

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

JEAN MICHEL

Bases des algèbres de Lie et série de Hausdorff

Séminaire Dubreil. Algèbre et théorie des nombres, tome 27, n° 1 (1973-1974), exp. n° 6,
p. 1-9

http://www.numdam.org/item?id=SD_1973-1974__27_1_A6_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1973-1974, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

BASES DES ALGÈBRES DE LIE ET SÉRIE DE HAUSDORFF

par Jean MICHEL

Introduction.

Un résultat de G. VIENNOT (cf. [6] et [7]) permet d'associer à certaines factorisations des monoïdes libres, les factorisations régulières gauches, des bases des algèbres de Lie libres, dont la base de Hall, habituellement utilisée, est un cas particulier.

Les factorisations régulières, qui possèdent de nombreuses propriétés supplémentaires par rapport aux factorisations régulières gauches en général, donnent des bases plus avantageuses pour étudier les algèbres de Lie libres, dont un exemple est la base de Lyndon-Širšov ; l'utilisation de cette base permet d'améliorer, et de simplifier, de nombreuses démonstrations dans les algèbres de Lie.

Nous étudions ensuite la convergence dans les cas réels et p -adique de la série de Hausdorff, en utilisant en premier lieu les propriétés de la base de Širšov.

1. La base de Širšov.

Nous rappelons d'abord quelques définitions et résultats de [5] et [6].

Une factorisation complète du monoïde libre X^* sur un ensemble X est une partie F de X^* , totalement ordonnée, telle que tout mot de X^* ait une décomposition unique en produit décroissant (strictement ou non) de mots de F .

Une telle factorisation est dite régulière gauche (resp. droite) si

$$(f, g, fg \in F) \Rightarrow (f \leq fg) \quad (\text{resp. } fg \leq g).$$

Une factorisation F est régulière si elle vérifie une des propriétés équivalentes :

- 1° F est régulière gauche et régulière droite,
- 2° $(f, g \in F \text{ et } f < g) \Rightarrow (fg \in F)$.

Nous allons considérer dans la suite des monômes en les générateurs dans l'algèbre de Lie libre L sur X . Nous noterons π l'application consistant à remplacer le crochet de Lie par la multiplication dans ces monômes (si on compose cette application avec l'application du magma libre M sur X dans L , obtenue en remplaçant les parenthèses par des crochets de Lie, on a la projection canonique de M sur X^*).

A toute factorisation régulière gauche F de X^* , on associe une base de L en définissant une application p , inverse de π , telle que $p(F)$ soit une base de L . Cette application est définie par récurrence sur la longueur des mots comme

suit :

Si $w \in F$, si $w = va$, où a est la dernière lettre de w , et si $v = v_1 \dots v_n$ est la décomposition unique de v en produit décroissant de mots de F , alors

$$p(w) = [p(v_1)[p(v_2)[\dots[p(v_n)a]\dots]] .$$

Enfin, la base de Širšov, H , est définie par la factorisation :

$S = \{\text{les mots de } X^* \text{ plus petits que leur permutés circulaires pour l'ordre lexicographique}\}$,

et

S est lui-même ordonné par l'ordre lexicographique.

Le principal intérêt de la base de Širšov provient des deux propositions suivantes :

PROPOSITION 1. - Soit $w = a_1 \dots a_n$ l'écriture comme suite d'éléments de X d'un mot de X^* ; posons $u_i = a_1 \dots a_i$, $v_i = a_{i+1} \dots a_n$. Alors le dernier mot de la décomposition unique en suite décroissante de mots de S de w est v_j , où

$$j = \sup\{i \text{ tels que } v_i u_i \leq u_i v_i\} .$$

Démonstration. - Il suffit de voir que l'on obtient une suite décroissante de mots de S en itérant la construction de v_j , l'unicité de la décomposition concluant alors. Cela se déduit facilement des propriétés de l'ordre lexicographique.

Remarquons que cette proposition rend constructive la définition de p .

PROPOSITION 2. - Le composé de l'injection canonique $L \hookrightarrow \text{Ass } X$ (algèbre associative libre sur X) par la projection sur le sous-module de $\text{Ass } X$, engendré par S , est un isomorphisme, et si on choisit comme bases au départ et à l'arrivée H et S , rangés dans leur ordre naturel, la matrice M exprimant cet isomorphisme est triangulaire, à coefficients entiers, et avec des 1 sur la diagonale (et cela reste évidemment vrai en remplaçant L et $\text{Ass } X$ par une de leur composantes multihomogènes de multi-degré fixé).

Démonstration. - Cela résulte immédiatement de la propriété suivante, qui se démontre par récurrence sur la longueur des mots :

Soient $u \in S$, et $p(u) = \sum_i a_i u_i$ la décomposition de $p(u)$ dans la base de $\text{Ass } X$ formée des monômes (qu'on peut identifier aux éléments de X^*) ; alors le plus petit des u_i , pour l'ordre lexicographique, est u , et son coefficient a_i vaut 1 .

Remarquons que cette proposition, en conjonction avec la proposition 1, fournit un algorithme efficace pour exprimer dans une base de L un élément de $\text{Ass } X$.

Cet algorithme a pu être utilisé (cf. [5]) pour calculer les coefficients de la série de Hausdorff dans une base de L jusqu'au degré 11, en utilisant les for-

mules de Goldberg [2] pour calculer les coefficients dans $\text{Ass } X$. Les méthodes connues précédemment ne permettaient pas de dépasser le degré 6 ou 7. Nous allons voir dans la suite d'autres applications de la proposition 2.

2. Valuation p-adique de la série de Hausdorff.

Dans la suite de ce paragraphe, p est un nombre premier fixé. On note $\underline{Z}_{(p)}$ les éléments de \underline{Q} dont le dénominateur est premier avec p . On notera $L_{(p)}$, $L_{\underline{Q}}$, $\text{Ass}(\underline{Z}_{(p)}, X)$ et $\text{Ass}(\underline{Q}, X)$ respectivement pour $L \otimes \underline{Z}_{(p)}$, $L \otimes \underline{Q}$, $\text{Ass } X \otimes \underline{Z}_{(p)}$ et $\text{Ass } X \otimes \underline{Q}$.

Soit $w \in L_{\underline{Q}}$ (resp. $u \in \text{Ass}(\underline{Q}, X)$) : on appellera valuation p-adique, notée $v_p(w)$ (resp. $v_p(u)$), l'entier

$$\inf\{i \text{ tels que } p^i w \in L_{(p)} \text{ (resp. } p^i u \in \text{Ass}(\underline{Z}_{(p)}, X))\}.$$

Notons le corollaire suivant, qui découle immédiatement de la proposition 2 :

PROPOSITION 3. - Si \bar{w} est la projection, dans le sous-module engendré par S de $\text{Ass } X$, d'un élément w de L , alors $v_p(\bar{w}) = v_p(w)$.

La convergence de la série de Hausdorff $H(x, y) = \log(e^x e^y)$, dans le cas d'une algèbre de Lie p-adique, est caractérisée par les valuations p-adiques des composantes bihomogènes $H_{m,n}$ de bidegré m en x et n en y .

M. LAZARD [3] a démontré que $-v_p(H_{m,n}) \leq (n+m-1)/(p-1)$, et que l'on n'a égalité que si n et m sont respectivement sommes de a et b puissances de p , avec $a+b=p$ (On se borne ici à l'étude du cas $m, n > 1$; si $m=1$ ou $n=1$, le problème se ramène à l'étude des nombres de Bernoulli B_i , car on a : $H_{n,1} = B_n/n!(\text{ad } x)^n y$).

Les points où l'on a égalité, dans la majoration de Lazard, sont assez rares, et on peut se demander s'il n'y a pas de grands "trous" entre. Les trois théorèmes qui suivent montrent que ce n'est pas le cas, en comparant $-v_p(H_{m,n})$, non à $(n+m-1)/(p-1)$, mais à $v_p(n!) + v_p(m!)$, fonction dont cette valuation est plus proche. Faisons d'abord la remarque suivante :

Soient n un nombre entier, et $\sum_{i=0}^r a_i p^i$ son écriture en base p . Posons $s(n) = \sum_{i=0}^r a_i$; alors

$$v_p(n!) = (n - s(n))/(p-1) \text{ et } n!/p^{v_p(n!)} \equiv a_0! \dots a_r! \text{ modulo } p.$$

Nous pouvons maintenant énoncer les théorèmes suivants.

THÉOREME 1. - $-v_p(H_{m,n}) \leq v_p(n!) + v_p(m!) + [\log_p(s(n) + s(m))]$, où $[]$ désigne la partie entière et \log_p le logarithme en base p .

THÉOREME 2. - $-v_p(H_{m,n}) \geq v_p(n!) + v_p(m!) + 1$ dans les cas suivants :

1° $p = 2$, et on est dans un des cas :

(a) $n \equiv m \pmod{2}$, et $n, m > 1$,

(b) $n = 1$ et $m \equiv 0 \pmod{2}$,

(c) $m = 1$ et $n \equiv 0 \pmod{2}$,

(d) $n = m = 1$;

2° $p \neq 2$ et $g(n) + g(m) > p$, où $g(n) = \underline{\text{l'entier positif congru à } n \pmod{p-1}}$ et appartenant à $[1, p-1]$.

THÉORÈME 3. - Supposons qu'il existe α, k entiers tels que :

1° $0 \leq k \leq \alpha - 2$,

2° $s(n) + s(m) = p^\alpha - k(p-1)$, et

2° $\sup(s(n), s(m)) \geq (p-1)p^{\alpha-1}$,

alors

$$-v_p(H_{m,n}) \geq v_p(n!) + v_p(m!) + \alpha - k.$$

D'après la remarque faite plus haut, ces théorèmes améliorent strictement les résultats de LAZARD. Notons que le théorème 3 dit que la majoration du théorème 1 est atteinte si $k = 0$ ou si $k = 1$, c'est-à-dire qu'on ne peut améliorer asymptotiquement le terme $[\log_p(s(n) + s(m))]$ qui s'y trouve, et que le théorème 2 dit que, pour une somme $m + n$ fixée, la moitié des composantes $H_{m,n}$ ont une valuation comprise entre

$$-v_p(n!) - v_p(m!) - 1 \text{ et } -v_p(n!) - v_p(m!) - [\log_p(s(n) + s(m))].$$

Le théorème 1 se démontre en appliquant la proposition 3, et en calculant la valuation p -adique des coefficients des mots de S , et le théorème 3 aussi, en étudiant plus précisément les coefficients de certains mots (cf. [5]). Le théorème 2 se démontre en partant de la remarque suivante :

PROPOSITION 4. - Soient $w \in L$, $\sum a_i w_i$ sa décomposition dans la base de Širšov, et $\sum b_i u_i$ sa projection sur le sous-module de $\text{Ass } X$ engendré par S : le coefficient a_i de $(-1)^m (\text{ad } X)^{n-1} (\text{ad } Y)^m X$ est égal au coefficient b_i de $X^n Y^m$ (ces deux monômes appartenant à H et S respectivement).

Cela découle immédiatement de la proposition 2, $X^n Y^m$ étant le plus petit mot de sa composante bihomogène.

On obtient le théorème 2 en étudiant le coefficient de $X^n Y^m$, partant de la formule donnée en fonction des nombres de Bernoulli pour ce coefficient par GOLDBERG [2].

3. Convergence de la série de Hausdorff dans le cas réel.

Le problème est le suivant : Etant donnée une algèbre de Lie banachique réelle,

munie d'une norme admissible N (c'est-à-dire telle que $N([x, x']) \leq N(x) N(x')$), déterminer le domaine des (N, N') tels que si $N(x) = N$ et $N(x') = N'$, alors $H(x, x')$ converge.

Les résultats connus pour une algèbre de Lie banachique générale sont les suivants :

1° Majorant H par la série analytique ayant pour coefficients la valeur absolue de ceux de H , on démontre que H converge dans le domaine : $N + N' \leq \log 2$ (cf. BOURBAKI [1]).

2° Dans [4], M. MÉRIGOT améliore ce résultat en étudiant l'existence des solutions de l'équation différentielle que vérifie la dérivée par rapport à une variable de $H(x, y)$. Il obtient la convergence dans le domaine :

$$N < \int_0^{2\pi} \frac{1}{N'} \frac{1}{(2 + (t/2)(1 - \cotg(t/2)))} dt .$$

Ce domaine n'étant pas symétrique par rapport à la première bissectrice, on peut lui rajouter son symétrique. Pour la divergence de la série, on peut faire les remarques suivantes :

(a) La fonction génératrice des coefficients de degré 1 en X (ou en Y) étant $t/(e^t - 1)$, la série diverge si $N \geq 2\pi$ ou $N' \geq 2\pi$, cette fonction ayant un rayon de convergence limité à 2π .

(b) La proposition 4 permet d'améliorer ce résultat : en étudiant la fonction génératrice que donne GOLDBERG [2] pour le coefficient de $X^n Y^m$, on conclut que la série diverge en général si $N + N' \geq 2\pi$.

(c) Enfin, on obtient le résultat le plus précis en considérant le cas de l'algèbre de Lie $SL_2(\mathbb{R}) = \{X \in M_2(\mathbb{R}) ; \text{Tr } X = 0\}$. $N(x) = \sqrt{2\text{Tr } x^2}$ est une norme admissible d'algèbre de Lie banachique sur SL_2 . En effet, paramétrons les éléments de SL_2 par 3 paramètres en posant :

$$(n, \theta, \varphi) = n/2 \begin{pmatrix} \cos \varphi \cos \theta & \cos \theta \sin \varphi + \sin \theta \\ \cos \theta \sin \varphi - \sin \theta & -\cos \varphi \cos \theta \end{pmatrix}$$

Alors si $X = (n, \theta, \varphi)$ et $X' = (n', \theta', \varphi')$, on a

$$N(X) = n, \quad N(X') = n'$$

et

$$N(X)^2 N(X')^2 - N([X, X'])^2 = n^2 n'^2 (\cos \theta \cos \theta' \cos(\varphi - \varphi') - \sin \theta \sin \theta')^2 \geq 0 .$$

D'autre part, on a

$$X^2 = -I \det X = + I\mu \quad \text{et} \quad e^X = I c(\mu) + X f(\mu),$$

si l'on pose

$$\mu = (n^2/4) \cos 2\theta$$

$$c(x) = \begin{cases} \cos \sqrt{|x|} & \text{si } x < 0 \\ \text{ch } \sqrt{x} & \text{si } x \geq 0 \end{cases}$$

et

$$f(x) = \begin{cases} \sin \sqrt{|x|} / \sqrt{|x|} & \text{si } x < 0 \\ \text{sh } \sqrt{x} / \sqrt{x} & \text{si } x \geq 0 \end{cases}$$

Donc on a

$$(\exists Y, X = e^Y) \iff (\text{Tr } X \geq -2) .$$

En particulier, la série de Hausdorff $H(X, X')$ ne peut converger si

$$(\text{Tr } e^X e^{X'} < -2) \iff (F(n, n', \theta, \theta', \varphi, \varphi') < 0) ,$$

où l'on pose

$$F(n, n', \theta, \theta', \varphi, \varphi') = 1 + c(\mu) c(\mu') + nn' \nu / 2f(\mu) f(\mu') ,$$

où $\nu = \cos \theta \cos \theta' \cos(\varphi - \varphi') - \sin \theta \sin \theta'$.

Nous nous intéressons à l'enveloppe des courbes $F(n, n', \theta, \theta', \varphi, \varphi')$ quand $\theta, \theta', \varphi, \varphi'$ varient. Dans l'équation de F , seul ν dépend de φ, φ' , et il dépend linéairement de $\cos(\varphi - \varphi')$, donc les extremas sont atteints pour $\cos(\varphi - \varphi')$ extremal, i. e. $\cos(\varphi - \varphi') = \eta = \pm 1$. Alors $\nu = \eta \cos(\theta + \eta\theta')$. Posant $\varepsilon = \text{signe de } \cos 2\theta \cos 2\theta'$ et reportant dans l'équation de F , on voit qu'on est ramené à trouver l'enveloppe des courbes

$$(t(\mu) t(\mu'))^2 + 2\eta A t(\mu) t(\mu') + \varepsilon = 0 ,$$

où $A = \cos(\theta + \eta\theta') / \sqrt{|\cos 2\theta \cos 2\theta'|}$ et

$$t(x) = \begin{cases} -\text{tg } \sqrt{|x|} / 2 & \text{si } x < 0 \\ \text{th } \sqrt{x} / 2 & \text{si } x \geq 0 \end{cases}$$

Résolvant l'équation du second degré ainsi obtenue, on obtient les deux racines :

$$t(\mu) t(\mu') = (\cos \theta' + \gamma \sin \theta') (\gamma \sin \theta - \eta \cos \theta) / \sqrt{|\cos 2\theta'|} \sqrt{|\cos 2\theta|} , \quad \gamma = \pm 1$$

t étant une fonction monotone, l'extremum est obtenu pour $|tt'|$ le plus petit possible, i. e. pour $\gamma = -\eta = 1$.

On est ramené à l'enveloppe des courbes :

$$P(n, \theta) P(n', \theta') = 1 , \quad \text{où } P(n, \theta) = t(n^2/4 \cos 2\theta) \sqrt{|\cos 2\theta|} / \varepsilon (\cos \theta + \sin \theta) .$$

L'enveloppe est obtenue pour $dP/d\theta = dP/d\theta' = 0$, ce qui donne

$$f(\mu) = \sin 2\theta \quad \text{et} \quad f(\mu') = \sin 2\theta' .$$

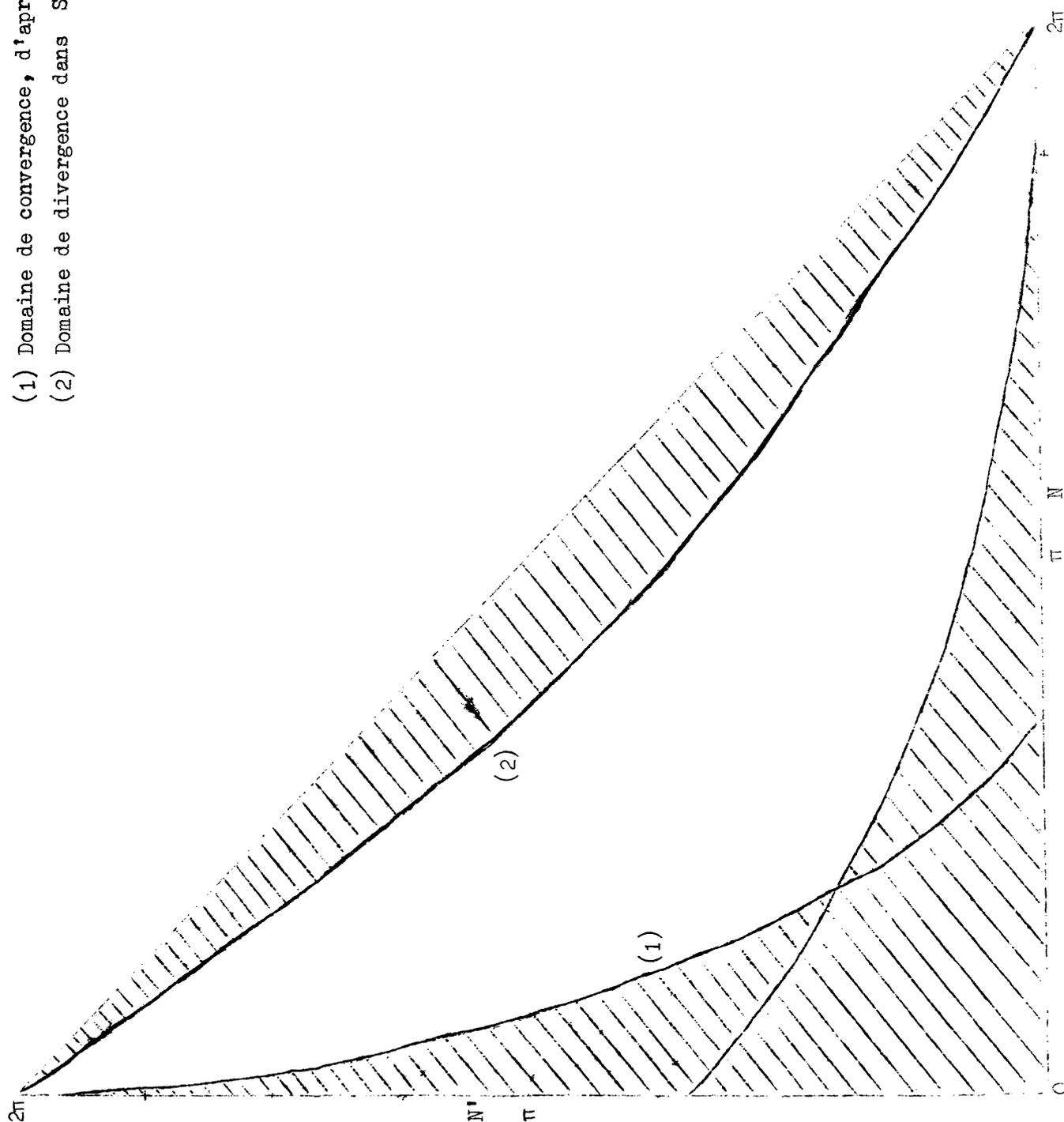
Posant $g =$ fonction réciproque de f , on a donc l'équation paramétrée du domaine cherché :

$$\begin{aligned} N &= g(\cos 2\theta) / \sqrt{\sin 2\theta} & N' &= g(\cos 2\theta') / \sqrt{\sin 2\theta'} \\ \text{tg}(g(\cos 2\theta)/2) & \text{tg}(g(\cos 2\theta')/2) & &= \sqrt{\text{tg } \theta \text{ tg } \theta'} . \end{aligned}$$

La figure montre le domaine obtenu, ainsi que le résultat de [4].

Figure 1.

- (1) Domaine de convergence, d'après [4].
 (2) Domaine de divergence dans $SL_2(\mathbb{R})$.



BIBLIOGRAPHIE

- [1] BOURBAKI (N.). - Groupes et algèbres de Lie, Chap. II et III. - Paris, Hermann, 1972 (Act. scient. et ind., 1349 ; Bourbaki, 37).
- [2] GOLDBERG (K.). - The formal power series for $\log(e^X e^Y)$, Duke math. J., t. 23, 1956, p. 13-21.
- [3] LAZARD (M.). - Quelques calculs concernant la formule de Hausdorff, Bull. Soc. math. France, t. 91, 1963, p. 435-451.
- [4] MÉRIGOT (M.). - Domaine de convergence de la série de Campbell-Hausdorff, Conférence faite à l'Université de Nice (multigraphie interne).
- [5] MICHEL (J.). - Bases des algèbres de Lie libres ; application à l'étude de la formule de Campbell-Hausdorff, Thèse 3e cycle, Math., Université Paris-Sud [Orsay] 1974.
- [6] VIENNOT (G.). - Factorisations des monoïdes libres et algèbres de Lie libres, Thèse Sc. math. Université Paris-7, 1974.
- [7] VIENNOT (G.). - Une théorie algébrique des bases et familles basiques des algèbres de Lie libres, Séminaire Dubreil : Algèbre, 27e année, 1973/74, n° 5.

(Texte reçu le 14 juin 1974)

Jean MICHEL
214 avenue du Maine
75014 PARIS
