

# *Astérisque*

JEAN MICHEL

**Calculs dans les algèbres de Lie libres : la série de Hausdorff et le problème de Burnside**

*Astérisque*, tome 38-39 (1976), p. 139-148

[http://www.numdam.org/item?id=AST\\_1976\\_\\_38-39\\_\\_139\\_0](http://www.numdam.org/item?id=AST_1976__38-39__139_0)

© Société mathématique de France, 1976, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) 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/>

CALCULS DANS LES ALGÈBRES DE LIE LIBRES :  
LA SÉRIE DE HAUSDORFF ET LE PROBLÈME DE BURNSIDE

par  
Jean MICHEL

1.- INTRODUCTION

La théorie des factorisations du monoïde libre (cf. [7]) fournit des bases mieux adaptées aux calculs dans les algèbres de Lie que la base classique de Hall, particulièrement dans le cas de la base de Lyndon-Širšov. Cet exposé montre deux problèmes où les calculs qui interviennent sont rendus possibles par l'utilisation de cette base. Les notations qui ne sont pas définies dans cet exposé, sont définies dans [7].

2.- CONVERGENCE DE LA FORMULE DE CAMPBELL-HAUSDORFF

Si  $x, y \in \mathbb{Q}\langle X \rangle$ , alors  $e^x e^y = e^{H(x,y)}$  où  $H(x,y) \in L_{\mathbb{Q}}$  (on notera  $L_{\mathbb{Q}}$ ,  $L_{\mathbb{Z}(p)}$  pour  $L \otimes \mathbb{Q}$  et  $L \otimes \mathbb{Z}(p)$ ).

Cette formule est au centre de la correspondance entre algèbres de Lie et groupes de Lie : sur une algèbre de Lie  $L$  où la série  $H$  converge, la loi  $(x,y) \mapsto H(x,y)$  est une loi de groupe.

On s'intéressera à la convergence de la formule dans une algèbre de Lie Banachique pour la norme  $p$ -adique.

Cette convergence est entièrement caractérisée par les entiers

$v_p(H_{n,m}(x,y))$  définis comme suit pour un élément  $u \in L_{\mathbb{Q}}$  :

$$-v_p(u) = \inf \{r/p^r \mid u \in L_{\mathbb{Z}(p)}\}$$

( $H_{n,m}(x,y)$  = composante de degrés  $n,m$  en  $x,y$  de  $H(x,y)$ ). ( $\mathbb{Z}(p)$  est le localisé de  $\mathbb{Q}$  par l'idéal  $(p)$ , c'est-à-dire les fractions dont le dénominateur est premier à  $p$ ).

M. Lazard [4] a démontré que  $-v_p(H_{n,m}) \leq (n+m-1)/(p-1)$  ce qui assure la convergence de  $H_{n,m}(u,v)$  si  $v_p(u)$  et  $v_p(v)$  sont  $\leq 1$ . De plus, il a démontré que l'on a égalité dans cette majoration si  $n$  et  $m$  sont respectivement somme de  $a$  et  $b$  puissances de  $p$ ,  $a+b=p$ . Ceci démontre que cette majoration est la meilleure pour  $\sup(|u|, |v|)$  donnée; mais on peut se demander s'il n'existe pas des droites  $v_p(u) = \lambda v_p(v)$  où la convergence est meilleure. Pour cela, le premier pas est de faire des conjectures sur  $v_p(H_{n,m})$ . Il faut donc déterminer systématiquement le plus grand nombre de coefficients possibles. 50 coefficients étaient connus (jusqu'en degré 6). Pour en calculer plus il faut :

a) calculer les coefficients de  $H(x,y)$  dans  $\mathbb{Q} \langle x,y \rangle$ . Le plus commode est d'utiliser la fonction génératrice donnée par Goldberg [3] :

si  $c_x(s_1, \dots, s_m) =$  coefficient de  $x^{s_1} y^{s_2} x^{s_3} \dots$  dans  $H(x,y)$

si  $c_y(s_1, \dots, s_m) =$  " "  $y^{s_1} x^{s_2} y^{s_3} \dots$ , alors :

$$c_x(s_1, \dots, s_m) = (-1)^{n-1} c_y(s_1, \dots, s_m) =$$

$$\int_0^1 t^{\lfloor m/2 \rfloor} (t-1)^{\lfloor (m-1)/2 \rfloor} G_{s_1}(t) \dots G_{s_m}(t) dt,$$

où  $\lfloor \ ]$  désigne la partie entière, et où les  $G_i$  sont les polynômes définis par :

$$G_1(t) = 1$$

et

$$i G_i(t) = d/dt((t^2 - t) G_{i-1}(t)).$$

b) pour calculer les coefficients dans l'algèbre de Lie, il suffit de retenir les coefficients des mots standards de Lyndon dans l'algèbre associative et d'appliquer la matrice triangulaire qui exprime l'isomorphisme entre l'algèbre de Lie et le sous-module engendré par les mots de Lyndon dans l'algèbre associative. De plus, cette matrice ayant 1 pour déterminant, il suffit, si on ne s'intéresse qu'à  $v_p(H_{m,n})$ , de calculer le p.p.c.m. des dénominateurs des coefficients dans l'algèbre associative.

Après le calcul de 2500 coefficients (jusqu'en degré 14), il apparaissait que  $-v_p(H_{m,n})$  est très proche de  $v_p(n!) + v_p(m!)$  (pour comparer cette valeur à la majoration de Lazard, il faut noter que si  $s(n)$  = somme des chiffres du nombre  $n$  écrit en base  $p$ , alors  $v_p(n!) = (n - s(n))/(p - 1)$ ).

Cette conjecture qui implique que la convergence est la même sur toutes les droites  $v_p(u) = \lambda v_p(v)$  a pu être précisée par les trois résultats suivants :

$$(1) \quad -v_p(H_{m,n}) \leq v_p(n!) + v_p(m!) + [\log_p(s(n) + s(m))]$$

([ ] désigne la partie entière et  $\log_p$  le logarithme de base  $p$ )

$$(2) \quad -v_p(H_{m,n}) \geq v_p(n!) + v_p(m!) + 1$$

dans les cas suivants :

(a)  $p = 2$  et  $n \equiv m \pmod{2}$  et  $n, m > 1$ , ou  $n$  ou  $m = 1$  et l'autre pair

(b)  $p \neq 2$  et  $g(n) + g(m) > p$ , où  $g(n) =$  l'entier positif  $\equiv n \pmod{p-1}$   
et compris entre 1 et  $p-1$ .

(3) Si il existe  $\alpha, k$  entiers tels que :

$$(a) \quad 0 \leq k \leq \alpha - 2$$

$$(b) \quad s(n) + s(m) = p^\alpha - k(p-1)$$

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



alors :

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

Notons que (3) dit que la majoration de (1) est atteinte si  $k=0$  ou  $1$ , c'est-à-dire qu'on ne peut l'améliorer asymptotiquement. La base de Lyndon-Siršov a encore servi pour la démonstration de ces résultats, qui ont été démontrés en étudiant directement les coefficients des mots standards dans l'algèbre associative (cf. [5]).

### 3.- LE PROBLÈME DE BURNSIDE RESTREINT

Parmi les groupes à un nombre fini de générateurs  $r$ , d'exposant fini  $e(x^e = 1 \forall x)$  y a-t-il un groupe fini maximal (appelé groupe de Burnside restreint et noté  $B(e,r)$ ) ?

(Le problème de Burnside général demande si un groupe qui a un nombre fini de générateurs et est d'exposant fini est toujours fini ; la réponse est non en général si  $r \geq 2$  et  $e \geq 665$  impair (Novikov, Adjan [9] ; ils espèrent étendre leur méthode à  $e \geq 101$ , peut être  $e \geq 33$ ) ; la réponse est oui si  $e = 2, 3, 4$  ou  $6$  et inconnue dans les autres cas).

Le problème restreint a été résolu pour  $e$  premier par Kostrikin [11] en 1959 en utilisant des méthodes basées sur les algèbres de Lie.

(Un théorème de réduction de Highman permet alors de résoudre le problème quand il n'y a qu'un nombre fini de groupes simples d'exposant  $e$ ).

Mais la démonstration d'existence de Kostrikin est non constructive, et de nombreux problèmes restent ouverts dont l'ordre du groupe.

Nous nous intéresserons uniquement au cas d'un exposant  $p$  premier. On a :  $B(p,r) = F/F^p$  où  $F$  est le groupe libre à  $r$  générateurs, et  $F^p$  le sous-groupe distingué engendré par les puissances  $p^{\text{ièmes}}$ .

Ce quotient correspond à un quotient d'algèbres de Lie : Soit  $L$  l'algèbre de Lie libre (algèbre de Lie du groupe libre en prenant comme suite

la suite centrale descendante). Soit  $I$  l'idéal correspondant à  $F^p$ . Alors  $B(p,r)$  existe  $\iff L/I$  est finie, et cette algèbre de Lie a alors le même cardinal que  $B(p,r)$ . Le problème est donc ramené à l'étude de  $I$ . Il est connu depuis Zassenhaus que :

a)  $I \supset pL$

b)  $I \supset \Lambda$ , où  $\Lambda$  est l'idéal de  $L$  engendré par les éléments de la forme  $[u|v^{p-1}]$  (où on note pour  $u \in L$ ,  $v \in \mathbb{Z}\langle X \rangle$ ,  $[u|v] = \delta_v(u)$ , où  $\delta_v$  est l'image de  $v$  par l'homomorphisme  $\mathbb{Z}\langle X \rangle \rightarrow \text{End}(L)$  défini par  $x_i \mapsto \text{ad } x_i$ ).

En fait,  $I$  ressemble beaucoup à  $\Lambda + pL$ . Kostrikin [10] a démontré que  $I \subset pL + \Lambda [1/p] \cap L$ , et Sanov [12] a démontré que la composante de degré  $i$  de  $I$  est égale à celle de degré  $i$  de  $\Lambda + pL$  en degré  $i \leq 2p-2$ . Il a conjecturé que c'était toujours vrai. Cette conjecture a été renforcée rapidement par un résultat de Kostrikin [10] qui a démontré que c'était vrai pour  $r=2$  et  $i=2p-1, 2p$ .

Or, G.E Wall [8] a donné une condition qui, si elle est vraie, implique que la composante de degré  $2p-1$  de  $I/\Lambda + pL$  est non nulle, et implique aussi que la conjecture de Hugues est fautive (cette conjecture dit que si  $G$  est un groupe d'ordre  $p^a$ , si  $H$  est le sous-groupe de  $G$  engendré par les éléments d'ordre supérieur à  $p$ , alors si  $H$  est non vide, il est d'indice 1 ou  $p$  dans  $G$  (c'est vrai pour  $p=2,3$ )).

Tout d'abord Wall a démontré que la composante de degré  $2p-1$  de  $I/\Lambda + pL$  est un module irréductible sous l'action de  $SL_r(\mathbb{Z})$  comme groupe de substitutions linéaires sur les variables. Pour tester la nullité de cette composante, il suffit de tester celle de l'élément  $\bar{\varphi}$  invariant par le groupe triangulaire. Il suffit aussi de considérer le cas de 3 variables. L'élément  $\bar{\varphi}$  se trouve alors être de degrés  $p-1$ ,  $p-1$  et 1 en les trois variables. Prenant un représentant  $\varphi$  de  $\bar{\varphi}$  dans  $I + pL/pL$  on est ramené à vérifier si  $\varphi$  appartient à  $\Lambda + pL/pL$ . Choissant une base convenable de  $L$ , on

peut écrire  $\varphi$  sous la forme  $[z|\theta(x,y)]$ . On peut "simplifier" par  $z$  et le problème est ramené à tester si  $\theta(x,y)$  appartient à l'idéal engendré dans  $\mathbb{Z}\langle x,y \rangle$  par les puissances  $p-1$ èmes des éléments de Lie.

Pour pouvoir donner l'expression de  $\theta$ , introduisons les notations suivantes :

$$\langle n_1 u_1, \dots, n_m u_m \rangle = \text{composante de degrés } n_1, \dots, n_m \text{ de } (u_1 + \dots + u_m)^{n_1 + \dots + n_m}.$$

On a alors :

$$\theta = \text{composante de degrés } (p-1, p-1) \text{ de } \langle R, (p-2)(X+Y) \rangle$$

où  $R$  est défini comme suit :

Un théorème de Zassenhaus dit que  $(X+Y)^p - X^p - Y^p$  est un élément de Lie modulo  $p$ . Ce théorème admet une forme explicite :

$$p! R = (X+Y)^p - X^p - Y^p - \sum_{m=1}^{p-1} (1/m) [X | \langle (m-1)X, (p-m)Y \rangle].$$

Après quelques calculs, on peut mettre  $\theta$  sous la forme :

$$\theta = \sum_{i=1}^{p-1} 1/(p-1)! \langle \langle iX, (p-i)Y \rangle - (1/i) [X | \langle (i-1)X, (p-i)Y \rangle] \rangle / p, (i-1)Y, (p-1-i)X \rangle$$

D'autre part, (cf. [2]), on peut démontrer que l'idéal  $J$  engendré par les puissances  $p-1$ èmes des éléments de Lie dans  $\mathbb{Z}\langle X \rangle$  admet comme système de générateurs linéaires, les éléments de la forme  $a \langle u_1, \dots, u_{p-1} \rangle$ , où  $a$  décrit une base de  $\mathbb{Z}\langle X \rangle$  et les  $u_i$  une base de  $L$ .

On détermine une base du quotient  $\mathbb{Z}\langle X \rangle / J$  et la table de multiplication dans cette base, comme suit :

- a) jusqu'en degré total  $p-2$ ,  $J=0$  : on prend comme base tous les monômes.
- b) par récurrence, disposant des bases  $\{e_h\}$  (resp.  $\{f_k\}$ ) de degré  $(i-1, j)$  (resp.  $(i, j-1)$ ) on détermine la base de degré  $(i, j)$  en retenant parmi les éléments de la forme  $x e_h$  (resp.  $y f_k$ ) ceux qui sont linéairement indépendants (on a donc une base formée d'images de monômes). Les relations entre



eux sont données par les  $\langle u_1, \dots, u_{p-1} \rangle$  calculés sous la forme

$x \sum_h \lambda_h e_h + y \sum_k \mu_k f_k$  à l'aide de la table de multiplication (connue en degrés  $\langle (i,j) \rangle$ ). Il suffit enfin de calculer la valeur de  $\theta$  modulo  $J$  dans

cette base à l'aide de cette table de multiplication.

4.- RÉSULTATS NUMÉRIQUES POUR  $p = 5$

a) Composante de degrés  $(4,4)$  de  $\mathbb{Z}\langle X \rangle / J$ .

Cette table représente la valeur des  $\lambda_k^i$  dans l'écriture  $x \cdot e_i = \sum \lambda_k^i g_k$  (resp. la valeur des  $\mu_k^j$  dans l'écriture  $y \cdot f_j = \sum \mu_k^j g_k$ ) où  $\{e_i\}$  (resp.  $\{f_j\}$ ) est une base de la composante de degré  $(4,3)$  (resp.  $(3,4)$ ) de  $\mathbb{Z}\langle X \rangle / J$ , et  $\{g_k\}$  une base de la composante de degré  $(4,4)$ .

		X X X Y Y Y Y Y Y Y Y Y Y
		Y Y Y X X X X X Y Y Y Y Y Y
		Y Y Y Y Y Y Y X X X X Y Y
$\{g_k\}$		X X X X X X Y Y X Y Y X X
		X Y Y Y Y X X Y X X Y X Y
		Y X X X X Y X Y X X Y X Y X
		X X Y X Y X Y X Y Y X X X X
		Y Y X Y X X X X X X X X X X
		X.XYXYXY 4 3 4 4 4 2 1 1 2 2 3 1 0 1
		X.YXYXYX 0 2 1 1 4 2 0 2 2 2 4 4 4 2
		X.YXYXYX 0 0 3 0 4 3 2 0 0 3 1 3 1 0
		X.YXYXYX 4 3 3 3 3 3 0 0 3 0 3 4 4 0
		X.YXYXYX 0 0 2 0 3 0 2 2 1 4 4 3 4 3
$\{x \cdot e_i\}$		X.YYXYXY 1 0 0 0 0 0 0 0 0 0 0 0 0 0
		X.YYXYXY 0 1 0 0 0 0 0 0 0 0 0 0 0 0
		X.YYXYXY 0 0 1 0 0 0 0 0 0 0 0 0 0 0
		X.YYXYXY 0 0 0 0 0 2 0 2 0 0 3 0 1 1
		X.YYXYXY 0 0 0 0 0 0 4 0 0 4 0 0 1 1
		X.YYXYXY 0 0 0 0 0 0 0 4 0 0 4 0 4 0
		Y.XYXYXY 0 0 0 1 0 0 0 0 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 1 0 0 0 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 1 0 0 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 1 0 0 0 0 0 0 0
$\{y \cdot f_j\}$		Y.XYXYXY 0 0 0 0 0 0 0 1 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 1 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 1 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 1 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 1 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 0 1 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 0 0 1
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		Y.XYXYXY 0 0 0 0 0 0 0 0 0 0 0 0 0 0

b) Valeur de  $\theta$  dans la base  $\{g_k\}$ .

$$2YXYXYXYX+3YXYXYXYX+2YXYXYXYX+2YXYXYXYX+4YXYXYXYX+YXYXYXYX$$

On constate que cette valeur n'est pas nulle.

Ces calculs ont été faits en langage APL, en utilisant au maximum les possibilités de traitement vectoriel de ce langage [13].

\*  
\* \*

BIBLIOGRAPHIE

- [1] CANNON J.J : "Some combinatorial and symbol manipulation programs in group theory" Computational problems in abstract algebra, p. 199-203. Oxford 1967 (Pergamon, Oxford 1970).
- [2] DIGNE F. et J. MICHEL : Communication personnelle à J.J Cannon.
- [3] GOLDBERG K. : "The formal power series for  $\text{Log}(e^x e^y)$ " Duke Math. Journal 23 (1956) p. 13-21.
- [4] LAZARD M. "Quelques calculs concernant la formule de Hausdorff" Bull. SMF, 11, 1963, p. 435-51.
- [5] MICHEL J : Thèse de 3<sup>ème</sup> cycle "Bases des algèbres de Lie - étude des coefficients de la formule de Campbell-Hausdorff". Publication mathématique de l'Université d'Orsay, N°55.
- [6] MICHEL J : "Bases des algèbres de Lie et série de Hausdorff", séminaire Dubreil (algèbre) 27<sup>ème</sup> année, 1973/74, N°6, 9 p.
- [7] VIENNOT G : exposé au séminaire Dubreil, N°5.
- [8] WALL G.E : "On the Lie ring of a group of prime exponent", Proc. second international conf. Theory of groups, Canberra, 1973, p. 667-690.
- [9] ADJAN : "Periodic groups of odd exponent". Proc. Second internat. conf. Theory of groups, Canberra, 1973, p. 8-12.
- [10] KOSTRIKIN A.I : "On the connection between periodic groups and Lie rings", Izv. Akad. Nauk SSSR Ser. Mat. 21 (1957), p. 289-310. Amer. Math. Soc. Transl. 45 (1965) p. 165-185.

- [11] KOSTRIKIN A.I : "The Burnside problem", *Izv. Acad. Nauk. SSSR, Ser. mat.* 23 (1959), p. 3-34, MR 23.
- [12] SANOV I.N : "Establishment of a connection between periodic groups of period a prime number and Lie rings". *Izv. Akad. Nauk. SSSR. Ser. Mat.* 16 (1952) p. 23-58, MR 13, 721.
- [13] DIGNE F et MICHEL J : "Le Workspace Lie", rapport de recherche.

Jean MICHEL  
Mathématiques - Bâtiment 425  
Université de Paris Sud  
91405 ORSAY