Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique p > 0.

Autor(en): **Dieudonné, Jean**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **28 (1954)**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-22613

Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p>0$

Par JEAN DIEUDONNÉ, Ann Arbor

1. Les récents travaux sur les groupes de Lie algébriques ([4], [7])[1]) montrent clairement que, lorsque le corps de base a une caractéristique $\neq 0$, le mécanisme de la théorie classique des groupes de Lie ne s'applique plus: on peut encore associer à un groupe de Lie son algèbre de Lie, mais la connaissance de cette dernière s'avère tout à fait insuffisante pour décrire le groupe dont elle est issue. En particulier, à des sous-groupes *distincts* d'un groupe de Lie peuvent alors correspondre la *même* algèbre de Lie. L'objet de ce travail est de définir, pour un groupe de Lie sur un corps de caractéristique $p > 0$, une «hyperalgèbre» associative qui correspond à l'«algèbre enveloppante» de l'algèbre de Lie dans le cas classique, mais possède ici une structure beaucoup plus compliquée ; la complexité de cette «hyperalgèbre» semble toutefois liée à la nature même de la question, et sa connaissance permet seule de déterminer complètement le groupe de Lie auquel elle correspond. Autrement dit, ce n'est que de cette façon que l'on peut rétablir le caractère fondamental de la théorie de Lie classique, savoir la correspondance *biunivoque* entre sous-groupes et sous-algèbres.

Une fois ce formalisme acquis, l'analogie avec la théorie de Lie classique pose aussitôt une foule de problèmes ; mais elle ne fournit qu'un bien faible secours lorsqu'il est question des méthodes à employer pour résoudre ces problèmes, où il faut tenir compte des phénomènes nouveaux qui s'introduisent, et que rien, dans la théorie classique, ne peut faire prévoir. Aussi n'avons-nous pu aborder, et à plus forte raison résoudre, qu'un petit nombre de ces problèmes ; nous espérons pouvoir revenir, dans un proche avenir, sur les plus importants d'entre eux, et notamment sur le rôle que jouent dans la théorie les séries «hyperexponentielles» que nous avons introduites dans un travail antérieur [7].

---

[1]) Les numéros entre crochets renvoient à la bibliographie placée à la fin de ce travail.

2. La notion de «groupe de Lie» que nous utiliserons est celle de «groupe de Lie formel» introduite par S. Bochner [1][2]). Etant donné un corps quelconque K, un *groupe de Lie formel de dimension n sur K* consiste en la donnée de n séries formelles sans terme constant

$$\varphi_i(x_1, \ldots, x_n, y_1, \ldots, y_n) \quad (1 \leqslant i \leqslant n)$$

par rapport à $2n$ indéterminées x_i, $y_i (1 \leqslant i \leqslant n)$, à coefficients dans K, satisfaisant aux deux conditions suivantes:

1. $\varphi_i(x_1, \ldots, x_n, 0, \ldots, 0) = x_i$, $\varphi_i(0, \ldots, 0, y_1, \ldots, y_n) = y_i (1 \leqslant i \leqslant n)$;

2. $\varphi_i(\varphi(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z}) = \varphi_i(\boldsymbol{x}, \varphi(\boldsymbol{y}, \boldsymbol{z}))$ $(1 \leqslant i \leqslant n)$

(condition d'associativité), dans laquelle le premier membre désigne la série formelle obtenue en substituant, dans la série $\varphi_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$, la série $\varphi_j(x_1, \ldots, x_n, y_1, \ldots, y_n)$ à x_j (pour $1 \leqslant j \leqslant n$), et z_k à y_k (pour $1 \leqslant k \leqslant n$), le second membre se définissant de façon analogue, et les $z_k (1 \leqslant k \leqslant n)$ étant de nouvelles indéterminées.

De la condition 1. il résulte aussitôt que l'on a nécessairement

$$\varphi_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = x_i + y_i + \psi_i(x_1, \ldots, x_n, y_1, \ldots, y_n) \qquad (1)$$

ψ_i étant une série formelle dont chaque terme est de degré $\geqslant 1$ par rapport aux x_j et de degré $\geqslant 1$ par rapport aux y_j. On déduit alors du théorème des fonctions implicites pour les séries formelles [2, p. 64, prop. 10 et p. 59, prop. 4] qu'il existe n séries formelles bien déterminées

$$\theta_i(x_1, \ldots, x_n) = -x_i + \omega_i(x_1, \ldots, x_n)$$

(où la série ω_i est d'ordre $\geqslant 2$) telles que l'on ait

$$\varphi_i(x_1, \ldots, x_n, \theta_1(x_1, \ldots, x_n), \ldots, \theta_n(x_1, \ldots, x_n)) = 0 \text{ pour } 1 \leqslant i \leqslant n. \qquad (2)$$

Utilisant le symbolisme de la théorie des groupes, nous noterons $\boldsymbol{xy}$ le système des n séries formelles $\varphi_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$, $\boldsymbol{x}^{-1}$ le système des n séries formelles $\theta_i(x_1, \ldots, x_n)$, $\boldsymbol{e}$ le système $(0, 0, \ldots, 0)$ formé des n séries nulles; le calcul sur ces symboles obéit alors aux lois usuelles, comme le montrent les raisonnements classiques de théorie des groupes.

3. Soit G' un second groupe de Lie formel de dimension m sur K, défini par m séries formelles $\varphi'_j(x'_1, \ldots, x'_m, y'_1, \ldots, y'_m)$. Un *homomorphisme* de G dans G' est par définition un système $\boldsymbol{f}(\boldsymbol{x})$ de m séries formelles $f_j(x_1, \ldots, x_n) (1 \leqslant j \leqslant m)$ sans terme constant, satisfaisant à m

[2]) Sur la liaison entre cette notion et celle de «groupe de Lie algébrique» de Chevalley, voir n° 28.

relations que l'on peut écrire sous la forme abrégée $f(xy) = f(x)f(y)$, avec les conventions faites ci-dessus. Il est clair que le composé de deux homomorphismes est un homomorphisme. Un homomorphisme f de G dans G' est un *isomorphisme* s'il existe un homomorphisme g de G' dans G tel que $g(f(x)) = x$ et $f(g(x')) = x'$. La considération des termes du premier ordre dans ces relations montre aussitôt que l'on a nécessairement alors $m = n$, et que les matrices jacobiennes $\left(\frac{\partial f_i}{\partial x_j}\right)$ et $\left(\frac{\partial g_i}{\partial x'_j}\right)$ sont inverses l'une de l'autre. Inversement, soit $g(x')$ un système de n séries formelles $g_i(x'_1, \ldots, x'_n)$ sans terme constant, tel que la matrice jacobienne $\left(\frac{\partial g_i}{\partial x'_j}\right)$ soit inversible ; il existe alors un système $f(x)$ de n séries formelles telles que l'on ait $f(g(x')) = x'$ et $g(f(x)) = x$ [2, p. 64, prop. 10] ; en posant $x'y' = f(g(x')g(y'))$ on définit un nouveau groupe de Lie formel G' tel que f soit un isomorphisme de G sur G' et g l'isomorphisme réciproque. Nous dirons que G' provient de G par «changement de variables» et nous l'identifierons parfois avec G.

4. Nous désignerons par $\mathfrak{o}(G)$, ou $\mathfrak{o}_0(G)$ (ou simplement $\mathfrak{o}$ ou $\mathfrak{o}_0$) l'anneau des séries formelles, à coefficients dans K, par rapport aux n indéterminées $x_1, \ldots, x_n$. Nous supposerons désormais que K est un corps de caractéristique $p > 0$. Alors, pour tout entier $r \geqslant 0$, nous désignerons par $\mathfrak{o}_r(G)$ ou $\mathfrak{o}_r$ le sous-anneau de $\mathfrak{o}(G)$ formé des séries formelles par rapport à $x_1^{p^r}, \ldots, x_n^{p^r}$. Il est clair que $\mathfrak{o}(G)$ peut être considéré comme un *module* par rapport à $\mathfrak{o}_r(G)$, admettant pour base les p^{rn} monômes $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, où $0 \leqslant \alpha_i < p^r$ pour $1 \leqslant i \leqslant n$. Nous dirons qu'un K-endomorphisme Δ de l'anneau $\mathfrak{o}$ est une *semi-dérivation de hauteur* r [5] si l'on a $\Delta(\mathfrak{o}_r) \subset \mathfrak{o}_r$ et si Δ vérifie l'identité

$$\Delta(fg) = f\Delta(g) + g\Delta(f) \tag{3}$$

pour $f \in \mathfrak{o}_r$ et $g \in \mathfrak{o}$; en faisant $f = 1$ dans cette identité, on voit que $\Delta(1) = 0$. La restriction de Δ à $\mathfrak{o}_r$ est une *dérivation* de cet anneau, à valeurs dans $\mathfrak{o}_r$; il résulte aussitôt de la formule de Leibniz que Δ s'annule dans $\mathfrak{o}_{r+1}$. Nous dirons qu'une semi-dérivation Δ de hauteur r est *spéciale* si $\Delta(f) = 0$ dans $\mathfrak{o}_r$; toute semi-dérivation de hauteur r est donc une semi-dérivation spéciale de hauteur $r + 1$. Le lemme suivant se vérifie trivialement :

Lemme 1. — *Si Δ est une semi-dérivation de hauteur r, il en est de même de Δ^p (p-ème itérée de Δ) et de $f\Delta$, pour $f \in \mathfrak{o}_r$. Si Δ, Δ' sont deux semi-dérivations de hauteur r, il en est de même de $[\Delta, \Delta'] = \Delta\Delta' - \Delta'\Delta$;*

en outre, $[\Delta, \Delta']$ *est spéciale si* Δ *ou* Δ' *est spéciale. Si* Δ *est une semi-dérivation spéciale de hauteur* r, *il en est de même de* $g\Delta$, *pour* $g \in \mathfrak{o}$; *si* Δ, Δ' *sont deux semi-dérivations spéciales de hauteur* r, *il en est de même de* $\Delta\Delta'$.

L'ensemble $\mathfrak{D}_r$ des semi-dérivations de hauteur r est donc une *p-algèbre de Lie* sur l'anneau $\mathfrak{o}_r$; l'ensemble $\mathfrak{S}_r$ des semi-dérivations spéciales de hauteur r est un *idéal* dans l'algèbre de Lie $\mathfrak{D}_r$; en outre, c'est une algèbre *associative* sur l'anneau $\mathfrak{o}$, qu'on peut identifier à l'algèbre (sur $\mathfrak{o}$) des endomorphismes du $\mathfrak{o}_r$-module $\mathfrak{o}$ s'annulant dans $\mathfrak{o}_r$.

5. Une semi-dérivation de hauteur r est entièrement définie par les valeurs qu'elle prend pour les monômes $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, où $0 \leqslant \alpha_i < p^{r+1}$. Désignons par D_{ri} la semi-dérivation de hauteur r telle que, si $\alpha_i = ap^r + b$, avec $0 \leqslant b < p^r$, on ait

$$D_{ri}(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) = a x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i - p^r} x_{i+1}^{\alpha_{i+1}} \dots x_n^{\alpha_n}. \qquad (4)$$

On vérifie immédiatement que D_{ri} satisfait bien à (3) pour $f \in \mathfrak{o}_r$ et $g \in \mathfrak{o}$, et que l'on a $D_{ri}^p = 0$ quels que soient $r \geqslant 0$ et $1 \leqslant i \leqslant n$; en outre, D_{ri} et D_{sj} commutent quels que soient les indices.

Lemme 2. — *Le* $\mathfrak{o}$*-module* $\mathfrak{S}_r$ *a une base formée des semi-dérivations* $\prod_{h=0}^{r-1} \prod_{i=1}^{n} D_{hi}^{\lambda_{hi}}$, *où* $0 \leqslant \lambda_{hi} < p$ *et* $\sum_{h,i} \lambda_{hi} > 0$; *le* $\mathfrak{o}_r$*-module* $\mathfrak{D}_r$ *est somme directe de* $\mathfrak{S}_r$ *et du* $\mathfrak{o}_r$*-module ayant pour base les* n *semi-dérivations* $D_{ri} (1 \leqslant i \leqslant n)$.

En effet, si Δ est une semi-dérivation de hauteur r, sa restriction à l'anneau $\mathfrak{o}_r$ est une dérivation, donc [2, p. 43, prop. 8] coïncide avec une combinaison linéaire uniquement déterminée des semi-dérivations $D_{ri} (1 \leqslant i \leqslant n)$, à coefficients dans $\mathfrak{o}_r$. Si on retranche de Δ cette combinaison linéaire, on a donc une semi-dérivation spéciale Δ' ; tout revient donc à démontrer la première assertion du lemme. Mais si on pose $D = \prod_{h=0}^{r-1} \prod_{i=1}^{n} D_{hi}^{\lambda_{hi}}$ et $\alpha_i = \sum_{h=0}^{r-1} \lambda_{hi} p^h \ (1 \leqslant i \leqslant n)$, il résulte des formules (4) que l'on a

$$D(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) = \prod_{h=0}^{r-1} \prod_{i=1}^{n} \lambda_{hi}! \neq 0 \quad \text{et} \quad D(x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}) = 0$$

pour tout système $(\beta_1, \dots, \beta_n)$ d'exposants $< p^r$, tels que $\beta_i < \alpha_i$ pour un indice i au moins. En vertu de la caractérisation de $\mathfrak{S}_r$ donnée au n° 4, cela prouve que les semi-dérivations D forment une base de $\mathfrak{S}_r$ par rapport à $\mathfrak{o}$, comme on le voit par exemple en ordonnant lexicographiquement les monômes $x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$.

Pour tout système $\alpha = (\alpha_1, \ldots, \alpha_n)$ de n entiers $\geqslant 0$, il nous sera commode de poser désormais $x_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ et $D_\alpha = \prod_{h=0}^{\infty} \prod_{i=1}^{n} D_{hi}^{\lambda_{hi}}$, où les λ_{hi} sont les coefficients des développements p-adiques

$$\alpha_i = \sum_{h=0}^{\infty} \lambda_{hi} p^h \quad (1 \leqslant i \leqslant n);$$

nous écrirons aussi $\alpha! = \prod_{h=0}^{\infty} \prod_{i=1}^{n} \lambda_{hi}!$, et $|\alpha| = \alpha_1 + \alpha_1 + \ldots + \alpha_n$.

6. Nous définirons maintenant un *opérateur différentiel* D dans $\mathfrak{o}(G)$ comme une combinaison linéaire finie $\sum_\alpha u_\alpha D_\alpha$, où $u_\alpha \in \mathfrak{o}$; le *poids* de cet opérateur est par définition le plus grand des nombres $|\alpha|$ pour lesquels $u_\alpha \neq 0$; il résulte du lemme 2 que la représentation de D comme somme $\sum_\alpha u_\alpha D_\alpha$ est unique. Les opérateurs différentiels dans $\mathfrak{o}(G)$ forment évidemment une *algèbre* associative $\mathcal{S}$ sur l'anneau $\mathfrak{o}$, réunion de la suite croissante des algèbres $\mathcal{S}_r$.

La définition précédente n'est toutefois pas assez générale: si A est un $\mathfrak{o}$-module, on peut définir un opérateur différentiel à valeurs dans A comme une somme $\sum_\alpha c_\alpha D_\alpha$, où les $c_\alpha \in A$, pourvu que cette somme (étendue à tous les indices α) ait un sens, c'est-à-dire que la somme $\sum_\alpha c_\alpha D_\alpha f$ ait un sens dans A pour tout $f \in \mathfrak{o}$. Il en sera ainsi lorsque $A = \mathfrak{o}$, ou plus généralement lorsque A est l'anneau des séries formelles par rapport aux x_i et à d'autres indéterminées, pourvu que l'ordre de la série formelle c_α augmente indéfiniment avec $|\alpha|$.

Un important exemple de tels «opérateurs différentiels» généralisés est fourni par les deux opérateurs suivants: si on pose

$$L_y f = f(yx), \; R_y f = f(xy) \tag{5}$$

(*opérateurs de translation* sur $\mathfrak{o}(G)$), alors $L_y - I$ et $R_y - I$ (I identité) sont des opérateurs différentiels. En effet, la *formule de Taylor* pour les séries formelles à n indéterminées [6] s'écrit, pour tout $f \in \mathfrak{o}(G)$

$$f(x + z) = \sum \frac{1}{\alpha!} z_\alpha D_\alpha f \tag{6}$$

avec les conventions précédentes[3]; remplaçant dans cette formule z_i par $y_i + \psi_i(y, x)$ (resp. par $y_i + \psi_i(x, y)$), on voit que chacun des deux

[3]) On convient dans cette somme de poser $D_{(0,0,\ldots,0)} = I$, que l'on écrit aussi D_0; naturellement, ce n'est pas un «opérateur différentiel» au sens défini ci-dessus.

opérateurs L_y, R_y peut se mettre sous la forme $\sum_\alpha v_\alpha(x, y)\, D_\alpha$, où v_α est une série formelle par rapport à x et y, dont l'ordre *par rapport aux* y_i est au moins égal à $|\alpha|$; de façon plus précise, $v_\alpha(x, y)$ ne contient qu'un seul terme d'ordre $|\alpha|$ par rapport aux $2n$ indéterminées x_i, y_i, égal à $\frac{1}{\alpha!}\, y_\alpha$, et tout autre terme contient *au moins un* x_i.

7. Soit D un opérateur différentiel dans $\mathfrak{o}(G)$, à valeurs dans un anneau A de séries formelles par rapport aux x_i et (éventuellement) à d'autres indéterminées ; nous supposons que $D = \sum_\alpha c_\alpha D_\alpha$, où l'ordre de la série formelle c_α augmente indéfiniment avec $|\alpha|$. Dans ces conditions, il est clair que les produits DL_y et $L_y D$ sont tous deux définis, et prennent leurs valeurs dans l'anneau des séries formelles par rapport aux y_i et aux indéterminées figurant dans A (supposées distinctes des y_i). Nous dirons que D est un opérateur différentiel *invariant à gauche* si

$$DL_y = L_y D\,. \tag{7}$$

Soit D un tel opérateur ; désignons par $D(e)\,f$ l'élément de A obtenu en substituant e à x dans Df, pour tout $f \in \mathfrak{o}(G)$. La relation (7) s'écrit pour tout $f \in \mathfrak{o}(G)$, $D(L_y f) = L_y(Df)$, d'où en substituant e à x,

$$D(e)(L_y f) = (Df)(y) \tag{8}$$

et par suite D est connu si l'application $D(e)$ de $\mathfrak{o}(G)$ dans A est connue. Réciproquement, donnons-nous *arbitrairement* une application de $\mathfrak{o}(G)$ dans A, de la forme $\sum_\alpha a_\alpha D_\alpha(e)$, où les a_α sont des séries formelles ne contenant pas x, et telles que la somme précédente ait un sens ; on peut alors *définir* un opérateur D dans $\mathfrak{o}(G)$ par la condition

$$(Df)(y) = \sum_\alpha a_\alpha D_\alpha(e)(L_y f) \tag{9}$$

et cet opérateur est invariant, car on a (pour des indéterminées z_i distinctes des y_i et de celles intervenant dans A)

$$(D(L_z f))(y) = \sum_\alpha a_\alpha D_\alpha(e)(L_y L_z f)$$

et comme $L_y L_z = L_{zy}$, on a $(D(L_z f))(y) = (Df)(zy) = (L_z(Df))(y)$, ce qui établit (7). Notre assertion sera donc prouvée si l'on montre que D est un opérateur *différentiel*, au sens donné plus haut. Pour cela, il suffit évidemment de considérer le cas particulier où $D(e) = D_\alpha(e)$; alors l'équation $(Df)(y) = D_\alpha(e)(L_y f)$ signifie que le premier membre est

égal au *coefficient de* $\frac{1}{\alpha!} x_\alpha$ dans le développement de $f(\boldsymbol{y}\boldsymbol{x})$ suivant les puissances des x_i, car $D_\alpha(\boldsymbol{e})\, x_\beta = 0$ pour $\beta \neq \alpha$. Il résulte de ce qui a été dit au n° 6 que l'on peut alors écrire

$$D = w_\alpha D_\alpha + \sum_\beta w_\beta D_\beta \tag{10}$$

où la sommation est étendue aux indices $\beta \neq \alpha$ tels que $|\beta| \leqslant |\alpha|$; en outre les w_β appartiennent à $\mathfrak{o}(G)$, w_α *a pour terme constant* 1 et les w_β pour $\beta \neq \alpha$ sont *sans terme constant.* On notera qu'en général on a $D \neq D_\alpha$ (bien que $D(\boldsymbol{e}) = D_\alpha(\boldsymbol{e})$; autrement dit, en général, D_α n'est pas invariant).

Nous noterons ici les particularités qui se présentent lorsque l'on prend pour D_α une semi-dérivation D_{hi} ; désignons par X_{hi} l'opérateur différentiel *invariant* tel que $X_{hi}(\boldsymbol{e}) = D_{hi}(\boldsymbol{e})$. On peut écrire alors la formule (10) sous la forme plus précise

$$X_{hi} = w_{hi}^{(i)} D_{hi} + \sum_{j \neq i} w_{hj}^{(i)} D_{hj} + \sum_\beta w_\beta^{(i)} D_\beta \tag{11}$$

où dans la seconde somme, les indices β sont distincts des n indices $(0, \ldots, p^h, \ldots, 0)$; la relation $|\beta| \leqslant p^h$ entraîne alors que les D_β sont des *semi-dérivations spéciales* de hauteur h. En outre, $w_{hj}^{(i)}$ est le coefficient de $y_i^{p^h}$ dans la série $(y_j + \psi_j(\boldsymbol{x}, \boldsymbol{y}))^{p^h}$; on en conclut que les $w_{hi}^{(i)}$ *appartiennent à* $\mathfrak{o}_h$ et n'ont pas de terme constant, sauf $w_{hi}^{(i)}$ qui a pour terme constant 1 ; les $w_\beta^{(i)}$ n'ont pas de terme constant. Il est clair enfin que X_{hi} est une *semi-dérivation d'ordre* h.

8. Il résulte aussitôt de l'équation (7) que le produit de deux opérateurs différentiels invariants à gauche est encore invariant à gauche. Pour tout $\alpha = (\alpha_1, \ldots, \alpha_n)$, où $\alpha_i = \sum_{h=0}^{r} \lambda_{hi} p^h$, considérons en particulier les opérateurs invariants

$$X_\alpha = X_{01}^{\lambda_{01}} X_{02}^{\lambda_{02}} \ldots X_{0n}^{\lambda_{0n}} X_{11}^{\lambda_{11}} \ldots X_{1n}^{\lambda_{1n}} \ldots X_{r1}^{\lambda_{r1}} \ldots X_{rn}^{\lambda_{rn}} \tag{12}$$

(on observera que les X_{hi} ne sont pas permutables deux à deux en général, et qu'il importe donc de spécifier l'ordre dans lequel on les compose). Nous allons démontrer le théorème fondamental suivant :

Théorème 1. *Le* $\mathfrak{o}$*-module* $\mathcal{S}_r$ *a une base formée des semi-dérivations spéciales* X_α, *ou* $0 \leqslant \alpha_i < p^{r-1}$ *et* $\sum_{i=1}^{n} \alpha_i > 0$; *le* $\mathfrak{o}_r$*-module* $\mathcal{D}_r$ *est somme directe de* $\mathcal{S}_r$ *et du* $\mathfrak{o}_r$*-module ayant pour base les* n *semi-dérivations* X_{ri} $(1 \leqslant i \leqslant n)$.

Remarquons tout d'abord que pour un h donné, les équations (11) par rapport aux $D_{hi}(1 \leqslant i \leqslant n)$ forment un système de n équations linéaires à n inconnues, dont le déterminant n'est pas nul. En effet ce déterminant a dans sa diagonale principale des séries ayant pour terme constant 1, et les autres termes sont des séries sans terme constant, d'où résulte aussitôt que le déterminant est une série formelle ayant pour terme constant 1. En outre, tous les $w_{hi}^{(j)}$ appartiennent à $\mathfrak{o}_r$; il résulte des formules de Cramer que l'on peut écrire

$$D_{hi} = u_{hi}^{(i)} X_{hi} + \sum_{j \neq i} u_{hj}^{(i)} X_{hj} + \sum_{\beta} u_{\beta}^{(i)} D_{\beta} \tag{13}$$

où les $u_{hi}^{(j)}$ appartiennent à $\mathfrak{o}_r$; en outre, $u_{hi}^{(i)}$ est une série ayant un terme constant égal à 1, et les $u_{hj}^{(i)}$ pour $j \neq i$ sont des séries sans terme constant. Comme par ailleurs les D_β sont des semi-dérivations spéciales de hauteur h, il résulte du lemme 2 que la seconde partie du th. 1 sera démontrée dès que l'on aura démontré la première.

Pour cela, nous allons raisonner par récurrence sur r, supposant donc le théorème démontré pour $\mathcal{S}_r$. En vertu du lemme 2, il suffira de prouver que chacun des opérateurs D_α pour $0 \leqslant \alpha_i < p^{r+1}(1 \leqslant i \leqslant n)$ peut s'exprimer comme combinaison linéaire des X_α relatifs aux α satisfaisant aux mêmes conditions, le nombre des X_α étant le même que celui des D_α.

Commençons par prouver le résultat suivant: tout produit de la forme

$$\Delta\, D_1 D_2 \,..\, D_m X_{m+1} \,..\, X_q \tag{14}$$

où Δ est une semi-dérivation spéciale de hauteur r, D_i une (quelconque) des semi-dérivations D_{rj}, X_i une (quelconque) des semi-dérivations X_{rj}, peut s'exprimer comme somme de produits de la même forme, mais où m est remplacé par $m - 1$ ou q par un nombre plus petit. En considérant le produit $\Delta\, D_1 D_2 \,..\, D_m$, on peut se borner au cas où $q = m$. Cela étant, la formule (13) montre que

$$D_q = \sum_{j=1}^{n} u_j X_{rj} + \Delta'$$

où Δ' est une semi-dérivation spéciale de hauteur r et les $u_j \in \mathfrak{o}_r(G)$. On est ramené à considérer les produits

$$\Delta\, D_1 D_2 \,..\, D_{q-1}(u_j X_{rj}) \tag{15}$$

$$\text{et} \quad \Delta\, D_1 D_2 \,..\, D_{q-1} \Delta' \tag{16}$$

Comme $u_j \in \mathfrak{o}_r$ et que D_{q-1} est une semi-dérivation de hauteur r, on a $D_{q-1}(u_j X_{rj}) = (D_{q-1} u_j) X_{rj} + u_j (D_{q-1} X_{rj})$. Le premier terme du se-

cond membre donne un produit analogue à (15), mais où q est remplacé par $q - 1$; le second donne le produit

$$\Delta\, D_1\, D_2 \,..\, D_{q-2}(u_j(D_{q-1}\, X_{rj})) \tag{17}$$

Par récurrence sur q, on voit donc que le produit (15) est une somme de produits de la forme

$$\Delta_1\, D_1\, D_2 \,..\, D_m\, X_{rj}$$

où Δ_1 est une semi-dérivation spéciale de hauteur r, et $m \leqslant q - 1$. D'autre part, on peut écrire

$$D_{q-1}\, \Delta' = \Delta'\, D_{q-1} + [D_{q-1}, \Delta']$$

et comme $[D_{q-1}, \Delta']$ est une semi-dérivation *spéciale* de hauteur r, le produit (16) est somme d'un produit de même forme, mais où q est remplacé par $q - 1$, et du produit

$$\Delta\, D_1\, D_2 \,..\, D_{q-2}\, \Delta'\, D_{q-1} \tag{18}$$

Par récurrence, on voit donc que le produit (16) est une somme de produits de la forme

$$\Delta_2\, D_1\, D_2 \,..\, D_m$$

où $m \leqslant q - 1$, et notre assertion est donc établie.

Cela établit que D_α peut s'écrire comme somme de produits de la forme $\Delta\, X_1\, X_2 \,..\, X_q$, où $\Delta \in \mathcal{S}_r$ et où chacun des X_i est un (quelconque) des X_{rj}, avec $q \leqslant p^n$. Montrons maintenant qu'un tel produit peut s'écrire comme somme de produits de la même forme, mais où les X_{rj} sont rangés par ordre d'indices j croissants. Pour cela, observons que l'on a $X_1\, X_2 = X_2\, X_1 + [X_1, X_2]$, et que $[X_1, X_2]$ est une semi-dérivation de hauteur r, donc combinaison linéaire $\sum_{j=1}^{n} v_j\, X_{rj} + \Delta'$, où $v_j \in \mathfrak{o}_r$ et Δ' est une semi-dérivation spéciale de hauteur r. Substituant à $X_1\, X_2$ la valeur ainsi obtenue, on voit que dans le produit $\Delta\, X_1\, X_2 \,..\, X_q$, on peut échanger X_1 et X_2, à condition d'ajouter une combinaison linéaire de produits de même forme mais correspondant à une valeur plus petite de l'indice q. On prouverait de la même manière le même résultat pour deux termes consécutifs quelconques.

On a ainsi ramené D_α à une somme de produits de la forme

$$\Delta\, X_{r1}^{\mu_1}\, X_{r2}^{\mu_2} \,\ldots\, X_{rn}^{\mu_n}, \quad \text{où} \quad \sum_{i=1}^{n} \mu_i \leqslant p^n .$$

Il peut se faire que certains des exposants μ_i soient $\geqslant p$; mais X_{ri}^{p},

étant une semi-dérivation de hauteur r, s'exprime comme somme d'une combinaison linéaire des X_{rj}, à coefficients dans $\mathfrak{o}_r$, et d'une semi-dérivation spéciale ; raisonnant comme ci-dessus pour $[X_1, X_2]$, on voit qu'on peut ainsi ramener tous les exposants μ_i à être $< p$, et le th. 1 est complètement démontré.

9. Nous appellerons *hyperalgèbre de Lie* du groupe G l'algèbre $\mathfrak{G}$ (sur le corps K) formé des opérateurs de $\mathcal{S}$ qui sont invariants à gauche. Nous poserons $\mathfrak{g}_r = \mathcal{D}_r \cap \mathfrak{G}$, $\mathfrak{s}_r = \mathcal{S}_r \cap \mathfrak{G}$; $\mathfrak{g}_0$ n'est autre que l'*algèbre de Lie* du groupe G (algèbre des *dérivations* invariantes à gauche). D'ailleurs, il est clair, en vertu du lemme 1, que chacun des ensembles $\mathfrak{g}_r$ est une *p-algèbre de Lie* sur K, dans laquelle $\mathfrak{s}_r$ est un *idéal*, et en même temps une *algèbre associative* sur K.

Théorème 2. *L'algèbre associative $\mathfrak{s}_r$ a pour base sur K les semi-dérivations spéciales X_α, ou $0 \leqslant \alpha_i < p^{r-1}$; l'algèbre de Lie $\mathfrak{g}_r$ est somme directe de $\mathfrak{s}_r$ et de l'espace vectoriel sur K ayant pour base $X_{r1}, \ldots, X_{rn}$.*

En vertu du th. 1, tout revient à prouver que si une semi-dérivation de hauteur r, $D = \sum_\alpha u_\alpha X_\alpha$, est invariante, alors les séries formelles u_α sont nécessairement des *constantes*. Or, l'identité (7) s'écrit, pour toute $f \in \mathfrak{o}(G)$

$$\sum_\alpha u_\alpha(x) \cdot (X_\alpha L_y) f = \sum_\alpha u_\alpha(yx) \cdot (L_y X_\alpha) f .$$

Si on tient compte de ce que $X_\alpha L_y = L_y X_\alpha$, en remplaçant x par e, il vient, d'après (8)

$$\sum_\alpha u_\alpha(e) \cdot (X_\alpha f)(y) = \sum_\alpha u_\alpha(y) \cdot (X_\alpha f)(y) ;$$

en remplaçant alors y par x, cela équivaut à

$$\sum_\alpha u_\alpha(e) X_\alpha = \sum_\alpha u_\alpha(x) \cdot X_\alpha$$

et comme les X_α sont linéairement indépendantes (th. 1), cela entraîne $u_\alpha = u_\alpha(e)$, autrement dit les séries formelles u_α sont réduites à leur terme constant.

On peut encore exprimer le résultat du th. 2 sous la forme suivante : considérons l'algèbre associative libre T_r sur les n^r éléments

$$X_{01}, \ldots, X_{0n}, X_{11}, \ldots, X_{1n}, \ldots, X_{r-1,1}, \ldots, X_{r-1,n}$$

(à coefficients dans K). On définit évidemment un homomorphisme de T_r sur $\mathfrak{s}_r$ en faisant correspondre au produit $Z_1 Z_2 \ldots Z_q$ dans T_r (où les Z_i sont certains des X_{hj}, distincts ou non, dans un ordre quelconque) le

produit $Z_1 Z_2 \ldots Z_q$ dans $\mathfrak{s}_r$. Nous avons vu que chacun des crochets $[X_{hi}, X_{kj}]$ peut s'écrire (dans $\mathfrak{s}_r$) comme combinaison linéaire

$$\sum_\alpha \lambda_{hikj}^{(\alpha)} X_\alpha ,$$

les coefficients étant dans K et les X_α dans $\mathfrak{s}_r$; de même X_{hi}^p est, dans $\mathfrak{s}_r$, égal à une combinaison linéaire $\sum_\alpha \mu_{hi}^{(\alpha)} X_\alpha$ du même type. Le th. 2 montre alors que le *noyau* de l'homomorphisme de T_r sur $\mathfrak{s}_r$ défini ci-dessus est *l'idéal I_r engendré par les éléments suivants de T_r*:

$$X_{hi} X_{kj} - X_{kj} X_{hi} - \sum_\alpha \lambda_{hikj}^{(\alpha)} X_\alpha \tag{19}$$

$$X_{hi}^p - \sum_\alpha \mu_{hi}^{(\alpha)} X_\alpha . \tag{20}$$

En effet, il est clair que I_r contient ces éléments, et d'autre part, on peut mettre tout élément de T_r sous forme d'une combinaison linéaire $\sum_\alpha c_\alpha X_\alpha$ et d'une somme d'éléments de l'idéal I_r, comme le montre un raisonnement tout à fait analogue à celui de la démonstration du th. 1 ; en vertu du th. 2, un tel élément ne correspond donc à 0 dans $\mathfrak{s}_r$ que s'il est dans I_r.

Nous verrons plus loin (n° 13) que les algèbres de Lie $\mathfrak{g}_r$ sont en outre liées les unes aux autres par l'existence de certains homomorphismes canoniques.

10. La condition d'associativité dans G est équivalente à la permutabilité des opérateurs L_y et R_z ; autrement dit, R_z est un opérateur *invariant à gauche*. On peut par suite écrire

$$R_z = \sum_\alpha P_\alpha(\boldsymbol{z}) X_\alpha \tag{21}$$

où les P_α sont des séries formelles[4]) ; cela résulte en effet du th. 2 et de la représentation de R_z comme série de la forme $\sum_\alpha v_\alpha(\boldsymbol{x}, \boldsymbol{z}) D_\alpha$: il suffit de remplacer, dans cette dernière série, chacun des D_α par son expression en fonction des X_β.

Nous allons étudier la forme des séries P_α. Comme on sait d'avance que les $P_\alpha(\boldsymbol{z})$ ne contiennent pas $\boldsymbol{x}$, on voit (cf. n° 6) que si

$$D_\alpha = \sum_\beta u_{\alpha\beta} X_\beta ,$$

$P_\alpha(\boldsymbol{z})$ est aussi le coefficient de X_α dans l'expression $\sum_{\beta,\gamma} \frac{1}{\beta!} z_\beta u_{\beta\gamma}(\boldsymbol{e}) X_\gamma$; tout revient donc à étudier l'expression de l'opérateur $D'_\alpha = \sum_\beta u_{\alpha\beta}(\boldsymbol{e}) X_\beta$.

[4]) On convient de poser $P_0 = 1$ et $X_0 = I$ (opérateur identique).

Pour tout $\alpha = (\alpha_1, \ldots, \alpha_n)$, soit $h(\alpha)$ le plus petit entier r pour lequel $\alpha_i < p^{r+1}$ pour $1 \leqslant i \leqslant n$; en divisant les α_i par p^r, on peut écrire $\alpha = \gamma + \delta$, où $\gamma = p^r \gamma' = (p^r \gamma'_1, \ldots, p^r \gamma'_n)$ avec $0 \leqslant \gamma'_i < p$, et $h(\delta) < h(\alpha)$; nous poserons $s(\alpha) = \sum_{i=1}^{n} \gamma'_i = |\gamma'|$. Nous allons montrer qu'on a

$$D'_\alpha = D'_\delta X_\gamma + \sum_\beta a_\beta X_\beta \tag{22}$$

où, dans la somme du second membre, on a $h(\beta) < h(\alpha)$ ou $h(\beta) = h(\alpha)$ et $s(\beta) < s(\alpha)$. Supposons la proposition établie pour $h(\alpha) < r$. Les remarques faites au sujet de la formule (13) montrent que $D'_{ri} = X_{ri} + \sum_\beta b_\beta D'_\beta$ avec $h(\beta) < r$ pour tous les termes de la somme du second membre ; notre résultat est donc vérifié dans ce cas, qui correspond à $s(\alpha) = 1$, $\delta = (0, 0, \ldots, 0)$. Raisonnons alors par récurrence sur $s(\alpha)$ (pour $h(\alpha) = r$) ; si $s(\alpha) = s$, on a

$$D_\alpha = D_\delta D_1 D_2 \ldots D_s$$

où chaque $D_i (1 \leqslant i \leqslant s)$ est une des semi-dérivations D_{rj}. Dans l'expression $D_\alpha = \sum_\beta u_{\alpha\beta} X_\beta$, la démonstration du th. 1 montre que tous les termes sont tels que $h(\beta) < r$ ou $h(\beta) = r$ et $s(\beta) < s$, sauf ceux de la forme

$$u_1 u_2 \ldots u_s D_\delta Z_1 Z_2 \ldots Z_s \tag{23}$$

où $u_i Z_i$ désigne *un* des termes $u_{rk}^{(j)} X_{rk}$ dans l'expression de $D_i = D_{rj}$ donnée par la formule (13) ; cela résulte en effet de ce que D_δ est une semi-dérivation spéciale de hauteur r, et que les u_i appartiennent à $\mathfrak{o}_r$. Lorsqu'on remplace x par e, le seul terme (23) pour lequel $u_1 u_2 \ldots u_s$ ne devient pas 0 provient du cas où $k = j$ pour *chacun* des u_i (les seuls termes $u_{rk}^{(j)}$ ayant un terme constant $\neq 0$ correspondant à $k = j$). On a donc bien la formule (22).

On en déduit l'expression des P_α ; avec les mêmes notations, on a

$$P_\alpha = \frac{1}{\gamma!} x_\gamma P_\delta + Q_\alpha \tag{24}$$

où Q_α est une série formelle dans laquelle les termes non nuls sont des monômes $b_\beta x_\beta$, où l'on a, *soit* $h(\beta) > h(\alpha)$, *soit* $h(\beta) = h(\alpha)$ et $s(\beta) > s(\alpha)$. En effet, P_α est le coefficient de X_α dans la somme

$$\sum_\beta \frac{1}{\beta!} x_\beta D'_\beta .$$

Il résulte de la formule (22) que X_α ne peut figurer que dans des D'_β pour lesquels $h(\beta) > h(\alpha)$, ou $h(\beta) = h(\alpha)$ et $s(\beta) \geqslant s(\alpha)$. Remarquons maintenant qu'on a $\frac{1}{\alpha!} x_\alpha = \frac{1}{\delta!} x_\delta \cdot \frac{1}{\gamma!} x_\gamma$ et $X_\alpha = X_\delta X_\gamma$, X_γ pouvant être appelée la partie de X_α contenant les semi-dérivations non spéciales de hauteur $h(\alpha)$; la formule (22) montre alors que si $h(\beta) = h(\alpha)$ et $s(\beta) = s(\alpha)$, D'_β ne pourra contenir un terme en X_α que si α et β ont *même «quotient euclidien»* γ' par p^r ; en outre la somme de tous ces termes est $\frac{1}{\gamma!} x_\gamma P'_\delta$, où P'_δ est le coefficient de X_δ dans la somme $\sum_\beta \frac{1}{\beta!} x_\beta D'_\beta$, étendue à tous les indices β *tels que* $h(\beta) < h(\alpha)$. Mais il est clair, par définition, que $P_\delta - P'_\delta$ est une série formelle dont tous les termes non nuls sont des monômes $b_\lambda x_\lambda$ tels que $h(\lambda) \geqslant h(\alpha)$, et pour un tel terme, si on pose $x_\lambda x_\gamma = x_\mu$, on a évidemment $s(\mu) > s(\alpha)$. La formule (24) est ainsi démontrée.

Nous pouvons maintenant démontrer le théorème suivant:

Théorème 3. *Toute relation de la forme* $\sum_\alpha c_\alpha P_\alpha = 0$, *où les* c_α *sont des séries formelles par rapport à des indéterminées autres que les* x_i, *entraîne* $c_\alpha = 0$ *pour tout* α.

Nous démontrerons en fait un résultat un peu plus précis: *si, dans la série* $\sum_\alpha c_\alpha P_\alpha$, *les termes en* x_β *sont nuls pour* $h(\beta) < r$ *et pour* $h(\beta) = r$ *et* $s(\beta) \leqslant s$, *alors les* c_α *sont nuls pour* $h(\alpha) < r$ *et pour* $h(\alpha) = r$ *et* $s(\alpha) \leqslant s$. Il suffit de raisonner par récurrence sur r et s. Supposons la proposition démontrée pour les nombres $r' < r$, et pour $r' = r$ et $s' < s$; alors les termes de $\sum_\alpha c_\alpha P_\alpha$ qui sont en x_β avec $h(\beta) = r$ et $s(\beta) = s$ ne peuvent provenir, en vertu de (24), que de la somme $\sum_\alpha \frac{1}{\gamma!} c_\alpha x_\gamma P_\delta$, étendue à tous les indices α pour lesquels $h(\alpha) = r$ et $s(\alpha) = s$; ils proviennent même de la somme $\sum_\alpha \frac{1}{\gamma!} c_\alpha x_\gamma P'_\delta$, où P'_δ est la somme des termes en x_β de P_δ, pour lesquels $h(\beta) < r$. Mais dans cette somme, les termes correspondant à deux valeurs différentes de γ ne peuvent évidemment se réduire ; on a donc $\sum_\alpha c_\alpha P'_\delta = 0$, la somme étant étendue à tous les α pour lesquels γ' (quotient euclidien de α par p^r) est le même. Or, cette dernière relation signifie que, dans la somme correspondante $\sum_\alpha c_\alpha P_\delta$, les coefficients des termes en x_β pour lesquels $h(\beta) < r$ sont nuls ; l'hypothèse de récurrence entraîne donc $c_\alpha = 0$ pour tous les α considérés, ce qui achève la démonstration.

11. La formule (21) s'écrit, pour toute série $f \in \mathfrak{o}$,

$$R_z f = \sum_\alpha P_\alpha(z)\, X_\alpha f ; \tag{25}$$

on en tire, d'une part

$$R_{yz} f = \sum_\gamma P_\gamma(yz)\, X_\gamma f, \tag{26}$$

de l'autre

$$R_y(R_z f) = \sum_\alpha P_\alpha(y)\, X_\alpha(R_z f) = \sum_{\alpha,\beta} P_\alpha(y)\, P_\beta(z) \cdot (X_\alpha X_\beta) f . \tag{27}$$

Mais la formule (25) donne aussi, en substituant e à x, puis x à z, la «formule de Taylor» dans G

$$f(x) = \sum_\alpha P_\alpha(x) \cdot X_\alpha(e) f , \tag{28}$$

et de la même manière, on déduit de (27)

$$f(xy) = \sum_{\alpha,\beta} P_\alpha(x)\, P_\beta(y) \cdot (X_\alpha X_\beta)(e) f \tag{29}$$

et en particulier

$$P_\gamma(yz) = \sum_{\alpha,\beta} c_{\alpha\beta\gamma}\, P_\alpha(y)\, P_\beta(z) \tag{30}$$

où on a posé $c_{\alpha\beta\gamma} = (X_\alpha X_\beta)(e)\, P_\gamma$.

Portant dans (26), il vient

$$R_{yz} f = \sum_\gamma \Big(\sum_{\alpha,\beta} c_{\alpha\beta\gamma}\, P_\alpha(y)\, P_\beta(z)\Big)\, X_\gamma f$$

et comme $R_{yz} = R_y R_z$, le th. 3 prouve que l'on a

$$X_\alpha X_\beta = \sum_\gamma c_{\alpha\beta\gamma} X_\gamma . \tag{31}$$

Autrement dit, les constantes $c_{\alpha\beta\gamma}$ définissent complètement la multiplication dans l'algèbre associative $\mathfrak{G}$; nous dirons que ce sont les *constantes de structure* de l'algèbre $\mathfrak{G}$, ou du groupe G.

Notons encore que (25) donne en particulier

$$P_\alpha(xy) = \sum_\beta P_\beta(y) \cdot X_\beta\, P_\alpha . \tag{32}$$

Si on compare cette formule à (30), il résulte du th. 3 que

$$X_\beta\, P_\alpha = \sum_\gamma c_{\gamma\beta\alpha}\, P_\gamma . \tag{33}$$

La formule (32), où on substitue e à x, donne aussi, en vertu du th. 3

$$X_\alpha(e)\, P_\beta = \delta_{\alpha\beta} \quad \text{(indice de Kronecker)}^5) . \tag{34}$$

---

[5]) Il faut se souvenir que dans toutes les formules (25) à (34) les indices peuvent prendre la valeur 0, avec les conventions $X_0 = I$, $P_0 = 1$ introduites ci-dessus. La formule (31) montre alors que $c_{\alpha 0\beta} = c_{0\alpha\beta} = \delta_{\alpha\beta}$, et $c_{\alpha\beta 0} = 0$ si $\alpha \neq 0$ et $\beta \neq 0$.

Enfin, le th. 3 et la formule (29) entraînent le

Théorème 4. *Pour que le groupe G soit abélien, il faut et il suffit que l'algèbre $\mathfrak{G}$ soit commutative.*

En effet, pour que G soit abélien, il faut et il suffit que $f(xy) = f(yx)$ pour toute série formelle $f \in \mathfrak{o}$; en vertu du th. 3 et de la formule (29), cela équivaut à $(X_\alpha X_\beta)(e) = (X_\beta X_\alpha)(e)$ pour tout couple d'indices α, β, et on sait que cela équivaut à $X_\alpha X_\beta = X_\beta X_\alpha$ (n° 7), ce qui signifie que $\mathfrak{G}$ est commutative.

Remarquons ici que l'*algèbre de Lie* $\mathfrak{g}_0$ de G peut être abélienne sans que G soit abélien, comme le montre l'exemple suivant de Chevalley [4, p. 145—146]: le groupe G est de dimension 2, et défini par la «loi de composition»

$$(x_1, x_2)(y_1, y_2) = (x_1 + y_1 + x_1 y_1, x_2 + y_2 + x_1 y_2 + x_2 y_1^p) .$$

On trouve facilement

$$X_{01} = (1 + x_1) D_{01}, X_{02} = (1 + x_1) D_{02}$$
$$X_{11} = (1 + x_1^p) D_{11} + x_2 D_{02}, X_{12} = (1 + x_1^p) D_{12}$$

d'où l'on déduit que $[X_{01}, X_{02}] = 0$, autrement dit l'algèbre de Lie $\mathfrak{g}_0$ est abélienne ; mais on a $[X_{11}, X_{02}] = -(1 + x_1) D_{02} = -X_{02}$, et l'algèbre $\mathfrak{g}_1$ n'est plus abélienne.

12. Soient G et $\overline{G}$ deux groupes de Lie formels, de dimensions respectives n et m, et soit $\boldsymbol{u} = (u_1, \ldots, u_m)$ une «application» de G dans $\overline{G}$, c'est-à-dire un système de m séries formelles sans terme constant par rapport aux x_i $(1 \leqslant i \leqslant n)$. Pour toute série formelle $\overline{f} \in \mathfrak{o}(\overline{G})$, soit $\overline{f} \circ \boldsymbol{u}$ la série formelle de $\mathfrak{o}(G)$ obtenue en substituant dans $\overline{f}$, à chaque indéterminée $\overline{x}_j$ $(1 \leqslant j \leqslant m)$, la série formelle $u_j(x_1, \ldots, x_n)$. Pour tout opérateur différentiel D dans $\mathfrak{o}(G)$, appartenant à $\mathcal{S}$, considérons la série formelle $D(\overline{f} \circ \boldsymbol{u})$, et désignons par $(\boldsymbol{u}'(D)(\overline{e}))\,\overline{f}$ son terme constant. Supposons maintenant que D appartienne à l'hyperalgèbre de Lie $\mathfrak{G}$ de G ; alors on peut définir un opérateur de l'hyperalgèbre de Lie $\overline{\mathfrak{G}}$ de $\overline{G}$, que nous désignerons par $\boldsymbol{u}'(D)$, par la formule

$$(\boldsymbol{u}'(D)\,\overline{f})(\overline{y}) = (\boldsymbol{u}'(D)(\overline{e}))\,(L_{\overline{y}}\,\overline{f}) . \tag{35}$$

Il est clair en effet que $D(\overline{f} \circ \boldsymbol{u})$ est combinaison linéaire, à coefficients dans $\mathfrak{o}(G)$, des $\overline{X}_\alpha(\overline{e})\,\overline{f}$, et la formule (35) définit bien par suite un opérateur différentiel invariant à gauche.

Cela étant:

Théorème 5. *Si u est un homomorphisme de G dans $\overline{G}$, u' est un homomorphisme de $\mathfrak{G}$ dans $\overline{\mathfrak{G}}$, appliquant $\mathfrak{g}_r$ dans $\overline{\mathfrak{g}}_r$ et $\mathfrak{s}_r$ dans $\overline{\mathfrak{s}}_r$ $(0 \leqslant r < +\infty)$.*

La relation $\overline{f}(u(yx)) = \overline{f}(u(y)\,u(x))$, valable par hypothèse pour toute série $\overline{f} \in \mathfrak{o}(\overline{G})$, peut s'écrire

$$L_y(\overline{f} \circ u) = (L_{u(y)}\,\overline{f}) \circ u\,. \tag{36}$$

En vertu de la formule (28), la formule (36), où on substitue e à x, puis x à y, donne

$$\sum_{\alpha} P_\alpha(x) \cdot (u'(X_\alpha)(\overline{e}))\,\overline{f} = \sum_{\bar{\alpha}} \overline{P}_{\bar{\alpha}}(u(x)) \cdot \overline{X}_{\bar{\alpha}}(\overline{e})\,\overline{f} = \overline{f}(u(x))\,. \tag{37}$$

Si on pose

$$u'(X_\alpha) = \sum_{\bar{\alpha}} a_{\alpha\bar{\alpha}}\,\overline{X}_{\bar{\alpha}} \tag{38}$$

on a par définition $(u'(X_\alpha)(\overline{e}))\,\overline{f} = \sum_{\bar{\alpha}} a_{\alpha\bar{\alpha}}\,\overline{X}_{\bar{\alpha}}(\overline{e})\,\overline{f}$, et il résulte donc de (37), en vertu de l'indépendance linéaire des $\overline{X}_{\bar{\alpha}}(\overline{e})$ sur $\mathfrak{o}(G)$

$$\overline{P}_{\bar{\alpha}}(u(x)) = \sum_{\alpha} a_{\alpha\bar{\alpha}}\,P_\alpha(x)\,. \tag{39}$$

La formule (36) donne de même, en utilisant (29)

$$\sum_{\alpha,\beta} P_\alpha(x)\,P_\beta(y)\,(u'(X_\alpha\,X_\beta)(\overline{e}))\,\overline{f} = \sum_{\bar{\alpha},\bar{\beta}} \overline{P}_{\bar{\alpha}}(u(x))\,\overline{P}_{\bar{\beta}}(u(y))(\overline{X}_{\bar{\alpha}}\,\overline{X}_{\bar{\beta}}(\overline{e}))\,\overline{f} \tag{40}$$

ou, en remplaçant les $\overline{P}_{\bar{\alpha}}(u(x))$ par leurs expressions (39)

$$\sum_{\alpha,\beta} P_\alpha(x)\,P_\beta(y)\,(u'(X_\alpha\,X_\beta)(\overline{e}))\,\overline{f} = \sum_{\alpha,\beta,\bar{\alpha},\bar{\beta}} a_{\alpha\bar{\alpha}}a_{\beta\bar{\beta}}\,P_\alpha(x)\,P_\beta(y)\,(\overline{X}_{\bar{\alpha}}\,\overline{X}_{\bar{\beta}}(\overline{e}))\,\overline{f}$$

d'où, en raison du th. 3

$$u'(X_\alpha\,X_\beta) = \sum_{\bar{\alpha},\bar{\beta}} a_{\alpha\bar{\alpha}}\,a_{\beta\bar{\beta}}\,\overline{X}_{\bar{\alpha}}\,\overline{X}_{\bar{\beta}} = u'(X_\alpha)\,u'(X_\beta) \tag{41}$$

ce qui prouve que u' est un homomorphisme de $\mathfrak{G}$ dans $\overline{\mathfrak{G}}$.

Il est immédiat en outre que si D est une semi-dérivation invariante de hauteur r (resp. une semi-dérivation spéciale), il en est de même de $u'(D)$, puisque $(\overline{f}\overline{g}) \circ u = (\overline{f} \circ u)(\overline{g} \circ u)$, et si $\overline{f} \in \mathfrak{o}_r(\overline{G})$, $\overline{f} \circ u \in \mathfrak{o}_r(G)$. Le théorème 5 est donc complètement démontré.

Nous dirons que u' est l'homomorphisme *dérivé* de u. On observera que deux homomorphismes *distincts* u_1, u_2 donnent des homomorphismes dérivés *distincts*: il résulte en effet de la formule (37) que la donnée de u'

détermine entièrement la valeur de $\bar{f}(\boldsymbol{u}(\boldsymbol{x}))$ pour toute $\bar{f} \in \mathfrak{o}(\bar{G})$, et en particulier les séries $u_j (1 \leqslant j \leqslant m)$, en prenant $\bar{f} = \bar{x}_j$.

13. On sait au contraire qu'on peut avoir $\boldsymbol{u}'(\mathfrak{g}_0) = 0$ même si $\boldsymbol{u}$ n'est pas l'homomorphisme nul [4, p. 146] ; c'est ce qui se passe *toujours* pour un homomorphisme «canonique» important que nous allons maintenant décrire.

Remarquons en premier lieu que si σ est un isomorphisme du corps K sur un corps K^σ et si φ_i^σ désigne la série formelle sur K^σ obtenue en appliquant aux coefficients de φ_i l'isomorphisme σ, les φ_i^σ définissent un «groupe formel» que nous noterons G^σ. Il est clair que pour le groupe G^σ, les séries formelles figurant dans les formules correspondant à (11) et (13) se déduisent des séries formelles de ces formules en appliquant à leurs coefficients l'automorphisme σ ; les «constantes de structure» de G^σ ne sont autres par suite que les $c_{\alpha\beta\gamma}^\sigma$, et les séries formelles coefficients des X_α pour le groupe G^σ sont les séries P_α^σ obtenues en appliquant σ aux coefficients de P_α.

Considérons en particulier l'isomorphisme $\xi \to \xi^p$ de K sur K^p, et désignons par $G^{(1)}$ le groupe correspondant, par $P_\alpha^{(1)}$ le coefficient de X_α pour ce groupe. Soit alors $\boldsymbol{p}$ l'application de G dans $G^{(1)}$ obtenue en remplaçant x_i par x_i^p $(1 \leqslant i \leqslant n)$; il s'agit bien d'un homomorphisme, car en vertu des définitions précédentes, on a

$$\varphi_i^{(1)}(\boldsymbol{p}(\boldsymbol{x}), \boldsymbol{p}(\boldsymbol{y})) = (\varphi_i(\boldsymbol{x}, \boldsymbol{y}))^p .$$

Cherchons alors l'image $\boldsymbol{p}'(X_{ri})$; on a, par définition

$$(\boldsymbol{p}'(X_{ri})(\boldsymbol{e}))\, f = X_{ri}(\boldsymbol{e})(f \circ \boldsymbol{p}) = D_{ri}(\boldsymbol{e})(f \circ \boldsymbol{p}) .$$

Mais, par définition des semi-dérivations D_{ri}, le dernier membre de cette formule n'est autre que $D_{r-1,i}(\boldsymbol{e})\, f$, d'où

$$\boldsymbol{p}'(X_{ri}) = X_{r-1,i} \tag{42}$$

en posant $X_{-1,i} = 0 (1 \leqslant i \leqslant n)$. Comme $\boldsymbol{p}'$ est un homomorphisme, on déduit de là aussitôt que l'on a

$$\left.\begin{aligned} &\boldsymbol{p}'(X_\alpha) = 0 \text{ si } \alpha \text{ n'est pas de la forme } p\beta = (p\beta_1, \ldots, p\beta_n) \\ &\boldsymbol{p}'(X_{p\beta}) = X_\beta . \end{aligned}\right\} \tag{43}$$

Si on applique l'homomorphisme $\boldsymbol{p}'$ à la formule (31), il vient

$$\left.\begin{aligned} &c_{\alpha,\beta,p\gamma} = 0 \text{ si } \alpha \text{ ou } \beta \text{ n'est pas multiple de } p \\ &c_{p\alpha,p\beta,p\gamma} = c_{\alpha\beta\gamma}^p . \end{aligned}\right\} \tag{44}$$

Enfin, la formule (39) donne, compte tenu de la définition de $P^{(1)}$

$$P_{p\alpha}(x) = (P_\alpha(x))^p \,. \tag{45}$$

La formule (42) peut encore s'interpréter en disant que p' applique sur 0 l'algèbre $\mathfrak{s}_1$ (et en particulier l'algèbre de Lie $\mathfrak{g}_0$) ; par passage au quotient, elle donne un *isomorphisme* de l'algèbre de Lie $\mathfrak{g}_r/\mathfrak{s}_r$ sur l'algèbre de Lie $\mathfrak{g}^{(1)}_{r-1}/\mathfrak{s}^{(1)}_{r-1}$ (i. e. l'algèbre de Lie obtenue en appliquant aux constantes de structure de $\mathfrak{g}_{r-1}/\mathfrak{s}_{r-1}$ l'isomorphisme $\xi \to \xi^p$).

14. Les résultats obtenus jusqu'ici sont en parfaite analogie avec ceux de la théorie de Lie classique. Cette analogie ne se poursuit malheureusement pas complètement lorsqu'il s'agit de «remonter» de l'hyperalgèbre de Lie $\mathfrak{G}$ au groupe G. En effet, la réciproque du th. 5 est *inexacte :* il peut y avoir des homomorphismes de $\mathfrak{G}$ dans $\overline{\mathfrak{G}}$, appliquant $\mathfrak{g}_r$ dans $\overline{\mathfrak{g}}_r$ et $\mathfrak{s}_r$ dans $\overline{\mathfrak{s}}_r$ pour tout r, et qui pourtant ne sont pas dérivés d'homomorphismes de $\overline{G}$ dans G.

Nous allons prendre comme exemple le cas où G et $\overline{G}$ sont identiques au groupe le plus simple, le groupe additif de dimension 1, définie par la loi de composition

$$(x, y) \to x + y \,.$$

Nous écrirons ici D_k au lieu de D_{k1} ; pour $\alpha = \sum_{h=0}^{r-1} \lambda_h p^h$, on a $X_\alpha = D_0^{\lambda_0} D_1^{\lambda_1} \ldots D_{r-1}^{\lambda_{r-1}}$, autrement dit, l'hyperalgèbre de Lie $\mathfrak{G}$ est engendrée par les D_k, qui commutent entre eux et sont soumis à la seule condition $D_k^p = 0$ pour tout k. Cela étant, un calcul direct montre facilement que tout homomorphisme u de G dans lui-même est de la forme

$$u(x) = \alpha_0 x + \alpha_1 x^p + \alpha_2 x^{p^2} + \cdots + \alpha_k x^{p^k} + \cdots$$

et l'homomorphisme dérivé est défini par

$$u'(D_k) = \alpha_0^{p^k} D_k + \alpha_1^{p^{k-1}} D_{k-1} + \cdots + \alpha_{k-1}^p D_1 + \alpha_k D_0 \,.$$

Mais il est bien évident qu'il y a beaucoup d'autres homomorphismes de $\mathfrak{G}$ appliquant $\mathfrak{g}_r$ et $\mathfrak{s}_r$ dans eux-mêmes pour tout r ; par exemple, si $p > 2$, il suffit de prendre $v(D_k) = D_k + D_{k-1}^2$.

15. Soient $G, \overline{G}$ et $\overline{\overline{G}}$ trois groupes de Lie formels, u un homomorphisme de G dans $\overline{G}$, v un homomorphisme de $\overline{G}$ dans $\overline{\overline{G}}$, $w = v \circ u$ l'homomorphisme composé. Pour tout élément $D \in \mathfrak{G}$, $w'(D)(\overline{\overline{e}})$ est défini par

$$(\boldsymbol{w}'(D)(\bar{\boldsymbol{e}}))\,\bar{\bar{f}} = (D(\boldsymbol{e}))(\bar{\bar{f}} \circ \boldsymbol{v} \circ \boldsymbol{u}) = (\boldsymbol{u}'(D)(\bar{\boldsymbol{e}}))(\bar{\bar{f}} \circ \boldsymbol{v}) = (\boldsymbol{v}'(\boldsymbol{u}'(D))(\bar{\bar{\boldsymbol{e}}}))\,\bar{\bar{f}}$$

d'où la relation de transitivité

$$(\boldsymbol{v} \circ \boldsymbol{u})' = \boldsymbol{v}' \circ \boldsymbol{u}' . \tag{46}$$

Cette relation nous donne une condition supplémentaire que doit vérifier le dérivé d'un homomorphisme $\boldsymbol{u}$ de G dans $\bar{G}$. En effet, si $\boldsymbol{u}^{(1)}$ désigne l'homomorphisme de $G^{(1)}$ dans $\bar{G}^{(1)}$ obtenu en élevant à la puissance p-ème tous les coefficients des séries u_j, on doit avoir, avec les notations précédentes, $\boldsymbol{p} \circ \boldsymbol{u} = \boldsymbol{u}^{(1)} \circ \boldsymbol{p}$. Tenant compte de (46) et (42), cela donne pour les coefficients $\alpha_{\alpha\bar{\alpha}}$ de la formule (38), les conditions

$$\left.\begin{aligned} a_{\alpha,p\bar{\alpha}} &= 0 \text{ si } \alpha \text{ n'est pas multiple de } p \\ a_{p\alpha,p\bar{\alpha}} &= a^{p}_{\alpha,\bar{\alpha}} . \end{aligned}\right\} \tag{47}$$

Mais ces conditions sont remplies dans l'exemple donné ci-dessus. Lorsqu'on examine la question de plus près, on constate que, pour une «application» *quelconque* $\boldsymbol{u}$ de G dans $\bar{G}$, il existe déjà des relations nécessaires entre les opérateurs $\boldsymbol{u}'(X_\alpha)$. Par exemple, G étant le groupe additif considéré au n° 14, en supposant $p = 3$, on voit que, si

$$u(x) = \lambda_1 x + \lambda_2 x^2 + \lambda_3 x^3 + \ldots ,$$

on a

$$u'(D_0) = \lambda_1 D_0 , \; u'(D_0^2) = \lambda_1^2 D_0^2 + 2\lambda_2 D_0 , \; u'(D_1) = \lambda_1^3 D_1 + \lambda_1 \lambda_2 D_0^2 + \lambda_3 D_0 ;$$

il est donc impossible que l'on ait $u'(D_0^2) = D_0^2$ et que $u'(D_1)$ contienne un terme en D_0^2, comme c'est le cas dans l'exemple précédent. J'espère pouvoir revenir prochainement sur ce sujet dans un autre travail.

16. Tout «changement de variables» (cf. n° 3) définit un changement de base dans l'hyperalgèbre $\mathfrak{G}$; de façon précise, si $\boldsymbol{u} = (u_1, \ldots, u_n)$ est un système de n séries formelles sans terme constant, dont le jacobien a un terme constant $\neq 0$, en définissant un groupe $\bar{G}$ par la loi de composition $\bar{\boldsymbol{x}} \cdot \bar{\boldsymbol{y}} = \boldsymbol{u}(\boldsymbol{u}^{-1}(\bar{\boldsymbol{x}})\,\boldsymbol{u}^{-1}(\bar{\boldsymbol{y}}))$, $\boldsymbol{u}$ est un isomorphisme de G sur $\bar{G}$, et il résulte de (46) que $\boldsymbol{u}'$ est un isomorphisme de $\mathfrak{G}$ sur $\bar{\mathfrak{G}}$, dont $(\boldsymbol{u}^{-1})'$ est l'isomorphisme réciproque. Cela étant, il est clair que les $Y_\alpha = (\boldsymbol{u}^{-1})'(\bar{X}_\alpha)$ constituent une base de $\mathfrak{G}$ pour laquelle les constantes de structure $\bar{c}_{\alpha\beta\gamma}$ sont celles de $\bar{\mathfrak{G}}$. L'exemple du n° 14 montre qu'un changement de base de $\mathfrak{G}$ n'est pas toujours «permis» en ce sens qu'il ne provient pas toujours d'un changement de variables sur G.

Dans ce qui suit, nous allons nous ramener à un type particulier de base pour $\mathfrak{G}$: les n séries formelles $P_{0i}(1 \leqslant i \leqslant n)$ ont chacune x_i comme terme du premier degré, donc un jacobien de terme constant 1 (formule (24)); en prenant $u_i = P_{0i}$, on définit donc un «changement de variables» tel que l'on ait $\boldsymbol{u}'(X_{0i}) = \overline{X}_{0i}$ et $\overline{P}_{0i} = \overline{x}_i$ pour $1 \leqslant i \leqslant n$; on notera par contre que pour $h \geqslant 1$, on n'a pas nécessairement $\boldsymbol{u}'(X_{hi}) = \overline{X}_{hi}$, en d'autres termes les nouvelles constantes de structure $\overline{c}_{\alpha\beta\gamma}$ ne sont pas nécessairement égales aux anciennes (contrairement à ce qui se passe en caractéristique 0, où les X_{0i} engendrent $\mathfrak{G}$). Nous dirons que $\overline{\boldsymbol{x}} \cdot \overline{\boldsymbol{y}}$ est la *loi de composition canonique* correspondant à la base $(\overline{X}_\alpha)$ de $\overline{\mathfrak{G}}$.

17. Un problème fondamental de la théorie consiste à *caractériser* abstraitement les algèbres associatives $\mathfrak{G}$ qui sont des hyperalgèbres d'un groupe de Lie (analogue du «troisième théorème de Lie» dans le cas classique). Ici encore, il se présente des phénomènes sans analogue en caractéristique 0, car les conditions nécessaires obtenues jusqu'ici pour les constantes de structure de $\mathfrak{G}$ *ne sont pas suffisantes*. On le voit aisément dans le cas le plus simple, où $n = 1$ et $p = 2$; en écrivant les équations (33) pour les plus petites valeurs des indices, on trouve entre autres, avec les notations du n° 9 (simplifiées du fait qu'on peut ici supprimer les indices i et j), la condition

$$\mu_0^{(1)}(\lambda_{10}^{(1)} - \lambda_{20}^{(3)}) = 0$$

entre les constantes qui définissent la structure de $\mathfrak{G}$. J'ignore comment se formulent les conditions nécessaires et suffisantes caractérisant les hyperalgèbres de Lie.

18. Soit G un groupe de Lie formel de dimension n. Nous dirons qu'un groupe de Lie formel H de dimension $m \leqslant n$ est un *sous-groupe* de G si, après avoir fait au besoin un changement de variables dans G, la loi de composition de H est donnée par les m séries formelles (en $\overline{\boldsymbol{x}} = (\overline{x}_1, \ldots, \overline{x}_m)$ et $\overline{\boldsymbol{y}} = (\overline{y}_1, \ldots, \overline{y}_m)$)

$$\varphi_i(\overline{x}_1, \ldots, \overline{x}_m, 0, \ldots, 0, \overline{y}_1, \ldots, \overline{y}_m, 0, \ldots, 0) \; (1 \leqslant i \leqslant m)$$

en supposant bien entendu (ce qui est essentiel pour que les conditions d'associativité soient vérifiées) que l'on a

$$\varphi_j(x_1, \ldots, x_m, 0, \ldots, 0, y_1, \ldots, y_m, 0, \ldots, 0) = 0 \qquad (49)$$

pour $m + 1 \leqslant j \leqslant n$. Cela peut encore s'exprimer en disant que l'appli-

cation $\boldsymbol{u}$ de H dans G telle que $u_i(\overline{x}_1, \ldots, \overline{x}_m) = \overline{x}_i$ pour $1 \leqslant i \leqslant m$, et $u_j(\overline{x}_1, \ldots, \overline{x}_m) = 0$ pour $m+1 \leqslant j \leqslant n$, est un homomorphisme. Il résulte aussitôt de la définition de l'homomorphisme dérivé $\boldsymbol{u}'$ que l'on a $\boldsymbol{u}'(\overline{X}_{hi}) = X_{hi}$ pour $1 \leqslant i \leqslant m$ et pour tout $h \geqslant 0$. On en conclut que $\boldsymbol{u}'(\overline{X}_\alpha) = X_\alpha$ pour tout indice $\alpha = (\alpha_1, \ldots, \alpha_n)$ tel que $\alpha_j = 0$ pour $m+1 \leqslant j \leqslant n$ (nous dirons pour abréger qu'un tel indice est *de dimension m*) ; par suite, dans la formule (38), on a ici $a_{\bar{\alpha}\alpha} = 1$ pour α de dimension m et $\alpha = \bar{\alpha}$, et $a_{\bar{\alpha}\alpha} = 0$ pour tout autre couple d'indices. Le th. 5 montre alors que l'on a $c_{\alpha\beta\gamma} = 0$ si α et β sont de dimension m et si γ n'est pas de dimension m ; en d'autres termes, le sous-espace $\mathfrak{H}$ de $\mathfrak{G}$ ayant pour base les X_α de dimension m est une *sous-algèbre* de $\mathfrak{G}$; nous dirons qu'une telle sous-algèbre est une *sous-algèbre typique* de $\mathfrak{G}$.

Comme on a d'après (39) $P_{0j}(\overline{\boldsymbol{x}}) = \sum_{\bar{\alpha}} a_{\bar{\alpha}\varepsilon_j} \overline{P}_{\bar{\alpha}}(\overline{\boldsymbol{x}})$ (où on a posé $\varepsilon_j = (0, \ldots, 0, 1, 0, \ldots, 0)$, 1 étant à la j-ème place), on conclut de ce qui précède que pour $j \geqslant m+1$, on a $P_{0j}(\overline{\boldsymbol{x}}) = 0$ et $P_{0j}(\overline{\boldsymbol{x}}) = \overline{P}_{0j}(\overline{\boldsymbol{x}})$ pour $j \leqslant m$. En d'autres termes, si on fait le changement de coordonnées $x'_i = P_{0i}(\boldsymbol{x})$, donnant sur G la loi de composition *canonique* (correspondant à la base (X_α))

$$\varphi'_i(x'_1, \ldots, x'_n, y'_1, \ldots, y'_n) \quad (1 \leqslant i \leqslant n)$$

alors la loi de composition canonique sur H (correspondant à la base $(\overline{X}_\alpha)$ de $\mathfrak{H}$) est donnée par

$$\varphi'_i(x'_1, \ldots, x'_m, 0, \ldots, 0, y'_1, \ldots, y'_m, 0, \ldots, 0) \quad (1 \leqslant i \leqslant m)\,.$$

Nous dirons que le groupe formel défini par cette loi de composition est un *sous-groupe typique* de G.

Il semble naturel de supposer que, réciproquement, toute sous-algèbre typique de $\mathfrak{G}$ est l'hyperalgèbre d'un sous-groupe typique de G, mais je ne sais démontrer ni infirmer cette conjecture.

19. Nous nous proposons maintenant d'étudier plus en détail les homomorphismes d'un groupe formel G dans un groupe formel $\overline{G}$ lorsque le corps de base K est *parfait*[6]). Soient m et n les dimensions de G et $\overline{G}$, et $\boldsymbol{u}$ un homomorphisme de G dans $\overline{G}$.

Théorème 6. *Par des changements de variables dans G et $\overline{G}$, on peut supposer que l'on a*

---

[6]) Pour la nécessité de cette restriction dans les considérations qui suivent, voir un contre-exemple de Chevalley [4, p. 119].

$$\left.\begin{aligned}
&u_i(x) = x_i \quad \textit{pour} \quad 1 \leqslant i \leqslant r_0 \\
&u_i(x) = x_i^p \quad \textit{pour} \quad r_0 + 1 \leqslant i \leqslant r_0 + r_1 \\
&\cdots\cdots\cdots \\
&u_i(x) = x_i^{p^t} \quad \textit{pour} \quad r_0 + \cdots + r_{t-1} + 1 \leqslant i \leqslant r_0 + \cdots + r_t \\
&u_i(x) = 0 \quad \textit{pour} \quad i > r_0 + \cdots + r_t
\end{aligned}\right\} \tag{54}$$

les r_h étant des entiers $\geqslant 0$, éventuellement nuls.

Nous démontrerons d'abord la forme affaiblie suivante de ce théorème:

Théorème 6′. *Par des changements de variables dans G et $\overline{G}$, on peut supposer que l'on a*

$$\left.\begin{aligned}
&u_i(x) = x_i \ \textit{pour} \ 1 \leqslant i \leqslant r_0 \\
&u_i(x) = x_i^p + S_i(x) \ \textit{pour} \ r_0 + 1 \leqslant i \leqslant r_0 + r_1 \\
&\cdots\cdots\cdots \\
&u_i(x) = x_i^{p^t} + S_i(x) \ \textit{pour} \ r_0 + \cdots + r_{t-1} + 1 \leqslant i \leqslant r_0 + \cdots + r_t \\
&u_i(x) = 0 \ \textit{pour} \ i > r_0 + \cdots + r_t
\end{aligned}\right\} \tag{55}$$

où les S_i sont des séries formelles telles que: 1° tout monôme de S_i contient au moins deux x_j d'indices distincts; 2° si $r_0 + \cdots + r_{h-1} + 1 \leqslant i \leqslant r_0 + \cdots + r_h$, tout monôme de S_i a un degré total $> p^h$.

Nous prouverons ensuite (n° 24) que le th. 6′ entraîne le th. 6.

20. Pour démontrer le th. 6′, nous allons procéder par récurrence sur l'indice h de r_h. Nous poserons $s_h = r_0 + \cdots + r_h$, et nous partirons de l'hypothèse de récurrence suivante:

(A_h) *Par des changements de variables dans G et $\overline{G}$, on peut supposer que l'on a*

$$u_i(x) = x_i^{p^k} + w_i(x) \ \textit{pour} \ s_{k-1} < i \leqslant s_k, \ 0 \leqslant k \leqslant h;$$
$$u_i(x) = (v_i(x))^{p^h} + w_i(x) \ \textit{pour} \ i > s_h$$

où les séries formelles v_i et w_i ont les propriétés suivantes:

a) *On a $w_i = 0$ pour $i \leqslant r_0 = s_0$. Pour $1 \leqslant k \leqslant h$ et $s_{k-1} + 1 \leqslant i \leqslant s_k$, on a $w_i = w_{i0} + w_{i1}^p + w_{i2}^{p^2} + \cdots + w_{i,k-1}^{p^{k-1}}$*

où tout monôme de w_i contient au moins deux x_j distincts, et tout monôme de w_{iq} contient un x_j d'indice j tel que $s_{q-1} + 1 \leqslant j \leqslant s_q (0 \leqslant q \leqslant k-1)$.

b) *Pour $i > s_h$, v_i ne contient aucun x_j tel que $j \leqslant s_h$, et*
$w_i = w_{i0} + w_{i1}^p + w_{i2}^{p^2} + \cdots + w_{ih}^{p^h}$

où tout monôme de w_i contient au moins deux x_j distincts, et tout monôme de w_{iq} contient un x_j d'indice j tel que $s_{q-1} + 1 \leqslant j \leqslant s_q$ $(0 \leqslant q \leqslant h)$.

c) *Pour $k \leqslant h$ et $s_{k-1} + 1 \leqslant i \leqslant s_k$, tout monôme de w_i a un degré total $> p^k$.*

d) *Pour $i > s_h$, tout monôme de v_i est au moins de degré total 2, et tout monôme de w_i est au moins de degré total $p^h + 1$.*

Partant de (A_h), nous allons démontrer (A_{h+1}) en plusieurs étapes.

I. *Si $v_i = 0$ pour $i > s_h$, on peut faire des changements de variables dans G et $\overline{G}$, laissant invariants les x_j et $\overline{x}_j$ d'indice $j \leqslant s_h$, et tels que $u_i = 0$ pour $i > s_h$.* En effet, l'hypothèse que $\boldsymbol{u}$ est un homomorphisme signifie que, pour $1 \leqslant i \leqslant n$, on a

$$\begin{aligned} &u_i(\boldsymbol{x}) + u_i(\boldsymbol{y}) + \overline{\psi}_i(\boldsymbol{u}(\boldsymbol{x}), \boldsymbol{u}(\boldsymbol{y})) = \\ &u_i(x_1 + y_1 + \psi_1(\boldsymbol{x}, \boldsymbol{y}), \ldots, x_m + y_m + \psi_m(\boldsymbol{x}, \boldsymbol{y})) \,. \end{aligned} \tag{56}$$

Appliquons cette formule à un $i > s_h$: considérons un des termes de $w_i (= u_i)$ de plus bas degré d, soit $c x_1^{\alpha_1} \ldots x_m^{\alpha_m}$, et montrons en premier lieu que ce terme ne peut contenir *aucun* x_j *d'indice* $j > s_h$. Supposons en effet le contraire, et soit $\alpha_j = a p^s$, où $a \not\equiv 0 \pmod{p}$. Alors le terme considéré fournit au second membre de (56) le terme

$$c a y_j^{p^s} \, x_1^{\alpha_1} \ldots x_j^{(a-1)p^s} \ldots x_m^{\alpha_m} \,. \tag{57}$$

Ce terme ne peut se réduire avec aucun autre terme du second membre de (56) ; en effet, un tel terme ne pourrait que provenir d'un monôme $c' x_1^{\beta_1} \ldots x_m^{\beta_m}$, où on remplace, ou bien p^s facteurs x_j par y_j, ou bien au moins un des x_k par $\psi_k(\boldsymbol{x}, \boldsymbol{y})$ et au plus $p^s - q$ facteurs x_j par y_j, si q facteurs x_k sont remplacés par un ψ_k. Mais dans le premier cas, on a un terme de la même forme que (57), mais avec des exposants des x_k qui ne peuvent être tous les mêmes, puisque $(\beta_1, \ldots, \beta_m) \neq (\alpha_1, \ldots, \alpha_m)$; et dans le second cas, comme tout terme de $\psi_k(\boldsymbol{x}, \boldsymbol{y})$ contient au moins un x_l, le degré des termes que l'on obtient, par rapport aux x_l, est au moins $d + 1 - p^s$, ce qui interdit toute réduction avec (57).

D'autre part, le terme (57) ne peut se réduire avec aucun terme du premier membre de (56). En effet, en vertu de l'hypothèse b) dans (A_h), il ne pourrait se réduire qu'avec un terme provenant de $\overline{\psi}_i(\boldsymbol{u}(\boldsymbol{x}), \boldsymbol{u}(\boldsymbol{y}))$. Mais un tel terme provient nécessairement d'un produit d'un $u_k(\boldsymbol{y})$ et d'autres séries formelles ; et l'hypothèse (A_h), jointe à l'hypothèse que $v_i = 0$ pour $i > s_h$, prouve qu'aucun $u_k(\boldsymbol{y})$ ne peut contenir de monômes où le seul y_l qui figure soit y_j.

Prouvons ensuite que, pour $s_{k-1} + 1 \leqslant j \leqslant s_k$, l'exposant α_j dans le terme considéré de w_i, est nécessairement *multiple de* p^k. Dans le cas contraire, on aurait encore $\alpha_j = ap^s$, avec $s < k$ et $a \not\equiv 0 \pmod{p}$, et le terme $cx_1^{\alpha_1} \ldots x_m^{\alpha_m}$ de w_i fournirait le terme (57) au second membre de (56). On voit exactement comme ci-dessus que ce terme ne peut se réduire avec aucun autre du second membre de (56) ; en outre, il ne peut se réduire avec aucun terme du premier membre de (56), car aucun $u_k(y)$ ne peut contenir de monômes $\lambda y_j^{p^s}$ avec $s < k$ en raison de l'hypothèse (A_h).

Soit alors f_d le polynôme homogène, somme des termes de plus bas degré total d dans w_i ; ce qui précède montre qu'il existe un polynôme $\overline{f}_d$ tel que

$$f_d(x_1, \ldots, x_{s_h}) = \overline{f}_d(x_1, \ldots, x_{r_0}, x_{r_0+1}^p, \ldots, x_{s_h}^{p^h})$$

Faisons dans $\overline{G}$ le changement de variables tel que $\overline{x}'_j = \overline{x}_j$ pour $j \neq i$, $\overline{x}'_i = \overline{x}_i - \overline{f}_d(\overline{x}_1, \ldots, \overline{x}_{r_0}, \overline{x}_{r_0+1}, \ldots, \overline{x}_{s_h})$; en vertu de l'hypothèse (A_h), les u_j d'indice $j \neq i$ ne sont pas modifiés, et u_i est remplacé par une série formelle du même type, mais dont les termes de plus bas degré sont au moins de degré $d + 1$. On peut donc poursuivre le procédé, et définir par récurrence une suite de polynômes isol-ares $\overline{f}_\nu(\overline{x}_1, \ldots, \overline{x}_{s_h})$ telle que $\overline{f}_\nu$ soit de poids $\nu \geqslant d$ et que, en posant $\overline{g} = \sum_{\nu=d}^{\infty} \overline{f}_\nu$, le changement de variables $\overline{x}'_j = \overline{x}_j$ pour $j \neq i$, $x'_i = \overline{x}_i - \overline{g}(\overline{x}_1, \ldots, \overline{x}_{s_h})$ laisse invariants les u_j d'indice $j \neq i$, mais remplace u_i par 0. Notre assertion est ainsi démontrée.

21. Dans le cas examiné dans I, le th. 6′ est démontré. Supposons maintenant que l'une au moins des séries $v_i (i > s_h)$ soit $\not\equiv 0$. Alors:

II. *Toutes les séries formelles* $v_i (i > s_h)$ *sont des puissances p-èmes exactes.* Posons $\boldsymbol{x}^{(h)} = (0, \ldots, 0, x_{s_h+1}, \ldots, x_m)$; les relations (56) donnent, en vertu de l'hypothèse (A_h), pour $s_{k-1} + 1 \leqslant i \leqslant s_k$

$$\overline{\psi}_i(\boldsymbol{u}(\boldsymbol{x}^{(h)}), \boldsymbol{u}(\boldsymbol{y}^{(h)})) = (\psi_i(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}))^{p^k} + w_i(\psi_1(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}), \ldots, \psi_{s_h}(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}),$$
$$x_{s_h+1} + y_{s_h+1} + \psi_{s_h+1}(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}), \ldots, x_m + y_m + \psi_m(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)})) . \qquad (58)$$

On déduit de cette formule, par récurrence sur k, que la série formelle $\psi_i(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)})^{p^k}$ *ne peut contenir de monômes dans lesquels les puissances des* y_l *se réduisent à* y_j^α *avec* $\alpha \leqslant p^h$ *et* $j > s_h$. En effet, c'est évident pour $k = 0$, car en vertu de (A_h), aucun $u_k(\boldsymbol{y})$ ne peut contenir de monôme λy_j^α avec $\alpha \leqslant p^h$ et $j > s_h$; et, en utilisant (A_h) et l'hypothèse

de récurrence, le même raisonnement s'applique pour tout k, en remarquant que, pour $0 \leqslant q \leqslant k-1$, tout monôme de w_{iq} contient un x_l tel que $s_{q-1}+1 \leqslant l \leqslant s_q$.

Cela étant, supposons que pour un $i > s_h$, $v_i \neq 0$ ne soit pas une puissance p-ème. Comme K est parfait, cela signifie qu'il y a au moins un monôme dans v_i dont les exposants ne sont pas multiples de p; soit $c\,x_{s_h+1}^{\lambda} \ldots x_m^{\nu}$ un de ces monômes de plus petit degré total d, et supposons que $\mu = \alpha_j \not\equiv 0 \pmod{p}$. Substituons $\boldsymbol{x}^{(h)}$ et $\boldsymbol{y}^{(h)}$ à $\boldsymbol{x}$ et $\boldsymbol{y}$ dans (56), ce qui donne

$$u_i(\boldsymbol{x}^{(h)}) + u_i(\boldsymbol{y}^{(h)}) + \overline{\psi}_i(\boldsymbol{u}(\boldsymbol{x}^{(h)}), \boldsymbol{u}(\boldsymbol{y}^{(h)}))$$

$$= (v_i(x_{s_h+1} + y_{s_h+1} + \psi_{s_h+1}(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}), \ldots, x_m + y_m + \psi_m(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)})))^{p^h}$$

$$+ w_i(\psi_1(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}), \ldots, \psi_{s_h}(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}),$$

$$x_{s_h+1} + y_{s_h+1} + \psi_{s_h+1}(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}), \ldots, x_m + y_m + \psi_m(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}))\ . \qquad (59)$$

Le monôme considéré dans v_i fournit au second membre de (59) le terme

$$(c\,\mu\, x_{s_h+1}^{\lambda} \ldots x_j^{\mu-1} \ldots x_m^{\nu}\, y_j)^{p^h}\ . \qquad (60)$$

Montrons d'abord que ce terme ne peut se réduire avec aucun autre du second membre de (59). En effet, on voit comme dans I qu'il ne peut se réduire avec aucun autre terme provenant d'un monôme de v_i de degré total $\geqslant d$; d'autre part, les monômes de v_i de degré total $< d$ sont par hypothèse des puissances p-èmes, et donnent donc au second membre de (59) des puissances p^{h+1}-èmes qui ne peuvent se réduire avec (60). Enfin, en vertu de (A_h), tout monôme de $w_{iq}(0 \leqslant q \leqslant h)$ contient un x_l tel que $s_{q-1}+1 \leqslant l \leqslant s_q$, donc tout terme du second membre de (59) qui provient de w_i est un monôme figurant dans un produit de séries formelles dont un des facteurs est un $(\psi_l(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}))^{p^q}$ où $s_{q-1}+1 \leqslant l \leqslant s_q$; du résultat démontré au début de ce n°, il suit qu'un tel produit ne peut contenir aucun monôme de la forme (60).

Comme (60) contient au moins un x_k, il ne pourrait être égal qu'à un terme du premier membre de (59) provenant de $\overline{\psi}_i(\boldsymbol{u}(\boldsymbol{x}^{(h)}), \boldsymbol{u}(\boldsymbol{y}^{(h)}))$; mais aucun terme tel que (60) ne peut figurer dans cette série formelle, puisqu'aucun des $u_k(\boldsymbol{y})$ ne contient de monôme λy_j^{α} avec $\alpha \leqslant p^h$ et $j > s_h$. Notre assertion est donc établie.

22. Posons $v_i = V_i^p$ pour $i > s_h$; nous allons supposer tout d'abord qu'une au moins des séries V_i n'est pas une puissance p-ème. Dans ces conditions:

III. *Il existe un indice* $i > s_h$ *au moins tel que* V_i *contienne un terme du premier degré.* Supposons en effet le contraire ; alors aucun $u_k(\boldsymbol{y})$ ne peut contenir de monôme λy_j^α avec $j > s_h$ et $\alpha \leqslant p^{h+1}$; on en déduit, comme au début du n° 21, que la série formelle $(\psi_i(\boldsymbol{x}^{(h)}, \boldsymbol{y}^{(h)}))^{p^k}$ (pour $s_{k-1} + 1 \leqslant i \leqslant s_k$) ne peut contenir de monômes dans lesquels les puissances des y_l se réduisent à y_j^α avec $j > s_h$ et $\alpha \leqslant p^{h+1}$. Considérons alors, dans un V_i, un monôme de plus bas degré d parmi ceux qui ne sont pas des puissances p-èmes (il en existe par hypothèse) ; soit $c\, x_{s_h+1}^\lambda \ldots x_m^\nu$ un de ces monômes, et supposons que $\mu = \alpha_j \not\equiv 0 \pmod{p}$. Ce monôme fournit au second membre de (59) le terme

$$(c\ \mu\ x_{s_h+1}^\lambda \ldots x_j^{\mu-1} \ldots x_m^\nu\ y_j)^{p^{h+1}} \tag{61}$$

qui contient au moins un x_k, puisque $d > 1$ par hypothèse. On voit alors, exactement comme au n° 21, que le terme (61) ne peut se réduire avec aucun autre, ni au second, ni au premier membre de (59).

Considérons alors dans chacune des $V_i (i > s_h)$ le polynôme formé par les termes du premier degré, et soit $r_{h+1} \geqslant 1$ le rang de ce système de formes linéaires ; par changements de variables linéaires dans G et dans $\overline{G}$ (laissant invariants les x_i et $\overline{x}_i$ d'indice $i \leqslant s_h$), on peut supposer que les termes du premier degré dans V_i se réduisent à x_i pour $s_h + 1 \leqslant i \leqslant s_h + r_{h+1} = s_{h+1}$, et qu'il n'y ait aucun terme du premier degré dans V_i pour $i > s_{h+1}$. Le changement de variables dans G, laissant invariants les x_i d'indice $\leqslant s_h$ ou $> s_{h+1}$ et tel que $x_i' = V_i$ pour $s_h + 1 \leqslant i \leqslant s_{h+1}$, permet de supposer que $V_i = x_i$ pour $s_h + 1 \leqslant i \leqslant s_{h+1}$.

Pour $i > s_{h+1}$, posons $V_i = f_i(x_{s_h+1}, \ldots, x_{s_{h+1}}) + W_i$, où tout monôme de W_i contient au moins un x_j tel que $j > s_{h+1}$; le changement de variables dans $\overline{G}$ tel que $\overline{x}_i' = \overline{x}_i$ pour $i \leqslant s_{h+1}$ et

$$\overline{x}_i' = \overline{x}_i - f_i^{(h)}(\overline{x}_{s_h+1}, \ldots, \overline{x}_{s_{h+1}})$$

pour $i > s_{h+1}$ (où $f_i^{(h)}$ désigne le polynôme obtenu en transformant les coefficients de f_i par l'isomorphisme $\xi \to \xi^{p^h}$) remplace les séries u_i, pour $i > s_{h+1}$, par des séries de même forme, mais où tout monôme de V_i contient au moins un x_j d'indice $j > s_{h+1}$; nous pouvons donc supposer désormais cette condition vérifiée.

Posons alors $V_i = \overline{v}_i(x_{s_h+1}, \ldots, x_m) + w_{i,h+1}$, où tout monôme de $w_{i,h+1}$ contient au moins deux x_j distincts, et au moins un x_j tel que $s_h + 1 \leqslant j \leqslant s_{h+1}$; en outre tout monôme de $\overline{v}_i$ est au moins de degré total 2.

23. Nous sommes donc parvenus à remplir toutes les conditions de (A_{h+1}), sauf les conditions $d)$ en ce qui concerne les degrés des monômes des w_i pour $i > s_{h+1}$. Comme tout monôme de w_i contient au moins deux x_j distincts, son degré total est $\geqslant 2p^{h+1}$ s'il est puissance p^{h+1}-ème. Considérons, parmi les monômes de w_i, un monôme de plus petit degré total d, et supposons que ce monôme $cx_1^{\alpha_1} \dots x_m^{\alpha_m}$ soit tel que $d \leqslant p^{h+1}$. Montrons d'abord que les α_j sont nuls pour $j > s_{h+1}$; comme tout monôme de w_i contient au moins deux x_j distincts, il suffira de prouver que α_j est nécessairement *multiple de* p^{h+1}. En effet, il suffit pour le voir de raisonner comme au n° 20, en remarquant qu'aucun $u_k(\mathbf{y})$ ne peut contenir de monôme $\lambda y_j^{p^s}$ avec $j > s_{h+1}$ et $s \leqslant h+1$ (puisque le degré total de $\bar{v}_i$ est $\geqslant 2$ pour $i > s_{h+1}$). Un raisonnement analogue montre que, pour $s_{k-1} < j \leqslant s_k$, avec $k \leqslant h+1$, α_j est nécessairement *multiple de* p^k. On voit donc que le polynôme f_d, somme des termes de plus bas degré d dans w_i, est tel que

$$f_d(x_1, \dots, x_m) = \bar{f}_d(x_1, \dots x_{r_0}, x_{r_0+1}^p, \dots, x_{s_h}^{p^h}) .$$

pour un polynôme $\bar{f}_d$ convenable. Procédant comme au n° 20, on peut donc faire un changement de variables dans $\bar{G}$ de sorte que le degré minimum des monômes de w_i soit $> p^{h+1}$.

Nous avons donc prouvé que la récurrence peut se poursuivre si aucune des séries V_i n'est une puissance p-ème. Dans le cas contraire, on peut écrire $V_i = U_i^{p^q}$, où une au moins des séries formelles U_i n'est pas puissance p-ème. Alors, aucun $u_k(\mathbf{y})$ ne peut contenir de monôme λy_j^{α} avec $j > s_h$ et $\alpha \leqslant p^{h+q+1}$; on en déduit comme au n° 22 que l'un au moins des U_i contient un terme du premier degré ; le raisonnement se poursuit alors comme ci-dessus, mais cette fois on passe directement des hypothèses (A_h) aux hypothèses (A_{h+q+1}) (avec $r_k = 0$ pour

$$h+1 \leqslant k \leqslant h+q) .$$

Le théorème 6′ est donc complètement démontré.

24. Montrons enfin comment on peut déduire le th. 6 du th. 6′. Supposons que $s_{h-1}+1 \leqslant i \leqslant s_h$, et considérons dans S_i un terme de plus bas degré d parmi ceux qui *ne sont pas puissances* p^h*-èmes* ; si $cx_1^{\alpha_1} \dots x_m^{\alpha_m}$ est un tel terme, alors, pour $s_{k-1}+1 \leqslant j \leqslant s_k$, α_j est *multiple de* p^k. En effet, si $\alpha_j = ap^s$, avec $a \not\equiv 0 \pmod{p}$ et $s < k$, le terme (57) ne peut se réduire au second membre de (56) avec aucun autre, par le même raisonnement qu'au n° 21 si $k < h$. Si au contraire $k \geqslant h$, il faut remarquer en outre que tout terme du second membre de

(56) qui provient d'un monôme de S_i qui est puissance p^h-ème est lui-même puissance p^h-ème ; or, cela ne pourrait être le cas de (57) que si $s \geqslant h$ et si les α_l d'indice $\neq j$ étaient multiples de p^h ; mais alors $c x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ serait une puissance p^h-ème, contrairement à l'hypothèse. On conclut alors le raisonnement en remarquant que (57) ne peut se réduire avec aucun monôme du premier membre de (56), car aucun $u_k(\boldsymbol{y})$ ne peut contenir de monôme λy_j^{α} avec $\alpha < p^k$, en raison des formules (55). Procédant comme au n° 20, on peut donc faire un changement de variables dans $\overline{G}$ de sorte que $S_i = T_i^{p^h}$ pour tout i tel que

$$s_{h-1} < i \leqslant s_h \quad (0 \leqslant h \leqslant t) ;$$

mais alors le changement de variables $x_i' = x_i + T_i(\boldsymbol{x})$ dans G donne finalement les formules (54), ce qui achève de démontrer le th. 6.

25. Nous dirons que le nombre $\varrho = r_0 + r_1 + \cdots + r_t$ est le *rang* de l'homomorphisme $\boldsymbol{u}$. Le th. 6 prouve que les relations $u_i(\boldsymbol{x}) = 0 (1 \leqslant i \leqslant n)$ sont équivalentes à $x_1 = x_2 = \ldots = x_\varrho = 0$; comme

$$\boldsymbol{u}(\boldsymbol{xy}) = \boldsymbol{u}(\boldsymbol{x})\, \boldsymbol{u}(\boldsymbol{y}) ,$$

les n séries formelles $u_i(\boldsymbol{xy})$ s'annulent quand on y annule les ϱ premières coordonnées de $\boldsymbol{x}$ et de $\boldsymbol{y}$; cela signifie que l'on a

$$\varphi_i(0, \ldots, 0, x_{\varrho+1}, \ldots, x_m, 0, \ldots, 0, y_{\varrho+1}, \ldots, y_m) = 0 \quad (1 \leqslant i \leqslant \varrho) ;$$

par suite, les séries formelles

$$\varphi_{\varrho+j}(0, \ldots, 0, x_{\varrho+1}, \ldots, x_m, 0, \ldots, 0, y_{\varrho+1}, \ldots, y_m) (1 \leqslant j \leqslant m - \varrho)$$

définissent un sous-groupe formel H de G, de dimension $m - \varrho$, le *noyau* de $\boldsymbol{u}$.

D'autre part, on a $u_i(\boldsymbol{xy}) = 0$ pour $i > \varrho$, et par suite, en vertu de (54)

$$\overline{\varphi}_i(x_1, \ldots, x_\varrho^{p^t}, 0, \ldots, 0, y_1, \ldots, y_\varrho^{p^t}, 0, \ldots, 0) = 0 \quad \text{pour} \quad i > \varrho$$

d'où on conclut aussitôt que les ϱ séries formelles

$$\overline{\varphi}_j(\overline{x}_1, \ldots, \overline{x}_\varrho, 0, \ldots, 0, \overline{y}_1, \ldots, \overline{y}_\varrho, 0, \ldots, 0) \quad (1 \leqslant j \leqslant \varrho)$$

définissent un sous-groupe formel L de $\overline{G}$, de dimension ϱ, *l'image* de $\boldsymbol{u}$. La somme des dimensions de H et de L est égale à la dimension m de G, ce qui, pour les groupes formels sur un corps parfait, démontre une conjecture de Chevalley [4, p. 119].

26. Remarquons maintenant que $\boldsymbol{u}'(X_{hi}(\boldsymbol{e}))\,\overline{f}$ est le coefficient de $x_i^{p^h}$ dans la série formelle $\overline{f}(\boldsymbol{u}(\boldsymbol{x}))$. Le th. 6 prouve que l'on a

$$\left.\begin{aligned}
&\boldsymbol{u}'(X_{hi}) = \overline{X}_{hi} \quad \text{pour} \quad 1 \leqslant i \leqslant r_0\\
&\boldsymbol{u}'(X_{hi}) = \overline{X}_{h-1,i} \quad \text{pour} \quad r_0 + 1 \leqslant i \leqslant r_0 + r_1\\
&\cdots\cdots\cdots\\
&\boldsymbol{u}'(X_{hi}) = \overline{X}_{0i} \quad \text{pour} \quad r_0 + \ldots + r_{h-1} + 1 \leqslant i \leqslant r_0 + \ldots + r_h\\
&\boldsymbol{u}'(X_{hi}) = 0 \quad \text{pour} \quad i > r_0 + \ldots + r_h .
\end{aligned}\right\} \tag{62}$$

Le sous-espace $\mathfrak{a}_0$ de $\mathfrak{g}_0$ engendré par les X_{0i} d'indice $i > r_0$ est donc un *p-idéal* de l'algèbre de Lie $\mathfrak{g}_0$ (c'est-à-dire que si $X \in \mathfrak{a}_0$, on a aussi $X^p \in \mathfrak{a}_0$, en vertu de la relation $\boldsymbol{u}'(X^p) = (\boldsymbol{u}'(X))^p$. D'autre part, d'après (44), si $[X_{0i}, X_{0j}] = \sum_k \lambda_{ijk} X_{0k}$, on a $[X_{hj}, X_{hj}] = \sum_k \lambda_{ijk}^{p^h} X_{hk} + Y$, où $Y \in \mathfrak{s}_h$; on déduit alors aussitôt de (62) que les X_{0i} d'indice

$$i > r_0 + \cdots + r_h$$

forment encore un p-idéal $\mathfrak{a}_h$ de l'algèbre de Lie $\mathfrak{g}_0$. On peut d'ailleurs définir les $\mathfrak{a}_h$ par récurrence de la façon suivante, comme on le vérifie aisément: les $X \in \mathfrak{a}_h$ sont les éléments de la forme $\boldsymbol{p}'^h(Y)$ tels que $Y \in \mathfrak{g}_h$, $\boldsymbol{u}'(Y) = 0$ et $\boldsymbol{p}'^h(Y) \in \mathfrak{a}_{h-1}$. Cette dernière définition prouve que les nombres $r_0, \ldots, r_t$ qui interviennent dans le th. 6 sont *invariants* par changements de variables dans G ou dans $\overline{G}$.

On a ainsi, correspondant à l'homomorphisme $\boldsymbol{u}$, non seulement un idéal $\mathfrak{a}_0$ de $\mathfrak{g}_0$, noyau de $\boldsymbol{u}'$, mais une chaîne descendante de p-idéaux

$$\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \ldots \supset \mathfrak{a}_t$$

dont le dernier est l'*algèbre de Lie du noyau H* de $\boldsymbol{u}$.

Considérons en particulier le cas où $\mathfrak{g}_0$ ne contient *aucun p-idéal non trivial* ; on a alors nécessairement $\mathfrak{a}_i = (0)$ ou $\mathfrak{a}_i = \mathfrak{g}_0$ pour tout indice $i \leqslant t$, et le raisonnement du th. 6 prouve que $r = m$, et que, par des changements de variables convenables, on peut supposer que l'on a $u_i(\boldsymbol{x}) = x_i^{p^h}$ pour $1 \leqslant i \leqslant m$ et pour un certain entier h. Plus particulièrement:

Théorème 7. *Si l'algèbre de Lie* $\mathfrak{g}_0$ *du groupe G ne contient aucun p-idéal non trivial* (et en particulier si $\mathfrak{g}_0$ est *simple*) *tout homomorphisme de G sur un groupe* $\overline{G}$ *définit un isomorphisme de G sur un groupe* $\overline{G}^{(-h)}$.

27. L'algèbre de Lie $\mathfrak{b}$ du groupe L, qui est engendrée par les $\overline{X}_{0i}$ tels que $1 \leqslant i \leqslant \varrho$, n'est nullement isomorphe à l'algèbre de Lie quotient $\mathfrak{g}_0/\mathfrak{a}_t$, comme on pourrait le croire ; par exemple, si $i \leqslant r_0$ et $r_0 < j \leqslant r_0 + r_1$, on a $[\overline{X}_{0i}, \overline{X}_{0j}] = \boldsymbol{u}'([X_{0i}, X_{1j}])$. Désignons par $\mathfrak{b}_h$ le sous-espace de $\mathfrak{b}$ engendré par les $\overline{X}_{0i}$ tels que $i \leqslant r_0 + r_1 + \cdots + r_h$; $\mathfrak{b}_h$ est une *sous-algèbre* de Lie de $\mathfrak{b}$, et $\mathfrak{b}_{h-1}$ un *p-idéal dans* $\mathfrak{b}_h$. En effet, raisonnant par récurrence sur h, il suffit de considérer un produit $[\overline{X}_{0i}, \overline{X}_{0j}]$ où $r_0 + \cdots + r_{h-1} < j \leqslant r_0 + \cdots + r_h$, et $i \leqslant r_0 + \cdots + r_h$; il résulte alors de (62) que $[\overline{X}_{0i}, \overline{X}_{0j}]$ est l'image par $\boldsymbol{u}'$ d'une semi-dérivation de $\mathfrak{s}_h$ si $i \leqslant r_0 + \cdots + r_{h-1}$ et d'une semi-dérivation de $\mathfrak{g}_h$ si $i > r_0 + \cdots + r_{h-1}$. En outre, dans ce dernier cas, on a $[\overline{X}_{0i}, \overline{X}_{0j}] = \boldsymbol{u}'([X_{hi}, X_{hj}]) = \Sigma\, \lambda_{ijk}^{p^h}\, \overline{X}_{0k} + \overline{Y}$, où $\overline{Y} \in \mathfrak{b}_{h-1}$. On voit donc en résumé que l'algèbre de Lie $\mathfrak{b}$ est réunion d'une chaîne ascendante de sous-algèbres

$$\mathfrak{b}_0 \subset \mathfrak{b}_1 \subset \ldots \subset \mathfrak{b}_t = \mathfrak{b}$$

telle que $\mathfrak{b}_{h-1}$ soit un p-idéal dans $\mathfrak{b}_h$, que $\mathfrak{b}_0$ soit isomorphe à l'algèbre de Lie quotient $\mathfrak{g}_0/\mathfrak{a}_0$, et $\mathfrak{b}_h/\mathfrak{b}_{h-1}$ isomorphe à l'algèbre de Lie $(\mathfrak{a}_{h-1}/\mathfrak{a}_h)^{(h)}$ (obtenue en appliquant aux constantes de structure de $\mathfrak{a}_{h-1}/\mathfrak{a}_h$ l'isomorphisme $\xi \to \xi^{p^h}$).

28. Pour terminer, indiquons rapidement comment les «groupes algébriques» définis par Chevalley [4] peuvent être considérés comme cas particuliers des «groupes de Lie formels» étudiés ici. Considérons un espace affine E de dimension m sur K, et une variété algébrique irréductible V contenue dans E, définie par l'idéal premier $\mathfrak{p}$ dans l'anneau $K[X_1, \ldots, X_m]$; nous supposerons que V est de dimension n, et que le point $(0, \ldots, 0)$ est un point *simple* $\boldsymbol{e}$ de V. On définit une *loi de groupe algébrique* sur V de la façon suivante. Considérons la variété produit $V \times V$, définie dans $E \times E$ par l'idéal $\mathfrak{q}$ engendré par $\mathfrak{p} \otimes 1 + 1 \otimes \mathfrak{p}$ dans l'anneau de polynômes $K[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$; soient $\mathfrak{A} = K[X_1, \ldots, X_m]/\mathfrak{p}$ l'anneau des polynômes sur V,

$$\mathfrak{A}' = K[X_1, \ldots, X_m, Y_1, \ldots, Y_m]/\mathfrak{q}$$

l'anneau des polynômes sur $V \times V$, $\mathfrak{R}$ et $\mathfrak{R}'$ les corps de fractions de $\mathfrak{A}$ et $\mathfrak{A}'$ respectivement (corps de fractions rationnelles sur V et $V \times V$). Une *application rationnelle* f (partout définie) de $V \times V$ dans V est déterminée par m éléments $f_1, \ldots, f_m$ de $\mathfrak{R}'$ tels que l'on ait

$$g(f_1, \ldots, f_m) = 0$$

pour tout polynôme g de l'idéal $\mathfrak{p}$; on définit de même des applications rationnelles de V dans V. Comme f_k est le quotient des classes mod. $\mathfrak{q}$ de deux polynômes u_k, v_k de $K[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$, on peut l'écrire $u_k(x_1, \ldots, x_m, y_1, \ldots, y_m)/v_k(x_1, \ldots, x_m, y_1, \ldots, y_m)$, où x_i (resp. y_i) est la classe de X_i (resp. Y_i) mod. $\mathfrak{q}$; on l'écrira aussi

$$f_k(x_1, \ldots, x_m, y_1, \ldots, y_m)$$

ou $f_k(\boldsymbol{x}, \boldsymbol{y})$. Cela étant, une loi de groupe algébrique sur V est donnée par une application rationnelle f de $V \times V$ dans V satisfaisant à la condition d'associativité $f(\boldsymbol{x}, f(\boldsymbol{y}, \boldsymbol{z})) = f(f(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z})$, aux relations $f(\boldsymbol{e}, \boldsymbol{x}) = f(\boldsymbol{x}, \boldsymbol{e}) = \boldsymbol{x}$, et telle qu'il existe une application rationnelle h de V dans V telle que $f(\boldsymbol{x}, h(\boldsymbol{x})) = f(h(\boldsymbol{x}), \boldsymbol{x}) = \boldsymbol{e}$.

La relation $f(\boldsymbol{e}, \boldsymbol{x}) = \boldsymbol{x}$ suppose implicitement que les

$$v_k(0, \ldots, 0, 0, \ldots, 0)$$

sont tous $\neq 0$; cela signifie que les $f_k(\boldsymbol{x}, \boldsymbol{y})$ appartiennent à l'*anneau local* $\mathfrak{L}'$ de $V \times V$ au point $(\boldsymbol{e}, \boldsymbol{e})$. Mais comme $\boldsymbol{e}$ est un point simple sur V, l'idéal maximal $\mathfrak{m}$ de $\mathfrak{L}'$ est engendré par $2n$ éléments

$$s_1, \ldots, s_n, t_1, \ldots, t_n,$$

linéairement indépendants mod. $\mathfrak{m}^2$, et il existe un isomorphisme du complété de $\mathfrak{L}'$ sur l'anneau des séries formelles sur K en $2n$ indéterminées $u_1, \ldots, u_n, v_1, \ldots, v_n$, qui applique s_i sur u_i et t_i sur v_i (cf. [3, p. 57—64]). Par cet isomorphisme, les f_k deviennent n séries formelles par rapport aux u_i et v_i, et les hypothèses sur f signifient que les f_k définissent une structure de *groupe de Lie formel*, ce qui établit le lien avec la théorie de Chevalley, et montre entre autres que tous nos résultats sont applicables aux groupes considérés par cet auteur.

BIBLIOGRAPHIE

[1] *S. Bochner*, Formal Lie groups, Ann. of Math., 47 (1946), p. 192—201.

[2] *N. Bourbaki*, Eléments de Mathématique: Algèbre, chap. IV—V, Actualités Sci. Ind., n° 1102, Paris, (Hermann), 1950.

[3] *C. Chevalley*, Intersections of algebraic and algebroid varieties, Trans. Amer. Math. Soc., 57 (1945), p. 1—85.

[4] *C. Chevalley*, Théorie des groupes de Lie, t. II: Groupes algébriques, Actualités Sc. Ind., n° 1152, Paris (Hermann), 1951.

[5] *J. Dieudonné*, Les semi-dérivations dans les extensions radicielles, C. R. Acad. Sci., Paris, 227 (1948), p. 1319—1320.

[6] *J. Dieudonné*, Semi-dérivations et formule de Taylor en caractéristique p, Arch. Math., 2 (1950), p. 364—366.

[7] *J. Dieudonné*, Les groupes de Lie algébriques sur un corps de caractéristique $p > 0$, Rend. Circ. Mat. Palermo, (2) t. 1 (1953), p. 380–402.

Reçu le 23 juin 1953