P. CARTIER

**Théorèmes d'Ado et d'Iwasawa**

*Séminaire "Sophus Lie"*, tome 1 (1954-1955), exp. nº 8, p. 1-5
<http://www.numdam.org/item?id=SSL_1954-1955__1__A12_0>

Exposé n° 8

# THÉORÈMES D'ADO ET D'IWASAWA

(Exposé par P. CARTIER, le 11.1.54)

---

## 1.- Introduction.

$\mathfrak{g}$ désignera désormais une algèbre de Lie de dimension finie sur le corps $K$ de caractéristique $0$ (cf. appendice pour le cas de caractéristique $p \neq 0$). Le but de cet exposé est de démontrer les deux théorèmes suivants :

Théorème 1.- (Ado) $\mathfrak{g}$ admet une représentation linéaire fidèle de dimension finie, le plus grand idéal nilpotent $\mathfrak{n}$ de $\mathfrak{g}$ étant représenté par des opérateurs nilpotents.

Théorème 2.- (Iwasawa) Si $M$ est un $\mathfrak{g}$-module de dimension finie et $u \in H^2(\mathfrak{g}, M)$, il existe un $\mathfrak{g}$-module de $N$ de dimension finie contenant $M$ telle que l'application canonique de $H^2(\mathfrak{g}, M)$ dans $H^2(\mathfrak{g}, N)$ annule $u$.

La méthode de démonstration suivie est dûe pour l'essentiel à Harish Chandra. En reprenant une méthode de démonstration du théorème 1, dûe à E. Cartan, Hochschild vient de démontrer l'analogue du théorème 2 pour tous les $H^p(\mathfrak{g}, M)$ lorsque $\mathfrak{g}$ est résoluble (résultat obtenu indépendamment par Koszul).

On aura besoin au cours de la démonstration du lemme suivant d'algèbre associative :

Lemme : Si $A$ est une algèbre associative engendrée par un nombre fini d'éléments, tout idéal bilatère $I$ de $A$ de codimension finie admet une base finie (comme idéal bilatère) et les idéaux $I^S$ sont de codimension finie.

On peut d'après les hypothèses faites sur $A$ et $I$ trouver un sous-espace $G \subset A$ de dimension finie tel que $G + I = A$ et que $G$ engendre $A$ comme algèbre. Si donc $g_1$, $g_2 \in G$ on a $g_1 g_2 = g + i$ avec $g \in G$ et $i \in I$ donc $i \in I \cap (G + G^2)$. Soit $Z$ l'idéal bilatère engendré par le sous-espace de dimension finie $I \cap (G + G^2)$. Modulo $Z$, $G$ est multiplicativement clos donc $G + Z$ est une sous-algèbre de $A$ qui est d'ailleurs égale à $A$ puisqu'elle contient $G$. Donc $G + Z = A$, $Z \subset I$ est de codimension finie et a un nombre fini de générateurs, donc $I$ a un nombre fini de générateurs.

$I/I^2$ est de manière évidente un $A$-bimodule donc l'annulateur contient $I$ donc un $A/I$-bimodule. $A/I$ est de dimension finie et $I$ admet un nombre fini de générateurs donc $I/I^2$ est de dimension finie donc aussi $A/I^2$ extension de $A/I$ par $I/I^2$. $I^2$ est de codimension finie donc par récurrence sur $n$, $I^{2^n}$ l'est aussi et $I^S$ également si $S < 2^n$.

2.- Le théorème préparatoire :

Théorème 3 : $\mathfrak{h}$ étant un idéal abélien de $\mathfrak{g}$ et $U$ l'algèbre enveloppante de $\mathfrak{g}$, il existe dans $U$ un idéal bilatère $Z$ avec les 4 propriétés suivantes :

1) $Z$ est de codimension finie
2) $Z \cap \mathfrak{h} = 0$
3) $Z$ contient $\mathfrak{h}\mathfrak{g}$
4) $Z$ contient $\mathfrak{n}^s$ pour $s$ assez grand.

Faisons quelques remarques préparatoires : un idéal bilatère de codimension finie de $U$ est le noyau d'une représentation linéaire de $\mathfrak{g}$ de dimension finie et réciproquement, en particulier tout idéal à gauche de codimension finie contient un idéal bilatère de codimension finie. De plus il résulte du théorème d'Engel que la condition 4) équivaut au fait que $Z$ contient une puissance convenable de tout élément de $\mathfrak{n}$. Enfin si $\mathfrak{a}_1 \dots \mathfrak{a}_k$ sont des idéaux de $\mathfrak{g}$ et $T$ l'idéal à gauche de $U$ engendré par $\mathfrak{a}_1 \dots \mathfrak{a}_k$, toute dérivation $D$ de $\mathfrak{g}$ qui laisse stable les $\mathfrak{a}_i$ a un prolongement à $U$ qui laisse stable $T$ car

$$\bar{D}(u\, a_1 \dots a_k) = \sum_{i=1}^{k} u \dots a_{i-1}\, Da_i \dots a_k + \bar{D}u\, a_1 \dots a_k \in T$$

Si en particulier $D = \operatorname{ad} g$ $\bar{D}u = gu - ug$ et il en résulte que $Tg \subset T$ donc que $T$ est un idéal bilatère de $U$.

Le premier pas de la démonstration du théorème 3 est le suivant :

Si $\mathfrak{g}$ est résoluble et $Z$ vérifie les conditions 1), 2), 3), 4), il existe un idéal bilatère $Z' \subset Z$ vérifiant ces mêmes conditions et de plus :

5) $Z'$ est invariant par toute dérivation $\bar{D}$ qui prolonge une dérivation $D$ de $\mathfrak{g}$ telle que $D\mathfrak{h} \subset \mathfrak{h}$

Soit $A \supset Z$ l'idéal bilatère de $U$ tel que $A/Z$ soit le radical de l'algèbre associative $U/Z$. $A/Z$ est un idéal nilpotent donc $A^r \subset Z$ pour $r$ assez grand. On sait d'autre part (Exposé n° 7 bis) que $\mathfrak{n} \subset A$ et que toute

dérivation

envoie $\mathfrak{g}$ dans $\mathfrak{n}$ (idem, noter que $\mathfrak{g}$ est résoluble). Donc si $u = g_1 \dots g_n$

$$\bar{D}\, u = \Sigma\, g_1 \dots D\, g_i \dots g_n \in A \qquad \bar{D}\, 1 = 0$$

donc $\bar{D}\, U \subset A$ en particulier $A$ est stable par $\bar{D}$. L'idéal à gauche $S$ engendré par $\mathfrak{h}\mathfrak{g}$ étant stable par toute dérivation $\bar{D}$ telle que $D\,\mathfrak{h} \subset \mathfrak{h}$ et étant de plus bilatère, si l'on pose $Z' = A^r + S$, $Z'$ vérifie 5). Il est clair que $Z' \subset Z$. De plus le lemme du 1 montre que $A^r$ est de codimension finie donc aussi $Z' \supset A^r$. 1) est donc vérifiée. Comme $Z' \cap \mathfrak{h} \subset Z \cap \mathfrak{h} = 0$, 2) l'est aussi. 3) l'est de même puisque $Z' \supset S \supset \mathfrak{h}\mathfrak{g}$. Enfin comme $\mathfrak{n} \subset A$ $\mathfrak{n}^r \subset Z'$ et 4) est vérifiée.

Le premier pas est terminé. Abordons le second.

Supposons $\mathfrak{g}$ somme directe de l'idéal résoluble $\mathfrak{p}$ et de la sous-algèbre $\mathfrak{L}$ et $\mathfrak{h} \subset \mathfrak{p}$ $\mathfrak{n} = \mathfrak{n} \cap \mathfrak{p} + \mathfrak{n} \cap \mathfrak{L}$. Si $U(\mathfrak{p})$ possède un idéal $Z'$ vérifiant les conditions 1) et 5), $U(\mathfrak{g})$ possède un idéal avec les propriétés 1) à 4).

Pour tout $g \in \mathfrak{g}$ on définit une dérivation $D_g$ de $\mathfrak{p}$ en restreignant $\operatorname{ad} g$ à $\mathfrak{p}$. $D_g\,\mathfrak{h} \subset \mathfrak{h}$ car $\mathfrak{h}$ est un idéal de $\mathfrak{g}$ donc $\bar{D}g\, Z' \subset Z'$.
$U(\mathfrak{g}) \approx U(\mathfrak{p}) \otimes U(\mathfrak{L})$ d'après Birkhoff-Witt cet isomorphisme étant seulement linéaire. L'idéal à gauche engendré par $Z'$ est donc $Z' \otimes U(\mathfrak{L})$ mais cet idéal est un idéal à droite car $gz - zg = \bar{D}_g\, Z \in Z'$ si $Z \in Z'$ ; de plus l'idéal à gauche engendré par $\mathfrak{L}$ dans $U(\mathfrak{g})$ est $U(\mathfrak{p}) \otimes \mathfrak{L}U(\mathfrak{L})$.
$V = Z' \otimes U(\mathfrak{L}) + U(\mathfrak{p}) \otimes \mathfrak{L}U(\mathfrak{L})$ est donc un idéal à gauche de $U(\mathfrak{g})$ et $U(\mathfrak{g})/V \simeq U(\mathfrak{p})/Z' \otimes U(\mathfrak{L})/\mathfrak{L}U(\mathfrak{L}) \simeq U(\mathfrak{p})/Z' = T$. $T$ est de dimension finie et il y a une représentation linéaire canonique $\theta$ de $U(\mathfrak{g})$ dans $T$ dont le noyau est le plus grand idéal bilatère $Z$ contenu dans $V$. Comme $p(u \otimes 1) = = P\, u \otimes 1$ et $b(u \otimes 1) = \bar{D}_b\, u \otimes 1 + u \otimes b \equiv \bar{D}_b\, u \otimes 1$ mod $Z'$ on voit que $\theta(p)\dot{u} = \widehat{p\, \dot{u}}$ $\theta(b)\dot{u} = \widehat{\bar{D}_b\, \dot{u}}$ ($\dot{u}$ est la classe de $u$ mod $Z'$ ).

On a $\theta(h)\, \dot{1} = \dot{h} \neq 0$ si $h \neq 0$ car $\mathfrak{h} \cap Z' = 0$ donc $\mathfrak{h} \cap Z = 0$.
$Z$ étant évidemment de codimension finie 1) et 2) sont vérifiés. Comme $Z' \supset \mathfrak{h}\mathfrak{p}$ $V \supset \mathfrak{h}\,\mathfrak{p} + \mathfrak{h}\,\mathfrak{L} = \mathfrak{h}\,\mathfrak{g}$ donc $V$ contient l'idéal à gauche engendré par $\mathfrak{h}\mathfrak{g}$, mais ce dernier idéal est bilatère donc contenu dans $Z$ et $\mathfrak{h}\mathfrak{g} \subset Z$ : voici pour 3). Enfin l'énsemble $E$ des $n \in \mathfrak{n}$ tels que $\theta(n)$ soit nilpotent est un sous-espace vectoriel de $\mathfrak{n}$ (cf. Exposé n° 7 bis).
$(\mathfrak{n} \cap \mathfrak{p})^S \subset Z'$ donc $(\mathfrak{n} \cap \mathfrak{p})^S \subset V$, mais l'idéal à gauche engendré par $(\mathfrak{n} \cap \mathfrak{p})^S$ est bilatère (cf. le cas de $\mathfrak{h}\mathfrak{g}$ ) et donc $(\mathfrak{n} \cap \mathfrak{p})^S \subset Z$ $\mathfrak{n} \cap \mathfrak{p} \subset E$.
Par ailleurs si $b \in \mathfrak{n} \cap \mathfrak{L}$ $\operatorname{ad} b$ est nilpotent donc $D_b$ est nilpotent sur $\mathfrak{p}$.
L'ensemble des $u \in U(\mathfrak{p})$ annulés par une puissance de $\bar{D}_b$ est une sous algèbre

d'après la formule de Leibniz donc est identique à $U(\mathfrak{p})$. Par suite une puissance de $\theta(b)$ annule $T$ et $b \in E$ $\mathfrak{u} \cap \mathfrak{b} \subset E$ et finalement $\mathfrak{u} \subset E$, 4) est vérifiée.

Il nous reste pour établir le théorème 3 à raisonner par récurrence sur la dimension de $\mathfrak{g}/\mathfrak{h}$. Si $\mathfrak{g} = \mathfrak{h}$ $U(\mathfrak{g}) \simeq S(\mathfrak{h})$. On prendra pour $Z$ l'idéal engendré par $\mathfrak{h}^2$, c'est-à-dire par l'ensemble des éléments homogènes de degré $\geqslant 2$. Les conditions 1) à 4) se vérifient trivialement. Si $\mathfrak{g} \neq \mathfrak{h}$ nous distinguerons deux cas : a) $\mathfrak{g}$ est résoluble, donc $\mathfrak{g}/\mathfrak{h} = \mathfrak{a}$ est résoluble $[\mathfrak{a},\mathfrak{a}] \neq \mathfrak{a}$ donc $[\mathfrak{g},\mathfrak{g}] + \mathfrak{h} \neq \mathfrak{g}$. Prenons pour $\mathfrak{p}$ un hyperplan contenant $[\mathfrak{g},\mathfrak{g}] + \mathfrak{h}$ et pour $\mathfrak{b}$ une droite supplémentaire de $\mathfrak{p}$ qui soit contenue de plus dans $\mathfrak{u}$ si $\mathfrak{u} \not\subset \mathfrak{p}$. $\mathfrak{g} = \mathfrak{p} \oplus b$, $\mathfrak{p}$ est un idéal résoluble, $\mathfrak{b}$ une sous-algèbre $\mathfrak{u} = \mathfrak{u} \cap \mathfrak{p} + \mathfrak{u} \cap \mathfrak{b}$

b) $\mathfrak{g}$ n'est pas résoluble, alors d'après le théorème de Levi $\mathfrak{g} = \mathfrak{p} + \mathfrak{b}$, $\mathfrak{p}$ étant le radical, $\mathfrak{b}$ une sous-algèbre semi-simple et $\mathfrak{u} \subset \mathfrak{p}$.

Comme $\dim \mathfrak{p}/\mathfrak{h} < \dim \mathfrak{g}/\mathfrak{h}$ on peut construire dans $U(\mathfrak{p})$ un idéal $Z_1$ vérifiant 1) à 4). Mais $\mathfrak{p}$ est résoluble et on peut donc l'astreindre (pas 1) à vérifier 5) en plus. Alors (pas 2), on peut construire un idéal $Z_2$ de $U(\mathfrak{g})$ vérifiant 1) à 4).

C.Q.F.D.

3.- Démonstration des théorèmes 1 et 2 :

Théorème 1 : Soit $\mathfrak{h}$ le centre de $\mathfrak{g}$ et construisons un idéal $Z$ de $U(\mathfrak{g})$ vérifiant 1), 2), 4). $Z$ est le noyau d'une représentation linéaire $\theta$ de dimension finie fidèle sur $\mathfrak{h}$ et représentant $\mathfrak{u}$ par des opérateurs nilpotents. Le noyau de la représentation adjointe $\theta'$ est $\mathfrak{h}$ et si $n \in \mathfrak{u}$ ad$n$ est nilpotent. Il est alors clair que la représentation $\psi$ somme directe de $\theta$ et $\theta'$ convient et démontre le théorème.

Théorème 2 : Soit $u \in H^2(\mathfrak{g}, M)$ ; la construction que l'on va faire pour "tuer" $u$ est analogue à celle de l'exposé n° 5 bis. Soit $\mathfrak{a}$ une extension de $\mathfrak{g}$ par $M$, soit $0 \longrightarrow M \xrightarrow{i} \mathfrak{a} \xrightarrow{\pi} \mathfrak{g} \longrightarrow 0$ correspondant à $u$ (Exposé n° 5) (on identifie $M$ et $i(M) \subset \mathfrak{a}$). $U(\mathfrak{a})$ est l'algèbre enveloppante de $\mathfrak{a}$ et $I = \mathfrak{a}\, U(\mathfrak{a})$ l'idéal maximal. $I$ est un $U(\mathfrak{a})$ module à gauche, c'est-à-dire un $\mathfrak{a}$-module, donc $I/MI = P$ est un $\mathfrak{a}/M$-module, c'est-à-dire un $\mathfrak{g}$-module. Comme $M \subset \mathfrak{a} \subset I$ il existe $\varphi : M \longrightarrow P$ ; $\varphi$ est un $\mathfrak{g}$-homomorphisme car si $m \in M$ $g \in \mathfrak{g}$ $\theta(g)m = [a,m]$ $\pi(a) = g$ mais $[a,m] \equiv a\,m$ mod $MI$ et par définition $g.\dot{m} = \widehat{a.m}$ d'où l'assertion sur $\varphi$. Soit $k \in u$

un cocycle de classe $u$ $k(x,y) = [\ell(x)\ell(y)] - \ell([x,y])$ $\ell$ étant une section $\mathfrak{g} \longrightarrow \mathfrak{a}$. Si on considère $\ell$ comme une fonction à valeurs dans $I$ on a $k(x,y) = \ell(x)\,\ell(y) - \ell([x,y]) - \ell(y)\,\ell(x)$ c'est-à-dire modulo $MI$ $\widehat{\dot{k}(x,y)} \equiv x \cdot \widehat{\dot{\ell}(y)} - \widehat{\dot{\ell}([x,y])} - y \cdot \widehat{\dot{\ell}(x)}$ donc $\varphi \circ k$ est un cobord dans $C^2(\mathfrak{g}, P)$ et par suite $\varphi_2^* u = 0$. $P$ est de dimension infinie mais d'après le théorème 3 il existe un idéal $Z \supset MI$ $Z \cap M = 0$ de codimension finie dans $U(\mathfrak{a})$. Alors $N = I/Z = P/_{Z/MI}$ est de dimension finie et comme $M \cap Z = 0$ $M$ plonge dans $N$. Comme $u$ est "tué" par $\varphi M \longrightarrow P$ elle l'est a fortiori par l'injection de $M$ dans $N$ composée de $\varphi$ et de $P \longrightarrow P/_{Z/MI}$.

C.Q.F.D.

Noter que le théorème 2 équivaut au fait que pour toute extension $\mathfrak{a}$ de $\mathfrak{g}$ par $M$ il existe une extension inessentielle $\mathfrak{b} \supset \mathfrak{a}$ de $\mathfrak{g}$ par $N$ telle que le diagramme suivant soit commutatif

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d] & \mathfrak{a} \arrow[r] \arrow[d] & \mathfrak{g} \arrow[r] & 0 \\ 0 \arrow[r] & N \arrow[r] & \mathfrak{b} \arrow[ur] & & \end{tikzcd}$$

## APPENDICE

$K$ est supposé de caractéristique $p \neq 0$. On va montrer qu'il existe dans $U(\mathfrak{g})$ un idéal $Z$ vérifiant les conditions 1) à 3) du théorème 3 ce qui assurera que $\mathfrak{g}$ a une représentation fidèle de dimension finie et que toute 2-classe de cohomologie est "tuée" comme dans le théorème 2. Soit $x_1 \dots x_k$ $y_1 \dots y_n$ une base de $\mathfrak{g}$ les $x_i$ étant dans $\mathfrak{h}$. $D_i = \operatorname{ad} y_i$ se prolonge en une dérivation $\overline{D}_i$ de $U(\mathfrak{g})$. Mais comme on est en caractéristique $p$ on peut vérifier que $\overline{D}_i^p u = [y_i^p, u]$ $(u \in U(\mathfrak{g}))$. Comme $\mathfrak{g}$ est de dimension finie, il existe des constantes $a_{i,j}$ telles que $\sum_j a_{i,j} \overline{D}_i^{p^j} = 0$ donc $\sum_j a_{i,j} y_i^{p^j}$ est dans le centre de $U(\mathfrak{g})$. Soit $Z$ l'idéal bilatère de $U(\mathfrak{g})$ engendré par ces éléments et $\mathfrak{h}\mathfrak{g}$. Le théorème de Birkhoff-Witt appliqué à la base formée des $x$ et des $y$ montre alors facilement que $Z$ est de codimension finie et que $\mathfrak{h} \cap Z = 0$.

C.Q.F.D.