MICHEL LAZARD

Groupes analytiques en caractéristique 0

Séminaire N. Bourbaki, 1954, exp. nº 76, p. 255-262
<http://www.numdam.org/item?id=SB_1951-1954__2__255_0>

GROUPES ANALYTIQUES EN CARACTÉRISTIQUE 0

par Michel LAZARD

Un germe de groupe analytique à r paramètres (groupe local de Lie) est déterminé par la donnée de r séries de puissances à $2r$ variables qui doivent, en tant que séries formelles, vérifier certaines relations déduites de l'associativité du produit et de l'existence de l'élément neutre dans le germe. L'étude de ces conditions algébriques se fait commodément dans certaines structures algébriques que nous appelons "analyseurs", et qui généralisent les séries formelles. Après avoir démontré des résultats concernant les analyseurs sur le corps Q des nombres rationnels, on en fera une application aux théorèmes classiques de Lie.

1. Fonctions analytiques et analyseurs.

On peut considérer les séries formelles (à un nombre fini quelconque d'indéterminées, à coefficients dans R, et sans termes constants) comme des fonctions de plusieurs variables opérant sur l'ensemble des séries formelles sans termes constants $E \subset R[[\alpha]]$. Sur E, que nous considérons avec sa seule structure de Q-module topologique, est ainsi définie une famille de fonctions dites analytiques vérifiant les axiomes suivants

1° Pour tout entier positif n, l'ensemble des fonctions analytiques $f(x_1, \ldots, x_n)$ est un Q-module n-gradué complet, c'est-à-dire est la somme directe complète de sous-modules correspondant aux suites de n entiers $\geqslant 0$, $(\alpha_1, \ldots, \alpha_n)$. Ces sous-modules sont constitués par des fonctions homogènes de degré α_i en x_i, (pour $1 \leq i \leq n$), c'est-à-dire vérifiant

$$f(\lambda_1 x_1, \ldots, \lambda_n x_n) = \lambda_1^{\alpha_1} \ldots \lambda_n^{\alpha_n} f(x_1, \ldots, x_n),$$

pour tous $\lambda_i \in Q$.

Les fonctions analytiques sont continues sur E, et si une somme infinie de fohctions analytiques de $x_1, \ldots, x_n$ converge "formellement" (1), elle converge dans E au sens de la convergence simple.

---

(1) C'est-à-dire au sens de la topologie produit des topologies discrètes sur les composantes homogènes du Q-module n-gradué complet.

2° Une fonction analytique $f(x_1, \dots, x_n)$ dont toutes les composantes homogènes non nulles sont de degré 0 en x_i ne dépend pas de x_i. Les fonctions obtenues à partir de fonctions analytiques par suppression ou adjonction de variables inutiles sont encore analytiques.

3° Si $f(x_1, \dots, x_n)$ et $g_i(y_1, \dots, y_p)$ sont analytiques (pour $1 \leq i \leq n$), la fonction composée $f(g_1, \dots, g_n)$ est analytique. La fonction identique x est analytique.

Par définition ces trois axiomes caractérisent, sur un Q-module topologique quelconque E, une famille de fonctions analytiques. L'étude de certains problèmes montre qu'il est utile de considérer les propriétés d'une famille de fonctions analytiques sans faire intervenir le Q-module où elles opèrent (analogie avec le passage des groupes de permutation aux groupes "abstraits"). On parvient alors à une structure algébrique d'une certaine espèce, dite analyseur (sur le corps Q), où sont définis :

a. des Q-modules n-gradués complets (correspondant aux fonctions analytiques de n variables) ;

b. des isomorphismes de certains de ces modules dans d'autres, qui permettent d'établir des identifications (correspondant aux identifications de fonctions qui ne diffèrent que par des variables inutiles) ;

c. une opération algébrique, dite composition, (correspondant à la composition des fonctions). Les axiomes sont choisis pour que chaque analyseur admette une "représentation fidèle" comme famille de fonctions analytiques opérant sur un Q-module convenable. Le système complet de ces axiomes est fastidieux à énoncer (encore est-il notablement plus simple que dans le cas général où Q doit être remplacé par un anneau commutatif quelconque). C'est pourquoi on adoptera provisoirement un point de vue "naïf", en considérant qu'un analyseur est constitué par une famille de fonctions analytiques opérant sur un Q-module dont on ne précise pas la nature.

Soient, dans un analyseur, $f(x)$ et $g(x)$ 2 fonctions et $f(g(x))$ la fonction composée. Pour trouver les composantes homogènes de $f(g(x))$, on introduit d'abord les composantes homogènes de degré α_i en x_i de $f(x_1 + \dots + x_n)$. Les opérateurs linéaires qui font passer de $f(x)$ à ces fonctions "dérivées" sont dits opérateurs de Taylor-Sanov ; ils permettent d'écrire l'analogue de la formule de Taylor, c'est-à-dire la décomposition de $f(x_1 + \dots)$ en ses composantes homogènes. En substituant aux x_i les composantes homogènes de $g(x)$, on parvient, après regroupement des termes de même degré, à la décomposition de $f(g(x))$ en ses composantes homogènes. Si $f(x)$ est homogène de degré k, toutes les composantes homogènes non nulles de $f(x_1 + \ldots)$ ont le degré total k. Ces définitions et propriétés s'établissent de même pour les fonctions $f(x, y, \ldots)$ de plusieurs variables.

2. Lois de groupes dans les analyseurs sur le corps Q des rationnels.

On appellera "loi de groupe" dans un analyseur une fonction $f(x, y)$ vérifiant :

a. $f(x, 0 = f(0, x)) = x$.

b. $f(f(x, y), z) - f(x, f(y, z)) = 0$.

Si $\varphi(x)$ est une fonction inversible (au sens de la composition), $\varphi(f(\overset{-1}{\varphi}(x), \overset{-1}{\varphi}(y)))$ est encore une loi de groupe, dite transmutée de f par φ et notée $f^{(\varphi)}(x, y)$. On va se restreindre à la considération des $\varphi(x)$ de la forme $x + \ldots$ (termes de degré $\geqslant 2$), et montrer que les lois de groupe sont alors partagées en classes d'équivalence, dont chacune contient précisément une loi canonique.

LEMME 1. - ("formule du binôme). Soit $f(x, y)$ une fonction vérifiant l'axiome a. ci-dessus. On pose $x^{(o)} = 0$, et, par récurrence, $x^{(n+1)} = f(x^{(n)}, x)$. Alors $x^{(n)} = \sum_{1 \leq j \leq i < \infty} \binom{n}{j} C_{i,j}(x)$, où $C_{i,j}(x)$ est une fonction homogène de degré i en x, et $\binom{n}{j} = \frac{n(n-1)\ldots(n-j+1)}{j!}$.

DÉMONSTRATION. - On pose $x^{(n)} = \sum_{1 \leq i < \infty} B_i(x, n)$, où $B_i(x, n)$ est homogène de degré i en x. On suppose que $B_i(x, n)$ a la forme voulue pour $i \leq k$; les propriétés de l'analyseur permettent de calculer

$$B_{k+1}(x, n+1) - B_{k+1}(x, n),$$

et de conclure grâce à la relation connue :

$$\binom{n+1}{j+1} - \binom{n}{j+1} = \binom{n}{j}.$$

On peut alors développer $\binom{n}{j}$ suivant les puissances de n, ce qui permet d'écrire :

$$x^{(n)} = \sum_{1 \leq j \leq i < \infty} n^j D_{i,j}(x),$$

où $D_{i,j}(x)$ est homogène de degré i. En particulier : $D_{i,i}(x) = \frac{1}{i!} C_{i,i}(x)$ et $D_{i,1}(x) = \sum_{1 \leq j \leq i} \frac{(-1)^{j+1}}{j} C_{ij}(x)$.

LEMME 2. – ("exponentielle et logarithme par $(1+\frac{x}{n})^n$ "). On suppose données, pour tous les couples d'entiers i , j (où $1 \leq j \leq i < \infty$) des fonctions $H_{i,j}(x)$ telles que :

1° $H_{i,j}(x)$ soit homogène de degré i en x ;

2° si on pose $x^{(n)} = \sum_{1\leq j \leq i < \infty} n^j H_{i,j}(x)$, on ait $x^{(1)} = x$, et $(x^{(m)})^{(n)} = x^{(mn)}$ pour tous les couples d'entiers positifs m , n .

Alors en posant $\operatorname{Log} x = \sum_{1\leq i<\infty} H_{i,1}(x)$ et $\exp x = \sum_{1 \leq i < \infty} H_{i,j}(x)$, on a : $\operatorname{Log}(\exp x) = \exp(\operatorname{Log} x) = x$; $\operatorname{Log} x^{(n)} = n \operatorname{Log} x$; $(\exp x)^{(n)} = \exp(nx)$

DÉMONSTRATION. – On écrit :

$$\sum_{1 \leq j \leq i < \infty} n^j H_{i,j}\Big(\sum_{1\leq \ell \leq k<\infty} m^\ell H_{k,\ell}(x)\Big) = \sum_{1 \leq j \leq i < \infty} n^j m^j H_{i,j}(x) .$$

D'après les propriétés de l'analyseur, le membre de gauche est, a priori, de la forme $\sum_{1\leq \rho \leq \sigma \leq \tau} n^\rho m^\sigma L_{\rho,\sigma,\tau}(x)$, où $L_{\rho,\sigma,\tau}(x)$ est homogène de degré τ en x .

a. On considère les termes où $\rho = 1$. Conclusion : $\operatorname{Log} x^{(m)} = m \operatorname{Log} x$.

b. On considère les termes où $\rho = 1$ et $\sigma = \tau$. Conclusion : $\operatorname{Log}(\exp x) = x$.

c. On considère les termes où $\rho = \sigma$. Conclusion : $\exp(mn \operatorname{Log} x) = x^{(mn)}$.

Une loi de groupe $g(x , y)$ est dite <u>canonique</u> si les puissances correspondantes x^n sont données par la formule $x^n = n x$ $(n \geqslant 0)$. Les lemmes précédents montrent que la loi transmutée d'une loi de groupe $f(x , y)$ par la fonction $\operatorname{Log} x$ associée est canonique. On voit facilement que c'est la seule loi canonique parmi les transmutées de f par des fonctions de la forme $x + \ldots$ On suppose désormais que la loi de groupe $f(x , y)$ est canonique. On emploiera, comme dans un "vrai" groupe, la notation multiplicative : $xy = f(x , y)$, etc.

Considérons $h(x , y) = xyx^{-1}$. On a : $h(x , y^n) = (h(x , y))^n$, d'où (loi canonique) : $h(x , ny) = nh(x , y)$, ce qui établit que $h(x , y)$ est linéaire (i.e. homogène de degré 1) en y . Evidemment $h(0 , y) = h(y , y) = y$.

L'ensemble des fonctions $h(x , y)$ linéaires en y peut être muni d'une structure <u>d'algèbre graduée avec unité</u> : l'addition est la même que dans l'analyseur ; la multiplication est définie par la composition (le produit de $h(x , y)$ et $h'(x , y)$ est $h(x , h'(x , y))$; enfin le degré est le degré en x . On notera $h^{(n)}$ les puissances dans cette algèbre.

On définit alors, quand $h(0 , y) = 0$, e^h et $\operatorname{Log}(1 + h)$ par les séries respectives : $\sum_{0 \leq n < \infty} \frac{h^{(n)}}{n!}$ et $\sum_{1 \leq n < \infty} (-1)^{n+1} \frac{h^{(n)}}{n}$. Posons $[x , y] = \operatorname{Log} h(x , y)$, où $h(x , y) = xyx^{-1}$. Alors $h(nx , y) = h(x^n , y) = (h(x , y))^{(n)}$, et, en passant aux logarithmes, $[nx , y] = n [x , y]$, c'est-à-dire que le crochet $[x , y]$ est une fonction bilinéaire de x et y .

Un calcul facile montre que $f(x , y) = x + y + \frac{1}{2}[x , y] + \ldots$ (termes de degré $\geqslant 3$). Il en résulte que $[x , y]$ est un crochet de Lie. La démonstration de $[x , x] = 0$ est immédiate ; l'identité de Jacobi peut se démontrer au moyen de l'identité de Philip Hall, valable dans un groupe quelconque : $\prod((x , y) , z^y) = e$ (notation multiplicative dans le groupe ; de plus $\prod$ désigne le produit des 3 permutations circulaires successives de ce qui est écrit ;

$$(x , y) = xyx^{-1}y^{-1} \quad ; \quad x^y = yxy^{-1} \quad ;$$

e est l'élément neutre du groupe).

Soit $\mathfrak{B}$ le sous-analyseur de l'analyseur donné engendré par $[x , y]$: $\mathfrak{B}$ est constitué par les fonctions obtenues en additionnant, multipliant par des scalaires rationnels, et composant de toutes les manières les fonctions x et $[x , y]$. On conçoit comment $\mathfrak{B}$ est l'image homomorphe de l'"analyseur de Lie universel" sur Q , noté $\mathfrak{L}(Q)$, dont les fonctions s'identifient à des séries formelles de crochets de Lie itérés.

THÉORÈME. - La loi de groupe canonique $f(x , y)$ est dans $\mathfrak{B}$ et est l'image d'une loi de groupe déterminée dans $\mathfrak{L}(Q)$.

DÉMONSTRATION. - On groupe les termes de même degré total dans

$$f(x , y) = \sum_{1 \leq i < \infty} A_i(x,y) \;\; ; \; A_1(x , y) = x + y \in \mathfrak{B} .$$

On suppose démontré $A_i(x , y) \in \mathfrak{B}$, pour $1 \leqslant i \leqslant k-1$ (récurrence).

La définition de $[x , y]$ et de $\mathfrak{B}$ montre que $h(x , y) = xyx^{-1} \in \mathfrak{B}$ (pour rejoindre les notations classiques, il contient de poser

$[yx^0] = y$, $[yx^{n+1}] = [[yx^n] , x]$; alors $x^{-1}yx = \sum_{0 \leq i < \infty} \frac{1}{i!} [yx^i]$.) .

Considérons l'identité $(xy)^2 = x^2y^2y^{-1}(y^{-1}x^{-1}yx)y$. Calculons les composantes de degré total k dans les deux membres. On trouve, à gauche, $2\,A_k(x , y)$. A droite, on sait successivement calculer, en restant dans $\mathfrak{B}$, $y^{-1}x^{-1}y$; puis, jusqu'au terme de degré k inclus, $y^{-1}x^{-1}yx$; puis, toujours jusqu'au degré k inclus, $y^{-1}(y^{-1}x^{-1}yx)y$. Par ailleurs, $x^2y^2 = \sum_{1 \leq i < \infty} 2^i A_i(x , y)$, d'où enfin l'expression de la composante homogène de degré k du membre de droite sous la forme : $2^k A_k(x , y) + B_k(x , y)$ (avec $B_k \in \mathfrak{B}$). Il en résulte $A_k(x,y) = \frac{1}{2-2^k} B_k(x,y) \in \mathfrak{B}$.

Notons E l'algèbre associative libre à deux générateurs a et b sur Q . Nous la complétons en $\bar{E}$ (comme un anneau de polynomes pour passer aux séries formelles), et nous considérons dans $\bar{E}$ la loi de groupe analytique $x + y + xy$. Mise sous forme canonique, cette loi s'écrit : $\mathrm{Log}\,(e^x e^y)$, où e^x et $\mathrm{Log}\, x$ sont donnés par les séries de puissances habituelles. Le crochet précédemment défini est $[x , y] = xy - yx$. On obtient alors, comme conséquence de ce qui a été démontré, la formule de Campbell-Pascal-Baker-Poincaré-Hausdorff (...?), qui exprime $\mathrm{Log}(e^a e^b)$ comme un élément de la sous-algèbre de Lie complétée engendrée par a et b dans $\bar{E}$ (au moyen du crochet $xy - yx$). Mais a et b engendrent ainsi une algèbre de Lie <u>libre</u>. Par conséquent les $A_k(x , y)$ précédemment obtenus sont des "spécialisations" des termes homogènes de degré k dans la formule de Hausdorff, dont l'"universalité" se trouve ainsi établie.

Notre théorème est ainsi complètement démontré. L'un de ses effets est de ramener l'étude et la classification des lois de groupe dans un analyseur sur Q à celles des crochets de Lie dans cet analyseur. C'est le fondement algébrique de la théorie infinitésimale des groupes de Lie.

3. Les théorèmes locaux de Lie.

Considérons l'analyseur $S(r , R)$ (resp. $S(r , C)$) , où les arguments $X_1 , \dots , X_n$ d'une fonction $f(X_1 , \dots , X_n)$ s'identifient à des "vecteurs" $(X_i = (x_{ij})_{1 \leq j \leq r})$ tandis que $f(X_1 , \dots , X_n)$ s'identifie à un vecteur dont les r composantes sont des séries de puissances par rapport aux nr variables $x_{i,j}$ (séries sans termes constants et à coefficients dans R (resp. C)). La composition des fonctions et leurs degrés sont définis "formellement", comme s'il s'agissait de séries admettant un domaine de convergence.

Les représentations analytiques des germes de groupes de Lie à r paramètres réels (resp. complexes) correspondent biunivoquement à certaines lois de groupes dans $S(r , R)$ (resp. $S(r , C)$) : les séries correspondantes doivent posséder un domaine de convergence. Nous dirons qu'il s'agit de <u>lois convergentes.</u> Pour retrouver les théorèmes classiques à partir des résultats de la partie 2, nous démontrerons les théorèmes suivants :

A. La fonction $\exp x$ associée (comme au lemme 2) à une loi de groupe convergente admet un domaine de convergence ; la loi canonique associée est convergente.

B. Toutes les lois canoniques sont convergentes (troisième théorème de Lie).

1. Soit $f(x, y)$ une loi convergente : nous pouvons donc substituer à x et y les vecteurs de C^n suffisamment petits. Donnons-nous une norme $\|x\|$ sur C^n. Il existe alors deux constantes strictement positives a et b, telles que pour $\|x\|<a$ et $\|y\|<a$, on ait

$$\|f(x, y)\| < \|x\| + \|y\| + b\|x\|\,\|y\| .$$

Dans le domaine $D \subset C^n$ défini par $\|x\| < \frac{\operatorname{Log}(1+ab)}{b}$, $\left(\frac{x}{n}\right)^n$ est défini et $\left\|\left(\frac{x}{n}\right)^n\right\| < a$.

Alors les r composantes de $\left(\frac{x}{n}\right)^n$ sont uniformément bornées dans D. Puisqu'elles convergent ainsi que toutes leurs dérivées pour $x = 0$ (cf. lemme 1), elles convergent uniformément sur tout compact intérieur à D vers des fonctions analytiques. Donc la fonction $\exp x$ définie formellement au lemme 2 converge dans D, ce qui conduit au théorème A.

2. Nous appellerons "permutation en V" une permutation σ des n chiffres $1, \ldots, n$ telles que $\alpha < \beta \leq \sigma^{-1}(1) \Longrightarrow \sigma(\alpha) > \sigma(\beta)$ et

$$\sigma^{-1}(1) \leq \alpha < \beta \Rightarrow \sigma(\alpha) < \sigma(\beta) \quad \text{(cf. le graphe).}$$

$A_\sigma^{(n)}$ sera posé à $(-1)^{\sigma^{-1}(1)+1}$ pour toute permutation en V, σ. Dans une algèbre de Lie L où le crochet est noté $[x, y]$ convenons d'écrire :

$$[x_1] = x_1 \quad ; [x_1 \ldots x_{n-1}\, x_n] = [[x_1 \ldots x_{n-1}], x_n] .$$

LEMME. – $\sum_{\sigma \in V}$ désignant une sommation étendue aux permutations en V,

a. si $n \geqslant 1$, $[[x_1 \ldots x_n], [y_1 \ldots y_p]] = \sum_{\sigma \in V} A_\sigma^{(p)} [x_1 \ldots x_n\, y_{\sigma(1)} \ldots y_{\sigma(p)}]$;

b. $\sum_{\sigma \in V} A_\sigma^{(n)} [x_{\sigma(1)} \ldots x_{\sigma(n)}] = n\,[x_1 \ldots x_n]$;

c. si φ est une représentation linéaire de L dans une algèbre associative A (c'est-à-dire que $\varphi([x, y]) = \varphi(x)\varphi(y) - \varphi(y)\varphi(x)$),

$$\varphi([x_1, \ldots x_n]) = \sum_{\sigma \in V} A_\sigma^{(n)} \varphi(x_{\sigma(1)}) \ldots \varphi(x_{\sigma(n)}) .$$

Considérons :

A, algèbre associative libre de générateurs $x_1, \ldots x_n$ (sur Q) ;

L, algèbre de Lie de générateurs $y_1, \ldots, y_n$ (sur Q) ;

φ : $L \to A$, représentation linéaire de L dans A dédinie par $\varphi(y_i) = x_i$;
ψ : $A \to L$, application linéaire de A dans L définie par

$$\psi(x_{i_1} \ldots x_{i_h}) = \frac{1}{h}[y_{i_1} \ldots y_{i_h}] .$$

Il résulte immédiatement du lemme (a , b et c) que $\psi \circ \varphi = 1$ (identité) .

COROLLAIRES. -

1. φ est biunivoque. Autrement dit l'algèbre de Lie $M = \varphi(L)$ engendrée par les x_i dans A (au moyen du crochet $xy - yx$) est libre.
2. $\varphi \circ \psi$ est un projecteur de A sur M .

Soit maintenant $F(x , y) = \operatorname{Log} e^x e^y$ dans l'algèbre $\bar{A}$ complétée de A , algèbre libre de générateurs x et y .

$$F(x , y) = \sum \frac{(-1)^{k+1}}{k} \frac{1}{i_1 ! j_1 ! \ldots i_k ! j_k !} x^{i_1} y^{j_1} \ldots x^{i_k} y^{j_k} ,$$

la sommation étant étendue, pour tous les entiers $k \geqslant 1$, à toutes les suites de k couples d'entiers i_α et j_α , tels que $i_\alpha \geqslant 0$, $j_\alpha \geqslant 0$, $i_\alpha + j_\alpha \geqslant 1$.
On sait que $F(x , y)$ est dans l'algèbre de Lie complétée engendrée par x et y , c'est-à-dire est invariante par le projecteur $\varphi \circ \psi$. On peut appliquer terme à terme ce projecteur à la série précédente, ce qui donne :

$$F(x , y) = \sum \frac{(-1)^{k+1}}{k} \frac{1}{i_1 ! j_1 ! \ldots i_k ! j_k !} \frac{1}{i_1 + j_1 + \ldots + i_k + j_k} [x^{i_1} y^{j_1} \ldots x^{i_k} y^{j_k}] ,$$

avec la convention de sommation précédente. Sous cette forme, la série de Hausdorff se laisse facilement majorer terme à terme. On supposera qu'on l'applique dans une algèbre de Lie normée complète où la norme vérifie : $\|[x , y]\| \leq \|x\| . \|y\|$.
Alors la série $F(x , y)$ converge absolument si $\|x\| + \|y\| < \operatorname{Log} 2$. Le théorème B est ainsi démontré comme cas particulier.

BIBLIOGRAPHIE

[1] DYNKIN (E.B.). - Algèbres de Lie normées et groupes analytiques, Uspekhi mat. Nauk, N.S., t. 5 (35), 1950, p. 135-186 (en russe).

[2] LAZARD (Michel). - Sur les groupes analytiques dans les modules filtrés, C. R. Acad. Sc., t. 235, 1952, p. 1465-1467.

ADDITIF

Les résultats de cet exposé sont repris dans les chapitre I et II de

LAZARD (Michel). - Lois de groupes et analyseurs, Ann. scient. Ec. Norm. Sup., Série 3, t. 72, 1955, p. 299-400.

[Octobre 1957]