SÉMINAIRE N. BOURBAKI

MICHEL LAZARD

Lois de groupes et analyseurs

Séminaire N. Bourbaki, 1956, exp. n° 109, p. 77-91

<http://www.numdam.org/item?id=SB_1954-1956__3__77_0>

Séminaire BOURBAKI
(Février 1955)

LOIS DE GROUPES ET ANALYSEURS.

par Michel LAZARD.

1. Deux exemples de lois de groupes.

1° Formule de Hausdorff. Soient G un groupe de Lie, $\mathfrak{g}$ son algèbre de Lie. L'application $x \to \exp x$ définit un homéomorphisme d'un voisinage de zéro U dans $\mathfrak{g}$ sur un voisinage de l'élément neutre dans G. On peut prendre $V \subset U$, voisinage de zéro assez petit pour que, pour tous $x, y \in V$, il existe un seul $z \in U$ vérifiant $\exp z = \exp x \exp y$. L'élément z se calcule suivant une formule, dite de Hausdorff, qui est universelle en ce sens qu'elle ne dépend pas du choix de G. Plus précisément :

$$z = x + y + \frac{1}{2}[x, y] + \frac{1}{12}[[x, y], y] + \frac{1}{12}[[y, x], x] + \frac{1}{24}[[[y, x], x], y] + \cdots$$

Les points de suspension désignent des termes de degré total supérieur à 4.

2° Vecteurs de Witt (groupe additif). Un vecteur x sera une suite $(x_i)_{i \in N}$ d'éléments pris dans un anneau qu'on précisera. Si $(x_i) = x$ et $(y_i) = y$ sont donnés, on définit $(z_i) = z$ par les formules :

$$\sum_{r=0}^{i} p^r z_r^{p^{i-r}} = \left(\sum_{r=0}^{i} p^r x_r^{p^{i-r}}\right) + \left(\sum_{r=0}^{i} p^r y_r^{p^{i-r}}\right),$$

valables pour tout i, et, où p est un nombre premier donné. Les z_i sont des polynômes à coefficients entiers en les (x_i), (y_i), qu'on réduit modulo p, après quoi on pose $x + y = z$. Usage de cette formule : on prend tous les x_i, y_i, ..., dans un corps parfait $\bar{k}$ de caractéristique p. Alors les "vecteurs" s'identifient canoniquement aux entiers du corps valué complet non ramifié k dont $\bar{k}$ est le corps des restes, et $z = x + y$ s'identifie à la somme de x et y dans k.

2. Problème.

Etudier, d'un point de vue algébrique (c'est-à-dire avec des convergences triviales) les formules genre Hausdorff, Witt et d'autres qu'on appellera dorénavant lois de groupes. Une définition précise des lois de groupes sera donnée au n° 7. Retenons seulement qu'une loi de groupe est une formule universelle en un certain sens, permettant éventuellement de construire des groupes. Pour

l'instant la théorie en question n'a permis de construire aucun groupe par des lois de groupes nouvelles. On se console avec quelques théorèmes en attendant (?) des résultats désirables sur les p-groupes finis, par exemple.

On cherchera des lois de groupes dans des structures algébriques susceptibles d'en contenir comme éléments. Ces structures seront appelées analyseurs. Leur définition est pénible, et sera précédée de considérations longues et fastidieuses.

3. Quelques conventions.

Ω : anneau commutatif unitaire, E : Ω-module unitaire. Une application $E^n \to E$ s'appellera une fonction de n arguments dans E et sera notée $f(x_1, \dots, x_n)$. L'ensemble des fonctions de n arguments dans E est muni de sa structure usuelle de Ω-module. Un argument x_i de $f(x_1, \dots, x_n)$ sera dit neutre si $f(a_1, \dots, a_n) = f(b_1, \dots, b_n)$ dès que $a_j = b_j$ pour $i \neq j$. La manière dont on peut accroître ou éventuellement diminuer le nombre d'arguments d'une fonction par adjonction ou suppression d'arguments neutres est évidente (on laisse les arguments restants rangés dans le même ordre).

On dira qu'une fonction $f(x_1, \dots, x_n)$ vérifie la relation d'homogénéité de degré $(\alpha_1, \dots, \alpha_n) = \alpha (\alpha \in N^n)$, si, pour tous $\lambda_1, \dots, \lambda_n \in \Omega$, $f(\lambda_1 x_1, \dots, \lambda_n x_n) = \lambda_1^{\alpha_1} \dots \lambda_n^{\alpha_n} f(x_1, \dots, x_n)$. Si l'un des degrés partiels, soit α_i , est nul, l'argument x_i devra être neutre.

4. Familles de fonctions polynomiales dans un Ω-module E .

Un ensemble $\mathfrak{P}$ de fonctions dans E s'appellera une famille de fonctions polynomiales si les axiomes suivants sont vérifiés :

(FP1) Le sous-ensemble $\mathfrak{P}^n \subset \mathfrak{P}$ constitué par les fonctions de n arguments est un Ω-module pour tout $n \geqslant 1$. De plus $\mathfrak{P}^n$ est la somme directe de sous-Ω-modules $\mathfrak{P}^n_\alpha$ $(\alpha \in N^n)$, et les fonctions de $\mathfrak{P}^n_\alpha$ vérifient la relation d'homogénéité de degré α .

On pourra donc parler des composantes homogènes d'une fonction, du degré total, etc. Toute $f \in \mathfrak{P}$ est somme finie de ses composantes homogènes.

(FP2) Si $f(x_1, \dots, x_m) \in \mathfrak{P}^m$ et si $g_i(y_1, \dots, y_n) \in \mathfrak{P}^n$ $(1 \leqslant i \leqslant m)$, la fonction composée $f(g_1, \dots, g_m)$ est dans $\mathfrak{P}^n$.

(FP3) Toute fonction obtenu à partir d'une fonction $f \in \mathfrak{P}$ par adjonction ou suppression d'arguments neutres appartient à $\mathfrak{P}$. L'adjonction ou la suppression

d'arguments neutres à une fonction homogène ne modifie pas les degrés par rapport aux arguments restants.

(FP4) La fonction identique x_1 (abus de langage pour parler de la bijection canonique de E sur lui-même) appartient à $\mathfrak{P}^1$. Elle est homogène de degré 1.

(FP5) Toute $f \in \mathfrak{P}$ dont tous les arguments sont neutres est nulle. Autrement dit, pas de fonction constante $\neq 0$ dans $\mathfrak{P}$.

Les 3 axiomes suivants sont des conséquences des 5 premiers, si Ω est un corps infini (on remarquera que (FP3) et (FP4) impliquent : $x_1 + \ldots + x_n \in \mathfrak{P}^n$)

(FP6) Soient $f \in \mathfrak{P}^m$ et $g_i \in \mathfrak{P}^n$ comme dans l'énoncé de (FP2). Si f est homogène de degré $\alpha = (\alpha_i)$ et les g_i homogènes de degrés respectifs $\beta_i = (\beta_{i,j})$ $(1 \leqslant i \leqslant m \ ; \ 1 \leqslant j \leqslant n)$, alors $f(g_1, \ldots, g_m)$ est homogène de degré $\gamma = (\gamma_j)$, avec $\gamma_j = \sum_i \alpha_i \beta_{i,j}$.

(FP7) Soit $f(x_1, \ldots, x_m) \in \mathfrak{P}^m$, homogène de degré q $(\in N)$ par rapport à x_1. Alors $f(y_1 + \ldots + y_n, x_2, \ldots, x_m) \in \mathfrak{P}^{m+n-1}$ est homogène de degré total q par rapport aux arguments $y_1, \ldots, y_n$.

(FP8) Soit $f(x_1, \ldots, x_m) \in \mathfrak{P}^m$ homogène de degré q en x_1. Désignons par $g(y_1, y_2, x_2, \ldots, x_m) \in \mathfrak{P}^{m+1}$ la composante homogène de degré $(r, q-r)$ en (y_1, y_2) de $f(y_1 + y_2, x_2, \ldots, x_m)$. Alors

$$g(x_1, x_1, x_2, \ldots, x_m) = \binom{q}{r} f(x_1, x_2, \ldots, x_m) .$$

(Cf. identité d'Euler pour les fonctions homogènes).

EXEMPLE. – Ω est un corps infini, E une Ω-algèbre associative et commutative, $\mathfrak{P}$ est l'ensemble des fonctions polynômes sans terme constant.

5. Homomorphismes de familles de fonctions polynomiales.

La notion d'homomorphisme qu'on introduit a pour but de nous débarrasser du module E, qui est seulement là pour faciliter l'axiomatique.

Soient : E, E' deux Ω-modules, $\mathfrak{P}$ et $\mathfrak{P}'$ deux familles de fonctions polynomiales dans E et E' respectivement. Un homomorphisme φ de $\mathfrak{P}$ dans $\mathfrak{P}'$ est une application de $\mathfrak{P}$ dans $\mathfrak{P}'$ telle que, pour tout n, la restriction de φ à $\mathfrak{P}^n$ soit une application Ω-linéaire de $\mathfrak{P}^n$ dans $\mathfrak{P}'^n$ respectant les degrés : $\varphi(\mathfrak{P}^n_\alpha) \subset \mathfrak{P}'^n_\alpha$. De plus φ devra faire correspondre les fonctions identiques dans E et E' (FP4). Enfin il faudra écrire des diagrammes

commutatifs pour exprimer que φ est compatible :

1° Avec la composition des fonctions :

$$(\varphi f)(\varphi g_1 , \dots , \varphi g_n) = \varphi(f(g_1 , \dots , g_n)) \ ;$$

2° Avec les adjonctions d'arguments neutres (c'est-à-dire certaines injections des $\mathfrak{P}^{\alpha}_n$ (resp. $\mathfrak{P}'^{n}_{\alpha}$) les uns dans les autres).

Un isomorphisme de $\mathfrak{P}$ sur $\mathfrak{P}'$ est un homomorphisme bijectif.

La définition des homomorphismes ne fait pas intervenir les modules E et E' . On dira qu'une application Ω-linéaire ψ de E dans E' est compatible avec l'homomorphisme φ de $\mathfrak{P}$ dans $\mathfrak{P}'$ si $\psi(f(a_1 , \dots , a_n)) = (\varphi f)(\psi a_1 , \dots , \psi a_n)$ pour tous $a_1 , \dots , a_n \in E$, $f \in \mathfrak{P}^n$. Autrement dit, φ se déduit de ψ par passage aux quotients (si ψ est injective). En général, on ne peut pas trouver de ψ .

Nous dirons que le module E est $\mathfrak{P}$-libre, avec la famille de générateurs $\mathfrak{P}$-indépendants $(a_\iota)_{\iota \in I}$ si :

1° Tout élément de E peut s'écrire $f(a_{\iota_1} , \dots , a_{\iota_n})$, avec $f \in \mathfrak{P}$; $\iota_1 , \dots , \iota_n \in I$;

2° Pour tout homomorphisme φ de $\mathfrak{P}$ dans une famille de fonctions polynomiales $\mathfrak{P}'$ dans un Ω-module E' , et toute famille $(a'_\iota)_{\iota \in I}$ d'éléments de E' , il existe une application (nécessairement unique) ψ de E dans E' , compatible avec φ et vérifiant $\psi(a_\iota) = a'_\iota$ pour tout $\iota \in I$.

6. Analyseurs.

Un analyseur incomplet est une famille de fonctions polynomiales $\mathfrak{P}$ dans un Ω-module E , considérée à un isomorphisme canonique près. Autrement dit, on laisse tomber E , et on conserve $\mathfrak{P}$ (famille de Ω-modules), avec la structure algébrique qui y a été définie et qui se laisse exprimer indépendamment de E .

Cette définition, un peu abusive, remplace une définition directe encore plus pénible, semble-t-il. Elle est rendue acceptable par le résultat suivant : si $\mathfrak{P}$ est une famille de fonctions polynomiales dans un Ω-module E , et I un ensemble d'indices infini, il existe une famille de fonctions polynomiales $\mathfrak{P}'$ isomorphe à $\mathfrak{P}$ définie dans un Ω-module E' qui est $\mathfrak{P}'$-libre avec la famille de générateurs $\mathfrak{P}'$-indépendants $(a_\iota)_{\iota \in I}$. Il est évident (fonctoriellement) que $\mathfrak{P}'$ et E' sont définis à un isomorphisme canonique près, ce qui fait reposer la définition sur une base solide.

Scholie. Dans le cas des Ω-algèbres associatives et commutatives, on distingue les fonctions polynômes dans une algèbre donnée, et les anneaux de polynômes $\Omega[(x_\nu)]$ (algèbres libres). On se place ici à un troisième point de vue, et l'on envisage les fonctions polynômes dans toutes les algèbres. En somme, on étudie le "calcul" dans l'espèce de structure algébrique envisagée.

L'intérêt de ce point de vue est qu'il permet d'énoncer des résultats valables pour des espèces de structures algébriques assez diverses (cf. par exemple HAUSDORFF et WITT au n° 1).

Complétion d'un analyseur incomplet. On généralise la complétion d'un anneau de polynômes en un anneau de séries formelles. Si on part d'un analyseur incomplet défini par une famille de fonctions polynomiales $\mathfrak{P}$ on définit l'analyseur (complet) $\mathfrak{A}$ associé comme la famille de modules $\mathfrak{A}^n$, où $\mathfrak{A}^n$ est la somme directe complète (ou produit direct) de $(\mathfrak{P}^n_\alpha)_{\alpha \in \mathbb{N}^n}$ (qu'on notera désormais $\mathfrak{A}^n_\alpha$). Si on suppose $\mathfrak{P}$ réalisé dans le Ω-module $\mathfrak{P}$-libre E, on peut compléter E en $\hat{E}$, ce qui permet d'identifier les éléments de $\mathfrak{A}$ à des fonctions (qu'on pourrait appeler analytiques) dans $\hat{E}$. Ces fonctions sont égales à la somme infinie (convergente au sens de la topologie de $\hat{E}$) de leurs composantes homogènes. Connaissant $\mathfrak{A}$, on retrouve l'analyseur incomplet correspondant en se restreignant aux fonctions qui n'ont qu'un nombre fini de composantes homogènes non nulles.

La considération des analyseurs (complets) est nécessaire pour étudier les lois de groupes.

7. Définition des lois de groupes.

Soit $\mathfrak{A}$ un analyseur. Si f, $g \in \mathfrak{A}$, on écrira $f \equiv g \pmod{\deg q}$ pour indiquer que les composantes homogènes non nulles de $f - g$ ont un degré total $\geqslant q$.

Une loi de groupe dans $\mathfrak{A}$ est un élément $f(x, y) \in \mathfrak{A}^2$ vérifiant :

$$(1) \qquad \begin{cases} f(x, y) \equiv x + y \pmod{\deg 2} \\ f(x, y, z) = f(f(x, y), z) - f(x, f(y, z)) = 0 . \end{cases}$$

Ces relations impliquent :

$$(2) \qquad f(x, 0) = f(0, x) = x ,$$

et l'existence de $g(x) \in \mathfrak{A}^1$, uniquement déterminé par :

$$(3) \qquad f(x, g(x)) = f(g(x), x) = 0 .$$

8. Opérations sur les analyseurs.

1° Adjonction d'une constante. - Soit $\mathcal{A}$ un analyseur. On considère les $f \in \mathcal{A}^{n+1}$ $(n \geqslant 1)$ qu'on écrit $f(a , x_1 , \dots , x_n)$ telles qu'aucune composante homogène de f ne soit de degré total 0 par rapport aux x_i. On convient de considérer a comme une "constante", et f comme une fonction des seuls arguments $x_1 , \dots , x_n$. On obtient ainsi le module $\mathcal{A}(a)^n$ des fonctions de n arguments dans un analyseur $\mathcal{A}(a)$.

2° Puissances cartésiennes. - Soit $\mathcal{A}$ un analyseur, q un entier > 0. On définit l'analyseur $\Pi^q \mathcal{A}$, qui lorsque $\mathcal{A}$ opère sur le module $\hat{E}$, opère sur la puissance cartésienne $\hat{E}^q$. Une fonction $F(X_1 , \dots , X_n)$ de $(\Pi^q \mathcal{A})^n$ s'identifie à une famille de q fonctions $f_i \in \mathcal{A}^{nq}$:

$$F(X_1 , \dots , X_n) = (f_i(x_{1,1} , \dots , x_{1,q} ; \dots ; \dots x_{n,q}))_{1 \leqslant i \leqslant q} .$$

Définition analogue de $\Pi^{(I)} \mathcal{A}$ si I est un ensemble infini quelconque. Exemple : si $\mathcal{A}$ est l'analyseur des séries formelles usuelles à coefficients dans F_p (corps premier), la loi de groupe des vecteurs de Witt est un élément de la puissance cartésienne dénombrable $\Pi^{(N)} \mathcal{A}$.

3° Produit tensoriel. - Si $\mathcal{A}$ est un analyseur sur Ω, Ω' une Ω-algèbre commutative unitaire, $\Omega : \otimes \mathcal{A}$ est un analyseur sur Ω', tel que $(\Omega' \otimes \mathcal{A})^n_\alpha = \Omega' \otimes \mathcal{A}^n_\alpha$.

9. Cohomologie d'un analyseur. Définitions.

On définit l'opérateur Ω-linéaire $\delta : \mathcal{A}^n \to \mathcal{A}^{n+1}$, pour tout n, par :

$$(4)\quad \delta f(x_1 , \dots , x_{n+1}) = f(x_2 , \dots , x_{n+1}) + \sum_{i=1}^{n} (-1)^i f(x_1, \dots, x_i + x_{i+1}, \dots, x_{n+1}) + (-1)^{n+1} f(x_1 , \dots , x_n) .$$

On a la bonne relation $\delta\delta = 0$, qui permet de définir, suivant un schéma suffisamment connu, cocycles, etc...

On notera $\mathcal{A}^n_q \subset \mathcal{A}^n$ le module des fonctions de n arguments de degré total q. Alors $\delta \mathcal{A}^n_q \subset \mathcal{A}^{n+1}_q$. Le groupe de cohomologie $H(\mathcal{A})$ est bigradué. On notera $H^n_q(\mathcal{A})$ le groupe $H(\mathcal{A}^n_q)$.

10. Cohomologie et lois de groupes. Prolongement des bourgeons et des transmutations.

Soit $f(x , y) \in \mathcal{A}^2$. Nous disons que f détermine un q-bourgeon si :

$$(5)\qquad \begin{cases} f(x\ ,\ y) \equiv x + y \pmod{\deg 2} \\ \Gamma f(x\ ,\ y\ ,\ z) = f(f(x\ ,\ y)\ ,z) - f(x\ ,\ f(y\ ,\ z)) \pmod{\deg (q+1)}. \end{cases}$$

La condition (5) est une forme affaiblie de la condition (1). Le q-bourgeon déterminé par f est constitué par l'ensemble des $f' \in \mathcal{A}^2$ telles que $f \equiv f' \pmod{\deg (q+1)}$. On peut supposer, en particulier, que f a toutes ses composantes homogènes de degré total $\geqslant (q+1)$ nulles.

Si f détermine un q-bourgeon, soit $\Gamma_{q+1}(x\ ,\ y\ ,\ z)$ la composante homogène de degré total $(q+1)$ de f. On démontre que $\Gamma_{q+1}(x\ ,\ y\ ,\ z)$ est un <u>cocycle</u> ($\Gamma_{q+1}(x\ ,\ y\ ,\ z) \in Z^3_{q+1}(\mathcal{A})$). Posons $f'(x\ ,\ y) = f(x\ ,\ y) + h(x\ ,\ y)$, où $h \in \mathcal{A}^2_{q+1}$. Alors $\Gamma_{q+1} f'(x\ ,\ y\ ,\ z) = \Gamma_{q+1} f(x\ ,\ y\ ,\ z) - \delta h(x\ ,\ y\ ,\ z)$. Ainsi, pour les f qui déterminent un q-bourgeon, les $\Gamma_{q+1} f$ parcourent une classe de cohomologie ($\in H^3_{q+1}(\mathcal{A})$) qu'on appellera l'<u>obstruction</u> du q-bourgeon. On définit d'une manière naturelle le prolongement d'un q-bourgeon en un $(q+r)$-bourgeon, ou en une loi de groupe.

PROPOSITION 1. - Pour qu'un q-bourgeon soit prolongeable en un $(q+1)$-bourgeon, il faut et il suffit que son obstruction soit nulle.

Nous appellerons <u>groupe adjoint</u> de $\mathcal{A}$ et noterons $G(\mathcal{A})$ l'ensemble des $\varphi(x) \in \mathcal{A}^1$ telles qu'existe $\varphi^{-1}(x)$ avec $\varphi(\varphi^{-1}(x)) = \varphi^{-1}(\varphi(x)) = x$; $G(\mathcal{A})$ est bien un groupe par rapport à la composition. Les sous-groupes invariants $G_i(\mathcal{A})$ de $G(\mathcal{A})$ sont définis par :

(6) $\varphi(x) \in G_i(\mathcal{A}) \Longleftrightarrow \varphi(x) \in \mathcal{A}^1$ et $\varphi(x) \equiv x \pmod{\deg (i+1)}$,

pour tout i entier $\geqslant 1$.

Si $f(x\ ,\ y) \in \mathcal{A}^2$, on appelle <u>transmutée</u> de f par φ et on note f^φ la fonction $\varphi(f(\varphi^{-1}(x)\ ,\ \varphi^{-1}(y)))$. Avec ces conventions, $G(\mathcal{A})$ <u>opère</u> (à gauche) sur l'ensemble des lois de groupes dans $\mathcal{A}$.

Si $f(x\ ,\ y) \equiv x + y \pmod{\deg 2}$ et $\varphi(x) \equiv x + h(x) \pmod{\deg (q+1)}$, $h \in \mathcal{A}^1_q$, $q \geqslant 2$, alors $f^\varphi(x\ ,\ y) \equiv f(x\ ,\ y) - \delta h(x\ ,\ y) \pmod{\deg (q+1)}$.

Deux problèmes se posent naturellement : construire les lois de groupes dans un analyseur $\mathcal{A}$ en déterminant successivement leurs composantes homogènes (par rapport au degré total) ; puis les classer suivant les relations d'équivalence (transitivité) correspondant aux groupes $G(\mathcal{A})$ et $G_1(\mathcal{A})$. Le premier problème

conduit à des obstructions dans $H^3(\mathcal{A})$, le deuxième problème à des obstructions dans $H^2(\mathcal{A})$.

On cherche donc à construire $f(x , y) = x + y + \sum_{i=2}^{\infty} h_i(x , y)$, f loi de groupe, $h_i \in \mathcal{A}_i^2$. Si $h_2 , \dots , h_{q-1}$ sont construits, $x + y + \sum_{i=2}^{q-1} h_i(x , y)$ doit être un $(q - 1)$-bourgeon. Pour qu'on puisse trouver un h_q , il faut que l'obstruction du $(q - 1)$-bourgeon soit nulle. S'il en est ainsi, deux h_q qui diffèrent par un cobord donnent naissance à des q-bourgeons transmutés l'un en autre par un élément de $G_q(\mathcal{A})$. Enoncés analogues pour la construction de $\varphi(x) \in G(\mathcal{A})$ tel que $f^{\varphi} = f'$, où f et f' sont deux lois de groupes. La grande difficulté est de comprendre comment, en supposant nulle une obstruction, le choix effectué lors du prolongement influe sur la nullité des obstructions suivantes.

11. Le complexe normalisé.

Soit $\mathcal{A}$ un analyseur. Nous noterons $\hat{\mathcal{A}}^n$ le sous-module de $\mathcal{A}^n$ constitué par les fonctions dont toutes les composantes homogènes ont au moins le degré 1 par rapport à chacun de leurs arguments ; $\hat{\mathcal{A}} = \bigcup_{n=1}^{\infty} \hat{\mathcal{A}}^n$.

On démontre que $S\hat{\mathcal{A}}^n \subset \hat{\mathcal{A}}^{n+1}$ et qu'il existe un projecteur d'homotopie de $\mathcal{A}$ sur $\hat{\mathcal{A}}$. En effet, soit $f \in \mathcal{A}^n$; pour que $f \in \hat{\mathcal{A}}^n$, il faut et il suffit que f s'annule dès qu'on remplace par 0 l'un de ses arguments. Il n'y a plus qu'à copier EILENBERG-MACLANE ([1] , p. 62). On pose $\hat{\mathcal{A}}_q^n = \hat{\mathcal{A}}^n \cap \mathcal{A}_q^n$. Alors $H_q^n(\mathcal{A}) = H(\hat{\mathcal{A}}_q^n)$.

THÉORÈME 1. - Pour tout analyseur $\mathcal{A}$, $H_q^n(\mathcal{A}) = (0)$ si $n > q$. En effet $\hat{\mathcal{A}}_q^n = (0)$ les arguments étant trop nombreux pour se partager le degré total.

12. Opérations du groupe symétrique $\mathfrak{S}_n$ sur $\mathcal{A}^n$. Les groupes H_n^n .

Si $f(x_1 , \dots , x_n) \in \mathcal{A}^n$, $\sigma \in \mathfrak{S}_n$ on pose

$$\sigma.f(x_1 , \dots , x_n) = f(x_{\sigma(1)} , \dots , x_{\sigma(n)}) \quad \text{(permutation des arguments)}$$

Ainsi $\mathfrak{S}_n$ opère à gauche sur $\mathcal{A}^n$, $\hat{\mathcal{A}}^n$, $\mathcal{A}_q^n$. On dira que $f \in \mathcal{A}^n$ est antisymétrique si $\sigma f = \varepsilon_\sigma f$ pour tout $\sigma \in \mathfrak{S}_n$ (ε_σ : signature de σ). On note α l'opérateur d'antisymétrisation $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_\sigma \sigma$ et on appelle antisymétrisée de f la fonction αf .

Pour étudier H_n^n, on considère $H_n^n(\hat{\mathcal{A}})$. Les fonctions de $\hat{\mathcal{A}}_n^n$ sont **multilinéaires.** Ce sont **toutes des cocycles, et on démontre :**

THÉORÈME 2. - Dans $\hat{\mathcal{A}}_n^n$, l'antisymétrisé de tout cobord est nul. Pour tout $f \in \hat{\mathcal{A}}_n^n$, $(n! - \alpha)f$ est un cobord.

Si on note $\mathcal{G}^n$ le sous-module des fonctions antisymétriques de $\hat{\mathcal{A}}_n^n$, on a un homomorphisme canonique φ de $\mathcal{G}^n$ dans $H_n^n(\mathcal{A})$, tel que le noyau et le conoyau de φ soient des groupes de torsion où l'ordre de chaque élément divise $n!$

Application. Pour que $f(x , y) = x + y + h(x , y)$ $(h \in \mathcal{A}_2^2)$ soit un 2-bourgeon, il faut et il suffit que h soit bilinéaire $(h \in \mathcal{A}_2^2)$. Alors

$$\Gamma f(x , y , z) = h(h(x , y) , z) - h(x , h(y , z)) .$$

Pour que f soit prolongeable en un 3-bourgeon, il faut que l'antisymétrisé de Γf soit nul. Posons $h(x , y) - h(y , x) = [x , y]$. Alors l'antisymétrisé de Γf s'écrit :

$$[[x , y] , z] + [[y , z] , x] + [[z , x] , y] .$$

Autrement dit : $[x , y]$ doit être un crochet de Lie.

13. Les groupes H_q^n pour $q > n$.

Convenons d'appeler groupe abélien de V_n-torsion un groupe abélien de torsion sans p-composantes pour p (premier) $> n$.

Nous noterons Q_n l'anneau des rationnels qui, écrits comme fractions irréductibles, n'ont au dénominateur que des facteurs premiers $\leq n$.

THÉORÈME 3. - Pour tout analyseur $\mathcal{A}$, $H_q^n(\mathcal{A})$ est un groupe de V_q-torsion si $q > n$.

DÉMONSTRATION. - Par récurrence sur q. On veut démontrer $H_q^n(\mathcal{A}) \otimes_{\mathbb{Z}} Q_q = (0)$ pour $q > n$. Les foncteurs H (homologie) et $\otimes_{\mathbb{Z}} Q_q$ commutent. On se ramène ainsi à démontrer que $H_q^n(Q_q \otimes_{\mathbb{Z}} \mathcal{A}) = (0)$. Supposons donc que l'anneau de base Ω de $\mathcal{A}$ est Q_q.

Considérons $\hat{\mathcal{A}}_q$, que nous appellerons A. Désignons par $A^{p,n}$ le module des $f \in \mathcal{A}_q^n$ dont toutes les composantes homogènes ont un degré $\leq p$ par rapport à x_1 (premier argument) ; $A^p = \bigcup_{n=1}^{\infty} A^{p,n}$. Comme $\delta A^p \subset A^p$, $A^0 = (0)$, $A^q = A$, on peut appliquer la suite spectrale. Les notations sont celles de SERRE ([3] ,

p. 428) en ce qui concerne les E_r^p. Mais, dans $E_r^{p,n}$, p désigne le degré filtrant et n le degré "nombre d'arguments". On a les différentielles d_r :

$$d_r : E_r^{p,n} \to E_r^{p-r,n+1} .$$

Le terme $E_o^{p,n} = A^{p,n}/A^{p-1,n}$ s'identifie canoniquement au module des $f \in A$ qui sont homogènes de degré p en x_1. La différentielle d_o, nulle sur $E_o^{p,1}$, est, pour $n \geqslant 2$ au signe près, celle qu'on obtient en considérant x, comme une constante, et en appliquant δ aux (n - 1) arguments suivants (cf. n° 8, 1). D'après le théorème 1 et l'hypothèse de réccurence, on en déduit, pour $n \geqslant 2$:

$$E_1^{p,n} \simeq H(E_o^{p,n}) = (0) ,$$

sauf éventuellement si $n + p = q + 1$. Il en résulte, par de simples considérations de degré pour les d_r, que $E_\infty^{p,n} = E_2^{p,n}$, pour tous p, n (démonstration directe, et facile, de $E_2^{q,1} = (0)$ si $q > 1$). Il reste à démontrer que $E_2^{q-n+1,n} = (0)$ pour $n < q$.

Le groupe $E_1^{q-n+1,n}$ s'identifie aux fonctions de $\hat{A}_q^n$ qui sont multilinéaires antisymétriques par rapport aux (n - 1) derniers arguments (théorème 2). On peut encore, par le procédé classique de multilinéarisation (ou polarisation), qui est applicable parce que A_q est un Q_q-module, l'identifier aux fonctions de $\hat{A}_q^q$ qui sont symétriques par rapport aux (q - n + 1) premiers arguments, et antisymétriques par rapport aux (n - 1) derniers arguments.

Une troisième identification de $E_1^{q-n+1,n}$ d'apparence bizarre, nous permettra de traduire commodément la différentielle d_1. Si $f(x_1, \ldots, x_q)$ est symétrique en $(x_1, \ldots, x_{q-n+1})$ et antisymétrique en $(x_{q-n+2}, \ldots, x_q)$, nous l'identifions à la cochaîne alternée $\tilde{f}$ à valeurs dans $\hat{A}_q^q$ définie sur le (n - 2)-squelette d'un simplexe $S = (a_1, \ldots, a_q)$ de dimension (q - 1) : $\tilde{f} \in C^{n-2}(S, \hat{A}_q^q)$ est définie par

$$\tilde{f}((a_{\sigma(q-n+2)}, \ldots, a_{\sigma(q)})) = \sigma f \text{ pour tout } \sigma \in \mathfrak{S}_q .$$

On vérifie que cette définition a un sens ; alors E_1^{q-n+1} s'identifie au sous-groupe de $C^{n-2}(S, A_q^q)$ fermé par les cochaînes équivariantes (par rapport aux opérateurs de $\mathfrak{S}_q$) et la différentielle d_1 s'identifie, au facteur $\frac{q-n+1}{n}$ près, à la restriction du cobord usuel appliquant $C^{n-2}(S, \hat{A}_q^q)$ dans $C^{n-1}(S, A_q^q)$ si $n < q$. Il est bien connu que tout cocycle équivariant est cobord

d'une cochaîne équivariante (faire la moyenne par rapport aux opérateurs de $\mathfrak{S}_q$). Ainsi $E_2^{q-n+1,n} = (0)$ si $n < q$,

C.Q.F.D.

REMARQUES. - 1° La dernière partie de la démonstration n'est qu'une traduction "géométrique" d'une propriété de l'algèbre du groupe symétrique $Z(\mathfrak{S}_q)$.

2° En poussant un peu la démonstration, on pourrait majorer, en fonction de n et q , les ordres des éléments de $H_q^n(\mathcal{A})$, pour un analyseur quelconque $\mathcal{A}$.

14. Application des théorèmes généraux. Les analyseurs rationnels.

Nous appellerons analyseur rationnel un analyseur $\mathcal{A}$ tel que $\mathcal{A}_n$ soit un Q_n-module pour tout $n \geqslant 1$. Autrement dit, il est possible de diviser univoquement par $n!$ les fonctions de degré total n . En particulier tout analyseur dont l'anneau de base est un corps de caractéristique 0 est rationnel.

D'après les théorèmes 1 , 2 , 3 : si $\mathcal{A}$ est un analyseur rationnel, $H_q^n(\mathcal{A}) = (0)$ pour $n \neq q$, et $H_n^n(\mathcal{A})$ s'identifie au module des fonctions n-linéaires antisymétriques.

Conséquences (cf. n° 10) :

1° Tout q-bourgeon est prolongeable en une loi de groupe si $q \geqslant 3$. Pour que $x + y + h(x , y)$, où h est bilinéaire, soit prolongeable en une loi de groupe, il faut et il suffit que $h(x , y) - h(y , x)$ soit un crochet de Lie.

2° Si f et g sont deux lois de groupes, $\varphi \in G(\mathcal{A})$ tel que $f^{\varphi} \equiv g \pmod{\deg 3}$, il existe $\varphi' \in G(\mathcal{A})$, avec $\varphi' \equiv \varphi \pmod{\deg 3}$ et $f^{\varphi'} = g$.

La loi de Hausdorff. Obtenue en prolongeant le 2-bourgeon $x + y + \frac{1}{2}[x , y]$ dans l'analyseur rationnel correspondant aux algèbres de Lie. Le prolongement est possible et unique. En effet, le choix de la composante de degré total n est déterminé à un cocycle près : comme $H_q^2 = (0)$ pour $q > 2$, ce cocycle est un cobord d'un élément de $\mathcal{A}_q^1$; mais $\mathcal{A}_q^1 = (0)$ pour $q > 1$ (le crochet est alterné), donc le cobord est nul.

La loi de Hausdorff $f(x , y)$, et ses images homomorphes, peuvent être caractérisées par $f(px , qx) = (p + q)x$ pour tout couple d'entiers p et q .

Les lois unilinéaires. Nous dirons que la loi de groupe $f(x , y)$ est unilinéaire à gauche si toute les composantes homogènes de $f(x , y) - y$ sont de degré 1 en x . Etudions dans quel cas un analyseur peut contenir une loi de groupe $f(x , y)$ unilinéaire à gauche. Soit $h(x , y) = x \circ y$ la composante bilinéaire de f .

En écrivant que $(x \circ y) \circ z - x \circ (y \circ z)$ est le cobord d'une fonction linéaire en x, nous trouvons la condition :

(6) $\qquad (x \circ y) \circ z - x \circ (y \circ z) - (x \circ z) \circ y + x \circ (z \circ y) = 0$.

Les algèbres (non associatives, en général) où la multiplication (notée $x \circ y$) vérifie l'identité (6) seront appelées algèbres de composition à gauche.

EXEMPLE. - On prend une algèbre associative, commutative et à dérivation (par exemple $\Omega[a]$ avec $D = \frac{d}{da}$), et on pose $x \circ y = Dx.y$.

Aux algèbres de composition à gauche correspond un analyseur rationnel $\mathfrak{A}$ bien déterminé. Dans $\mathfrak{A}$ existe une loi de groupe unilinéaire à gauche $\Phi(x, y)$, entièrement déterminée comme prolongement du 2-bourgeon $x + y + x \circ y$. Si l'on a un analyseur rationnel $\mathfrak{B}$, et une loi unilinéaire à gauche f dans $\mathfrak{B}$, il existe un homomorphisme (cf. n° 5) et un seul de $\mathfrak{A}$ dans $\mathfrak{B}$ appliquant Φ sur f .

Définition analogue pour les lois unilinéaires à droite. On trouve ainsi deux lois de groupes, aussi uniques et universelles dans leur genre que la loi de Hausdorff, mais apparemment nouvelles.

Conséquence : pour écrire la formule de Taylor usuelle pour des polynômes : $P(x + Q(x)) = \sum_{n=0}^{\infty} \frac{D^n P(x)}{n!} [Q(x)]^n$, il suffit de savoir calculer le produit d'un polynôme par la dérivée d'un autre (on pose $P \circ Q = DP.Q$, et on a $D^2 P.Q^2 = (P \circ Q) \circ Q - P \circ (Q \circ Q)$, etc.) .

Problèmes. Etudier les lois unilinéaires quand l'anneau de base de l'analyseur est un corps de caractéristique $p \neq 0$. Quels sont les germes de groupes de Lie obtenus à partir des algèbres de composition de dimension finie sur les corps R ou C ? Les lois unilinéaires conduisent-elles alors (comme dans le cas de Hausdorff) à des séries convergentes ?

15. Quelques résultats sur les lois de groupes de Lie formels.

Les théorèmes 1 , 2 , 3 constituent des résultats généraux, valables pour tous les analyseurs. Il doit exister des théorèmes généraux, permettant de relier la cohomologie d'une puissance cartésienne $\Pi^n \mathfrak{A}$ à celle de $\mathfrak{A}$. Malheureusement, je ne possède que des résultats très partiels, concernant seulement les groupes H^1 et H^2 .

La partie "fine" de la théorie, dont on ne connait encore presque rien, concerne l'étude d'analyseurs particuliers, où les groupes H_q^n ne sont pas tous triviaux pour $n < q$.

Voici des résultats concernant <u>l'analyseur classique</u> $\mathcal{A}$ (séries formelles usuelles) <u>sur l'anneau</u> Z des entiers.

$$H_q^1(\mathcal{A}) = \begin{cases} Z & \text{si } q = 1 \\ (0) & \text{si } q > 1 \end{cases}$$

$$H_q^2 = \begin{cases} (0) & \text{si } q \text{ n'est pas une puissance d'un nombre premiers,} \\ & \text{ou si } q = 1 . \\ F_p & \text{si } q = p^h , \ p \text{ premier, } h \text{ entier } > 0 . \end{cases}$$

$H_q^3 = F_{p_1} + \ldots + F_{p_r}$, où $p_1 , \ldots , p_r$ sont tous les nombres premiers tels que q soit somme de 2 puissaces distinctes de chacun d'eux (exemple $q = 10$, $p_1 = 2$, $p_2 = 3$).

Sur ces calculs repose la démonstration de quelques théorèmes concernant les lois de groupes de Lie formels (lois de groupe dans une puissance cartésienne de $\Omega \otimes_{\mathbb{Z}} \mathcal{A}$, où Ω est l'anneau des coefficients). Une loi $f(x , y)$ est abélienne si $f(x , y) = f(y , x)$; définition analogue pour les bourgeons abéliens.

Si l'anneau des coefficients Ω est <u>sans éléments nilpotents</u>, toute loi à <u>un paramètre</u> (c'est-à-dire dans $\Omega \otimes \mathcal{A}$) est <u>abélienne</u> (se démontre sans cohomologie, avec utilisation de l'ordre lexicographique pour les composantes homogènes). Un bourgeon n'est alors prolongeable en une loi de groupe que s'il est abélien, mais il peut exister des bourgeons non abéliens.

Dans le cas général $(\Pi^{(I)}\Omega \otimes \mathcal{A})$, <u>tout bourgeon abélien est prolongeable en une loi de groupe</u>.

Bornons-nous au cas où le nombre des paramètres est fini pour énoncer le théorème de la <u>loi de groupe de Lie formel abélienne universelle à</u> n <u>paramètres</u> : il existe <u>un anneau de polynômes à coefficients entiers</u> Ω et une loi <u>abélienne</u> $F(x , y)$ dans $\Pi^n \Omega \otimes \mathcal{A}$ telle que, <u>pour tout anneau</u> Ω', <u>toute loi de groupe abélienne dans</u> $\Pi^n \Omega' \otimes \mathcal{A}$ <u>soit obtenue à partir de</u> F <u>par un homomorphisme et un seul de</u> Ω <u>dans</u> Ω' (plus précisément par l'homomorphisme de $\Pi^n \Omega \otimes \mathcal{A}$ dans $\Pi^n \Omega' \otimes \mathcal{A}$ canoniquement associé). De plus, pour tout entier q , $F(x , y)$ <u>détermine un</u> q-<u>bourgeon abélien universel</u> à n paramètres (dont <u>tout</u> q-bourgeon abélien de loi de groupe de Lie formel est une image homomorphe).

Ce théorème revient à dire que la variété algébrique définie par les coefficients des séries formelles (resp. polynômes) d'une loi de groupe (resp. bourgeon) de Lie formel à n paramètres est un espace affine de dimension infinie (resp. finie).

Résultat analogue, à une petite modification près, pour les lois à une infinité de paramètres.

Application. On comprend le "mystère" des vecteurs de Witt, car toute loi abélienne de groupe de Lie formel à coefficients dans F_p se remonte en une loi à coefficients dans Z qui, considérée comme loi à coefficients dans Q, se laisse transmuter en $x + y$.

Les lois abéliennes à 1 paramètre et à coefficients dans un corps de caractéristique $p \neq 0$ algébriquement clos se laissent classer : il existe une infinité dénombrable de classes inéquivalentes. Le problème du prolongement des transmutations se laisse assez bien étudier : on rencontre un problème d'obstruction "retardée", autrement dit, en supposant nulle la k-ième obstruction, le choix effectué alors dans la construction de la transmutation de la loi de groupe f en g, détermine la nullité de la $(k + h)$-ième obstruction, où h ne dépend pas de k (c'est la "hauteur" de la loi f). On obtient aussi quelques renseignements sur les stabilisateurs des lois considérées (groupe de φ tels que $f\varphi = f$).

Il faudra chercher à généraliser, dans la mesure du possible, ces résultats aux lois de groupes de Lie formels abéliennes à n paramètres. D'après DIEUDONNÉ, qui a étudié la question par une autre méthode, le problème de classification de ces lois se ramène à un problème de classification pour certains modules de type fini.

16. Problèmes ouverts.

Ils sont nombreux. Outre la question de la cohomologie des puissances cartésiennes, il faudrait aborder l'étude des extensions d'un analyseur (avec la définition naturelle des sous-analyseurs, etc.). Peut-on ainsi "tuer" les obstructions gênantes ? Si l'analyseur (incomplet) opère sur un module E, quelles conditions devraient vérifier E pour qu'on puisse y faire opérer l'analyseur-extension, qui tue l'obstruction (outre une condition évidente concernant la cohomologie du groupe abélien E opérant trivialement sur lui-même) ?

Quel critère suffisamment simple peut-on donner pour qu'un q-bourgeon de groupe de Lie formel à n paramètres à coefficients dans un corps de caractéristique

$p \neq 0$ soit prolongeable en une loi de groupe ? Quels résultats sérieux pourrait-on énoncer sur les lois de groupes de Lie formels non abéliennes ?

Quelles lois de groupes se rapprochent le plus de la loi de Hausdorff quand l'anneau de base est un corps de caractéristique $p \neq 0$?

Ce dernier problème paraît très lié à celui des groupes d'exposant p (groupes où tout élément $\neq 1$ est d'ordre p). D'une façon générale, on peut espèrer construire des groupes nilpotents (cf. HAUSDORFF pour les groupes de Lie nilpotents simplement connexes), parce qu'ils se laissent parfois bien "étaler" sur des modules.

Je signale enfin loyalement que pour fabriquer des p-groupes avec les lois de groupes, la définition donnée ici de ces dernières n'est ni la plus générale, ni peut-être la meilleure (cf. la thèse de KALOUJNINE [2]).

BIBLIOGRAPHIE

[1] EILENBERG (S.) and MACLANE (S.). - Cohomology theory in abstract groups. I , Annals of Math., Series 2, t. 48, 1947, p. 51-78.

[2] KALOUJNINE (Leo). - La structure des p-groupes de Sylow des groupes symétriques finis et quelques généralisations infinies de ces groupes, Ann. scient. Ec. Norm. Sup., Série 3, t. 65, p. 239-276 (Thèse Sc. math. Paris. 1948).

[3] SERRE (Jean-Pierre). - Homologie singulière des espaces fibrés, Annals of Math., Series 2, t. 54, 1951, p. 425-505.

ADDITIF

Les résultats de cet exposé sont repris dans les chapitres I, III et IV de :

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

[Octobre 1957]