Séminaire "Sophus Lie"

P. Cartier

Exemples d'hyperalgèbres

Séminaire "Sophus Lie", tome 2 (1955-1956), exp. n° 3, p. 1-15
<http://www.numdam.org/item?id=SSL_1955-1956__2__A5_0>

Faculté des Sciences de Paris
-:-:-:-

Séminaire "Sophus LIE"
Année 1955/1956
-:-:-:-

Exposé n° 3

EXEMPLES D'HYPERALGÈBRES

(Exposé de P. CARTIER, le 3.2.56)

1.- Rappels sur les algèbres de Lie.

Rappelons qu'une algèbre de Lie sur un anneau K est une algèbre non associative $\mathfrak{g}$ sur K qui vérifie les identités génériques :

(1) $\qquad [x , x] = 0 \qquad [x ,[y , z]] + [y ,[z , x]] + [z ,[x , y]] = 0$

Un exemple quasi-universel d'algèbre de Lie est le suivant : si A est une algèbre associative et $\mathfrak{g}$ un sous-module de A qui contient $ab - ba$ avec a et b, on posera : $[a , b] = ab - ba$.

L'algèbre enveloppante universelle de $\mathfrak{g}$ est le quotient de l'algèbre tensorielle $T(\mathfrak{g})$ du module $\mathfrak{g}$ par l'idéal bilatère J engendré par les éléments $u(x , y) = x \otimes y - y \otimes x - [x , y]$, $(x , y \in \mathfrak{g})$ on la notera $U(\mathfrak{g})$; si $x \in \mathfrak{g}$, la classe de x modulo J sera notée $i(x)$ d'où la relation :

(2) $\qquad i([x , y]) = i(x)\, i(y) - i(y)\, i(x)$

de plus pour toute application linéaire f de $\mathfrak{g}$ dans une algèbre associative A telle que $f([x , y]) = f(x)\, f(y) - f(y)\, f(x)$, il existe un homomorphisme f' et un seul de l'algèbre $U(\mathfrak{g})$ dans A tel que $f = f' \circ i$.

Si f est un homomorphisme de l'algèbre de Lie $\mathfrak{g}$ dans l'algèbre de Lie $\mathfrak{h}$, on peut alors définir un homomorphisme $U(f)$ de $U(\mathfrak{g})$ dans $U(\mathfrak{h})$ par la condition $U(f)(i(x)) = i(f(x))$ pour $x \in \mathfrak{g}$; on a $U(f \circ g) = U(f) \circ U(g)$ et $U(I) = I$ (I étant l'identité). Si $\mathfrak{g}_i$ $(i = 1, 2)$ sont deux algèbres de Lie et si f_i désigne l'injection de $\mathfrak{g}_i$ dans $\mathfrak{g}_1 \times \mathfrak{g}_2$, on définit un homomorphisme h de $U(\mathfrak{g}_1) \otimes U(\mathfrak{g}_2)$ dans $U(\mathfrak{g}_1 \times \mathfrak{g}_2)$ par la condition

(3) $\qquad h(a_1 \otimes a_2) = U(f_1)(a_1)\, U(f_2)(a_2) \qquad a_i \in U(\mathfrak{g}_i)$

mais si l'on définit $h' : U(\mathfrak{g}_1 \times \mathfrak{g}_2) \longrightarrow U(\mathfrak{g}_1) \otimes U(\mathfrak{g}_2)$ par $h'(i(x_1 , x_2)) = i(x_1) \otimes 1 + 1 \otimes i(x_2)$ $(x_i \in \mathfrak{g}_i)$, on vérifie facilement que h et h' sont des isomorphismes réciproques par lesquels on identifie $U(\mathfrak{g}_1 \times \mathfrak{g}_2)$ à $U(\mathfrak{g}_1) \otimes U(\mathfrak{g}_2)$.

On introduit comme d'habitude une filtration croissante dans $U(\mathfrak{g})$ compatible avec la structure d'algèbre en appelant $U_n(\mathfrak{g})$ le sous-module de $U(\mathfrak{g})$ engendré par les produits de $m \leq n$ éléments $i(x_i) \in \mathfrak{g}$. Il est alors clair que dans l'identification de $U(\mathfrak{g} \times \mathfrak{h})$ à $U(\mathfrak{g}) \otimes U(\mathfrak{h})$, $U_n(\mathfrak{g} \times \mathfrak{h})$ s'identifie à $\sum_{m=0}^{n} U_m(\mathfrak{g}) \otimes U_{n-m}(\mathfrak{h})$. Par ailleurs la formule (2) montre que les classes $\pi(x) = i(x) \bmod U_0(\mathfrak{g})$ commutent deux à deux dans l'algèbre graduée G associée à l'algèbre filtrée $U(\mathfrak{g})$. Il en résulte que l'application $x \longrightarrow \pi(x)$ se prolonge en un homomorphisme de l'algèbre symétrique $S(\mathfrak{g})$ dans G . On a alors le théorème fondamental suivant :

Théorème 1 (Poincaré-Witt) : Si l'algèbre de Lie $\mathfrak{g}$ admet une base sur l'anneau K , l'homomorphisme canonique de $S(\mathfrak{g})$ dans G est bijectif.

Corollaire 1 : l'application $x \longrightarrow i(x)$ de $\mathfrak{g}$ dans $U(\mathfrak{g})$ est injective si $\mathfrak{g}$ est un module libre.

Corollaire 2 : si $\mathfrak{g}$ est une algèbre de Lie sur un corps K de caractéristique 0 , $T(\mathfrak{g})$ est somme directe de l'idéal J et du sous-espace des tenseurs symétriques.

Cela résulte de ce que le sous-espace des tenseurs symétriques est supplémentaire dans $T(\mathfrak{g})$ de l'idéal I engendré par les tenseurs $x \otimes y - y \otimes x$, de ce que I est le noyau de l'application $T(\mathfrak{g}) \longrightarrow S(\mathfrak{g})$ et de techniques usuelles de filtration.

Du théorème 1, on déduit facilement que si $\mathfrak{g}$ a une base $\{x_i\}$ totalement ordonnée, $U(\mathfrak{g})$ admet pour base les monômes $\prod_i x_i^{\alpha_i}$ et que $U_n(\mathfrak{g})$ admet pour base les monômes $\prod_i x_i^{\alpha_i}$ avec $|\alpha| = \sum_i \alpha_i \leq n$. Si K est un corps de caractéristique 0 , $U(\mathfrak{g})$ admet aussi pour base les monômes $Z_\alpha = \prod_i x_i^{\alpha_i}/\alpha_i !$ pour $\alpha = (\alpha_i) \in \mathbb{N}^{(I)}$ (monoïde abélien libre construit sur I).

2.- p-algèbres de Lie.

Rappelons qu'on appelle alternant une expression constituée en itérant l'opération de crochet, par exemple : $[x , [[y , z] , [t , x]]]$ i.e , un monôme non associatif en des variables x , y , ... pour une opération notée $[.,.]$.

Proposition 1 (Jacobson) : Il existe une somme $\Lambda_p(x , y)$ bien déterminée d'alternants en des variables x et y , telle que dans tout anneau de caractéristique p , où l'on pose $[x , y] = xy - yx$, on ait l'identité :

$$(x + y)^p = x^p + y^p + \Lambda_p(x , y) \tag{4}$$

Dans toute algèbre associative A , on posera $G_x y = xy = D_y x$ et $\operatorname{ad} x.y = xy - yx$; on a alors $G_x D_z = D_z G_x$ et $\operatorname{ad} x = G_x - D_x$, d'où par la formule du binôme :

$$(5) \qquad (G_x - D_x)^n = (\operatorname{ad} x)^n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} G_x^i D_x^{n-i}$$

Si A est de caractéristique p , on déduit de cette formule et des congruences $\binom{p}{i} \equiv 0 \bmod p$ pour $1 \leq i \leq p-1$ et $\binom{p-1}{i} \equiv (-1)^i \bmod p$ pour $0 \leq i \leq p-1$ que l'on a :

$$(6) \qquad (\operatorname{ad} x)^p . y = (G_x^p - D_x^p).y = x^p y - y x^p = (\operatorname{ad} x^p).y$$

$$(7) \qquad (\operatorname{ad} x)^{p-1} . y = \sum_{i=0}^{p-1} G_x^i D_x^{p-1-i} . y = \sum_{i=0}^{p-1} x^i y x^{p-1-i}$$

Ceci dit, nous allons considérer des polynomes à coefficients entiers modulo p en des variables x , y , ... qui ne commutent pas entre elles. Nous poserons $f_k(x_1 , \ldots , x_k) = \sum_{\sigma} x_{\sigma(1)} \cdots x_{\sigma(k)}$, la sommation étant étendue à toutes les permutations σ des k premiers entiers ; f_k n'est autre que la somme des termes multilinéaires de $(x_1 + \ldots + x_k)^k$. De même, on appellera $g_{i,j}(x , y)$ la somme des monômes distincts de degré (i , j) en (x , y) , i.e la composante de degré (i , j) de $(x + y)^{i+j}$. Le nombre des permutations σ de l'intervalle $[1 , k]$ compatibles avec la partition $[1 , k] = [1 , i] \cup [i + 1 , k]$ étant égal à $i ! (k - i) !$, on voit que si l'on remplace $x_1 , \ldots , x_i$ par x et $x_{i+1} , \ldots , x_k$ par y dans f_k on trouve $i ! (k - i) ! \; g_{i,k-i}(x , y)$.

Or l'identité (7) où l'on fait $x = x_1 + \ldots x_{p-1}$ et $y = x_p$ et où l'on ne considère que les termes multilinéaires donne :

$$(8) \qquad f_{p-1}(\operatorname{ad} x_1 , \ldots , \operatorname{ad} x_{p-1}).x_p = f_p(x_1 , \ldots , x_p)$$

car au second membre de (7) y prend chaque place une fois et une seule. Faisant $x_1 = \ldots = x_i = x$ et $x_{i+1} = \ldots = x_p = y$, on en déduit :

$$(9) \qquad g_{i,p-1-i}(\operatorname{ad} x , \operatorname{ad} y) - y = (p - i) \, g_{i,p-i}(x , y) \qquad 0 < i < p$$

d'où résulte la formule (4) si l'on tient compte de :

$$(10) \qquad (x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} g_{i,p-i}(x , y)$$

Les formules (9) et (10) donnent même une formule explicite pour $\Lambda_p(x , y)$.

C.Q.F.D.

Nous pouvons maintenant définir les p-algèbres de Lie.

Définition 1 : on appelle p-algèbre de Lie $\mathfrak{g}$ sur un anneau K de caractéristique p, la donnée d'une algèbre de Lie $\mathfrak{g}$ et d'une application $x \to x^{\underline{p}}$ de $\mathfrak{g}$ dans elle-même dite p-application qui vérifie les axiomes :

a) $\operatorname{ad} x^{\underline{p}} = (\operatorname{ad} x)^p$ pour tout $x \in \mathfrak{g}$

b) $(\lambda x)^{\underline{p}} = \lambda^p x^{\underline{p}}$ pour tous $x \in \mathfrak{g}$, $\lambda \in K$

c) $(x + y)^{\underline{p}} = x^{\underline{p}} + y^{\underline{p}} + \Lambda_p(x, y)$ pour tous $x, y \in \mathfrak{g}$

Exemple : un sous-module d'une algèbre associative stable pour les opérations $[x, y] = xy - yx$ et $x^{\underline{p}} = x^p$

Soit $x \to x^{[p]}$ une seconde p-application définie dans $\mathfrak{g}$ et $f(x) = x^{\underline{p}} - x^{[p]}$. Les formules a) à c) montrent alors que $f(x)$ est dans le centre de $\mathfrak{g}$ pour tout $x \in \mathfrak{g}$, et que $f(\lambda x) = \lambda^p f(x)$, $f(x + y) = f(x) + f(y)$ et que réciproquement si $f(x)$ vérifie ces conditions $x^{\underline{p}} + f(x)$ est une p-application ; Donc, l'ensemble des applications vérifiant les axiomes a) à c) est donné par $x \to x^{\underline{p}} + f(x)$ où f est une application semi-linéaire (par rapport à $\lambda \to \lambda^p$) de $\mathfrak{g}$ dans son centre.

Proposition 2 : Soit $\mathfrak{g}$ une algèbre de Lie sur l'anneau K de caractéristique p, que l'on peut identifier à un sous-module de $U(\mathfrak{g})$. Pour qu'une application $x \to x^{\underline{p}}$ de $\mathfrak{g}$ dans $\mathfrak{g}$ vérifie les axiomes a), b), c) précédents, il faut et il suffit que l'application $x \to \rho(x) = x^p - x^{\underline{p}}$ soit une application semi-linéaire de $\mathfrak{g}$ dans le centre de $U(\mathfrak{g})$.

Compte tenu de la formule (6) et de $[x, y] = xy - yx$ pour $x, y \in \mathfrak{g} \subset U(\mathfrak{g})$ on voit que a) équivaut à $\rho(x)\, y = y\, \rho(x)$ pour $x, y \in \mathfrak{g}$, donc au fait que $\rho(x)$ appartient au centre de $U(\mathfrak{g})$ qui est l'algèbre engendrée par $\mathfrak{g}$. De même comme $(\lambda x)^p = \lambda^p x^p$, b) équivaut à $\rho(\lambda x) = \lambda^p \rho(x)$. Enfin d'après la formule (4) appliquée à l'anneau $U(\mathfrak{g})$, on a $\Lambda_p(x, y) = (x + y)^p - x^p - y^p$, donc c) équivaut à la condition $\rho(x + y) = \rho(x) + \rho(y)$.

Corollaire : soit $\mathfrak{g}$ une algèbre de Lie sur l'anneau K de caractéristique p ayant une base $\{x_i\}$. Pour que $\mathfrak{g}$ puisse être munie d'une structure de p-algèbre de Lie, il faut et il suffit que pour tout i, il existe $b_i \in \mathfrak{g}$ avec $(\operatorname{ad} x_i)^p = \operatorname{ad} b_i$. La condition $x_i^{\underline{p}} = b_i$ détermine alors entièrement $x^{\underline{p}}$ pour tout $x \in \mathfrak{g}$.

On peut identifier $\mathfrak{g}$ à un sous-module de $U(\mathfrak{g})$ d'après le corollaire du théorème 1.

Posons alors $\rho(\sum_i \lambda_i x_i) = \sum_i \lambda_i^p (x_i^p - b_i)$; comme on a $(\operatorname{ad} x_i)^p = \operatorname{ad} b_i$ la formule (6) montre que $\rho(x)$ est dans le centre de $U(\mathfrak{g})$. Comme par ailleurs, il est clair que $\rho(x)$ dépend semi-linéairement de x et comme la proposition 1 montre que $(\sum_i \lambda_i x_i)^p - \sum_i \lambda_i^p x_i^p \in \mathfrak{g}$, il en résulte que $x^{\underline{p}} = x^p - \rho(x) \in \mathfrak{g}$ et que $x \to x^{\underline{p}}$ est l'unique application vérifiant les axiomes a) à c) telle que $x_i^{\underline{p}} = b_i$.

Nous allons maintenant introduire la notion d'algèbre enveloppante restreinte d'une p-algèbre de Lie $\mathfrak{g}$: cette algèbre notée $\tilde{U}(\mathfrak{g})$ est le quotient de $U(\mathfrak{g})$ par l'idéal bilatère J_p engendré par les éléments $i(x)^p - x^{\underline{p}}$ ou encore le quotient de l'algèbre tensorielle $T(\mathfrak{g})$ par l'idéal bilatère engendré par les tenseurs $x \otimes y - y \otimes x - [x , y]$ et $x^{\otimes p} - x^{\underline{p}}$ (où l'on désigne par $x^{\otimes m}$ la puissance m^e de x dans $T(\mathfrak{g})$) ; on notera $\tilde{i}(x)$ l'image de $x \in \mathfrak{g} \subset T(\mathfrak{g})$ dans $\tilde{U}(\mathfrak{g})$; on a donc

$$\tilde{i}([x , y]) = \tilde{i}(x)\,\tilde{i}(y) - \tilde{i}(y)\,\tilde{i}(x) \quad \tilde{i}(x^{\underline{p}}) = \tilde{i}(x)^p \quad x,y \in \mathfrak{g} \tag{11}$$

Réciproquement si f est une application linéaire de la p-algèbre de Lie $\mathfrak{g}$ dans une algèbre associative A vérifiant les conditions $f([x , y]) = f(x)\,f(y) - f(y)\,f(x)$ et $f(x^{\underline{p}}) = f(x)^p$, il existe un homomorphisme f' et un seul de $\tilde{U}(\mathfrak{g})$ dans A tel que $f = f' \circ \tilde{i}$. Comme dans le cas des algèbres de Lie usuelles (cf. paragraphe 1) on en déduit la définition de $\tilde{U}(f)$: $\tilde{U}(\mathfrak{g}) \longrightarrow \tilde{U}(\mathfrak{h})$ pour un homomorphisme f de $\mathfrak{g}$ dans $\mathfrak{h}$ tel que $f(x^{\underline{p}}) = f(x)^{\underline{p}}$ ($\mathfrak{g}$ et $\mathfrak{h}$ étant deux p-algèbres de Lie) et de même si l'on définit sur le produit $\mathfrak{g}_1 \times \mathfrak{g}_2$ de deux p-algèbres une p-application par $(x_1 , x_2)^{\underline{p}} = (x_1^{\underline{p}} , x_2^{\underline{p}})$, on a un isomorphisme "naturel" de $\tilde{U}(\mathfrak{g}_1 \times \mathfrak{g}_2)$ sur $\tilde{U}(\mathfrak{g}_1) \otimes \tilde{U}(\mathfrak{g}_2)$.

Enfin, on introduit une filtration croissante dans $\tilde{U}(\mathfrak{g})$ en appelant $\tilde{U}_n(\mathfrak{g})$ l'image de $U_n(\mathfrak{g})$ par l'homomorphisme canonique de $U(\mathfrak{g})$ sur $\tilde{U}(\mathfrak{g})$; cette filtration a les mêmes propriétés que celle de $U(\mathfrak{g})$.

Ceci dit, en nous appuyant sur le théorème 1, nous allons démontrer un théorème analogue pour les p-algèbres de Lie.

Théorème 2 : Si $\mathfrak{g}$ est une p-algèbre admettant une base $\{x_i\}_{i \in I}$ (que nous ordonnerons totalement), l'application $\tilde{i}$ est injective, et si l'on identifie $x \in \mathfrak{g}$ et $\tilde{i}(x) \in \tilde{U}(\mathfrak{g})$, les monômes $\prod_i x_i^{\alpha_i}$ $(0 \leq \alpha_i < p)$ forment une base de $\tilde{U}(\mathfrak{g})$.

Soit $\alpha = (\alpha_i) \in \mathbb{N}^{(I)}$ un indice composé ; posons $\alpha_i = \beta_i + p\gamma_i$ avec $0 \leq \beta_i < p$ et dans $U(\mathfrak{g}) = U$ définissons l'élément $T_\alpha = \prod_i x_i^{\beta_i} \rho(x_i)^{\gamma_i}$ avec les notations de la proposition 2. Si $|\alpha| = \sum_i \alpha_i = n$, il est clair que $T_\alpha \equiv \prod_i x_i^{\alpha_i} \bmod U_{n-1}$, donc comme par le théorème 1, les monômes $\prod_i x_i^{\alpha_i}$ avec $|\alpha| = n$ forment une base de $U_n \bmod U_{n-1}$, il en résulte que les T_α avec $|\alpha| = n$ forment une base de $U_n \bmod U_{n-1}$, et par suite que $U(\mathfrak{g})$ admet les T_α pour base. Or l'idéal J engendré par les $\rho(x)$ est aussi engendré par les $\rho(x_i)$ et ces éléments sont centraux, d'où résulte que J' admet pour base les T_α avec $\gamma = (\gamma_i) \neq 0$ et finalement que les T_α avec $\gamma = 0$ i.e $0 \leq \alpha_i < p$ forment une base de U modulo J', d'où le théorème.

Remarque : de la démonstration résulte que $\tilde{U}_n(\mathfrak{g})$ admet pour base les monômes $\prod_i x_i^{\alpha_i}$ avec $|\alpha| \leq n$ et $0 \leq \alpha_i < p$. Mais si $\alpha_i < p$, $1/\alpha_i!$ existe puisque K est un anneau de caractéristique p, et $\hat{U}(\mathfrak{g})$ admet aussi pour base les monômes $Z_\alpha = \prod_i x_i^{\alpha_i}/\alpha_i!$ avec $0 \leq \alpha_i < p$.

Nous allons terminer ce paragraphe en montrant comment on ramène l'étude des algèbres de Lie sur un anneau de caractéristique p à celle des p-algèbres de Lie.

Proposition 3 : Soit $\mathfrak{g}$ une algèbre de Lie sur un anneau K de caractéristique p ayant une base ; le sous-module $\tilde{\mathfrak{g}}$ de $U(\mathfrak{g})$ engendré par les x^{p^h} $(x \in \mathfrak{g}, h \in \mathbb{N})$ est une p-algèbre de Lie pour la p-application $x \longrightarrow x^p$, et l'application identique de $\tilde{\mathfrak{g}}$ dans $U(\mathfrak{g})$ se prolonge en un isomorphisme de $\tilde{U}(\tilde{\mathfrak{g}})$ sur $U(\mathfrak{g})$.

La formule (6) montre que $\operatorname{ad} x^{p^h} = (\operatorname{ad} x)^{p^h}$, d'où $[x^{p^h}, y^{p^k}] = (\operatorname{ad} x)^{p^h-1}(-\operatorname{ad} y)^{p^k}.x$ pour $x, y \in \mathfrak{g}$, ce qui prouve que $\tilde{\mathfrak{g}}$ est stable pour le crochet ; par ailleurs, la formule de Jacobson (4), montre que l'ensemble des $x \in \hat{\mathfrak{g}}$ tels que $x^p \in \tilde{\mathfrak{g}}$ est un sous-module de $\tilde{\mathfrak{g}}$, donc est égal à $\hat{\mathfrak{g}}$ puisqu'il contient les x^{p^h} pour $x \in \mathfrak{g}$. Soit enfin $\{x_i\}$ une base de $\mathfrak{g}$; toujours par la formule (4) et le théorème 1, on voit que les $x_i^{p^h} = x_{h,i}$ forment une base de $\tilde{\mathfrak{g}}$; si on pose alors pour $\alpha = (\alpha_i)$ $\alpha_i = \sum_{h \geq 0} \alpha_{h,i} p^h$ $(0 \leq \alpha_{h,i} < p)$ et $T_\alpha = \prod_{h,i} x_{h,i}^{\alpha_{h,i}}/\alpha_{h,i}!$, T_α est congru à Z_α modulo des termes de filtration $< |\alpha|$ d'après le théorème 1, donc les T_α forment une base de $U(\mathfrak{g})$; si l'on compare $\{T_\alpha\}$ à la base de $\tilde{U}(\tilde{\mathfrak{g}})$ attachée à la base $\{x_{h,i}\}$ de $\tilde{\mathfrak{g}}$ (remarque suivant le théorème 2), on voit que l'application canonique de $\tilde{U}(\tilde{\mathfrak{g}})$ dans $U(\mathfrak{g})$ est bijective.

3.- Algèbres de puissances divisées.

Soit K un anneau commutatif (avec unité comme toujours) M un K-module unitaire ; suivant Cartan et d'autres, on définira l'algèbre commutative $\Gamma(M)$ des puissances divisées construite sur M de la manière suivante :

$\Gamma(M)$ est définie par les générateurs $m^{(h)}$ ($m \in M$; h entier $\geqslant 0$) et par les relations :

$$(12) \qquad (m + m')^{(h)} = \sum_{i+j=h} m^{(i)} m'^{(j)} \qquad m, m' \in M \quad \lambda \in K$$

$$(13) \qquad (\lambda m)^{(h)} = \lambda^h m^{(h)}$$

$$(14) \qquad m^{(h)} m^{(k)} = ((h, k)) m^{(h+k)} \qquad m^{(0)} = 1$$

entre ces générateurs. (On a posé pour abréger $((h, k)) = (h+k)!/h!k!$).

Si l'on attribue le degré h à $m^{(h)}$, les relations écrites sont isobares et il existe donc une graduation sur $\Gamma(M)$ compatible avec la structure d'algèbre pour laquelle $m^{(h)}$ est de degré h. Les seules relations entre les $m^{(1)}$ qui sont de degré 1 sont conséquence linéaire des suivantes :

$$(15) \qquad (m + m')^{(1)} = m^{(1)} + m'^{(1)} \qquad (\lambda m)^{(1)} = \lambda m^{(1)}$$

et on peut donc identifier par $m \to m^{(1)}$ M à l'ensemble $\Gamma_1(M)$ des éléments de degré 1 de $\Gamma(M)$.

De la formule (14), on tire $(h!\, m^{(h)})(k!\, m^{(k)}) = (h+k)!\, m^{(h+k)}$ d'où $h!\, m^{(h)} = m^h$; si K contient le corps des rationnels, on pourra poser $m^{(h)} = m^h/h!$ et les relations (12) et (13) seront conséquence de cette définition, ce qui prouve amplement que $\Gamma(M)$ n'est autre dans ce cas que l'algèbre symétrique $S(M)$ du module M ; en tout cas, le nom de "puissances divisées" est maintenant justifié.

Si f est une application linéaire de M dans N, il existe un homomorphisme de l'algèbre $\Gamma(M)$ dans $\Gamma(N)$ et un seul noté $\Gamma(f)$ qui envoie $m^{(h)}$ sur $(f(m))^{(h)}$; il est clair que $\Gamma(f \circ g) = \Gamma(f) \circ \Gamma(g)$ et $\Gamma(I) = I$ et $\Gamma(f)$ est compatible avec les graduations.

Proposition 4 : Si M est somme directe des sous-modules M_i, et si f_i est l'injection de M_i dans M, l'application $\varphi = \bigotimes_{(I)} \Gamma(f_i)$ de $\bigotimes_{(I)} \Gamma(M_i)$ dans $\Gamma(M)$ définit un isomorphisme de la première algèbre graduée sur la seconde.

Rappelons que $\bigotimes_{(I)} \Gamma(M_i)$ est le produit tensoriel infini (éventuellement) des algèbres $\Gamma(M_i)$ (Bourbaki, Alg. III , App. I) et que φ est défini par $\varphi(\bigotimes_i a_i) = \prod_i \Gamma(f_i)(a_i)$.

Introduisant la série formelle à une indéterminée T à coefficients dans $\Gamma(M)$, $e(m , T) = \sum_{h>0} m^{(h)} T^h$, les relations (12) à (14) prennent la forme équivalente.

(12') $\qquad e(m + m' , T) = e(m , T)\, e(m' , T)$

(13') $\qquad e(\lambda m , T) = e(m , \lambda T)$

(14') $\qquad e(m , T + T') = e(m , T)\, e(m , T') \qquad e(m , 0) = 1$

où T' est une nouvelle indéterminée indépendante de T .

Les m_i étant nuls sauf un nombre fini, la définition de φ s'écrit $\varphi(\bigotimes_i e(m_i , T)) = \prod_i e(m_i , T) = e(\sum_i m_i , T)$. Inversement, nous allons définir un homomorphisme Ψ de $\Gamma(M)$ dans $\bigotimes_{(I)} \Gamma(M_i)$ par la formule symbolique suivante $\Psi(e(m , T)) = \bigotimes_i e(m_i , T)$ si $m = \sum_i m_i \in M$ $(m_i \in M_i)$, formule qui signifie que $\Psi(m^{(h)}_i)$ n'est autre que le coefficient de T^h dans le second membre. Pour que Ψ soit bien défini, il faut et il suffit qu'on ait :

(12") $\qquad \Psi(e(m + m' , T)) = \Psi(e(m , T))\ \Psi(e(m' , T))$

(13") $\qquad \Psi(e(\lambda m , T)) = \Psi(e(m , \lambda T))$

(14") $\qquad \Psi(e(m , T + T')) = \Psi(e(m , T))\ \Psi(e(m , T'))$

identités dont la vérification est parfaitement triviale.

D'autre part, il est clair que $\Psi(\varphi(\bigotimes_i e(m_i , T))) = \bigotimes_i e(m_i , T)$ et $\varphi(\Psi(e(m , T)) = e(m , T)$ d'où comme les éléments en question engendrent les algèbres qui les contiennent, le fait que φ et Ψ sont des applications réciproques.

<u>Corollaire</u> : <u>si</u> M <u>admet une base</u> $\{e_i\}$, $\Gamma(M)$ <u>admet pour base les monômes</u> $Z_\alpha = \prod_i e_i^{(\alpha_i)}$ $(\alpha = (\alpha_i) \in \mathbb{N}^{(I)})$ <u>avec</u> $Z_\alpha\, Z_\beta = ((\alpha , \beta))\, Z_{\alpha+\beta}$ (on pose $((\alpha , \beta)) = \prod_i ((\alpha_i , \beta_i))$).

Posant $M_i = Ke_i$, on voit que $\Gamma(M)$ est isomorphe à $\bigotimes_{(I)} \Gamma(M_i)$, donc admet pour base le produit tensoriel des bases des $\Gamma(M_i)$, ce qui ramène immédiatement au cas où M a une base d'un élément e . Or dans ce cas on voit

tout de suite que les relations (12') à (14') sont conséquences des relations $e(\lambda e , T) = e(e , \lambda T)$ et $e(e , T)e(e , T') = e(e , T+T')$ i.e. $(\lambda e)^{(h)} = \lambda^h e^{(h)}$ et $e^{(h)}e^{(k)} = ((h , k))\, e^{(h+k)}$ ce qui prouve que $\Gamma(K.e)$ a pour base les $e^{(h)}$ avec la table de multiplication désirée.

Nous allons maintenant définir une algèbre **analogue** à $\Gamma(M)$. Si $T(M)$ est l'algèbre tensorielle de M , on fait agir le groupe symétrique $\mathfrak{S}_n$ sur $T^n(M) = \overset{n}{\otimes} M$ par $\sigma(\overset{n}{\underset{i=1}{\otimes}} m_i) = \overset{n}{\underset{i=1}{\otimes}} m_{\sigma^{-1}(i)}$ d'où $\sigma(\tau(x)) = (\sigma\tau)(x)$ pour $x \in T^n(M)$ et on dénote par $TS^n(M)$ l'ensemble des $x \in T^n(M)$ tels que $\sigma(x) = x$ pour $\sigma \in \mathfrak{S}_n$. Nous noterons $H_{n_1,\dots,n_k}$ le sous-groupe de $\mathfrak{S}_n$ $(n = n_1 + \dots + n_k)$ défini par les conditions $n_r < \sigma(i) \leq n_{r+1}$ pour $n_r < i \leq n_{r+1}$ $(1 \leq r < k)$.

Soient $x \in TS^m(M)$, $y \in TS^n(M)$ et $x \otimes y \in T^{m+n}(M)$; comme $x \otimes y$ est invariant par les $\sigma \in H_{m,n}$, $\sigma(x \otimes y)$ ne dépend que de la classe $\sigma H_{m,n}$ et on peut former $x * y = \sum_{\sigma \in \mathfrak{S}_n / H_{m,n}} \sigma(x \otimes y)$. On définit ainsi sur $TS(M) = \sum_{n \geq 0} TS^n(M)$ par linéarité une multiplication associative et commutative. comme on le voit facilement.

Proposition 5 : Il existe un homomorphisme k et un seul de $\Gamma(M)$ dans $TS(M)$ qui envoie $m^{(h)}$ sur $m^{\otimes h} \in TS^h(M)$; k est bijectif si M est libre.

Il suffit évidemment de vérifier que k est compatible avec les relations entre les $m^{(h)}$: si $m = m_1 + m_2$, on a $m^{\otimes h} = \sum_f \overset{h}{\underset{i=1}{\otimes}} m_{f(i)}$ où la somme est étendue à toutes les applications f de $[1 , h]$ dans $[1 , 2]$; or les monômes de cette somme pour lesquels 2 intervient i fois et j intervient j fois $(i + j = h)$ sont tous les monômes $\sigma(m_1^{\otimes i} \otimes m_2^{\otimes j})$ formellement distincts donc la somme de ces monômes vaut $m_1^{\otimes i} * m_2^{\otimes j}$ et par suite $k((m_1 + m_2)^{(h)}) = (m_1 + m_2)^{\otimes h} = \sum_{i+j=h} m_1^{\otimes i} * m_2^{\otimes j} = \sum_{i+j=h} k(m_1^{(i)}) * k(m_2^{(j)})$. La formule $k(\lambda m)^{(h)}) = \lambda^h k(m^{(h)})$ est évidente. Enfin $m^{\otimes h} * m^{\otimes k} = [\mathfrak{S}_{h+k} : H_{h,k}]\, m^{\otimes h+k} = ((h , k))\, m^{\otimes h+k}$ d'où la compatibilité de k avec la dernière relation.

Si M admet une base e_i , $T^n(M)$ admet pour base les monômes $e_S = e_{i_1} \otimes \dots \otimes e_{i_n}$ pour les suites $S = \{i_1 , \dots , i_n\}$, et pour que $x = \sum_S x(S) e_S$ soit invariant par $\mathfrak{S}_n$, il faut et il suffit que $x(i_1 , \dots , i_n) = x(i_{\sigma(1)} , \dots , i_{\sigma(n)})$ pour tout σ . Ceci prouve que

$TS^n(M)$ admet pour base les éléments T_α somme des e_S pour lesquels il y a α_i indices dans S égaux à i. Si on appelle $i_1, \dots, i_p$ les indices distincts pour lesquels $\alpha_i \neq 0$, on a $T_\alpha = \sum \sigma(e_{i_1}^{\otimes \alpha_{i_1}} \otimes \dots \otimes e_{i_p}^{\otimes \alpha_{i_p}}) = \underset{i}{*} e_i^{\alpha_i}$.

Il en résulte que $\underline{k}$ applique la base Z_α de $\Gamma(M)$ biunivoquement sur la base T_α de $TS(M)$ et par suite $\underline{k}$ est bijectif.

Nous allons terminer ce paragraphe en élucidant la structure des algèbres $\Gamma(M)$ lorsque K est un corps.

Théorème 3 : Soit M un espace vectoriel sur un corps K ;

a) si K est de caractéristique 0, $\Gamma(M)$ est canoniquement isomorphe à l'algèbre symétrique $S(M)$

b) si K est de caractéristique $p \neq 0$, et si M admet une base $\{m_i\}$, $\Gamma(M)$ est engendrée par les éléments $X_{h,i} = m_i^{(p^h)}$ et l'idéal des relations algébriques entre les $X_{h,i}$ est engendré par les relations $X_{h,i}^p = 0$ (M) admet pour base les monômes $X_\alpha = \prod_{h,i}^{\alpha_{h,i}} / \alpha_{h,i}!$ pour $\alpha_i = \sum_h \alpha_{h,i}\, p^h$ $(0 \leq \alpha_{h,i} < p)$.

Le a) a été démontré dans les remarques suivant la définition de $\Gamma(M)$. Pour démontrer le b), on prouve d'abord un lemme arithmétique :

Lemme : si a, b, c sont des entiers et p un nombre premier tels que $0 \leq a < p^k$, $0 \leq b < p$, $0 \leq c \leq p$, on a les congruences modulo p :

$$((a\ ,\ bp^k)) \equiv 1 \tag{16}$$

$$(c/p^k) = (cp^k)!/c!\,(p^k!)^c \equiv 1 \tag{17}$$

Les congruences étant prises modulo p on a :

$$(x+y)^{a+bp^k} \equiv (x+y)^a (x^{p^k} + y^{p^k})^b = \sum_{\substack{0 \leq a' \leq a \\ 0 \leq b' \leq b}} y^{a'}\, x^{a-a'} \binom{a}{a'} x^{b'p^k}\, y^{(b-b')p^k} \binom{b}{b'} =$$

$$= \sum_{a',b'} \binom{a}{a'} \binom{b}{b'} x^{a+(b'p^k-a')}\, y^{bp^k-(b'p^k-a')}$$

où $a' \leq a < p^k$ et $b' \leq b < p$ donc $b'\,p^k - a' = 0$ équivaut à $a' = b' = 0$; le coefficient de $x^a y^{bp^k}$ vaut donc $((a\ ,\ bp^k))$ au premier membre et 1 dans le second d'où la congruence (16).

Désignant par Z_p l'anneau des fractions a/b avec b non divisible par p , on sait que $pZ_p \cap Z = pZ$. Or de $u \equiv v \bmod p$; on déduit $u^c \equiv v^c \bmod p$ pour $0 \leq c < p$ et $u^p \equiv v^p \bmod p^2$; de la congruence $(\sum x_i)^{p^k} \equiv \sum x_i^{p^k} \bmod p$ on déduit donc

$$(x_1 + \ldots + x_c)^{cp^k}/c! \equiv (x_1^{p^k} + \ldots + x_c^{p^k})^c/c! \quad \bmod pZ_p$$

La congruence (17) se déduit de ceci en comparant les coefficients de $(x_1 \ldots x_c)^{p^k}$ dans les deux membres, en utilisant le fait que le premier membre de (17) est entier et l'égalité $pZ_p \cap Z = pZ$.

Ce lemme étant démontré, soit $a = \sum \lambda_k p^k$ un entier ≥ 0 $(0 \leq \lambda_k < p)$ et m un élément de M ; nous poserons $m_k = m^{(p^k)}$ et $a_k = \sum_{h<k} \lambda_h p^h$. La relation (14) montre alors que l'on a :

$$\begin{aligned}
\prod_{k\geq 0} (m_k)^{\lambda_k}/\lambda_k! &= m^{(a)}\ (\textstyle\sum \lambda_k p^k)!\ /\ \prod_{k\geq 0} \lambda_k!\,(p^k!)^{\lambda_k} \\
&= m^{(a)}\, a!\ \prod_{k\geq 0} (\lambda_k | p^k)/(\lambda_k p^k)! \\
&= m^{(a)}\ \prod_{k\geq 0} \{a_{k+1}!/a_k!\,(\lambda_k p^k)!\}\ (\lambda_k | p^k) \\
&= m^{(a)}\ \prod_{k\geq 0} ((a_k\ ,\ \lambda_k p^k))\ (\lambda_k | p^k)
\end{aligned}$$

et de plus :

$$(m_k)^p = m_{k+1}\ (p^{k+1})!/(p^k!)^p = p!\ (p|p^k)\ m_{k+1}\ .$$

Ces formules et le lemme montrent que si K est un anneau de caractéristique p on a $Z_\alpha = X_\alpha$ et $X_{h,i}^p = 0$.

L'assertion sur la base de $\Gamma(M)$ résulte alors de ce qui précède et du corollaire de la proposition 4. Enfin, le fait que les relations entre les $X_{h,i}$ soient conséquence des relations $X_{h,i}^p = 0$ résulte de ce que modulo ces relations, tout polynome en les $X_{h,i}$ est congru à un polynome de degré $< p$ en chaque variable, et le fait que les X_α forment une base de $\Gamma(M)$.

4.- Définition d'hyperalgèbres.

Soit $\mathfrak{g}$ une algèbre de Lie, $U(\mathfrak{g})$ son algèbre enveloppante ; on a identifié $U(\mathfrak{g} \times \mathfrak{g})$ à $U(\mathfrak{g}) \otimes U(\mathfrak{g})$ au paragraphe 1, et par suite si δ est l'homomorphisme $x \to (x\ ,\ x)$ de $\mathfrak{g}$ dans $\mathfrak{g} \times \mathfrak{g}$, $U(\delta) = \Delta$ est un homomorphisme de $U(\mathfrak{g})$ dans $U(\mathfrak{g}) \otimes U(\mathfrak{g})$. De plus si on identifie $U(0)$ à K , l'application $\eta : x \to 0$ de $\mathfrak{g}$ dans (0) définit un homomorphisme $\varepsilon = U(\eta)$ de $U(\mathfrak{g})$ sur K , i.e. une augmentation. Enfin, on a défini une

filtration sur $U(\mathfrak{g})$ au paragraphe 1 . Nous allons voir que $U(\mathfrak{g})$ muni de l'application Δ et de l'augmentation ε vérifie les axiomes des hyperalgèbres:

a) $(\Delta \otimes I) \circ \Delta = (U(\delta) \otimes U(I)) \circ U(\delta) = U((\delta \times I) \circ \delta) = U(\delta')$. Or $\delta'(x) = (x, x, x)$ et un calcul analogue montre que $(I \otimes \Delta) \circ \Delta = U(\delta')$ d'où l'associativité de Δ . Si S est la symétrie $a \otimes b \longrightarrow b \otimes a$ de $U(\mathfrak{g}) \otimes U(\mathfrak{g})$ on a $U(\sigma) = S$ avec $\sigma(x, y) = (y, x)$ et par suite $\sigma \circ \delta = \delta$ et $S \circ \Delta = \Delta$ ce qui prouve que Δ est symétrique.

b) $(\varepsilon \otimes I) \circ \Delta = U((\eta \times I) \circ \delta) = U(\eta')$; or $\eta'(x) = (\eta \times I)(x, x) = 0 + x = x$, et on voit alors que $(I \otimes \varepsilon) \circ \Delta = U(\eta') = I$

c) on a $\varepsilon(1) = 1$ et $\Delta(1) = 1 \otimes 1$

d) enfin la filtration est compatible avec la structure d'algèbre et aussi avec Δ par la formule $U_n(\mathfrak{g} \times \mathfrak{g}) = \sum_{m=0}^{n} U_m(\mathfrak{g}) \otimes U_{n-m}(\mathfrak{g})$.

A l'aide des "foncteurs" $\tilde{U}(\mathfrak{g})$ pour les p-algèbres de Lie et $\Gamma(M)$, on définit de la même manière des hyperalgèbres et la vérification des axiomes est parfaitement analogue. $\Gamma(M)$ est même une hyperalgèbre graduée au sens de l'exposé 2 .

Faisant l'hypothèse que les modules qui interviennent ont des bases, nous allons déterminer la filtration canonique de ces hyperalgèbres et la structure de l'algèbre duale. Nous nous appuyerons pour cela sur le lemme suivant :

Lemme 2 : Soit A une coalgèbre ayant pour base des éléments Z_α tels que $\Delta(Z_\alpha) = \sum_{\beta+\gamma=\alpha} Z_\beta \otimes Z_\gamma$ pour $\alpha = (\alpha_i) \in N^{(I)}$ et $0 \leq \alpha_i < \lambda_i$, λ_i étant fini ou non ; l'algèbre duale de A est isomorphe au quotient de l'algèbre des séries formelles $K[[X_i]]$ par l'idéal engendré par les $X_i^{\lambda_i}$ et le module A_n de la filtration canonique a pour base les Z_α avec $|\alpha| \leq n$.

Définissons P_α par la formule $\langle Z_\alpha , P_\beta \rangle = \delta_{\alpha\beta}$; toute forme linéaire sur A s'écrit alors d'une manière et d'une seule sous la forme de la série simplement convergente $\sum_\alpha c(\alpha) P_\alpha$. De plus, on a :

$$(18)\quad \langle Z_\alpha , P_\beta P_\gamma \rangle = \langle \Delta(Z_\alpha), P_\beta \otimes P_\gamma \rangle = \sum_{\alpha=\beta'+\gamma'} \langle Z_{\beta'} \otimes Z_{\gamma'} , P_\beta \otimes P_\gamma \rangle =$$

$$= \sum_{\alpha=\beta'+\gamma'} \delta_{\beta\beta'} \delta_{\gamma\gamma'} = \delta_{\alpha, \beta+\gamma}$$

donc $P_\beta P_\gamma = P_{\beta+\gamma}$ à condition de poser $P_\alpha = 0$ si l'un des α_i est $\geq \lambda_i$.

Si l'on pose $X_i = P_{\xi_i}$, on a alors immédiatement $P_\alpha = \prod_i x_i^{\alpha_i}$ pour $\alpha_i < \lambda_i$ et il faut négliger tous les monômes de degré $\geqslant \lambda_i$ en X_i pour au moins un i, ce qui montre bien que A' est isomorphe à $K[[X_i]]/(X_i^{\lambda_i})$.

P_0 étant élément unité de A' il en résulte que $\varepsilon(Z_\alpha) = \delta_{\alpha 0}$, donc que A^+ a pour base les Z_α avec $\alpha \neq 0$ de plus $\varepsilon(Z_0) = 1$ et $\Delta(Z_0) = Z_0 \otimes Z_0$ donc Z_0 est élément unité de A ; supposons alors démontré que pour $n = 0, 1, \ldots, k$ A_n^+ a pour base les Z_α avec $\alpha \neq 0$ et $|\alpha| \leqslant n$ et soit $x = \sum x(\alpha) Z_\alpha$ un élément de A. On a :

$$\Delta(x) - x \otimes Z_0 - Z_0 \otimes x = \sum_{\beta,\gamma \neq 0} x(\beta+\gamma) Z_\beta \otimes Z_\gamma \tag{19}$$

donc pour que $x \in A_{k+1}^+$, il faut et il suffit que l'on ait $x(\beta+\gamma) = 0$ pour $\beta, \gamma \neq 0$ et $|\beta + \gamma| > k+1$; comme l'assertion sur A_0^+ est triviale, on a donc $k > 0$ et comme tout indice α avec $|\alpha| \geqslant 2$ s'écrit $\alpha = \beta\ \gamma$ avec $\beta, \gamma \neq 0$, on en conclut que l'appartenance de x à A_{k+1}^+ équivaut à $x(\alpha) = 0$ pour $|\alpha| > k+1$, donc A_{k+1}^+ admet pour base les Z_α avec $|\alpha| \leqslant k+1$.

Soit alors K un anneau contenant le corps des rationnels et $\mathcal{G}$ une algèbre de Lie sur K ayant une base $\{x_i\}$. On a vu au paragraphe 1 que $U(\mathcal{G})$ admet pour base les éléments $Z_\alpha = \prod_i x_i^{\alpha_i}/\alpha_i!$ pour tous les $\alpha \in \mathbb{N}^{(I)}$, et le théorème 2 montre que si $\mathcal{G}$ est une p-algèbre de Lie sur un anneau K de caractéristique p, ayant une base $\{x_i\}$, les Z_α définis de la même manière que précédemment pour $0 \leqslant \alpha_i < p$ forment une base de $\tilde{U}(\mathcal{G})$. Or la définition de Δ montre que l'on a $\Delta(x) = x \otimes 1 + 1 \otimes x$ pour $x \in \mathcal{G}$, donc comme Δ est multiplicative $\Delta(x^m/m!) = \sum_{i+j=m} x^i/i! \otimes x^j/j!$ si ceci a un sens et donc immédiatement $\Delta(Z_\alpha) = \sum_{\beta+\gamma=\alpha} Z_\beta \otimes Z_\gamma$. On en déduit alors :

Proposition 6 : Si $\mathcal{G}$ est une algèbre de Lie sur un anneau contenant les nombres rationnels (resp. une p-algèbre de Lie sur un anneau K de caractéristique p) ayant une base, la filtration canonique sur l'hyperalgèbre $U(\mathcal{G})$ (resp. $\tilde{U}(\mathcal{G})$) est la filtration $U_n(\mathcal{G})$ (resp. $\tilde{U}_n(\mathcal{G})$) et en particulier $\mathcal{G}$ est l'ensemble des éléments primitifs de $U(\mathcal{G})$ (resp. $\tilde{U}(\mathcal{G})$). L'algèbre duale de $U(\mathcal{G})$ est isomorphe à l'algèbre des séries formelles en des variables X_i (resp. les séries formelles en les X_i mod X_i^p) en correspondance biunivoque avec les éléments d'une base de $\mathcal{G}$.

Corollaire : Si $\mathcal{G}$ est une algèbre de Lie ayant une base sur l'anneau K de caractéristique p , la sous-algèbre de Lie sous-tendue par les x^{p^h} pour $x \in \mathcal{G}$ et h entier ≥ 0 , est l'ensemble des éléments primitifs de $U(\mathcal{G})$.

Etudions maintenant le cas de l'algèbre $\Gamma(M)$; explicitant Δ , on voit que $\Delta(m^{(h)}) = \sum_{i+j=h} m^{(i)} \otimes m^{(j)}$. Si M admet les e_i pour base, $\Gamma(M)$ admet les $Z_\alpha = \prod_i e_i^{(\alpha_i)}$ pour base et de ce qui précède et du fait que Δ est multiplicative, on déduit que $\Delta(Z_\alpha) = \sum_{\beta+\gamma=\alpha} Z_\beta \otimes Z_\gamma$; mais ici on peut expliciter l'application diagonale Δ' dans le dual F de $\Gamma(M)$. En effet définissant les P_α par $\langle Z_\alpha , P_\beta \rangle = \delta_{\alpha\beta}$, on a

$$(20) \quad \langle Z_\beta \otimes Z_\gamma , \Delta'(P_\alpha) \rangle = \langle Z_\beta Z_\gamma , P_\alpha \rangle = ((\beta,\gamma)) \langle Z_{\beta+\gamma} , P_\alpha \rangle = ((\beta,\gamma)) \delta_{\alpha,\beta+\gamma}$$

d'où $\Delta'(P_\alpha) = \sum_{\beta+\gamma=\alpha} ((\beta,\gamma)) P_\beta \otimes P_\gamma$ en particulier $\Delta'(X_i) = X_i \otimes 1 + 1 \otimes X_i$

On en déduit la proposition :

Proposition 7 : Si M est un module sur l'anneau K ayant une base $\{e_i\}$, l'algèbre duale de l'hyperalgèbre $\Gamma(M)$ est isomorphe à l'algèbre des séries formelles en des variables X_i $(i \in I)$ et l'application diagonale Δ' du dual de $\Gamma(M)$ est définie par $\Delta'(X_i) = X_i \otimes 1 + 1 \otimes X_i$.

Autrement dit, " $\Gamma(M)$ est l'hyperalgèbre du groupe additif de M , défini par $\varphi_i(\underline{X} , \underline{Y}) = X_i + Y_i$ " (on peut donner un sens intrinsèque à cette affirmation à l'aide de la notion de "fonction analytique dans un module").

Remarque : on étudiera de plus près l'hyperalgèbre $U(\mathcal{G})$ d'une algèbre de Lie sur un corps de caractéristique 0 et on déterminera le groupe formel strict correspondant à l'exposé 6).

5.- Algèbres de Lie des hyperalgèbres.

Nous allons appliquer les résultats du paragraphe 4 à une première étude de la structure d'une hyperalgèbre quelconque. Des résultats plus précis ne pourront pas être obtenus avant les exposés 6,7,8.

Lemme 3 : Soit U une hyperalgèbre sur un anneau K (resp. de caractéristique p). Les éléments primitifs de U constituent une algèbre de Lie pour le crochet $[x , y] = xy - yx$ (resp. une p-algèbre de Lie avec $x^{\underline{p}} = x^p$).

Si x et y sont primitifs, on a $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\Delta(y) = y \otimes 1 + 1 \otimes y$, d'où $\Delta(xy) = xy \otimes 1 + 1 \otimes xy + x \otimes y + y \otimes x$ et par suite $\Delta([x , y]) = [x , y] \otimes 1 + 1 \otimes [x , y]$ et $[x , y]$ est bien primitif. Si K est de caractéristique p , comme $x \otimes 1$ et $1 \otimes x$ commutent, on a :

$$\Delta(x^p) = (x \otimes 1 + 1 \otimes x)^p = 1 \otimes x^p + x^p \otimes 1$$ et x^p est primitif.

Proposition 8 : Soient U une hyperalgèbre sur un corps K et $\mathcal{g}$ l'algèbre de Lie des éléments primitifs de U (resp. la p-algèbre de Lie si K est de caractéristique $p \neq 0$). L'injection canonique de $\mathcal{g}$ dans U se prolonge en un monomorphisme d'hyperalgèbres de $U(\mathcal{g})$ (resp. $\hat{U}(\mathcal{g})$) dans U .

D'après ce qu'on a vu dans la définition de $U(\mathcal{g})$ et de $\hat{U}(\mathcal{g})$, il existe un homomorphisme d'algèbres f de $U(\mathcal{g})$ (resp. $\hat{U}(\mathcal{g})$) dans U prolongeant l'injection de $\mathcal{g}$ dans U ; cet homomorphisme est compatible avec les applications diagonales car $(f \otimes f) \circ \Delta$ et $\Delta \circ f$ prennent la même valeur $f(x) \otimes 1 + 1 \otimes f(x)$ sur les $x \in \mathcal{g}$, donc sont égaux puisque ce sont des homomorphismes d'algèbres et que $\mathcal{g}$ engendre $U(\mathcal{g})$ (resp. $\hat{U}(\mathcal{g})$) . Pour démontrer la compatibilité avec l'augmentation de f , il suffit de remarquer que si $x \in U$ est primitif, on a $\varepsilon(x) = 0$:

$$x = (\varepsilon \otimes I)(\Delta(x)) = \varepsilon(x) + x \tag{21}$$

Enfin le fait que f soit injectif résulte d'un résultat de l'exposé 2.