BULLETIN DE LA S. M. F.

JEAN DIEUDONNÉ

Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. (V)

Bulletin de la S. M. F., tome 84 (1956), p. 207-239

<http://www.numdam.org/item?id=BSMF_1956__84__207_0>

Bull. Soc. math. France,
84, 1956, p. 207 à 239.

GROUPES DE LIE ET HYPERALGÈBRES DE LIE SUR UN CORPS DE CARACTÉRISTIQUE $p > 0$ (V);

PAR

M. JEAN DIEUDONNÉ.

1. Dans les articles précédents de cette série ([7], [8], [9]), consacrés aux groupes formels *abéliens*, la notion d'hyperalgèbre de Lie *libre* (abélienne) a joué un rôle prépondérant; c'est grâce à elle que nous avons pu donner une description complète des groupes formels abéliens et de leurs homomorphismes dans [9]. La structure d'*algèbre* de cette hyperalgèbre libre est effectivement une structure d'algèbre (abélienne) libre, c'est-à-dire une algèbre de polynômes. D'autre part, la théorie classique (en caractéristique o) associe aussi les notions d'algèbre de Lie libre et d'algèbre associative libre (algèbre des polynômes non commutatifs); essentiellement, l'algèbre enveloppante d'une algèbre de Lie libre est une algèbre de polynômes non commutatifs. Il y avait donc lieu de penser qu'il existe une notion analogue d'hyperalgèbre *libre* pour les groupes formels non abéliens; c'est à la définition et à la démonstration d'existence d'une telle hyperalgèbre et de ses propriétés « universelles » qu'est consacrée la plus grande partie de ce travail; comme on pouvait s'y attendre, on montre que la structure d'algèbre d'une telle hyperalgèbre est bien celle d'une algèbre de polynômes non commutatifs (ou algèbre tensorielle). Comme dans le cas classique, cette hyperalgèbre libre a « le moins possible » de générateurs, étant adaptée aux groupes formels à loi *canonique*; mais en ajoutant des « degrés de liberté » supplémentaires, on obtient une autre hyperalgèbre libre, d'utilisation plus souple (th. 3), à laquelle on peut rattacher les propriétés formelles de types variés d'opérateurs (n° 17). Enfin, il se trouve que c'est des relations entre ces deux types d'hyperalgèbre libre que l'on peut, par une méthode que nous croyons nouvelle, dériver la plus importante des formules « universelles » de la théorie de Lie, la *formule de Hausdorff*, dont nous obtenons ainsi l'analogue pour les groupes formels en caractéristique $p > 0$ (n^{os} 18-21).

2. Commençons par rappeler rapidement les relations entre les notions d'hyperalgèbre et de groupe formel, sous leur forme la plus générale (*cf.* [8], n° 4); comme me l'a fait observer P. CARTIER, la manière la plus sugges-

tive dont on puisse présenter cette théorie consiste à faire usage du langage de la *dualité* en algèbre linéaire.

Soit K un corps commutatif de caractéristique $p > 0$ (1), et soit I un ensemble arbitraire ; par $\mathbf{N}^{(I)}$ on désignera l'ensemble de toutes les familles $\alpha = (\alpha_i)_{i \in I}$ d'entiers $\geqq 0$, nuls sauf un nombre fini d'entre eux ; cet ensemble est *ordonné* de la façon habituelle, la relation $(\alpha_i) \leqq (\beta_i)$ signifiant que $\alpha_i \leqq \beta_i$ pour tout $i \in I$; on écrit 0 pour la famille (α_i) dont tous les termes sont nuls, on pose $\alpha + \beta = (\alpha_i + \beta_i)_{i \in I}$ et $\alpha - \beta = (\alpha_i - \beta_i)_{i \in I}$ si $\alpha \geqq \beta$. La *hauteur* $h(\alpha)$ est le plus petit entier r tel que $\alpha_i \leqq p^{r+1}$ pour tout $i \in I$; le *degré* $d(\alpha)$ est la somme $\sum_i \alpha_i$. Une *hyperalgèbre* sur K correspondant à l'ensemble d'indices I est une algèbre (associative) $\mathfrak{G}$ sur K munie d'une base (dite *structurale*) (Z_α) ayant $\mathbf{N}^{(I)}$ pour ensemble d'indices, telle que : 1° $Z_0 = I$ est l'élément unité, et les Z_α d'indice $\neq 0$ forment la base d'un idéal bilatère de $\mathfrak{G}$; 2° pour tout $r \geqq 0$, les Z_α de hauteur $h(\alpha) \leqq r$ forment la base d'une sous-algèbre $\mathfrak{s}_r$ de $\mathfrak{G}$ (2) ; 3° si, dans $\mathfrak{G} \otimes \mathfrak{G}$, on pose, pour tout α,

$$(1) \qquad Z_\alpha^0 = \sum_{0 \leqq \beta \leqq \alpha} Z_\beta \otimes Z_{\alpha - \beta}$$

les Z_α^0 forment une base d'une sous-algèbre $\mathfrak{G}^0$ de $\mathfrak{G} \otimes \mathfrak{G}$ (d'ailleurs nécessairement isomorphe à $\mathfrak{G}$ par $Z_\alpha \to Z_\alpha^0$).

En tant qu'espace vectoriel, $\mathfrak{G}$ est isomorphe à $K^{(\mathbf{N}^{(I)})}$, et a donc pour dual le produit $K^{\mathbf{N}^{(I)}}$, que nous noterons $\mathfrak{o}$ [ou $\mathfrak{o}(K)$] ; soient x^α ($\alpha \in \mathbf{N}^{(I)}$) les formes coordonnées sur $\mathfrak{G}$, de sorte que $\langle Z_\alpha, x^\beta \rangle = \delta_{\alpha\beta}$ (indice de Kronecker). Le dual de $\mathfrak{G} \otimes \mathfrak{G}$ est, en tant qu'espace vectoriel, $K^{\mathbf{N}^{(I)} \times \mathbf{N}^{(I)}}$, et les formes coordonnées (correspondant à la base formée des $Z_\alpha \otimes Z_\beta$) sont les produits tensoriels $x^\alpha \otimes x^\beta$; par abus de langage, on notera ce dual $\mathfrak{o} \otimes \mathfrak{o}$ (en fait, si $\mathfrak{o}'$ est l'espace vectoriel ayant pour base les x^α, le dual de $\mathfrak{G} \otimes \mathfrak{G}$ est le complété de $\mathfrak{o}' \otimes \mathfrak{o}'$ pour la topologie faible correspondante). Considérons alors l'application linéaire M de $\mathfrak{G}$ dans $\mathfrak{G} \otimes \mathfrak{G}$ (dite *structurale*), telle que $M(Z_\alpha) = Z_\alpha^0$; on vérifie immédiatement que sa transposée ${}^tM$ est une application linéaire continue (pour la topologie faible) de $\mathfrak{o} \otimes \mathfrak{o}$ dans $\mathfrak{o}$, telle que ${}^tM(x^\alpha \otimes x^\beta) = x^{\alpha+\beta}$. Soit ε_i l'élément de $\mathbf{N}^{(I)}$ dont la coordonnée d'indice i est 1, les autres 0, et posons $x_i = x^{\varepsilon_i}$; l'application bilinéaire $(f, g) \to {}^tM(f \otimes g)$ définit sur $\mathfrak{o}$ une structure d'algèbre (par rapport à K), et ce qui précède

(1) On peut développer une théorie analogue sur un corps de caractéristique 0, en supprimant, dans ce qui suit, tous les passages où intervient le nombre p (ce qu'on peut exprimer, en termes plus imagés, en disant qu'on « fait tendre p vers $+\infty$ ») ; l'hyperalgèbre $\mathfrak{G}$ est alors l'*algèbre enveloppante* de l'algèbre de Lie libre sur les $X_{0i} = Z_{\varepsilon_i}$ (*voir* plus loin n° 5 et n° 18).

(2) En fait, on peut montrer que cette condition est conséquence des deux autres [*voir* p. 211, note (3)].

montre que l'algèbre $\mathfrak{a}$ ainsi définie est l'algèbre des *séries formelles* à coefficients dans K, par rapport aux $x_i (i \in I)$; on écrira donc tout élément $f = (a_\alpha) \in \mathfrak{a}$ sous la forme habituelle $f = \sum_\alpha a_\alpha x^\alpha$, et l'on a $x^\alpha = \prod_{i \in I} x_i^{\alpha_i}$.

Considérons maintenant la multiplication $(U, V) \to UV$ dans l'algèbre $\mathfrak{G}$; elle définit une application linéaire $C : U \otimes V \to UV$ de $\mathfrak{G} \otimes \mathfrak{G}$ dans $\mathfrak{G}$; sa transposée ${}^tC$ est une application linéaire de $\mathfrak{a}$ dans $\mathfrak{a} \otimes \mathfrak{a}$; si la table de multiplication dans $\mathfrak{G}$ est

$$Z_\alpha Z_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma \tag{2}$$

[$d_{\alpha\beta\gamma} \in K$, nuls (pour α et β donnés) sauf pour un nombre fini d'indices γ], on a

$${}^tC(x^\gamma) = \sum_{\alpha,\beta} d_{\alpha\beta\gamma} (x^\alpha \otimes x^\beta).$$

Mais on peut identifier $\mathfrak{a} \otimes \mathfrak{a}$ à l'algèbre des séries formelles par rapport aux x_i et à un nouveau système d'indéterminées y_i $(i \in I)$, $x^\alpha \otimes x^\beta$ étant identifié à $x^\alpha y^\beta$; pour toute série formelle $f \in \mathfrak{a}$, ${}^tC(f)$ est donc une série formelle en les x_i et y_i. On vérifie alors aussitôt que le fait que M soit un homomorphisme de l'algèbre $\mathfrak{G}$ dans l'algèbre $\mathfrak{G} \otimes \mathfrak{G}$ a pour conséquence, par transposition, la relation ${}^tC(fg) = {}^tC(f)\,{}^tC(g)$; autrement dit, si l'on pose

$$\varphi_i(\mathbf{x}, \mathbf{y}) = {}^tC(x_i) = \sum_{\alpha,\beta} d_{\alpha\beta\varepsilon_i} x^\alpha y^\beta \tag{3}$$

[où $\mathbf{x}$, $\mathbf{y}$ désignent les systèmes d'indéterminées (x_i), (y_i)], ${}^tC(x^\gamma)$ est égal à la série formelle obtenue en remplaçant chacun des x_i par $\varphi_i(\mathbf{x}, \mathbf{y})$ dans $\prod_i x_i^{\gamma_i}$. Le fait que Z_0 est élément unité de $\mathfrak{G}$ et que les Z_α pour $\alpha \neq 0$ forment un idéal entraîne $d_{0\beta\gamma} = \delta_{\beta\gamma}$, $d_{\alpha 0\gamma} = \delta_{\alpha\gamma}$ et $d_{\alpha\beta 0} = 0$ sauf si $\alpha = \beta = 0$; on en conclut que

$$\varphi_i(\mathbf{x}, \mathbf{y}) = x_i + y_i - \psi_i(\mathbf{x}, \mathbf{y}),$$

où dans ψ_i tous les monômes contiennent au moins un x_j et au moins un y_j. En outre, l'associativité de la multiplication dans $\mathfrak{G}$ donne, par transposition, la relation

$$\varphi(\varphi(\mathbf{x}, \mathbf{y}), \mathbf{z}) = \varphi(\mathbf{x}, \varphi(\mathbf{y}, \mathbf{z}))$$

[où $\varphi = (\varphi_i)$ et $\mathbf{z} = (z_i)$, troisième système d'indéterminées]. Les φ_i définissent donc un *groupe formel* correspondant à l'ensemble d'indices I.

Comme ${}^tC$ est un homorphisme de $\mathfrak{a}$ dans $\mathfrak{a} \otimes \mathfrak{a}$, on a

$${}^tC(x^{p\gamma}) = {}^tC((x^\gamma)^p) = ({}^tC(x^\gamma))^p = \left(\sum_{\alpha,\beta} d_{\alpha\beta\gamma} x^\alpha y^\beta\right)^p = \sum_{\alpha,\beta} d^p_{\alpha\beta\gamma} x^{p\alpha} y^{p\beta},$$

autrement dit

$$(4)\qquad \begin{cases} d_{\alpha,\beta,p\gamma} = 0 & \text{si } \alpha \text{ ou } \beta \text{ n'est pas multiple de } p, \text{ et} \\ d_{p\alpha,p\beta,p\gamma} = d^{p}_{\alpha\beta\gamma}. \end{cases}$$

Soit alors $\mathfrak{G}^{(1)}$ l'hyperalgèbre obtenue en appliquant l'isomorphisme $\xi \to \xi^p$ aux constantes $d_{\alpha\beta\gamma}$ qui définissent la multiplication dans $\mathfrak{G}$; le groupe formel correspondant est défini par les séries

$$\varphi_i^{(1)}(\mathbf{x}, \mathbf{y}) = \sum_{\alpha,\beta} d^{p}_{\alpha\beta\varepsilon_i} x^{\alpha} y^{\beta}.$$

On peut encore exprimer les relations (4) en disant que l'application $\mathbf{p}'$ de $\mathfrak{G}$ dans $\mathfrak{G}^{(1)}$, semi-linéaire pour $\xi \to \xi^{p-1}$ et telle que

$$(5)\qquad \begin{cases} \mathbf{p}'(\mathrm{Z}_\alpha) = 0 & \text{si } \alpha \text{ n'est pas un multiple de } p, \\ \mathbf{p}'(\mathrm{Z}_{p\alpha}) = \mathrm{Z}^{(1)}_{\alpha} & \text{(élément d'indice } \alpha \text{ de la base structurale de } \mathfrak{G}^{(1)}) \end{cases}$$

est un homomorphisme d'anneaux (« homomorphisme de Frobenius »).

3. Montrons maintenant qu'on peut faire opérer $\mathfrak{G}$ dans $\mathfrak{o}$. d'une façon bien déterminée, de sorte que l'on ait

$$(6)\qquad \langle \mathrm{UV}, f\rangle = \langle \mathrm{U}, \mathrm{V}f\rangle$$

quels que soient U, V dans $\mathfrak{G}$ et f dans $\mathfrak{o}$. Il suffit, en effet, que cette relation soit vérifiée pour $\mathrm{U} = \mathrm{Z}_\gamma$, $\mathrm{V} = \mathrm{Z}_\alpha$ et $f = x^\beta$, et cela donne l'unique solution

$$(7)\qquad \mathrm{Z}_\alpha x^\beta = \sum_{\gamma} d_{\gamma\alpha\beta}\, x^{\gamma}.$$

Il en résulte que l'on peut écrire

$$(8)\qquad {}^{t}C(f) = \sum_{\alpha} y^{\alpha} \mathrm{Z}_\alpha f$$

et, par suite, la relation ${}^{t}C(fg) = {}^{t}C(f)\,{}^{t}C(g)$ donne les identités

$$(9)\qquad \mathrm{Z}_\alpha(fg) = \sum_{0 \leq \beta \leq \alpha} (\mathrm{Z}_\beta f)(\mathrm{Z}_{\alpha-\beta} g).$$

Soit $\mathfrak{o}_r$ ($r \geqq 0$) la sous-algèbre de $\mathfrak{o}$ formée des séries formelles par rapport aux $x_i^{p^r}$. Les formules (7) et (4) montrent que l'on a $\mathrm{Z}_\alpha f = 0$ pour $h(\alpha) < r$ et $f \in \mathfrak{o}_r$; on conclut alors de (9) que l'on a, pour $h(\alpha) < r$, $f \in \mathfrak{o}$ et $g \in \mathfrak{o}_r$,

$$\mathrm{Z}_\alpha(fg) = g\,\mathrm{Z}_\alpha(f),$$

autrement dit, Z_α est une *semi-dérivation spéciale* de hauteur r. Inversement,

soit $\Delta = \sum_{\alpha} c_\alpha Z_\alpha$ une semi-dérivation spéciale de hauteur r appartenant à $\mathfrak{G}$.

On a donc, pour $f \in \mathfrak{o}$ et $g \in \mathfrak{G}_r$, $\Delta(fg) = g\Delta(f)$, c'est-à-dire d'après (9),

$$\sum_{\alpha} c_\alpha \left(f Z_\alpha g + \sum_{0<\beta<\alpha} (Z_\beta f)(Z_{\alpha-\beta} g) \right) = 0.$$

Montrons que si $h(\alpha) \geqq r$, on a $c_\alpha = 0$. En effet, on peut écrire alors

$$x^\alpha = x^{p^r\beta} x^\gamma, \qquad \text{avec} \quad \beta \neq 0 \qquad \text{et} \qquad h(\gamma) < r;$$

remplaçons f par x^γ et g par $x^{p^r\beta}$ dans la relation précédente. En se rappelant que le terme constant de $Z_\alpha x^\beta$ est $\delta_{\alpha\beta}$, on voit que $c_\alpha = 0$ en égalant à zéro le terme constant du premier membre. Ainsi toute semi-dérivation spéciale de hauteur r appartenant à $\mathfrak{G}$ est dans la sous-algèbre (3) $\mathfrak{s}_{r-1}$. Le même raisonnement montre que, si l'on pose $X_{ri} = Z_{p^r\varepsilon_i}$, les X_{ri} sont des *semi-dérivations* de hauteur r, et que toute semi-dérivation de hauteur r appartenant à $\mathfrak{G}$ est combinaison linéaire des X_{ri} ($i \in I$) et d'éléments de $\mathfrak{s}_{r-1}$; ces semi-dérivations forment une *p-algèbre de Lie* $\mathfrak{g}_r$, dans laquelle $\mathfrak{s}_{r-1}$ est un *p-idéal* (4).

4. Nous dirons que la sous-algèbre $\mathfrak{s}_r (r \geqq 0)$ est le *bourgeon de hauteur r* de l'hyperalgèbre $\mathfrak{G}$. Il est immédiat que les Z_α pour $\alpha \in J_r^{(I)}$, où J_r est l'intervalle $0 \leqq q < p^r$, forment une base pour $\mathfrak{s}_r$, satisfaisant aux conditions 1°, 2° et 3° du n° 2 (à cela près que, dans la condition 2°, il faut remplacer r par t et la condition $r \geqq 0$ par $0 \leqq t \leqq r$). De façon générale, nous dirons qu'une algèbre munie d'une base satisfaisant à ces conditions est un *bourgeon d'hyperalgèbre de hauteur r* (sans préjuger de la question d'existence d'une hyperalgèbre dont l'algèbre donnée est le bourgeon). On peut développer, pour les bourgeons d'hyperalgèbres, une théorie parallèle à celle des n^{os} 2 et 3 : l'algèbre $\mathfrak{o}$ des séries formelles par rapport aux x_i est alors remplacée par son quotient $\mathfrak{o}/\mathfrak{u}_r$, où $\mathfrak{u}_r$ désigne l'idéal de $\mathfrak{o}$ engendré par les $x_i^{p^r} (i \in I)$; autrement dit, on calcule dans cette algèbre comme dans une algèbre de séries formelles, à cela près qu'on remplace par 0 tout monôme contenant un $x_i^{p^r}$.

Dans ce qui suit, nous aurons à nous occuper d'un cas particulier où l'on suppose attaché à chaque indice $i \in I$ un *poids* $\pi(i)$, entier > 0 tel qu'il n'y ait

(3) On notera que dans tout ce qui précède, on ne s'est pas servi du fait que $\mathfrak{s}_r$ est une sous-algèbre de $\mathfrak{G}$; ses éléments étant caractérisés comme les semi-dérivations spéciales de hauteur $r+1$ appartenant à $\mathfrak{G}$, on voit ainsi que la condition 2° du n° 2, introduite dans la définition des hyperalgèbres, est en fait *une conséquence des deux autres conditions* 1° et 3°.

(4) On aura soigneusement à distinguer, dans ce qui suit, la notion d'*algèbre de Lie* de celle de *p-algèbre de Lie* (« restricted Lie algebra characteristic p » de Jacobson), où, en plus du crochet, intervient une seconde opération $x \to x^p$.

qu'un nombre fini d'indices de poids inférieur à un entier donné ; pour tout $\alpha=(\alpha_i)\in\mathbf{N}^{(I)}$, on pose $\pi(\alpha)=\sum_i \alpha_i\pi(i)$, de sorte que $\pi(\alpha+\beta)=\pi(\alpha)+\pi(\beta)$.

Nous supposerons de plus que la loi de composition du bourgeon $\mathfrak{s}_r$ soit *isobare*, c'est-à-dire que $d_{\alpha\beta\gamma}=0$ sauf lorsque $\pi(\gamma)=\pi(\alpha)+\pi(\beta)$. Dans ces conditions, pour tout entier $m\geqq 0$, les Z_α dont l'indice est de poids $\pi(\alpha)>m$ forment la base d'un *idéal* bilatère $\mathfrak{v}_{r,m}$; soit $\mathfrak{t}_{r,m}$ l'algèbre quotient $\mathfrak{s}_r/\mathfrak{v}_{r,m}$; nous dirons que $\mathfrak{t}_{r,m}$ est le *bourgeon* $\mathfrak{s}_r$ *tronqué au poids m*. Si Z'_α désigne la classe mod $\mathfrak{v}_{r,m}$ de Z_α, les Z'_α tels que $h(\alpha)\leqq r$ et $\pi(\alpha)\leqq m$ forment une base de $\mathfrak{t}_{r,m}$, et cette base (qui est *finie*) satisfait encore aux conditions analogues ([5]) à celles qui définissent un bourgeon de hauteur r, auxquelles il faut ajouter l'hypothèse que la loi de composition est *isobare*, ce qui entraîne $Z'_\alpha Z'_\beta=0$ pour $\pi(\alpha)+\pi(\beta)>m$. Inversement, nous dirons qu'une algèbre ayant une base satisfaisant à ces conditions est un *bourgeon tronqué de type* (r, m) (ici encore, sans préjuger de la possibilité d'obtenir cette algèbre à partir d'un bourgeon $\mathfrak{s}_r$). Si l'on développe ici la théorie analogue à celle des n°s 2 et 3, on obtient pour algèbre « duale » l'algèbre $\mathfrak{a}_{r,m}$ quotient de l'algèbre des polynômes par rapport aux x_i, par l'idéal des monômes x^α tels que $h(\alpha)>r$ ou $\pi(\alpha)>m$; autrement dit, cette algèbre a pour base les x^α tels que $h(\alpha)\leqq r$ et $\pi(\alpha)\leqq m$, et l'on a $x^\alpha x^\beta=x^{\alpha+\beta}$ si $h(\alpha+\beta)\leqq r$ et $\pi(\alpha)+\pi(\beta)\leqq m$, $x^\alpha x^\beta=0$ dans le cas contraire. En outre, on a ici le résultat suivant, dont nous nous servirons ci-dessous : rangeons dans un ordre arbitraire les éléments X'_{hi} tels que $h\leqq r$ et $p^h\pi(i)\leqq m$; pour tout $\alpha=(\alpha_i)$ tel que $h(\alpha)\leqq r$ et $\pi(\alpha)\leqq m$, posons $\alpha_i=\sum_{h=0}^{\infty}\alpha_{hi}p^h$ (développement p-adique), et désignons par X'_α le produit des puissances $X'^{\alpha_{hi}}_{hi}$, pris dans l'ordre fixé. Alors, les X'_α ($h(\alpha)\leqq r$, $\pi(\alpha)\leqq m$) *forment une base* du bourgeon tronqué considéré ; la démonstration est la même que dans ([5], p. 92-96), aux changements évidents près qu'entraîne le remplacement de l'algèbre $\mathfrak{o}$ par l'algèbre $\mathfrak{a}_{r,m}$.

5. Rappelons maintenant comment on forme l'*algèbre de Lie libre* $\mathfrak{L}(E)$ et la *p-algèbre de Lie libre* $\mathfrak{L}_p(E)$ engendrées par un ensemble E, sur le corps K ; on supposera pour la commodité l'ensemble E écrit sous forme de famille $(U_j)_{j\in J}$, la représentation paramétrique étant biunivoque. Considérons l'ensemble des mots significatifs ([3], p. 51) formés avec les lettres U_j, de poids 0, et un signe c de poids 2, et soit $\mathfrak{M}(E)$ l'espace vectoriel sur K ayant pour base cet ensemble. Pour deux mots significatifs X', Y', $cX'Y'$ est encore un mot significatif ; muni de la loi de composition $(X', Y')\to cX'Y'$, $\mathfrak{M}(E)$

([5]) Dans la condition correspondant au 3° des conditions du n° 2, il faut toutefois remplacer l'algèbre $\mathfrak{G}\otimes\mathfrak{G}$, non par $\mathfrak{t}_{r,m}\otimes\mathfrak{t}_{r,m}$, mais par le quotient de cette dernière algèbre par l'idéal bilatère engendré par les $Z'_\alpha\otimes Z'_\beta$ tels que $\pi(\alpha)+\pi(\beta)>m$.

n'est autre que l'*algèbre non associative libre* engendrée par E. Le *degré* $d_j(X')$ d'un mot significatif par rapport à U_j est le nombre de fois que U_j figure dans ce mot; on a donc $d_j(cX'Y') = d_j(X') + d_j(Y')$. Considérons alors dans $\mathfrak{N}(E)$ l'idéal bilatère $\mathfrak{A}$ engendré par les éléments de la forme

$$cX'X', \quad cX'Y' + cY'X', \quad cX'cY'Z' + cY'cZ'X' + cZ'cX'Y',$$

où X', Y', Z' sont des mots significatifs quelconques. Il est immédiat que $\mathfrak{A}$ est un idéal *homogène* pour chacun des degrés d_j. L'algèbre quotient $\mathfrak{N}(E)/\mathfrak{A}$ est l'*algèbre de Lie libre* sur E, $\mathfrak{L}(E)$; les images des mots significatifs dans $\mathfrak{L}(E)$ sont appelés les *alternants* sur les U_j, et si X, Y sont les alternants images des mots X', Y', l'image de $cX'Y'$ se note [X, Y]. Pour tout $\lambda = (\lambda_j) \in \mathbf{N}^{(J)}$, soit $\mathfrak{N}_\lambda$ le sous-espace de $\mathfrak{N}(E)$ ayant pour base les mots X' tels que $d_j(X') = \lambda_j$ pour tout $j \in J$; $\mathfrak{L}(E)$ est somme directe des sous-espaces vectoriels $\mathfrak{L}_\lambda = \mathfrak{N}_\lambda/(\mathfrak{N}_\lambda \cap \mathfrak{A})$ puisque $\mathfrak{A}$ est homogène; on dit que les alternants appartenant à $\mathfrak{L}_\lambda$ sont de *degré* λ_j par rapport à U_j; en vertu du théorème d'échange, il existe une base de chaque $\mathfrak{L}_\lambda$ formée d'alternants; en particulier, on peut identifier la base de $\mathfrak{L}_{\varepsilon_j}$ (qui est de dimension 1) à U_j, et, pour $j \neq k$, la base de $\mathfrak{L}_{\varepsilon_j + \varepsilon_k}$ (qui est aussi de dimension 1) à $[U_j, U_k]$ [si l'on a $j < k$ pour un ordre total fixé (arbitrairement) sur J]. Pour toute algèbre de Lie $\mathfrak{g}$ sur K engendrée par une famille de générateurs $(V_j)_{j \in J}$, il existe un homomorphisme u et un seul de $\mathfrak{L}(E)$ sur $\mathfrak{g}$ tel que $u(U_j) = V_j$ pour tout $j \in J$.

En particulier, considérons l'*algèbre associative libre* $\mathfrak{T}(E)$ sur E (ayant pour base tous les produits $U_{j_1} U_{j_2} \dots U_{j_m}$); c'est une algèbre de Lie pour la loi $[X, Y] = XY - YX$. Il existe donc un homomorphisme de $\mathfrak{L}(E)$ sur la sous-algèbre de Lie $\mathfrak{L}'(E)$ de $\mathfrak{T}(E)$ engendrée par les U_j, qui applique chaque U_j sur lui-même, et l'on montre que cet homomorphisme est un *isomorphisme*, ce qui permet d'identifier $\mathfrak{L}(E)$ et $\mathfrak{L}'(E)$. Cela étant, choisissons une base $(T_\mu)_{\mu \in M}$ de $\mathfrak{L}(E)$ formée d'alternants, et un bon ordre sur l'ensemble M. Le *théorème de Birkhoff-Witt* affirme que les produits de la forme

$$T_{\mu_1}^{\nu_1} T_{\mu_2}^{\nu_2} \dots T_{\mu_m}^{\nu_m},$$

où $\mu_1 < \mu_2 < \dots < \mu_m$, et où les ν_i sont des entiers > 0 (m et les μ_i et ν_i arbitraires sous les conditions précédentes) forment une *base* de l'algèbre $\mathfrak{T}(E)$.

Notons maintenant que, puisque K est de caractéristique p, $\mathfrak{T}(E)$ est aussi une *p-algèbre de Lie* pour la loi $X \to X^p$; on a les formules

$$[X^p, Y] = \overbrace{[X, [X, [\dots, [X, Y]\dots]]]}^{p \text{ fois}}$$

et

$$(X+Y)^p = X^p + Y^p + \Lambda(X, Y),$$

où $\Lambda(X, Y)$ est une somme d'alternants bien déterminés par rapport à X et Y

(formules de Jacobson). Soit $\mathfrak{L}_p(E)$ la p-sous-algèbre de Lie de $\mathfrak{T}(E)$ engendrée par les U_j; c'est la *p-algèbre de Lie libre* sur E (6). Elle a pour base, d'après ce qui précède, les puissances $T_\mu^{p^h}(\mu \in \mathbf{M}, h \in \mathbf{N})$; posons $T_\mu^{p^h} = S_{\mu,h}$, et ordonnons le produit $R = M \times \mathbf{N}$ suivant l'ordre lexicographique; le théorème de Birkhoff-Witt s'exprime encore en disant que les produits

$$S_{\rho_1}^{\nu_1} S_{\rho_2}^{\nu_2} \dots S_{\rho_m}^{\nu_m}, \tag{10}$$

où $\rho_1 < \rho_2 < \dots < \rho_m$, et où cette fois les entiers ν_i sont tels que $0 \leq \nu_i \leq p-1$, forment une *base* de $\mathfrak{T}(E)$.

6. Nous allons appliquer ce qui précède au cas où E est réunion de n suites infinies (U_{hi}) $(h \in \mathbf{N}, 1 \leq i \leq n)$. Prenons une base formée d'alternants dans $\mathfrak{L}(E)$, de la façon suivante : considérons d'abord les sous-espaces $\mathfrak{L}_{\lambda_0}$ (n° 5) des alternants de degré > 0 par rapport à l'un au moins des $U_{0i}(1 \leq i \leq n)$, et prenons une base d'alternants dans chacun de ces sous-espaces. Si maintenant $\mathfrak{L}_\lambda$ est un sous-espace dont les alternants ne contiennent aucun U_{0i}, soit r le plus petit entier tel que le degré de ces alternants par rapport à un $U_{ri}(1 \leq i \leq n)$ au moins soit > 0; soit $\mathfrak{L}_{\lambda_0}$ le sous-espace des alternants dont le degré en U_{hi} est égal au degré des alternants de $\mathfrak{L}_\lambda$ par rapport à $U_{h+r,i}(h \in \mathbf{N}, 1 \leq i \leq n)$; il est clair qu'on obtient une base de $\mathfrak{L}_\lambda$ en remplaçant, dans les alternants qui forment une base de $\mathfrak{L}_{\lambda_0}$, chaque U_{hi} par $U_{h+r,i}$; nous désignerons par $T_{r,\mu}$ l'alternant de $\mathfrak{L}_\lambda$ ainsi obtenu à partir d'un alternant $T_{0,\mu}$ de la base de $\mathfrak{L}_{\lambda_0}$. Les éléments $T_{k,\mu}^{p^h}$ de $\mathfrak{T}(E)$ forment alors une base de la p-algèbre de Lie $\mathfrak{L}_p(E)$, où $h \in \mathbf{N}$, $k \in \mathbf{N}$ et μ parcourt un ensemble d'indices M tel que $(T_{0,\mu})_{\mu \in M}$ soit une base de la somme des sous-espaces $\mathfrak{L}_{\lambda_0}$; on peut supposer que M contient l'intervalle J : $1 \leq i \leq n$, et que pour $\mu = i$ dans cet intervalle, $T_{k,i} = U_{ki}$. Nous ordonnerons (pour fixer les idées) l'ensemble $\mathbf{N} \times M \times \mathbf{N}$ des triplets (k, μ, h) en prenant un bon ordre quelconque sur M et en prenant sur le produit l'ordre lexicographique.

Définissons maintenant un *poids* π pour tout monôme de $\mathfrak{T}(E)$ en prenant $\pi(U_{ki}) = p^k$, et $\pi(XY) = \pi(X) + \pi(Y)$. Il en résulte immédiatement que tous les alternants sur les U_{ki} sont *isobares*; il en est donc de même de tous les éléments de la base de $\mathfrak{L}_p(E)$ que nous venons de définir. Nous nous proposons de démontrer le théorème suivant :

THÉORÈME 1. — *Dans l'algèbre associative libre $\mathfrak{T}(E)$ sur le corps premier $\mathbf{F}_p$, il existe une base formée d'éléments isobares, pour laquelle $\mathfrak{T}(E)$ est une hyperalgèbre correspondant à l'ensemble d'indices $R = M \times \mathbf{N}$.*

7. Pour tout $\rho = (\mu, h) \in R$, posons $\pi(\rho) = p^h \pi(T_{0,\mu}) = \pi(T_{0,\mu}^{p^h})$, et

(6) On peut démontrer en effet que $\mathfrak{L}_p(E)$ possède, vis-à-vis des p-algèbres de Lie, la propriété « universelle » analogue à celle de $\mathfrak{L}(E)$ vis-à-vis des algèbres de Lie, que nous avons rappelée plus haut; mais nous n'aurons pas à faire usage de ce résultat.

pour $\alpha=(\alpha_\rho)\in\mathbf{N}^{(\mathbf{R})}$, soit $\pi(\alpha)=\sum_\rho \alpha_\rho\pi(\rho)$, que nous appellerons le *poids* de α; posons $S_{k,\rho}=S_{k,\mu,h}=T^h_{k,\mu}$; si $\alpha_\rho=\sum_{k=0}^{\infty}\alpha_{k\rho}p^k$ est le développement p-adique de α_ρ, nous désignerons par S_α le produit

$$S^{\nu_1}_{\sigma_1}S^{\nu_2}_{\sigma_2}\dots S^{\nu_m}_{\sigma_m},$$

où $(\sigma_i)_{1\leq i\leq m}$ est la suite des couples (k,ρ) dans $\mathbf{N}\times\mathbf{M}\times\mathbf{N}=\mathbf{N}\times\mathbf{R}$ tels que $\alpha_{k\rho}\neq 0$, rangés par ordre croissant, et $\nu_i=\alpha_{k\rho}$ pour $\sigma_i=(k,\rho)$. D'après le théorème de Birkhoff-Witt, les S_α forment une *base* de $\mathfrak{T}(E)$.

Pour tout entier $m\geq 1$, soit $\mathfrak{t}_m$ le sous-espace vectoriel de $\mathfrak{T}(E)$ engendré par les monômes de poids $\leq m$, et qui a pour base les S_α de poids $\leq m$. En tant qu'espace vectoriel, $\mathfrak{t}_m$ s'identifie au quotient de $\mathfrak{T}(E)$ par l'idéal bilatère engendré par les éléments isobares de poids $>m$; on peut donc considérer sur $\mathfrak{t}_m$ la structure d'algèbre quotient de l'algèbre $\mathfrak{T}(E)$ par cet idéal, ce qui revient à prendre pour produit dans $\mathfrak{t}_m$ de deux éléments isobares de poids a et b, leur produit dans $\mathfrak{T}(E)$ si $a+b\leq m$, et 0 dans le cas contraire. L'application linéaire $\theta_{m,m+1}$ de $\mathfrak{t}_{m+1}$ sur $\mathfrak{t}_m$ qui est l'identité dans $\mathfrak{t}_m$ et transforme en 0 tout élément isobare de poids $m+1$, est un homomorphisme de $\mathfrak{t}_{m+1}$ sur $\mathfrak{t}_m$ [la limite projective des algèbres $\mathfrak{t}_m$ pour ces homomorphismes n'est autre que $\mathfrak{T}(E)$, complété pour la topologie définie par la filtration du poids].

Pour démontrer le théorème 1, nous allons procéder par récurrence sur m, en définissant sur chaque $\mathfrak{t}_m$ une structure de *bourgeon tronqué* ayant une base structurale (V_α), où α parcourt l'ensemble des éléments de $\mathbf{N}^{(\mathbf{R})}$ de poids $\leq m$, avec les conditions suivantes : 1° V_α est *isobare et de poids* $\pi(\alpha)$; 2° si (V'_α) est la base structurale de $\mathfrak{t}_{m+1}$, on a $\theta_{m,m+1}(V'_\alpha)=V_\alpha$ pour $\pi(\alpha)\leq m$; 3° $V_{p^k\varepsilon_i}=U_{ki}$ pour $k\geq 0$, $1\leq i\leq n$ et $p^k\leq m$.

Lorsque la base (V_α) sera définie dans $\mathfrak{t}_m$, on posera $W_{k,\rho}=V_{p^k\varepsilon_\rho}$ [pour $p^k\pi(\rho)\leq m$]; pour tout $\alpha=(\alpha_\rho)\in\mathbf{N}^{(\mathbf{R})}$ de poids $\leq m$, on désignera par W_α l'élément obtenu à partir des $W_{k,\rho}$ comme S_α à partir des $S_{k,\rho}$; la remarque finale du n° 4 montre que les W_α tels que $\pi(\alpha)\leq m$ forment une *base* de $\mathfrak{t}_m$.

8. Pour $m=1$, la solution est immédiate : les U_{0i} $(1\leq i\leq n)$ et l'unité forment une base de $\mathfrak{t}_1$ ayant toutes les propriétés voulues, de façon triviale. Supposons donc (V_α) obtenue pour $m\geq 1$, et écrivons la table de multiplication correspondante

$$V_\alpha V_\beta=\sum_\gamma d_{\alpha\beta\gamma}V_\gamma;$$

$d_{\alpha\beta\gamma}$ [que nous écrirons aussi $d(\alpha,\beta,\gamma)$ pour raisons typographiques] est donc défini pour $\pi(\alpha)\leq m$, $\pi(\beta)\leq m$, $\pi(\gamma)\leq m$, et nul lorsque

$\pi(\alpha)+\pi(\beta)\not\geq\pi(\gamma)$. En outre, la condition 1° du n° 2 équivaut à $d_{0\beta\gamma}=\delta_{\beta\gamma}$, $d_{\alpha\beta 0}=0$, sauf si $\alpha=\beta=0$, auquel cas $d_{000}=1$; et la condition 3° du n° 2 équivaut aux relations

$$(11)\qquad d(\alpha,\beta,\lambda+\lambda')=\sum_{0\leq\xi\leq\alpha,\ 0\leq\eta\leq\beta} d(\xi,\eta,\lambda)\,d(\alpha-\xi,\beta-\eta,\lambda')$$

lorsque $\pi(\lambda)+\pi(\lambda')\leq m$, $\lambda>0$ et $\lambda'>0$.

Supposons le problème résolu ; $\mathfrak{t}_{m+1}$ doit alors avoir une base (V'_α) $(\pi(\alpha)\leq m+1)$ telle que, si l'on pose

$$V'_\alpha V'_\beta=\sum_\gamma d'_{\alpha\beta\gamma}V'_\gamma,$$

les $d'_{\alpha\beta\gamma}$ satisfassent aux conditions analogues aux précédentes où l'on a simplement remplacé m par $m+1$. On doit avoir en outre $\theta_{m,m+1}(V'_\alpha)=V_\alpha$ lorsque $\pi(\alpha)\leq m$, ce qui entraîne déjà $d'_{\alpha\beta\gamma}=d_{\alpha\beta\gamma}$ lorsque $\pi(\alpha)+\pi(\beta)\leq m$; tout revient donc à définir les $d'_{\alpha\beta\gamma}$ lorsque $\pi(\alpha)\leq m$, $\pi(\beta)\leq m$ et $\pi(\alpha)+\pi(\beta)=\pi(\gamma)=m+1$ [puisque l'on doit avoir $d'_{\alpha\beta\gamma}=0$ si $\pi(\alpha)+\pi(\beta)>m+1$].

Supposons d'abord que γ ne soit pas un des éléments minimaux ε_ρ $(\pi(\rho)=m+1)$ de $\mathbf{N}^{(R)}$; on peut alors écrire $\gamma=\lambda+\lambda'$, où λ et λ' sont tous deux >0, et par suite *de poids* $\leq m$. D'après l'analogue de la condition (11) pour $\mathfrak{t}_{m+1}$, on doit donc avoir

$$d'(\alpha,\beta,\lambda+\lambda')=\sum_{0\leq\xi\leq\alpha,\ 0\leq\eta\leq\beta} d'(\xi,\eta,\lambda)\,d'(\alpha-\xi,\beta-\eta,\lambda').$$

Mais au second membre les seuls termes non nuls corrrespondent à des éléments ξ, η tels que

$$\pi(\xi)+\pi(\eta)\leq m,\qquad \pi(\alpha-\xi)+\pi(\beta-\eta)\leq m,$$

et, par suite, on a nécessairement, si le problème est possible

$$(12)\qquad d'(\alpha,\beta,\lambda+\lambda')=\sum_{\xi,\eta} d(\xi,\eta,\lambda)\,d(\alpha-\xi,\beta-\eta,\lambda'),$$

où la sommation est étendue aux couples (ξ,η) tels que $0\leq\xi\leq\alpha$, $0\leq\eta\leq\beta$.

Pour voir que le problème est possible, il faut commencer par vérifier que l'expression du second membre de (12) ne dépend pas de l'expression de γ comme somme $\lambda+\lambda'$ de deux termes >0. Or, si $\gamma=\lambda+\lambda'=\nu+\nu'$, il y a quatre éléments δ_{ij} de $\mathbf{N}^{(R)}$ tels que

$$\lambda=\delta_{11}+\delta_{12},\qquad \nu=\delta_{11}+\delta_{21},\qquad \lambda'=\delta_{21}+\delta_{22},\qquad \nu'=\delta_{12}+\delta_{22}.$$

On est ramené immédiatement à prouver que les expressions de

$d'(\alpha, \beta, \lambda+(\lambda'+\lambda''))$ et de $d'(\alpha, \beta, (\lambda+\lambda')+\lambda'')$ obtenues par la formule (12) sont identiques. Mais en vertu de (11), ces expressions sont toutes deux égales à

$$\sum_{\xi,\eta,\xi',\eta'} d(\xi, \eta, \lambda)\, d(\xi', \eta', \lambda')\, d(\alpha-\xi-\xi', \beta-\eta-\eta', \lambda''),$$

la sommation étant étendue à tous les systèmes (ξ, η, ξ', η') tels que

$$\xi+\xi' \leqq \alpha, \qquad \eta+\eta' \leqq \beta.$$

Notons ensuite que les $d'_{\alpha\beta\gamma}$ doivent vérifier les *conditions d'associativité*

$$\sum_{\nu} d'_{\alpha\beta\nu}\, d'_{\nu\gamma\delta} = \sum_{\nu} d'_{\alpha\nu\delta}\, d'_{\beta\gamma\nu}. \tag{13}$$

Notons que si $\pi(\alpha)+\pi(\beta)+\pi(\gamma)<m+1$, les conditions (13) sont vérifiées grâce à l'hypothèse de récurrence, et si $\pi(\alpha)+\pi(\beta)+\pi(\gamma)>m+1$ les deux membres de (13) sont nuls. On peut donc se limiter au cas où

$$\pi(\alpha)+\pi(\beta)+\pi(\gamma)=\pi(\delta)=m+1,$$

et où en outre $\alpha>0$, $\beta>0$, $\gamma>0$. Considérons en premier lieu le cas où $\delta=\lambda+\lambda'$, avec $\lambda>0$, $\lambda'>0$; on peut, dans les deux membres de (13), se limiter à ne considérer que les termes où $\pi(\nu)\leqq m$, les autres étant nuls. Remplaçons alors $d'_{\nu\gamma\delta}$ et $d'_{\alpha\nu\delta}$ par leurs expressions tirées de (12)

$$d'(\nu, \gamma, \delta) = \sum_{\theta,\zeta} d(\theta, \zeta, \lambda)\, d(\nu-\theta, \gamma-\zeta, \lambda'),$$

$$d'(\alpha, \nu, \delta) = \sum_{\xi,\theta} d(\xi, \theta, \lambda)\, d(\alpha-\xi, \nu-\theta, \lambda')$$

et notons, d'autre part, que $d'_{\alpha\beta\gamma}=d_{\alpha\beta\gamma}$, $d'_{\beta\gamma\nu}=d_{\beta\gamma\nu}$; d'après (11) on a donc, pour tout θ tel que $0\leqq\theta\leqq\nu$,

$$d'(\alpha, \beta, \nu) = \sum_{\xi,\eta} d(\xi, \eta, \theta)\, d(\alpha-\xi, \beta-\eta, \nu-\theta),$$

$$d'(\beta, \gamma, \nu) = \sum_{\eta\,\xi} d(\eta, \zeta, \theta)\, d(\beta-\eta, \gamma-\zeta, \nu-\theta)$$

et l'on voit alors que les deux membres de (13) sont égaux, en raison des relations d'associativité

$$\sum_{\theta} d(\xi, \eta, \theta)\, d(\theta, \zeta, \lambda) = \sum_{0} d(\xi, \theta, \lambda)\, d(\eta, \zeta, \theta),$$

$$\sum_{\theta'} d(\alpha-\xi, \beta-\eta, \theta')\, d(\theta', \gamma-\zeta, \lambda') = \sum_{\theta'} d(\alpha-\xi, \theta', \lambda')\, d(\beta-\eta, \gamma-\zeta, \theta')$$

vérifiées dans $\mathfrak{t}_m$.

9. Nous n'avons pas encore défini les éléments $d'_{\alpha\beta\varepsilon_\rho}$ pour $\pi(\rho)=m+1$; mais il est immédiat que si l'on prenait $d'_{\alpha\beta\varepsilon_\rho}=0$, toutes les conditions (13) seraient vérifiées. Nous allons utiliser cette remarque pour introduire un *bourgeon tronqué* auxiliaire $\bar{\mathfrak{t}}_{m+1}$: il est défini par une base $(\overline{V}_\alpha)$ ayant pour ensemble d'indices l'ensemble des $\alpha\in\mathbf{N}^{(R)}$ de poids $\leq m+1$, et pour table de multiplication

$$\overline{V}_\alpha\overline{V}_\beta=\sum_\gamma \bar{d}_{\alpha\beta\gamma}\overline{V}_\gamma, \tag{14}$$

où $\bar{d}_{\alpha\beta\gamma}=d'_{\alpha\beta\gamma}$ est donné par (12) si $\gamma=\lambda+\lambda'$, $\lambda>0$, $\lambda'>0$, et $\bar{d}_{\alpha\beta\varepsilon_\rho}=0$ pour $\pi(\rho)=m+1$. Que l'on ait ainsi une base structurale résulte des remarques précédentes; on notera en outre que $\bar{d}_{\alpha\beta\gamma}=0$ si $\pi(\gamma)\neq\pi(\alpha)+\pi(\beta)$, si bien qu'on peut encore dire que la loi de composition de $\bar{\mathfrak{t}}_{m+1}$ est *isobare*.

Les relations $d_{\alpha\beta\varepsilon_\rho}=0$ pour $\pi(\rho)=m+1$ montrent que dans $\bar{\mathfrak{t}}_{m+1}$, les éléments $\overline{V}_\alpha$ tels que $\pi(\alpha)\leq m+1$ et $\alpha\neq\varepsilon_\rho$ si $\pi(\rho)=m+1$ forment la base d'une *sous-algèbre* $\bar{\mathfrak{w}}_{m+1}$ de $\bar{\mathfrak{t}}_{m+1}$. Pour tout $\rho\in R$ de poids $\leq m+1$, posons $\overline{W}_{k,\rho}=\overline{V}_{p^k\varepsilon_\rho}$, et pour tout $\alpha=(\alpha_\rho)\in\mathbf{N}^{(R)}$ de poids $\leq m+1$, soit $\overline{W}_\alpha$ l'élément de $\bar{\mathfrak{t}}_{m+1}$ défini à partir des $\overline{W}_{k,\rho}$ comme les S_α à partir des $S_{k,\rho}$ (n° 7); ces éléments forment une *base* de $\bar{\mathfrak{t}}_{m+1}$ avec une table de multiplication isobare. En outre, les relations $\bar{d}_{\alpha\beta\varepsilon_\rho}=0$ pour $\pi(\rho)=m+1$ montrent que les $\overline{W}_\alpha$ tels que $\pi(\alpha)\leq m+1$ et $\alpha\neq\varepsilon_\rho$ pour $\pi(\rho)=m+1$, forment une *base* de $\bar{\mathfrak{w}}_{m+1}$.

Posons $\overline{W}_{k,i,0}=\overline{V}_{p^k\varepsilon_i}=\overline{U}_{ki}$ pour $p^k\leq m+1$ ($1\leq i\leq n$); ce sont des éléments de $\bar{\mathfrak{w}}_{m+1}$ puisque $m\geq 1$. On définit donc un homomorphisme F de l'algèbre libre $\mathfrak{T}(E)$ dans $\bar{\mathfrak{w}}_{m+1}$ en posant $F(U_{ki})=\overline{U}_{ki}$ pour $p^k\leq m+1$, $1\leq i\leq n$, $F(U_{ki})=0$ si $p^k>m+1$. L'image par F de tout élément de $\mathfrak{T}(E)$, de poids $>m+1$, est alors nulle; en passant au quotient, on obtient donc un *homomorphisme* f de $\mathfrak{t}_{m+1}$ dans $\bar{\mathfrak{w}}_{m+1}$, tel que $f(U_{ki})=\overline{U}_{ki}$ pour $p^k\leq m+1$, $1\leq i\leq n$. L'hypothèse de récurrence implique que la restriction de f à $\mathfrak{t}_m$ est un isomorphisme (d'espace vectoriel) sur le sous-espace $\bar{\mathfrak{t}}_m$ ayant pour base les $\overline{V}_\alpha$ de poids $\leq m$, et l'on a $f(V_\alpha)=\overline{V}_\alpha$ pour ces indices. Soit $\mathfrak{n}_{m+1}$ le sous-espace de $\mathfrak{t}_{m+1}$, supplémentaire de $\mathfrak{t}_m$, engendré par les éléments de poids $m+1$ dans $\mathfrak{T}(E)$; soient d'autre part $\bar{\mathfrak{q}}_{m+1}$ le sous-espace de $\bar{\mathfrak{w}}_{m+1}$ ayant pour base les $\overline{V}_\alpha$ correspondant aux indices α de poids $m+1$ tels que $\alpha\neq\varepsilon_\rho$ (les $\overline{W}_\alpha$ correspondant aux mêmes indices formant ainsi une base de $\bar{\mathfrak{q}}_{m+1}$), et $\bar{\mathfrak{r}}_{m+1}$ le sous-espace de $\bar{\mathfrak{t}}_{m+1}$ ayant pour base les $\overline{V}_{\varepsilon_\rho}=\overline{W}_{0,\rho}$ où $\pi(\rho)=m+1$; $\bar{\mathfrak{w}}_{m+1}$ est somme directe de $\bar{\mathfrak{t}}_m$ et de $\bar{\mathfrak{q}}_{m+1}$, $\bar{\mathfrak{t}}_{m+1}$ somme directe de $\bar{\mathfrak{w}}_{m+1}$ et de $\bar{\mathfrak{r}}_{m+1}$, et f applique $\mathfrak{n}_{m+1}$ dans $\bar{\mathfrak{q}}_{m+1}$.

10. Nous allons montrer que $f(\mathfrak{n}_{m+1})=\bar{\mathfrak{q}}_{m+1}$, autrement dit, que pour tout indice α de poids $m+1$, distinct des ε_ρ, il existe W_α dans $\mathfrak{n}_{m+1}$ tel

que $f(W_\alpha) = \overline{W}_\alpha$. Supposons d'abord que α ne soit pas de la forme $p^k\varepsilon_\rho$; alors, dans $\alpha = (\alpha_\rho)$, deux aux moins des α_ρ sont $\neq 0$ et par suite tous les $\alpha_\rho\varepsilon_\rho$ sont de poids $\leq m$; on peut par suite définir W_α à partir des $W_{k,\rho}$ (déjà connus, puisque de poids $\leq m$) comme S_α à partir des $S_{k,\rho}$ (n° 7), les produits étant pris *dans* $\mathfrak{t}_{m+1}$. Comme f est un homomorphisme, on a bien $f(W_\alpha) = \overline{W}_\alpha$ par définition de $\overline{W}_\alpha$.

Supposons maintenant $\alpha = p^k\varepsilon_\rho$, avec $k \geq 1$; considérons l'image

$$\mathfrak{p}'(\overline{W}_{k,\rho}) = \overline{W}_{k-1,\rho}$$

par l'homomorphisme de Frobenius (qui ici applique $\bar{\mathfrak{t}}_{m+1}$ dans lui-même, puisque le corps des scalaires est $\mathbf{F}_p$). On a $f(W_{k-1,\rho}) = \overline{W}_{k-1,\rho}$ par l'hypothèse de récurrence; or, $W_{k-1,\rho}$ s'exprime d'une seule manière comme combinaison linéaire de monomes par rapport aux U_{hi}, de poids $p^{k-1}\pi(\rho)$; remplaçons dans chacun de ces monomes U_{hl} par $U_{h+1,i}$, pour tout couple d'indices (h, i); on obtient un élément $Y_{k,\rho}$ de $\mathfrak{t}_{m+1}$, isobare et de poids $p^k\pi(\rho) = m+1$, donc appartenant à $\mathfrak{n}_{m+1}$, et il est clair que si l'on pose $\overline{Y}_{k,\rho} = f(Y_{k,\rho})$, on a $\mathfrak{p}'(\overline{W}_{k,\rho} - \overline{Y}_{k,\rho}) = 0$. Cela signifie que, dans $\bar{\mathfrak{t}}_{m+1}$, $\overline{W}_{k,\rho} - \overline{Y}_{k,\rho}$ est combinaison linéaire de $\overline{W}_\lambda$, où λ *n'est pas divisible par p* et n'est pas de la forme ε_ρ (puisque $\overline{W}_{k,\rho} - \overline{Y}_{k,\rho}$ est dans la sous-algèbre $\bar{\mathfrak{w}}_{m+1}$); mais, d'après ce qui précède, ces éléments $\overline{W}_\lambda$ sont images par f des W_λ correspondants. Il existe donc bien un élément $W_{k,\rho}$ de $\mathfrak{n}_{m+1}$ (qui n'est pas déterminé de façon unique), tel que $f(W_{k,\rho}) = \overline{W}_{k,\rho}$. Lorsque $\varepsilon_\rho = \varepsilon_i$ $(1 \leq i \leq n)$ (ce qui suppose $p^k = m+1$), on a par définition $\overline{W}_{k,\rho} = \overline{U}_{ki}$, et l'on prendra $W_{k,\rho} = U_{ki}$.

Les W_α ainsi définis, de poids $m+1$, et correspondant aux $\alpha \neq \varepsilon_\rho$, sont évidemment linéairement indépendants dans $\mathfrak{n}_{m+1}$ et forment une base d'un sous-espace $\mathfrak{q}_{m+1}$ de $\mathfrak{n}_{m+1}$, supplémentaire du noyau $\mathfrak{r}_{m+1}$ de f. Il est clair que $\mathfrak{r}_{m+1}$ et $\mathfrak{r}_{m+1}$ ont même dimension; on achèvera de définir la base (W_α) de $\mathfrak{n}_{m+1}$ en prenant pour les $W_{0,\rho}$ [où ρ parcourt l'ensemble des éléments de R de poids $\pi(\rho) = m+1$] une base *arbitraire* de $\mathfrak{r}_{m+1}$.

11. Nous sommes maintenant en état de définir la base structurale (V'_α) de $\mathfrak{t}_{m+1}$. Pour $\pi(\alpha) \leq m$, on prendra $V'_\alpha = V_\alpha$. Pour $\pi(\alpha) = m+1$, et $\alpha \neq \varepsilon_\rho$, on a

$$\overline{V}_\alpha = \sum_\lambda a_{\alpha\lambda}\overline{W}_\lambda, \tag{15}$$

où, dans le second membre, λ parcourt l'ensemble des indices de poids $m+1$, distincts des ε_ρ; comme les $\overline{V}_\alpha$ [avec $\pi(\alpha) = m+1$, $\alpha \neq \varepsilon_\rho$] forment une base de $\bar{\mathfrak{q}}_{m+1}$, la matrice carrée $(a_{\alpha\lambda})$ est *inversible*. Nous poserons alors

$$V'_\alpha = \sum_\lambda a_{\alpha\lambda}W_\lambda. \tag{16}$$

Enfin, pour $\alpha = \varepsilon_\rho$, $\pi(\rho) = m+1$, nous prendrons $V'_{\varepsilon_\rho} = W_{0,\rho}$; avec ces choix, il est clair que (V'_α) est une *base* de $\mathfrak{t}_{m+1}$. Reste à voir qu'elle définit sur $\mathfrak{t}_{m+1}$ une structure de bourgeon tronqué.

Or, on a par construction $f(V'_\alpha) = \overline{V}_\alpha$ si $\pi(\alpha) \leqq m$, ou si $\pi(\alpha) = m+1$ et $\alpha \neq \varepsilon_\rho$, et $f(V'_{\varepsilon_\rho}) = 0$ pour $\pi(\rho) = m+1$. On en déduit que, pour $\alpha > 0$, $\beta > 0$, $\pi(\alpha) + \pi(\beta) = m+1$, on a

$$f(V'_\alpha V'_\beta) = \overline{V}_\alpha \overline{V}_\beta = \sum_\gamma \overline{d}_{\alpha\beta\gamma} \overline{V}_\gamma \tag{17}$$

et, par suite, le noyau de f étant $\mathfrak{r}_{m+1}$, qui a pour base les V'_{ε_ρ} [où $\pi(\rho) = m+1$], on peut écrire

$$V'_\alpha V'_\beta = \sum_\gamma d''_{\alpha\beta\gamma} V'_\gamma, \tag{18}$$

avec $d''_{\alpha\beta\gamma} = \overline{d}_{\alpha\beta\gamma} = d'_{\alpha\beta\gamma}$ si γ (de poids $m+1$) est distinct des ε_ρ. Les conditions analogues à (11) pour les éléments $d''_{\alpha\beta\gamma}$ sont par suite vérifiées, ce qui achève la démonstration du théorème 1.

On notera que la méthode suivie fournit sur $\mathfrak{T}(E)$ une structure d'hyperalgèbre dont la loi est *canonique* (*voir* [6] et ([7], n° 4])). Il y a en outre une très large part d'arbitraire dans le choix de la base structurale (V_α). Nous allons préciser un peu le choix de cette base, en vue d'applications aux numéros suivants.

Pour tout entier $r \geqq 0$, nous désignerons par $\mathfrak{m}_r$ la sous-algèbre (libre) de $\mathfrak{T}(E)$ engendrée par les éléments U_{ki} tels que $1 \leqq i \leqq n$ et $0 \leqq k \leqq r$. On a une *base* de $\mathfrak{m}_r$ en prenant les monomes S_α qui ne contiennent que les facteurs $S_{k,\mu,h} = T_{k,\mu}^{p^h}$ provenant d'alternants $T_{k,\mu}$ ne contenant que les U_{li}, où $l \leqq r$; désignons par A_r l'ensemble des indices $\alpha \in \mathbf{N}^{(\mathbf{R})}$ correspondants; on remarquera que les relations $\alpha \in A_r$, $\beta \leqq \alpha$ entraînent $\beta \in A_r$ et que $A_r \subset A_{r+1}$. Nous allons montrer qu'on peut prendre la base structurale (V_α) dans $\mathfrak{T}(E)$ de sorte que *les* V_α *tels que* $\alpha \in A_r$ *forment une base de* $\mathfrak{m}_r$ (pour tout $r \geqq 0$).

Observons pour cela que l'algèbre $\mathfrak{t}_m$ est réunion de la suite croissante des sous-algèbres $\mathfrak{t}_m \cap \mathfrak{m}_r$ (ou d'ailleurs $\mathfrak{t}_m \cap \mathfrak{m}_r = \mathfrak{t}_m$ dès que $p^r \geqq m$). Raisonnant par récurrence sur m, nous supposerons que les V_α tel que $\pi(\alpha) \leqq m$ et $\alpha \in A_r$ forment une base de $\mathfrak{t}_m \cap \mathfrak{m}_r$ (pour tout r tel que $p^r \leqq m$); les relations $\alpha \in A_r$, $\beta \in A_r$, $\pi(\alpha) + \pi(\beta) \leqq m$ entraînent alors $d_{\alpha\beta\gamma} = 0$ si $\gamma \notin A_r$. Les formules (12) prouvent alors que l'on a aussi $d'_{\alpha\beta\gamma} = 0$ pour $\alpha \in A_r$, $\beta \in A_r$, $\pi(\alpha) + \pi(\beta) = m+1$ et $\gamma \notin A_r$, $\pi(\gamma) = m+1$: en effet, si γ n'est pas de la forme $p^k \varepsilon_\rho$ ($k \geqq 1$), on peut décomposer γ en une somme $\lambda + \lambda'$, où $\lambda > 0$, $\lambda' > 0$, et un au moins des deux termes λ, λ' n'appartient pas à A_r, d'après la définition de A_r et des S_α; si $\gamma = p^k \varepsilon_\rho$, la formule (4) montre que $d'_{\alpha\beta\gamma} = 0$ sauf si α et β sont multiples de p^k; on est alors [en vertu de (4) et de la définition des $T_{k,\mu}$ lorsque $k \geqq 1$] ramené au cas $k = 0$, $\pi(\rho) \leqq m$,

et notre assertion résulte de l'hypothèse de récurrence. Autrement dit, les $\overline{V}_\alpha$ tels que $\pi(\alpha) \leqq m+1$ et $\alpha \in A_r$ forment la base d'une *sous-algèbre* $\bar{\mathfrak{t}}_{m+1,r}$ de $\bar{\mathfrak{t}}_{m+1}$, et ceux pour lesquels $\alpha \neq \varepsilon_\rho$ $(\pi(\rho) = m+1)$ forment la base de la sous-algèbre $\bar{\mathfrak{w}}_{m+1,r} = \bar{\mathfrak{w}}_{m+1} \cap \bar{\mathfrak{t}}_{m+1,r}$; on désignera par $\mathfrak{q}_{m+1,r}$ (resp. $\bar{\mathfrak{r}}_{m+1,r}$) le sous-espace de $\bar{\mathfrak{q}}_{m+1}$ (resp. $\bar{\mathfrak{r}}_{m+1}$) engendré par les $\overline{V}_\alpha$ d'indice $\alpha \in A_r$ dans $\bar{\mathfrak{q}}_{m+1}$ (resp. $\bar{\mathfrak{r}}_{m+1}$). On notera que, par définition, les $\overline{W}_\alpha$ tels que $\alpha \in A_r$ appartiennent à $\bar{\mathfrak{t}}_{m+1,r}$, et comme ils sont linéairement indépendants, ils forment une *base* de cette algèbre, et ceux qui correspondent aux indices distincts des ε_ρ de poids $m+1$ forment une base de $\bar{\mathfrak{w}}_{m+1,r}$; de même, les W_α tels que $\pi(\alpha) \leqq m$ et $\alpha \in A_r$ forment une base de $\mathfrak{t}_m \cap \mathfrak{m}_r$, par le même raisonnement.

Cela étant, il est clair que $f(\mathfrak{t}_{m+1} \cap \mathfrak{m}_r) \subset \bar{\mathfrak{w}}_{m+1,r}$ par définition de f, et par suite $f(\mathfrak{n}_{m+1} \cap \mathfrak{m}_r) \subset \bar{\mathfrak{q}}_{m+1,r}$ pour tout r. On peut préciser le raisonnement du n° 10 en prouvant que, pour tout α tel que $\overline{W}_\alpha \in \bar{\mathfrak{q}}_{m+1,r}$, il existe W_α *dans* $\mathfrak{n}_{m+1} \cap \mathfrak{m}_r$ tel que $f(W_\alpha) = \overline{W}_\alpha$. C'est immédiat si α n'est pas de la forme $p^k\varepsilon_\rho$ $(k \geqq 1)$, en vertu de la remarque, faite plus haut, que $\alpha \in A_r$ et $\beta \leqq \alpha$ entraîne $\beta \in A_r$. Si ensuite $\alpha = p^k\varepsilon_\rho$, $k \geqq 1$, la définition des S_α (nos 6 et 7) est telle que la relation $p^k\varepsilon_\rho \in A_r$ entraîne $p^{k-1}\varepsilon_\rho \in A_{r-1}$, donc $W_{k-1,\rho} \in \mathfrak{m}_{r-1}$; l'élément $Y_{k,\rho}$ construit au n° 10 appartient donc à $\mathfrak{m}_r$, donc les $\overline{W}_\lambda$ qui figurent dans l'expression de $\overline{W}_{k,\rho} - \overline{Y}_{k,\rho}$ appartiennent à $\bar{\mathfrak{q}}_{m+1,r}$, et l'on en conclut comme au n° 10 qu'il existe $W_{k,\rho}$ dans $\mathfrak{n}_{m+1} \cap \mathfrak{m}_r$, tel que $f(W_{k,\rho}) = \overline{W}_{k,\rho}$. Considérons ensuite, pour chaque r, l'intersection $\mathfrak{r}_{m+1,r} = \mathfrak{r}_{m+1} \cap \mathfrak{m}_r$, noyau de la restriction de f à $\mathfrak{n}_{m+1} \cap \mathfrak{m}_r$. Ce qui précède montre que $\mathfrak{r}_{m+1,r}$ et $\bar{\mathfrak{r}}_{m+1,r}$ ont même dimension; on peut donc achever de déterminer les W_α en prenant pour les $V_{0,\rho}$ une base de $\mathfrak{r}_{m+1}$ telle que les $W_{0,\rho}$ correspondant aux indices tels que $\varepsilon_\rho \in A_r$ forment une base de $\mathfrak{r}_{m+1,r}$ (on procède pour cela par récurrence sur r). Enfin, dans (15), la relation $\alpha \in A_r$ entraîne $a_{\alpha\lambda} = 0$ pour $\lambda \notin A_r$; on peut donc encore définir les V'_α par les relations (16), et la base structurale (V_α) ainsi obtenue pour $\mathfrak{T}(E)$ satisfait bien aux conditions voulues.

Nous désignerons par $\mathfrak{H}_n(\mathbf{F}_p)$ l'hyperalgèbre obtenue en munissant $\mathfrak{T}(E)$ d'une base structurale ayant la propriété précédente, par $\mathfrak{H}_n(K)$ l'hyperalgèbre de même base obtenue en étendant à K le corps des scalaires, et nous dirons que $\mathfrak{H}_n(K)$ est *une hyperalgèbre libre* (*sur* K) *à n* « *générateurs* » (U_{kl}) $(1 \leqq i \leqq n)$ *et à loi canonique*. Il y a encore évidemment un très grand arbitraire dans le choix des V_α, et la notation $\mathfrak{H}_n(K)$ est donc abusive. Nous allons voir toutefois que cette hyperalgèbre possède bien la propriété « universelle » à laquelle on s'attend.

12. Soient $\mathfrak{G}$, $\overline{\mathfrak{G}}$ deux hyperalgèbres sur le même corps K, M et $\overline{M}$ les applications structurales de $\mathfrak{G}$ et $\overline{\mathfrak{G}}$ dans $\mathfrak{G} \otimes \mathfrak{G}$ et $\overline{\mathfrak{G}} \otimes \overline{\mathfrak{G}}$; un *homomorphisme d'hyperalgèbre* $\mathfrak{u}'$ de $\mathfrak{G}$ dans $\overline{\mathfrak{G}}$ est un homomorphisme d'algèbre

transformant l'élément unité en élément unité et les semi-dérivations de hauteur r en semi-dérivations de hauteur r (7), et tel que l'on ait en outre

$$(\mathbf{u}'\otimes\mathbf{u}')\circ M=\overline{M}\circ\mathbf{u}' \tag{25}$$

ou encore

$$(\mathbf{u}'\otimes\mathbf{u}')(\mathrm{Z}_\alpha^0)=(\mathbf{u}'(\mathrm{Z}_\alpha))^0 \tag{26}$$

pour tout élément de la base structurale (Z_α) de $\mathfrak{G}$ (il suffit d'ailleurs pour cela que $\mathbf{u}'\otimes\mathbf{u}'$ transforme $\mathfrak{G}^0$ en une sous-algèbre de $\overline{\mathfrak{G}}^0$).

THÉORÈME 2. — *Si $\mathfrak{G}$ est une hyperalgèbre de dimension n sur* K, *il existe une hyperalgèbre $\overline{\mathfrak{G}}$ isomorphe à $\mathfrak{G}$, et un homomorphisme $\mathbf{u}'$ de $\mathfrak{H}_n(\mathrm{K})$ sur $\overline{\mathfrak{G}}$ tel que l'on ait*

$$\mathbf{u}'(\mathrm{V}_\alpha)=\overline{\mathrm{Z}}_\alpha \tag{27}$$

pour tout $\alpha\in\mathbf{N}^{\mathrm{J}}$, où $\mathrm{J}\subset\mathrm{M}$ est l'intervalle $1\leqq i\leqq n$, et $(\overline{\mathrm{Z}}_\alpha)$ la base structurale de $\overline{\mathfrak{G}}$.

Avec les notations du n° 11, supposons qu'il existe un homomorphisme $\mathbf{u}'$ de l'algèbre libre $\mathfrak{m}_r$ sur le bourgeon $\mathfrak{s}_r$ de l'hyperalgèbre $\mathfrak{G}$ tel que l'on ait

$$\mathbf{u}'(\mathrm{V}_\alpha)=\mathrm{Z}_\alpha \tag{28}$$

pour tout $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$, avec $\alpha_i<p^r$. Comme $\mathfrak{m}_{r+1}$ est une algèbre libre, on prolonge $\mathbf{u}'$ en un homomorphisme (encore noté $\mathbf{u}'$) de $\mathfrak{m}_{r+1}$ sur $\mathfrak{s}_{r+1}$ en posant

$$\mathbf{u}'(\mathrm{U}_{r+1,i})=\mathrm{X}_{r+1,i}\qquad\text{pour}\quad 1\leqq i\leqq n. \tag{29}$$

En raison de (28), il s'ensuit que l'on a

$$(\mathbf{u}'\otimes\mathbf{u}')(\mathrm{U}_{r+1,i}^0)=\mathrm{X}_{r+1,i}^0=(\mathbf{u}'(\mathrm{U}_{r+1,i}))^0 \tag{30}$$

et par suite [les applications structurales dans $\mathfrak{H}_n(\mathrm{K})$ et $\mathfrak{G}$ étant des homomorphismes], (30) et l'hypothèse de récurrence prouvent que

$$(\mathbf{u}'\otimes\mathbf{u}')(\mathrm{V}_\alpha^0)=(\mathbf{u}'(\mathrm{V}_\alpha))^0 \tag{31}$$

pour tous les $\alpha\in\mathrm{A}_{r+1}$. Il résulte de là que, pour tout $k\leqq r+1$ tel que $p^k\varepsilon_\rho\in\mathrm{A}_{r+1}$, $\mathbf{u}'(\mathrm{W}_{k,\rho})$ est une *semi-dérivation de hauteur k* dans $\mathfrak{G}$. C'est immédiat en vertu de l'hypothèse de récurrence si $p^k\varepsilon_\rho\in\mathrm{A}_r$; et en général cela résulte de (31) par récurrence sur k, car (31) prouve que

$$(\mathbf{u}'(\mathrm{W}_{k,\rho}))^0=\mathrm{I}\otimes\mathbf{u}'(\mathrm{W}_{k,\rho})+\mathbf{u}'(\mathrm{W}_{k,\rho})\otimes\mathrm{I}+\sum_{0<\beta<p^k\varepsilon_\rho}\mathbf{u}'(\mathrm{V}_\beta)\otimes\mathbf{u}'(\mathrm{V}_{p^k\varepsilon_\rho-\beta})$$

(7) En fait, cette seconde condition résulte des deux autres, comme le montre la remarque faite ci-dessous dans la démonstration du théorème 2, après la formule (31).

d'où notre assertion, car en vertu de l'hypothèse de récurrence, les $\mathbf{u}'(V_\beta)$, pour $\beta < p^k\varepsilon_\rho$, sont des semi-dérivations spéciales de hauteur k.

13. Dans $\mathfrak{s}_{r+1}$, nous posons (pour $\alpha \in \mathbf{N}^J$) $Z'_\alpha = Z_\alpha$ si $h(\alpha) \leqq r$, $Z'_\alpha = \mathbf{u}'(V_\alpha)$ si $h(\alpha) = r+1$. Nous allons montrer que *les* Z'_α *forment une base de* $\mathfrak{s}_{r+1}$. Il suffira évidemment pour cela de prouver que les X_α pour $h(\alpha) \leqq r+1$ sont combinaisons linéaires des Z'_α; cela étant évident pour $h(\alpha) \leqq r$ en vertu de l'hypothèse de récurrence, on peut se limiter au cas où $h(\alpha) = r+1$; on a alors

$$X_\alpha = X_\beta X_{r+1,1}^{\nu_1} X_{r+1,2}^{\nu_2} \cdots X_{r+1,n}^{\nu_n}.$$

où $h(\beta) \leqq r$ et $0 \leqq \nu_i \leqq p-1$ pour $1 \leqq i \leqq n$. Posons $d_{r+1}(\alpha) = \sum_{i=1}^{n} \nu_i$; nous prouverons par récurrence sur m, que les X_α tels que $d_{r+1}(\alpha) \leqq m$ sont combinaisons linéaires des Z'_λ tels que $d_{r+1}(\lambda) \leqq m$, et *vice-versa*.

Plus généralement, pour tout $\alpha = (\alpha_\rho) \in \mathbf{N}^{R)}$, de hauteur $\leqq k$, désignons par $d_k(\alpha)$ la somme des coefficients de p^k dans le développement p-adique de chacun des α_ρ. Notre assertion résultera du lemme suivant sur l'hyperalgèbre libre $\mathfrak{H}_n(K)$:

LEMME 1. — *Si* $h(\alpha) \leqq k$, *et* $d_k(\alpha) = m$, *on a*

$$V_\alpha = W_\alpha + \sum_\lambda b_{\alpha\lambda} W_\lambda, \tag{32}$$

où, dans la somme, tous les termes de coefficients $\neq 0$ *sont tels que* $d_k(\lambda) < m$.

Supposons, en effet, ce lemme démontré, et rappelons que $\mathbf{u}'(W_{k+1,\rho})$ est une semi-dérivation de hauteur $r+1$, donc combinaison linéaire des $X_{r+1,i}$ et des X_β tels que $h(\beta) \leqq r$; la formule (32) appliquée pour $k = r+1$ et $\alpha \in \mathbf{N}^J$, montre que $Z'_\alpha - X_\alpha$ est combinaison linéaire des X_λ tels que $d_{r+1}(\lambda) < m$, et cela établira notre assertion.

Le lemme 1 est évident pour $m = 0$, puisqu'alors $h(\alpha) < k$, et par suite $h(\lambda) < k$ dans les termes du second membre de (32). Procédons par récurrence sur m; on peut écrire, par définition, $W_\alpha = W_\beta W_{k,\rho}$, où $d_k(\beta) = m-1$; il suffira de montrer que, dans l'expression du produit

$$V_\beta W_{k,\rho} = \sum_\gamma d(\beta, p^k\varepsilon_\rho, \gamma) V_\gamma,$$

on a $d(\beta, p^k\varepsilon_\rho, \alpha) = 1$ et $d(\beta, p^k\varepsilon_\rho, \gamma) = 0$ pour tout autre indice γ tel que $d_k(\gamma) \geqq m$.

Considérons d'abord le cas où l'on peut écrire $\gamma = p^k\varepsilon_\sigma + \lambda$, avec $\lambda > 0$;

la formule (11) donne dans ce cas

$$(33)\quad d(\beta, p^k\varepsilon_\rho, p^k\varepsilon_\sigma+\lambda)=\sum_{\xi,\eta} d(\xi,\eta,p^k\varepsilon_\sigma)\,d(\beta-\xi,p^k\varepsilon_\rho-\eta,\lambda),$$

la somme du second membre étant étendue aux indices tels que $0\leq\xi\leq\beta$, $0\leq\eta\leq p^k\varepsilon_\rho$. Mais, d'après (4), on a $d(\xi,\eta,p^k\varepsilon_\sigma)=0$, sauf lorsque ξ et η sont multiples de p^k, ce qui entraîne $\eta=0$ ou $\eta=p^k\varepsilon_\rho$. Mais alors, dans le second membre de (33), il n'y a que deux termes éventuellement non nuls, savoir $d(\beta-p^k\varepsilon_\sigma,p^k\varepsilon_\rho,\lambda)$ et $d(\beta-\lambda,p^k\varepsilon_\rho,p^k\varepsilon_\sigma)$ (en supposant que $\beta\geq p^k\varepsilon_\sigma$, sans quoi le premier de ces termes est remplacé par 0). L'hypothèse de récurrence montre que le premier de ces termes est nul si $d_k(\lambda)>m-1$, ou si $d_k(\lambda)=m-1$ et λ est distinct de $\beta-p^k\varepsilon_\sigma+p^k\varepsilon_\rho$, c'est-à-dire si $\gamma\neq\alpha$; et pour $\gamma=\alpha$, ce premier terme est 1 par l'hypothèse de récurrence. Quant au second terme, il ne peut être $\neq 0$ que si $\beta-\lambda=p^k\delta$, avec $h(\delta)=0$, auquel cas il est égal à $(d(\delta,\varepsilon_\rho,\varepsilon_\sigma))^{p^k}$, d'après (4). On est donc ramené à examiner le cas $k=0$. Mais il est immédiat alors que $V_\alpha=\frac{1}{\alpha!}W_\alpha$, la loi de $\mathfrak{H}_n(K)$ étant canonique ([7], prop. 3, p. 223) et, par suite, $d(\delta,\varepsilon_\rho,\varepsilon_\sigma)=0$, sauf si $\delta=0$ et $\rho=\sigma$, auquel cas on a encore $\gamma=\alpha$ et les deux termes considérés ci-dessus se confondent et donnent bien $d(\beta,p^k\varepsilon_\rho,\alpha)=1$. Reste enfin à examiner le cas où l'on aurait $\gamma=p^k\varepsilon_\sigma$; mais le raisonnement qui vient d'être fait prouve alors que $d(\beta,p^k\varepsilon_\rho,p^k\varepsilon_\sigma)=0$, sauf si $\beta=0$ et $\rho=\sigma$, cas trivial; ce qui achève de démontrer le lemme 1.

14. Il est maintenant facile d'achever la démonstration du théorème 2. Il est clair, d'après la définition des Z'_α, que ces derniers forment une base structurale pour une structure de bourgeon sur $\mathfrak{s}_{r+1}$; désignons par $\mathfrak{s}'_{r+1}$ le bourgeon ainsi obtenu, par $d'_{\alpha\beta\gamma}$ ses constantes de structure; on a $d'_{\alpha\beta\gamma}=d_{\alpha\beta\gamma}$ lorsque les indices sont de hauteur $\leq r$ [en désignant ici par $d_{\alpha\beta\gamma}$ les constantes de structure de l'hyperalgèbre $\mathfrak{G}$, et non plus de $\mathfrak{H}_n(K)$]. Appliquons à $\mathfrak{s}_{r+1}$ et $\mathfrak{s}'_{r+1}$ les isomorphismes « standards » $\mathbf{v}'$ et $\mathbf{w}'$, qui transforment ces bourgeons en des bourgeons $\bar{\mathfrak{s}}_{r+1}$ et $\bar{\mathfrak{s}}'_{r+1}$ à lois *canoniques* (*cf.* [6] et [7, n° 4]). Notons que les structures d'algèbre de $\mathfrak{s}_{r+1}$ et $\mathfrak{s}'_{r+1}$ sont identiques par définition, et ont même table de multiplication si l'on prend pour base les $X_\alpha\,(h(\alpha)\leq r+1)$. D'autre part, de l'hypothèse $Z'_\alpha=Z_\alpha$ pour $h(\alpha)\leq r$, et de la définition des isomorphismes standards $\mathbf{v}'$ et $\mathbf{w}'$, il suit aussitôt que si l'on a

$$(34)\quad \begin{cases} \mathbf{v}'(X_\alpha)=\sum_\lambda g_{\alpha\lambda}\overline{X}_\lambda \qquad \text{pour} \quad h(\alpha)\leq r, \\ \mathbf{v}'(X_{r+1,i})=\overline{X}_{r+1,i}+\sum_\lambda h_{i\lambda}\overline{X}_\lambda \end{cases}$$

[sommations sur les indices λ tels que $h(\lambda) \leqq r$], on a aussi

$$(35) \qquad \begin{cases} \mathbf{w}'(X_\alpha) = \sum_\lambda g_{\alpha\lambda} \overline{X}'_\lambda \quad \text{pour} \quad h(\alpha) \leqq r, \\ \mathbf{w}'(X_{r+1,i}) = \overline{X}_{r+1,i} + \sum_\lambda h_{i\lambda} \overline{X}'_\lambda, \end{cases}$$

avec les *mêmes* coefficients aux seconds membres. On en conclut que la table de multiplication de $\bar{\mathfrak{s}}_{r+1}$ pour la base $(\overline{X}_\alpha)$ est la *même* que celle de $\bar{\mathfrak{s}}'_{r+1}$ pour la base $(\overline{X}'_\alpha)$; les lois de ces deux bourgeons étant canoniques, le théorème d'unicité ([6], th. 2) prouve que les tables de multiplication pour les bases $(\overline{Z}_\alpha)$ et $(\overline{Z}'_\alpha)$ sont aussi les *mêmes*. Par suite, si l'on identifie ces deux bourgeons, on voit que $\mathbf{q}^{(r+1)} = \mathbf{w}'^{-1}\mathbf{v}'$ est un isomorphisme de $\mathfrak{s}_{r+1}$ sur $\mathfrak{s}'_{r+1}$ pour la structure de bourgeon.

Pour terminer la démonstration, il suffit maintenant de procéder comme d'ordinaire à un raisonnement de récurrence sur r, suivi d'un « passage à la limite » : on suppose déjà défini un isomorphisme $\mathbf{s}^{(r)}$ de $\mathfrak{G}$ sur une hyperalgèbre $\mathfrak{G}^{(r)}$ de sorte que l'hypothèse faite au début de la démonstration soit vérifiée pour le bourgeon $\mathfrak{s}_r^{(r)}$ de $G^{(r)}$; on considère alors l'isomorphisme $\mathbf{s}^{r+1} = \mathbf{q}^{(r+1)}\mathbf{s}^{(r)}$ de $\mathfrak{G}$ sur une hyperalgèbre [8] $\mathfrak{G}^{(r+1)}$ et comme $\mathbf{q}^{(r+1)}$ est l'identité dans $\mathfrak{s}_r$, l'hypothèse du début de la démonstration est maintenant vérifiée pour le bourgeon $\mathfrak{s}_{r+1}^{(r+1)}$ (identifiable à $\mathfrak{s}'_{r+1}$) de $\mathfrak{G}^{(r+1)}$. Le « passage à la limite » sur les $\mathbf{s}^{r)}$ conduit finalement à un isomorphisme $\mathbf{s}'$ de $\mathfrak{G}$ sur une hyperalgèbre $\overline{\mathfrak{G}}$, pour laquelle les conditions du théorème 2 sont vérifiées.

Nous avons suivi d'assez près, dans cette démonstration, la méthode utilisée dans le théorème 3 de [9]. On observera que par la méthode du théorème 1 ci-dessus, il serait facile de démontrer l'existence d'une hyperalgèbre *libre abélienne* à n générateurs et à loi canonique, si l'on ne connaissait pas déjà cette hyperalgèbre (qui, on le sait, est l'hyperalgèbre du produit de n groupes hyperexponentiels ([8], prop. 3)).

15. Dans le théorème 2, il faut effectuer au préalable un isomorphisme de $\mathfrak{G}$ sur une autre hyperalgèbre $\overline{\mathfrak{G}}$ pour pouvoir avoir (27) pour tout

---

([8]) Pour que ceci soit tout à fait correct, il faut prolonger $\mathbf{q}^{(r+1)}$ à tout $\mathfrak{G}$. Le plus simple est sans doute de raisonner par « dualité » sur les groupes formels correspondants. L'isomorphisme $\mathbf{q}^{(r+1)}$ a pour transposé un isomorphisme sur $\mathfrak{o}/\mathfrak{u}_{r+1}$ (notations du n° 4) d'une algèbre analogue $\mathfrak{o}'/\mathfrak{u}'_{r+1}$, isomorphisme qui provient d'un « changement de variables » $x'_i = u_i((x_j))$ où les seconds membres peuvent être considérés comme des polynomes de degré $< p^{r+1}$ par rapport à chaque x_j, et où l'on remplace par zéro tous les monomes par rapport aux x_j contenant un $x_j^{p^{r+1}}$. Le prolongement de $\mathbf{q}^{(r+1)}$ correspondra au *même* « changement de variables », mais faisant passer de l'anneau de séries formelles $\mathfrak{o}'$ à l'anneau de séries formelles $\mathfrak{o}$.

indice α dans $\mathbf{N}^J$. Nous allons maintenant construire une autre hyperalgèbre libre pour laquelle ce passage ne sera pas nécessaire.

Désignons par P l'ensemble des suites $\omega = (\omega_1, \ldots, \omega_n) \in \mathbf{N}^J$ qui *ne sont pas multiples de p;* à chacun de ces $\omega \in P$ nous associerons une suite infinie $(U_{k,\omega})$ $(k \in \mathbf{N}, \omega \in P)$ et nous écrirons encore U_{ki} au lieu de U_{k,ε_i} $(1 \leqq i \leqq n)$. Soit E la réunion de toutes ces suites $(U_{k,\omega})$; on forme une base d'alternants de $\mathfrak{L}(E)$ par le même procédé qu'au n° 6, à cela près que les U_{ki} sont remplacés par les $U_{k,\omega}$. Désignons encore ces alternants par $T_{k,\mu}$, où μ parcourt un ensemble M bien ordonné de façon quelconque; on peut encore supposer que $P \subset M$ et $T_{k,\omega} = U_{k,\omega}$ lorsque $\omega \in P$. On définit ensuite un poids π pour tout monome de $\mathfrak{T}(E)$ en posant

$$\pi(U_{k,\omega}) = p^k d(\omega) \qquad \text{et} \qquad \pi(XY) = \pi(X) + \pi(Y),$$

de sorte que les alternants $T_{k,\mu}$ sont isobares.

Cela étant, nous allons définir une base formée d'éléments isobares de $\mathfrak{T}(E)$ pour laquelle $\mathfrak{T}(E)$ sera encore une *hyperalgèbre correspondant à l'ensemble d'indices* $R = M \times \mathbf{N}$. La construction étant très analogue à celle qui a été exposée en détail aux n^{os} 7-11, nous en donnerons seulement les grandes lignes. Les notations étant les mêmes qu'au n° 7, la construction du bourgeon tronqué $\mathfrak{t}_{m+1}$ n'est en rien modifiée. On définit ensuite l'homomorphisme F de $\mathfrak{T}(E)$ dans $\overline{\mathfrak{w}}_{m+1}$ en posant $F(U_{k,\omega}) = \overline{W}_{k,\omega} = \overline{U}_{k,\omega}$ pour $k \geqq 1$ et $p^k d(\omega) \leqq m+1$ et pour $k = 0$ et $d(\omega) < m+1$, et $F(U_{k,\omega}) = 0$ pour $p^k d(\omega) > m+1$ et pour $k = 0$ et $d(\omega) = m+1$. On passe au quotient et l'on obtient un homomorphisme f de $\mathfrak{t}_{m+1}$ dans $\overline{\mathfrak{w}}_{m+1}$. On montre comme au n° 10 que $f(\mathfrak{u}_{m+1}) = \overline{\mathfrak{w}}_{m+1}$, en choisissant les W_α de poids $m+1$ tels que $f(W_\alpha) = \overline{W}_\alpha$; ce choix comporte un certain arbitraire, et si $\alpha = p^k \varepsilon_\omega$ $(\omega \in P)$ on prend $W_{k,\omega} = U_{k,\omega}$ $(k \geqq 1)$. Pour choisir les $W_{0,\rho}$ tels que $\pi(\rho) = m+1$, il faut prendre une base de $\mathfrak{r}_{m+1}$; par construction, si $\omega \in P$ et $d(\omega) = m+1$, on a $fU_{(0,\omega)} = 0$, donc les $U_{0,\omega}$ appartiennent à $\mathfrak{r}_{m+1}$, et l'on prendra les $W_{0,\rho}$ pour $\pi(\rho) = m+1$ tels que $W_{0,\omega} = U_{0,\omega}$ si $\omega \in P$ et $d(\omega) = m+1$ (ce qui est possible puisque les $U_{k,\omega}$ sont linéairement indépendants par définition).

Resté à définir les V'_α pour $\pi(\alpha) = m+1$; les $a_{\alpha\lambda}$ étant définis par (15), on définit encore V'_α par la formule (16) (pour α distinct des ε_ρ), *sauf* si $\alpha = \omega \in P$ [et $\pi(\omega) = d(\omega) = m+1$], auquel cas on prend

$$V'_\omega = W_{0,\omega} + \sum_\lambda a_{\alpha\lambda} W_\lambda. \tag{36}$$

Il est immédiat, par le même raisonnement qu'au n° 11, que la base (V'_α) ainsi définie détermine une structure de bourgeon tronqué sur $\mathfrak{t}_{m+1}$, ce qui achève la démonstration. On notera que, par construction, dans l'expression des V_α comme combinaison linéaire des W_λ, il ne figure *aucune dérivation* $W_{0,\omega}$ si α n'appartient pas à P; si $\alpha = \omega \in P$, $V_{\varepsilon_i} = U_{0i}$ est une dérivation

(pour $1 \leq i \leq n$), et, pour $d(\omega) > 1$, la *seule* dérivation figurant dans V_ω est $W_{0,\omega} = V_{\varepsilon_\omega}$ avec le coefficient 1.

Pour tout entier $r > 0$, désignons par $\mathfrak{m}_r$ la sous-algèbre (libre) de $\mathfrak{T}(E)$ engendrée par les $U_{k,\omega}$ tels que $p^k d(\omega) \leq r$; une base de $\mathfrak{m}_r$ est formée des S_α qui ne contiennent que les facteurs $T^{p^h}_{k,\mu}$ provenant d'alternants $T_{k,\mu}$ qui ne contiennent que des $U_{l,\omega}$ pour lesquels $p^l d(\omega) \leq r$; désignons par A_r l'ensemble des indices $\alpha \in \mathbf{N}^{(\mathbf{R})}$ correspondants; les relations $\alpha \in A_r$ et $\beta \leq \alpha$ entrainent encore $\beta \in A_r$. On montre comme au n° 11 qu'on peut prendre la base structurale (V_α) de telle sorte que les V_α tels que $\alpha \in A_r$ forment une *base* de $\mathfrak{m}_r$ pour tout $r > 0$, à cela près que ce qui est désigné par r au n° 11 doit être ici remplacé par p^r; il faut simplement noter que, par définition, si $d(\omega) = r = m + 1$, $U_{0,\omega}$ appartient à $\mathfrak{r}_{m+1,r}$ et non à $\mathfrak{r}_{m+1,r-1}$, et par suite on peut prendre une base d'un supplémentaire de $\mathfrak{r}_{m+1,r-1}$ par rapport à $\mathfrak{r}_{m+1,r} = \mathfrak{r}_{m+1}$ qui contient les $U_{0,\omega}$ tels que $d(\omega) = r = m + 1$.

Dans ces conditions, pour tout $\omega \in P$, dans l'expression de V_ω comme combinaison linéaire des W_λ, *tous les termes sauf* $U_{0,\omega}$ *appartiennent à* $\mathfrak{m}_{r-1}$, où $r = d(\omega)$. En effet, comme $\mathbf{p}'(V_\omega) = 0$ puisque ω n'est pas multiple de p, il ne peut figurer dans V_ω aucun terme W_λ où λ soit multiple de p. Les seuls termes du premier degré parmi les W_λ sont donc de la forme $W_{0,\rho}$ avec $\pi(\rho) = \pi(\omega) = d(\omega) = r$, et l'on a vu plus haut que le seul terme de cette forme figurant dans V_ω est $U_{0,\omega}$. Quant aux termes W_λ qui ne sont pas du premier degré par rapport aux $U_{k',\omega'}$, ils appartiennent nécessairement à $\mathfrak{m}_{r-1}$ puisqu'ils sont produits d'au moins deux facteurs de poids $\leq r - 1 = \pi(\omega) - 1$, et ne peuvent par suite contenir que des $U_{k',\omega'}$ tels que $p^{k'} d(\omega') \leq r - 1$.

Montrons maintenant de même que, pour tout $k \geq 1$, dans l'expression de $V_{p^k\omega}$ comme combinaison linéaire des W_λ, *tous les termes sauf* $U_{k,\omega}$ *appartiennent à* $\mathfrak{m}_{r-1}$, où $r = p^k d(\omega)$. Il suffit de raisonner par récurrence sur k, puisqu'on vient de démontrer la proposition pour $k = 0$. Or, les seuls W_λ qui soient du premier degré par rapport aux $U_{k',\omega'}$, et dont l'image par l'homomorphisme de Frobenius $\mathbf{p}'$ soit nulle, sont les termes de la forme $W_{0,\varrho}$, et l'on a vu plus haut qu'il ne figure aucun terme de cette forme dans $V_{p^k\omega}$ si $k \geq 1$. Comme $\mathbf{p}'(V_{p^k\omega}) = V_{p^{k-1}\omega}$, l'hypothèse de récurrence prouve que $V_{p^{k-1}\omega}$ est somme de $U_{k-1,\omega}$ et de termes appartenant à $\mathfrak{m}_{s-1}$, où $s = p^{k-1} d(\omega)$. On en conclut que $V_{p^k\omega}$ est somme de $U_{k,\omega}$, de termes appartenant à $\mathfrak{m}_{p(s-1)} \subset \mathfrak{m}_{ps-1}$, et de termes W_λ dont l'indice n'est pas divisible par p. Comme aucun de ces derniers ne peut être du premier degré par rapport aux $U_{k',\omega'}$, on voit comme ci-dessus que tous ces termes sont dans $\mathfrak{m}_{ps-1}$, ce qui prouve notre assertion. Avec le même abus de notation qu'au n° 11, désignons par $\mathfrak{f}_n(\mathbf{F}_p)$ l'hyperalgèbre définie en prenant dans $\mathfrak{T}(E)$ une base structurale (V_α) satisfaisant aux conditions précédentes, et par $\mathfrak{f}_n(K)$ l'hyperalgèbre de même base obtenue en étendant à K le corps des scalaires; nous dirons que $\mathfrak{f}_n(K)$ est *une hyperalgèbre (sur* K) *à loi de composition non canonique engendrée par les* $U_{k,\omega}$.

16. Il est maintenant facile de démontrer la propriété « universelle » de l'hyperalgèbre $\mathfrak{f}_n(K)$:

THÉORÈME 3. — *Soient $\mathfrak{A}$ une algèbre associative sur K, (Z_α) un système de générateurs de $\mathfrak{A}$, ayant $\mathbf{N}^J$ comme ensemble d'indices. Il existe alors un homomorphisme et un seul $\mathbf{u}'$ de $\mathfrak{f}_n(K)$ sur $\mathfrak{A}$ tel que l'on ait*

$$\mathbf{u}'(V_\alpha) = Z_\alpha \tag{39}$$

pour tout $\alpha \in \mathbf{N}^J$.

Comme $\mathfrak{f}_n(K)$ est l'algèbre libre engendrée par les $U_{k,\omega}$, il suffit de définir $\mathbf{u}'(U_{k,\omega})$; raisonnons par récurrence sur le poids $p^k d(\omega) = r$. On vient de voir au n° 15 que l'on peut écrire

$$U_{k,\omega} = V_{p^k\omega} - \sum_\lambda a_{\omega\lambda} W_\lambda,$$

où les W_λ appartiennent tous à $\mathfrak{m}_{r-1}$. En vertu de l'hypothèse de récurrence, les $\mathbf{u}'(W_\lambda)$ sont donc déjà déterminés, et l'on posera

$$\mathbf{u}'(U_{k,\omega}) = Z_{p^k\omega} - \sum_k a_{\omega\lambda}\, \mathbf{u}'(W_\lambda),$$

ce qui détermine donc l'homomorphisme $\mathbf{u}'$ de façon à satisfaire (39) pour tout $\alpha \in \mathbf{N}^J$.

17. Les cas les plus intéressants sont ceux où il existe un homomorphisme M de $\mathfrak{A}$ dans l'algèbre $\mathfrak{A} \otimes \mathfrak{A}$ satisfaisant aux conditions

$$M(Z_\alpha) = \sum_{0 \leq \beta \leq \alpha} Z_\beta \otimes Z_{\alpha-\beta} \tag{40}$$

pour tout $\alpha \in \mathbf{N}^J$. Le fait que (V_α) soit une base structurale pour $\mathfrak{f}_n(K)$ entraîne alors que l'on a

$$(\mathbf{u}' \otimes \mathbf{u}')(M(V)) = M(\mathbf{u}'(V)) \tag{41}$$

pour tout $V \in \mathfrak{f}_n(K)$, en désignant par M l'application structurale de $\mathfrak{f}_n(K)$ dans $\mathfrak{f}_n(K) \otimes \mathfrak{f}_n(K)$. En particulier, si $\mathfrak{A}$ est une hyperalgèbre de base structurale (Z_α), $\mathbf{u}'$ sera un *homomorphisme d'hyperalgèbre.*

On a aussi un homomorphisme canonique $\mathbf{u}'$ de $\mathfrak{f}_n(K)$ sur $\mathfrak{H}_n(K)$ par application du théorème 3; en considérant la sous-algèbre (libre) de $\mathfrak{f}_n(K)$ engendrée par les U_{ki} $(1 \leq i \leq n,\ k \geq 0)$, on voit facilement, par un raisonnement de récurrence analogue à ceux des nos 11 et 15, que l'on peut choisir la base structurale de $\mathfrak{f}_n(K)$ [une fois celle de $\mathfrak{H}_n(K)$ déterminée] de sorte que l'homomorphisme $\mathbf{u}'$ soit tel que

$$\mathbf{u}'(U_{ki}) = U_{ki} \qquad \text{et} \qquad \mathbf{u}'(U_{k,\omega}) = 0$$

pour les $\omega \in P$ distincts de ε_i $(1 \leq i \leq n)$.

Enfin, un autre type assez fréquent d'algèbre $\mathfrak{A}$ à laquelle il semble intéressant d'appliquer le théorème 3 est obtenu de la façon suivante. Soient $\mathfrak{U}$ une algèbre sur K ayant un élément unité, $\mathfrak{E}$ l'algèbre des endomorphismes de l'espace vectoriel $\mathfrak{U}$. Soit $\mathfrak{A}$ une sous-algèbre de $\mathfrak{E}$, engendrée par un système de générateurs (Z_α), où $\alpha \in \mathbf{N}^J$. On peut donc définir un homomorphisme $\mathbf{u}'$ de $\mathcal{L}_n(K)$ sur $\mathfrak{A}$ vérifiant (39). Supposons maintenant, que, pour tout $\alpha \in \mathbf{N}^J$, on ait, quels que soient x, y dans $\mathfrak{U}$

$$Z_\alpha(xy) = \sum_{0 \leq \beta \leq \alpha} Z_\beta(x)\, Z_{\alpha-\beta}(y). \tag{42}$$

Soit alors V un élément quelconque de $\mathcal{L}_n(K)$, et soit $Z = \mathbf{u}'(V)$; si

$$M(V) = \sum_{\lambda,\mu} c_{\lambda\mu}\, V_\lambda \otimes V_\mu,$$

on conclut de (42) et du fait que M est l'application structurale, que l'on a, en posant $Z_\lambda = \mathbf{u}'(V_\lambda)$ pour *tout* $\lambda \in \mathbf{N}^{(R)}$,

$$Z(xy) = \sum_{\lambda,\mu} c_{\lambda\mu}\, Z_\lambda(x)\, Z_\mu(y). \tag{43}$$

De cette remarque, on conclut aussitôt par exemple que les éléments $\mathbf{u}'(V_{\varepsilon_\xi})$ dans $\mathfrak{A}$ sont des *dérivations* de l'algèbre $\mathfrak{U}$; par récurrence sur k, tout X de la forme $\mathbf{u}'(V_{p^k\varepsilon_\xi})$ est une « semi-dérivation de hauteur k » dans $\mathfrak{U}$, c'est-à-dire que l'on a

$$X(x^{p^k}y) = X(x^{p^k})y + x^{p^k}X(y), \qquad X(yx^{p^k}) = y\,X(x^{p^k}) + X(y)\,x^{p^k},$$

tandis que les Y de la forme $\mathbf{u}'(V_\alpha)$, où $h(\alpha) < k$, sont des « semi-dérivations spéciales de hauteur k », autrement dit satisfont à

$$Y(x^{p^k}y) = x^{p^k}Y(y), \qquad Y(yx^{p^k}) = Y(y)\,x^{p^k}.$$

Un exemple d'algèbre $\mathfrak{A}$ du type précédent qui joue un rôle important en topologie algébrique est l'*algèbre de Steenrod* A_p, qui peut être considérée comme algèbre d'endomorphismes de l'algèbre de cohomologie $H^*(U; \mathbf{F}_p)$, où U est un espace topologique convenable [4]; on a ici $n = 1$, et les générateurs de A_p se notent P_p^k ou simplement P^k, k parcourant l'ensemble des entiers $\geqq 0$ (on écrit Sq^k pour $p = 2$). J. ADEM [1], [2] et H. CARTAN [4] ont déterminé explicitement les relations entre ces générateurs; mais ces relations ne font pas apparaître la structure « hyperalgébrique » de A_p qui résulte des identités (42), et il faudrait pour cela déterminer explicitement les éléments $\mathbf{u}'(V_{p^k\varepsilon_\xi})$ dans A_p.

18. Les résultats qui précèdent ont naturellement leurs analogues (consi-

dérablement simplifiés) sur un corps K de caractéristique zéro; les U_{kt} (resp. $U_{k,\omega}$) disparaissent alors pour $k \geqq 1$, ainsi que les $T_{0,\mu}^{p^h}$, et les théorèmes 1 et 2 sont essentiellement bien connus. On peut alors écrire T_μ au lieu de $T_{0,\mu}$, les T_μ formant une base de l'algèbre de Lie libre $\mathfrak{L}(E)$ engendrée par $U_1, U_2, \ldots, U_n$ (on supprime là aussi l'indice zéro), $\mathfrak{H}_n(K)$ est alors l'algèbre enveloppante de $\mathfrak{L}(E)$, et pour tout $\alpha = (\alpha_\mu) \in \mathbf{N}^{(M)}$, on a ([7], prop. 3)

$$V_\alpha = \frac{1}{\alpha!} T_{\sigma_1}^{\nu_1} T_{\sigma_2}^{\nu_2} \ldots T_{\sigma_m}^{\nu_m} = \frac{W_\alpha}{\alpha!}, \tag{44}$$

où $\sigma_1 < \sigma_2 < \ldots < \sigma_m$ est la suite des indices $\mu \in M$ tels que $\alpha_\mu \neq 0$, rangés par ordre croissant, et où l'on a posé

$$\nu_j = \alpha_{\sigma_j} \quad \text{et} \quad \alpha! = \prod_\mu \alpha_\mu !.$$

On obtient une expression analogue pour les éléments V_ω de la base structurale de $\mathfrak{F}_n(K)$; bornons-nous au cas $n = 1$. Alors $\mathfrak{F}_1(K)$ est l'algèbre enveloppante de l'algèbre de Lie libre $\mathfrak{L}(E)$ engendrée par U_1 et les éléments V_{ε_k}, où k (qui remplace le ω du n° 15) parcourt ici l'ensemble des entiers $\geqq 2$; on peut identifier U_1 (resp. V_{ε_k}) à un élément de la base de $\mathfrak{L}(E)$, qu'on notera T_1 (resp. T_k) (ce qui revient à supposer que l'ensemble d'indices M de la base (T_μ) de $\mathfrak{L}(E)$ contient l'ensemble P des entiers $\geqq 1$). On vérifie alors facilement (9) que, pour tout entier $k \geqq 1$, l'élément $V_{k\varepsilon_1}$, que nous écrirons V_k, est donné par

$$V_k = \sum_\alpha \frac{1}{\alpha!} W_\alpha, \tag{45}$$

où la somme est étendue aux suites $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots) \in \mathbf{N}^{(P)}$ de poids $\pi(\alpha) = \sum_n n\alpha_n = k$, avec

$$W_\alpha = T_1^{\alpha_1} T_2^{\alpha_2} \ldots T_n^{\alpha_n} \ldots \quad \text{(nombre fini de facteurs)}.$$

Il revient au même de dire que V_k est la somme des termes de poids k dans le développement du produit (non commutatif)

$$(\exp T_1)(\exp T_2)\ldots(\exp T_n).$$

Nous allons utiliser le théorème 3 (pour un corps K de caractéristique zéro) pour retrouver par une voie nouvelle la *formule de Hausdorff*; cela

(9) L'exposé qui suit dans ce numéro est très schématique et ne prétend pas à une parfaite rigueur; pour voir comment on peut faire les démonstrations dans le détail, voir les nos 19-21, où cela est fait dans le cas (nettement plus compliqué) de caractéristique $p > 0$.

nous montrera comment cette formule peut se généraliser aux corps de caractéristique > 0.

Dans l'algèbre $\mathfrak{H}_2(K)$, considérons, pour tout $k \geqq 1$, l'élément

$$Z_k = \sum_{\alpha} V_\alpha,$$

la somme étant étendue aux $\alpha = (\alpha_1, \alpha_2) \in \mathbf{N}^2$ tels que $\pi(\alpha) = \alpha_1 + \alpha_2 = k$. L'homomorphisme structural N de $\mathfrak{H}_2(K)$ dans $\mathfrak{H}_2(K) \otimes \mathfrak{H}_2(K)$ est tel alors que

$$N(Z_k) = \sum_{0 \leq h \leq k} Z_h \otimes Z_{k-h} \tag{46}$$

comme il résulte aussitôt de la définition de Z_k, car des relations

$$N(V_\alpha) = \sum_{0 \leq \beta \leq \alpha} V_\beta \otimes V_{\alpha-\beta},$$

il résulte que $N(Z_k) = \sum_{\lambda, \mu} V_\lambda \otimes V_\mu$, où (λ, μ) parcourt tous les couples d'éléments de $\mathbf{N}^2$ tels que $\pi(\lambda) + \pi(\mu) = k$. D'après le théorème 3, il existe un homomorphisme $\mathfrak{u}'$ de $\mathfrak{f}_1(K)$ sur la sous-algèbre de $\mathfrak{H}_2(K)$ engendrée par les Z_k et tel que $\mathfrak{u}'(V_k) = Z_k$ pour tout $k \geqq 1$; en outre, en raison de (46), $\mathfrak{u}'$ est un homomorphisme d'hyperalgèbre, et en particulier transforme toute dérivation en dérivation, autrement dit en un élément de l'algèbre de Lie libre engendrée par U_1 et U_2. Cela étant, les formules (44) montrent que Z_k est la somme des termes de degré k dans le produit $(\exp U_1)(\exp U_2)$. Si l'on pose $Y_k = \mathfrak{u}'(T_k)$ qui est, comme nous venons de le remarquer, une *dérivation*, on voit que l'on peut écrire la formule

$$(\exp U_1)(\exp U_2) = (\exp Y_1)(\exp Y_2) \dots (\exp Y_n) \dots \tag{47}$$

dont on calcule facilement les premiers termes Y_i

$$Y_1 = U_1 + U_2,$$

$$Y_2 = \frac{1}{2}[U_1, U_2],$$

$$Y_3 = \frac{1}{3}[U_2, [U_2, U_1]] - \frac{1}{6}[U_1, [U_1, U_2]],$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

Ceci n'est pas encore la formule de Hausdorff, mais une formule analogue, pour les groupes de Lie, à la formule de Ph. Hall pour les groupes quelconques ([10], p. 51). Pour obtenir la formule de Hausdorff, observons qu'on peut opérer de la même manière que ci-dessus en remplaçant $\mathfrak{H}_2(K)$ par $\mathfrak{H}_m(K)$,

où m est un entier > 0 quelconque. Mais on a même une formule semblable en remplaçant $\mathfrak{H}_2(K)$ par $\mathfrak{H}_\infty(K)$, algèbre libre engendrée par une infinité dénombrable de générateurs $U_1, U_2, \ldots, U_n, \ldots$; il faut alors prendre

$$Z_k = \sum_\alpha V_\alpha$$

la somme (infinie formelle) étant étendue aux $\alpha = (\alpha_i) \in \mathbf{N}^{(\mathbf{P})}$ tel que $\sum_{i=1}^{\infty} \alpha_i = k$; on obtient la formule

$$(48) \quad (\exp U_1)(\exp U_2)\ldots(\exp U_n)\ldots = (\exp \Phi_1)(\exp \Phi_2)\ldots(\exp \Phi_n)\ldots,$$

où Φ_n est une somme (infinie formelle) d'alternants de degré total n par rapport aux U_i

$$\Phi_1 = U_1 + U_2 + \ldots + U_n + \ldots,$$
$$\Phi_2 = \frac{1}{2}\sum_{i<j}[U_i, U_j],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

On peut alors *itérer* la formule (48) en remplaçant dans chaque alternant figurant dans Φ_n, chacun des U_i par $\Phi_i(U_1, \ldots, U_n, \ldots)$; le degré de Φ_n par rapport aux U_i augmentant indéfiniment avec n, on obtient ainsi des sommes ayant un sens, car il n'y a qu'un nombre fini d'alternants par rapport aux Φ_i qui sont de dégré inférieur à un entier donné, par rapport aux U_i. On continue ainsi indéfiniment, et après la $k^{\text{ième}}$ opération, on obtient

$$(49) \quad (\exp U_1)(\exp U_2)\ldots(\exp U_n)\ldots = (\exp \Phi_1^{(k)})(\exp \Phi_2^{(k)})\ldots(\exp \Phi_n^{(k)})\ldots,$$

avec

$$\Phi_1^{(k)} = \Phi_1^{(k-1)} + \Phi_2^{(k-1)} + \ldots + \Phi_n^{(k-1)} + \ldots,$$
$$\Phi_2^{(k)} = \frac{1}{2}\sum_{i<j}[\Phi_i^{(k-1)}, \Phi_j^{(k-1)}],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

d'où résulte sans peine que $\Phi_n^{(k)}$, pour $n \geqq 2$, est une somme d'alternants par rapport aux U_i, de degré au moins égal à $n + k - 1$; en outre, pour tout entier $m > n + k - 1$, $\Phi_n^{(k)}$ ne contient qu'un nombre fini d'alternants de degré $\leqq m$ par rapport aux U_i. Il est clair dans ces conditions que les termes de $\Phi_1^{(k)}$ de degré $\leqq k$ sont les mêmes que dans tous les $\Phi_1^{(k+h)}$, $h > 0$; désignant par $\Phi_1^{(\infty)}$ la somme dont les termes de degré $\leqq k$ sont ceux de $\Phi_1^{(k)}$ pour tout $k \geqq 1$, on voit qu'on a aussi

$$(50) \qquad (\exp U_1)(\exp U_2)\ldots(\exp U_n)\ldots = \exp(\Phi_1^{(\infty)}),$$

ce qui est la *formule de Hausdorff* générale (la formule usuelle s'obtenant en remplaçant tous les U_i d'indice $i \geqq 3$ par 0).

19. Voyons maintenant comment on peut procéder de même lorsque K est de caractéristique $p > 0$. Remarquons tout d'abord que la manière dont on a bien ordonné l'ensemble $\mathbf{N} \times M \times \mathbf{N} = \mathbf{N} \times R$ au n° 6 est sans aucune importance pour la démonstration des théorèmes 1, 2 et 3 (mais bien entendu, l'expression des S_α, des W_α et des V_α comme somme de monomes par rapport aux U_{ki} dépend essentiellement de cet ordre). Soit M_i la partie de M formée des indices μ tels que l'alternant $T_{k,\mu}$ (notations du n° 6) ne contienne que les U_{hi} ($0 \leqq h < +\infty$); les éléments $T^h_{k,\mu}$ où μ parcourt M_i, forment évidemment la base de la p-algèbre de Lie libre $\mathfrak{L}_p(U_{0i}, U_{1i}, \ldots, U_{ki}, \ldots)$ engendrée par les U_{ki}; nous prendrons un bon ordre dans M_i, et l'on peut évidemment supposer établie entre M_i et M_j ($j \neq i$) une correspondance biunivoque $\mu_i \leftrightarrow \mu_j$, de sorte que l'alternant T_{k,μ_j} se déduise de T_{k,μ_i} en remplaçant chacun des U_{hi} figurant dans ce dernier par l'élément U_{hj} correspondant; en outre, on peut supposer que cette correspondance biunivoque conserve l'ordre des indices dans M_i et M_j. Soit $R_i = M_i \times \mathbf{N}$; on prendra dans chaque R_i l'ordre lexicographique. Cela étant, M est réunion des M_i ($1 \leqq i \leqq n$) et d'un ensemble M'; on prendra sur $R' = M' \times \mathbf{N}$ l'ordre lexicographique, et sur R l'ordre qui en fait la *somme ordinale* des ensembles $R_1, R_2, \ldots, R_n, R'$ pris dans cet ordre.

Reprenons les notations du théorème 1, et pour $1 \leqq i \leqq n$, désignons par $\mathfrak{T}_i(E)$ la sous-algèbre (libre) de $\mathfrak{T}(E)$ engendrée par les U_{ki} ($k \geqq 0$). Supposons que, pour $n = 1$, on ait fixé la base structurale dans $\mathfrak{H}_1(K)$; on peut alors utiliser l'arbitraire dont on dispose dans le choix de la base structurale de $\mathfrak{T}(E)$ de façon à satisfaire à la condition suivante : si un indice $\alpha_i \in \mathbf{N}^{(R_i)}$ correspond à un indice $\alpha_1 \in \mathbf{N}^{(R_1)}$ dans la correspondance biunivoque établie entre R_1 et R_i, alors V_{α_i} s'obtient en remplaçant, dans l'expression de V_{α_1} comme combinaison linéaire de monomes en $U_{01}, U_{11}, \ldots, U_{k1}, \ldots$, chacun des U_{k1} par l'élément U_{ki} correspondant. Ceci se voit sans peine en reprenant la construction des V_α décrite dans la démonstration du théorème 1 et en raisonnant par récurrence sur le poids m : on montre ainsi d'abord que si $\alpha_i, \beta_i, \gamma_i$ dans $\mathbf{N}^{(R_i)}$ correspondent respectivement à $\alpha_1, \beta_1, \gamma_1$ dans $\mathbf{N}^{(R_1)}$, on a

$$\overline{d}(\alpha_i, \beta_i, \gamma_i) = \overline{d}(\alpha_1, \beta_1, \gamma_1),$$

et que le sous-espace $\mathfrak{r}_{m+1} \cap \mathfrak{T}_i(E)$ se déduit de $\mathfrak{r}_{m+1} \cap \mathfrak{T}_1(E)$ en substituant à chaque U_{k1} l'élément U_{ki} dans les combinaisons linéaires de monomes qui appartiennent à $\mathfrak{r}_{m+1} \cap \mathfrak{T}_1(E)$; on choisit alors chacun des éléments de base W_{0,ρ_i} ($\pi(\rho_i) = m + 1$, $\rho_i \in R_i$) de $\mathfrak{r}_{m+1} \cap \mathfrak{T}_i(E)$ de sorte qu'il se déduise de W_{0,ρ_1} par la correspondance précédente, si $\rho_1 \in R_1$ est l'indice correspondant à ρ_i. Le choix des $W_{0,\rho'}$ pour $\rho' \in R'$ demeure arbitraire, sous les seules restrictions fixées au n° 11.

Cela étant, soit $\alpha = (\beta_1, \beta_2, \ldots, \beta_n)$ un indice de $\mathbf{N}^{(R)}$ n'ayant *aucune composante non nulle dans* R′, et où β_i appartient à $\mathbf{N}^{(R_i)}$; montrons qu'avec les conventions précédentes, on a la relation

$$V_\alpha = V_{\beta_1} V_{\beta_2} \ldots V_{\beta_n}. \tag{53}$$

Il suffit évidemment, par récurrence sur i, de prouver que

$$V_{(\beta_1, \ldots, \beta_{i-1})} V_{\beta_i} = V_{(\beta_1, \ldots, \beta_i)} \tag{54}$$

et, une fois i fixé, de démontrer (54) par récurrence sur le poids $m = \pi(\beta_1) + \ldots + \pi(\beta_i)$. Posons $\gamma = (\beta_1, \ldots, \beta_{i-1})$; on peut évidemment se borner au cas où γ et β_i sont tous deux > 0, sans quoi la formule (54) est triviale. Notons, en outre, que si $\xi \leq \gamma$ (resp. $\eta \leq \beta_i$), on a nécessairement $\xi = (\xi_1, \ldots, \xi_{i-1})$, où $\xi_k \in \mathbf{N}^{(R_k)}$ et $\eta \in \mathbf{N}^{(R_i)}$; la formule (12), où l'on remplace α par γ et β par β_i, montre que si $\lambda > 0$, $\lambda' > 0$, le second membre est nul sauf si $\lambda + \lambda' = (\beta_1, \ldots, \beta_i)$, cas où il est égal à 1. Dans le bourgeon tronqué $\bar{\mathfrak{t}}_{m+1}$, on a donc bien

$$\overline{V}_{(\beta_1, \ldots, \beta_i)} = \overline{V}_{\beta_1} \overline{V}_{\beta_2} \ldots \overline{V}_{\beta_i};$$

si l'on pose $\overline{V}_{\beta_k} = \sum_{\lambda_k} c(\beta_k, \lambda_k) \overline{W}_{\lambda_k}$, où λ_k appartient à $\mathbf{N}^{(R_k)}$ ($1 \leq k \leq i$), on a donc

$$\overline{V}_{(\beta_1, \ldots, \beta_i)} = \Sigma c(\beta_1, \lambda_1) \ldots c(\beta_i, \lambda_i) \overline{W}_{\lambda_1} \overline{W}_{\lambda_2} \ldots \overline{W}_{\lambda_i}.$$

Mais, en raison du choix de l'ordre dans R, on a

$$\overline{W}_{(\lambda_1, \lambda_2, \ldots, \lambda_i)} = \overline{W}_{\lambda_1} \overline{W}_{\lambda_2} \ldots \overline{W}_{\lambda_i}$$

et la définition des V_α dans $\mathfrak{t}_{m+1}$ donne donc

$$V_{(\beta_1, \ldots, \beta_i)} = \Sigma c(\beta_1, \lambda_1) \ldots c(\beta_i, \lambda_i) W_{\lambda_1} W_{\lambda_2} \ldots W_{\lambda_i} = V_{\beta_1} V_{\beta_2} \ldots V_{\beta_i}$$

en vertu de l'hypothèse de récurrence, ce qui prouve (54).

Posons

$$E(U_{01}, U_{11}, \ldots, U_{k1}, \ldots) = \sum_{k=0}^{\infty} V_{k\varepsilon_1}, \tag{55}$$

série formelle que l'on peut considérer comme un élément de $\mathfrak{H}_1(K)$ complété. Les considérations précédentes et la formule (53) montrent que le produit

$$E(\mathbf{U}_1) E(\mathbf{U}_2) \ldots E(\mathbf{U}_n), \tag{56}$$

où l'on a posé $\mathbf{U}_i = (U_{0i}, U_{1i}, \ldots, U_{ki}, \ldots)$ pour abréger, est la *somme de tous les* V_α, où α parcourt les indices de la forme $k_1\varepsilon_1 + \ldots + k_n\varepsilon_n$, chacun des k_i parcourant $\mathbf{N}$.

20. Nous allons maintenant préciser de la même manière le choix d'une base structurale dans $\mathfrak{f}_1(K)$ (n° 15). Comme ici J est réduit à un seul élément, P est l'ensemble des entiers *m premiers à p*; on écrira $\overline{U}_{km}$ au lieu de $U_{k,\omega}$ et en particulier $\overline{U}_{k1}$ au lieu de U_{k1}. Désignons encore par M_m la partie de M formée des indices μ tels que l'alternant $T_{k,u}$ ne conttenne que les $\overline{U}_{hm}$ ($0 \leq h < +\infty$). Procédant comme au n° 19, prenons un bon ordre sur chacun des M_m, avec une correspondance biunivoque $\mu_m \leftrightarrow \mu_q$ conservant l'ordre entre M_m et M_q, telle que T_{k,μ_q} se déduise de T_{k,μ_m} par substitution de $\overline{U}_{hq}$ à $\overline{U}_{hm}$ dans son expression (pour tout $h \geq 0$). Soit $R_m = M_m \times \mathbf{N}$, muni de l'ordre lexicographique; soit M′ le complémentaire dans M de la réunion des M_m, qu'on munit d'un bon ordre arbitraire, et soit $R' = M' \times \mathbf{N}$, ordonné lexicographiquement. Enfin, soit $[m(1) = 1, m(2), \ldots, m(n), \ldots]$ la suite des entiers m premiers à p, rangés par ordre strictement croissant; on prend sur R l'ordre qui en fait la *somme ordinale* des ensembles $R_{m(1)}$, $R_{m(2)}, \ldots, R_{m(n)}, \ldots$, R′ pris dans cet ordre (de type ordinal $\omega + 1$). Comme au n° 19, on voit d'abord, en reprenant la construction de la base structurale (V_α) donnée au n° 15, que l'on peut utiliser l'arbitraire dont on dispose pour que la condition suivante soit vérifiée [en utilisant les notations surlignées pour les éléments de $\mathfrak{f}_1(K)$, afin de les distinguer de ceux de $\mathfrak{H}_n(K)$]: *pour tout* $m > 1$ dans P, si un indice $\alpha_m \in \mathbf{N}^{(R_m)}$ correspond à un indice $\alpha_1 \in \mathbf{N}^{(R_1)}$ par la correspondance biunivoque établie entre R_m et R_1, alors $\overline{V}_{\alpha_m}$ s'obtient en remplaçant, dans l'expression de V_{α_1} [dans $\mathfrak{H}_1(K)$] en fonction des U_{h1} ($h \geq 0$), chacun des U_{h1} par l'élément $\overline{U}_{hm}$ correspondant ($h \geq 0$).

Pour $\alpha_1 \in \mathbf{N}^{(R_1)}$, $\overline{V}_{\alpha_1}$ contient par contre des $\overline{U}_{hm}$ où $m > 1$, en vertu de la détermination de la base structurale de $\mathfrak{f}_1(K)$, et nous n'essaierons pas d'obtenir la forme générale de ces éléments; il nous suffira pour notre objet de déterminer les $\overline{V}_{k\varepsilon_1}$ pour tout $k \geq 1$. Désignons par $V'_{k\varepsilon_1}$ l'élément de $\mathfrak{f}_1(K)$ obtenu en substituant à chaque U_{h1} l'élément $\overline{U}_{h1}$ dans l'expression de $V_{k\varepsilon_1}$ [*dans* $\mathfrak{H}_1(K)$] à l'aide des U_{h1}. Nous allons prouver que l'on a

$$\overline{V}_{k\varepsilon_1} = \Sigma V'_{k_1\varepsilon_1} \overline{V}_{k_2\varepsilon_{m(2)}} \cdots \overline{V}_{k_n\varepsilon_{m(n)}}, \tag{58}$$

la somme étant étendue à tous les systèmes d'entiers $(k_1, \ldots, k_n)$ (n variable) tels que l'on ait $\sum_j k_j m(j) = k$. Il suffit de raisonner par récurrence sur k, puisque $\overline{V}_{\varepsilon_1} = \overline{U}_{01}$. Nous allons montrer tout d'abord que la différence des deux membres de (58) est une *dérivation*; il revient au même de prouver que les images des deux membres de (58) par l'application structurale diffèrent d'une expression de la forme $I \otimes Y + Y \otimes I$. Or, on a

$$\overline{V}''_{k\varepsilon_1} = \sum_{h=0}^{k} \overline{V}_{h\varepsilon_1} \otimes \overline{V}_{(k-h)\varepsilon_1}$$

et, de même,

$$V'^{0}_{k_1\varepsilon_1} = \sum_{h_1=0}^{k_1} V'_{h_1\varepsilon_1} \otimes V'_{(k_1-h_1)\varepsilon_1}$$

et

$$\overline{V}^{0}_{k_i\varepsilon_{m(i)}} = \sum_{h_i=0}^{k_i} \overline{V}_{h_i\varepsilon_{m(i)}} \otimes \overline{V}_{(k_i-h_i)\varepsilon_{m(i)}} \qquad (2 \leqq i \leqq n),$$

la seconde de ces relations résultant de la définition des $V'_{k\varepsilon_1}$ et de la relation analogue dans $\mathfrak{H}_1(K)$. Tenant compte de l'hypothèse de récurrence, notre assertion résulte des formules précédentes. Cela étant, on sait (n° **15**) que dans $\overline{V}_{k\varepsilon_1}$, il ne figure que la dérivation $\overline{W}_{0,k} = \overline{W}_{\varepsilon_k}$ (avec le coefficient 1) si k est premier à p, et aucune dérivation si k est multiple de p. D'autre part (n° **11**), il ne figure aucune dérivation dans $V'_{k\varepsilon_1}$ si $k > 1$, ni dans $\overline{V}_{k\varepsilon_{m,i)}}$ si $k > 1$ et $i > 1$. Mais, en vertu du choix de l'ordre sur R, pour tout $\alpha = (\beta_1, \beta_2, \ldots, \beta_n)$, ou $\beta_i \in \mathbf{N}^{(\mathbf{R}_{m,i)})}$, on a

$$\overline{W}_\alpha = \overline{W}_{\beta_1}\overline{W}_{\beta_2}\ldots\overline{W}_{\beta_n}, \tag{59}$$

D'autre part, $V'_{k\varepsilon_1}$ est par définition combinaison linéaire des $\overline{W}_{\alpha_1}$ où $\alpha_1 \in \mathbf{N}^{(\mathbf{R}_1)}$, et $\overline{V}_{k\varepsilon_{m,i)}}$ combinaison linéaire des $\overline{W}_{\alpha_i}$, où $\alpha_i \in \mathbf{N}^{(\mathbf{R}_{m,i)})}$. Utilisant la formule (59), on voit que les seules dérivations qui puissent figurer au second membre de (58) correspondent au cas où tous les k_j sauf un sont nuls, l'unique k_j non nul étant égal à 1 ; cela implique bien entendu que $k = m(j)$, donc $k \in \mathrm{P}$, et lorsqu'il en est ainsi, il n'y a au second membre que la seule dérivation $\overline{W}_{\varepsilon_k}$ avec le coefficient 1, ce qui achève de prouver (58).

On peut encore exprimer ce résultat de la façon suivante : considérons le produit infini

$$\mathrm{E}(\overline{\mathbf{U}}_1)\,\mathrm{E}(\overline{\mathbf{U}}_{m(2)})\ldots\mathrm{E}(\overline{\mathbf{U}}_{m(n)})\ldots, \tag{60}$$

où l'on a posé, comme plus haut

$$\overline{\mathbf{U}}_m = (\overline{\mathrm{U}}_{0m}, \overline{\mathrm{U}}_{1m}, \ldots, \overline{\mathrm{U}}_{km}, \ldots) \qquad \text{pour tout} \quad m \in \mathrm{P}.$$

On observera que dans $\mathrm{E}(\overline{\mathbf{U}}_m)$ tous les termes sauf le terme constant (égal à 1) sont de poids $\geqq m$. Par suite, dans le produit (60) il n'y a qu'un nombre fini de facteurs qui puissent donner des termes de poids $\leqq m$, et dans chaque facteur, il n'y a évidemment qu'un nombre fini de monomes de poids $\leqq m$. Le produit a donc un sens dans $\mathfrak{F}_1(\mathrm{K})$ complété pour la topologie définie par la filtration correspondant au poids. La formule (58) montre, en outre, que la série (60) n'est autre que la *somme de tous les* $\overline{V}_{k\varepsilon_1}$ $(0 \leqq k < +\infty)$ dans $\mathfrak{F}_1(\mathrm{K})$ complété.

21. Après ces préliminaires, nous pouvons développer le raisonnement esquissé dans le n° 18 pour la caractéristique o. Pour tout n fixé, et tout entier $k \geqq 0$, posons, dans $\mathfrak{H}_n(K)$

$$Z_k = \sum_{\alpha} V_{\alpha},$$

où α parcourt l'ensemble des éléments $k_1\varepsilon_1 + k_2\varepsilon_2 + \ldots + k_n\varepsilon_n$ tels que

$$k_1 + k_2 + \ldots + k_n = \pi(\alpha) = k.$$

Il est immédiat que les Z_k satisfont aux relations (46), où N est l'application structurale de $\mathfrak{H}_n(K)$ dans $\mathfrak{H}_n(K) \otimes \mathfrak{H}_n(K)$. Soit $\mathbf{u}'_n$ l'homomorphisme de $\mathfrak{L}_1(K)$ sur la sous-algèbre de $\mathfrak{H}_n(K)$ engendrée par les Z_k, telle que $\mathbf{u}'_n(\overline{V}_{k\varepsilon_1}) = Z_k$ pour tout entier $k \geqq 0$, dont l'existence résulte du théorème 3; la formule (46) montre alors que l'image par $\mathbf{u}'_n$ de toute dérivation (resp. semi-dérivation de hauteur r, semi-dérivation spéciale de hauteur r) dans $\mathfrak{L}_1(K)$, est une dérivation (resp. semi-dérivation de hauteur r, semi-dérivation spéciale de hauteur r) dans $\mathfrak{H}_n(K)$. D'autre part, les résultats des n°s 19 et 20 donnent la formule

$$(61) \qquad E(\mathbf{U}_1)\,E(\mathbf{U}_2)\ldots E(\mathbf{U}_n) = E(\mathbf{Y}_1)\,E(\mathbf{Y}_{m(2)})\ldots E(\mathbf{Y}_{m(n)})\ldots,$$

où l'on a posé

$$Y_{km} = \mathbf{u}'_n(\overline{U}_{km}) \quad \text{pour } m \in P \qquad \text{et} \qquad \mathbf{Y}_m = (Y_{0m}, Y_{1m}, \ldots, Y_{km}, \ldots).$$

On notera que l'on a

$$(62) \qquad Y_{01} = U_{01} + U_{02} + \ldots + U_{0n},$$

mais, pour $k \geqq 1$,

$$(63) \qquad Y_{k1} = U_{k1} + U_{k2} + \ldots + U_{kn} + Y'_k,$$

où $Y'_k \neq 0$ est isobare de poids p^k et de hauteur $< k$; en général Y_{0m} ($m \in P$) est une dérivation [donc combinaison linéaire des W_{ε_ϱ} dans $\mathfrak{H}_n(K)$], Y_{km}, pour $k \geqq 1$, une semi-dérivation de hauteur k, et l'on a bien entendu $\mathbf{p}'(Y_{km}) = Y_{k-1,m}$; en outre, Y_{km} est isobare et de poids $p^k m$. Cette dernière remarque montre que dans $E(\mathbf{Y}_m)$ tous les termes sauf le terme constant sont de poids $\geqq m$.

Écrivons maintenant l'identité analogue à (61) pour tout $q > n$

$$(64) \qquad E(\mathbf{U}_1)\ldots E(\mathbf{U}_q) = E(\mathbf{Y}_2^{(q)})\,E(\mathbf{Y}_{m(2)}^{(q)})\ldots E(\mathbf{Y}_{m(n)}^{(q)})\ldots.$$

L'élément $Y_{km}^{(q)}$ est combinaison linéaire de monomes en les U_{hj} ($h \leqq k$, $1 \leqq j \leqq q$); substituons à chaque U_{hj} l'élément $Y_{h,m(j)}$, ce qui donne un élément $Y_{km}^{(q,2)}$ de $\mathfrak{H}_n(K)$ qui est encore une semi-dérivation de hauteur k; cet élément n'est plus isobare, mais, *si* $m > 1$, tous ses termes sont *de poids* $\geqq p^k m + 1$. En effet, le seul U_{hj} pour lequel $Y_{h,m(j)}$ soit de même

poids p^h correspond à $j=1$; pour qu'il y ait dans $Y_{km}^{(q,2)}$ des termes de poids $p^k m$, il faudrait donc qu'ils proviennent de monomes *ne contenant que les* U_{h1} $(0 \leq h \leq k)$. Or, s'il existait de tels monomes dans l'expression de $Y_{km}^{(q)}$, ce terme ne se réduirait pas à o lorsqu'on remplace par o tous les U_{hl} tels que $2 \leq i \leq q$; mais cela est absurde, car pour $n=1$, l'homomorphisme $\mathfrak{u}'_n$ est l'homomorphisme canonique de $\mathfrak{f}_1(K)$ dans $\mathfrak{G}_1(K)$ (n° 17), qui transforme tous les $\overline{U}_{km}$ en o pour $m>1$.

Notons d'autre part que, comme $m(j) \geq j$, les termes de poids $\leq q$ sont *les mêmes* dans $Y_{km}^{(q,2)}$ et $Y_{km}^{(r,2)}$ pour $q<r$, car les termes substitués à U_{hj} pour $j>q$ sont tous de poids $>q$, et les termes ne contenant que les U_{hj} tels que $j \leq q$ sont *les mêmes* dans $Y_{km}^{(q)}$ et $Y_{km}^{(r)}$ comme il résulte de la définition de l'homomorhisme $\mathfrak{u}'_q$ de $\mathfrak{f}_1(K)$ dans $\mathfrak{G}_q(K)$. Or, l'identité (64) donne

$$(65) \qquad E(\mathbf{Y}_1)\,E(\mathbf{Y}_{m(2)}) \dots E(\mathbf{Y}_{m(q)}) = (\mathbf{Y}_1^{(q,2)})\,E(\mathbf{Y}_{m(2)}^{(q,2)}) \dots E(\mathbf{Y}_{m(n)}^{(q,2)}) \dots .$$

Désignons alors par $Y_{km}^{(2)}$ la série formelle [élément de $\mathfrak{G}_n(K)$ complété] définie par la condition que ses termes de poids $\leq q$ sont ceux de $Y_{km}^{(q,2)}$, ce qui a un sens en vertu de la remarque précédente; $Y_{km}^{(2)}$ est encore une « semi-dérivation de hauteur k » en un sens convenablement généralisé, c'est-à-dire est combinaison linéaire *infinie*, dans $\mathfrak{G}_n(K)$ complété, d'éléments $W_{k,\rho}$ et d'éléments W_α tels que $h(\alpha)<k$; on a alors à partir de (65), par un passage à la limite évident [et tenant compte de (61)]

$$(66) \qquad E(\mathbf{U}_1) \dots E(\mathbf{U}_n) = E(\mathbf{Y}_1^{(2)})\,E(\mathbf{Y}_{m(2)}^{(2)}) \dots E(\mathbf{Y}_{m(n)}^{(2)}) \dots .$$

En outre, pour $m>1$, tous les termes de $Y_{km}^{(2)}$ sont de poids au moins égal à $p^k m+1$.

On procède maintenant par récurrence; supposons que l'on ait

$$(67) \qquad E(\mathbf{U}_1) \dots E(\mathbf{U}_n) = E(\mathbf{Y}_1^{(s)})\,E(\mathbf{Y}_{m(2)}^{(s)}) \dots E(\mathbf{Y}_{m(n)}^{(s)}) \dots ,$$

où $Y_{km}^{(s)}$ $(m \in P)$ est une combinaison linéaire infinie de termes $W_{k,\rho}$ et de termes W_α de hauteur $h(\alpha)<k$ et de poids $\geq p^k m+s-1$ si $m>1$, de poids $\geq p^k$ si $m=1$. Pour tout $q>n$, on substitue à chaque U_{hj} $(h \leq k,\ 1 \leq j \leq q)$ l'élément $Y_{h,m(j)}^{(s)}$ dans l'expression de l'élément $Y_{km}^{(q)}$ de la formule (64); cela donne un élément $Y_{km}^{(q,s+1)}$ du complété de $\mathfrak{G}_n(K)$, combinaison linéaire infinie de termes $W_{k,\rho}$ et de termes W_α de hauteur $h(\alpha)<k$ et de poids p^k si $m=1$, de poids $\geq p^k m+s$ si $m>1$, comme on le voit aussitôt par récurrence. On passe ensuite à la limite comme ci-dessus, et l'on voit ainsi que la récurrence peut se poursuivre.

Cela étant, dans (67), les facteurs du second membre contribuent tous des termes de poids $\geq s$, sauf le premier. Reste à comparer $\mathbf{Y}_1^{(s)}$ et $\mathbf{Y}_1^{(s+1)}$. Or, comme le second membre de (63) se réduit à U_{k1} lorsqu'on y annule tous les U_{hj} tels que $j>1$, en vertu du même raisonnement que plus haut, on voit que $Y_{k1}^{(q,s+1)}$ est somme de $Y_{k1}^{(s)}$ et de monomes dont chacun contient au moins un $Y_{hm}^{(s)}$ avec $m>1$; les termes de poids $<s$ de $Y_{k1}^{(q,s+1)}$ sont donc *les*

mêmes que ceux de $Y_{k1}^{(s)}$, quel que soit $q > n$; par définition, on voit donc que $Y_{k1}^{(s+1)}$ a les mêmes termes de poids $< s$ que $Y_{k1}^{(s)}$. On peut donc définir l'élément $Y_{k1}^{(\infty)}$ comme combinaison linéaire infinie de termes $W_{k,\rho}$ et de termes W_α de hauteur $< k$ dans $\mathfrak{G}_n(K)$ complété, dont tous les termes de poids $< s$ sont ceux de $Y_{k1}^{(s)}$. On peut alors faire tendre s vers l'infini dans (67) et l'on obtient finalement la *formule de Hausdorff pour les corps de caractéristique* $p > 0$

$$E(\mathbf{U}_1)\,E(\mathbf{U}_2)\ldots E(\mathbf{U}_n) = E(\mathbf{Y}_1^{(\infty)}), \tag{68}$$

où l'on observera que les coefficients des W_α dans l'expression de chacun des $Y_{k1}^{(\infty)}$, sont des éléments du corps premier $\mathbf{F}_p$, indépendants du corps K.

BIBLIOGRAPHIE.

[1] J. ADEM, *The iteration of the Steenrod squares in algebraic topology* (*Proc. Nat. Acad. Sc. U. S. A.*, t. 38, 1952, p. 720-726).

[2] J. ADEM, *Relations on iterated reduced powers* (*Proc. Nat. Acad. Sc. U. S. A.*, t. 39, 1953, p. 636-638).

[3] N. BOURBAKI, *Théorie des ensembles*, chap. I-II (*Act. scient. et ind.*, n° 1212, Paris, Hermann, 1954).

[4] H. CARTAN, *Sur l'itération des opérations de Steenrod* (*Comm. Math. Helv.*, t. 29, 1955, p. 40-58).

[5] J. DIEUDONNÉ, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique* $p > 0$ (*Comm. Math. Helv.*, t. 28, 1954, p. 87-118).

[6] J. DIEUDONNÉ, *Sur la notion de variables canoniques* (*Anais da Acad. Bras. de Ciencias*, t. 27, 1955, p. 251-258).

[7] J. DIEUDONNÉ, *Lie groups and Lie hyperalgebras over a field of characteristic* $p > 0$ (II) (*Amer. J. Math.*, t. 77, 1955, p. 218-244).

[8] J. DIEUDONNÉ, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique* $p > 0$ (III) (*Math. Z.*, t. 63, 1955, p. 53-75).

[9] J. DIEUDONNÉ, *Lie groups and Lie hyperalgebras over a field of characteristic* $p > 0$ (IV) (*Amer. J. Math.*, t. 77, 1955, p. 429-452).

[10] M. LAZARD, *Sur les groupes nilpotents et les anneaux de Lie* (*Thèse*, Paris, 1954).