

**Zeitschrift:** Commentarii Mathematici Helvetici  
**Herausgeber:** Schweizerische Mathematische Gesellschaft  
**Band:** 28 (1954)

**Artikel:** Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique  $p > 0$ .  
**Autor:** Dieudonné, Jean  
**DOI:** <https://doi.org/10.5169/seals-22613>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 15.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# 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])<sup>1)</sup> 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].

---

<sup>1)</sup> 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]<sup>2</sup>). 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

$$\varphi_i(x_1, \dots, x_n, y_1, \dots, y_n) \quad (1 \leq i \leq n)$$

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

1.  $\varphi_i(x_1, \dots, x_n, 0, \dots, 0) = x_i, \varphi_i(0, \dots, 0, y_1, \dots, y_n) = y_i (1 \leq i \leq n)$ ;
2.  $\varphi_i(\varphi(x, y), z) = \varphi_i(x, \varphi(y, z)) \quad (1 \leq i \leq n)$

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

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

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

$\psi_i$  étant une série formelle dont chaque terme est de degré  $\geq 1$  par rapport aux  $x_j$  et de degré  $\geq 1$  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

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

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

$$\varphi_i(x_1, \dots, x_n, \theta_1(x_1, \dots, x_n), \dots, \theta_n(x_1, \dots, x_n)) = 0 \quad \text{pour } 1 \leq i \leq n. \quad (2)$$

Utilisant le symbolisme de la théorie des groupes, nous noterons  $\mathbf{x}\mathbf{y}$  le système des  $n$  séries formelles  $\varphi_i(x_1, \dots, x_n, y_1, \dots, y_n)$ ,  $\mathbf{x}^{-1}$  le système des  $n$  séries formelles  $\theta_i(x_1, \dots, x_n)$ ,  $\mathbf{e}$  le système  $(0, 0, \dots, 0)$  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  $\varphi'_j(x'_1, \dots, x'_m, y'_1, \dots, y'_m)$ . Un *homomorphisme* de  $G$  dans  $G'$  est par définition un système  $\mathbf{f}(\mathbf{x})$  de  $m$  séries formelles  $f_j(x_1, \dots, x_n) (1 \leq j \leq m)$  sans terme constant, satisfaisant à  $m$

<sup>2</sup>) 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  $f(\mathbf{x}\mathbf{y}) = f(\mathbf{x})f(\mathbf{y})$ , 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  $g(f(\mathbf{x})) = \mathbf{x}$  et  $f(g(\mathbf{x}')) = \mathbf{x}'$ . La considération des termes du premier ordre dans ces relations montre aussitôt que l'on a nécessairement alors  $m = n$ , et que les matrices jacobienne  $\left(\frac{\partial f_i}{\partial x_j}\right)$  et  $\left(\frac{\partial g_i}{\partial x'_j}\right)$  sont inverses l'une de l'autre. Inversement, soit  $g(\mathbf{x}')$  un système de  $n$  séries formelles  $g_i(x'_1, \dots, x'_n)$  sans terme constant, tel que la matrice jacobienne  $\left(\frac{\partial g_i}{\partial x'_j}\right)$  soit inversible; il existe alors un système  $f(\mathbf{x})$  de  $n$  séries formelles telles que l'on ait  $f(g(\mathbf{x}')) = \mathbf{x}'$  et  $g(f(\mathbf{x})) = \mathbf{x}$  [2, p. 64, prop. 10]; en posant  $\mathbf{x}'\mathbf{y}' = f(g(\mathbf{x}')g(\mathbf{y}'))$  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  $x_1, \dots, x_n$ . Nous supposerons désormais que  $K$  est un corps de caractéristique  $p > 0$ . Alors, pour tout entier  $r \geq 0$ , 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  $x_1^{p^r}, \dots, x_n^{p^r}$ . 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  $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ , où  $0 \leq \alpha_i < p^r$  pour  $1 \leq i \leq n$ . Nous dirons qu'un  $K$ -endomorphisme  $\Delta$  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  $\Delta$  vérifie l'identité

$$\Delta(fg) = f\Delta(g) + g\Delta(f) \quad (3)$$

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  $\Delta$  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  $\Delta$  s'annule dans  $\mathfrak{o}_{r+1}$ . Nous dirons qu'une semi-dérivation  $\Delta$  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  $\Delta$  est une semi-dérivation de hauteur  $r$ , il en est de même de  $\Delta^p$  ( $p$ -ième itérée de  $\Delta$ ) et de  $f\Delta$ , pour  $f \in \mathfrak{o}_r$ . Si  $\Delta, \Delta'$  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  $\Delta$  ou  $\Delta'$  est spéciale. Si  $\Delta$  est une semi-dérivation spéciale de hauteur  $r$ , il en est de même de  $g\Delta$ , pour  $g \in \mathfrak{o}$ ; si  $\Delta, \Delta'$  sont deux semi-dérivations spéciales de hauteur  $r$ , il en est de même de  $\Delta\Delta'$ .

L'ensemble  $\mathcal{D}_r$  des semi-dérivations de hauteur  $r$  est donc une *p*-algèbre de Lie sur l'anneau  $\mathfrak{o}_r$ ; l'ensemble  $\mathcal{S}_r$  des semi-dérivations spéciales de hauteur  $r$  est un idéal dans l'algèbre de Lie  $\mathcal{D}_r$ ; 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  $0 \leq \alpha_i < p^{r+1}$ . Désignons par  $D_{ri}$  la semi-dérivation de hauteur  $r$  telle que, si  $\alpha_i = ap^r + b$ , avec  $0 \leq b < p^r$ , on ait

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

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  $r \geq 0$  et  $1 \leq i \leq n$ ; en outre,  $D_{ri}$  et  $D_{sj}$  commutent quels que soient les indices.

**Lemme 2.** — Le  $\mathfrak{o}$ -module  $\mathcal{S}_r$  a une base formée des semi-dérivations  $\prod_{h=0}^{r-1} \prod_{i=1}^n D_{hi}^{\lambda_{hi}}$ , où  $0 \leq \lambda_{hi} < p$  et  $\sum_{h,i} \lambda_{hi} > 0$ ; 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  $D_{ri} (1 \leq i \leq n)$ .

En effet, si  $\Delta$  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  $D_{ri} (1 \leq i \leq n)$ , à coefficients dans  $\mathfrak{o}_r$ . Si on retranche de  $\Delta$  cette combinaison linéaire, on a donc une semi-dérivation spéciale  $\Delta'$ ; 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  $\alpha_i = \sum_{h=0}^{r-1} \lambda_{hi} p^h (1 \leq i \leq n)$ , 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  $\mathcal{S}_r$  donnée au n° 4, cela prouve que les semi-dérivations  $D$  forment une base de  $\mathcal{S}_r$  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  $\alpha = (\alpha_1, \dots, \alpha_n)$  de  $n$  entiers  $\geq 0$ , il nous sera commode de poser désormais  $x_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$  et  $D_\alpha = \prod_{h=0}^{\infty} \prod_{i=1}^n D_{h_i}^{\lambda_{hi}}$ , où les  $\lambda_{hi}$  sont les coefficients des développements  $p$ -adiques

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

nous écrirons aussi  $\alpha! = \prod_{h=0}^{\infty} \prod_{i=1}^n \lambda_{hi}!$ , et  $|\alpha| = \alpha_1 + \alpha_2 + \dots + \alpha_n$ .

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  $\alpha$ ) 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  $c_{\alpha}$  augmente indéfiniment avec  $|\alpha|$ .

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

$$L_y f = f(yx), \quad R_y f = f(xy) \quad (5)$$

(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  $f \in \mathfrak{o}(G)$

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

avec les conventions précédentes<sup>3)</sup>; remplaçant dans cette formule  $z_i$  par  $y_i + \psi_i(\mathbf{y}, \mathbf{x})$  (resp. par  $y_i + \psi_i(\mathbf{x}, \mathbf{y})$ ), on voit que chacun des deux

<sup>3)</sup> On convient dans cette somme de poser  $D_{(0,0,\dots,0)} = I$ , 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  $\sum_{\alpha} v_{\alpha}(\mathbf{x}, \mathbf{y}) D_{\alpha}$ , où  $v_{\alpha}$  est une série formelle par rapport à  $\mathbf{x}$  et  $\mathbf{y}$ , dont l'ordre *par rapport aux*  $y_i$  est au moins égal à  $|\alpha|$ ; de façon plus précise,  $v_{\alpha}(\mathbf{x}, \mathbf{y})$  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  $c_{\alpha}$  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

$$DL_y = L_y D. \quad (7)$$

Soit  $D$  un tel opérateur; désignons par  $D(\mathbf{e})f$  l'élément de  $A$  obtenu en substituant  $\mathbf{e}$  à  $\mathbf{x}$  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  $\mathbf{e}$  à  $\mathbf{x}$ ,

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

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

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

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

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

et comme  $L_y L_z = L_{zy}$ , on a  $(D(L_z f))(\mathbf{y}) = (Df)(z\mathbf{y}) = (L_z(Df))(\mathbf{y})$ , 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  $D(\mathbf{e}) = D_{\alpha}(\mathbf{e})$ ; alors l'équation  $(Df)(\mathbf{y}) = D_{\alpha}(\mathbf{e})(L_y f)$  signifie que le premier membre est

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

$$D = w_\alpha D_\alpha + \sum_{\beta} w_\beta D_\beta \quad (10)$$

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

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

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

où dans la seconde somme, les indices  $\beta$  sont distincts des  $n$  indices  $(0, \dots, p^h, \dots, 0)$ ; la relation  $|\beta| \leq p^h$  entraîne alors que les  $D_{\beta}$  sont des semi-dérivations spéciales de hauteur  $h$ . En outre,  $w_{hj}^{(i)}$  est le coefficient de  $y_j^{p^h}$  dans la série  $(y_j + \psi_j(\mathbf{x}, \mathbf{y}))^{p^h}$ ; 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  $\alpha = (\alpha_1, \dots, \alpha_n)$ , où  $\alpha_i = \sum_{h=0}^r \lambda_{hi} p^h$ , considérons en particulier les opérateurs invariants

$$X_\alpha = X_{01}^{\lambda_{01}} X_{02}^{\lambda_{02}} \dots X_{0n}^{\lambda_{0n}} X_{11}^{\lambda_{11}} \dots X_{1n}^{\lambda_{1n}} \dots X_{r1}^{\lambda_{r1}} \dots X_{rn}^{\lambda_{rn}} \quad (12)$$

(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  $X_\alpha$ , où  $0 \leq \alpha_i < p^{r-1}$  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  $X_{ri}$  ( $1 \leq i \leq n$ ).*

Remarquons tout d'abord que pour un  $h$  donné, les équations (11) par rapport aux  $D_{hi} (1 \leq i \leq n)$  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

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

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  $D_{\beta}$  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  $D_{\alpha}$  pour  $0 \leq \alpha_i < p^{r+1} (1 \leq i \leq n)$  peut s'exprimer comme combinaison linéaire des  $X_{\alpha}$  relatifs aux  $\alpha$  satisfaisant aux mêmes conditions, le nombre des  $X_{\alpha}$  étant le même que celui des  $D_{\alpha}$ .

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

$$\Delta D_1 D_2 \dots D_m X_{m+1} \dots X_q \quad (14)$$

où  $\Delta$  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  $\Delta D_1 D_2 \dots D_m$ , 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  $\Delta'$  est une semi-dérivation spéciale de hauteur  $r$  et les  $u_j \in \mathfrak{o}_r(G)$ . On est ramené à considérer les produits

$$\Delta D_1 D_2 \dots D_{q-1} (u_j X_{rj}) \quad (15)$$

$$\text{et } \Delta D_1 D_2 \dots D_{q-1} \Delta' \quad (16)$$

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

$$\Delta D_1 D_2 \dots D_{q-2}(u_j(D_{q-1} X_{rj})) \quad (17)$$

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

$$\Delta_1 D_1 D_2 \dots D_m X_{rj}$$

où  $\Delta_1$  est une semi-dérivation spéciale de hauteur  $r$ , et  $m \leq q - 1$ . 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

$$\Delta D_1 D_2 \dots D_{q-2} \Delta' D_{q-1} \quad (18)$$

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

$$\Delta_2 D_1 D_2 \dots D_m$$

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

Cela établit que  $D_\alpha$  peut s'écrire comme somme de produits de la forme  $\Delta X_1 X_2 \dots X_q$ , où  $\Delta \in \mathcal{S}_r$  et où chacun des  $X_i$  est un (quelconque) des  $X_{rj}$ , avec  $q \leq p^n$ . 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  $v_j \in \mathfrak{d}_r$  et  $\Delta'$  est une semi-dérivation spéciale de hauteur  $r$ . Substituant à  $X_1 X_2$  la valeur ainsi obtenue, on voit que dans le produit  $\Delta X_1 X_2 \dots X_q$ , 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  $D_\alpha$  à une somme de produits de la forme

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

Il peut se faire que certains des exposants  $\mu_i$  soient  $\geq p$ ; 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  $\mathfrak{d}_r$ , 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  $\mu_i$  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  $X_\alpha$ , ou  $0 \leq \alpha_i < p^{r-1}$ ; l'algèbre de Lie  $\mathfrak{g}_r$  est somme directe de  $\mathfrak{s}_r$  et de l'espace vectoriel sur  $K$  ayant pour base  $X_{r1}, \dots, X_{rn}$ .*

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  $u_{\alpha}$  sont nécessairement des constantes. Or, l'identité (7) s'écrit, pour toute  $f \in \mathfrak{d}(G)$

$$\sum_{\alpha} u_{\alpha}(\mathbf{x}) \cdot (X_{\alpha} L_{\mathbf{y}}) f = \sum_{\alpha} u_{\alpha}(\mathbf{y}\mathbf{x}) \cdot (L_{\mathbf{y}} X_{\alpha}) f.$$

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

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

en remplaçant alors  $\mathbf{y}$  par  $\mathbf{x}$ , cela équivaut à

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

et comme les  $X_{\alpha}$  sont linéairement indépendantes (th. 1), cela entraîne  $u_{\alpha} = u_{\alpha}(\mathbf{e})$ , autrement dit les séries formelles  $u_{\alpha}$  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

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

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

produit  $Z_1 Z_2 \dots Z_a$  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  $X_{\alpha}$  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  $T_r$ :

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

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

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

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

où les  $P_{\alpha}$  sont des séries formelles<sup>4)</sup>; cela résulte en effet du th. 2 et de la représentation de  $R_z$  comme série de la forme  $\sum_{\alpha} v_{\alpha}(x, z) D_{\alpha}$ : il suffit de remplacer, dans cette dernière série, chacun des  $D_{\alpha}$  par son expression en fonction des  $X_{\beta}$ .

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

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

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

<sup>4)</sup> On convient de poser  $P_0 = 1$  et  $X_0 = I$  (opérateur identique).

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

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

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  $D'_{r_i} = X_{r_i} + \sum_{\beta} b_\beta D'_\beta$  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  $s(\alpha) = 1$ ,  $\delta = (0, 0, \dots, 0)$ . Raisonnons alors par récurrence sur  $s(\alpha)$  (pour  $h(\alpha) = r$ ); si  $s(\alpha) = s$ , on a

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

où chaque  $D_i (1 \leq i \leq s)$  est une des semi-dérivations  $D_{r_j}$ . 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

$$u_1 u_2 \dots u_s D_\delta Z_1 Z_2 \dots Z_s \quad (23)$$

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

On en déduit l'expression des  $P_\alpha$ ; avec les mêmes notations, on a

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

où  $Q_\alpha$  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,  $P_\alpha$  est le coefficient de  $X_\alpha$  dans la somme

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

Il résulte de la formule (22) que  $X_\alpha$  ne peut figurer que dans des  $D'_\beta$  pour lesquels  $h(\beta) > h(\alpha)$ , ou  $h(\beta) = h(\alpha)$  et  $s(\beta) \geq s(\alpha)$ . Remarquons maintenant qu'on a  $\frac{1}{\alpha!} x_\alpha = \frac{1}{\delta!} x_\delta \cdot \frac{1}{\gamma!} x_\gamma$  et  $X_\alpha = X_\delta X_\gamma$ ,  $X_\gamma$  pouvant être appelée la partie de  $X_\alpha$  contenant les semi-dérivations non spéciales de hauteur  $h(\alpha)$ ; la formule (22) montre alors que si  $h(\beta) = h(\alpha)$  et  $s(\beta) = s(\alpha)$ ,  $D'_\beta$  ne pourra contenir un terme en  $X_\alpha$  que si  $\alpha$  et  $\beta$  ont même «quotient euclidien»  $\gamma'$  par  $p^r$ ; en outre la somme de tous ces termes est  $\frac{1}{\gamma!} x_\gamma P'_\delta$ , où  $P'_\delta$  est le coefficient de  $X_\delta$  dans la somme  $\sum_\beta \frac{1}{\beta!} x_\beta D'_\beta$ , étendue à tous les indices  $\beta$  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  $h(\lambda) \geq h(\alpha)$ , 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  $c_\alpha$  sont des séries formelles par rapport à des indéterminées autres que les  $x_i$ , entraîne  $c_\alpha = 0$  pour tout  $\alpha$ .*

Nous démontrerons en fait un résultat un peu plus précis: si, dans la série  $\sum_\alpha c_\alpha P_\alpha$ , les termes en  $x_\beta$  sont nuls pour  $h(\beta) < r$  et pour  $h(\beta) = r$  et  $s(\beta) \leq s$ , alors les  $c_\alpha$  sont nuls pour  $h(\alpha) < r$  et pour  $h(\alpha) = r$  et  $s(\alpha) \leq s$ . 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  $x_\beta$  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  $\alpha$  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  $P'_\delta$  est la somme des termes en  $x_\beta$  de  $P_\delta$ , pour lesquels  $h(\beta) < r$ . Mais dans cette somme, les termes correspondant à deux valeurs différentes de  $\gamma$  ne peuvent évidemment se réduire; on a donc  $\sum_\alpha c_\alpha P'_\delta = 0$ , la somme étant étendue à tous les  $\alpha$  pour lesquels  $\gamma'$  (quotient euclidien de  $\alpha$  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  $x_\beta$  pour lesquels  $h(\beta) < r$  sont nuls; l'hypothèse de récurrence entraîne donc  $c_\alpha = 0$  pour tous les  $\alpha$  considérés, ce qui achève la démonstration.

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

$$R_{\mathbf{z}} f = \sum_{\alpha} P_{\alpha}(\mathbf{z}) X_{\alpha} f; \quad (25)$$

on en tire, d'une part

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

de l'autre

$$R_{\mathbf{y}}(R_{\mathbf{z}} f) = \sum_{\alpha} P_{\alpha}(\mathbf{y}) X_{\alpha}(R_{\mathbf{z}} f) = \sum_{\alpha, \beta} P_{\alpha}(\mathbf{y}) P_{\beta}(\mathbf{z}) \cdot (X_{\alpha} X_{\beta}) f. \quad (27)$$

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

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

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

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

et en particulier

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

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

Portant dans (26), il vient

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

et comme  $R_{\mathbf{yz}} = R_{\mathbf{y}} R_{\mathbf{z}}$ , le th. 3 prouve que l'on a

$$X_{\alpha} X_{\beta} = \sum_{\gamma} c_{\alpha\beta\gamma} X_{\gamma}. \quad (31)$$

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

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

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

$$X_{\beta} P_{\alpha} = \sum_{\gamma} c_{\gamma\beta\alpha} P_{\gamma}. \quad (33)$$

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

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

<sup>5)</sup> 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  $f(\mathbf{xy}) = f(\mathbf{yx})$  pour toute série formelle  $f \in \mathfrak{v}$ ; en vertu du th. 3 et de la formule (29), cela équivaut à  $(X_\alpha X_\beta)(\mathbf{e}) = (X_\beta X_\alpha)(\mathbf{e})$  pour tout couple d'indices  $\alpha, \beta$ , 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

$$\begin{aligned} X_{01} &= (1 + x_1) D_{01}, X_{02} = (1 + x_1) D_{02} \\ X_{11} &= (1 + x_1^p) D_{11} + x_2 D_{02}, X_{12} = (1 + x_1^p) D_{12} \end{aligned}$$

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  $\bar{G}$  deux groupes de Lie formels, de dimensions respectives  $n$  et  $m$ , et soit  $\mathbf{u} = (u_1, \dots, u_m)$  une «application» de  $G$  dans  $\bar{G}$ , c'est-à-dire un système de  $m$  séries formelles sans terme constant par rapport aux  $x_i$  ( $1 \leq i \leq n$ ). Pour toute série formelle  $\bar{f} \in \mathfrak{v}(\bar{G})$ , soit  $\bar{f} \circ \mathbf{u}$  la série formelle de  $\mathfrak{v}(G)$  obtenue en substituant dans  $\bar{f}$ , à chaque indéterminée  $\bar{x}_j$  ( $1 \leq j \leq m$ ), la série formelle  $u_j(x_1, \dots, x_n)$ . Pour tout opérateur différentiel  $D$  dans  $\mathfrak{v}(G)$ , appartenant à  $\mathcal{S}$ , considérons la série formelle  $D(\bar{f} \circ \mathbf{u})$ , et désignons par  $(\mathbf{u}'(D)(\mathbf{e})) \bar{f}$  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  $\bar{\mathfrak{G}}$  de  $\bar{G}$ , que nous désignerons par  $\mathbf{u}'(D)$ , par la formule

$$(\mathbf{u}'(D) \bar{f})(\bar{\mathbf{y}}) = (\mathbf{u}'(D)(\mathbf{e})) (L_{\bar{\mathbf{y}}} \bar{f}) . \quad (35)$$

Il est clair en effet que  $D(\bar{f} \circ \mathbf{u})$  est combinaison linéaire, à coefficients dans  $\mathfrak{v}(G)$ , des  $\bar{X}_\alpha(\mathbf{e}) \bar{f}$ , 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  $\bar{G}$ ,  $u'$  est un homomorphisme de  $\mathfrak{G}$  dans  $\bar{\mathfrak{G}}$ , appliquant  $\mathfrak{g}_r$  dans  $\bar{\mathfrak{g}}_r$  et  $\mathfrak{s}_r$  dans  $\bar{\mathfrak{s}}_r$  ( $0 \leq r < +\infty$ ).*

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

$$L_y(\bar{f} \circ u) = (L_{u(y)} \bar{f}) \circ u. \quad (36)$$

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

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

Si on pose

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

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

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

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

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

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

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

d'où, en raison du th. 3

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

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

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  $(\bar{f}\bar{g}) \circ u = (\bar{f} \circ u)(\bar{g} \circ u)$ , et si  $\bar{f} \in \mathfrak{D}_r(\bar{G})$ ,  $\bar{f} \circ u \in \mathfrak{D}_r(G)$ . 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  $\bar{f}(\mathbf{u}(\mathbf{x}))$  pour toute  $\bar{f} \in \mathfrak{o}(\bar{G})$ , et en particulier les séries  $u_j (1 \leq j \leq m)$ , en prenant  $\bar{f} = \bar{x}_j$ .

13. On sait au contraire qu'on peut avoir  $\mathbf{u}'(\mathfrak{g}_0) = 0$  même si  $\mathbf{u}$  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  $\sigma$  est un isomorphisme du corps  $K$  sur un corps  $K^\sigma$  et si  $\varphi_i^\sigma$  désigne la série formelle sur  $K^\sigma$  obtenue en appliquant aux coefficients de  $\varphi_i$  l'isomorphisme  $\sigma$ , les  $\varphi_i^\sigma$  définissent un «groupe formel» que nous noterons  $G^\sigma$ . Il est clair que pour le groupe  $G^\sigma$ , 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  $\sigma$ ; les «constantes de structure» de  $G^\sigma$  ne sont autres par suite que les  $c_{\alpha\beta\gamma}^\sigma$ , et les séries formelles coefficients des  $X_\alpha$  pour le groupe  $G^\sigma$  sont les séries  $P_\alpha^\sigma$  obtenues en appliquant  $\sigma$  aux coefficients de  $P_\alpha$ .

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

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

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

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

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

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

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

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

Si on applique l'homomorphisme  $\mathbf{p}'$  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  $P^{(1)}$

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

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  $\mathfrak{g}_{r-1}^{(1)}/\mathfrak{s}_{r-1}^{(1)}$  (i. e. l'algèbre de Lie obtenue en appliquant aux constantes de structure de  $\mathfrak{g}_{r-1}/\mathfrak{s}_{r-1}$  l'isomorphisme  $\xi \rightarrow \xi^p$ ).

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

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

Nous écrirons ici  $D_k$  au lieu de  $D_{k1}$ ; pour  $\alpha = \sum_{h=0}^{r-1} \lambda_h p^h$ , on a  $X_\alpha = D_0^{\lambda_0} D_1^{\lambda_1} \dots D_{r-1}^{\lambda_{r-1}}$ , 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

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

et l'homomorphisme dérivé est défini par

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

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  $D \in \mathfrak{G}$ ,  $w'(D)(e)$  est défini par

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

d'où la relation de transitivité

$$(\mathbf{v} \circ \mathbf{u})' = \mathbf{v}' \circ \mathbf{u}' . \quad (46)$$

Cette relation nous donne une condition supplémentaire que doit vérifier le dérivé d'un homomorphisme  $\mathbf{u}$  de  $G$  dans  $\bar{G}$ . En effet, si  $\mathbf{u}^{(1)}$  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,  $\mathbf{p} \circ \mathbf{u} = \mathbf{u}^{(1)} \circ \mathbf{p}$ . Tenant compte de (46) et (42), cela donne pour les coefficients  $\alpha_{\alpha\bar{\alpha}}$  de la formule (38), les conditions

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

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  $\mathbf{u}$  de  $G$  dans  $\bar{G}$ , il existe déjà des relations nécessaires entre les opérateurs  $\mathbf{u}'(X_\alpha)$ . Par exemple,  $G$  étant le groupe additif considéré au n° 14, en supposant  $p = 3$ , on voit que, si

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

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  $\mathbf{u} = (u_1, \dots, u_n)$  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  $\bar{\mathbf{x}} \cdot \bar{\mathbf{y}} = \mathbf{u}(\mathbf{u}^{-1}(\bar{\mathbf{x}}) \mathbf{u}^{-1}(\bar{\mathbf{y}}))$ ,  $\mathbf{u}$  est un isomorphisme de  $G$  sur  $\bar{G}$ , et il résulte de (46) que  $\mathbf{u}'$  est un isomorphisme de  $\mathfrak{G}$  sur  $\bar{\mathfrak{G}}$ , dont  $(\mathbf{u}^{-1})'$  est l'isomorphisme réciproque. Cela étant, il est clair que les  $Y_\alpha = (\mathbf{u}^{-1})'(\bar{X}_\alpha)$  constituent une base de  $\bar{\mathfrak{G}}$  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  $P_{0i} (1 \leq i \leq n)$  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  $u'(X_{0i}) = \bar{X}_{0i}$  et  $\bar{P}_{0i} = \bar{x}_i$  pour  $1 \leq i \leq n$ ; on notera par contre que pour  $h \geq 1$ , on n'a pas nécessairement  $u'(X_{hi}) = \bar{X}_{hi}$ , en d'autres termes les nouvelles constantes de structure  $\bar{c}_{\alpha\beta\gamma}$  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  $\bar{x} \cdot \bar{y}$  est la *loi de composition canonique* correspondant à la base  $(\bar{X}_\alpha)$  de  $\bar{\mathfrak{G}}$ .

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  $m \leq n$  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  $\bar{x} = (\bar{x}_1, \dots, \bar{x}_m)$  et  $\bar{y} = (\bar{y}_1, \dots, \bar{y}_m)$ )

$$\varphi_i(\bar{x}_1, \dots, \bar{x}_m, 0, \dots, 0, \bar{y}_1, \dots, \bar{y}_m, 0, \dots, 0) \quad (1 \leq i \leq m)$$

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

$$\varphi_j(x_1, \dots, x_m, 0, \dots, 0, y_1, \dots, y_m, 0, \dots, 0) = 0 \quad (49)$$

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

cation  $u$  de  $H$  dans  $G$  telle que  $u_i(\bar{x}_1, \dots, \bar{x}_m) = \bar{x}_i$  pour  $1 \leq i \leq m$ , et  $u_j(\bar{x}_1, \dots, \bar{x}_m) = 0$  pour  $m+1 \leq j \leq n$ , est un homomorphisme. Il résulte aussitôt de la définition de l'homomorphisme dérivé  $u'$  que l'on a  $u'(\bar{X}_{hi}) = X_{hi}$  pour  $1 \leq i \leq m$  et pour tout  $h \geq 0$ . On en conclut que  $u'(\bar{X}_\alpha) = X_\alpha$  pour tout indice  $\alpha = (\alpha_1, \dots, \alpha_n)$  tel que  $\alpha_j = 0$  pour  $m+1 \leq j \leq n$  (nous dirons pour abrégé qu'un tel indice est de dimension  $m$ ); par suite, dans la formule (38), on a ici  $a_{\bar{\alpha}\alpha} = 1$  pour  $\alpha$  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  $\alpha$  et  $\beta$  sont de dimension  $m$  et si  $\gamma$  n'est pas de dimension  $m$ ; en d'autres termes, le sous-espace  $\mathfrak{S}$  de  $\mathfrak{G}$  ayant pour base les  $X_\alpha$  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)  $P_{0j}(\bar{\mathbf{x}}) = \sum_{\bar{\alpha}} a_{\bar{\alpha}\varepsilon_j} \bar{P}_\alpha(\bar{\mathbf{x}})$  (où on a posé  $\varepsilon_j = (0, \dots, 0, 1, 0, \dots, 0)$ , 1 étant à la  $j$ -ème place), on conclut de ce qui précède que pour  $j \geq m+1$ , on a  $P_{0j}(\bar{\mathbf{x}}) = 0$  et  $P_{0j}(\bar{\mathbf{x}}) = \bar{P}_{0j}(\bar{\mathbf{x}})$  pour  $j \leq m$ . En d'autres termes, si on fait le changement de coordonnées  $x'_i = P_{0i}(\bar{\mathbf{x}})$ , donnant sur  $G$  la loi de composition canonique (correspondant à la base  $(X_\alpha)$ )

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

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

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

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  $\bar{G}$  lorsque le corps de base  $K$  est parfait<sup>6</sup>). Soient  $m$  et  $n$  les dimensions de  $G$  et  $\bar{G}$ , et  $u$  un homomorphisme de  $G$  dans  $\bar{G}$ .

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

---

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

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

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

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

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

$$\left. \begin{aligned} u_i(\mathbf{x}) &= x_i && \text{pour } 1 \leq i \leq r_0 \\ u_i(\mathbf{x}) &= x_i^p + S_i(\mathbf{x}) && \text{pour } r_0 + 1 \leq i \leq r_0 + r_1 \\ \dots\dots\dots \\ u_i(\mathbf{x}) &= x_i^{p^t} + S_i(\mathbf{x}) && \text{pour } r_0 + \dots + r_{t-1} + 1 \leq i \leq r_0 + \dots + r_t \\ u_i(\mathbf{x}) &= 0 && \text{pour } i > r_0 + \dots + r_t \end{aligned} \right\} \quad (55)$$

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  $r_0 + \dots + r_{h-1} + 1 \leq i \leq r_0 + \dots + r_h$ , 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  $s_h = r_0 + \dots + r_h$ , et nous partirons de l'hypothèse de récurrence suivante :

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

$$\begin{aligned} u_i(\mathbf{x}) &= x_i^{p^k} + w_i(\mathbf{x}) && \text{pour } s_{k-1} < i \leq s_k, \quad 0 \leq k \leq h ; \\ u_i(\mathbf{x}) &= (v_i(\mathbf{x}))^{p^h} + w_i(\mathbf{x}) && \text{pour } i > s_h \end{aligned}$$

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

a) On a  $w_i = 0$  pour  $i \leq r_0 = s_0$ . Pour  $1 \leq k \leq h$  et  $s_{k-1} + 1 \leq i \leq s_k$ , on a  $w_i = w_{i_0} + w_{i_1}^p + w_{i_2}^{p^2} + \dots + w_{i_{k-1}}^{p^{k-1}}$

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

b) Pour  $i > s_h$ ,  $v_i$  ne contient aucun  $x_j$  tel que  $j \leq s_h$ , et

$$w_i = w_{i_0} + w_{i_1}^p + w_{i_2}^{p^2} + \dots + w_{i_h}^{p^h}$$

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

c) Pour  $k \leq h$  et  $s_{k-1} + 1 \leq i \leq s_k$ , 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  $\bar{G}$ , laissant invariants les  $x_j$  et  $\bar{x}_j$  d'indice  $j \leq s_h$ , et tels que  $u_i = 0$  pour  $i > s_h$ . En effet, l'hypothèse que  $\mathbf{u}$  est un homomorphisme signifie que, pour  $1 \leq i \leq n$ , on a

$$\begin{aligned} u_i(\mathbf{x}) + u_i(\mathbf{y}) + \bar{\psi}_i(\mathbf{u}(\mathbf{x}), \mathbf{u}(\mathbf{y})) = \\ u_i(x_1 + y_1 + \psi_1(\mathbf{x}, \mathbf{y}), \dots, x_m + y_m + \psi_m(\mathbf{x}, \mathbf{y})) . \end{aligned} \quad (56)$$

Appliquons cette formule à un  $i > s_h$ : considérons un des termes de  $w_i (= u_i)$  de plus bas degré  $d$ , soit  $c x_1^{\alpha_1} \dots x_m^{\alpha_m}$ , 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

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

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  $c' x_1^{\beta_1} \dots x_m^{\beta_m}$ , où on remplace, ou bien  $p^s$  facteurs  $x_j$  par  $y_j$ , ou bien au moins un des  $x_k$  par  $\psi_k(\mathbf{x}, \mathbf{y})$  et au plus  $p^s - q$  facteurs  $x_j$  par  $y_j$ , si  $q$  facteurs  $x_k$  sont remplacés par un  $\psi_k$ . 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  $(\beta_1, \dots, \beta_m) \neq (\alpha_1, \dots, \alpha_m)$ ; et dans le second cas, comme tout terme de  $\psi_k(\mathbf{x}, \mathbf{y})$  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  $\bar{\psi}_i(\mathbf{u}(\mathbf{x}), \mathbf{u}(\mathbf{y}))$ . Mais un tel terme provient nécessairement d'un produit d'un  $u_k(\mathbf{y})$  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  $u_k(\mathbf{y})$  ne peut contenir de monômes où le seul  $y_l$  qui figure soit  $y_j$ .

Prouvons ensuite que, pour  $s_{k-1} + 1 \leq j \leq s_k$ , l'exposant  $\alpha_j$  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  $cx_1^{\alpha_1} \dots x_m^{\alpha_m}$  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  $u_k(\mathbf{y})$  ne peut contenir de monômes  $\lambda y_j^s$  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  $\bar{f}_d$  tel que

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

Faisons dans  $\bar{G}$  le changement de variables tel que  $\bar{x}'_j = \bar{x}_j$  pour  $j \neq i$ ,  $\bar{x}'_i = \bar{x}_i - \bar{f}_d(\bar{x}_1, \dots, \bar{x}_{r_0}, \bar{x}_{r_0+1}, \dots, \bar{x}_{s_h})$ ; 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  $\bar{f}_v(\bar{x}_1, \dots, \bar{x}_{s_h})$  telle que  $\bar{f}_v$  soit de poids  $v \geq d$  et que, en posant  $\bar{g} = \sum_{v=d}^{\infty} \bar{f}_v$ , le changement de variables  $\bar{x}'_j = \bar{x}_j$  pour  $j \neq i$ ,  $\bar{x}'_i = \bar{x}_i - \bar{g}(\bar{x}_1, \dots, \bar{x}_{s_h})$  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  $\neq 0$ . Alors:

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

$$\bar{\psi}_i(\mathbf{u}(\mathbf{x}^{(h)}), \mathbf{u}(\mathbf{y}^{(h)})) = (\psi_i(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}))^{p^k} + w_i(\psi_1(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \dots, \psi_{s_h}(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), x_{s_h+1} + y_{s_h+1} + \psi_{s_h+1}(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \dots, x_m + y_m + \psi_m(\mathbf{x}^{(h)}, \mathbf{y}^{(h)})). \quad (58)$$

On déduit de cette formule, par récurrence sur  $k$ , que la série formelle  $\psi_i(\mathbf{x}^{(h)}, \mathbf{y}^{(h)})^{p^k}$  ne peut contenir de monômes dans lesquels les puissances des  $y_l$  se réduisent à  $y_j^\alpha$  avec  $\alpha \leq p^h$  et  $j > s_h$ . En effet, c'est évident pour  $k = 0$ , car en vertu de  $(A_h)$ , aucun  $u_k(\mathbf{y})$  ne peut contenir de monôme  $\lambda y_j^\alpha$  avec  $\alpha \leq p^h$  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  $0 \leq q \leq k - 1$ , tout monôme de  $w_{i_q}$  contient un  $x_l$  tel que  $s_{q-1} + 1 \leq l \leq s_q$ .

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  $c x_{s_{h+1}}^\lambda \dots x_m^\nu$  un de ces monômes de plus petit degré total  $d$ , et supposons que  $\mu = \alpha_j \not\equiv 0 \pmod{p}$ . Substituons  $\mathbf{x}^{(h)}$  et  $\mathbf{y}^{(h)}$  à  $\mathbf{x}$  et  $\mathbf{y}$  dans (56), ce qui donne

$$\begin{aligned} & u_i(\mathbf{x}^{(h)}) + u_i(\mathbf{y}^{(h)}) + \bar{\psi}_i(\mathbf{u}(\mathbf{x}^{(h)}), \mathbf{u}(\mathbf{y}^{(h)})) \\ &= (v_i(x_{s_{h+1}} + y_{s_{h+1}} + \psi_{s_{h+1}}(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \dots, x_m + y_m + \psi_m(\mathbf{x}^{(h)}, \mathbf{y}^{(h)})))^{p^h} \\ & \quad + w_i(\psi_1(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \dots, \psi_{s_h}(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \\ & x_{s_{h+1}} + y_{s_{h+1}} + \psi_{s_{h+1}}(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}), \dots, x_m + y_m + \psi_m(\mathbf{x}^{(h)}, \mathbf{y}^{(h)})) . \end{aligned} \quad (59)$$

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

$$(c \mu x_{s_{h+1}}^\lambda \dots x_j^{\mu-1} \dots x_m^\nu y_j)^{p^h} . \quad (60)$$

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  $\geq d$ ; 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  $w_{i_q}$  ( $0 \leq q \leq h$ ) contient un  $x_l$  tel que  $s_{q-1} + 1 \leq l \leq s_q$ , 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  $(\psi_l(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}))^{p^q}$  où  $s_{q-1} + 1 \leq l \leq s_q$ ; du résultat démontré au début de ce n<sup>o</sup>, 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  $\bar{\psi}_i(\mathbf{u}(\mathbf{x}^{(h)}), \mathbf{u}(\mathbf{y}^{(h)}))$ ; mais aucun terme tel que (60) ne peut figurer dans cette série formelle, puisqu'aucun des  $u_k(\mathbf{y})$  ne contient de monôme  $\lambda y_j^\alpha$  avec  $\alpha \leq p^h$  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  $i > s_n$  au moins tel que  $V_i$  contienne un terme du premier degré. Supposons en effet le contraire ; alors aucun  $u_k(\mathbf{y})$  ne peut contenir de monôme  $\lambda y_j^\alpha$  avec  $j > s_n$  et  $\alpha \leq p^{h+1}$  ; on en déduit, comme au début du n° 21, que la série formelle  $(\psi_i(\mathbf{x}^{(h)}, \mathbf{y}^{(h)}))^{p^k}$  (pour  $s_{k-1} + 1 \leq i \leq s_k$ ) ne peut contenir de monômes dans lesquels les puissances des  $y_l$  se réduisent à  $y_j^\alpha$  avec  $j > s_n$  et  $\alpha \leq p^{h+1}$ . 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  $c x_{s_{h+1}}^\lambda \dots x_m^\nu$  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

$$(c \mu x_{s_{h+1}}^\lambda \dots x_j^{\mu-1} \dots x_m^\nu y_j)^{p^{h+1}} \quad (61)$$

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

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

$$\bar{x}'_i = \bar{x}_i - f_i^{(h)}(\bar{x}_{s_{h+1}}, \dots, \bar{x}_{s_{h+1}})$$

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

Posons alors  $V_i = \bar{v}_i(x_{s_{h+1}}, \dots, x_m) + w_{i, h+1}$ , où tout monôme de  $w_{i, h+1}$  contient au moins deux  $x_j$  distincts, et au moins un  $x_j$  tel que  $s_n + 1 \leq j \leq s_{n+1}$  ; en outre tout monôme de  $\bar{v}_i$  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  $\geq 2p^{h+1}$  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  $c x_1^{\alpha_1} \dots x_m^{\alpha_m}$  soit tel que  $d \leq p^{h+1}$ . Montrons d'abord que les  $\alpha_j$  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  $\alpha_j$  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  $s \leq h+1$  (puisque le degré total de  $\bar{v}_i$  est  $\geq 2$  pour  $i > s_{h+1}$ ). Un raisonnement analogue montre que, pour  $s_{k-1} < j \leq s_k$ , avec  $k \leq h+1$ ,  $\alpha_j$  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  $\lambda y_j^\alpha$  avec  $j > s_h$  et  $\alpha \leq p^{h+q+1}$ ; 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

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

Le théorème 6' est donc complètement démontré.

24. Montrons enfin comment on peut déduire le th. 6 du th. 6'. Supposons que  $s_{h-1} + 1 \leq i \leq s_h$ , et considérons dans  $S_i$  un terme de plus bas degré  $d$  parmi ceux qui ne sont pas puissances  $p^h$ -èmes; si  $c x_1^{\alpha_1} \dots x_m^{\alpha_m}$  est un tel terme, alors, pour  $s_{k-1} + 1 \leq j \leq s_k$ ,  $\alpha_j$  est multiple de  $p^k$ . En effet, si  $\alpha_j = a p^s$ , 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  $k \geq h$ , 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  $s \geq h$  et si les  $\alpha_l$  d'indice  $\neq j$  étaient multiples de  $p^h$  ; mais alors  $c x_1^{\alpha_1} \dots x_m^{\alpha_m}$  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  $u_k(\mathbf{y})$  ne peut contenir de monôme  $\lambda y_j^\alpha$  avec  $\alpha < p^k$ , en raison des formules (55). Procédant comme au n° 20, on peut donc faire un changement de variables dans  $\bar{G}$  de sorte que  $S_i = T_i^{p^h}$  pour tout  $i$  tel que

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

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

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

$$\mathbf{u}(\mathbf{x}\mathbf{y}) = \mathbf{u}(\mathbf{x}) \mathbf{u}(\mathbf{y}) ,$$

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

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

par suite, les séries formelles

$$\varphi_{\varrho+j}(0, \dots, 0, x_{\varrho+1}, \dots, x_m, 0, \dots, 0, y_{\varrho+1}, \dots, y_m) \quad (1 \leq j \leq m - \varrho)$$

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

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

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

d'où on conclut aussitôt que les  $\varrho$  séries formelles

$$\bar{\varphi}_j(\bar{x}_1, \dots, \bar{x}_\varrho, 0, \dots, 0, \bar{y}_1, \dots, \bar{y}_\varrho, 0, \dots, 0) \quad (1 \leq j \leq \varrho)$$

définissent un sous-groupe formel  $L$  de  $\bar{G}$ , de dimension  $\varrho$ , l'*image* de  $\mathbf{u}$ . 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  $u'(X_{hi}(\bar{e}))\bar{f}$  est le coefficient de  $x_i^{p^h}$  dans la série formelle  $\bar{f}(u(x))$ . Le th. 6 prouve que l'on a

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

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  $u'(X^p) = (u'(X))^p$ . D'autre part, d'après (44), si  $[X_{0i}, X_{0j}] = \sum_k \lambda_{ijk} X_{0k}$ , on a  $[X_{hj}, X_{hj}] = \sum_k \lambda_{ijk}^p X_{hk} + Y$ , où  $Y \in \mathfrak{s}_h$ ; on déduit alors aussitôt de (62) que les  $X_{0i}$  d'indice

$$i > r_0 + \dots + r_h$$

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  $p'^h(Y)$  tels que  $Y \in \mathfrak{g}_h$ ,  $u'(Y) = 0$  et  $p'^h(Y) \in \mathfrak{a}_{h-1}$ . Cette dernière définition prouve que les nombres  $r_0, \dots, r_t$  qui interviennent dans le th. 6 sont *invariants* par changements de variables dans  $G$  ou dans  $\bar{G}$ .

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

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

dont le dernier est l'algèbre de Lie du noyau  $H$  de  $u$ .

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  $i \leq t$ , 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  $u_i(x) = x_i^{p^h}$  pour  $1 \leq i \leq m$  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  $\bar{G}$  définit un isomorphisme de  $G$  sur un groupe  $\bar{G}^{(-h)}$ .*

27. L'algèbre de Lie  $\mathfrak{b}$  du groupe  $L$ , qui est engendrée par les  $\overline{X}_{0i}$  tels que  $1 \leq i \leq \rho$ , n'est nullement isomorphe à l'algèbre de Lie quotient  $\mathfrak{g}_0/\mathfrak{a}_t$ , comme on pourrait le croire ; par exemple, si  $i \leq r_0$  et  $r_0 < j \leq r_0 + r_1$ , on a  $[\overline{X}_{0i}, \overline{X}_{0j}] = \mathbf{u}'([X_{0i}, X_{1j}])$ . Désignons par  $\mathfrak{b}_h$  le sous-espace de  $\mathfrak{b}$  engendré par les  $\overline{X}_{0i}$  tels que  $i \leq r_0 + r_1 + \dots + r_h$ ;  $\mathfrak{b}_h$  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  $r_0 + \dots + r_{h-1} < j \leq r_0 + \dots + r_h$ , et  $i \leq r_0 + \dots + r_h$ ; il résulte alors de (62) que  $[\overline{X}_{0i}, \overline{X}_{0j}]$  est l'image par  $\mathbf{u}'$  d'une semi-dérivation de  $\mathfrak{s}_h$  si  $i \leq r_0 + \dots + r_{h-1}$  et d'une semi-dérivation de  $\mathfrak{g}_h$  si  $i > r_0 + \dots + r_{h-1}$ . En outre, dans ce dernier cas, on a  $[\overline{X}_{0i}, \overline{X}_{0j}] = \mathbf{u}'([X_{hi}, X_{hj}]) = \sum \lambda_{ijk}^p \overline{X}_{0k} + \overline{Y}$ , 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

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

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  $\xi \rightarrow \xi^{p^h}$ ).

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  $K[X_1, \dots, X_m]$ ; nous supposons que  $V$  est de dimension  $n$ , et que le point  $(0, \dots, 0)$  est un point simple  $e$  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  $K[X_1, \dots, X_m, Y_1, \dots, Y_m]$ ; soient  $\mathfrak{A} = K[X_1, \dots, X_m]/\mathfrak{p}$  l'anneau des polynômes sur  $V$ ,

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

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  $f_1, \dots, f_m$  de  $\mathfrak{R}'$  tels que l'on ait

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

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  $K[X_1, \dots, X_m, Y_1, \dots, Y_m]$ , on peut l'écrire  $u_k(x_1, \dots, x_m, y_1, \dots, y_m)/v_k(x_1, \dots, x_m, y_1, \dots, y_m)$ , où  $x_i$  (resp.  $y_i$ ) est la classe de  $X_i$  (resp.  $Y_i$ ) mod.  $\mathfrak{q}$  ; on l'écrira aussi

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

ou  $f_k(\mathbf{x}, \mathbf{y})$ . 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  $f(\mathbf{x}, f(\mathbf{y}, \mathbf{z})) = f(f(\mathbf{x}, \mathbf{y}), \mathbf{z})$ , aux relations  $f(\mathbf{e}, \mathbf{x}) = f(\mathbf{x}, \mathbf{e}) = \mathbf{x}$ , et telle qu'il existe une application rationnelle  $h$  de  $V$  dans  $V$  telle que  $f(\mathbf{x}, h(\mathbf{x})) = f(h(\mathbf{x}), \mathbf{x}) = \mathbf{e}$ .

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

$$v_k(0, \dots, 0, 0, \dots, 0)$$

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

$$s_1, \dots, s_n, t_1, \dots, t_n,$$

linéairement indépendants mod.  $\mathfrak{m}^2$ , et il existe un isomorphisme du complété de  $\mathfrak{Q}'$  sur l'anneau des séries formelles sur  $K$  en  $2n$  indéterminées  $u_1, \dots, u_n, v_1, \dots, v_n$ , 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