Séminaire "Sophus Lie"

P. Cartier

Théorème de conjugaison des algèbres de Cartan

Séminaire "Sophus Lie", tome 1 (1954-1955), exp. n° 15, p. 1-5
<http://www.numdam.org/item?id=SSL_1954-1955__1__A18_0>

Exposé n° 15

THÉORÈME DE CONJUGAISON DES ALGÈBRES DE CARTAN

(Exposé de P. CARTIER, le 8.3.1955)

1.- Préliminaires de géométrie algébrique

Nous rappellerons quelques définitions et résultats du livre de Chevalley sur les groupes algébriques.

Soit V un espace vectoriel de dimension finie sur un corps K infini ; $K[V]$ désigne l'algèbre de fonctions (à valeurs dans K) engendrée par les fonctions constantes et les fonctions linéaires. $K[V]$ est une algèbre graduée isomorphe à l'algèbre symétrique sur le dual V^* de V, les éléments de degré 0 étant les constantes et ceux de degré 1 les fonctions linéaires. Les éléments de $K[V]$ s'appellent les fonctions polynomes sur V ce sont les fonctions qui s'écrivent sous la forme d'un polynome par rapport à un système de coordonnées quelconque.

Une application f de V dans un espace W de dimension finie est dite polynomiale si $P\circ f \in K[V]$ pour toute $P \in K[W]$; pour qu'il en soit ainsi, il suffit que $P\circ f \in K[V]$ pour P linéaire sur W. $P \to P\circ f$ est un homomorphisme de $K[W]$ dans $K[V]$ qui envoie 1 sur 1 ; réciproquement, soit φ un homomorphisme de $K[W]$ dans $K[V]$ avec $\varphi(1) = 1$. Si P est linéaire sur W $\varphi(P)(v)$ est pour $v \in V$ fixe une fonction linéaire en P donc $\varphi(P)(v) = \langle P , f(v) \rangle$ où f est donc une application polynomiale de V dans W ; or on a $\varphi(P) = P\circ f$ pour P constante et P linéaire, donc pour toute $P \in K[W]$ puisque ces fonctions engendrent $K[W]$. En particulier si $V = (0)$ $K[V] \approx K$ donc les homomorphismes $\neq 0$ de $K[W]$ dans K correspondent aux éléments de W.

Si $f : V \to W$ est polynomiale, pour toute P linéaire sur W, on peut décomposer $P\circ f$ en ses composantes homogènes, d'où l'on voit facilement que $f = \sum_n f_n$, f_n étant une application polynomiale telle que $P\circ f_n$ soit la composante de degré n de $P\circ f$. Si f et g sont polynomiales, il est clair que $g\circ f$ l'est aussi.

Soit $f = \sum_{m \geq m_0} f_m$ et $g = \sum_{n \geq n_0} g_n$ $(m_0 \geq 1)$, je vais montrer que les composantes de degré $< m_0 n_0$ de $h = g\circ f$ sont nulles et que $h_{m_0 n_0} = g_{m_0} \circ f_{n_0}$;

comme il faut examiner les composantes de $P\circ h = (P\circ g)\circ f$ pour P linéaire on se ramène tout de suite au cas où g est à valeurs dans K. Soit d'abord g homogène de degré n $g = \sum_j \prod_i P_{i,j}$ où les P sont linéaires. Mais alors

$P_{i,j}\circ f = \sum_m P_{i,j}\circ f_m$ et $g\circ f = \sum_j \prod_i P_{i,j}\circ f = \sum_j \sum_{(m_i)} \prod_i P_{i,j}\circ f_{m_i}$ chaque terme de cette somme ayant le degré $\sum_i m_i \geqslant nm_0$ car les m_i sont au moins égaux à m_0, f n'ayant pas de termes de degré $< m_0$. Donc il n'y a pas de termes de degré $< m_0 n$ dans h et pour obtenir le terme de degré $m_0 n$, il faut faire tous les m_i égaux à m_0 car f n'a pas de termes de degré 0 $(m_0 \geqslant 1)$ c'est-à-dire qu'on obtient les termes du développement de $g\circ f_{m_0}$. Comme $g = \sum g_n$ les g_n étant homogènes de degré n, on passe de là immédiatement au cas général.

Si f est une application polynomiale de V dans W, $f(v + X) - f(v) = \Delta f(X, v)$ est polynomiale en X pour $v \in V$ fixé et sa composante de degré 1, soit $df(X, v) = (df)_v(X)$ s'appelle <u>la différentielle de</u> f <u>en</u> v ; $(df)_v$ est une fonction linéaire de X. Soit $h = g\circ f$ et $w = f(v)$ on a alors

$$(1) \quad \Delta h(X, v) = g(f(v + X)) - g(f(v)) = g(w + \Delta f(X, v)) - g(w)$$
$$= \Delta g(\Delta f(X, v), w)$$

Or Δf et Δg sont sans termes constants donc en prenant les termes de degré 1 dans l'égalité (1) on trouve $(dh)_v = (dg)_w\circ(df)_v$

Supposons que pour un v donné, $(df)_v$ applique V sur W et prenons dans la formule (1) une fonction polynome P pour h. Si $P \neq 0$, $\Delta P(X, w) \neq 0$; soit ΔP_m son terme de plus bas degré. D'après la formule (1) et ce qu'on a déjà démontré, le terme de degré m de Δh est égal à $\Delta P_m\circ(df)_v$ qui est différent de 0 car $(df)_v$ applique V <u>sur</u> W, donc $\Delta h \neq 0$ et $h = P\circ f \neq 0$.

<u>Lemme</u> : <u>Soit</u> f <u>une application polynome de</u> V <u>dans</u> W <u>telle que pour un</u> v <u>donné</u> $(df)_v$ <u>applique</u> V <u>sur</u> W. <u>Alors si le corps</u> K <u>est algébriquement clos pour toute fonction polynome</u> $P \neq 0$ <u>sur</u> V, <u>il existe une fonction polynome</u> $Q \neq 0$ <u>sur</u> W <u>telle que si</u> w <u>n'annule pas</u> Q, <u>il soit l'image par</u> f <u>d'un</u> $v \in V$ <u>qui n'annule pas</u> P.

a) D'après ce qu'on vient de voir, $P \to P\circ f$ est une application biunivoque de $K[W]$ dans $K[V]$. Les éléments de V correspondant aux homomorphismes $\neq 0$ de $K[V]$ dans K, il suffit de montrer qu'on peut trouver $Q \in K[W]$

non nul tel que tout homomorphisme de $K[W]$ dans K qui n'annule pas Q se prolonge en un homomorphisme de $K[V]$ dans K qui n'annule pas P.

b) Posons $A = K[V]$ et appelons B l'image de $K[W]$ dans A. A a un nombre fini $z_1 \dots z_h$ de générateurs ; posons $A_k = B[z_{k+1},\dots,z_h]$ donc $A_0 = A$, $A_h = B$ et $A_{k-1} = A_k[z_k]$. Si l'on suppose qu'on sache faire le pas de A_k à A_{k+1} on trouvera successivement $P_1 \in A_1$, tel que tout homomorphisme de A_1 dans K qui n'annule pas P_1 se prolonge en un homomorphisme de A dans K qui n'annule pas $P_0 = P$, puis $P_2 \in A_2$ tel que tout homomorphisme de A_2 dans K qui n'annule pas P_2 se prolonge en un homomorphisme de A_1 dans K qui n'annule pas P_1, etc...

c) Soit donc C et $D = C[z]$ deux anneaux d'intégrité et $p \neq 0$ dans D. Si z ne vérifie aucune équation algébrique à coefficients dans C, D est l'anneau des polynomes en z à coefficients dans C et p a au moins un coefficient $a \neq 0$. Soit f un homomorphisme de C dans K et $\bar{P}$ le polynome à coefficients dans K obtenu en appliquant f aux coefficients de p. Si $f(a) \neq 0$, on a $\bar{P} \neq 0$, donc il existe $b \in K$ avec $\bar{P}(b) \neq 0$ et si $\bar{f}$ est l'homomorphisme bien déterminé de D dans K qui prolonge f et envoie z sur b, on a $\bar{f}(p) = \bar{P}(b) \neq 0$, donc tout homomorphisme de C dans K qui n'annule pas a se prolonge en un homomorphisme de D dans K qui n'annule pas p.

Si z vérifie au moins une équation algébrique sur C, pour définir un homomorphisme $\bar{f}$ de D dans K prolongeant un homomorphisme donné f de C dans K et vérifiant $\bar{f}(z) = b$, il faut chercher $b \in K$ vérifiant toutes les équations $\bar{P}(b) = 0$ où $\bar{P}$ est le polynome obtenu en appliquant f aux coefficients d'un polynome P annulé par z. Soit $P(z) = 0$ une équation de degré minimal pour z, $P(Z) = \sum_{i=1}^{n} a_i Z^i$; si Q est un autre polynome l'identité de la division s'écrit $a_n^k Q(Z) = U(Z)P(Z) + V(Z)$ avec k assez grand et $\deg V < \deg P$. Si $Q(z) = 0$, on en déduit $V(z) = 0$, donc $V = 0$ par raison de degré et $a_n^k Q(Z) = U(Z)P(Z)$; par suite si $f(a_n) \neq 0$ et $\bar{P}(b) = 0$ on en déduit $f(a_n)^k \bar{Q}(b) = 0$ et donc $\bar{Q}(b) = 0$. Or <u>puisque K est algébriquement clos</u>, il existe $b \in K$ avec $\bar{P}(b) = 0$, donc f a un prolongement $\bar{f}$ pourvu que $f(a_n) \neq 0$. Maintenant tout élément de D vérifie une équation algébrique sur C puisque le corps des quotients de D est algébrique sur celui de C ; soit donc $H(p) = 0$, H étant une équation de degré minimum pour p, donc en particulier $H(0) \neq 0$. Or de $H(p) = 0$ on tire $\bar{H}(\bar{f}(p)) = 0$ d'où si $f(H(0)) \neq 0$ $\bar{f}(p) \neq 0$ car $\bar{H}(0) = f(H(0)) \neq 0$.

En résumé si f n'annule pas $a_n H(0)$, elle n'annule ni l'un ni l'autre et se prolonge en $\bar{f}$ avec $\bar{f}(p) \neq 0$

C.Q.F.D.

2.- Application aux algèbres de Lie

Le corps K est algébriquement clos de caractéristique 0. Soit $\mathfrak{g}$ une algèbre de Lie sur K et $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{g}$, $\mathfrak{g} = \mathfrak{h} + \sum_{\alpha \neq 0} \mathfrak{g}^\alpha$ la décomposition associée. On sait que $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] \subset \mathfrak{g}^{\alpha+\beta}$, donc pour $X \in \mathfrak{g}^\alpha$, adX applique $\mathfrak{g}^\beta$ dans $\mathfrak{g}^{\alpha+\beta}$ et $\mathrm{ad}^k X$ applique $\mathfrak{g}^\beta$ dans $\mathfrak{g}^{\beta+k\alpha}$; comme les racines de $\mathfrak{g}$ sont en nombre fini, il en résulte que adX est nilpotent. On peut donc former $\exp \mathrm{ad}\, X = \sigma(X)$ qui est un automorphisme de $\mathfrak{g}$ (cf. Exp. 5) ; numérotons les racines de $\mathfrak{g}$ de manière arbitraire et considérons l'application $f : (X_1, \dots, X_n, H) \to \sigma(X_1) \dots \sigma(X_n) \cdot H$ de $\mathfrak{g}^{\alpha_1} \times \dots \mathfrak{g}^{\alpha_n} \times \mathfrak{h}$ dans $\mathfrak{g}$. Nous allons calculer la différentielle de f au point $(0, \dots, 0, H_0)$, or

$$(2) \quad f(X_1, \dots, X_n, H + H_0) = \sum [X_1^{m_1}, [X_2^{m_2} \dots H] \dots] / \prod_i m_i ! +$$

$$+ \sum [X_1^{m_1}, [\dots H_0] \dots] / \prod_i m_i ! \quad \text{où l'on pose } [X^k, Y] = \mathrm{ad}^k X . Y$$

les termes contenant H sont de degré $m_1 + \dots + m_n + 1$ et ceux contenant H_0 de degré $m_1 + \dots + m_n$. Les termes de degré 1 de (2) sont donc H et $[X_i, H_0]$ donc $df(X_1, \dots, X_n, H ; 0, \dots, 0, H_0) = H + \sum_i [X_i, H_0]$; supposons que $\prod_\alpha \alpha(H_0) \neq 0$ alors le déterminant de $\mathrm{ad} H_0$ dans $\sum_\alpha \mathfrak{g}^\alpha$ qui est égal à $\prod_\alpha \alpha(H_0)$ est différent de 0 et $df(X, H ; 0, H_0) = 0$ implique $X_i = 0$. df est donc un isomorphisme de $\mathfrak{g}$ dans $\mathfrak{g}$ au point $(0 ; H_0)$ ce qui permet d'appliquer le lemme : donc si G est le groupe d'automorphismes de $\mathfrak{g}$ engendré par les $\sigma(X)$ pour $X \in \mathfrak{g}^\alpha$, il existe un polynome $Q \neq 0$ sur $\mathfrak{g}$ tel que tout élément de $\mathfrak{g}$ qui n'annule pas Q soit conjugué par G d'un élément H de $\mathfrak{h}$ avec $\prod_\alpha \alpha(H) \neq 0$.
L'ensemble des élements réguliers de $\mathfrak{g}$, soit R, est défini par la condition $\varphi_k(x) \neq 0$ où φ_k est une fonction polynome sur $\mathfrak{g}$ non nulle ; d'autre part R est invariant par tous les automorphismes de $\mathfrak{g}$ par sa définition même, en particulier il est invariant par G. Soit donc $x \in \mathfrak{g}$ avec $Q(x)\varphi_k(x) \neq 0$, on a $\varphi_k(x) \neq 0$ donc x est régulier et $Q(x) \neq 0$ donc $x = g \cdot H$ avec $\prod_\alpha \alpha(H) \neq 0$ et $g \in G$ donc H est régulier.

Or $\mathfrak{g}(H\ ,\ 0) = \mathfrak{h} = \mathfrak{g}(H'\ ,\ 0)$ si $\prod_{\alpha} \alpha(H') \neq 0$ donc H' est aussi régulier ; en résumé tout $x \in \mathfrak{g}$ régulier tel que $Q(x) \neq 0$ est conjugué par G d'un élément régulier de $\mathfrak{h}$. Si $\mathfrak{h}'$ est une autre algèbre de Cartan, il existe de même Q' tel que si $Q'(x) \neq 0$, x régulier est conjugué par G' d'un élément régulier de $\mathfrak{h}'$. G et G' sont tous deux contenus dans le groupe A d'automorphismes de $\mathfrak{g}$ engendré par les $\exp \operatorname{ad} X$ pour $\operatorname{ad} X$ nilpotent. Si $Q(x)Q'(x)$ est non nul, x régulier est conjugué par A à la fois d'un élément régulier H de $\mathfrak{h}$ et d'un élément régulier H' de $\mathfrak{h}'$. Donc H et H' sont conjugués par A et comme $\mathfrak{h} = \mathfrak{g}(H\ ,\ 0)$ $\mathfrak{h}' = \mathfrak{g}(H'\ ,\ 0)$ $\mathfrak{h}$ et $\mathfrak{h}'$ sont conjuguées par A . Finalement, on a le théorème suivant :

Théorème : Soit $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{g}$; tout élément H de $\mathfrak{h}$ qui n'annule aucune des racines de $\mathfrak{g}$ suivant $\mathfrak{h}$ est régulier et donc $\mathfrak{h} = \mathfrak{g}(H\ ,\ 0)$. De plus deux sous-algèbres de Cartan de $\mathfrak{g}$ sont conjuguées par un élément du groupe A d'automorphismes de $\mathfrak{g}$ engendré par les $\exp \operatorname{ad} X$ ($\operatorname{ad} X$ étant nilpotent)