

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

KARL H. HOFMANN

Théorie directe des groupes de Lie, I

Séminaire Dubreil. Algèbre et théorie des nombres, tome 27, n° 1 (1973-1974), exp. n° 1,
p. 1-24

http://www.numdam.org/item?id=SD_1973-1974__27_1_A1_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/>

THÉORIE DIRECTE DES GROUPES DE LIE, I.

par Karl H. HOFMANN

Sommaire

	Pages
Introduction générale.	1-01
I. La théorie algébrique de la fonction exponentielle.	1-03
1. Algèbres de Banach.	1-03
2. Théorie de l'exponentielle formelle.	1-05
3. Formule de Campbell, Baker, Hausdorff et Dynkin.	1-08
4. Bigèbres.	1-11
5. Bigèbres primitivement engendrées. Compléments.	1-17
6. Automorphismes et dérivations.	1-19
7. Références.	1-23

Introduction générale

Dans cette suite d'exposés, il s'agit des groupes de Lie classiques (plus précisément, des groupes de Lie sur le corps réel sans restriction de dimension). On propose ici une méthode de définition et un traitement de la théorie de base des groupes de Lie du point de vue de l'algèbre topologique pure. On envisage la catégorie des groupes de Lie comme une catégorie pleine d'objets spéciaux dans la catégorie des groupes topologiques en s'intéressant essentiellement à la structure d'un groupe de Lie comme groupe topologique, c'est-à-dire qu'on s'intéresse aux sous-groupes, groupes quotients, morphismes, noyaux, représentation, et aux questions concernant les constructions naturelles comme, par exemple, le groupe de commutateurs, le centre, la résolubilité, la nilpotence, la semisimplicité, etc. On met ici l'accent sur l'appareil qui rend ces questions particulièrement accessibles : c'est l'appareil des algèbres de Lie et de Dynkin qui interviennent par l'intermédiaire d'une fonction exponentielle.

Notons que la théorie des groupes de Lie touche beaucoup de disciplines en dehors de la théorie des groupes topologiques : l'analyse dans la théorie des équations différentielles (qui fut, historiquement, le point de départ de la théorie), la géométrie et la topologie différentielle dans la théorie des variétés, des espaces homogènes et symétriques et dans la géométrie riemannienne. Par conséquent, traditionnellement, on utilise les outils fournis par ces théories librement dans les définitions mêmes et pour les fondations ; cependant, on observe, que, après avoir atteint un certain niveau, elles ne sont plus nécessaires pour traiter les questions de théorie des groupes indiquées ci-dessus. Pour l'enseignement des groupes de Lie dans le cadre des cours sur les groupes topologiques et leurs représentations, j'ai cherché, depuis quelques années, une méthode d'introduction des groupes de Lie

qui satisfasse aux critères suivants :

1° La théorie se développe à partir des définitions le plus rapidement et le plus directement possible,

2° Les concepts utilisés dans les définitions doivent être directs et ne dépendre que de théories sous-jacentes intervenant dans la théorie de la structure elle-même,

3° Les critères de définition doivent être vérifiés sans peine dans le cas des exemples naturels (comme par exemple, celui des groupes linéaires),

4° Il faudrait que les définitions entraînent une théorie aussi générale que possible (par exemple sans restriction de dimensions, mais avec la possibilité d'adapter aux autres corps de base, et de généraliser la théorie aux classes de groupes topologiques ultérieures et même aux demi-groupes topologiques).

J'admet aussi une motivation, qui, en étant peut-être moins systématique que les autres, est néanmoins une considération significative pour la formation des mathématiciens.

5° La présentation de la théorie doit conduire assez vite les étudiants qui ont parcouru un programme général modérément avancé, mais qui, d'autre part, ne sont pas encore spécialisés aux questions de recherche possibles à ce niveau.

Mes premières tentatives dans cette direction ont été indiquées d'une façon informelle dans [2]. J'espère présenter les détails dans un texte ultérieur. Le principe des idées a été brièvement indiqué plus récemment dans [3]. Cet article est aussi une source de références sur le sujet ; mais il ne contient pas encore la référence à N. BOURBAKI [1], qui vient de paraître. Pour beaucoup de détails, on peut se rapporter à cette oeuvre, qui s'occupe de notre sujet, et qui sera sa source encyclopédique pour longtemps. (Au demeurant, il me paraît significatif pour la difficulté du sujet, du point de vue de la présentation, que ce livre soit paru si tard, après l'achèvement de presque tous les autres projets, et même plusieurs années après d'autres volumes antérieurs et ultérieurs de la série "Groupe et algèbres de Lie".) Néanmoins je ne crois pas que cet exposé soit rendu superflu par le livre de BOURBAKI ; celui-ci n'est pas un texte pour les étudiants ; donc même après sa parution, la question persiste :

"Comment enseigner les groupes de Lie ?"

Pour décrire provisoirement notre définition, rappelons que pour le groupe linéaire $Gl(n) = GL(\mathbb{R}^n)$ des automorphismes de \mathbb{R}^n nous trouvons facilement une fonction exponentielle $\exp : L(\mathbb{R}^n) \rightarrow Gl(n)$, définie sur l'algèbre (complètement normable) de tous les endomorphismes de \mathbb{R}^n qui est localement inversible par le logarithme et qui nous sert à "linéariser" la structure locale de $Gl(n)$. Les propriétés significatives sont les suivantes :

(i) La fonction exponentielle classe tous les sous-groupes à un paramètre de $Gl(n)$ et vérifie $\exp(X + Y) = \exp X \exp Y$ si X et Y commutent.

(ii) La structure d'espace vectoriel de $L(\widetilde{\mathbb{R}^n})$ est retrouvée en termes du groupe $Gl(n)$ et de la fonction exponentielle au moyen de la formule

$$(A) \quad \exp(sX + tY) = \lim(\exp \frac{s}{n} X \exp \frac{t}{n} Y)^n .$$

Bien qu'il soit impossible de retrouver la structure de l'algèbre associative de $L(\widetilde{\mathbb{R}^n})$, nous notons que

(iii) La structure de l'algèbre de Lie donnée sur $L(\widetilde{\mathbb{R}^n})$ par le crochet $[X, Y] = XY - YX$ est déterminée par $Gl(n)$ au moyen d'une formule analogue à

(A) :

$$(B) \quad \exp[X, Y] = \lim \text{comm}(\exp \frac{1}{n} X, \exp \frac{1}{n} Y)^{n^2}, \quad \text{comm}(g, h) = ghg^{-1}h^{-1} .$$

Ainsi nous avons reconnu que le groupe topologique $G = Gl(n)$ admet une fonction exponentielle qui est définie sur une algèbre de Lie L (sur $L(\widetilde{\mathbb{R}^n})$) normable, qui induit un homéomorphisme local, et qui relie la structure locale de G et la structure de l'algèbre de Lie L . Alors, notre exposé doit rendre plus précis ce que nous entendons sous la définition suivante.

Définition vague. - Un groupe de Lie est un groupe topologique muni d'une fonction exponentielle.

Notre discussion procédera par étapes

I : La théorie algébrique de la fonction exponentielle.

II : Algèbres de Dynkin, Théorie de Lie locale.

III : Théorie globale des groupes de Lie.

IV : Conclusion. Revue et comparaisons.

Notations. - Comme d'habitude, $\widetilde{\mathbb{Z}}$, $\widetilde{\mathbb{R}}$, $\widetilde{\mathbb{C}}$ désignent les ensembles de nombres entiers, réels, complexes, respectivement, et $\widetilde{\mathbb{R}}^+ = \{r \in \widetilde{\mathbb{R}} ; r \geq 0\}$. Nous écrivons $\widetilde{\mathbb{N}} = \widetilde{\mathbb{Z}} \cap \widetilde{\mathbb{R}}^+$.

I. La théorie algébrique de la fonction exponentielle

Nous ne considérons que des corps de caractéristique 0 (ce qui est naturel si l'on se souvient de la série exponentielle) ; notons K un corps valué ; la norme $|| \cdot ||$ sur K peut être discrète ($|r| = 1$ pour $r \in K \setminus \{0\}$).

1. Algèbres de Banach.

I.1. DÉFINITION. - Une algèbre de Banach A (sur K) est une algèbre associative topologique complète sur le corps topologique K , muni d'une norme $|| \cdot || : A \rightarrow \widetilde{\mathbb{R}}^+$ telle que, quels que soient $x, y \in A$, $r \in K$, on ait

$$(i) \quad ||x|| = 0 \iff x = 0 ,$$

- (ii) $\|x + y\| \leq \|x\| + \|y\|$,
 (iii) $\|xy\| \leq \|x\| \|y\|$,
 (iv) $\|rx\| = |r| \|x\|$.

Nous dirons que A est ultramétrique, si, au lieu de (ii), on a la relation plus forte

$$(ii') \quad \|x + y\| \leq \max\{\|x\|, \|y\|\} .$$

Appelons A fortement ultramétrique si A est ultramétrique et si le corps de base K est discret. Si $K = \mathbb{R}$ ou \mathbb{C} a la norme archimédienne, nous appelons A un espace de Banach classique.

Si A est ultramétrique (resp. fortement ultramétrique), la topologie de A est définie par une base de filtre dénombrable des idéaux de la boule-unité au sens de R -algèbre, ou $R = \{r \in K ; |r| \leq 1\}$ (resp. au sens de K -algèbre). Le cas ultramétrique avec $K = \mathbb{Q}_p$, c'est le cas p -adique, est important pour des généralisations de la théorie, mais il est délibérément omis dans ces exposés. On remarque que le cas d'une algèbre discrète est compris dans $|\cdot|$: C'est le cas ultramétrique où K et A sont discrètement normés tous les deux.

Le cas classique jouera son rôle dans le chapitre II ; le cas fortement ultramétrique est le cadre approprié pour l'algèbre formelle de séries de puissances formelles, notamment pour la théorie algébrique des fonctions exponentielle et logarithme. Nous nous occuperons, dans le présent chapitre, presque exclusivement du cas fortement ultramétrique.

Envisageons d'abord quelques conventions. Une algèbre de Banach fortement ultramétrique est dite bornée si A est égale à sa boule-unité. Les seules algèbres dont nous allons nous occuper seront unifères **et bornées**. Soit \mathcal{B} la catégorie des algèbres unifères fortement ultramétriques bornées et les morphismes d'algèbres unifères qui conservent ou abaissent la norme. Pour $A \in \mathcal{B}$, notons

$$A_1 = \{x \in A ; \|x\| < 1\} .$$

Alors A_1 est un idéal propre (parce qu'il ne contient pas 1 , compte tenu de I.1.(iii)). Alors $1 + A_1 = \{y \in A ; \|y - 1\| < 1\}$; dans chaque algèbre de Banach, cet ensemble est formé des éléments inversibles ; étant multiplicativement stable, $1 + A_1$ est un groupe. Si A est une algèbre unifère topologique séparée complète sur K dont la topologie est définie par une suite $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots$ d'idéaux, nous définissons une norme en posant

$$\|x\| = 2^{-v(x)} , \quad v(x) = \max\{m \in \mathbb{N} ; x \in A_m\} ,$$

et nous disons que A est un objet de la catégorie \mathcal{B} par rapport à cette norme.

L'exemple suivant est typique et joue un rôle important dans la théorie.

I.2. EXEMPLE. - Soit X un ensemble. Le monoïde libre $M(X)$ engendré par X a

une filtration $\{M^n(X) ; n = 0, 1, \dots\}$ décroissante telle que $M^n(X)$ contient tous les mots à n lettres au moins. Cette filtration induit une filtration sur l'algèbre du monoïde $F(X) = K[M(X)]$. (Remarquons que l'algèbre fixée $F(X)$ est la même chose que l'algèbre tensorielle de l'espace vectoriel des combinaisons linéaires formelles des éléments de X , munie de la filtration évidente.) Notons $\overline{F}(X)$ l'algèbre de Banach fortement ultramétrique complétée de $F(X)$.

Cas importants spéciaux :

(a) $X = \{\xi\}$. Alors $\overline{F}(X) = K[[\xi]]$ est l'algèbre des séries de puissances formelles à une variable.

(b) $X = \{\xi, \eta\}$. Ici $\overline{F}(X) = K[[\xi, \eta]]$ est l'algèbre des séries formelles à deux variables non permutables.

Observons une propriété importante de $\overline{F}(X)$, que l'algebriste appellera "la propriété universelle", et l'analyste "le calcul fonctionnel dans les algèbres de Banach fortement ultramétriques".

I.3. PROPOSITION. - Soient X un ensemble, et $A \in \mathcal{B}$. Quelle que soit la fonction $f : X \rightarrow A_1$, il existe un morphisme $f' : \overline{F}X \rightarrow A$ (de \mathcal{B}), et un seul qui prolonge f .

Autrement dit, \overline{F} est un foncteur adjoint à gauche au foncteur

$$A \mapsto |A_1| : \mathcal{B} \rightarrow \text{Ens},$$

où $| \cdot |$ signifie l'ensemble sous-jacent.

I.4. COROLLAIRE. - Soit $x \in A_1$, alors il y a un morphisme unique $K[[\xi]] \rightarrow A$ qui envoie ξ sur x .

Nous écrivons $p(x)$ l'image d'une série de puissances p par ce morphisme. Notons que, dans chaque algèbre de Banach fortement ultramétrique, le rayon de convergence d'une série $p = \sum_0^\infty a_n \xi^n \in K[[\xi]]$ est 1 ; autrement dit, $\sum_0^\infty a_n x^n$ converge absolument pour $x \in A_1$, et nous avons $p(x) = \sum_0^\infty a_n x^n$. Remarquons que la proposition I.3 s'applique au cas $A = K[[\xi]]$ en donnant, pour tout

$$q = b_1 \xi + b_2 \xi^2 + \dots \in K[[\xi]]_1,$$

le résultat $p(q)$ de la substitution de q dans p . Cette notation nous donne aussi $p = p(\xi)$. L'unicité dans I.3 entraîne la formule

$$(1) \quad p(q)(x) = p(q(x)), \quad x \in A, \quad p, q \in K[[\xi]], \quad \| \cdot \| < 1.$$

2. Théorie de l'exponentielle formelle.

Définissons maintenant les fonctions exponentielles et logarithmiques, et établissons leurs propriétés élémentaires.

I.5. DÉFINITION. - Les éléments \exp , $L \in K[[\xi]]$ sont définis par

$$(2) \quad \exp = 1 + \xi + \frac{1}{2!} \xi^2 + \frac{1}{3!} \xi^3 + \dots$$

$$(3) \quad L = \xi - \frac{1}{2} \xi^2 + \frac{1}{3} \xi^3 - + \dots .$$

On écrit aussi $L = L(\xi) = \log(1 + \xi)$.

Si $A \in \mathcal{B}$, alors on définit (par abus de notation), des fonctions

$$(4) \quad \exp : A_1 \rightarrow 1 + A_1 \quad \text{par } x \mapsto \exp(x),,$$

$$(5) \quad \log : 1 + A_1 \rightarrow A_1 \quad \text{par } x \mapsto L(x - 1) .$$

Notons que $\exp(x)$ et $L(x - 1)$ sont des éléments bien définis de A tenant compte du I.4 et des remarques qui suivent ce numéro. On écrit aussi $\log(x)$ au lieu de $L(x - 1)$ (mais il faut bien se souvenir que $\log(x)$ n'est pas le résultat de la substitution de x dans \log). Si on prend $A = K[[\xi]]$, on retrouve $\exp = \exp(\xi)$ et $\log(1 + \xi) = L(\xi)$.

La proposition suivante se démontre comme le cas classique élémentaire par des raisonnements de séries de puissances.

I.6. PROPOSITION (Équation fonctionnelle simple de \exp). - Si $A \in \mathcal{B}$ et si $u, v \in A_1$ commutent, on a : $\exp(u + v) = \exp(u) \exp(v)$.

Les lemmes suivants ne servent qu'à démontrer que \exp et \log sont des fonctions inverses.

I.7. LEMME. - Il existe une dérivation unique $D : K[[\xi]] \rightarrow K[[\xi]]$ tel que $D\xi = 1$. Elle a les propriétés suivantes :

$$(a) \quad \ker D = K .$$

$$(b) \quad \text{Si } p \in K[[\xi]] \text{ et } q \in K[[\xi]]_1, \text{ alors } D(p(q)) = (Dp)(q) \cdot Dq .$$

$$(c) \quad D(\exp) = \exp .$$

$$(d) \quad (1 + \xi)DL = 1 .$$

I.8. LEMME.

$$(a) \quad \log(\exp) (= L(\exp - 1)) = \xi .$$

$$(b) \quad \exp(\log(1 + \xi)) (= \exp(L)) = 1 + \xi .$$

Démonstration.

(a) On applique D aux deux membres de l'équation en notant que

$$\log(\exp) - \xi \in \ker D .$$

On détermine la constante en substituant 0 .

(b) Posons $p = \exp(L)$, calculons $(1 + \xi)Dp$. Notons $p(0) = 1$, résolvons l'équation différentielle pour $p = 1 + a_1 \xi + a_2 \xi^2 + \dots$, en trouvant $a_1 = 1$,

$a_2 = \dots = 0$ par récurrence.

Le calcul fonctionnel et la formule (1) donnent immédiatement le résultat suivant :

I.9. PROPOSITION. - Pour $A \in \mathcal{B}$, les fonctions \exp et \log de I.4 sont des fonctions inverses.

Cela nous donne deux conséquences immédiates :

I.10. COROLLAIRE (Équation fonctionnelle simple de \log). - Si $A \in \mathcal{B}$ et si $u, v \in 1 + A_1$ commutent, on a : $\log(uv) = \log u + \log v$.

I.11. COROLLAIRE. - Par transport de structure, A_1 est muni d'une structure de groupe isomorphe au groupe multiplicatif $1 + A_1$. L'opération sur A_1 est donnée par $x * y = L(\exp(x) \exp(y) - 1)$, et satisfait $x * y = x + y$ dès que x et y sont permutables. En particulier, $-x$ est l'inverse de x . On a l'équation fonctionnelle $\exp(x * y) = \exp(x) \exp(y)$ quels que soient $x, y \in A_1$.

Il est possible de trouver un développement en série de puissance pour $\xi * \eta$ dans $K[[\xi, \eta]]$, (I.2 (b)). En fait

$$\exp(\xi) \exp(\eta) - 1 = \sum (1/p!q!) \xi^p \eta^q,$$

sommé sur $p + q \geq 1$. Soit σ cette somme. Alors

$$\sigma^n = \sum (p_1!q_1! \dots p_n!q_n!)^{-1} \xi^{p_1} \eta^{q_1} \dots \xi^{p_n} \eta^{q_n},$$

sommé sur $p_1 + q_1 \geq 1, \dots, p_n + q_n \geq 1$. Finalement, on a

$$\xi * \eta = L(\sigma) = \sum - (-1)^m / m \sigma^m, \quad m = 1, 2, \dots,$$

ce qui donne la formule cherchée.

I.12. LEMME (Formule de Campbell-Hausdorff-Dynkin provisoire).

$$\xi * \eta = \sum c(p_1, q_1, \dots, p_n, q_n) \xi^{p_1} \eta^{q_1} \dots \xi^{p_n} \eta^{q_n},$$

sommé sur $n = 1, 2, \dots, p_1 + q_1 \geq 1, \dots, p_n + q_n \geq 1$, où

$$c(p_1, q_1, \dots, p_n, q_n) = - \frac{(-1)^n}{n \cdot p_1! q_1! \dots p_n! q_n!}.$$

On préfèrerait transformer cette formule en une autre, plus systématique, du type

$$(6) \quad \xi * \eta = \sum_{\mu \in M(\xi, \eta)} q(\mu) \mu,$$

où $M(\xi, \eta)$ est le monoïde libre engendré par ξ et η , et où les $q(\mu)$ sont des nombres rationnel bien déterminés. Ce serait un problème d'analyse combinatoire de trouver (si possible) une formule explicite pour $q(\mu)$, problème qui, à ma connaissance, n'est pas résolu. Une formule explicite serait d'une importance mineure pour la théorie, mais assez intéressante du point de vue de l'analyse combinatoire et numérique. Il est facile de trouver

$$q(\xi) = q(\eta) = 1, \quad q(\xi\eta) = -q(\eta\xi) = 1/2.$$

A chaque algèbre associative A , on associe trivialement une algèbre de Lie ΛA en considérant, sur A , la multiplication crochet $[a, b] = ab - ba$. (Rappelons qu'une algèbre de Lie est une algèbre à multiplication $(a, b) \mapsto [a, b]$ bilinéaire satisfaisant à

$$(i) \quad [a, b] = -[b, a],$$

(ii) (JACOBI) $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$ quels que soient a, b, c . Dès que la caractéristique du corps de base diffère de 2, on peut remplacer (i) par (i') $[a, a] = 0$.) Alors, si $A = K[[\xi, \eta]]$, les éléments ξ, η engendrent une algèbre de Lie \bar{L} fermée dans ΛA . Le reste du chapitre s'occupe de la démonstration du fait que $\xi * \eta \in \bar{L}$. C'est la partie plus sophistiquée de la théorie algébrique de la fonction exponentielle.

Mais avant que nous finissions cette partie de la théorie algébrique de la fonction exponentielle, nous indiquons les calculs (d'ailleurs bien connus) qui sont nécessaires pour déduire de la formule donnée dans I.12 et de

$$(7) \quad \xi * \eta \in \bar{L}$$

(à démontrer par la suite) la forme finale de la formule de Campbell et Hausdorff.

3. Formule de Campbell, Baker, Hausdorff et Dynkin.

Soit V l'espace sous-jacent de l'algèbre libre $F(X)$. Pour $a \in F(X)$, soit $\text{ad}(a) \in \text{End } V$, défini par $\text{ad}(a)(v) = av - va$. D'après la propriété universelle de $F(X)$, la fonction $x \mapsto \text{ad}(x) : X \rightarrow \text{End } V$ se prolonge d'une façon unique en un morphisme d'algèbres, $\psi : F(X) \rightarrow \text{End } V$. Désignons par V_1 le $F(X)$ -module régulier donné par $(a, v) \mapsto av$, $a \in F(X)$, $v \in V$, et par V_2 le $F(X)$ -module défini par $a.v = \psi(a)(v)$, $a \in F(X)$, $v \in V$. Un morphisme $\varphi : V \rightarrow V$ d'espaces vectoriels est déterminé par son effet sur 1 et sur des éléments générateurs $x_1 \dots x_n$, $x_j \in X$; posons $\varphi(1) = 0$, $\varphi(x) = x$, $\varphi(x_1 \dots x_n) = (x_1 \dots x_{n-1}) \cdot x_n$ pour $n > 1$. Remarquons que

$$\varphi(x_1 \dots x_n) = x_1 x_2 \dots x_n = \text{ad}(x_1) \dots \text{ad}(x_{n-1})(x_n).$$

Par linéarité, on en déduit d'abord

$$(8) \quad \varphi(xv) = x \cdot \varphi(v), \quad x \in X, \quad v \in V,$$

puis

$$(9) \quad \varphi(av) = a \cdot \varphi(v), \quad a \in F(X), \quad v \in V.$$

Autrement dit, $\varphi : V_1 \rightarrow V_2$ est un morphisme de $F(X)$ -modules. La fonction $\text{ad} : \Lambda F(X) \rightarrow \Lambda \text{End}(X)$ est un morphisme des algèbres de Lie, et il en est de même de ψ ; puisqu'on a $\text{ad}(x) = \psi(x)$ pour $x \in X$, on en déduit $\text{ad}(a) = \psi(a)$ pour tous les éléments a de l'algèbre de Lie L engendrée par X . Cette proposition est équivalente à la suivante :

$$(10) \quad [a, v] = a.v, \quad a \in L, \quad v \in V.$$

Une combinaison de (9) et (10) donne

$$(11) \quad \varphi(av) = [a, \varphi(v)], \quad a \in L, \quad v \in V.$$

Nous affirmons que

$$(12) \quad \varphi(v) = nv \quad \text{pour } v \in L, \quad v \text{ homogène de degré } n.$$

Nous démontrerons (12) par récurrence sur n . C'est certainement vrai pour $n = 0, 1$; supposons-le vrai pour $m < n$, ou $n > 1$. Puisque $v = \sum [a_j, b_j]$, avec une famille finie d'éléments a_j, b_j homogènes de L de degrés $< n$, nous pouvons supposer que

$$v = [a, b], \quad a, b \in L, \quad a, b \text{ homogènes, } p = \deg a < n, \quad q = \deg b < n, \quad p + q = n.$$

Alors

$$\varphi(v) = \varphi[a, b] = \varphi(ab) - \varphi(ba) = [a, \varphi(b)] - [b, \varphi(a)] \text{ d'après (11).}$$

Par récurrence,

$$\varphi(a) = pa, \quad \varphi(b) = qb.$$

$$\text{Puis } \varphi(v) = [a, pb] - [b, qa] = (p + q)[a, b] = nv.$$

Définissons $\varphi^n : V^n \rightarrow V^n$ par $\varphi^n = \frac{1}{n} \varphi^n$, où V^n est la composante homogène de V de degré n . Le morphisme $\varphi = \varphi^0 + \varphi^1 + \dots$ d'espaces vectoriels gradués applique V dans L , d'après la définition de φ , et induit l'identité sur L . Par conséquent, φ est une rétraction de V sur L .

La rétraction $\varphi : F(X) \rightarrow F(X)$ est évidemment continue par rapport à la topologie induite par celle de $\overline{F}(X)$; elle se prolonge donc à une rétraction φ unique de $\overline{F}(X)$ sur \overline{L} . Cela nous donne le résultat suivant :

I.13. PROPOSITION. - Soient X un ensemble, $\overline{F}(X)$ l'algèbre de Banach fortement ultramétrique de I.2, et $\overline{L}(X)$ l'algèbre de Lie fermée engendrée dans $\overline{F}(X)$ par X . Si $M(X)$ est le monoïde libre engendré par X , et $\{\mu_j ; j \in J\}$ une famille d'éléments de $M(X)$ tels que la famille $\{j \in J ; \deg \mu_j = m\}$ soit finie pour $m = 0, 1, 2, \dots$, alors l'élément $a = \sum_j r_j \mu_j$ est bien défini quelle que soit la famille $\{r_j \in K ; j \in J\}$, et les propositions suivantes sont équivalentes :

1° $a \in \overline{L}(X)$ (c'est-à-dire a peut être exprimé comme une série éventuellement infinie de polynômes de Lie),

$$2° \quad a = \sum_j (\deg \mu_j)^{-1} r_j \overline{\mu_j}, \quad \text{où } \overline{x_1 \dots x_m} = (\text{ad}(x_1) \dots \text{ad}(x_{m-1}) x_m).$$

Cela nous met en mesure de donner la formulation finale de la formule trouvée d'abord dans I.12 :

I.14. THÉORÈME (Formule de Campbell-Hausdorff-Baker-Dynkin).

1° Si A est une algèbre de Banach fortement ultramétrique bornée, l'ensemble A_1 des éléments p , vérifiant $\|p\| < 1$, est une algèbre de Lie fermée dans ΛA , et un groupe par rapport à l'opération $(x, y) \mapsto x * y$ qui s'exprime par la

formule suivante : Pour $\xi, \eta \in K[[\xi, \eta]]$, on a

$$(13) \quad \xi * \eta = \sum \frac{c(p_1, q_1, \dots, p_n, q_n)}{p_1 + q_1 + \dots + p_n + q_n} \overline{\xi^{p_1} \eta^{q_1} \dots \xi^{p_n} \eta^{q_n}},$$

sommée sur $n = 1, 2, \dots, p_1 + q_1 \geq 1, \dots, p_n + q_n \geq 1$, où

$$(i) \quad c(p_1, q_1, \dots, p_n, q_n) = - \frac{(-1)^n}{n \cdot p_1! q_1! \dots p_n! q_n!}$$

$$(ii) \quad \overline{x_1 \dots x_m} = (\text{ad } x_1) \dots (\text{ad } x_{n-1}) x_n \text{ pour } x_j \in \{\xi, \eta\}.$$

Si on écrit $\xi * \eta = \sum_{\mu \in M(\xi, \eta)} q(\mu) \mu$ comme dans (6), alors on a aussi

$$(14) \quad \xi * \eta = \xi + \eta + \frac{1}{2} [\xi, \eta] + \sum_{\mu \in M(\xi, \eta)} r(\mu) \overline{\mu \xi \eta},$$

où $r(\mu) = (\text{deg } \mu + 2)^{-1} (q(\mu \xi \eta) - q(\mu \eta \xi)) \in \mathbb{Q}$ (voir (6)).

2° Pour tous les éléments $u, v \in A_1$ on a

$$\exp(u * v) = \exp(u) \exp(v),$$

et exp applique A_1 bijectivement sur le groupe multiplicatif $1 + A_1$.

Notons que, dans (13), beaucoup de sommants sont 0, parce qu'on a $\overline{x_1 \dots x_m} = 0$ dès que $x_{m-1} = x_m$; cela nous permet d'observer que, après avoir appliqué $\overline{}$ à la formule (6), les seuls indices de $M(\xi, \eta)$, qui contribuent encore à la somme, sont $\xi, \eta, [\xi, \eta]$ et $\overline{\mu \xi \eta}$, où $\mu \in M(\xi, \eta)$. Mettons l'accent sur le fait que, bien que la formule (13) soit intéressante en elle-même, et pour les questions de convergence (Chap. II), c'est vraiment la formule (14) qui est significative pour la théorie des groupes de Lie, même si les nombres rationnels $r(\mu)$ ne sont pas explicitement connus. Comme nous l'avons déjà souligné dans le contexte de la formule provisoire (voir I.12 et (6)) pour les nombres $q(\mu)$, on n'a pas encore résolu, même partiellement, le problème suivant.

PROBLÈME. - Trouver, s'il est possible, une formule, pour les nombres rationnels $r(\mu)$ de (14). Si non, chercher des propriétés des $r(\mu)$, du point de vue de la théorie des nombres, de l'analyse combinatoire, de l'analyse numérique (par exemple, des propriétés asymptotiques).

Tucker HAWTHORNE [Tulane University] a formulé un programme en FORTRAN II pour le calcul des $r(\mu)$ sur ordinateur, ce qui est un problème combinatoire, entre autres choses. On a calculé les $r(\mu)$ jusqu'à $\text{deg } \mu \leq 7$ (ce qui donne les termes de la série (14) jusqu'au degré 9). Par exemple, il y a $2^7 = 128$ nombres $r(\mu)$ pour le seul degré 7; le temps requis pour ces calculs est considérable, même sur les ordinateurs à grande vitesse. On a observé, par exemple, que, pour l'involution $t : [[\xi, \eta]] \rightarrow K[[\xi, \eta]]$, donnée par $t(\xi) = \eta, t(\eta) = \xi$, on a

$$r(t(\mu)) = \pm r(\mu),$$

ce qu'on pourrait démontrer d'une façon générale. Après avoir fait les calculs jusqu'à $\text{deg } \mu \leq 6$, on était convaincu que, dans la forme réduite, le nombre rationnel $r(\mu)$ est toujours de la forme $\pm 1/n$ avec $n \in \mathbb{N}$, mais pour $\text{deg } \mu = 7$ on

a trouvé des dénominateurs 13 , 19 , 31 . Empiriquement, $r(\mu)$ est petit pour des mots "réguliers" comme $\mu = \xi^n$, et relativement grand pour des mots "mélangés" comme $\xi_\eta \xi_\eta \dots \xi_\eta$. Par exemple,

$$- r(\xi^7) = 1/1209600 , \quad r(\eta(\xi\eta)^3) = 1/5040 ;$$

les valeurs absolues des autres sont intermédiaires. On observe aussi des différences entre les deux cas $\deg(\mu) \equiv 0 , 1 (2)$: un terme $r(\mu)$ sur quatre est nul pour $\deg(\mu) = 5 , 7$; les termes $r(\xi^n)$, $r(\eta^n)$ sont les seuls qui sont nuls pour $\deg(\mu) = n = 2 , 4 , 6$.

4. Bigèbres.

Il nous faut comprendre que, pour des espaces de Banach quelconques (définis par I.1. (i), (ii), (iv)), on peut introduire un produit tensoriel. En fait, considérons, sur le produit tensoriel algébrique de A et B , $A \otimes B$ la fonction $\| \| : A \otimes B \rightarrow \mathbb{R}^+$ donnée par

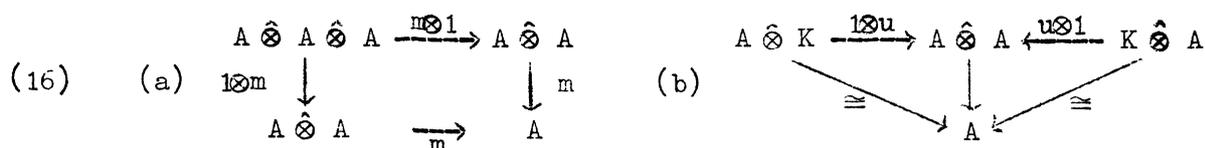
$$(15) \quad \|z\| = \inf_{\mathbb{F}} \sum \|a_j\| \|b_j\| ,$$

où la borne inférieure est prise sur l'ensemble de toutes les familles finies $\mathbb{F} = \{(a_j , b_j) ; j = 1 , \dots , n(\mathbb{F})\}$ telles que $z = \sum_1^{n(\mathbb{F})} a_j \otimes b_j$.

On montre que $\| \|$ définit une norme sur $A \otimes B$. (Si A et B sont ultramétriques et si les topologies de A et B définies par des filtrations A_n , B_n , alors la topologie définie par cette norme sur $A \otimes B$ est donnée par la filtration $(A \otimes B)_n = \sum A_p \otimes B_q$, sommée sur $p + q = n$.) Soit $A \hat{\otimes} B$ l'espace de Banach complété par rapport à cette norme.

Le produit tensoriel ainsi défini a la propriété universelle : Si $b : A \otimes B \rightarrow C$ est une fonction bilinéaire continue, il existe un morphisme continu, et un seul, $b' : A \hat{\otimes} B \rightarrow C$ tel que $b(x , y) = b'(x \otimes y)$ quels que soient $x \in A , y \in B$.

Une algèbre de Banach unifère peut alors être caractérisée par la donnée de deux morphismes $m : A \hat{\otimes} A \rightarrow A$ et $u : K \rightarrow A$ d'espaces de Banach tels que les diagrammes



soient commutatifs.

I.15. DEFINITION. - Une cogèbre de Banach A est un espace de Banach A avec des morphismes $c : A \rightarrow A \hat{\otimes} A$, $\alpha : A \rightarrow K$ d'espaces de Banach tels que les diagrammes duaux de (8) soient commutatifs avec c remplaçant m , α remplaçant u . On dit que c est une co-multiplication et α une co-identité ou co-unité ; mais, dans ce contexte, on préfère l'appeler une augmentation. Autrement dit, c satisfait la condition

$$(17) \quad (1 \otimes c)c = (c \otimes 1)c ,$$

et α les conditions

$$(18) \quad (1 \otimes \alpha) c(a) = a \otimes 1 , \quad (\alpha \otimes 1) c(a) = 1 \otimes a , \quad a \in A .$$

Une bigèbre de Banach est une algèbre de Banach unifère avec une co-multiplication c et une augmentation α telles que c et α soient des morphismes continus d'algèbres. (On note que le produit tensoriel $A \hat{\otimes} B$ de deux algèbres de Banach est une algèbre de Banach telle que

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' .)$$

Il s'entend qu'on a ces concepts pour des algèbres discrètes ; en effet, dans un sens technique, ce cas est compris dans notre définition en ce qu'une algèbre discrète sur K est une algèbre de Banach ultramétrique par rapport aux normes discrètes sur K et A .

Nos exemples d'algèbres de Banach fortement ultramétriques sont des bigèbres de diverses façons.

I.16. EXEMPLE. - Soient X un ensemble, et $\overline{F}(X)$ l'algèbre de Banach de I.2. Par la propriété universelle de $\overline{F}(X)$, (I.3), on peut définir deux \mathcal{B} -morphisms $c, d : \overline{F}(X) \rightarrow \overline{F}(X) \otimes \overline{F}(X)$ tels que

$$c(x) = x \otimes 1 + 1 \otimes x , \quad d(x) = x \otimes x ,$$

quel que soit $x \in X$, et deux \mathcal{B} -morphisms $\alpha, \beta : \overline{F}(X) \rightarrow K$ tels que

$$\alpha(X) = \{0\} , \quad \beta(X) = \{1\} .$$

On vérifie qu'on a

$$(1 \otimes c) c(x) = x \otimes 1 \otimes 1 + 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes x = (c \otimes 1) c(x)$$

et

$$(1 \otimes d) d(x) = x \otimes x \otimes x = (d \otimes 1) d(x) , \quad x \in X$$

ce qui suffit à montrer que c et d sont des co-multiplications (parce que des \mathcal{B} -morphisms sont déterminés par leur donnée sur tout ensemble de générateurs). On vérifie aussi que les conditions (18) sont satisfaites pour c, α et d, β , en prenant pour a un générateur $x \in X$, ce qui suffit dans ce cas pour montrer que α et β sont des augmentations pour c et d , respectivement.

Dans les bigèbres, il y a deux types d'éléments qui jouent un rôle important.

I.17. DÉFINITION. - Soit a un élément d'une bigèbre A (de Banach). On dit que a est primitif si

$$(19) \quad c(a) = a \otimes 1 + 1 \otimes a ,$$

et monoïdal, si

$$(20) \quad c(a) = a \otimes a , \quad a \neq 0 .$$

L'ensemble des éléments primitifs (resp. monoïdaux) est appelé $P(A)$ (resp. $G(A)$).
Si A est fortement ultramétrique, nous écrivons

$$P_1(A) = P(A) \cap A_1 \quad \text{et} \quad G_1(A) = G(A) \cap (1 + A_1) .$$

I.18. PROPOSITION. - Soit A une bigèbre de Banach.

1° $P(A)$ est une algèbre de Lie fermée dans ΛA tel que $P(A) \subseteq \alpha^{-1}(0) = \ker \alpha$.
De plus, $P_1(A)$ est une sous-algèbre de Lie fermée.

2° $G(A)$ est un monoïde fermé dans le monoïde multiplicatif de A tel que
 $G(A) \subseteq \alpha^{-1}(1) .$

De plus, $G_1(A)$ est un sous-groupe fermé.

Les démonstrations sont élémentaires à partir des définitions.

I.19. PROPOSITION. - Soit A une bigèbre de Banach fortement ultramétrique. Alors les fonctions exponentielle et logarithme induisent des fonctions inverses

$$P_1(A) \begin{array}{c} \xrightarrow{\exp_P} \\ \xleftarrow{\log_G} \end{array} G_1(A) .$$

En particulier, $P_1(A)$ est un sous-groupe de $(A, *)$.

Démonstration.

1° Soit $a \in P_1(A)$. Puisque c est un β -morphisme, nous avons

$$c(\exp(a)) = \exp(c(a)) .$$

Mais

$$\exp(c(a)) = \exp(a \otimes 1 + 1 \otimes a) = \exp(a \otimes 1) \exp(1 \otimes a) ,$$

car $a \in P(A)$, et on peut appliquer I.6 puisque $a \otimes 1$ et $1 \otimes a$ commutent dans $A \otimes A$. Evidemment,

$$\exp(a \otimes 1) = (\exp(a)) \otimes 1 \quad \text{et} \quad \exp(1 \otimes a) = 1 \otimes \exp(a) ,$$

d'où finalement

$$c(\exp(a)) = \exp(a) \otimes \exp(a) .$$

2° Similairement, on voit que $a \in G_1(A)$ entraîne $c(\log(a)) = \log(a) \otimes 1 + 1 \otimes \log(a)$, en utilisant I.10, cette fois.

3° Nous avons alors les restrictions et co-restrictions \exp_P et \log_G comme indiquées dans la proposition. Tenant compte de I.5 ce sont des fonctions inverses. Le reste est immédiat à cause de I.11.

C'est le premier résultat de cette théorie où la fonction exponentielle apparaît avec une algèbre de Lie comme domaine de définition. Dans notre exemple fondamental $(\mathbb{F}(X), c, \alpha)$ (voir I.2 et I.16), nous avons $X \subseteq P_1(A) = P(A)$ d'après la définition. Soit $\bar{L}(X)$ l'algèbre de Lie fermée engendrée par X dans ΛA . Alors

$\overline{L}(X) \subseteq P(A)$ d'après I.18, 1°, et $x * y \in P_1(A)$ d'après I.19, quels que soient $x, y \in X$. Pour conclure que, en fait, $x * y \in \overline{L}(X)$, il faut que nous démontrions l'égalité $\overline{L}(X) = P(A)$. Cela demande d'abord quelques observations sur les bigèbres discrètes.

Soit A une bigèbre. La multiplication $(p_1, \dots, p_n) \mapsto p_1 \dots p_n : P(A)^n \rightarrow A$ induit un morphisme d'espaces vectoriels $\mu : \otimes^n P(A) \rightarrow A$; posons $F^n A = K + \text{im } \mu^n$. Alors $F^0 A = K$, $F^1 A = K + P(A)$, $F^2 A$, ... est une filtration croissante, satisfaisant à $F^m A F^n A \subseteq F^{m+n} A$, dite filtration primitive. Nous disons que A est primitivement engendrée si $A = \sum_m F^m A$. La définition $c(p) = p \otimes 1 + 1 \otimes p$ pour $p \in P(A)$ entraîne $c(F^m A) \subseteq \sum F^r A \otimes F^s A$, sommé sur $r + s = m$. Si nous définissons une filtration sur un produit tensoriel d'algèbres filtrées par

$$F^m(A \otimes B) = \sum F^r A \otimes F^s A,$$

sommé sur $r + s = m$, nous obtiendrons que c est un morphisme d'algèbres filtrées.

Commençons par quelques observations sur des filtrations croissantes et les graduations associées. Soit A un espace vectoriel; une filtration (croissante) sur A est une suite $F^0 A \subseteq F^1 A \subseteq \dots$ de sous-espaces vectoriels, et la donnée d'une filtration sur A fait de A un espace vectoriel filtré. Si A et B sont des espaces vectoriels filtrés, un morphisme d'espaces vectoriels filtrés $f : A \rightarrow B$ est une application linéaire telle que $f(F^m A) \subseteq F^m B$, $m = 0, 1, \dots$. Le produit tensoriel $A \otimes B$ de deux espaces vectoriels filtrés est le produit tensoriel de A et B avec la filtration définie par

$$F^m(A \otimes B) = \sum F^r A \otimes F^s B, \quad r + s = m.$$

On a évidemment une catégorie $F\text{-vect}$ d'espaces vectoriels filtrés munie d'un produit tensoriel. Un espace vectoriel gradué est un espace A somme directe $A^0 \oplus A^1 \oplus \dots$ de sous-espaces vectoriels. Un morphisme d'espaces vectoriels gradués conserve les sommants directs. Si A et B sont des espaces vectoriels gradués, alors leur produit tensoriel est gradué aussi, avec

$$(A \otimes B)^m = \sum A^r \otimes B^s, \quad r + s = m.$$

Nous venons de définir la catégorie $G\text{-vect}$ d'espaces vectoriels gradués, qui, elle aussi, est munie d'un produit tensoriel. Définissons un foncteur $G : F\text{-vect} \rightarrow G\text{-vect}$ par

$$(GA)^m = F^m A / F^{m-1} A, \quad m = 0, 1, \dots, \quad F^{-1} A = 0;$$

le prolongement de ce foncteur défini sur des objets aux morphismes est évident. La suite exacte

$$0 \rightarrow F^{r-1} A \otimes F^s B + F^r A \otimes F^{s-1} B \rightarrow F^r A \otimes F^s B \rightarrow G^r A \otimes G^s B \rightarrow 0$$

nous permet de définir un morphisme

$$\varphi^m : \sum_{r+s=m} G^r A \otimes G^s B \rightarrow G^m(A \otimes B),$$

pour $r + s = m$, par

$$\varphi^m((a_r + F^{r-1} A) \otimes (b_s + F^{s-1} B)) = a_r \otimes b_s + \sum_{p+q=m-1} F^p A \otimes F^q B,$$

Cela nous donne un morphisme naturel

$$\varphi_{AB} : GA \otimes GB \rightarrow G(A \otimes B),$$

qui est visiblement surjectif. Mais on peut démontrer (en comparant les deux foncteurs additifs $GA \otimes G(?)$ et $G(A \otimes (?))$) sur des espaces vectoriels filtrés de dimension ≤ 1 , et en observant que chaque espace vectoriel filtré est somme directe de sous-espaces filtrés de dimension ≤ 1) :

I.20. LEMME. - $\varphi_{AB} : GA \otimes GB \rightarrow G(A \otimes B)$ est un isomorphisme.

Autrement dit, G est un "foncteur monoïdal". Dans une catégorie d'espaces vectoriels, munie d'un produit tensoriel, nous pouvons définir des algèbres (unifères), des cogèbres, des bigèbres, parce que ces concepts sont caractérisés seulement par des diagrammes comme (16) et leurs duaux qui comportent des morphismes de la catégorie. Nous pouvons parler, ensuite, sans ambiguïté, des algèbres, cogèbres, bigèbres filtrées et des algèbres, cogèbres, bigèbres graduées. En effet, nous avons vu le résultat suivant.

I.21. LEMME. - Si A est une bigèbre, alors $FA = \bigcup_m F^m A$ est une bigèbre filtrée primitivement engendrée. On a $P(FA) = P(A)$.

Puisque le foncteur G conserve les diagrammes (16) et leurs duaux d'après I.20, on peut conclure que GA est une algèbre, cogèbre, bigèbre graduée chaque fois que A est une algèbre, cogèbre, bigèbre filtrée.

I.22. LEMME. - Soit A une bigèbre filtrée par sa filtration primitive. Alors GA est une bigèbre graduée commutative.

Démonstration. - Nous avons $GA = GFA$, et puisque FA est engendrée par $K.1 + P(A)$, alors GA est engendrée par $G^1 A = (K.1 + PA)/K.1$. Il suffit donc de montrer que les éléments de $G^1 A$ commutent deux à deux. Soient donc

$$\bar{a}, \bar{b} \in G^1 A, \quad \bar{a} = a + K.1, \quad \bar{b} = b + K.1, \quad a, b \in P(A),$$

alors $ab \in F^2 A$; mais

$$[a, b] = ab - ba \in P(A) \subseteq F^1 A \text{ d'après I.18,}$$

donc

$$\overline{ab} - \overline{ba} = [a, b] + F^1 A = \bar{0}.$$

I.23. LEMME. - Soit A une bigèbre graduée commutative engendrée par $A^0 + A^1$. Si $A^1 \subseteq P(A)$, alors $P(A) \subseteq A^0 + A^1$.

Démonstration. - Soit $p \in P(A)$; il faut démontrer $p \in A^1$. Soit $p = p_0 + p_1 + p_2 + \dots$

la décomposition de p en composantes homogènes ; on voit sans peine que $p_m \in PA$, $m = 0, 1, 2, \dots$. Donc il suffit de supposer $p = p_m \in A^m$, $m \geq 1$ et de montrer $m = 1$. Puisque $A^0 + A^1$ engendre A , nous avons

$$p = \sum p_{ij} \dots p_{mj} \text{ pour une famille } \{p_{ij} \in A_1 \subseteq P(A), i=1, \dots, m, j=1, \dots, k\}.$$

Soit $\mu : A \otimes A \rightarrow A$ la multiplication d'algèbre. Alors

$$\mu c(p) = \mu(p \otimes 1 + 1 \otimes p) = p + p = 2p.$$

D'autre part,

$$c(p) = \sum_i \prod_j c(p_{ij}) \sum_i \prod_j (p_{ij} \otimes 1 + 1 \otimes p_{ij});$$

or, A étant commutative, m est un morphisme d'algèbres, donc

$$\mu c(p) = \sum_i \prod_j (p_{ij} + p_{ij}) = 2^m p.$$

Il en résulte que $2^m p = 2p$. Mais $p \neq 0$, et car $K \neq 2$, donc $m = 1$.

I.24. LEMME. - Si A est une bigèbre filtrée telle que $F^1 A \subseteq F^0 A + P(A) \subseteq FA$ et que FA soit engendrée par $F^1 A$, alors $F^1 A = F^0 A + P(A)$.

Démonstration. - Soit $p \in P(A)$, et soit m minimal tel que $p \in F^m A$. Il faut montrer $m \leq 1$. On vérifie que l'élément $p + F^{m-1} A$ de $G^m A$ est dans PGA . Donc $G^1 A \subseteq PGA$. Puisque $F^1 A$ engendre FA , alors $G^0 A + G^1 A$ engendre GA . Après I.23, nous avons $G^1 A = PGA$, ce qui entraîne $m \leq 1$.

I.25. PROPOSITION. - Soit A une bigèbre. Soit $V \subseteq P(A)$ un sous-espace vectoriel tel que l'algèbre A est engendrée par $K.1 + V$. Alors $V = P(A)$.

Démonstration. - Définissons une filtration de A par $F^0 A = K.1$, $F^1 A = K.1 + V$, $F^m A =$ espace vectoriel engendré par des produits $v_1 \dots v_k$, $v_j \in V$, $k \leq m$. De $V \subseteq P(A)$ nous déduisons $c(V) \subseteq V \otimes 1 + 1 \otimes V$, donc cette filtration est une filtration de bigère. Le lemme précédent montre alors que $K.1 + V = K.1 + P(A)$. Puisque $V \subseteq P(A)$ et $K.1 \cap P(A) = \{0\}$ (d'après I.18, 1°), la proposition est démontrée.

I.26. COROLLAIRE. - Soit $(\overline{F}(X), c, \alpha)$ la bigèbre de Banach de I.16. Alors $P(\overline{F}(X))$ est la sous-algèbre de Lie fermée engendrée par X .

Démonstration. - Soit $F(X)$ l'algèbre engendrée dans $\overline{F}(X)$ par X (I.2) ; c'est en fait l'algèbre libre engendrée par X . On voit que $c(F(X)) \in F(X) \otimes F(X)$. Donc $F(X)$ est une bigèbre. D'après la définition de c , nous savons que $X \subseteq P(F(X))$. Soit L l'algèbre de Lie engendrée dans $F(X)$ par X . Alors $L \subseteq P(F(X))$ (I.15). Puisque $F(X)$ est engendrée comme algèbre unifère par X , il est engendré, a fortiori, par $K.1 + L$. La proposition I.22 montre alors que $L = P(F(X))$. Donc $\overline{L} = P(F(X))^-$. Tout revient donc à montrer

$$P(\overline{F}(X)) \subseteq P(F(X))^-.$$

Soit $p \in P(\overline{F}(X))$. Mais $\overline{F}(X)$ est le produit direct des sous-espaces vectoriels $F(X)^{(n)}$ des polynômes homogènes de degré n , et on écrit $p = p_0 + p_1 + \dots$, $p_n \in F(X)^{(n)}$. On vérifie que

$$c(p_0) + c(p_1) + \dots = c(p) = p \otimes 1 + 1 \otimes p = (p_0 \otimes 1 + 1 \otimes p_0) + (p_1 \otimes 1 + 1 \otimes p_1) + \dots,$$

donc $p_m \in P(F(X))$ pour tous m . Puisque $p = \lim_m (p_0 + \dots + p_m)$ cela montre $p \in P(F(X))$.

I.27. COROLLAIRE. - $\xi * \eta$ est dans l'algèbre de Lie fermée engendrée par ξ et η dans $K[[\xi, \eta]]$.

Démonstration. - On a

$$\xi * \eta \in P_1(K[[\xi, \eta]]) = P(K[[\xi, \eta]]) \text{ après I.16, I.17, I.19 ;}$$

alors I.26 achève le corollaire.

Ce résultat nous donne la formule (7), formule fondamentale permettant d'obtenir la formule finale de Campbell-Hausdorff.

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
MATHÉMATIQUES PURES
PIERRE FOURIER

5. Bigèbres primitivement engendrées. Compléments.

Tandis que les résultats précédents suffisent pour la théorie de base des groupes de Lie, nous avons touché, avec les bigèbres, un sujet fortement intéressant. On peut compléter la théorie sans grands efforts par les propositions que nous allons énoncer sous le titre de compléments.

I.28. LEMME (MILNOR-MOORE). - Soit $f : A \rightarrow B$ un morphisme de bigèbres graduées tel que $A^0 = K.1$, et que $PA = A^1$. Alors f est injectif si, et seulement si, f^1 est injectif.

Démonstration. - Supposons f^1 injectif, posons

$$\ker f = J^0 + J^1 + J^2 + \dots ;$$

alors $J^0 = J^1 = 0$. Montrons $J^n = 0$ par récurrence sur n . Supposons que $J^m = 0$ pour $m < n$; alors

$$\ker(f^p \otimes f^q) = J^p \otimes A^q + A^p \otimes J^q = 0 \text{ pour } p, q < n.$$

Prenons $x \in J^n$; puisque f est un morphisme de cogèbres, nous avons

$$c_B^n f^n = (f \otimes f)^n c_A^n,$$

alors,

$$0 = c_B^n f^n(x) = (f \otimes f)^n c_A^n(x),$$

donc

$$c_A^n(x) \in \ker(f \otimes f)^n = A^0 \otimes J^n + J^n \otimes A^0,$$

donc $c_A^n(x) = x' \otimes 1 + 1 \otimes x''$. D'après la propriété de l'augmentation, nous avons

$$1 \otimes x = (\alpha \otimes 1) c_A(x) = \alpha(x') \otimes 1 + 1 \otimes x'' ,$$

donc $x'' = x$. Similairement $x = x'$. Alors $x \in P(A) = A^1$. Donc $x \in A^1 \cup \{0\}$.

Quel que soit l'espace vectoriel V , on peut former l'algèbre symétrique $S(V)$ (l'algèbre quotient de l'algèbre tensorielle $T(V)$ modulo l'idéal engendré par les $v \otimes w - w \otimes v$, $v , w \in V \subseteq T(V)$) ; alors $S(V)$ a la propriété universelle que chaque morphisme $f : V \rightarrow A$ d'espaces vectoriels dans une algèbre graduée commutative telle que $\text{im } f \subseteq A^1$ se prolonge d'une façon unique en un morphisme d'algèbres graduées $f' : S(V) \rightarrow A$. Cela nous permet de noter que $S(V)$ est une bigèbre graduée telle que $c(v) = v \otimes 1 + 1 \otimes v$, $v \in V$. D'après I.25 on voit $V = P(S(V))$, et si le A ci-dessus est une bigèbre, alors f' est un morphisme des bigèbres, dès que $A^1 = P(A)$.

Soit A une bigèbre primitivement filtrée, donc GA est une bigèbre commutative telle que $G^1 A = PGA$ (I.22, 23). Par la propriété universelle de $S(|PGA|)$ ($| \cdot |$ dénotant l'espace vectoriel sous-jacent), nous définissons un morphisme

$$\varphi_A : S(|PGA|) \rightarrow GA$$

de bigèbres. On voit $|PGA| = |PA|$.

I.29. THÉORÈME (MILNOR-MOORE). - $\varphi_A : S(|PA|) \rightarrow GA$ est un isomorphisme.

Démonstration. - φ_A est surjective parce que GA est engendrée par $A^1 = PGA$. Mais, d'après I.28, φ_A est injectif.

Ce théorème donne une description approximative de la structure des bigèbres primitivement engendrées ; dans le sens de I.29, elles ressemblent aux algèbres symétriques (c'est-à-dire aux algèbres de polynômes commutatifs). Aussi, I.29 explique le rôle de $P(A)$ dans une bigèbre, notamment en quel sens $P(A)$ "est libre dans A ". On a un phénomène de "liberté" pour l'ensemble $G(A)$ des éléments monoïdaux de A (qui est d'ailleurs plus facile à vérifier) : l'ensemble $G(A)$ est libre (linéairement indépendant).

Mais dans la proposition I.29, la structure de l'algèbre de Lie de PA est délibérément oubliée . Considérons une algèbre de Lie L et l'algèbre tensorielle $T(|L|)$.

Posons $U(L) = T(|L|)/I$, où I est l'idéal engendré par $v \otimes w - w \otimes v - [v, w]$, $v , w \in L$. Soit $\lambda : L \rightarrow \Lambda U(L)$ le morphisme d'algèbres de Lie canonique donné par $\lambda(v) = v + I$. Alors, pour chaque morphisme $f : L \rightarrow \Lambda A$ d'algèbres de Lie tel que A est une algèbre associative unifère, on trouve un morphisme d'algèbres unifères $f' : U(L) \rightarrow A$ et un seul tel que $f' \lambda = f$. On appelle $U(L)$ l'algèbre enveloppante de L . Le morphisme

$$v \mapsto \lambda(v) \otimes 1 + 1 \otimes \lambda(v) : L \rightarrow \Lambda(U(L) \otimes U(L))$$

d'algèbres de Lie donne un morphisme $c : U(L) \rightarrow U(L) \otimes U(L)$. Alors c est une

comultiplication qui fait de $U(L)$ une bigèbre telle que $\lambda(L) \subseteq P(U(L))$. De I.25, on déduit $\lambda(L) = P(U(L))$; notons que $U(L)$ est primitivement engendrée.

Soit maintenant A une bigèbre primitivement engendrée. Alors il existe un morphisme d'algèbres $\rho : U(PA) \rightarrow A$ unique qui se déduit du morphisme $PA \rightarrow \Lambda A$ d'algèbres de Lie. On vérifie que c'est un morphisme de bigèbres. Il est surjectif parce que A est primitivement engendrée. On utilise I.28 pour montrer que $G_\rho : GU(PA) \rightarrow GA$ est injectif, cela implique immédiatement que ρ est injectif. Alors on a le résultat suivant.

I.30. THÉORÈME. - Chaque bigèbre primitivement engendrée A est canoniquement isomorphe à la bigèbre enveloppante $U(PA)$.

On a un résultat parallèle pour des bigèbres A qui sont engendrées par l'ensemble $G(A)$ des éléments monoïdaux : elles sont isomorphes à l'algèbre de monoïde $K[G(A)]$ (ce qui est assez simple à voir).

Nous avons vu que nous pouvons retrouver une bigèbre primitivement engendrée A à partir de son algèbre de Lie $P(A)$ d'éléments primitifs. Est-il possible de retrouver une algèbre de Lie L à partir de sa bigèbre enveloppante ? Nous avons noté qu'on peut reconstruire $\lambda(L) = PU(L)$. On retrouve, en fait, L elle-même. C'est contenu dans le théorème suivant.

I.31. THÉORÈME (POINCARÉ, BIRKHOFF, WITT). - $L \cong \lambda(L)$ (sous la corestriction $\lambda : L \rightarrow \lambda(L)$).

Pour la démonstration de ce théorème, il suffirait de trouver une représentation fidèle $L \rightarrow \Lambda A$. Les démonstrations connues utilisent des raisonnements récursifs transfinis assez compliqués. (Dans sa thèse à la Tulane University, David WALLACE a donné une démonstration directe de l'injectivité de λ par des méthodes tout à fait différentes.) Les théorèmes I.30 et I.31, ensemble, montrent que les catégories des algèbres de Lie et des bigèbres primitivement engendrées sont équivalentes. Naturellement, le théorème I.29 s'applique au cas de $A = U(L)$.

6. Automorphismes et dérivations.

Pour la théorie des groupes et des algèbres de Lie, il est bon de comprendre le rapport entre les automorphismes et les dérivations ; on peut traiter cette question dans le cadre de la théorie algébrique de la fonction exponentielle. Nous avons besoin de quelques préliminaires.

I.32. DÉFINITION. - Soit A une algèbre de Banach unifère sur K . Nous disons qu'un élément $a \in A$ est exponentiellement engendré si la série exponentielle converge absolument sur une boule ouverte contenant a , et si a est un élément de la sous-algèbre de Banach unifère engendrée par $\exp a$.

I.33. PROPOSITION. - Soit A une algèbre de Banach unifère fortement ultramétrique. Alors un élément $a \in A$ est exponentiellement engendré si, et seulement si,
 $a \in A_1$.

Démonstration. - Puisque le rayon de convergence de la série exponentielle est 1 (le corps de base étant discrètement valué), cette condition est évidemment nécessaire. Montrons qu'elle est suffisante. Supposons donc $a \in A_1$. Nous pouvons supposer que A est engendrée par a . D'après I.4, il existe un morphisme unique $K[[\xi]] \rightarrow A$ unique qui envoie X sur a . Il envoie $\exp X$ sur $\exp a$; pour montrer que a est contenu dans l'algèbre de Banach unifère engendrée par $\exp a$, il suffit de montrer que ξ est exponentiellement engendré dans $K[[\xi]]$. Mais K est engendré par tout élément $p = a_1 \xi^1 + a_2 \xi^2 + \dots$ tel que $a_1 \neq 0$, parce qu'on peut résoudre l'équation fonctionnelle $q(p(\xi)) = \xi$ par une série $q = b_1 \xi + \dots$ convenablement construite. Alors $K[[\xi]]$ est engendré, comme une algèbre de Banach unifère, par $\exp - 1$, donc par \exp .

Nous utilisons un lemme purement technique, qui néanmoins reflète des propriétés de la fonction exponentielle :

I.34. LEMME. - Soient A et L des algèbres de Banach unifères telles que $A \otimes A \subseteq L$ de façon que les fonctions $x \mapsto x \otimes 1$, $1 \otimes x : A \rightarrow L$ soient continues. Pour $a \in A$, posons

$$\bar{a} = (a \otimes 1 + 1 \otimes a , a) \in L \times A .$$

Alors $\exp \bar{a} = (\exp a \otimes \exp a , \exp a)$. Pour toute sous-algèbre fermée unifère M de $L \times A$, la relation $\bar{a} \in M$ entraîne $(\exp a \otimes \exp a , \exp a) \in M$, et si \bar{a} est exponentiellement engendré dans $L \times A$, alors on a l'implication inverse.

Démonstration. - Tenant compte de la permutabilité de $a \otimes 1$ et $1 \otimes a$ et de la continuité de $x \mapsto x \otimes 1$, $1 \otimes x : A \rightarrow L$ on calcule

$$\exp \bar{a} = (\exp a \otimes \exp a , \exp a)$$

(calcul qui est d'ailleurs analogue à celui de la démonstration de I.18, 1°). Le reste est alors immédiat.

Les concepts d'automorphisme et de dérivation ont trait à une "algèbre de Banach non nécessairement associative" ; d'une façon précise, nous avons la définition suivante.

I.35. DÉFINITION. - Soit E un espace de Banach muni d'une application continue bilinéaire $(x , y) \mapsto xy : E \times E \rightarrow E$, nommée produit. Un automorphisme a de E est un automorphisme continu d'espace vectoriel vérifiant l'identité

$$a(xy) = a(x) a(y) .$$

Une dérivation d de E est un endomorphisme continu d'espace vectoriel tel que $d(xy) = d(x) y + x d(y)$ quels que soient $x , y \in E$.

Si E est un espace de Banach et $L(E)$ l'espace de Banach de tous les endomorphismes continus de E , on peut identifier le produit tensoriel algébrique $L(E) \otimes L(E)$ à une sous-algèbre de $L(E \hat{\otimes} E)$ de façon que $(S \otimes T)(x \otimes y) = Sx \otimes Ty$. Les applications $T \mapsto T \otimes 1$, $1 \otimes T : L(E) \rightarrow L(E \hat{\otimes} E)$ sont continues.

I.36. THÉOREME. - Soit E un espace de Banach muni d'un produit (I.35), et soit $d \in L(E)$. Si d est une dérivation, alors $\exp d$ est un automorphisme. Si $(d \otimes 1 + 1 \otimes d, d)$ est exponentiellement engendré dans $L(E \hat{\otimes} E) \times L(E)$ (I.32), et si $\exp d$ est un automorphisme, alors d est une dérivation.

Démonstration. - D'après la propriété universelle du produit tensoriel $\hat{\otimes}$ nous obtenons un morphisme $m : E \hat{\otimes} E \rightarrow E$, et un seul, tel que $m(x \otimes y) = xy$ pour tous $x, y \in E$. Posons

$$M = \{(S, T) \in L(E \hat{\otimes} E) \times L(E) : mS = Tm\}.$$

Alors M est une sous-algèbre unifère fermée de $L(E \hat{\otimes} E) \times L(E)$. Nous calculons

$$dm(x \otimes y) = d(xy),$$

$$(\exp d) m(x \otimes y) = (\exp d)(xy),$$

$$m(d \otimes 1 + 1 \otimes d)(x \otimes y) = d(x)y + xd(y),$$

$$m(\exp d \otimes \exp d)(x \otimes y) = (\exp d)(x) \otimes (\exp d)(y),$$

nous en déduisons que d est une dérivation si, et seulement si, $(d \otimes 1 + 1 \otimes d, d) \in M$, et que $\exp d$ (étant toujours inversible) est un automorphisme si, et seulement si, $(\exp d \otimes \exp d, \exp d) \in M$. Alors le théorème résulte du lemme I.34.

Appliquons le théorème au cas fortement ultramétrique. Convenons d'appeler un endomorphisme d'un espace de Banach une contraction stricte, si

$$\|f\| = \sup\{\|f(x)\| ; \|x\| \leq 1\} < 1.$$

I.37. COROLLAIRE. - Soit E un espace de Banach fortement ultramétrique muni d'un produit. Soit $d \in L(E)$. Si d est une dérivation, alors $\exp d$ est un automorphisme. Si d est une contraction stricte et $\exp d$ est un automorphisme, alors d est une dérivation.

Démonstration. - D'après I.36, nous devons montrer que $(d \otimes 1 + 1 \otimes d, d)$ est exponentiellement engendrée pour une contraction stricte d . Mais

$$\|(d \otimes 1 + 1 \otimes d, d)\| \leq \max\{\|d \otimes 1 + 1 \otimes d\|, \|d\|\}$$

d'après la définition du produit direct d'espaces de Banach, et

$$\|d \otimes 1 + 1 \otimes d\| \leq \max\{\|d \otimes 1\|, \|1 \otimes d\|\}$$

parce que E est ultramétrique. Finalement

$$\|d \otimes 1\| = \|1 \otimes d\| = \|d\| < 1 ;$$

donc $\|(d \otimes 1 + 1 \otimes d, d)\| < 1$ et la proposition I.33 montre l'affirmation.

CONVENTION. - Si nous traitons des algèbres de Banach A , nous avons une fonction exponentielle définie sur une partie de A , nommée \exp . Mais si nous parlons aussi de l'algèbre de Banach $L(|A|)$ de tous les endomorphismes continus de l'espace vectoriel sous-jacent $|A|$, nous avons aussi à considérer une fonction exponentielle de $L(|A|)$. Nous convenons d'écrire celle-ci sous la forme $T \mapsto e^T$ à fin d'éviter toute confusion.

Par exemple nous avons le corollaire suivant.

I.38. COROLLAIRE. - Soit A une algèbre de Banach unifère fortement ultramétrique, et soit d une contraction de $|A|$. Si d est une dérivation, alors $\exp d$ est un automorphisme du groupe $(A_1, *)$ (I.11), i. e. $e^d(x * y) = e^d x * e^d y$. Inversement, si d est une contraction stricte et e^d est un automorphisme de $(A_1, *)$, alors d est une dérivation.

Démonstration. - Si d est une contraction, alors $d(A_1) \subseteq A_1$. Le corollaire résulte donc de I.37, puisqu'une contraction a de $|A|$ qui est un automorphisme de A satisfait à $p(a(x)) = a(p(x))$ quel que soit $p \in K[[\xi]]$.

On a des dérivations et des automorphismes d'un type spécial. Le lemme suivant est immédiat.

I.39. LEMME. - Soit A une algèbre de Banach unifère. Quel que soit $a \in A$, la fonction $\text{ad } a : A \rightarrow A$, $(\text{ad } a)(x) = [a, x] = ax - xa$ est une dérivation, et si a est inversible, la fonction $\text{int } a : A \rightarrow A$, $(\text{int } a)(x) = axa^{-1}$ est un automorphisme.

La fonction $\text{ad } a$ est appelée la dérivation intérieure (définie par a), et la fonction $\text{int } a$, l'automorphisme intérieur (défini par a). Evidemment, des dérivations intérieures peuvent être introduites dans les algèbres de Lie.

I.40. LEMME. - Soit A une algèbre de Banach unifère fortement ultramétrique. Soit $a \in A_1$; alors $\text{ad } a$ est une contraction stricte.

Démonstration.

$$\|(\text{ad } a)(x)\| = \|ax - xa\| \leq \max\{\|ax\|, \|xa\|\} \leq \|a\| \|x\|,$$

alors

$$\|\text{ad } a\| \leq \|a\| < 1.$$

Nous complétons maintenant les corollaires I.37 et I.38 :

I.41. PROPOSITION. - Soit A une algèbre de Banach unifère fortement ultramétrique, et soit $a \in A_1$. Alors

$$1^\circ e^{\text{ad } a} = \text{int}(\exp a).$$

2° $e^{\text{ad } a}(x) = a * x * (-a)$, quel que soit $x \in A_1$.

Démonstration. - Posons $L_a, R_a \in L(|A|)$, $L_a x = ax$, $R_a = xa$; alors L_a, R_a sont des contractions strictes (Cf. la démonstration de I.40) et $\text{ad } a = L_a - R_a$. Puisque A est associative, L_a et R_a commutent, donc

$$e^{\text{ad } a} = e^{R_a - L_a} = e^{R_a} e^{-L_a} \text{ d'après I.6 (appliqué à } L(|A|) \text{)}.$$

Mais on voit que

$$e^{R_a} e^{-L_a}(x) = \sum_{p,q=0}^{\infty} \frac{1}{p!} \frac{(-1)^q}{q!} a^p x a^q = (\exp a) x (\exp -a) = (\text{int } a)(x),$$

d'où le 1°. Supposons alors que $x \in A_1$. On trouve

$$\exp(a * x * (-a)) = (\exp a)(\exp x)(\exp -a) = e^{\text{ad } a}(\exp x) = \exp(e^{\text{ad } a}(x))$$

d'après I.11 et le 1° ci-dessus (Cf. aussi la démonstration de I.38). En prenant le log nous en déduisons le 2°.

La relation I.41, 2° est une sorte de linéarisation de l'opération $*$ dans certains cas ; par exemple elle entraîne un nouveau corollaire.

I.42. COROLLAIRE. - Soient A une algèbre de Banach fortement ultramétrique et N une sous-algèbre de Lie fermée de ΛA_1 . Alors N est un idéal de ΛA_1 si, et seulement si, N est un sous-groupe distingué de A ; s'il en est ainsi, on a la relation $a + N = a * N$ pour les classes de $(A_1, *)$ suyvant $(N, *)$.

Démonstration. - On sait que N est un sous-groupe de $(A_1, *)$ d'après I.14. Si N est un idéal de ΛA_1 , alors $(\text{ad } a)N \subseteq N$, donc $e^{\text{ad } a}N \subseteq N$ pour chaque $a \in A_1$, donc $(N, *)$ est distingué d'après I.41, 2°.

Inversement, si $(N, *)$ est distingué, on trouve $e^{\text{ad } a}N \subseteq N$ quel que soit $a \in A_1$.

Posons

$$M = \{S \in L(|A|) ; SN \subseteq N\}.$$

Alors $e^{\text{ad } a} \in M$, et M est une sous-algèbre unifère fermée de $L(|A|)$, parce que N est fermé. Suivant I.40 et I.33, $\text{ad } a$ est exponentiellement engendré dans M ; donc $\text{ad } a \in M$. Il s'en suit que N est un idéal de ΛA_1 .

Finalement, la relation $(\text{ad } a)N \subseteq N$ et la formule de Campbell-Hausdorff (I.14) entraînent

$$a * n \in a + N \text{ et } -a * (a + n) \in N$$

quels que soient $n \in N$.

7. Références.

- [1] BOURBAKI (Nicolas). - Groupes et algèbres de Lie. Chap. 2 et 3. - Paris, Hermann, 1972 (Act. scient. et ind., 1349 ; Bourbaki, 37).

- [2] HOFMANN (Karl H.). - Introduction to the theory of compact groups, I and II. Lecture Notes 1966/67 and 1968/69. - New Orleans, Tulane University, Department of Mathematics.
- [3] HOFMANN (Karl H.). - Die Formel von Campbell, Hausdorff und Dynkin, und die Definition Liescher Gruppen. "Theory of sets and topology, Volume in honour of Felix Hausdorff", p. 251-264. - Berlin, VEB Deutscher Verlag der Wissenschaften, 1972.

(Texte reçu le 4 décembre 1973)

Karl H. HOFMANN
Résidence de l'Ormaille
Pavillon 9
91440 BURES SUR YVETTE
