French Spring 16

Algebra

SOUS-GROUPES D'INDICE FINI DANS $SL(n, Z)$

PAR H. BASS, M. LAZARD ET J-P. SERRE

Communicated by Deane Montgomery, November 18, 1963

1. **Enoncé du théorème et schéma de démonstration.** Soit n un entier $\geqq 2$, et soit $G(n) = SL(n, Z)$. Si q est un entier $\geqq 1$, nous noterons $G_q(n)$ le noyau de l'homomorphisme canonique

$$SL(n, Z) \to SL(n, Z/qZ).$$

Un sous-groupe de $G(n)$ est appelé un *sous-groupe de congruence* s'il contient l'un des $G_q(n)$. Un tel sous-groupe est évidemment d'indice fini dans $G(n)$. Réciproquement:

THÉORÈME 1. *Si $n \geqq 3$, tout sous-groupe d'indice fini de* $\boldsymbol{SL}(n, \boldsymbol{Z})$ *est un groupe de congruence.*[1]

(Pour $n=2$, il est bien connu que l'énoncé analogue est *faux*.)

Soit $\hat{G}(n)$ (resp. $A(n)$) le complété de $G(n)$ pour la topologie des sous-groupes d'indice fini (resp. des sous-groupes de congruence). Les groupes $\hat{G}(n)$ et $A(n)$ sont des groupes *profinis*, cf. [4]. On notera que, d'après le théorème d'approximation dans le groupe SL_n, le groupe $A(n)$ s'identifie au produit des groupes $SL(n, Z_p)$, pour tous les nombres premiers p (on note $\boldsymbol{Z}_p$ l'anneau des entiers p-adiques). Il est clair que $A(n)$ s'identifie au quotient de $\hat{G}(n)$ par un sous-groupe distingué fermé $C(n)$. La suite exacte correspondante:

$$1 \to C(n) \to \hat{G}(n) \to A(n) \to 1$$

sera notée (X_n). *Le Théorème* 1 *équivaut à dire que* $C(n) = 1$ *pour* $n \geqq 3$.

L'étude des groupes $C(n)$ utilise la méthode de "suspension" de [1]. De façon précise, soit $S: G(n) \to G(n+1)$ l'homomorphisme défini par la formule:

$$S(x) = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}, \qquad x \in G(n).$$

Cet homomorphisme se prolonge par continuité en un homomorphisme (encore noté S) de la suite exacte (X_n) dans la suite exacte (X_{n+1}); en particulier, $S: C(n) \to C(n+1)$ est bien défini.

[1] (Note ajoutée le 27 novembre 1963.) Nous apprenons que le théorème 1 a été également démontré par J. Mennicke; sa démonstration doit paraître dans les Ann. of Math.

Les trois propriétés suivantes seront démontrées dans les n^{os} 2 et 3:

(1) *Pour* $n \geqq 3$, *l'homomorphisme* S: $C(n-1) \rightarrow C(n)$ *est surjectif.*

(2) *Pour* $n \geqq 3$, $C(n)$ *est contenu dans le centre de* $\hat{G}(n)$.

(3) *On a* $H^1(A(2), \boldsymbol{Q}/\boldsymbol{Z}) = \boldsymbol{Z}/12\boldsymbol{Z}$ *et* $H^2(A(2), \boldsymbol{Q}/\boldsymbol{Z}) = 0$. (Il s'agit ici de cohomologie des groupes profinis, cf. [4, Chap. I]; de plus, le groupe $A(2)$ opère trivialement sur le groupe de coefficients $\boldsymbol{Q}/\boldsymbol{Z}$.)

Montrons comment ces propriétés entraînent le Théorème 1:

La suite spectrale des extensions de groupes, appliquée à (X_2) et au groupe de coefficients $I = \boldsymbol{Q}/\boldsymbol{Z}$, donne la suite exacte:

$$0 \rightarrow H^1(A(2), I) \rightarrow H^1(\hat{G}(2), I) \rightarrow H^1(C(2), I)^{A(2)} \rightarrow H^2(A(2), I).$$

D'après (3), on a $H^1(A(2), I) = \boldsymbol{Z}/12\boldsymbol{Z}$. D'autre part, le groupe $H^1(\hat{G}(2), I)$ s'identifie à $\operatorname{Hom}(G(2), I)$, qui est aussi cyclique d'ordre 12 (cela se voit, par exemple, sur la présentation standard de $G(2)$ au moyen de deux générateurs x, y liés par les relations $x^4 = 1$, $x^2 = y^3$). Il suit de là que $H^1(A(2), I) \rightarrow H^1(\hat{G}(2), I)$ est bijectif. La suite exacte écrite plus haut, jointe à la propriété (3), montre alors que $H^1(C(2), I)^{A(2)} = 0$. Mais ce groupe est dual du quotient $C(2)/D(2)$, où $D(2)$ désigne l'adhérence du groupe de commutateurs $(\hat{G}(2), C(2))$. Ainsi, $(\hat{G}(2), C(2))$ est dense dans $C(2)$. La propriété (1), appliquée au cas $n = 3$, montre alors que $(S(\hat{G}(2)), C(3))$ est dense dans $C(3)$; d'après la propriété (2), on a donc $C(3) = 1$, d'où $C(n) = 1$ pour tout $n \geqq 3$ d'après la propriété (1).

2. **Démonstration des propriétés (1) et (2).** Soit R un anneau commutatif, et soit M un R-module. Un élément $x \in M$ est dit *unimodulaire* s'il existe une forme linéaire f sur M telle que $f(x) = 1$.

LEMME 1. *Soit* $x = (x_1, \cdots, x_m)$ *un élément unimodulaire de* R^m. *Si l'anneau* R *est semi-local, il existe une famille* $(y_2, \cdots, y_m)$ *d'éléments de* R *telle que* $x_1 + y_2x_2 + \cdots + y_mx_m$ *soit inversible dans* R.

Quitte à diviser par le radical de R, on peut supposer que R est semi-simple; dans ce cas, c'est un composé direct de corps commutatifs, et le lemme est immédiat.

Rappelons d'autre part qu'une matrice carrée $s \in \boldsymbol{M}_n(\boldsymbol{Z})$ est dite *élémentaire* si elle est de la forme $s = 1 + aE_{ij}$, avec $i \neq j$, $a \in \boldsymbol{Z}$. Du fait que $\boldsymbol{Z}$ est un anneau *euclidien*, le groupe engendré par les matrices élémentaires est égal à $SL(n, \boldsymbol{Z}) = G(n)$. Pour tout entier $q \geqq 1$, nous noterons $E_q(n)$ le *sous-groupe distingué* de $G(n)$ engendré par les matrices élémentaires appartenant à $G_q(n)$, autrement dit de la forme $1 + aE_{ij}$, avec $i \neq j$, $a \in q\boldsymbol{Z}$.

LEMME 2. *Soient* $x = (x_1, \cdots, x_n)$ *et* $x' = (x_1', \cdots, x_n')$ *deux élé-*

ments de $\boldsymbol{Z}^n$. *Soit* I *une partie de* $[1, n]$ *telle que* $x_i = x_i'$ *pour* $i \in I$, *et soit* $\mathfrak{a}$ *l'idéal de* $\boldsymbol{Z}$ *engendré par les* x_i, $i \in I$. *Supposons que l'on ait*

$$x_j' \equiv x_j \text{ mod. } q\mathfrak{a} \qquad \textit{pour tout } j \notin I.$$

Il existe alors $s \in E_q(n)$ *qui transforme* x *en* x'.

Par hypothèse, on a $x_j' = x_j + \sum_{i \in I} q t_{ij} x_i$, avec $t_{ij} \in \boldsymbol{Z}$. On prend alors pour s le produit des matrices $1 + q t_{ij} E_{ji}$, pour tous les couples (i, j) tels que $i \in I$, $j \notin I$.

PROPOSITION 1. *Supposons* $n \geqq 3$, *et* $q \geqq 1$. *Soient* $a = (a_1, \cdots, a_n)$ *et* $a' = (a_1', \cdots, a_n')$ *deux éléments unimodulaires de* $\boldsymbol{Z}^n$ *tels que* $a \equiv a'$ mod. q. *Il existe alors* $s \in E_q(n)$ *qui transforme* a *en* a'.

Il est clair que le groupe $E_1(n) = G(n)$ opère transitivement sur l'ensemble des éléments unimodulaires de $\boldsymbol{Z}^n$. On peut donc supposer que a' est égal au vecteur coordonnée $e_1 = (1, 0, \cdots, 0)$ et que $q > 1$. Posons $a_1 = 1 - r$, avec $r \in q\boldsymbol{Z}$. L'image de $(a_2, ra_3, \cdots, ra_n)$ dans le $(\boldsymbol{Z}/a_1\boldsymbol{Z})$-module $(\boldsymbol{Z}/a_1\boldsymbol{Z})^{n-1}$ est unimodulaire. Comme $\boldsymbol{Z}/a_1\boldsymbol{Z}$ est semi-local, le Lemme 1 montre qu'il existe des entiers $t_3, \cdots, t_n$ tels que l'élément $b = a_2 + \sum_{i \geq 3} t_i r a_i$ soit inversible mod. a_1. En appliquant le Lemme 2 avec $I = [3, n]$, on voit qu'il existe $s_1 \in E_q(n)$ tel que $s_1(a)$ soit égal à l'élément $c' = (a_1, b, a_3, \cdots, a_n)$. Comme a_1 et b sont premiers entre eux, le Lemme 2 (appliqué avec $I = [1, 2]$ cette fois) montre qu'il existe $s_2 \in E_q(n)$ transformant c' en $a'' = (a_1, b, r, 0, \cdots, 0)$. Soit maintenant θ l'élément de $SL(n, \boldsymbol{Z})$ qui laisse fixes les vecteurs coordonnées e_i $(i \neq 3)$ et transforme e_3 en $e_3 + e_1$. On a $\theta e_1 = e_1$, et $\theta a'' = (1, b, r, 0, \cdots, 0)$. Le Lemme 2, appliqué avec $I = \{1\}$, montre qu'il existe $s_3 \in E_q(n)$ transformant $\theta a''$ en e_1. L'élément $\theta^{-1} s_3 \theta \cdot s_2 s_1$ transforme alors a en e_1, ce qui achève de démontrer la proposition.

COROLLAIRE 1. *Pour* $n \geqq 3$, $G_q(n) = E_q(n) \cdot G_q(n-1)$.

(On convient d'identifier $G(n-1)$ à un sous-groupe de $G(n)$ au moyen de l'homomorphisme de suspension S.)

Soit $t \in G_q(n)$. On peut appliquer la Proposition 1 aux éléments $e_n = (0, \cdots, 0, 1)$ et $t(e_n)$ de $\boldsymbol{Z}^n$; il existe donc $s \in E_q(n)$ tel que $st(e_n) = e_n$. La matrice de st est de la forme

$$\begin{pmatrix} A & 0 \\ x & 1 \end{pmatrix},$$

avec $A \in G_q(n-1)$ et $x \in q\boldsymbol{Z}^{n-1}$. Soit $y = -xA^{-1}$; en multipliant à gauche

$$\begin{pmatrix} A & 0 \\ x & 1 \end{pmatrix} \quad \text{par} \quad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

on obtient

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

qui appartient à $G_q(n-1)$. Comme on a évidemment

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \in E_q(n),$$

cela montre bien que t appartient à $E_q(n)\cdot G_q(n-1)$.

COROLLAIRE 2. *Pour* $n \geqq 3$, *on a* $(G(n), G_q(n)) \subset E_q(n)$.

Il suffit de prouver que, si $s \in G_q(n)$, et si t est élémentaire, le commutateur $(s, t) = s^{-1}t^{-1}st$ appartient à $E_q(n)$. Après conjugaison, on peut supposer t de la forme

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

avec $x \in \boldsymbol{Z}^{n-1}$; le Corollaire 1 montre qu'on peut d'autre part supposer s de la forme

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

avec $A \in G_q(n-1)$. On a alors:

$$(s, t) = \begin{pmatrix} 1 & 0 \\ x(1-A) & 1 \end{pmatrix},$$

et il est immédiat que cet élément appartient à $E_q(n)$.

COROLLAIRE 3. *Pour* $n \geqq 3$, *les sous-groupes* $E_q(n)$ *sont d'indice fini dans* $G(n)$.

On utilise le lemme suivant, qui est bien connu:

LEMME 3. *Soit* $1 \to H \to G \to \pi \to 1$ *une suite exacte de groupes. Si* π *et* $G/(G, G)$ *sont finis,* $G/(G, H)$ *l'est aussi.*

(Rappelons la démonstration: il suffit de prouver que $H/(G, H)$ est fini; cela résulte de la suite exacte:

$$H_2(\pi, \boldsymbol{Z}) \to H/(G, H) \to G/(G, G),$$

et du fait que $H_2(\pi, \boldsymbol{Z})$ est fini.)

En appliquant ce lemme au groupe $G = G(n)$, et au sous-groupe distingué $H = G_q(n)$, on voit que $(G(n), G_q(n))$ est d'indice fini dans $G(n)$, et il en est donc de même de $E_q(n)$, d'après le Corollaire 2.

Démonstration des propriétés (1) *et* (2) *du n°*1. Soit $n \geqq 3$. Soit H un sous-groupe d'indice fini de $G(n)$; il existe un sous-groupe distingué H' d'indice fini dans $G(n)$ qui est contenu dans H (par exemple l'intersection des conjugués de H). Si $q = (G: H')$, on a $E_q(n) \subset H'$, puisque $E_q(n)$ est engendré par des puissances q ièmes. Ce résultat, joint au Corollaire 3 ci-dessus, montre que les $E_q(n)$ sont *cofinaux* parmi les sous-groupes d'indice fini de $G(n)$. Cela nous permet d'écrire:

$$\hat{G}(n) = \text{lim. proj. } G(n)/E_q(n), \qquad A(n) = \text{lim. proj. } G(n)/G_q(n),$$

d'où:

$$C(n) = \text{lim. proj. } G_q(n)/E_q(n).$$

Les propriétés (1) et (2) sont alors conséquences immédiates des Corollaires 1 et 2, respectivement.

3. **Cohomologie des groupes $SL(2, Z_p)$.** Posons, pour simplifier les notations:

$$G_p = SL(2, Z_p), \qquad I = Q/Z, \qquad I_p = Q_p/Z_p.$$

Le groupe $A(2)$ est produit des groupes G_p. On en conclut facilement que la propriété (3) du n°1 est conséquence de la proposition plus précise suivante:

PROPOSITION 2. (a) *On a* $H^1(G_2, I) = Z/4Z$, $H^1(G_3, I) = Z/3Z$ *et* $H^1(G_p, I) = 0$ *pour* $p \geqq 5$.

(b) *On a* $H^2(G_p, I) = 0$ *pour tout* p.

Soit V le groupe des commutateurs de G_p. C'est un sous-groupe ouvert de G_p. L'assertion (a) équivaut à dire que G_p/V est isomorphe à $Z/4Z$ pour $p = 2$, $Z/3Z$ pour $p = 3$, et est trivial pour $p \geqq 5$, ce qui se vérifie sans difficultés.

Pour prouver (b), il suffit de voir que $H^2(G_p, I_l) = 0$ pour tout nombre premier l. Or, si $l \neq p$, les l-groupes de Sylow de G_p sont isomorphes à ceux de $SL(2, F_p)$, et sont cycliques finis (ou quaternioniens si $l = 2$); leur deuxième groupe de cohomologie à valeurs dans I_l est donc nul, et l'on a *a fortiori* $H^2(G_p, I_l) = 0$. *Reste donc à prouver que* $H^2(G_p, I_p) = 0$.

LEMME 4. *On a* $H^1(V, I_p) = 0$.

La suite spectrale des extensions de groupes donne la suite exacte:

$$0 \to H^1(G_p/V, I_p) \to H^1(G_p, I_p) \to H^0(G_p/V, H^1(V, I_p)) \to H^2(G_p/V, I_p).$$

Analysis

Séminaire BOURBAKI
18e année, 1965/66, n° 310

Juin 1966

SOMMES PARTIELLES DES SERIES DE FOURIER

d'après L. CARLESON

par Jean-Pierre KAHANE

Histoire du problème

A toute fonction $f \in L^1(-\pi,\pi)$ on associe sa série de Fourier

$$\sum_{-\infty}^{\infty} \hat{f}_n e^{inx} \quad . \tag{1}$$

Les "sommes partielles" de (1) sont les

$$S_n(x,f) = \sum_{-n}^{n} \hat{f}_m\, e^{imx} \quad . \tag{2}$$

f étant donnée, est-il vrai que $S_n(x,f)$ tende vers $f(x)$ en tout point x, resp. en presque tout point x, resp. en un point x au moins ?

Ce problème avait déjà été posé par Fourier. Pour en mesurer la difficulté, voici d'abord quelques résultats négatifs.

1. Il existe une f continue dont la série de Fourier diverge en un point (du Bois Reymond 1876 ; exemple classique, Fejer 1911)

2. Il existe une f sommable dont la série de Fourier diverge presque partout (Kolmogoroff 1923).

3. Il existe une f sommable dont la série de Fourier diverge partout (Kolmogoroff 1926).

4. Etant donné un ensemble E de mesure nulle, il existe une f continue dont la série de Fourier diverge sur E (Kahane-Katznelson 1965).

Aucun de ces exemples n'exclut l'hypothèse que, pour $p > 1$, toute $f \in L^p$ ait sa série de Fourier convergente presque partout. Pour $p = 2$, c'était là l'hypothèse de Lusin.

En fait, le comportement presque partout des sommes partielles (2) lorsque $f \in L^p$ a été l'objet d'études sérieuses. En 1965, les meilleurs résultats connus étaient les suivants :

1. Si $f \in L^1$, $S_n(x,f) = o(\log n)$ p.p. (Hardy)

2. Si $f \in L^2$, $S_n(x,f) = o(\sqrt{\log n})$ p.p. (Kolmogoroff-Seliverstoff 1925, Plessner 1926).

3. Si $f \in L^p$, $S_n(x,f) = o((\log n)^{1/p})$ p.p. (Littlewood-Paley 1931).

La cohérence de ces résultats et la grande difficulté du dernier avaient fait penser aux spécialistes qu'ils étaient vraisemblablement les meilleurs possibles. D'où un scepticisme, justifié jusqu'il y a quelques mois, à l'égard des démonstrations proposées de l'hypothèse de Lusin.

Là s'inscrivent les résultats de Carleson :

1. Si $f(\log^+|f|)^{1+\delta} \in L^1$ $(\delta > 0)$, $S_n(x,f) = o(\log\log n)$ p.p.

2. Si $f \in L^p$ $(p > 1)$, $S_n(x,f) = o(\log\log\log n)$ p.p.

3. Si $f \in L^2$, $S_n(x,f)$ est convergente p.p.

Quoique le manuscrit de Carleson soit assez court (37 pages), les démonstrations sont ardues ; on se bornera ici à donner une idée assez complète de celle du premier résultat, et très partielle de celle du dernier. Les estimations en o résultent très facilement d'estimations en O, et la convergence d'une estimation en $O(1)$; il s'agira donc d'obtenir pour $S_n(x,f)$ des estimations en O hors d'un ensemble de mesure petite.

Le dernier résultat de Carleson est définitif : pour chaque $p \geq 2$, les ensembles de divergence des $f \in L^p$ sont exactement les ensembles de mesure nulle ; il en est de même pour les fonctions continues. Les principaux problèmes qui restent sont les suivants :

1. Est-il vrai que pour toute $f \in L^1$ on ait $S_n(x,f) = o(\log\log n)$ p.p. ?

2. Est-il vrai que pour toute $f \in L^p$ $(p > 1)$ la série de Fourier converge p.p. ?

La méthode de Carleson

Au lieu d'étudier les sommes partielles (2), on peut étudier

$$\sum_{n}^{\infty} \hat{f}_m \, e^{imx}$$

ou aussi bien la transformée de Hilbert de $f(x)e^{-inx}$. Pour simplifier, on suppose f réelle, ce qui permet de prendre $n > 0$. On prolonge f par périodicité et on pose

$$(3) \qquad s(x,n) = \int_{-2n}^{2n} \frac{f(t)\, e^{-int}}{x - t}\, dt \qquad (x \in [-\pi,\pi]).$$

Si $s(x,n) = O(w_n)$, on a aussi $S_n(x,f) = O(w_n)$.

Plus généralement, pour un sous-intervalle ω^{**} de $[-2\pi,2\pi]$, on pose

$$(4) \qquad s(x,n,\omega^{**}) = \int_{\omega^{**}} \frac{f(t)e^{-int}}{x - t}\, dt \; .$$

Dans la suite, la longueur de ω^{**} sera de la forme

$$|\omega^{**}| = 4\pi . 2^{-j}$$

Si $n|\omega^{**}|$ est multiple de 2π, c'est-à-dire n multiple de 2^{j-1}, on dit que n est adapté à ω^{**}.

Lorsque x est plus près du milieu de ω^{**} que des extrémités on dit que x est strictement intérieur à ω^{**}, ou que ω^{**} entoure x. Dans ce cas, (4) est majoré par la transformée de Hilbert maximale de $f(t)e^{-int}$, convenablement définie. Cette dernière remarque ne sera utilisée que pour $n = 0$, et tous nos efforts vont tendre à nous ramener, par étapes, à ce cas.

On commence par se donner un entier N, et on se restreint aux $n \in [2^{N-1}, 2^N]$. On définit (et c'est très laborieux) un ensemble exceptionnel $X \subset [-\pi,\pi]$. Pour $x \notin X$, on définit une suite finie de couples (n_j, ω_j^{**}) de sorte que

1°) $n_o = n$, $\omega_o^{**} = \;]-2\pi, 2\pi[$

2°) $\omega_j^{**} \subset \omega_{j-1}^{**}$, et ω_j^{**} entoure x $(j = 1,2,\ldots)$

3°) n_j soit adapté à ω_j^{**} $(j = 1,2,\ldots)$

4°) le dernier des n_j soit nul, soit $n_\nu = 0$.

Pour majorer $s(x,n)$, on écrit

$$(5)\qquad \left\{\begin{array}{l} s(x,n_j,\omega_j^{**}) = s(x,n_j,\omega_{j+1}^{**}) + R_j(x) \\ e^{in_jx}\, s(x,n_j,\omega_{j+1}^{**}) = e^{in_{j+1}x}\, s(x,n_{j+1},\omega_{j+1}^{**}) + S_j(x) \end{array}\right.$$

et par conséquent

$$(6)\qquad |s(x,n)| \leq \sum_{j=0}^{\nu-1} (|R_j(x)|+|S_j(x)|) + |s\,(x,0,\omega_\nu^{**})|$$

On s'efforce simultanément de rendre la mesure de X petite et le second membre de (6) pas trop grand.

Ce schéma vaut pour les trois théorèmes de Carleson. C'est la définition de X qui change d'un cas à l'autre. On va donner la construction de X dans le premier cas (en se restreignant, pour simplifier, à $f \in L^p$, $p > 1$) et obtenir l'estimation en $O(\log\log n)$. Puis on indiquera les idées nouvelles qui permettent de conclure dans le cas $f \in L^2$.

<u>Les principaux lemmes</u>.

<u>Lemme</u> 1. Soit $f \in L^1(\omega^{**})$, x un point strictement intérieur à ω^{**}. En désignant génériquement par σ un sous-intervalle de ω^{**} qui entoure x, la mesure de l'ensemble des $x \in \omega^{**}$ tels que

$$(7)\qquad \sup_\sigma \left|\int_\sigma \frac{f(t)}{x-t}\,dt\right| > \lambda_1$$

tend vers zéro quand $\lambda_1 \to \infty$.

Classique (Zygmund I, p. 279).

Lemme **2.** Soit $E \in L^{\infty}(\omega^{**})$ **, et** σ **comme ci-dessus. La mesure** de l'ensemble T des $x \in \omega^{**}$ tels que

$$(8) \qquad \sup_{\sigma} \left| \int_{\omega^{**} \setminus \sigma} \frac{E(t)}{x-t}\, dt \right| > \lambda \| E \|_{\infty}$$

satisfait à

$$(9) \qquad \operatorname{mes} T \leqq C\, e^{-c\lambda}\, |\omega^{**}|$$

(C désigne une constante absolue grande, et c une constante absolue petite ; on pourra éventuellement les modifier, d'une formule à l'autre, pour que toutes les inégalités déjà écrites soient valables).

C'est un théorème du type maximal de Hardy-Littlewood (Zygmund I, p. 155).

Lemme 3. Soit Ω un partage de ω^{**} en sous-intervalles ω_{κ} . Soit t_{κ} le milieu de ω_{κ} , et

$$(10) \qquad \Delta(x) = \sum \frac{|\omega_{\kappa}|^2}{(x-t_{\kappa})^2 + |\omega_{\kappa}|^2} \qquad x \in \omega^{**} .$$

Le mesure de l'ensemble V des $x \in \omega^{**}$ tels que

$$(\mathrm{II}) \qquad \Delta(x) > \lambda$$

satisfait à

$$(12) \qquad \operatorname{mes} V \leqq C\, e^{-c\lambda}\, |\omega^{**}| \quad .$$

Carleson donne une preuve assez simple, utilisant le fait que, pour toute fonction sommable g on a :

$$\int \Delta(x) g(x)\, dx = \pi \sum |\omega_{\kappa}|\, g(t_{\kappa}, |\omega_{\kappa}|) \quad ,$$

$g(x,y)$ désignant le prolongement harmonique de g dans le demi-plan $y > 0$.

Lemme 4. Soit $\bar{\omega}$ un intervalle, et $\phi \in L^1(\bar{\omega})$. On pose

$$(13) \qquad \gamma(\bar{\omega}, \phi) = \gamma(\bar{\omega}) = \frac{1}{|\bar{\omega}|} \sup_{\alpha, \beta \in \bar{\omega}} \left| \int_{\alpha}^{\beta} \phi(t)\, dt \right| \quad .$$

a) **pour toute fonction** g **à variation bornée** sur $\bar{\omega}$, on a

$$(14) \qquad \frac{1}{|\bar{\omega}|} \left| \int_{\bar{\omega}} \phi g \right| \leqq \phi(\bar{\omega}) \left(V(g) + \min_{t \in \bar{\omega}} |g(t)| \right)$$

Topology

Séminaire BOURBAKI
(Décembre 1958)

L'HOMOTOPIE STABLE DES GROUPES CLASSIQUES D'APRÈS R. BOTT. APPLICATIONS

par Michel A. KERVAIRE

1. Le théorème de suspension.

Soient M une variété de Riemann compacte connexe de classe C^∞ et $\mu = (P, Q)$ un couple de points sur M. On désignera par $\Omega_\mu M$ l'ensemble des arcs différentiables par morceaux, joignant P à Q sur M, paramétrisés entre 0 et 1 proportionnellement à la longueur d'arc et muni de la métrique

$$\rho(c, c') = \max d[c(t), c'(t)] + |J(c) - J(c')| ,$$

le maximum étant pris sur $t \in [0, 1]$ (d, distance sur M ; $J(c)$, longueur de c).

A tout segment de géodésique $s \in \Omega_\mu M$ est attaché un <u>index</u> $\lambda(s)$ défini comme suit (cf. [3], proposition 3.2) : Un champ η de vecteurs tangents à M le long de s est dit "de Jacobi" s'il satisfait à l'équation différentielle de Jacobi $D_t^2 \eta^\alpha + R^\alpha_{\beta\gamma\delta} \dot{x}^\beta \eta^\gamma \dot{x}^\delta = 0$ (D_t^2, dérivée covariante seconde le long de s). Soit $\Lambda_s(X)$, pour X un point de s, l'espace vectoriel des champs de Jacobi sur s qui s'annulent en P et X. On pose $\lambda(s) = \sum_X \dim \Lambda_s(X)$, où la sommation s'étend à tous les $X \in s$, $X \neq P, Q$. (Cette somme est finie car $\dim \Lambda_s(X) = 0$, si X n'est pas conjugué de P).

Soit alors $|\mu|$ le plus petit index positif des géodésiques de $\Omega_\mu M$. ($|\mu| = \infty$ s'il n'existe pas de géodésique d'index positif).

Soit $M^\mu \subset \Omega_\mu M$ une composante connexe du sous-espace des géodésiques de longueur minimale. On a le

THÉORÈME 1. - <u>Si M est un espace symétrique, alors</u>

1° <u>M^μ est également un espace symétrique</u> ;

2° <u>l'inclusion</u> $f : M^\mu \to \Omega_\mu M$ <u>induit un isomorphisme</u>

$$f_* : \pi_k(M^\mu) \to \pi_k(\Omega_\mu M)$$

<u>pour</u> $0 < k < |\mu| - 1$ <u>et un épimorphisme pour</u> $k = |\mu| - 1$.

NOTE. - $\Omega_\mu M$ n'a pas en général le même type d'homotopie que l'espace des lacets sur M muni de la topologie de la convergence compacte. Ces deux espaces ont cependant des groupes d'homotopie isomorphes. En particulier, $\pi_i(\Omega_\mu M) \cong \pi_{i+1}(M)$.

EXEMPLES. - Soient $M = S^{n+1}$ et $\mu = (P , Q)$ un couple de points antipodiques, $M^\mu = S^n$ et $f_* : \pi_k(S^n) \to \pi_k(\Omega_\mu S^{n+1}) \cong \pi_{k+1}(S^{n+1})$ est la suspension de Freudenthal. On voit facilement qu'une géodésique de longueur $(2m+1)\pi$, joignant P à Q , a pour indexe $2mn$. Donc $|\mu| = 2n$ et f_* est un isomorphisme pour $k \leq 2n-2$ et un épimorphisme pour $k = 2n-1$.

Soit $M = U(2n)$, $P = E$ la matrice unité dans $U(2n)$ et $Q = -E$. Les géodésiques de longueur minimale sont données par $x.s(t).x^{-1}$, où $s(t) = e^{-i\pi t}E_n \times e^{i\pi t}E_n$, E_n étant la matrice unité à n lignes et n colonnes. L'ensemble M^μ $(\mu = (P , Q))$ de ces géodésiques est homéomorphe à la grassmannienne $U(2n)/U(n) \times U(n)$ et $|\mu| = 2n+2$. En passant à la limite $(n \to \infty)$, on obtient $\pi_k(B_U) \cong \pi_{k+1}(U)$ pour tout k ; comme $\pi_{k-1}(U) \cong \pi_k(B_U)$ par la suite exacte d'homotopie de la fibration classifiante, on a $\pi_{k-1}(U) \cong \pi_{k+1}(U)$ pour tout k . On sait que $\pi_0(U) = 0$, $\pi_1(U) \cong Z$.

L'application 8 fois itérée du théorème 1, en partant de $M = SO(16n)$ fournit la période 8 pour les groupes d'homotopie stables du groupe orthogonal et la relation $\pi_k(SO) \cong \pi_{k+4}(Sp)$. On obtient également, entre autres, l'isomorphisme $\pi_k(SO/U) \cong \pi_{k+1}(SO)$, donc en particulier $\pi_{4n-1}(SO/U) \cong Z_{b_n}$, $b_n = 2$ ou 1 suivant que n est pair ou impair, résultat qui sera utilisé au n° 3.

<u>Esquisse de la démonstration du théorème</u> 1. — M étant tout d'abord une variété de Riemann compacte connexe quelconque, soit $\Omega_\mu^a M$ le sous-espace de $\Omega_\mu M$ caractérisé par $J(c) \leq a$. On démontre que $\Omega_\mu^a M$ a la même type d'homotopie que le sous-espace N^b de $N = M \times M \times \dots \times M$ (n fois) défini par $N^b = \{x \in N \mid \Phi(x) \leq b\}$, où $\Phi(x) = \sum_0^n [d(x_i , x_{i+1})]^2$, $x_0 = P$, $x_{n+1} = Q$, n est assez grand pour que $a/\sqrt{(n+1)} < \tilde{\rho}$ = longueur élémentaire sur M , et $b = a^2/(n+1)$. Une homotopie équivalence $\alpha : \Omega_\mu^a M \to N^b$ est donnée par $\alpha(c) = c(t_1) , \dots , c(t_n)$, avec $t_i = i/(n+1)$. L'application inverse (à l'homotopie près) est donnée par $\beta(x)$ = polygône géodésique $[Px_1][x_1x_2] \dots [x_nQ]$. (Deux points dont la distance est inférieure à $\tilde{\rho}$ sont extrémités d'un segment de géodésique unique qui varie continûment avec ses extrémités).

On constate que x est critique pour Φ si et seulement si $x = \alpha(s)$, où $s \in \Omega_{\mu}^{a} M$ est un segment de géodésique.

De plus, si $x = \alpha(s)$, le <u>corang</u> de la hessienne H_{Φ} de Φ en x vaut $\dim \Lambda_s(Q)$; l'<u>index</u> de H_{Φ} en x vaut $\lambda(s)$. (Cf. M. MORSE [15], chapitre III, Théorèmes 6.1 et 6.2 respectivement).

Si M est en outre symétrique ($M = G/K$, G muni d'un automorphisme involutif α et $K = \{g \in G \mid \alpha g = g\}$), G opérant par isométries, l'action de G est "<u>variationnellement complète</u>". Cela signifie que tout champ de Jacobi le long de s qui s'annule en P est la restriction sur s d'un déplacement infinitésimal de G (cf. R. BOTT [3], paragraphe 6). Ceci implique :

1° M^{μ} est une variété de Riemann symétrique. En fait, M^{μ} est homéomorphe à K_{μ}/K_s (K_A, stabilisateur de l'ensemble A).

2° Les ensembles critiques de Φ sont des sous-variétés de N. La dimension d'une composante connexe V est donnée par $\dim V = \dim \Lambda_s(Q)$, avec $\alpha(s) \in V$. La dimension de V est donc égale au corang de H_{Φ} en $x \in V$: les variétés V sont des <u>variétés critiques non dégénérées</u>. (Cf. R. BOTT [2]).

Le reste de la démonstration du théorème 1 consiste à généraliser les idées de l'article [19] de R. THOM au cas où les ensembles critiques d'une fonction Φ sur une variété N sont des variétés critiques non-dégénérées (et non plus nécessairement des points isolés non-dégénérés). Soit c une valeur critique de Φ on obtient $N^{c+\varepsilon}$ ($\varepsilon > 0$, tel que $[c - \varepsilon , c + \varepsilon]$ ne contienne pas d'autre valeur critique pour Φ que c) en "attachant" à $N^{c-\varepsilon}$ des espaces E_V fibrés en boules sur V par une application f_V du bord de E_V dans $N^{c-\varepsilon}$ (V parcourt l'ensemble des composantes connexes de l'ensemble critique $\Phi = c$). La dimension des boules (fibres de E_V) est égale à l'index de H_{Φ} en $x \in V$. Le théorème 1 s'ensuit après décomposition cellulaire de E_V en cellules de dimensions nulles ou $\geq$ index de H_{Φ} en $x \in V$.

2. <u>Le groupe</u> $\pi_{2m}(U(m))$.

Le calcul de ce groupe (instable) est basé sur le

THÉORÈME 2. - <u>Soit</u> h <u>l'homomorphisme de Hurewicz</u> $h : \pi_{2n}(B_U) \to H_{2n}(B_U)$. <u>l'image par</u> h <u>d'un générateur de</u> $\pi_{2n}(B_U) \cong Z$ <u>est exactement divisible par</u> $(n-1)!$.

Montrons que la formule $\pi_{2m}(U(m)) \cong Z_{m!}$ est une conséquence de ce théorème : Soit $f : S^{2n} \to B_U$ une application représentant un générateur de $\pi_{2n}(B_U)$.

L'application f induit sur S^{2n} un fibré principal ξ de groupe $U(N)$, $N \geqslant n$. Soit ξ' le fibré associé de fibre $U(N)/U(n-1)$. Soient $\chi(\xi) \in \pi_{2n-1}(U(N))$ et $\chi(\xi') \in \pi_{2n-1}(U(N)/U(n-1))$ les "classes caractéristiques" de ces fibrés $\chi(\xi)$ est un générateur de $\pi_{2n-1}(U(N))$; la projection

$$q_* : \pi_{2n-1}(U(N)) \rightarrow \pi_{2n-1}(U(N)/U(n-1))$$

envoie $\chi(\xi)$ sur $\chi(\xi')$; $\chi(\xi') = c_n[S^{2n}]$. La suite exacte d'homotopie de $U(N)/U(n-1)$ montre que $\pi_{2n-2}(U(n-1))$ est cyclique et en outre que son ordre q_n satisfait à $c_n[S^{2n}] = q_n$. Comme $h\{f\}$ est exactement divisible par $c_n[S^{2n}]$, on a $q_n = (n-1)!$.

A. BOREL et F. HIRZEBRUCH ([1], 26.5) ont donné un exemple de fibré $U(N)$ sur S^{2n} dont la classe de Chern vaut $(n-1)!$. Pour démontrer le théorème 2, il est donc suffisant de démontrer que $\operatorname{Im} h \subset (n-1)!\, H_{2n}(B_U)$.

Soit $f : U(2N)/U(N) \times U(N) \rightarrow \Omega U(2N)$ l'application de Bott (cf. n° 1), et $\lambda_0 = \partial^{-1} \partial_{\Omega}^{-1}$, $f_* : \pi_k(B_U) \rightarrow \pi_{k+2}(B_U)$ l'isomorphisme qui fournit la périodicité (∂ et ∂_{Ω} sont les homomorphismes bord des fibrations $U \rightarrow E_U \rightarrow B_U$ et $\Omega U \rightarrow LU \rightarrow U$, respectivement). On a un homomorphisme analogue en cohomologie $\lambda = f^* S_{\Omega}^* S^* : H^{k+2}(B_U) \rightarrow H^k(B_U)$, où S^* est la suspension en cohomologie. On voit immédiatement que $\operatorname{Im} h \subset (n-1)!\, H_{2n}(B_U)$ est équivalente à $\operatorname{Im} \lambda^{n-1} \subset (n-1)!\, H^2(B_U)$, $\lambda^{n-1} : H^{2n}(B_U) \rightarrow H^2(B_U)$ étant obtenue par itération de λ. Comme λ annule les éléments décomposables (par le produit cup), il est suffisant de montrer que pour tout m, $\lambda(c_m)$ est un multiple de $(m-1)c_{m-1}$ plus des éléments décomposables. Pour cela on introduit dans B_U la multiplication μ induite par le couplage naturel $G_{p,q} \times G_{p',q'} \rightarrow G_{p+p',q+q'}$ où $G_{r,s}$ est la variété des r-plans (complexes) de C^{r+s}. On démontre alors que

1° Les éléments dans l'image de λ sont primitifs (v est primitif si $\mu^* v = v \otimes 1 + 1 \otimes v$) ;

2° Les éléments primitifs de $H^{2m}(B_U)$ sont les multiples de $p_m = m.c_m$ + éléments décomposables.

La démonstration de 2° est un exercice d'algèbre élémentaire, compte tenu de la formule de dualité de Whitney qui s'exprime ici par

$$\mu^* c_m = c_m \otimes 1 + c_{m-1} \otimes c_1 + \dots + c_1 \otimes c_{m-1} + 1 \otimes c_m \ .$$

D'après un théorème général (cf. par exemple G.W. WHITEHEAD [21]), les éléments dans l'image de $S^*_\Omega S^* : H^{k+2}(B_U) \to H^k(\Omega U)$ sont primitifs relativement à la multiplication μ' dans ΩU . Il reste donc à voir que $f^* : H^*(\Omega U) \to H^*(B_U)$ préserve la "primitivité". Cela revient à démontrer que le diagramme

$$\begin{tikzcd} B_U \times B_U \arrow[r, "f\times f"] \arrow[d, "\mu"] & \Omega U \times \Omega U \arrow[d, "\mu'"] \\ B_U \arrow[r, "f"] & \Omega U \end{tikzcd}$$

est commutatif à l'homotopie près.

APPLICATIONS

3. Parallélisme sur les sphères et groupes d'homotopie non-stables de $SO(m)$.

Une variété différentiable M^k est dite parallélisable si elle admet un champ de k-repères tangents. (Cf. E. STIEFEL [18]).

Pour les sphères, on voit aisément que S^k est parallélisable si et seulement si l'homomorphisme $\pi_k(SO(k+1)) \to \pi_k(S^k)$ induit par la projection $SO(k+1) \to S^k$ est surjectif.

L'existence d'un parallélisme sur S^1 est trivial. H. HOPF [8] a montré l'existence d'un parallélisme sur S^3 et S^7 en utilisant les algèbres de divisions des quaternions et des nombres de Cayley. B. ECKMANN [7] et G.W. WHITEHEAD [20] ont montré que les sphères de dimensions $4n+1$ avec $n \geqslant 1$ ne sont pas parallélisables. Les résultats précédents de R. BOTT entraînent que S^{4n-1} n'est pas parallélisable pour $n \geqslant 3$. (Cf. [6] et [9]). On retrouve d'ailleurs également le résultat de B. ECKMANN-G.W. WHITEHEAD.

En effet, $\pi_k(SO(k+1)) \to \pi_k(S^k)$ est surjectif si et seulement si $\Phi : \pi_k(SO(m)) \to \pi_k(V_{m,m-k})$ est surjectif $(m \geqslant k+2)$. Pour $k = 4n-1$, le premier de ces groupes est $\cong Z$, l'autre $\cong Z_2$. Comme $\pi_{4n-1}(V_{m-4n+2}) \cong Z_4$, pour que S^{4n-1} soit parallélisable, il faut que

$$\Phi' : \pi_{4n-1}(SO(m)) \to \pi_{4n-1}(V_{m,m-4n+2})$$

soit surjectif. Or on a la diagramme commutatif