac{(n+1)\rho(H\alpha)}{\rho(H\alpha)} = (n+1)^N \qquad \text{où } N = \dim U .$$

c) Soit $r > 0$, prenons $n = p^r - 1$. D'après Steinberg (Nagoya Math. Journ., 22 (1963)), il existe une unique représentation irréductible $E''_{n\rho}$ du groupe fini $G(\mathbb{F}_{p^r})$ de plus haut poids $n\rho$, et on a $\dim E''_{n\rho} = p^{rN}$. Comme $E''_{n\rho} \subset E'_{n\rho} \subset \overline{E}_{n\rho}$ et $\dim E''_{n\rho} = \dim \overline{E}_{n\rho}$, on a $E'_{n\rho} = \overline{E}_{n\rho}$.

La proposition 2 et donc le théorème résultent aussitôt de a) et c). C.Q.F.D.

Remarques.- 1) La démonstration de la proposition 1 donne

$$A(G)^\lambda = \varinjlim E_{\lambda+n\rho} \otimes E_{n\rho} .$$

2) Reprenons la démonstration du théorème 1 pour un schéma en groupes déployé sur $\mathbb{Z}$, avec les mêmes notations, et considérons l'homomorphisme $\varphi_n : E^*_{n\rho} \to E_{n\rho}$. On sait que $\varphi_n \otimes \mathbb{Q}$ est un isomorphisme. Soit a_n le plus petit entier > 0 tel que $\varphi_n(E^*_{n\rho}) \supset a_n E_{n\rho}$. Le polynôme Q_n composé du diagramme

$$E_{n\rho} \otimes E_{n\rho} \xrightarrow{a_n\varphi^{-1} \otimes \mathrm{Id}} E^*_{n\rho} \otimes E_{n\rho} \xrightarrow{\det} \mathbb{Z}$$

est invariant et tel que $Q_n(1) = \det(a_n\,\mathrm{id}) = a_n^{\dim E_{n\rho}}$. La démonstration précédente montre que si $n = p^r - 1$, alors $a_n \not\equiv 0 \ (p)$, donc $Q_n(1) \not\equiv 0 \ (p)$.

On en déduit aussitôt que, pour tout entier $n \geq 0$, le pgcd des $Q_m(1)$ pour $m \geq n$ est 1 ; il existe donc une combinaison $\mathbb{Z}$-linéaire P_n des Q_m, $m \geq n$

telle que $P_m(1) = 1$. Par conséquent :

PROPOSITION 3.- *Soient* G *un* $\mathbb{Z}$*-groupe semi-simple simplement connexe déployé et* T *un tore maximal déployé de* G . *Alors le* $\mathbb{Z}$*-module* $A(G)^T$ *est réunion filtrante de sous-modules facteurs directs* G*-stables* F_n *tels qu'il existe pour chaque* n *un polynôme invariant* P_n *sur* F_n *tel que* $P_n(1) = 1$, $P_n(0) = 0$.

4. Le passage au quotient

Soient G un groupe algébrique réductif opérant sur un schéma algébrique affine X d'algèbre A ; soit Y le schéma affine d'algèbre A^G et soit π le morphisme canonique. Les propriétés a), b), c) du n° 1 sont vraies :

a) A^G *est de type fini*. Cela a été prouvé par Nagata être une conséquence de la propriété (CM).

b) *Deux fermés de* X *stables par* G *et disjoints ont des images disjointes dans* Y : soient I et J deux idéaux de A stables par G , tels que $I + J = A$; appliquons (CM*) à l'application canonique $I \to A/J$ et à l'élément 1 de A/J ; on obtient un élément x de I^G tel que $1 - x \in J$, donc $1 - x \in J^G$ et $I^G + J^G = A^G$.

c) π *est surjectif et* Y *a la topologie quotient*. Soit I un idéal de A^G . Appliquons (CM*) à l'application canonique $f : A \otimes I \to AI$; on trouve que, pour tout élément y de $(AI)^G$, il existe $k \in \mathbb{N}$ et $x \in A^G \otimes I$ tel que $f(x) = y^k$, de sorte que $y^k \in (AI)^G$. Les idéaux I et $(AI)^G$ ont donc même racine, ce qui montre que π est surjectif. D'après b), chaque fibre de π contient exactement une orbite fermée, et π est ouverte aux points des orbites fermées, donc Y a la topologie quotient.

Nous renvoyons au rapport déjà cité de Seshadri et à un article de lui à paraître pour le développement de la théorie du passage au quotient et ses applications aux problèmes de modules sur un corps ou une base arbitraire.