Séminaire "Sophus Lie"

P. Cartier

Le théorème de Poincaré-Birkhoff-Witt

Séminaire "Sophus Lie", tome 1 (1954-1955), exp. n° 1, p. 1-10
<http://www.numdam.org/item?id=SSL_1954-1955__1__A3_0>

Exposé n° 1

LE THÉORÈME DE POINCARÉ-BIRKHOFF-WITT

(Exposé de P. CARTIER du 9.11.1954)

1.- Préliminaires.

Pour tous ces préliminaires, on pourra se reporter par exemple à (1) .

Définition. On appelle algèbre de Lie $\mathcal{G}$ sur un anneau commutatif K ayant un élément unité un K-module unitaire $\mathcal{G}$ muni d'une application bilinéaire $(x,y) \to [x,y]$ de $\mathcal{G} \times \mathcal{G}$ dans $\mathcal{G}$, appelée crochet de x et de y, et qui vérifie les deux axiomes suivants :

(i) $[x,x] = 0$ d'où l'on déduit : $[x,y] = -[y,x]$

(ii) $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$ (identité de Jacobi) .

Dans ce séminaire, on se bornera en principe, au cas où K est un corps de caractéristique nulle.

Exemples.

1°) Algèbre de Lie libre. Soit S un ensemble quelconque, $\bar{S}$ l'ensemble des mots non associatifs d'éléments de S (i.e. on met autant de parenthèses qu'il est nécessaire). Le module E des combinaisons linéaires formelles d'éléments de $\bar{S}$ à coefficients dans K est muni trivialement d'une structure multiplicative n'ayant d'autres propriétés que d'être une application bilinéaire de $E \times E$ dans E . En passant au quotient par la relation d'équivalence que définissent (i) et (ii) , on obtient une algèbre de Lie sur K que l'on appelle l'algèbre de Lie libre construite sur S .

2°) Algèbre de Lie abélienne. Sur un K-module E , posons $[x,y] = 0$ quels que soient x et $y \in E$. E est ainsi muni d'une structure d'algèbre de Lie. On dit que E est une algèbre de Lie abélienne (pour des raisons tirées de la théorie des groupes de Lie, - et aussi de (i)).

3°) Soit A une algèbre associative sur K , et posons $[a,b] = ab - ba$. Cette opération crochet munit le K-module A d'une structure d'algèbre de Lie $\bar{A}$ sur K . Si en particulier A est l'algèbre associative des endomorphismes d'un K-module M , $\bar{A}$, noté en général $\mathcal{gl}(M)$, s'appelle l'algèbre de Lie des endomorphismes de M.

4°) Produit direct. Soient $\mathfrak{g}_1$ et $\mathfrak{g}_2$ deux algèbres de Lie sur K . Définissons sur le K-module $\mathfrak{g} = \mathfrak{g}_1 \times \mathfrak{g}_2$ une opération crochet en posant :

$$[(x_1 , x_2),(y_1 , y_2)] = ([x_1 , y_1] , [x_2 , y_2]) \quad (x_i \text{ et } y_i \in \mathfrak{g}_i).$$

Cette opération satisfait aux axiomes (i) et (ii) et munit le module $\mathfrak{g}$ d'une structure d'algèbre de Lie : l'algèbre de Lie produit direct des algèbres $\mathfrak{g}_i$.

5°) A partir d'une algèbre de Lie donnée, on peut en fabriquer d'autres par extension ou restriction de l'anneau des scalaires.

Définitions. Un sous-module $\mathfrak{h}$ de $\mathfrak{g}$ est une sous-algèbre (resp. un idéal) de $\mathfrak{g}$ si $x \in \mathfrak{h}$, $y \in \mathfrak{h}$ (resp. $x \in \mathfrak{g}$, $y \in \mathfrak{h}$) entrainent $[x,y] \in \mathfrak{h}$. Il n'y a pas lieu de distinguer idéal à gauche et idéal à droite, vu (i) .

Si $\mathfrak{h}$ est un idéal de $\mathfrak{g}$, l'opération crochet passe au quotient dans $\mathfrak{g}/\mathfrak{h}$ qui est ainsi muni d'une structure d'algèbre de Lie quotient.

Un homomorphisme d'une algèbre de Lie $\mathfrak{g}$ dans une algèbre de Lie $\mathfrak{g}'$ est une application K-linéaire de $\mathfrak{g}$ dans $\mathfrak{g}'$ respectant le crochet (i.e. une application K-linéaire f telle que $f([x,y]) = [f(x),f(y)])$.

Une linéarisation d'une algèbre de Lie $\mathfrak{g}$ dans une algèbre associative A avec élément unité (sur le même anneau K) est une application de $\mathfrak{g}$ dans A qui est un homomorphisme dans l'algèbre de Lie $\bar{A}$ (i.e. qui vérifie $f([x,y]) = f(x)f(y) - f(y)f(x)$) . Une représentation linéaire de $\mathfrak{g}$ dans un K-module M est une linéarisation de $\mathfrak{g}$ dans l'algèbre des endomorphismes de M (ou, si l'on veut, un homomorphisme de $\mathfrak{g}$ dans $\mathfrak{gl}(M)$) .

Exemples.

1°) Les applications $x_1 \dashrightarrow (x_1 , 0)$ et $x_2 \dashrightarrow (0 , x_2)$ des algèbres de Lie $\mathfrak{g}_1$ et $\mathfrak{g}_2$ dans l'algèbre produit $\mathfrak{g} = \mathfrak{g}_1 \times \mathfrak{g}_2$ sont des monomorphismes permettant d'identifier $\mathfrak{g}_i$ (i = 1 , 2) à un idéal de $\mathfrak{g}$. Avec cette identification $[\mathfrak{g}_1 , \mathfrak{g}_2] = 0$; pour que $\mathfrak{g}$ soit isomorphe au produit direct de deux sous-algèbres $\mathfrak{g}'$ et $\mathfrak{g}''$, il faut et il suffit que $\mathfrak{g} = \mathfrak{g}' + \mathfrak{g}''$, $\mathfrak{g}' \cap \mathfrak{g}'' = \{0\}$, $[\mathfrak{g}' , \mathfrak{g}''] = \{0\}$.

2°) $\mathfrak{a}$ et $\mathfrak{b}$ étant deux parties de $\mathfrak{g}$, désignons par $[\mathfrak{a},\mathfrak{b}]$ l'ensemble des combinaisons linéaires des crochets d'un élément de $\mathfrak{a}$ par un élément de $\mathfrak{b}$. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux, il en est de même de $[\mathfrak{a},\mathfrak{b}]$ (résulte de Jacobi) . En particulier, posons :

$$\mathfrak{g} = \mathfrak{g}^{(1)} = \mathfrak{g}_1 \; ; \; \mathfrak{g}^{(n)} = [\mathfrak{g}^{n-1}, \mathfrak{g}^{n-1}] \; ; \; \mathfrak{g}_n = [\mathfrak{g}, \mathfrak{g}_{n-1}]$$

$\mathfrak{g}^{(n)}$ (resp. $\mathfrak{g}_n$) est un idéal de $\mathfrak{g}^{(r)}$ (resp. $\mathfrak{g}_r$) $(0 \leq r \leq n)$. La suite des $\mathfrak{g}_n$ est la série centrale descendante et $\mathfrak{g}^{(n)}$ la série dérivée. L'algèbre $\mathfrak{g}$ est dite <u>résoluble</u> (resp. <u>nilpotente</u>) s'il existe un entier $n > 0$ tel que $\mathfrak{g}^{(n)}$ (resp. $\mathfrak{g}_n$) soit nul. $\mathfrak{g}^{(2)}$ s'appelle l'idéal <u>dérivé</u> de $\mathfrak{g}$.

3°) L'ensemble des $x \in \mathfrak{g}$ tels que $[x,y] = 0$ pour tout $y \in \mathfrak{g}$ est un <u>idéal</u> appelé <u>centre</u> de $\mathfrak{g}$.

4°) On appelle <u>dérivation</u> d'une algèbre de Lie $\mathfrak{g}$ tout endomorphisme D du K-module $\mathfrak{g}$ vérifiant la condition $D[x,y] = [Dx,y] + [x,Dy]$. L'ensemble des dérivations de $\mathfrak{g}$ constitue une <u>sous-algèbre de l'algèbre de Lie</u> des endomorphismes du K-module $\mathfrak{g}$, notée $\mathfrak{D}(\mathfrak{g})$.

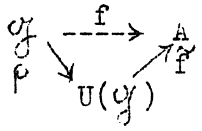
L'application $x \to \mathrm{ad}(x)$ de $\mathfrak{g}$ dans $\mathfrak{D}(\mathfrak{g})$ définie par :

$$\mathrm{ad}(x) : y \to [x,y]$$

est un homomorphisme (on le vérifie, de même que le fait que $\mathrm{ad}(x)$ est une dérivation, grâce à Jacobi), donc une représentation linéaire de $\mathfrak{g}$ dans le K-module $\mathfrak{g}$, appelée <u>représentation adjointe</u>. Son noyau est le centre $\mathfrak{z}$ de $\mathfrak{g}$, ce qui permet de plonger $\mathfrak{g}/\mathfrak{z}$ dans $\mathfrak{D}(\mathfrak{g})$, et son image est un <u>idéal</u> de $\mathfrak{D}(\mathfrak{g})$, (car $[D, \mathrm{ad}(x)] = \mathrm{ad}(Dx)$) appelé <u>idéal des dérivations intérieures.</u>

2.- <u>Algèbre enveloppante universelle.</u>

Nous allons montrer qu'on peut associer à toute algèbre de Lie $\mathfrak{g}$ sur K une algèbre associative $U(\mathfrak{g})$ sur K munie d'un élément unité, et une linéarisation ρ de $\mathfrak{g}$ dans U, telle qu'à tout couple (A,f) formé d'une algèbre associative sur K avec élément unité A et d'une linéarisation f de $\mathfrak{g}$ dans A on puisse associer uh homomorphisme d'algèbre $\tilde{f}$ de U dans A vérifiant $f = \tilde{f} \circ \rho$ et $\tilde{f}(1) = 1$.



On peut évidemment se restreindre au cas où U est engendrée (comme K-algèbre) par $\rho(\mathfrak{g})$ et l'unité. Il est alors clair que s'il y a une solution, elle est unique à un isomorphisme près. (En effet, s'il y avait deux solutions, (U,ρ) et (U',ρ'), les endomorphismes $\tilde{\rho}\tilde{\rho}'$ (resp. $\tilde{\rho}'\tilde{\rho}$) seraient l'identité sur la sous-

algèbre de U (resp. U') engendrée par $\rho(\mathfrak{g})$ et 1 (resp. $\rho'(\mathfrak{g})$ et 1).

Soit $T = \sum_r T^r$ l'algèbre tensorielle de $\mathfrak{g}$ sur K ($T^0 = K$, $T^1 = \mathfrak{g}$). Toute application linéaire f du K-module $\mathfrak{g}$ dans A se prolonge en un homomorphisme multiplicatif f^0 de T dans A en posant :

$$f^0(x_1 \otimes \dots \otimes x_k) = f(x_1) \dots f(x_k)$$

Si de plus f est une linéarisation, f^0 s'annule sur l'idéal J de T engendré par les éléments de la forme $x \otimes y - y \otimes x - [x,y]$, et définit une application $\tilde{f}$ de $U = T/J$ dans A . Réciproquement, soit ρ la restriction à $\mathfrak{g} = T^1$ de l'application canonique de T sur U . Pour toute linéarisation f de $\mathfrak{g}$ dans une algèbre associative unitaire A , et tout $z \in U$, qui soit la classe mod. J d'un tenseur décomposable $x_1 \otimes \dots \otimes x_k$, posons :

$$\tilde{f}(z) = f(x_1) \dots f(x_k) .$$

Il est immédiat que U , ρ , $\tilde{f}$ répondent aux conditions du problème. U=T/J s'appelle l'<u>algèbre enveloppante universelle de</u> $\mathfrak{g}$.

<u>Exemples</u> :

1°) Supposons $\mathfrak{g}$ <u>abélienne.</u> Alors J est engendré par les tenseurs de la forme $x \otimes y - y \otimes x$, et U est l'<u>algèbre symétrique</u> $S(\mathfrak{g})$ sur $\mathfrak{g}$. Si (x_i) est une base de $\mathfrak{g}$ sur K , U est isomorphe à l'algèbre des polynômes en les x_ι .

2°) Si $\mathfrak{g}$ est une algèbre <u>libre</u> de générateurs a_ι ($\iota \in I$) , soit L l'algèbre des polynômes <u>non commutatifs</u> en les b_ι ($\iota \in I$) et $\bar{L}$ l'algèbre de Lie déduite de l'algèbre associative L . Puisque $\mathfrak{g}$ est libre, l'application $a_\iota \to b_\iota$ se prolonge en un homomorphisme de $\mathfrak{g}$ dans $\bar{L}$, donc en une linéarisation ρ de $\mathfrak{g}$ dans L . Soit f une linéarisation de $\mathfrak{g}$ dans une algèbre A . Posons $c_\iota = f(a_\iota)$. Il existe un homomorphisme $\tilde{f}$ de L dans A et un seul tel que $f(1) = 1$ et $f(b_\iota) = c_\iota$ (car L est une algèbre associative libre). Alors f et $\tilde{f} \circ \rho$ sont des linéarisations qui coïncident sur les générateurs de $\mathfrak{g}$, donc partout, et (L, ρ) est l'algèbre enveloppante de $\mathfrak{g}$.

3°) Supposons que $\mathfrak{g}$ soit isomorphe au produit direct de deux sous-algèbres $\mathfrak{g}_1$, $\mathfrak{g}_2$, et soit (U_i, ρ_i) l'algèbre enveloppante de $\mathfrak{g}_i$ (i=1,2). Posons $V = U_1 \otimes U_2$ et soit ρ l'application de $\mathfrak{g}$ dans V :

$$\rho : x_1 + x_2 \to \rho_1(x_1) \otimes 1 + 1 \otimes \rho_2(x_2) \qquad (x_i \in \mathfrak{g}_i)$$

Il est immédiat que ρ est une linéarisation de $\mathcal{G}$ dans V. De plus si f est une linéarisation de $\mathcal{G}$ dans A, $f(x_1)$ et $f(x_2)$ commutent car $[x_1,x_2] = 0$. Donc si $\tilde{f}_i : U_i \to A$ est le prolongement à U_i de la restriction de f à $\mathcal{G}_i$, $\tilde{f}_1(U_1)$ et $\tilde{f}_2(U_2)$ commutent. Par suite, il existe un <u>homomorphisme</u> $\tilde{f}$ de $U_1 \otimes U_2$ dans A et un seul tel que :

$$\tilde{f}(a \otimes b) = \tilde{f}_1(a)\tilde{f}_2(b) .$$

Il est alors immédiat que :

$$\tilde{f}(\rho(x_1 + x_2)) = f(x_1) + f(x_2)$$

et que : $$\tilde{f}(1 \otimes 1) = 1 \times 1 = 1 .$$

Donc (V, ρ) est l'algèbre enveloppante de $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$

4°) Soit $\mathcal{G}$ une algèbre de Lie, $\mathcal{H}$ un idéal de $\mathcal{G}$, $(U(\mathcal{G}), \rho)$ l'algèbre enveloppante de $\mathcal{G}$, $\mathcal{R}$ l'idéal bilatère engendré dans U par $\rho(\mathcal{H})$, p (resp. p') la projection canonique de $\mathcal{G}$ sur $\mathcal{G}/\mathcal{H}$ (resp. de U sur $U/\mathcal{R}$). Il existe une application ρ' de $\mathcal{G}/\mathcal{H}$ dans $U/\mathcal{R}$ et une seule telle que $\rho' \circ p = p' \circ \rho$, et c'est une linéarisation. Toute linéarisation f de $\mathcal{G}/\mathcal{H}$ dans une algèbre A définit une linéarisation $f \circ p$ de $\mathcal{G}$ dans A, donc un homomorphisme $\widetilde{f \circ p}$ de $U(\mathcal{G})$ dans A qui définit à son tour par passage au quotient un homomorphisme $\tilde{f}$ de $U(\mathcal{G})/\mathcal{R}$ dans A (le lecteur est prié de faire un diagramme !). $\tilde{f}$ vérifie toutes les propriétés mirifiques souhaitées, de sorte que l'algèbre enveloppante de $\mathcal{G}/\mathcal{H}$ est $(U/\mathcal{R}, \rho')$.

<u>Remarque</u>. Comme $\rho(h)\rho(g) = \rho[h,g] + \rho(g)\rho(h)$, que $\mathcal{H}$ est un idéal et que U est engendré par $\rho(\mathcal{G})$ et l'unité, il est immédiat que $\mathcal{R}$ est identique à l'<u>idéal à gauche</u> engendré par $\rho(\mathcal{H})$ dans U.

3.- <u>Le Théorème de Poincaré-Birkhoff-Witt</u>.

Avant d'énoncer le théorème, il faut introduire quelques notations. Pour simplifier les notations, nous poserons $\rho(x) = \underline{x}$ $(x \in \mathcal{G})$.

Soit U_p l'ensemble des combinaisons linéaires des éléments de U qui peuvent s'écrire comme produits de q éléments $\underline{x}$ avec $q \leq p$. Les U_p déterminent une <u>filtration croissante</u> de U (i.e. $U_p \subset U_{p+1}$, $U_p U_q \subset U_{p+q}$, U est identique à la réunion des U_p). On a en particulier :

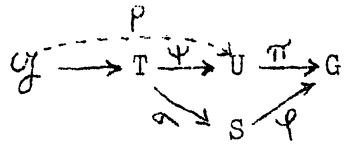
$$U_{-1} = \{0\}, \quad U_0 = K \ , \quad U_1 = U_0 + \mathcal{G} \ .$$

Remarquons que U est somme directe de l'idéal (à gauche, par exemple) engendré dans U par $\mathcal{G}$ et de U_0. La classe mod U_0 de $\underline{x}$ se note $\hat{x}$.

Soit G l'algèbre graduée associée à l'algèbre filtrée U : c'est la somme directe des modules G_p où $G_p = U_p/U_{p-1}$ et où le produit $g_p g_q$ est la classe modulo U_{p+q-1} du produit d'un représentant dans U_p de g_p et d'un représentant dans U_q de g_q $(g_i \in G_i)$: $G_p G_q \subset G_{p+q}$. G_0 est isomorphe à K et G_1 s'identifie à $\mathcal{G}$. De plus G est engendré par l'unité et G_1 puisque U_1 engendre U.

G est une algèbre <u>commutative</u>. En vertu de la remarque ci-dessus, il suffit en effet de vérifier que le produit de deux éléments $\hat{x}$ et $\hat{y}$ de G_1 est commutatif. Or $\hat{x}$ (resp. $\hat{y}$) est l'image de $\underline{x}$ (resp. $\underline{y}$) de $\mathcal{G}$, et il suffit donc de vérifier que $\underline{x}\,\underline{y} - \underline{y}\,\underline{x}$ est dans U_1, ce qui est évident, puisque ce dernier élément n'est autre que $[x,y]$.

L'application $x \longrightarrow \hat{x}$ de $\mathcal{G}$ dans G se prolonge en un homomorphisme de T <u>sur</u> G, lequel passe au quotient modulo l'idéal I de T engendré par les tenseurs de la forme $x \otimes y - y \otimes x$ comme nous venons de le voir, donc définit un <u>homomorphisme</u> φ de l'algèbre symétrique $S(\mathcal{G})$ de $\mathcal{G}$ sur G.



On remarquera que K et $\mathcal{G}$ sont plongés dans S comme dans T et que φ respecte les graduations.

Nous sommes en mesure d'énoncer le théorème. :

<u>THÉORÈME 1</u> : <u>Si</u> K <u>est un corps de caractéristique</u> 0, φ <u>est un isomorphisme de</u> $S(\mathcal{G})$ <u>sur</u> G.

Soit $(x_\iota)_{\iota \in I}$ une base de $\mathcal{G}$ que l'on ordonne totalement. Pour toute famille $M = (m_\iota)$ de $N^{(I)}$ (i.e. ensemble des applications de I dans l'ensemble N des entiers ≥ 0 nulles sauf pour un nombre fini d'indices), nous poserons, en désignant par Ψ, π, σ les applications canoniques de T dans U, U dans G, T dans S (cf. diagramme) :

$$|M| = \sum_\iota m_\iota \ ; \quad x^M = \otimes_\iota x_\iota^{m_\iota} \ ; \quad \underline{x}^M = \pi_\iota \underline{x}_\iota^{m_\iota} = \Psi(x^M) \ ; \quad z^M = \sigma(x^M) \ ,$$

en prenant soin de bien respecter l'ordre donné sur la base.

Le théorème 1 va résulter du théorème 1' :

THÉORÈME 1' : Les $\underline{x}^M$ forment une base de U .

Avant de voir comment le théorème 1 résulte de 1' , nous démontrerons d'abord 1' . Il est d'abord immédiat que les $\underline{x}^M$ engendrent l'espace vectoriel U . En effet, puisque G est commutatif, tout monôme de degré p en les $\underline{x}_\iota$ de U_p est congru modulo U_{p-1} à un $\underline{x}^M$ (réordonner les termes) ce qui montre bien, par récurrence sur p , que les $\underline{x}^M$ avec $|M| \leq p$ engendrent U_p .

Cela étant, le théorème 1' va résulter des trois lemmes :

LEMME 1 : Soient $\mathcal{G}$ une algèbre de Lie et $\mathfrak{h}$ un idéal de $\mathcal{G}$. Si le théorème 1' est vrai pour $\mathcal{G}$, il l'est aussi pour $\mathcal{G}/\mathfrak{h}$.

LEMME 2 : Si l'application $\rho : \mathcal{G} \longrightarrow U(\mathcal{G})$ est biunivoque, le théorème 1' est vrai pour $\mathcal{G}$.

LEMME 3 : Si $\mathcal{G}$ est une algèbre de Lie libre, l'application $\rho : \mathcal{G} \longrightarrow U(\mathcal{G})$ est biunivoque. [En effet si $\mathcal{G}$ est libre ρ est biunivoque (lemme 3) donc le théorème 1' est vrai pour $\mathcal{G}$ (lemme 2) mais toute algèbre de Lie est quotient d'une algèbre libre donc le théorème 1' est toujours vrai (lemme 1) .

Nous renvoyons au paragraphe suivant les démonstrations des lemmes, et nous allons tirer tout de suite des conséquences du théorème 1', et tout d'abord la :

Démonstration du théorème 1 .- Les $\underline{x}^M$ avec $|M| \leq p$ formant une base de U_p , les $\pi(\underline{x}^M)$ avec $|M| = p$ forment une base de G_p ; mais comme ces éléments ne sont autres que les $\varphi(z^M)$, et que les z^M forment une base de S_p , φ est bien biunivoque.

COROLLAIRE 1 .- Soient $\mathfrak{S}_n \subset T^n$ l'ensemble des tenseurs symétriques de T^n , et $\mathfrak{S} = \Sigma_n \mathfrak{S}_n$. La restriction à $\mathfrak{S}$ de $\Psi : T \longrightarrow U$ est un isomorphisme sur.

En effet, les symétrisés Sx^M des x^M avec $|M| = n$ forment une base de $\mathfrak{S}_n$, et $\pi\Psi(Sx^M) = \varphi\sigma(Sx^M) = \varphi\sigma(x^M) = \varphi(z^M)$, ce qui montre que les (Sx^M) forment une base de U_n/U_{n-1} , ce qui comme chacun sait (ou peut voir) entraîne bien l'isomorphisme annoncé.

COROLLAIRE 2 .- ρ est un isomorphisme de $\mathcal{G}$ sur $\mathcal{G}$.

COROLLAIRE 3 .- Si $\mathcal{G}'$ est une sous-algèbre de $\mathcal{G}$, $U(\mathcal{G}')$ se plonge dans $U(\mathcal{G})$. Si $\mathcal{G}'$ a une sous-algèbre $\mathcal{G}''$ supplémentaire dans $\mathcal{G}$, $U(\mathcal{G})$ s'identifie comme espace vectoriel (mais pas comme algèbre!) à $U(\mathcal{G}') \otimes U(\mathcal{G}'')$.

COROLLAIRE 4 .- Tout élément inversible de $U(\mathcal{G})$ est un scalaire.

COROLLAIRE 5 .- L'algèbre $U(\mathcal{G})$ n'a pas de diviseurs de 0 .

COROLLAIRE 6 .- L'algèbre $U(\mathcal{G})$ n'a pas de radical (au sens de Jacobson, i.e. il n'existe pas de $x \neq 0$ dans U annulé pour tout U-module simple) .

COROLLAIRE 7 .- Si $\mathcal{G}$ est de dimension finie, tout idéal à gauche dans $U(\mathcal{G})$ a une base finie.

4.- Il reste à démontrer les lemmes.

Démonstration du lemme 1 .- Soit (b_ν) une base de $\mathcal{H}$; prolongeons-la grâce aux (a_μ) en une base de $\mathcal{G}$, et ordonnons le tout de façon que les μ précédent les ν . Alors $\underline{x}^M = \underline{a}^P \underline{b}^Q$ avec $P = (p_\mu)$, $Q = (q_\nu)$. D'après l'exemple 4 du n°2, $U(\mathcal{G}/\mathcal{H}) = U(\mathcal{G})/\mathcal{R}$ où $\mathcal{R}$ est sous-tendu par les $\underline{x}^M \underline{b}_\nu = \underline{a}^P \underline{b}^Q \underline{b}_\nu$; mais $\underline{b}^Q \underline{b}_\nu = \sum_\iota \underline{b}^{Q'_\iota}$ puisque les $\underline{b}^Q$ sous-tendent $U(\mathcal{H})$. Bref $\mathcal{R}$ est sous-tendu par les $\underline{a}^P \underline{b}^Q$ avec $Q \neq \emptyset$. Si le théorème 1' est vrai pour $\mathcal{G}$, les $\underline{x}^M$ sont linéairement indépendants ; a fortiori les $\underline{a}^P \underline{b}^\emptyset = \underline{a}^P$ sont linéairement indépendants mod. $\mathcal{R}$. Les a_μ formant une base de $\mathcal{G}/\mathcal{H}$, les $\underline{a}^P$ engendrent $U(\mathcal{G}/\mathcal{H}) = U(\mathcal{G})/\mathcal{R}$ dont ils forment donc une base.

Démonstration du lemme 2 .- Il s'agit de voir que si les $\underline{x}_\iota$ sont linéairement indépendants, il en est de même des $\underline{x}^M$.

Or l'application $x \longrightarrow \underline{x} \otimes 1 + 1 \otimes \underline{x}$ est une linéarisation de $\mathcal{G}$ dans $U \otimes U$, donc définit un homomorphisme H de U dans $U \otimes U$. On a :

$$H(\underline{x}^m) = (\underline{x} \otimes 1 + 1 \otimes \underline{x})^m = \sum_{p+q=m} \binom{m}{p} \underline{x}^p \otimes \underline{x}^q \quad ,$$

car $\underline{x} \otimes 1$ et $1 \otimes \underline{x}$ commutent. En posant :

$$\binom{M}{P} = \prod_{\iota \in I} \binom{m_\iota}{p_\iota}$$

on obtient :

$$(1) : t^M = (\underline{x}^M) - 1 \otimes \underline{x}^M - \underline{x}^M \otimes 1 = \sum \binom{M}{P} \underline{x}^P \otimes \underline{x}^Q \qquad (P+Q=M \ ; \ P,Q \neq \emptyset) \ .$$

La démonstration procède par récurrence sur $|M|$; par hypothèse, les $\underline{x}^N$ sont linéairement indépendants si $|N| = 1$; supposons-les linéairement indépendants pour $|N| \leq m$, et $|M| \leq m+1$. Alors les $y^{P,Q} = \underline{x}^P \otimes \underline{x}^Q$ intervenant dans l'expression de t^M sont linéairement indépendants dans $U_m \otimes U_m$. Les t^M ne sont pas nuls si $m > 1$ (corps de caractéristique 0 !) , et si $M \neq M'$ $(m > 1)$ t^M et $t^{M'}$ ne font pas intervenir les mêmes $y^{P,Q}$ car dans t^M interviennent les

$y^{P,Q}$ avec $P + Q = M$ et dans $t^{M'}$ les $y^{P,Q}$ avec $P + Q = M' \neq M$: ils sont donc linéairement indépendants.

Supposons alors qu'il y ait une relation linéaire $\sum a_M \underline{x}^M = 0$ entre les $\underline{x}^M$. On en déduit :

$$\sum a_M t^M = \sum a_M H(\underline{x}^M) - 1 \otimes \sum a_M \underline{x}^M - \sum a_M \underline{x}^M \otimes 1$$

ceci implique donc $a_M = 0$ sauf si $|M| = 1$. Mais alors $\underline{x}^M = x_\iota$ et on a supposé les $\underline{x}_\iota$ linéairement indépendants ; donc tous les a_M sont nuls et les $\underline{x}^M$ sont linéairement indépendants.

Démonstration du lemme 3 .- Soient a_ι les générateurs de $\mathcal{G}$, b_ι ceux de $U(\mathcal{G}) = L$ (cf. exemple 2 du paragraphe 2), L' l'ensemble des éléments de L sans terme constant. Soit P l'application linéaire de L' dans $\mathcal{G}$ définie par:

$$P(b_{\iota_1} \dots b_{\iota_n}) = [a_{\iota_1} \dots [a_{\iota_{n-1}}, a_{\iota_n}]] \dots]$$

Soit θ l'homomorphisme de l'algèbre associative libre L dans l'algèbre associative des endomorphismes de l'espace vectoriel $\mathcal{G}$ définie par : $\theta(1) = 1$; $\theta(b_\iota) = \mathrm{ad}(a_\iota)$.

Il est immédiat que si $u \in L$, $v \in L'$: $P(uv) = \theta(u) P(v)$.

D'autre part $(\theta(\rho[x,y])) = \theta(\rho(x)\rho(y) - \rho(y)\rho(x))$

$= \theta(\rho(x))\theta(\rho(y)) - \theta(\rho(y))\theta(\rho(x))$ comme par ailleurs $\mathrm{ad}[x\ y] = \mathrm{adx}\ \mathrm{ady} - \mathrm{ady}\ \mathrm{adx}$ les x tels que $\theta(\rho(x)) = \mathrm{adx}$ forment une algèbre de Lie qui contient les a_ι donc est égale à $\mathcal{G}$ et $\theta(\rho(x)) = \mathrm{adx}$ $(x \in \mathcal{G})$.

Par suite :

$$P(\rho([x,y])) = P(\rho(x)\rho(y) - \rho(y)\rho(x))$$
$$= \theta(\rho(x))\, P(\rho(y)) - \theta(\rho(y))\, P(\rho(x)) .$$

Soit, en posant $Q = P \circ \rho$,

$$Q([x,y]) = \mathrm{ad}\, x\, Q(y) - \mathrm{ad}\, y\, Q(x) = [x, Q(y)] + [Q(x), y] .$$

Autrement dit Q est une dérivation de $\mathcal{G}$. Comme elle coïncide avec l'identité sur les générateurs de $\mathcal{G}$, Q est la dérivation qui multiplie un élément de $\mathcal{G}$ de degré q (par rapport aux a_ι) par q , et comme l'anneau de base est un corps de caractéristique 0 , Q est biunivoque. A fortiori ρ aussi.

Remarques.

1) Le théorème de Birkhoff-Witt est valable sous la forme 1' chaque fois que $\mathcal{G}$

possède une base sur l'anneau K . Sous la forme 1 , Lazard a démontré qu'il est vrai en tout cas si K est un anneau principal. D'une manière générale les hypothèses à faire concernant la structure additive exclusivement. Chirchoff a montré par contre qu'il est des cas où le théorème est faux.

2) On verra dans un exposé ultérieur comment déduire la formule de Campbell-Hausdorff des lemmes 2 et 3 .

3) Il résulte de la démonstration du lemme 2 que $t^M = 0$ implique $|M| = 1$, donc que les $\underline{x} \in \mathcal{J}$ sont caractérisés par $H(\underline{x}) = 1 \otimes \underline{x} + \underline{x} \otimes 1$.