Jean-Pierre Serre

EXPOSÉS DE SÉMINAIRES (1950 – 1999)

DEUXIÈME ÉDITION, AUGMENTÉE

DOCUMENTS MATHÉMATIQUES 1

Société Mathématique de France 2008

EXPOSÉS DE SÉMINAIRES (1950 – 1999)

DEUXIÈME ÉDITION, AUGMENTÉE

Jean-Pierre Serre

Documents Mathématiques

série dirigée par Pierre COLMEZ

Secrétariat : Nathalie Christiaën

Documents Mathématiques
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France

Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
revues@smf.ens.fr • http://smf.emath.fr/

ISSN 1629-4939

ISBN 978-2-85629-242-6

Directeur de la publication : Stéphane JAFFARD

DOCUMENTS MATHÉMATIQUES 1

EXPOSÉS DE SÉMINAIRES (1950 – 1999)

DEUXIÈME ÉDITION, AUGMENTÉE

Jean-Pierre Serre

Société Mathématique de France 2008

TABLE DES MATIÈRES

PRÉFACE

Les textes composant le présent volume reproduisent des exposés que j'avais faits dans les séminaires Bourbaki, Cartan, Chevalley et Delange-Pisot-Poitou entre 1950 et 1999 (en fait, la plupart datent des années 1950–1960). Aucun d'eux ne figure dans les volumes de « Collected Papers » publiés par Springer-Verlag en 1986 et 2000.

Les sujets abordés sont assez divers : Groupes de Lie, Homotopie, Fonctions de variables complexes, Algèbre homologique, Géométrie algébrique, Théorie des nombres, Formes modulaires.

La transcription en TEX(*) m'a permis de faire un grand nombre de corrections de détail, portant notamment sur les notations : j'ai remplacé le couple « biunivoque, sur » des années 50 par « injectif, surjectif »; « décemment ramifié » est devenu « modérément ramifié », et « $x \to f(x)$ » s'est transformé en « $x \mapsto f(x)$ ». Je n'ai pas hésité non plus à corriger les erreurs de calcul, ou de raisonnement, et à compléter certaines démonstrations.

Des notes, placées à la fin, apportent des renseignements complémentaires; elles sont indiquées dans le texte par un chiffre de renvoi placé dans la marge.

Paris, décembre 2000

J.-P. Serre

Dans la présente édition (2008) deux textes plus récents ont été ajoutés, l'un sur un théorème de Jordan, l'autre sur la notion de complète réductibilité.

(*) La frappe du texte a été effectuée par P. Colmez et ses collaborateurs; je les remercie très vivement.

Séminaire Bourbaki mars 1950
1949-50, exposé n° 27

EXTENSIONS DE GROUPES LOCALEMENT COMPACTS

d'après Iwasawa et Gleason

Cet exposé n'étudie que les extensions finies de groupes de Lie, ou plus généralement, de groupes localement compacts. Les extensions infinies (c'est-à-dire les limites projectives) feront l'objet d'un exposé ultérieur. 1

1. Extensions de groupes discrets (cf. Baer et Eilenberg-Maclane)

Un groupe E est dit extension du groupe F par le groupe B s'il admet F 2
pour sous-groupe invariant et si E/F = B. Dans toute la suite, B et F seront considérés comme connus, et l'on cherchera à construire le groupe E.

a) F étant invariant, les automorphismes intérieurs de E définissent des automorphismes de F, d'où une représentation E → Aut(F). Dans cette représentation, F est envoyé sur Int(F), d' où, par passage au quotient, une représentation 3
$\theta : \mathrm{B} \to \mathrm{Aut(F)}/\mathrm{Int(F)}$, qui est un premier *invariant* de l'extension E.

b) Cette représentation étant connue, considérons la représentation

$$\mathrm{E} \longrightarrow \mathrm{Aut(F)} \times \mathrm{B},$$

produit des représentations canoniques de E dans Aut(F) et dans B. Le noyau de cette représentation est le centre C de F, et l'image est le sous-groupe H formé des couples (σ, b) où $\sigma = \theta(b)$. H et C sont donc connus et l'on voit que *l'on s'est ainsi ramené à étudier les extensions de noyau abélien.*

c) Dans ce dernier cas, soit f une section (c'est-à-dire une application B → E telle que $p \circ f(b) = b$ pour tout $b \in \mathrm{B}$, p désignant la projection de E sur B) et posons $f(x) \cdot f(y) = u(x, y) f(xy)$. La fonction u est à valeurs dans F; c'est une 2-*cochaîne* sur B. Si l'on calcule $f(x) \cdot f(y) \cdot f(z)$, on trouve que u vérifie l'identité $\theta_x u(y, z) + u(x, yz) = u(x, y) + u(xy, z)$. Si l'on convient d'appeler

cobord de la n-cochaîne $g(x_1, \ldots, x_n)$ la $n+1$-cochaîne :

$$dg(x_1, \ldots, x_{n+1}) = \theta_{x_1} g(x_2, \ldots, x_{n+1}) + \sum_{i=1}^{n} (-1)^i g(x_1, \ldots, x_i \cdot x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} g(x_1, \ldots, x_n),$$

on voit que u est un 2-*cocycle*. En outre, si l'on remplace f par une section $f'(x) = v(x)f(x)$ où $v(x) \in \mathrm{F}$, f' définit un cocycle $u' = u + dv$. D'où :

Les extensions de F *par* B (correspondant à une représentation $\mathrm{B} \to \mathrm{Aut}(\mathrm{F})$ donnée) *correspondent bijectivement aux éléments du groupe de cohomologie de dimension* 2 *du groupe* B *à coefficients dans* F.

2. Extensions de groupes topologiques

Définitions évidentes. Les résultats précédents se transposent de la façon suivante :

a) Remplacer automorphisme par automorphisme de groupe topologique. Si F est localement compact, on munit Aut(F) de la topologie de la convergence compacte et la représentation θ est continue.

b) Le seul changement est que l'on peut simplement dire que E admet une *représentation continue* de noyau C sur H.

c) On ne peut appliquer la méthode de la cohomologie que *si l'on a une section continue*, ce qui est une exigence extrêmement forte.

Remarque. — Toutes les méthodes précédentes s'appliquent de façon locale,
4 et, en particulier, valent aussi bien pour un noyau de groupe. La méthode c) n'exige alors que l'existence de *sections locales continues.*

3. Espaces fibrés principaux

L'existence, sous certaines conditions, de sections locales continues est un cas particulier d'un résultat valable pour les espaces fibrés principaux.

DÉFINITION. — Soient E un espace topologique et F un groupe topologique opérant sur E. On dit que E est un *fibré principal de groupe* F si, pour tout
5 couple (x, x') d'éléments de E, il existe au plus un $s \in \mathrm{F}$ avec $x' = x \cdot s$ et si cet s est fonction continue de (x, x').

Les *fibres* sont les classes de la relation d'équivalence $x' \equiv x \cdot s$. La *base* est le quotient de E par cette relation. Si E est un groupe topologique et F un sous-groupe fermé, les fibres sont les classes à droite et la base est l'espace

homogène associé. Si la base et le groupe structural sont localement compacts, E l'est aussi.

THÉORÈME 1 (GLEASON). — *Si le groupe structural* F *est un groupe de Lie et si* E *est un espace complètement régulier* (en particulier un groupe topologique séparé)*,* E *est localement trivial* (localement trivial signifie que par tout point passe une section locale continue)*.*

D'après un théorème d'ADO, il existe une représentation linéaire locale fidèle de F. Soit M l'algèbre de matrices où F est ainsi plongé. Le groupe F opère sur M et, en particulier, sur le groupe G des matrices inversibles. Soit $g : O \longrightarrow G$ une application continue d'un voisinage O d'un point donné de E, vérifiant la condition $g(xs) = g(x) \cdot s$ pour $s \in F$ assez petit. L'image réciproque par g d'une section locale du F-fibré G donne une section locale de E. Tout revient 6
donc à construire une telle application g.

Pour cela, on prend une fonction réelle positive, continue, égale à 1 en un point déterminé de la fibre étudiée et nulle en dehors d'un voisinage convenable, soit f. Posons $g(x) = \int 1_M f(xs)s^{-1}ds$ (ds : mesure de Haar à gauche sur F; 1_M : unité de M). On a bien $g(xt) = g(x)t$ (pour t assez petit) et $g(x) \in G$ pour x assez près du point donné, c.q.f.d.

Remarque. — Le caractère local de la démonstration montre que l'on a :

THÉORÈME 2. — *Si* E *est un noyau de groupe admettant pour noyau de sous-groupe un noyau de groupe de Lie,* E *admet une section locale continue.*

4. Extensions d'un groupe de Lie par un groupe de Lie

Nous allons démontrer le théorème suivant :

THÉORÈME 3 (IWASAWA-GLEASON). — *Toute extension d'un groupe de Lie par un groupe de Lie est un groupe de Lie.*

La démonstration étant purement locale montrera même que toute extension d'un *noyau* de groupe de Lie par un autre est un noyau de groupe de Lie.

Appliquons les méthodes du n° 1. Aut(F) est un noyau de groupe de Lie ainsi que Aut(F)/ Int(F). Toute représentation continue d'un noyau de groupe de Lie dans un autre étant analytique, il en résulte que θ est analytique et que H est un noyau de groupe de Lie. On est donc ramené au cas abélien.

Pour étudier ce dernier, remarquons que, d'après le théorème 2, E admet une section locale continue, et correspond donc à une classe de cohomologie de dimension 2. Si l'on choisit une telle section locale (et de ce fait un cocycle), on

peut identifier l'espace E au produit $B \times F$ et le munir de la structure différentiable produit. Mais pour que la loi de groupe soit différentiable, on voit tout de suite qu'il faut et qu'il suffit que le cocycle en question soit différentiable sur $B \times B$. Nous avons donc à montrer que *toute classe de cohomologie contient un cocycle indéfiniment différentiable.*

Soient donc u un 2-cocycle continu et $k(x)$ une fonction indéfiniment différentiable sur B, à support compact, et telle que $\int k(x)\ dx = 1$ (dx mesure de
7 Haar à gauche). Posons $v(x) = \int u(x,t)k(t)\ dt$. Un calcul immédiat montre que :

$$(1) \qquad (u - dv)(x,y) = \int u(x,yt)k(t)\ dt - \int u(x,t)k(t)\ dt.$$

Le cocycle u est donc cohomologue au cocycle du membre de droite. Mais ce dernier est indéfiniment différentiable par rapport à y (produit de composition). Nous allons passer de ce résultat à la différentiabilité par rapport au couple (x,y) en utilisant le fait que, pour tout cocycle u, le cocycle $v(x,y) = -\theta_{xy}u(y^{-1},x^{-1})$ lui est cohomologue [car, si u est relatif à une section f, v est relatif à la section $x \mapsto f(x^{-1})^{-1}$].

On voit alors, en échangeant x et y, que tout cocycle est cohomologue à un cocycle différentiable en x. Appliquant à ce dernier l'identité (1) on trouve bien un cocycle indéfiniment différentiable par rapport à (x,y).

5. Extensions d'un $\mathbf{R}^n$ par un compact

D'après le théorème 1, une telle extension est un fibré localement trivial (puisque le groupe structural est $\mathbf{R}^n$). Mais alors elle est topologiquement triviale (prolonger une section partielle en utilisant le fait que $\mathbf{R}^n$ est un rétracte
8 absolu). On peut donc appliquer les méthodes cohomologiques.

Soit alors u un 2-cocycle, et appliquons-lui l'identité (1) où l'on a pris pour $k(x)$ la fonction constante égale à 1. On trouve $u - dv = 0$, ce qui montre que le second groupe de cohomologie de B est nul. D'où :

THÉORÈME 4 (IWASAWA). — *Dans toute extension d'un $\mathbf{R}^n$ par un groupe compact, il y a une section qui est un sous-groupe.*

En fait, une extension évidente de la méthode précédente montre que

9 THÉORÈME 5. — *Tous les groupes de cohomologie d'un groupe compact dans $\mathbf{R}^n$ sont nuls.*

Si l'on applique ceci au premier groupe de cohomologie, on voit que cela donne : dans les hypothèses du théorème 4, *deux sous-groupes sections sont conjugués* (IWASAWA).

Remarque. — Ces démonstrations étaient employées depuis longtemps dans le cas des groupes *finis* (cf. par exemple ZASSENHAUS, [3] Chap. 4, th. 25).

6. Extensions de groupes compacts

THÉORÈME 6 (IWASAWA). — *Si* F *est un groupe compact, le groupe quotient* $\mathrm{Aut(F)/\,Int(F)}$ *est totalement discontinu.*

Dans le cas abélien, cela revient à dire que Aut(F) est totalement discontinu, ce qui est évident puisque $\mathrm{Aut(F)} = \mathrm{Aut}(\hat{\mathrm{F}})$ et que $\hat{\mathrm{F}}$ est discret.

Dans le cas général, on remarque que tout automorphisme appartenant à la composante connexe de l'unité dans Aut(F) laisse les caractères de F invariants (cela tient à ce que *les caractères forment un ensemble discret* pour la topologie de la convergence uniforme d'après les relations d'orthogonalité de Schur). Si F_i est l'image de F dans une représentation linéaire, cet automorphisme passe donc au quotient et définit sur F_i un automorphisme intérieur (il s'agit, en somme, de vérifier le théorème 6 pour les groupes de Lie, ce qui n'est pas difficile, vu que l'on connaît leur structure). On en déduit, par un raisonnement de compacité, que l'automorphisme de F étudié est intérieur, ce qui achève la démonstration.

On en déduit aussitôt les résultats suivants :

THÉORÈME 7 (IWASAWA). — *Tout groupe compact à centre nul est facteur direct dans toute extension connexe.*

[Appliquer 1.b), en remarquant que $\theta = 0$ et que $\mathrm{C} = 0$.]

THÉORÈME 8 (IWASAWA). — *Tout groupe compact abélien est contenu dans le centre de toute extension connexe* (car $\theta = 0$).

THÉORÈME 9 (IWASAWA). — *Tout groupe résoluble compact connexe est abélien.*

7. Structure des groupes de Lie résolubles

(Rappelons que résoluble signifie : qui admet une suite de composition à quotients abéliens.)

THÉORÈME 10 (CHEVALLEY). — *Tout groupe de Lie connexe résoluble est homéomorphe au produit d'un tore par un* $\mathbf{R}^n$. **10**

Le groupe étudié, G, admet une suite de composition formée de sous-groupes fermés connexes tels que les quotients soient abéliens : il suffit de prendre les commutateurs successifs de G.

On démontre le théorème 10 en raisonnant par récurrence sur la longueur de la chaîne précédente et en utilisant le lemme suivant :

Lemme 1. — *Toute extension de* $\mathbf{R}^n$ *ou d'un tore* $\mathbf{T}^p$ *par* $\mathbf{R}$ *ou* $\mathbf{T}$ *admet une section continue qui est un sous-groupe.*

La démonstration du lemme est immédiate : on sépare les divers cas, et l'on fait usage des théorèmes 4 et 9.

Le théorème 10 se laisse préciser comme suit :

Soit $\mathbf{T}^p$ *un tore, sous-groupe compact maximum d'un groupe résoluble* E. *Le groupe* E *possède des sous-groupes à* 1 *paramètre,* $\mathrm{R}_1, \ldots, \mathrm{R}_q$ *isomorphes à* $\mathbf{R}$ *et tels que tout* $x \in \mathrm{E}$ *s'écrive d'une façon et d'une seule sous la forme*

$$x = t \cdot r_1 \cdots r_q, \quad \textit{avec } t \in \mathbf{T}^p \textit{ et } r_i \in \mathrm{R}_i.$$

Bibliographie

[1] A. GLEASON, *On the structure of locally compact groups*, Proc. Nat. Acad. Sc. U.S.A. **35** (1949), 384–386.

[2] K. IWASAWA, *On some types of topological groups*, Ann. of Math. **50** (1949), 507–558.

[3] H. ZASSENHAUS, *The Theory of Groups*, Chelsea, New York, 1949.

Additif [Avril 1957]

Les résultats d'IWASAWA et GLEASON donnés dans le présent exposé étaient destinés à faciliter l'étude de la structure des groupes localement compacts; depuis, cette structure a été complètement élucidée, grâce aux travaux de GLEASON, MONTGOMERY-ZIPPIN, YAMABE.

On trouvera un bon exposé de la question dans :

D. MONTGOMERY and L. ZIPPIN, *Topological Transformation Groups*, New York, Interscience, 1955 (Interscience Tract nº 1).

Séminaire Cartan
1950-51, exposé n° 5

18 décembre 1950

APPLICATIONS ALGÉBRIQUES DE LA COHOMOLOGIE DES GROUPES I

1. Préliminaires

Dans cet exposé et le suivant, il sera exclusivement question de *cohomologie* des groupes, et non d'homologie.

Rappelons qu'étant donné un groupe G (non nécessairement abélien) et un groupe abélien A sur lequel G opère à gauche, on a défini les groupes de cohomologie $\mathrm{H}^i(\mathrm{G},\mathrm{A})$; ces groupes peuvent être définis, par exemple, au moyen des *cochaînes* sur G à valeurs dans A, munies du cobord habituel :

$$(\delta f)(x_1,\dots,x_{i+1}) = x_1 \cdot f(x_2,\dots,x_{i+1}) + \sum_{j=1}^{i}(-1)^j f(x_1,\dots,x_jx_{j+1},\dots,x_{i+1}) + (-1)^{i+1} f(x_1,\dots,x_i)\,.$$

Si A est muni d'un ensemble d'opérateurs S permutant avec les opérateurs de G, alors on peut faire opérer S sur les groupes $\mathrm{H}^i(\mathrm{G},\mathrm{A})$: cela résulte de l'axiome (II_c) de l'exposé 1, ou bien d'une définition directe à partir des cochaînes. En particulier, si A est un espace vectoriel sur un corps k, et si les opérations de G sont k-linéaires, $\mathrm{H}^i(\mathrm{G},\mathrm{A})$ est un espace vectoriel sur k.

Enfin, signalons le résultat suivant :

Soit G un groupe fini à n éléments, et soit $h \in \mathrm{H}^i(\mathrm{G},\mathrm{A}), i > 0$; on a $nh = 0$.

Soit f un cocycle de la classe h, et écrivons que $(\delta f)(x_1,\dots,x_{i+1}) = 0$. On obtient une certaine identité faisant intervenir les $i+1$ variables $x_1,\dots,x_{i+1}$. Faisons parcourir à x_{i+1} le groupe G, et ajoutons les identités ainsi obtenues. Si l'on pose :

$$g(x_1,\dots,x_{i-1}) = \sum_{x_i \in \mathrm{G}} f(x_1,\dots,x_i)\,,$$

on obtient $nf = (-1)^i \delta g$.

Autre démonstration. On écrit A comme sous-groupe stable d'un groupe G-injectif ; on s'aperçoit alors, en écrivant la suite exacte de l'axiome (IV_c), qu'il suffit de démontrer le résultat en question pour $i = 1$, et que, pour $i = 1$, il est presque évident.

2. Le premier groupe de cohomologie. Application à l'étude des représentations linéaires

Les 1-cochaînes sont les applications : $f : \mathrm{G} \to \mathrm{A}$. Les *cocycles* sont celles qui vérifient :

$$f(xy) = f(x) + x \cdot f(y)\,,$$

on les appelle *homomorphismes croisés.* Si par hasard G opère trivialement sur A, ce sont simplement les homomorphismes de G dans A.

Les *cobords* sont les cochaînes de la forme :

$$f(x) = x \cdot a - a,\ a \in \mathrm{A}\,.$$

On les appelle homomorphismes croisés *principaux.* Si G opère trivialement sur A, tous les cobords sont donc nuls. D'où : *Si* G *opère trivialement sur* A, *on a* : $\mathrm{H}^1(\mathrm{G}, \mathrm{A}) = \mathrm{Hom}(\mathrm{G}, \mathrm{A})$.
(Signalons que l'on a aussi, dans ce cas, $\mathrm{H}_1(\mathrm{G}, \mathrm{A}) = \mathrm{G}^{\mathrm{ab}} \otimes \mathrm{A}$, où G^{ab} désigne le quotient de G par son groupe des commutateurs ; ces deux résultats peuvent s'obtenir par voie topologique, en utilisant le théorème d'Hurewicz et la formule des coefficients universels.)

Nous allons maintenant utiliser le groupe H^1 pour étudier les *extensions* de représentations linéaires.

Considérons une suite exacte :

$$0 \longrightarrow \mathrm{V} \longrightarrow \mathrm{E} \longrightarrow \mathrm{W} \longrightarrow 0\,,$$

où $\mathrm{V}, \mathrm{E}, \mathrm{W}$ désignent des espaces vectoriels sur un corps commutatif k sur lesquels opère le groupe G ; bien entendu, on suppose d'une part que les opérateurs de k et G commutent (on a donc des représentations linéaires de G), et d'autre part que les applications $i : \mathrm{V} \to \mathrm{E}$ et $p : \mathrm{E} \to \mathrm{W}$ commutent tant avec k qu'avec G. Nous nous proposons, V et W étant donnés, de chercher tous les E possibles ; on observera que la somme directe $\mathrm{V} \oplus \mathrm{W}$ convient toujours.

Pour cela nous allons définir une *classe caractéristique* dont la donnée déterminera E sans ambiguïté (à isomorphisme près). Désignons par $\mathrm{Hom}(\mathrm{A}, \mathrm{B})$ l'espace vectoriel des applications linéaires de l'espace vectoriel A dans l'espace vectoriel B. On a la suite exacte :

$$(\mathrm{A}) \qquad 0 \longrightarrow \mathrm{Hom}(\mathrm{W}, \mathrm{V}) \longrightarrow \mathrm{Hom}(\mathrm{W}, \mathrm{E}) \longrightarrow \mathrm{Hom}(\mathrm{W}, \mathrm{W}) \longrightarrow 0\,.$$

Que cette suite soit exacte résulte du fait que E est isomorphe, *en tant qu'espace vectoriel*, à la somme directe de V et W.

On peut faire opérer le groupe G dans chacun des termes de la suite exacte précédente, en faisant correspondre à l'homomorphisme $u : A \to B$, l'homomorphisme $x \cdot u$ défini par

$$(x \cdot u)(a) = x \cdot u(x^{-1} \cdot a)\,.$$

Pour que u soit un G-homomorphisme, il faut et il suffit que $x \cdot u = u$ pour tout $x \in G$. Autrement dit : $H^0(G, \mathrm{Hom}(A, B)) = \mathrm{Hom}_G(A, B)$.

Appliquons alors à la suite (A) l'axiome de la suite exacte. On obtient :

$$\text{(B)}\quad 0 \longrightarrow \mathrm{Hom}_G(W, V) \longrightarrow \mathrm{Hom}_G(W, E) \longrightarrow \mathrm{Hom}_G(W, W) \xrightarrow{\delta} H^1(G, \mathrm{Hom}(W, V))\,.$$

Soit $I \in \mathrm{Hom}_G(W, W)$ l'application identique de W sur W, et posons $J = \delta I$. On a $J \in H^1(G, \mathrm{Hom}(W, V))$; c'est la classe caractéristique cherchée.

Pour que E soit somme directe (en tant que représentation) de V et W, il faut et il suffit que l'on puisse trouver un G-homomorphisme : $W \xrightarrow{K} E$, tel que $K \circ p = I$; ceci signifie que I est contenu dans l'image de $\mathrm{Hom}_G(W, E)$, ou encore que $J = 0$, puisque (B) est une suite exacte. D'où :

Pour que E *soit somme directe des représentations* V *et* W*, il faut et il suffit que* $J = 0$.

Calcul de la classe fondamentale. — Écrivons E comme somme directe de V et d'un supplémentaire W. Si E_x désigne l'automorphisme de E défini par x, on peut écrire E_x sous forme d'une matrice

$$E_x = \begin{pmatrix} V_x & R_x \\ 0 & W_x \end{pmatrix}$$

(dans cette formule, V_x et W_x ne sont autres que les automorphismes définis par x sur V et W). Considérons la 1-cochaîne : $j(x) = R_x \cdot {W_x}^{-1}$, à valeurs dans $\mathrm{Hom}(W, V)$; en remontant à la définition de l'homomorphisme δ de la suite exacte on voit que :
La cochaîne $j(x) = R_x \cdot {W_x}^{-1}$ *est un cocycle qui appartient à la classe* J. Ceci permet donc de calculer explicitement J lorsque E_x est donné.

Corollaire (Théorème de Maschke). — *Soit* G *un groupe fini à* n *éléments et supposons que la caractéristique de* k *ne divise pas* n*. Alors* E *est somme directe de* V *et* W. (D'où le fait que toute représentation de G est somme directe de représentations irréductibles.)

En effet d'après le n° 1, on a $n\mathrm{J} = 0$, d'où $\mathrm{J} = 0$.

Réciproque. — Soit J une classe de cohomologie de $\mathrm{H}^1(\mathrm{G}, \mathrm{Hom}(\mathrm{W}, \mathrm{V}))$, et soit $j(x)$ un cocycle appartenant à J. Montrons qu'il existe une représentation E_x correspondant à J.
Nous n'avons qu'à définir E_x par la matrice :

$$\mathrm{E}_x = \begin{pmatrix} \mathrm{V}_x & j(x)\mathrm{W}_x \\ 0 & \mathrm{W}_x \end{pmatrix} .$$

Il faut simplement vérifier que $\mathrm{E}_x \cdot \mathrm{E}_y = \mathrm{E}_{xy}$. Or on a :

$$\begin{pmatrix} \mathrm{V}_x & j(x)\mathrm{W}_x \\ 0 & \mathrm{W}_x \end{pmatrix} \begin{pmatrix} \mathrm{V}_y & j(y)\mathrm{W}_y \\ 0 & \mathrm{W}_y \end{pmatrix} = \begin{pmatrix} \mathrm{V}_x\mathrm{V}_y & \mathrm{V}_x j(y)\mathrm{W}_y + j(x)\mathrm{W}_x\mathrm{W}_y \\ 0 & \mathrm{W}_x\mathrm{W}_y \end{pmatrix} .$$

Il faut donc voir que

$$j(xy)\mathrm{W}(xy) = \mathrm{V}_x j(y)\mathrm{W}_y + j(x)\mathrm{W}_x\mathrm{W}_y,$$

ou

$$j(xy) = \mathrm{V}_x j(y){\mathrm{W}_x}^{-1} + j(x)\,,$$

ce qui exprime bien que $j(x)$ est un cocycle. On voit donc que :

Les classes de représentations de G, *qui sont des extensions de* V *par* W, *correspondent aux éléments de* $\mathrm{H}^1(\mathrm{G}, \mathrm{Hom}(\mathrm{W}, \mathrm{V}))$.

Remarque. — L'ensemble de ces classes se trouve donc muni d'une structure d'espace vectoriel, celle de $\mathrm{H}^1(\mathrm{G}, \mathrm{Hom}(\mathrm{W}, \mathrm{V}))$, qui correspond, sous la forme matricielle ci-dessus, à la structure vectorielle des R_x. On peut donner une définition directe de la somme de deux classes. Cf. Bibliographie.

Généralisations diverses

a) Au lieu d'étudier des représentations linéaires de G, on aurait pu considérer le cas plus général où on se donne des opérateurs S commutant avec les opérateurs de G. Les démonstrations précédentes s'appliquent sans changement, à condition de supposer que E est *somme directe de* V *et* W *pour les opérateurs de* S.

b) On peut étudier de façon analogue les représentations linéaires d'algèbres associatives, ou d'algèbres de Lie, moyennant une définition convenable de leur cohomologie. Par exemple, si L est une algèbre de Lie semi-simple, on démontre en employant le critère de Cartan et les opérateurs de Casimir que $\mathrm{H}^1(\mathrm{L}, \mathrm{A}) = 0$ pour toute représentation de L, d'où la complète réductibilité des représentations (J.H.C. Whitehead, *Quat. Jour.* **8** (1937), 220–237).

3. Extensions de groupes à noyau abélien

On se propose d'étudier les suites exactes de la forme :

$$0 \longrightarrow \mathrm{A} \xrightarrow{i} \mathrm{E} \xrightarrow{p} \mathrm{G} \longrightarrow 1\,,$$

où A est un groupe abélien, noté additivement, sous-groupe invariant d'un groupe E, le quotient étant le groupe (non nécessairement abélien) G. Les groupes E et G seront notés multiplicativement.

Les éléments de E opèrent sur E au moyen des automorphismes intérieurs ; ces derniers respectent A, et opèrent donc sur A. Comme A est abélien, A opère trivialement sur lui-même par la représentation précédente. On obtient alors par passage au quotient une représentation : $\mathrm{G} \to \mathrm{Aut}(\mathrm{A})$ qui sera notée θ. On a donc, si $y \in \mathrm{E}$:

$$\theta(p(y)) \cdot a = yay^{-1} \quad \text{pour tout } a \in \mathrm{A}\,.$$

A partir de maintenant nous étudierons uniquement les extensions E de G par A qui correspondent à des opérateurs donnés sur A. On va voir que ces extensions correspondent aux éléments de $\mathrm{H}^2(\mathrm{G}, \mathrm{A})$.

Nous aurons besoin de l'exercice II de l'exposé 2, exercice qui affirme que l'on ne change rien à la cohomologie de G en se bornant à considérer les cochaînes nulles lorsque l'une des variables vaut 1 (cochaînes *normalisées*). 1

Cela étant, soit E une extension, et soit k une *section*, c'est-à-dire une application de G dans E telle que $p \circ k = 1$. On a :

$$k(x)k(y) = u(x,y) \cdot k(xy) \tag{1}$$

avec

$$u(x,y) \in \mathrm{A}\,. \tag{2}$$

En outre, si l'on suppose que $k(1) = 1$, ce qui est licite, on a $u(1,y) = u(x,1) = 0$. On a donc défini une 2-cochaîne normalisée sur G à valeurs dans A.

Cette cochaîne (ou système de facteurs de E) détermine la structure de groupe de E. De façon précise, identifions $\mathrm{A} \times \mathrm{G}$ à E par l'application : $(a,x) \mapsto a \cdot k(x)$. On obtient ainsi une multiplication sur $\mathrm{A} \times \mathrm{G}$ que l'on détermine en écrivant

$$\begin{aligned} a \cdot k(x) \cdot b \cdot k(y) &= a \cdot k(x) b k(x)^{-1} \cdot k(x)k(y) \\ &= a \cdot k(x) b k(x)^{-1} \cdot u(x,y) \cdot k(xy)\,. \end{aligned} \tag{3}$$

D'où la formule du produit

$$(a,x) \cdot (b,y) = (a + x \cdot b + u(x,y),\ xy)\,. \tag{4}$$

On voit ainsi que deux extensions qui ont même système de facteurs sont isomorphes. Réciproquement, soit u une 2-cochaîne normalisée, et définissons une structure multiplicative sur $A \times G$ au moyen de la formule (4). Cette multiplication est-elle associative? On a :

$$((a,x)(b,y))(c,z) = (a + xb + u(x,y) + xyc + u(xy,z),\ xyz)\,, \tag{5}$$

$$(a,x)((b,y)(c,z)) = (a + xb + xyc + xu(y,z) + u(x,yz),\ xyz)\,. \tag{6}$$

En comparant (5) et (6), on voit que l'associativité est équivalente à :

$$xu(y,z) - u(xy,z) + u(x,yz) - u(x,y) = 0\,, \tag{7}$$

ce qui signifie que u *est un* 2*-cocycle.*

Cette condition étant supposée satisfaite, on vérifie tout de suite que l'élément $(0,1)$ est élément neutre, et que l'inverse de (x,a) est l'élément $(-x^{-1}\cdot a - u(x^{-1},x)\,,\ x^{-1})$; on a bien obtenu une extension de G par A.

Reste maintenant à voir comment le cocycle u dépend de la section k choisie. Si l'on prend une autre section k', on peut l'écrire :

$$k'(x) = v(x)k(x) \text{ avec } v(x) \in A \text{ et } v(1) = 1\,. \tag{8}$$

Calculons le système de facteurs u' relatif à k' :

$$\begin{aligned} k'(x)k'(y) &= v(x)k(x)v(y)k(y) = v(x)k(x)v(y)k(x)^{-1}k(x)k(y) \\ &= v(x)\cdot k(x)v(y)k(x)^{-1}\cdot u(x,y)\cdot k(xy) \\ &= v(x)\cdot k(x)v(y)k(x)^{-1}\cdot u(x,y)\cdot v(x,y)^{-1}\cdot k'(xy)\,, \end{aligned} \tag{9}$$

ce qui montre que :

$$k'(x)k'(y) = u'(x,y)k'(xy)\,, \tag{10}$$

avec :

$$u'(x,y) = u(x,y) + x\cdot v(y) - v(xy) + v(x)\,, \tag{11}$$

ou encore

$$u' = u + \delta v\,. \tag{12}$$

La formule (12) montre que u *est un cocycle déterminé à un cobord près*, autrement dit, définit canoniquement un élément de $H^2(G,A)$.

On a bien montré que *les classes d'extensions de* G *par* A *correspondent bijectivement aux éléments de* $H^2(G,A)$ (lorsque les opérateurs définis par G sur A sont donnés).

Exemple. — L'extension de G par A qui correspond à l'élément 0 de $H^2(G, A)$ s'appelle le *produit semi-direct* de G par A ; elle est caractérisée par l'existence d'une section k correspondant à un système de facteurs nul, c'est-à-dire par l'existence d'*une section qui soit un homomorphisme*. Le groupe E est alors le produit de A et du sous-groupe section, image de k. On notera que ce dernier sous-groupe n'est *invariant* que si G opère trivialement sur A, auquel cas on a : $E = A \times G$.

Deux sections qui sont des homomorphismes diffèrent par une 1-cochaîne v qui, d'après (12), doit être un cocycle. En particulier, si l'on sait que $H^1(G, A) = 0$, v est un cobord, ce qui se traduit par l'existence d'un $a \in A$ tel que :

$$k'(x) = ak(x)a^{-1}. \tag{13}$$

Donc :
Si $H^1(G, A) = 0$*, deux sous-groupes sections sont conjugués par un élément de* A. (Dans la théorie des algèbres de Lie, le résultat analogue, valable pour les algèbres semi-simples, est connu sous le nom de théorème de Malcev.)

D'après le n° 1, c'est en particulier le cas si G est fini d'ordre n, et si la division par n est possible d'une seule manière dans A.

Exemple de produit semi-direct

Le groupe des déplacements de $\mathbf{R}^3$ est produit semi-direct du groupe $\mathbf{SO}(3)$ des rotations par le sous-groupe normal $A = \mathbf{R}^3$ des translations. Les différents groupes sections sont les rotations autour d'un point de $\mathbf{R}^3$; ce sont bien des groupes conjugués par des translations, conformément au théorème de Malcev. Pour montrer qu'il n'y a pas d'autres sous-groupes sections (sans utiliser ce dernier théorème), on peut utiliser le fait que tout groupe compact de déplacements a un point fixe (évident, au moyen des centres de gravité).

Appendice — Multiplication de Baer

Soient E, E' deux extensions d'un même groupe G par un même groupe abélien A ; on suppose en outre que G opère de la même façon sur A dans les deux cas. On va construire une extension E'', *produit* de E par E'. Pour cela, considérons le sous-groupe (E, E') de $E \times E'$ formé des couples (e, e') ayant la même projection dans G. On définit de façon évidente un homomorphisme de (E, E') sur G, dont le noyau est l'ensemble des (a, a'), avec a et $a' \in A$. Soit Q le sous-groupe de ce noyau formé des $(a, -a)$. Posons $E'' = (E, E')/Q$; on vérifie immédiatement que E'' est une extension de G par A correspondant aux opérateurs donnés sur A.

Reste à voir que cette multiplication est la même que celle que l'on définit par l'addition des cocycles. Soient k, k' des sections de E, E'. L'application (k, k') définit une section de E'' (par passage au quotient) et si u et u' sont les cocycles correspondant à k et k', le cocycle correspondant à (k, k') est $u + u'$. Ceci achève la démonstration.

Bibliographie

On la trouvera dans :

S. Eilenberg, *Topological methods in abstract algebra. Cohomology theory of groups*, Bull. A.M.S. **55** (1949), 3–27.

Séminaire Cartan 8 et 15 janvier 1951
1950-51, exposés n^{os} 6 et 7

APPLICATIONS ALGÉBRIQUES DE LA COHOMOLOGIE DES GROUPES II : THÉORIE DES ALGÈBRES SIMPLES

Bibliographie

M. Deuring, *Algebren* (Ergebnisse der Mathematik IV-1), Berlin, Springer, 1935.
E. Artin, C. Nesbitt et R.M. Thrall, *Rings with minimum condition*, Ann Arbor, Univ. of Michigan Press, 1948.

Notations

Toutes les algèbres considérées par la suite ont un élément unité, noté 1. Le corps de base est identifié aux multiples de cet élément unité. Si E est un espace de représentation de l'algèbre A (sur le corps k), E est supposé de dimension finie sur k, et l'élément $1 \in A$ définit l'automorphisme identique de E. On dit que E est une représentation irréductible de A si $E \neq 0$ et si tout sous-espace stable de E est égal à 0 ou E ; E est dit complètement réductible s'il est somme directe de sous-espaces stables par A et irréductibles. Un tel espace peut être considéré comme un groupe semi-simple (à opérateurs) et on peut, par exemple, utiliser les résultats démontrés dans Bourbaki, Alg. I, § 6, n^{o} 15. 1

1. Le théorème de Wedderburn

Rappelons qu'une algèbre est dite *simple* si elle est $\neq 0$ et si elle n'a pas d'autres idéaux bilatères qu'elle-même et 0.

Théorème 1. — *Soit* A *une algèbre simple de dimension finie sur un corps commutatif k. Alors* A *est isomorphe à une algèbre de matrices sur un corps gauche qui contient k dans son centre, et est fini sur k.*

Soit E une représentation irréductible de A ; une telle représentation existe : il n'y a qu'à prendre un idéal minimal à gauche de A, par exemple. Soit L(E) l'algèbre des endomorphismes du k-espace vectoriel E, et soit K l'ensemble des éléments de L(E) qui commutent aux opérateurs de A. On a :

Lemme 1 (Schur). — K *est un corps gauche.*

Soit en effet $u \neq 0$, $u \in \mathrm{K}$. Posons $\mathrm{V} = u^{-1}(0)$; si $x \in \mathrm{V}$, on a $0 = au \cdot x = ua \cdot x$ pour tout $a \in \mathrm{A}$, ce qui montre que V est stable par A, et, comme on a supposé que $u \neq 0$, ceci entraîne $\mathrm{V} = 0$, d'où le fait que u est inversible dans L(E) ; il est alors évident que son inverse est dans K.

Ceci démontré, remarquons d'abord que la représentation E est *fidèle* : en effet, le noyau de cette représentation est un idéal bilatère de A qui ne contient pas 1, donc qui est réduit à 0.

Soit alors B le commutant de K dans L(E), i.e. l'ensemble des $b \in \mathrm{L(E)}$ tels que $b \cdot u = u \cdot b$ pour tout $u \in \mathrm{K}$. Il est évident que $\mathrm{A} \subset \mathrm{B}$; en fait, nous allons montrer que $\mathrm{A} = \mathrm{B}$. Quand ceci sera fait, on pourra dire que A n'est autre que l'ensemble des K-*endomorphismes* de E (considéré comme espace vectoriel à gauche sur le corps K), et il en résultera que A est isomorphe à une algèbre de matrices à coefficients dans le corps K° opposé de K.

Reste donc à voir que $\mathrm{A} = \mathrm{B}$. C'est l'objet du lemme plus général suivant :

Lemme 2. — Soit E une représentation complètement réductible et fidèle d'une algèbre A ; *soient* K *le commutant de* A *dans* L(E) *et* B *le commutant de* K *dans* L(E). *On a* $\mathrm{A} = \mathrm{B}$.

Soit d'abord $x \in \mathrm{E}$ et $b \in \mathrm{B}$. Nous allons montrer qu'il existe $a \in \mathrm{A}$ tel que $ax = bx$.

Soit en effet V le sous-espace stable de E défini par $\mathrm{V} = \mathrm{A}x$; il admet un supplémentaire stable (Bourbaki, *loc. cit.*); soit p un projecteur de E sur V. Le projecteur p, étant A-linéaire, appartient à K. On en conclut : $pbx = bpx = bx$, d'où $bx \in \mathrm{V}$, c.q.f.d.

Ce résultat partiel établi, nous allons démontrer le lemme 2. Il résultera tout de suite du suivant :

Lemme 3. — Dans les conditions du lemme 2, soient $x_1, \ldots, x_n \in \mathrm{E}$ *et* $b \in \mathrm{B}$. *Il existe* $a \in \mathrm{A}$ *tel que* $ax_1 = bx_1, \ldots, ax_n = bx_n$.

Soit F l'espace somme directe de n fois la représentation E. On peut considérer F comme formé des éléments $(y_1, \ldots, y_n)$ $(y_i \in \mathrm{E})$ sur lesquels A opère par la formule :

$$a \cdot (y_1, \ldots, y_n) = (ay_1, \ldots, ay_n).$$

La représentation F est complètement réductible. Le commutant de A dans L(F) est formé des matrices $(u_{ij}), u_{ij} \in K$, et il en résulte que, si l'on fait opérer B sur F par la formule :

$$b \cdot (y_1, \ldots, y_n) = (by_1, \ldots, by_n)\,,$$

les éléments de L(F) ainsi définis appartiennent au commutant du commutant de A (le « bicommutant »). En appliquant alors à $x = (x_1, \ldots, x_n) \in F$, et à $b \in B$, le résultat démontré après l'énoncé du lemme 2, on obtient bien le lemme 3, ce qui achève la démonstration.

Nous noterons K_n l'algèbre des matrices à n lignes et n colonnes sur le corps K. Si K contient k dans son centre, on a : $K_n = k_n \otimes K$, comme on le voit aisément.

2. Représentations des algèbres simples

Soit A une algèbre et faisons opérer A sur elle-même par multiplication à gauche. On obtient ainsi une représentation linéaire de A qui est dite représentation régulière gauche. Si A est une algèbre de matrices K_n de base canonique (e_{ij}), les éléments e_{ij} où j est fixé, engendrent un sous-espace vectoriel N_j de A ; on vérifie aisément que N_j est un idéal à gauche minimal, et que les représentations linéaires de A fournies par les différents N_j sont toutes isomorphes. En d'autres termes : la représentation régulière gauche de K_n est la somme de n représentations irréductibles isomorphes. Plus généralement :

THÉORÈME 2. — *Toute représentation d'une algèbre simple* A *est isomorphe à une somme directe de représentations irréductibles toutes isomorphes.*

Soit E une représentation linéaire de A, et soit (e_i) un système fini de générateurs de E $(1 \leqslant i \leqslant p)$. Considérons l'application de A^p sur E définie par :

$$(a_1, \ldots, a_p) \longmapsto a_1e_1 + a_2e_2 + \cdots + a_pe_p\,.$$

Cette application permet d'identifier E à un quotient de A^p (A^p étant considéré comme la somme directe de p fois la représentation régulière gauche de A). Comme le théorème 2 a été vérifié pour A^p, il est donc démontré pour E (BOURBAKI, *loc. cit.*).

COROLLAIRE 1. — *Toute représentation de* A *est complètement réductible.*

COROLLAIRE 2. — *Deux représentations de* A *qui ont même dimension sur* k *sont isomorphes.*

3. Produits tensoriels d'algèbres simples

Donnons d'abord un lemme :

Lemme 4. — Soient A *et* A′ *deux algèbres sur* k*, ayant un élément unité. Soient* B *et* B′ *des sous-algèbres de* A *et* A′ *respectivement,* C *et* C′ *leur commutant dans* A *et* A′*. Alors le commutant de* $\mathrm{B} \otimes \mathrm{B}'$ *dans* $\mathrm{A} \otimes \mathrm{A}'$ *est égal à* $\mathrm{C} \otimes \mathrm{C}'$*.*

Cherchons d'abord le commutant de $\mathrm{B} \otimes 1$. Pour cela, soit a'_i une base de A′. Tout $x \in \mathrm{A} \otimes \mathrm{A}'$ s'écrit d'une seule façon sous la forme :

$$x = \sum_i a_i \otimes a'_i\,, \qquad \text{avec } a_i \in \mathrm{A}\,.$$

Si l'on écrit que x commute avec $b \otimes 1$, on obtient : $a_i b = b a_i$, c'est-à-dire $a_i \in \mathrm{C}$ pour tout i. On voit ainsi que le commutant de $\mathrm{B} \otimes 1$ n'est autre que $\mathrm{C} \otimes \mathrm{A}'$. De même, celui de $1 \otimes \mathrm{B}'$ est $\mathrm{A} \otimes \mathrm{C}'$. Il en résulte que le commutant de $\mathrm{B} \otimes \mathrm{B}'$ est égal à l'intersection des commutants de $\mathrm{B} \otimes 1$ et $1 \otimes \mathrm{B}'$, c'est-à-dire à $(\mathrm{C} \otimes \mathrm{A}') \cap (\mathrm{A} \otimes \mathrm{C}') = \mathrm{C} \otimes \mathrm{C}'$, c.q.f.d.

De ce lemme résulte par exemple que le centre d'un produit tensoriel est le produit tensoriel des centres. En appliquant ceci à une algèbre simple (de rang fini) : $\mathrm{A} = k_n \otimes \mathrm{K}$, on voit que le centre de A est $k \otimes \mathrm{C}$, C désignant le centre de K. D'où :

Corollaire. — *Le centre d'une algèbre simple, finie sur* k*, est un corps* (commutatif)*.*

On s'intéressera particulièrement par la suite aux algèbres de centre k. Une telle algèbre sera dite *centrale.*

Théorème 3. — *Soient* A *et* A′ *deux algèbres simples, finies sur* k*, dont l'une est centrale. Alors le produit tensoriel* $\mathrm{A} \otimes \mathrm{A}'$ *est une algèbre simple.*

Supposons que $\mathrm{A}' = k_n \otimes \mathrm{K}'$ soit centrale, autrement dit que le centre du corps gauche K′ soit réduit à k. Il suffira de voir que $\mathrm{A} \otimes \mathrm{K}'$ est une algèbre simple. En effet, si ceci est démontré, on aura $\mathrm{A} \otimes \mathrm{K}' = k_m \otimes \mathrm{K}''$ où K″ est un corps, et $\mathrm{A} \otimes \mathrm{A}' = k_m \otimes k_n \otimes \mathrm{K}'' = k_{mn} \otimes \mathrm{K}'' = \mathrm{K}''_{mn}$. L'algèbre $\mathrm{A} \otimes \mathrm{A}'$ sera donc isomorphe à une algèbre de matrices pour laquelle la simplicité se vérifie immédiatement. Reste donc à voir $\mathrm{A} \otimes \mathrm{K}'$ est simple. Cela résulte du théorème :

Théorème 4. — *Soient* A *une algèbre sur* k *et* K′ *un corps gauche de centre* k*. Tout idéal bilatère* N *de* $\mathrm{A} \otimes \mathrm{K}'$ *est engendré* (en tant qu'espace vectoriel à

gauche sur K′), *par son intersection avec* A ⊗ 1. (Ni A ni K′ ne sont supposés finis sur k.)

Notons d'abord que l'on peut faire opérer K′ à gauche sur A ⊗ K′ par :

$$k'(a \otimes k'') = a \otimes k'k'' .$$

Si N est un idéal bilatère de l'algèbre A ⊗ K′, c'est en particulier un K′-*sous-espace vectoriel à gauche de* A ⊗ K′.

Soit a_i une base de A sur k ; les éléments $a_i \otimes 1$ forment également une base du K′-espace vectoriel A ⊗ K′. Soit x un élément *primordial* de N par rapport 2
à cette base (BOURBAKI, Alg. II, § 5) :

$$x = \sum_i a_i \otimes k'_i .$$

Considérons l'élément $x \cdot m$ ($m \in$ K′) ; on a $x \cdot m \in$ N (N est un idéal bilatère), et d'autre part :

$$x \cdot m = \sum_i a_i \otimes k'_i m .$$

Il résulte alors des propriétés des éléments primordiaux qu'il existe $n \in$ K′ tel que

$$k'_i m = n k'_i \text{ pour tout } i.$$

Comme l'un des k'_i est égal à 1, on a $m = n$, et l'égalité précédente signifie que k'_i commute avec tout $m \in$ K′, i.e. que $k'_i \in k$. On peut alors écrire $x = a \otimes 1$, en posant $a = \sum_i k'_i a_i$. On a donc montré que *tout élément primordial x est dans* A ⊗ 1 ; le théorème en résulte aussitôt puisque tout sous-espace vectoriel est engendré par ses éléments primordiaux.

COROLLAIRE 1. — *Le produit tensoriel de deux algèbres simples centrales et finies sur k est du même type.*

COROLLAIRE 2. — *Soit* A *une algèbre centrale simple, de centre k, et telle que* $[A : k] = n$. *Si* A° *désigne l'algèbre opposée, on a* :

$$A \otimes A^\circ = k_{n^2}$$

(algèbre des matrices à n^2 lignes et n^2 colonnes, sur le corps k).

Désignons par E l'algèbre A considérée comme espace vectoriel sur k. On peut faire opérer A sur E par multiplication à gauche ou par multiplication à droite. Cela revient à identifier A et A° à des sous-algèbres de l'algèbre L(E) des k-endomorphismes de E. Comme les algèbres A et A° commutent dans L(E), on peut définir un homomorphisme canonique de A ⊗ A° dans L(E) qui

prolonge les injections : $A \to L(E)$ et $A^\circ \to L(E)$. L'algèbre $A \otimes A^\circ$ étant simple (th. 3), cet homomorphisme est injectif; comme en outre :

$$[A \otimes A^\circ : k] = [A : k]^2 = n^2 = [L(E) : k],$$

c'est un isomorphisme de $A \otimes A^\circ$ sur $L(E) = k_{n^2}$, c.q.f.d.

Remarque. — Si aucune des deux algèbres A et A′ du théorème 3 n'est centrale, l'algèbre $A \otimes A'$ n'est pas simple en général. Toutefois, si le centre de A, par exemple, est une extension *galoisienne* de k, on montre que $A \otimes A'$ est un produit direct d'algèbres simples.

4. Groupe de Brauer. Définition

Soit A une algèbre simple sur k, centrale et finie sur k. D'après le théorème de Wedderburn, on a : $A = k_n \otimes K$, où K est un corps gauche de centre k fini sur k. *Le corps gauche* K *est bien déterminé par* A, à k-isomorphisme près. En effet, on peut le caractériser comme l'opposé du commutant de A dans une représentation irréductible quelconque de A (et on sait que deux telles représentations sont isomorphes). Nous pouvons donc parler *du* corps gauche associé à une algèbre A.

Nous dirons que deux algèbres centrales sur k, A et A′ sont *semblables* lorsque les corps gauches associés à A et A′ sont les mêmes (à k-isomorphisme près). Cette relation de similitude partage les algèbres centrales sur k en *classes*, qui correspondent biunivoquement aux corps gauches de centre k et finis sur k.

Nous allons munir cet ensemble de classes d'une loi de *groupe* : si B et B′ sont deux classes, et A et A′ des éléments de ces classes, on voit tout de suite que les algèbres $A \otimes A'$ sont toutes contenues dans une même classe, que nous appellerons le *produit* des classes B et B′.

La classe qui contient l'algèbre $A = k$ est évidemment l'élément neutre de cette loi de produit ; c'est la classe formée de toutes les algèbres de matrices sur k.

Le produit des classes est *commutatif*, puisque $A \otimes A'$ est k-isomorphe à $A' \otimes A$; on montre de même qu'il est *associatif*.

Si A parcourt une classe de B, les algèbres opposées A° parcourent une classe B° qui n'est autre que l'inverse de B (cor. 2 au th. 4). En résumé :

THÉORÈME 5. — *Les classes d'algèbres simples, centrales et finies sur k, munies de la loi de composition du produit tensoriel, forment un groupe abélien.*

Ce groupe est appelé le *groupe de Brauer* de k, et nous le noterons Br_k.

5. Groupe de Brauer. Exemples

a) k est *algébriquement clos*. Alors $\mathrm{Br}_k = 0$.

Soit en effet K un corps gauche de centre k, fini sur k ; nous devons montrer que $\mathrm{K} = k$. Sinon, il existerait $x \in \mathrm{K}, x \notin k$. Soit C le corps engendré par x et k; c'est un corps commutatif (puisque k et x commutent), extension finie de k ; donc $\mathrm{C} = k$, ce qui est absurde.

b) $k = \mathbf{R}$, *corps des réels*. Alors $\mathrm{Br}_{\mathbf{R}} = \mathbf{Z}/2\mathbf{Z}$.

On connaît un corps de centre $\mathbf{R}$, non réduit à $\mathbf{R}$: le corps K des quaternions. Nous verrons au n° 13 que c'est le seul. Il en résultera bien que $\mathrm{Br}_{\mathbf{R}} = \mathbf{Z}/2\mathbf{Z}$.

c) k est un corps *fini*. Alors $\mathrm{Br}_k = 0$.

Voir n° 13.

d) k est un corps p-adique $\mathbf{Q}_p$. Alors $\mathrm{Br}_k = \mathbf{Q}/\mathbf{Z}$ (« rationnels mod 1 »).

Voir DEURING (*Algebren*, Chap. VII, § 2).

e) $k = \mathbf{Q}$, corps des *rationnels*. Alors $\mathrm{Br}_{\mathbf{Q}}$ est un certain sous-groupe de la somme directe $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Q}/\mathbf{Z} \oplus \mathbf{Q}/\mathbf{Z} \oplus \cdots$. 3

Voir DEURING, *loc. cit.* § 5, ainsi que S. WANG, *Annals* 1950.

Les deux derniers exemples montrent que le groupe de Brauer d'un corps k peut être assez compliqué ; mais dans les deux cas, on peut remarquer qu'il est limite inductive de sous-groupes bien plus simples [par exemple dans le cas d), de sous-groupes cycliques]. Ce sont ces sous-groupes que nous allons étudier dans la suite, et ramener à des groupes de cohomologie.

6. Extension du corps de base

THÉORÈME 6. — *Soit* A *une algèbre simple, centrale et finie sur* k, L *un corps commutatif, extension de* k (finie ou infinie). *L'algèbre* $\mathrm{A} \otimes \mathrm{L}$ *est simple.*

Si A est un corps gauche, on peut appliquer le théorème 4 : tout idéal bilatère de $\mathrm{A} \otimes \mathrm{L}$ est engendré par son intersection avec L, qui est (0) ou L, donc $\mathrm{A} \otimes \mathrm{L}$ est simple.

Si A est quelconque, on peut écrire $\mathrm{A} = k_n \otimes \mathrm{K}$, où K est un corps, d'où :

$$\mathrm{A} \otimes \mathrm{L} = k_n \otimes (\mathrm{K} \otimes \mathrm{L}) = k_n \otimes \mathrm{K}'_m \,,$$

K' étant un autre corps gauche. Il en résulte :

$$\mathrm{A} \otimes \mathrm{L} = \mathrm{K}'_{mn} \,,$$

d'où le théorème.

COROLLAIRE. — *Soit* A *une algèbre simple, centrale et finie sur* k. *Alors* $[\mathrm{A} : k]$ *est un carré.*

Prenons pour L une extension algébriquement close de k. L'algèbre $\mathrm{A} \otimes \mathrm{L}$ peut être munie d'une structure d'algèbre sur L, et l'on a :

$$[\mathrm{A} \otimes \mathrm{L} : \mathrm{L}] = [\mathrm{A} : k] .$$

Mais $\mathrm{A} \otimes \mathrm{L}$ est une algèbre simple, centrale sur L, et finie sur L. Il résulte alors de 5-a) que c'est une algèbre de matrices sur L, et $[\mathrm{A} \otimes \mathrm{L} : \mathrm{L}]$ est bien un carré.

A toute algèbre centrale, simple et finie sur k, soit A, faisons correspondre son produit tensoriel avec L, considéré comme algèbre centrale, simple et finie sur L. Autrement dit, étendons le corps de base de A de k à L. Il est clair que deux algèbres semblables restent semblables : on obtient ainsi une application canonique $\varphi_{k,\mathrm{L}}$ du groupe de Brauer Br_k dans le groupe de Brauer Br_L. Je dis que $\varphi_{k,\mathrm{L}}$ est un *homomorphisme*. Cela résulte de la formule :

$$(\mathrm{A} \otimes_k \mathrm{L}) \otimes_\mathrm{L} (\mathrm{A}' \otimes_k \mathrm{L}) = (\mathrm{A} \otimes_k \mathrm{A}') \otimes_k \mathrm{L} ,$$

où $\otimes_k$ et $\otimes_\mathrm{L}$ désignent les produits tensoriels pris sur k et sur L respectivement. Nous désignerons le noyau de $\varphi_{k,\mathrm{L}}$ par $\mathrm{H}_{k,\mathrm{L}}$. C'est un sous-groupe du groupe de Brauer Br_k, le sous-groupe formé des classes d'algèbres qui deviennent des algèbres de matrices quand on étend le corps de base à L. On dit aussi que ce sont les algèbres qui admettent L comme *corps de décomposition* (ou qui sont *neutralisées* par L).

Toute algèbre A admet L pour corps de décomposition si L est algébriquement clos, puisqu'alors $\mathrm{Br}_\mathrm{L} = (0)$. En fait, des extensions finies suffisent :

THÉORÈME 7. — *Le groupe* Br_k *est réunion des sous-groupes* $\mathrm{H}_{k,\mathrm{L}}$ *où* L *parcourt l'ensemble des extensions finies de* k.

Soit A une algèbre de base (e_i), de table de multiplication (c_{ijk}) ; nous devons montrer qu'il existe une extension finie L de k, telle que $\mathrm{A} \otimes \mathrm{L}$ soit une algèbre de matrices sur L. On sait que ceci est réalisé si on prend pour corps une extension algébriquement close M de k. Ceci signifie qu'il existe des $m_{ij} \in \mathrm{M}$ tels que $\sum m_{ij} e_j = \mathrm{E}_i$ aient pour table de multiplication la table bien connue des algèbres de matrices. Soit $\mathrm{L} = (k, m_{i,j})$ le corps obtenu en adjoignant à k les m_{ij}; il est clair que L répond à la question.

Remarque. — On peut montrer qu'il suffit de considérer les extensions qui sont *galoisiennes* sur k, cf. no 10.

7. Le théorème de Skolem-Noether

THÉORÈME 8. — *Soit* A *une algèbre simple finie et centrale sur* k ; *soient* f *et* g *deux* k*-homomorphismes d'une algèbre simple* B *dans* A. *Il existe alors un élément inversible* $x \in \mathrm{A}$, *tel que* $f(b) = x \cdot g(b) \cdot x^{-1}$ *pour tout* $b \in \mathrm{B}$.

Si A est une algèbre de matrices sur k, le théorème précédent signifie que deux représentations matricielles de B de même degré sont isomorphes, ce qui a déjà été démontré (cor. 2 au th. 2).

Dans le cas général, soit A° l'algèbre opposée de A ; formons $\mathrm{B} \otimes \mathrm{A}^\circ$ et $\mathrm{A} \otimes \mathrm{A}^\circ$, et prolongeons f et g en des homomorphismes f' et g' de la première algèbre dans la seconde, en posant :

$$f'(b \otimes a) = f(b) \otimes a, \quad g'(b \otimes a) = g(b) \otimes a \qquad (b \in \mathrm{B},\ a \in \mathrm{A}^\circ)\,.$$

Comme $\mathrm{A} \otimes \mathrm{A}^\circ$ est une algèbre de matrices sur k (cor. 2 au th. 4), il existe, d'après la première partie de la démonstration, un $x \in \mathrm{A} \otimes \mathrm{A}^\circ$ tel que :

$$f'(b \otimes a) = x \cdot g'(b \otimes a) \cdot x^{-1}\,.$$

Si l'on prend $b = 1$, on voit que x commute aux éléments de la forme $1 \otimes a$ ($a \in \mathrm{A}^\circ$), donc appartient à $\mathrm{A} \otimes 1$ (Lemme 4), et on peut l'écrire $x \otimes 1$, avec $x \in \mathrm{A}$. On a alors :

$$f(b) = x \cdot g(b) \cdot x^{-1}\,, \qquad \text{c.q.f.d.}$$

COROLLAIRE. — *Tout* k*-automorphisme d'une algèbre simple finie et centrale sur* k *est un automorphisme intérieur.*

8. La commutation dans les algèbres simples

THÉORÈME 9. — *Soit* A *une algèbre simple, finie et centrale sur* k. *Soient* B *une sous-algèbre simple de* A, *et* C *le commutant de* B *dans* A. *Alors* C *est simple,* B *est le commutant de* C, *et* $[\mathrm{B} : k] \cdot [\mathrm{C} : k] = [\mathrm{A} : k]$.

Désignons par E l'algèbre B considérée comme k-espace vectoriel, et soit L(E) l'algèbre des k-endomorphismes de E. On peut faire opérer B sur E par multiplication à gauche : cela revient à plonger B dans L(E). On sait que le commutant de B dans L(E) n'est autre que l'algèbre des multiplications à droite de E, isomorphe à B°.

Ceci étant, considérons l'algèbre simple $\mathrm{A} \otimes \mathrm{L(E)}$. On peut y plonger B de deux façons : par $\mathrm{B} \otimes 1$ et par $1 \otimes \mathrm{B}$. Le commutant de $\mathrm{B} \otimes 1$ est $\mathrm{C} \otimes \mathrm{L(E)}$, et celui de $1 \otimes \mathrm{B}$ est $\mathrm{A} \otimes \mathrm{B}^\circ$ (Lemme 4).

Mais d'après le théorème 8, il existe un automorphisme intérieur de $\mathrm{A} \otimes \mathrm{L(E)}$ qui transforme $\mathrm{B} \otimes 1$ en $1 \otimes \mathrm{B}$; cet automorphisme transforme donc aussi les

commutants de ces deux algèbres l'un dans l'autre, et, en particulier, ces deux algèbres sont isomorphes.

Il en résulte d'abord que $C \otimes L(E)$ est simple puisque $A \otimes B^\circ$ l'est, donc C est simple.

D'autre part :

$$[C \otimes L(E) : k] = [C : k]\cdot[B : k]^2 \quad \text{et} \quad [A \otimes B^\circ : k] = [A : k]\cdot[B : k].$$

D'où :
$$[A : k] = [B : k]\cdot[C : k].$$

Si B' désigne le commutant de C dans A, on a $B' \supset B$. Mais d'après ce qui vient d'être démontré : $[A : k] = [C : k]\cdot[B' : k]$, d'où $[B : k] = [B' : k]$ et $B = B'$.

Corollaire 1. — *Si* B *est centrale sur* k, B *et* C *sont linéairement disjoints sur* k, *et* $A = B \otimes C$.

Les centres de B et de C sont égaux à $B \cap C$, donc sont réduits à k. L'algèbre $B \otimes C$ est donc simple et centrale sur k, et l'homomorphisme canonique de cette algèbre sur le produit de B et de C dans A est un isomorphisme. Comme $B \otimes C$ et A ont même dimension, cet isomorphisme applique $B \otimes C$ *sur* A.

Corollaire 2. — *Soit* L *un sous-corps commutatif d'une algèbre* A *simple, finie et centrale sur* k. *Pour que* L *soit son propre commutant dans* A, *il faut et il suffit que* $[A : k] = [L : k]^2$ *ou que* L *soit un sous-anneau commutatif maximal de* A.

Soit L' le commutant de L dans A ; puisque L est commutatif, on a $L' \supset L$. D'après le th. 9, il est clair que $L' = L$ équivaut à :

$$[L : k]^2 = [A : k]\,.$$

D'autre part, si $L' = L$, tout sous-anneau commutatif de A contenant L est contenu dans L', donc égal à L, et L est un sous-anneau commutatif maximal de A. Réciproquement, s'il en est ainsi, tout élément commutant à L est dans L, d'où $L' = L$.

Corollaire 3. — *Tout sous-corps commutatif maximal* L *d'un corps gauche* D *est tel que* $[L : k]^2 = [D : k]$.

Résulte du corollaire précédent et du fait que tout sous-anneau de D est un sous-corps.

9. Le critère de décomposition

Soient k un corps commutatif, Br_k le groupe de Brauer de k et W un élément de Br_k, c'est-à-dire une classe d'algèbres simples, finies et centrales sur k. Si L est une extension de k, rappelons que L est dit *corps de décomposition* de W si l'image de W dans Br_L est 0.

THÉORÈME 10. — *Les deux conditions suivantes sont équivalentes* :

a) L *est un corps de décomposition de* W ;

b) *Il existe* $\mathrm{A} \in \mathrm{W}$, *avec* $\mathrm{L} \subset \mathrm{A}$ *et* $[\mathrm{A} : k] = [\mathrm{L} : k]^2$.

a) $\Rightarrow$ b) – Soit $\mathrm{B} \in \mathrm{W}$; puisque L est corps de décomposition de B, il l'est aussi de B° et $\mathrm{B}^\circ \otimes \mathrm{L}$ est une algèbre de matrices sur L, ou encore l'algèbre $\mathrm{L}(\mathrm{E}_\mathrm{L})$ des endomorphismes d'un L-espace vectoriel E_L. Soit E l'algèbre des k-endomorphismes de E_L. L'algèbre B° se trouve donc plongée dans L(E), et son algèbre commutante est L (c'est ce qui exprime le fait que $\mathrm{B}^\circ \otimes \mathrm{L}$ est l'algèbre des L-endomorphismes de E_L). Soit A l'algèbre commutante de B° dans L(E). Je dis que A répond aux conditions imposées.

Tout d'abord, il est clair que A contient L, et que A est une algèbre simple. En outre $[\mathrm{B} : k]\cdot[\mathrm{A} : k] = [\mathrm{L}(\mathrm{E}) : k] = [\mathrm{B}^\circ \otimes \mathrm{L} : k]\cdot[\mathrm{L} : k]$, d'où

$$[\mathrm{A} : k] = [\mathrm{L} : k]^2 .$$

Enfin, d'après le corollaire 1 au th. 9, A est centrale sur k et $\mathrm{B}^\circ \otimes \mathrm{A} = \mathrm{L}(\mathrm{E})$; ceci montre que la classe de A est l'opposée de celle de B°, donc est W.

b) $\Rightarrow$ a) – Il suffit de montrer que A est décomposée par L. Pour cela, remarquons que, d'après le corollaire 2 au th. 4, on a $\mathrm{A} \otimes \mathrm{A}^\circ = \mathrm{L}(\mathrm{V})$, algèbre des k-endomorphismes de l'espace vectoriel V. Plongeons L dans A° ; son commutant dans L(V) est alors $\mathrm{A} \otimes \mathrm{L}$. Mais ceci signifie que $\mathrm{A} \otimes \mathrm{L}$ est l'algèbre des L-endomorphismes de V, et W est bien décomposée par L.

COROLLAIRE 1. — *Tout sous-corps commutatif maximal d'un corps gauche* D *est corps de décomposition de* D.

Résulte immédiatement du corollaire 3 au th. 9.

COROLLAIRE 2. — *Soit* D *un corps gauche et posons* $[\mathrm{D} : k] = r^2$. *Pour tout corps de décomposition* L *de* D, $[\mathrm{L} : k]$ *est un multiple de* r.

L'algèbre A du théorème précédent est une algèbre de matrices d'ordre n sur D. On a donc $[\mathrm{A} : k] = n^2 r^2$, d'où $[\mathrm{L} : k] = nr$.

Remarque. — Il ne faudrait pas croire cependant que tout corps de décomposition de D contienne un sous-corps commutatif maximal de D, ni que les sous-corps commutatifs maximaux de D soient isomorphes.

10. Existence de corps de décomposition galoisiens

Lemme 5. — Soit D *un corps gauche fini sur son centre k, et distinct de k. Il existe un sous-corps commutatif* M *de* D *sur k, séparable sur k, et distinct de k.*

Sinon tout élément de D est radiciel sur k, c'est-à-dire vérifie la condition :

$$x^{p^e} \in k \text{ pour au moins un } e\,.$$

Comme D est fini sur k, on voit tout de suite qu'il existe un entier e tel que l'équation précédente ait lieu pour tout $x \in \mathrm{D}$.

Soit alors e_i une base de D sur k, telle que $e_1 = 1$. Si l'on écrit un élément $x \in \mathrm{D}$ sous la forme $x = \sum_i x_i e_i$, l'élément x^{p^e} s'écrit sous la forme :

$$x^{p^e} = \sum_j \mathrm{P}_j(x_i) e_j\,,$$

où les P_j sont des polynômes par rapport aux x_i dont les coefficients s'expriment au moyen des éléments de la table de multiplication de D. Par hypothèse, on a $\mathrm{P}_j(x_i) = 0$ $(j \neq 1)$ pour tout système de valeurs des x_i. Comme on peut supposer que k est *infini* (puisque toute extension finie d'un corps fini est séparable), ceci montre que les P_j $(j \neq 1)$ sont tous identiquement nuls.

Mais alors, on a encore la même condition : $x^{p^e} \in k$ lorsqu'on étend le corps de base. En particulier, étendons-le à une clôture algébrique de k; on obtient une algèbre de matrices qui contient des idempotents x qui mettent en défaut le résultat précédent. Ceci achève la démonstration.

Théorème 11. — *Tout corps gauche* D*, fini sur son centre k, contient un sous-corps commutatif maximal qui est séparable sur k.*

Soit L un sous-corps séparable maximal de D. Montrons que L est un sous-corps commutatif maximal de D ; pour cela, soit D' le commutant de L dans D; c'est un corps gauche, de centre L. S'il n'était pas confondu avec L, il y aurait, d'après le lemme, un corps L', avec $\mathrm{L} \subset \mathrm{L}' \subset \mathrm{D}'$, $\mathrm{L} \neq \mathrm{L}'$, et L' séparable sur L. Mais alors L' serait séparable sur k, ce qui est contraire au caractère maximal de L. Il en résulte que $\mathrm{D}' = \mathrm{L}$, et L est bien un sous-corps commutatif maximal de D.

Corollaire. — *Tout* $\mathrm{W} \in \mathrm{Br}_k$ *admet un corps de décomposition qui est galoisien sur k.*

Il suffit de le voir pour un corps gauche D. Or, d'après le th. 11 et le cor. 1 au th. 10, D admet un corps de décomposition L qui est séparable sur k. Si

L' désigne une extension galoisienne quelconque de k qui contienne L (et il y en a), L' est *a fortiori* corps de décomposition de D.

11. Correspondance entre algèbres simples et extensions de groupes

Soit k un corps, L une extension galoisienne et finie de k ; nous allons étudier le sous-groupe $H_{k,L}$ de Br_k formé des classes d'algèbres simples centrales et finies sur k qui admettent L pour corps de décomposition.

Soit G le groupe de Galois de L/k, L^* le groupe multiplicatif des éléments non nuls de L. Le groupe G *opère* sur L^*, et on peut définir le groupe $Q(G, L^*)$ des extensions de G par L^* (*voir* Exposé 5).

THÉORÈME 12. — *Les groupes* $H_{k,L}$ *et* $Q(G, L^*)$ *sont isomorphes.*

Ce théorème sera démontré dans ce n° et dans le suivant.

Nous allons commencer par définir une application $u : H_{k,L} \to Q(G, L^*)$. Si $W \in H_{k,L}$, il existe, d'après le théorème 10 une algèbre $A \in W$ contenant L et telle que $[A : k] = [L : k]^2$. Cette algèbre est donc bien déterminée, à k-isomorphisme près. Plongeons L dans A, ce que nous savons être possible, et soit E l'ensemble des éléments inversibles de A qui définissent des automorphismes intérieurs laissant stable L. Autrement dit, $x \in E$ signifie que $x \cdot L \cdot x^{-1} = L$.

Un tel élément définit un automorphisme de L/k, c'est-à-dire un élément $g \in G$. Je dis que la suite :

$$1 \longrightarrow L^* \longrightarrow E \longrightarrow G \longrightarrow 1$$

est *exacte* (les deux homomorphismes étant, le premier, l'injection de L^* dans E, et le second, celui qui vient d'être défini). Il y a deux choses à vérifier :

a) que $E \longrightarrow G$ est surjectif. Ceci signifie que tout k-automorphisme peut être prolongé en un automorphisme intérieur de A, ce qui résulte du th. 8.

b) que le noyau de $E \longrightarrow G$ n'est autre que L^*. Ceci signifie que les seuls éléments de E qui commutent à L^* sont les éléments de L^*, ce qui résulte du corollaire 2 au th. 9.

Le groupe E définit un élément $u(W) \in Q(G, L^*)$. Il résulte du th. 8 que cet élément ne dépend pas de la façon dont on a plongé L dans A.

Lemme 6. — L'application $u : H_{k,L} \to Q(G, L^*)$ *définie ci-dessus est un homomorphisme.*

(Nous utiliserons la définition de la multiplication dans $Q(G, L^*)$ donnée par BAER — *Voir* Appendice.)

Soient $W, W', W'' = W + W' \in H_{k,L}$, et soient $B \in W$, $B \in W'$, $B \otimes B' \in W''$.

Les algèbres $B^\circ \otimes L$ et $B'^\circ \otimes L$ sont isomorphes aux algèbres des L-endomorphismes des L-espaces vectoriels, V et V'. Il en résulte que $B^\circ \otimes B'^\circ \otimes L$ est isomorphe à l'algèbre des L-endomorphismes de $V \otimes_L V' = V''$.

Cherchons les algèbres A, A', A'', telles que $A \in W, A' \in W', A'' \in W''$ et que

$$[A : k] = [A' : k] = [A'' : k] = [L : k]^2.$$

D'après la démonstration du théorème 10, on peut les obtenir en prenant les k-endomorphismes de V, V' et V'' qui commutent avec $B^\circ, B'^\circ, B^\circ \otimes B'^\circ$ respectivement.

Désignons par E, E', E'' les éléments inversibles de A, A', A'' qui définissent des automorphismes intérieurs laissant L stable. Soient $u \in E, \lambda \in L, x \in V$, et notons λ^g le transformé de λ par l'image g de u dans G, groupe de Galois de L/k. Par définition, on a :

$$u\lambda u^{-1} = \lambda^g .$$

En appliquant ceci à $u(x)$, on obtient $u(\lambda x) = \lambda^g u(x)$, ce qui exprime que u est *semi-linéaire relativement à* g. On peut donc donner une autre caractérisation de E : E est formé des automorphismes semi-linéaires de V qui commutent à B°. Idem pour E' et E''.

Soient alors $u \in E, u' \in E'$, définissant le même élément $g \in G$. On peut définir l'opérateur $u \otimes u'$ sur $V \otimes_L V'$ par la formule :

$$(u \otimes u')(x \otimes x') = u(x) \otimes u'(x') .$$

Soit (E, E') le sous-groupe de $E \times E'$ formé des éléments ayant même projection dans G. L'application $(u, u') \mapsto u \otimes u'$ définit un homomorphisme de (E, E') dans E'', car on voit tout de suite que les automorphismes $u \otimes u'$ sont semi-linéaires relativement au même g, et commutent à $B^\circ \otimes B'^\circ$. Soit E_1 l'image de (E, E') par cette application. E_1 contient évidemment les homothéties par les éléments de L^*, et, pour tout $g \in G$, contient des éléments g-semi-linéaires. Il en résulte que $E_1 = E''$. D'autre part, le noyau de $(E, E') \to E''$ contient les couples $(\lambda, \lambda^{-1}), \lambda \in L^*$, et *rien d'autre* comme on le voit immédiatement. Il s'ensuit que E'' est obtenu à partir de E et E' par le procédé de Baer, ce qui achève la démonstration.

12. Construction d'un produit croisé

Nous allons maintenant procéder en sens inverse et définir une application

$$v : \mathrm{Q}(\mathrm{G}, \mathrm{L}^*) \longrightarrow \mathrm{H}_{k,\mathrm{L}}.$$

Pour cela, soit donnée une suite exacte :

$$1 \longrightarrow \mathrm{L}^* \longrightarrow \mathrm{E} \longrightarrow \mathrm{G} \longrightarrow 1\,.$$

Nous allons construire à partir de là une algèbre A, dite *produit croisé* de L/k par E.

Construction — Soit $\mathbf{Z}(\mathrm{E})$ l'algèbre de E sur l'anneau $\mathbf{Z}$ des entiers ; tout élément $z \in \mathbf{Z}(\mathrm{E})$ peut s'écrire d'une et d'une seule façon sous la forme : 4

$$z = \sum_x n_x \mathrm{X}_x, \quad n_x \in \mathbf{Z}, \quad x \in \mathrm{E}\,.$$

En particulier, les éléments X_λ sont définis si $\lambda \in \mathrm{L}^*$.
Considérons l'idéal bilatère $\mathfrak{a}$ engendré par :

$$(1) \qquad \begin{cases} \mathrm{X}_\lambda + \mathrm{X}_\mu - \mathrm{X}_{\lambda+\mu} & \lambda, \mu, \lambda+\mu \in \mathrm{L}^*\,, \\ \mathrm{X}_\lambda + \mathrm{X}_{-\lambda} & \lambda \in \mathrm{L}^*\,. \end{cases}$$

THÉORÈME 13. — *L'anneau quotient* $\mathrm{A} = \mathbf{Z}(\mathrm{E})/\mathfrak{a}$ *contient* L *et a pour centre* k ; *en outre c'est une algèbre simple sur* k, *telle que* $[\mathrm{A} : k] = [\mathrm{L} : k]^2$.

Remarquons d'abord que $\mathfrak{a}$ est égal à l'idéal à gauche engendré par les éléments de la forme (1). En effet, on a :

$$(\mathrm{X}_\lambda + \mathrm{X}_{-\lambda}) \cdot \mathrm{X}_x = \mathrm{X}_x \cdot (\mathrm{X}_{x^{-1}\lambda x} + \mathrm{X}_{-x^{-1}\lambda x})\,,$$
$$(\mathrm{X}_\lambda + \mathrm{X}_\mu - \mathrm{X}_{\lambda+\mu}) \cdot \mathrm{X}_x = \mathrm{X}_x \cdot (\mathrm{X}_{x^{-1}\lambda x} + \mathrm{X}_{x^{-1}\mu x} + \mathrm{X}_{x^{-1}(\lambda+\mu)x})\,.$$

Soit maintenant $g \in \mathrm{G}$, et notons I_g l'ensemble des $x \in \mathrm{E}$ se projetant sur g, M_g le sous-groupe de $\mathbf{Z}(\mathrm{G})$ engendré par les éléments de I_g, N_g l'image de M_g dans $\mathrm{A} = \mathbf{Z}(\mathrm{E})/\mathfrak{a}$.

$\mathbf{Z}(\mathrm{E})$ est somme directe des $\mathrm{M}_g, g \in \mathrm{G}$. Je dis que $\mathfrak{a}$ est aussi somme directe des $\mathfrak{a} \cap \mathrm{M}_g$. Il suffit de voir que $\mathfrak{a}$ est engendré par les $\mathfrak{a} \cap \mathrm{M}_g$. Or $\mathfrak{a}$ est engendré par les produits des X_x et des éléments de la forme (1) ; comme chacun de ces produits est contenu dans un M_g, il en résulte que $\mathfrak{a}$ est bien engendré (en tant que groupe abélien) par ceux de ses éléments qui sont dans l'un des M_g. Il en résulte que A *est somme directe des* $\mathrm{N}_g, g \in \mathrm{G}$. Nous allons déterminer ces N_g.

Tout élément de M_g est congru modulo $\mathfrak{a}$ à 0 ou à un $X_x, x \in I_g$. En effet, il suffit de le voir pour $X_x + \varepsilon X_y$, avec $\varepsilon = \pm 1$. Or $y = \lambda x$, $\lambda \in L^*$, et on a donc :

$$\begin{cases} X_x + \varepsilon X_y \equiv X_{1+\varepsilon\lambda} \text{ mod. } \mathfrak{a} & \text{si } 1 + \varepsilon\lambda \neq 0, \\ X_x + \varepsilon X_y \equiv 0 \text{ mod. } \mathfrak{a} & \text{si } 1 + \varepsilon\lambda = 0\,. \end{cases}$$

Montrons qu'une telle représentation est unique : soit $x_0 \in I_g$ et écrivons tout $y \in I_g$ sous la forme : $y = \lambda_y \cdot x_0$, $\lambda_y \in L^*$. A tout $z \in M_g$ faisons correspondre un élément $u(z) \in L$, en prolongeant par linéarité l'application $y \mapsto \lambda_y$. Un calcul immédiat montre que $u(z)$ est nul pour tout $z \in \mathfrak{a} \cap M_g$. Il en résulte que $u(z)$ prend la même valeur pour deux éléments z, z' congrus modulo $\mathfrak{a}$. En appliquant cela à X_x et $X_{x'}$, $x \neq x'$, on voit que X_x et $X_{x'}$ ne sont pas congrus mod. $\mathfrak{a}$, et ne sont pas non plus congrus à 0. D'où l'unicité cherchée. Nous avons donc démontré ceci :

A *est somme directe des* N_g ; *chaque* N_g *peut être considéré comme la réunion de* I_g *et d'un élément noté* 0. *L'addition est définie dans* N_g *par transport par translation à partir de l'addition de* L. *La multiplication est celle de* E.

(On aurait pu prendre ce qui précède comme définition de A.)

En particulier, les éléments de N_1 forment un sous-anneau de A isomorphe à L, et on a : $[A : k] = [L : k] \cdot (\text{ordre de G}) = [L : k]^2$.

L est son propre commutant dans A et k est le centre de A.

Reste à voir que A est *simple*. Pour cela, soit $u_g (g \in G)$ un élément quelconque $\neq 0$ de N_g. Les u_g forment une base de A considéré comme L-espace vectoriel à gauche. Si $\mathfrak{m}$ est un idéal bilatère de A, soit $x = \sum_g \lambda_g u_g$ un élément primordial de $\mathfrak{m}$ par rapport aux u_g. Soit $\mu \in L$, et formons $x \cdot \mu \in \mathfrak{m}$. On a :

$$x \cdot \mu = \sum_g \lambda_g \cdot u_g \cdot \mu = \sum_g \lambda_g \cdot \mu^g \cdot u_g\,.$$

D'après les propriétés des éléments primordiaux, il en résulte que μ^g ne dépend pas de g, lorsque g est tel que $\lambda_g \neq 0$. Ceci exige qu'il n'y ait qu'un seul g jouissant de cette propriété, et l'élément u_g correspondant est alors dans $\mathfrak{m}$. Comme u_g est inversible, ceci entraîne $\mathfrak{m} = A$, c.q.f.d.

Le théorème précédent nous permet de définir une application canonique

$$v : Q(G, L^*) \longrightarrow H_{k,L}\,.$$

On a : $u \circ v = 1$.

Ceci signifie que, lorsqu'on fait la construction précédente, et que l'on prend A dans l'ensemble des éléments définissant des automorphismes intérieurs stabilisant L, on retrouve la suite exacte dont on était parti. C'est évident.

On a : $v \circ u = 1$.

Soit A une algèbre simple et centrale sur k, contenant L, et telle que l'on ait $[A : k] = [L : k]^2$. Elle définit une suite exacte, à partir de laquelle on définit une algèbre A'. Il faut montrer que A' est isomorphe à A.

En effet, l'application canonique de E dans A définit un homomorphisme canonique $\mathbf{Z}(E) \to A$. Dans cet homomorphisme, les éléments du type (1) donnent 0, d'où par passage au quotient un homomorphisme $A' \to A$, qui prolonge $E \to A$. Comme A' est simple, cet homomorphisme est injectif, et, comme A et A' ont même dimension sur k, l'image de cet homomorphisme est A.

La démonstration du théorème 12 est donc achevée.

13. Exemples

On a montré dans l'exposé précédent que $Q(G, L^*) = H^2(G, L^*)$. On a donc :

THÉORÈME 14. — *Le groupe* $H_{k,L}$ *est isomorphe au second groupe de cohomologie* $H^2(G, L^*)$ *de* G *à valeurs dans le groupe multiplicatif de* L.

COROLLAIRE. — *Tout élément de* Br_k *est d'ordre fini.*

En effet, il suffit de montrer que tout élément de $H_{k,L}$ est d'ordre fini si L est une extension galoisienne de L. Or, on a vu que tout élément de $H^i(G, A)$, $i \geqslant 1$, est d'ordre divisant n, nombre d'éléments de G.

Remarque. — En fait, on peut, au moyen des systèmes de facteurs de Brauer, donner un résultat plus précis : si $W \in Br_k$, et si D est le corps gauche contenu dans W, on a $r \cdot W = 0$, où r est l'entier tel que $[D : k] = r^2$.

Examinons plus particulièrement le cas où G est *cyclique*. On sait que, si A est un groupe sur lequel opère G, on a :

$$H^2(G, A) = A'/A'',$$

où A' désigne le sous-groupe de A formé des $a \in A$ tels que $g \cdot a = a$ pour tout $g \in G$, et où A'' désigne le sous-groupe de A formé des $\sum_{g \in G} g \cdot a$.

Dans le cas qui nous intéresse ici, c'est-à-dire $A = L^*$, on a $A' = k^*$, et $A'' = N_{L/k}(L^*)$, groupe multiplicatif des *normes* des éléments de L^*. On a donc :

THÉORÈME 15. — *Si le groupe de Galois de* L/k *est cyclique, on a* :

$$H_{k,L} = k^*/N_{L/k}(L^*).$$

COROLLAIRE 1. — *Tout corps fini est commutatif.*

Ceci veut dire que $\mathrm{Br}_k = 0$ si k est fini ; il suffit de voir que $\mathrm{H}_{k,\mathrm{L}} = 0$ pour toute extension finie de k. Mais L est alors cyclique sur k, et tout élément de k^* est norme d'un élément de L^* (Bourbaki, Alg. V, § 11). Le corollaire en résulte.

Corollaire 2. — $\mathrm{Br}_{\mathbf{R}} = \mathbf{Z}/2\mathbf{Z}$.

En effet, la seule extension galoisienne non triviale du corps des nombres réels est $\mathbf{C}$, et l'on a $\mathrm{N}_{\mathbf{C}/\mathbf{R}}(\mathbf{C}) = \mathbf{R}_+$. Comme $\mathbf{R}^*/\mathbf{R}_+^* = \mathbf{Z}/2\mathbf{Z}$, ceci démontre le corollaire.

Corollaire 3. — *Toute algèbre simple centrale sur* $\mathbf{R}$ *est semblable à* $\mathbf{R}$ *ou au corps des quaternions.*

Résulte immédiatement du corollaire 2.

Bibliographie supplémentaire (pour les produits croisés en particulier)

J. Dieudonné, *La théorie de Galois des anneaux simples et semi-simples*, Comm. Math. Helv. **21** (1948), 154–184.

Séminaire Cartan
1953-54, exposés n^{os} IV et V

21 décembre 1953 et 11 janvier 1954

FONCTIONS AUTOMORPHES D'UNE VARIABLE : APPLICATION DU THÉORÈME DE RIEMANN-ROCH

§ 1. Enoncé du théorème de Riemann-Roch

Soit X une variété analytique complexe de dimension 1 (i.e. une « surface de Riemann ») connexe et *compacte*. Au point de vue topologique X est une surface orientable, donc son premier nombre de Betti est pair, soit $2g$. L'entier positif g est dit le *genre* de X.

Conformément aux définitions générales (cf. exposé I, Appendice), un *diviseur* D sur X est un élément du groupe libre admettant comme base l'ensemble des points de X. Autrement dit, on a :

$$\mathrm{D} = \sum_{\mathrm{P}\in\mathrm{X}} n_{\mathrm{P}} \cdot \mathrm{P},$$

où les n_{P} sont des éléments de $\mathbf{Z}$ nuls sauf un nombre fini d'entre eux.

Le diviseur D est dit *positif* si $n_{\mathrm{P}} \geqslant 0$ pour tout $\mathrm{P} \in \mathrm{X}$; ainsi le groupe des diviseurs est un groupe ordonné (partiellement).

Le *degré* du diviseur D est l'entier :

$$\deg(\mathrm{D}) = \sum_{\mathrm{P}\in\mathrm{X}} n_{\mathrm{P}}.$$

Soit P un point de X et soit t_{P} une uniformisante locale en P, c'est-à-dire une carte locale en P appliquant P sur 0. Si f est une fonction méromorphe au voisinage de P, on peut définir l'*ordre* de f en P : c'est l'unique entier n tel que $f = (t_{\mathrm{P}})^n \cdot g$, où g est holomorphe et non nulle au voisinage de P (si $f = 0$, on prend $n = +\infty$, par convention). L'entier n dépend de P et de f; nous le noterons $\mathrm{o}_{\mathrm{P}}(f)$. On a $\mathrm{o}_{\mathrm{P}}(f_1 + f_2) \geqslant \mathrm{Inf}\big(\mathrm{o}_{\mathrm{P}}(f_1), \mathrm{o}_{\mathrm{P}}(f_2)\big)$ et $\mathrm{o}_{\mathrm{P}}(f_1 f_2) = \mathrm{o}_{\mathrm{P}}(f_1) + \mathrm{o}_{\mathrm{P}}(f_2)$. Si $f \neq 0$, les $\mathrm{o}_{\mathrm{P}}(f)$ sont nuls sauf un nombre fini d'entre eux, et l'expression

$$(f) = \sum_{\mathrm{P}\in\mathrm{X}} \mathrm{o}_{\mathrm{P}}(f) \cdot \mathrm{P}$$

est un diviseur, appelé le *diviseur de* f (f étant une fonction méromorphe sur X tout entier, bien entendu). Cette définition est en accord avec la définition générale donnée dans l'exposé I, Appendice.

Un diviseur de la forme (f) est dit *linéairement équivalent à* 0. Les diviseurs linéairement équivalents à 0 forment un sous-groupe du groupe des diviseurs; le groupe quotient est appelé groupe des *classes de diviseurs*; deux diviseurs D_1 et D_2 sont dits linéairement équivalents (ce que l'on écrit $D_1 \sim D_2$) si $D_1 - D_2$ est linéairement équivalent à 0, c'est-à-dire si D_1 et D_2 appartiennent à la même classe.

Si $D_1 \sim D_2$, *on a* $\deg(D_1) = \deg(D_2)$. Il suffit de voir que $\deg(f) = 0$ pour toute fonction méromorphe $f \neq 0$ définie sur X tout entier; or $\deg(f)$ n'est autre que la somme des résidus de la différentielle méromorphe df/f, et la formule $\deg(f) = 0$ résulte alors du théorème des résidus (cf. plus bas). On peut également démontrer que $\deg(f) = 0$ en prouvant tout d'abord (par un raisonnement local classique) que le nombre de points P tels que $f(P) = \lambda$ ($\lambda \in \mathbf{C} \cup \{\infty\}$) est localement constant quand λ varie, donc constant (à condition de compter ces points avec leur ordre de multiplicité) et en appliquant ceci à $\lambda = 0$ et $\lambda = \infty$, on trouve bien $\deg(f) = 0$.

On peut donc parler du degré d'une classe de diviseurs.

Si $D = \sum_{P \in X} n_P \cdot P$ est un diviseur, nous noterons $L(D)$ l'espace vectoriel des fonctions méromorphes f telles que $o_P(f) \geqslant -n_P$ pour tout $P \in X$; pour qu'une fonction $f \neq 0$ appartienne à $L(D)$, il faut et il suffit que le diviseur de f vérifie $(f) \geqslant -D$, ou encore $(f) + D \geqslant 0$. Inversement, si D' est un diviseur $\geqslant 0$ linéairement équivalent à D, on peut écrire $D' = (f) + D$, où $f \in L(D)$ est déterminé à un facteur scalaire près. Si l'on note $\ell(D)$ la dimension de l'espace vectoriel $L(D)$, on voit donc que $\ell(D) \geqslant 1$ signifie qu'il existe un diviseur $D' \geqslant 0$, $D' \sim D$; dans ce cas, on a évidemment $\deg(D) \geqslant 0$.

Si $D_1 \sim D_2$, $L(D_1)$ est isomorphe à $L(D_2)$, d'où $\ell(D_1) = \ell(D_2)$. Si $\ell(D) > 1$, il existe $D' \sim D$, $D' \geqslant 0$, et l'on a $\ell(D') = \ell(D)$; or $L(0)$ est de dimension 1, donc $D' \neq 0$, et $\deg(D) = \deg(D') > 0$. Ainsi, pour que $\ell(D) > 1$, il est *nécessaire* (mais non suffisant en général, si $g \neq 0$) que $\deg(D) > 0$.

Sur X, on a la notion de *différentielle méromorphe* : c'est une forme différentielle ω de degré 1 qui, au voisinage de chaque point $P \in X$, peut s'écrire $\omega = f \cdot dt_P$, où f est méromorphe, et où t_P désigne une uniformisante locale en P. L'*ordre* de ω en P, $o_P(\omega)$, est égal par définition à $o_P(f)$. Le *diviseur* (ω) de ω est

$$(\omega) = \sum_{P \in X} o_P(\omega) \cdot P.$$

Le *résidu* en P de ω est le coefficient de $1/t_P$ dans le développement de f en série de Laurent; il ne dépend pas du choix de t_P; on le note $\mathrm{res}_P(\omega)$. Le *théorème des résidus* affirme que

$$\sum_{P \in X} \mathrm{res}_P(\omega) = 0.$$

(Pour démontrer le théorème des résidus, on peut, par exemple, appliquer la formule de Stokes à ω et au domaine formé en retirant de X des petits disques contenant les pôles de ω.)

Si $D = \sum_{P \in X} n_P \cdot P$ est un diviseur, nous noterons I(D) l'espace vectoriel des formes méromorphes ω telles que $o_P(\omega) \geqslant n_P$ pour tout $P \in X$, et $i(D) = \dim I(D)$. Pour que $\omega \neq 0$ appartienne à I(D) il faut et il suffit que $(\omega) \geqslant D$. Si $D \sim D'$, I(D) est isomorphe à I(D′) et $i(D) = i(D')$.

Nous pouvons maintenant énoncer le théorème de Riemann-Roch :

THÉORÈME DE RIEMANN-ROCH. — *Pour tout diviseur* D *sur* X, *on a* :

$$\ell(D) - i(D) = \deg(D) + 1 - g \tag{1}$$

[Pour la démonstration, voir par exemple :

H. WEYL, *Die Idee der Riemannschen Fläche*, Teubner, Leipzig (1913), p. 122;

L. SCHWARTZ, *Sur un mémoire de Kodaira*, Sém. Bourbaki, exposé n° 32, Mai 1950.

La théorie des faisceaux analytiques permet de présenter ces démonstrations 1
sous une forme plus agréable, et surtout mieux adaptée à une généralisation à n variables. Cf. des notes récentes de Kodaira et Spencer aux Proc. Nat. Acad. Sc. U.S.A. 1953.

Lorsque l'on sait déjà que le corps des fonctions méromorphes sur X a le degré de transcendance 1 et sépare les points de X (c'est le cas dans l'application que nous ferons au § 2), on peut appliquer les démonstrations *algébriques* de Riemann-Roch; voir par exemple :

A. WEIL, *Zur algebraischen Theorie der algebraischen Funktionen*, J. Crelle **179**, 1938, 129–133,

C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*, Math. Surveys VI (Th. 7, p. 33).

Si l'on procède ainsi, il faut en outre montrer que le genre de X (défini de façon purement algébrique) est bien la moitié du premier nombre de Betti – cela peut se faire en remarquant que le nombre algébrique de zéros d'une différentielle holomorphe est égal à l'opposé de la caractéristique d'Euler-Poincaré de X, d'après un théorème classique de HOPF.]

Nous nous bornerons ici à donner quelques conséquences immédiates du théorème de Riemann-Roch :

a) Il existe une *fonction méromorphe non constante* sur X.

En effet, si $\deg(D)$ est assez grand, on a $\ell(D) > 1$, ce qui serait impossible si les seules fonctions méromorphes étaient les constantes.

Il s'ensuit, d'après l'exposé II, que le corps des fonctions méromorphes sur X est un *corps de fonctions algébriques d'une variable.*

b) Il existe une *différentielle méromorphe ω non identiquement nulle* sur X.

On prend $\omega = df$, où f est méromorphe non constante (on peut aussi appliquer la formule de Riemann-Roch, avec $\deg(D)$ assez petit).

Toute différentielle méromorphe ω' peut alors s'écrire $\omega' = f \cdot \omega$ où f est méromorphe; d'où $(\omega') = (f) + (\omega)$, ce qui montre que les diviseurs des différentielles méromorphes $\neq 0$ forment une seule classe de diviseurs, appelée *classe canonique.*

c) Si $K = (\omega)$ appartient à la classe canonique, et si D est un diviseur sur X, *l'espace* $I(D)$ *est isomorphe à l'espace* $L(K - D)$.

En effet, pour que $\omega' = f \cdot \omega$ appartienne à $I(D)$, il faut et il suffit que $(\omega') = (f) + K \geqslant D$, c'est-à-dire $(f) \geqslant -(K - D)$ i.e. $f \in L(K - D)$.

On a donc $i(D) = \ell(K - D)$, et le théorème de Riemann-Roch peut s'écrire sous la forme équivalente :

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g. \tag{2}$$

d) En faisant $D = 0$ dans (1), on voit que $i(0) = g$; *l'espace vectoriel des formes différentielles holomorphes est de dimension g.*

On a $\ell(K) = i(0) = g$, et $i(K) = \ell(0) = 1$. En faisant $D = K$ dans (1), on trouve donc :

$$\deg(K) = 2g - 2.$$

e) *Si* $\deg(D) > 2g - 2$, *on a*

$$\ell(D) = \deg(D) + 1 - g. \tag{3}$$

En effet, on a alors $\deg(K - D) < 0$, d'où $\ell(K - D) = 0$ d'après ce qui a été dit plus haut, et on applique la formule (2).

La formule (3) montre donc que, si $\deg(D)$ est « assez grand », $\ell(D)$ est déterminé par $\deg(D)$, ce qui est très commode dans les applications. Par exemple :

f) *Si* $\deg(D) > 2g - 1$, *pour tout* $P \in X$ *il existe* $D' \sim D$, $D' \geqslant 0$ *tel que* $P \notin D'$.

(Autrement dit, la série linéaire complète $|D|$, formée des diviseurs positifs D' équivalents à D, n'a pas de points fixes.)

Si n_P est le coefficient de P dans D, l'assertion f) revient à dire qu'il existe $f \in L(D)$ avec $o_P(f) = -n_P$; or, si une telle fonction n'existait pas, on aurait $L(D) = L(D - P)$, d'où $\ell(D) = \ell(D - P)$, ce qui est en contradiction avec (3).

g) *Soit* $f_0, \ldots, f_h$ *une base de* L(D), D *étant un diviseur tel que* $\deg(D) > 2g$. *Pour tout* $x \in X$, *soit* $F(x)$ *le point de l'espace projectif* $\mathbf{P}_h(\mathbf{C})$ *de coordonnées homogènes* $f_0(x), \ldots, f_h(x)$. *L'application* F *est un isomorphisme analytique de* X *sur une sous-variété sans singularités de* $\mathbf{P}_h(\mathbf{C})$ *et le diviseur* D *est équivalent à une section hyperplane de* F(X). 2

Il est évident que F ne change pas lorsque l'on remplace D par un diviseur équivalent; en particulier on peut supposer [d'après f)] que D est positif. La fonction constante 1 appartient à L(D) et peut s'écrire $1 = \sum c_i \cdot f_i$; appliquant à nouveau f) on montre alors que la section de F(X) par l'hyperplan $\sum c_i \cdot X_i = 0$ est F(D).

Soit n_P le coefficient de P dans D; si $P \neq Q$, il y a $f \in L(D)$ tel que $o_P(f) \geqslant -n_P + 1$ et $o_Q(f) = -n_Q$ [appliquer f) au diviseur $D - P$]; cela signifie qu'il existe un hyperplan de $\mathbf{P}_h(\mathbf{C})$ passant par F(P) mais pas par F(Q) : donc F est injectif.

Enfin, pour tout $P \in X$, il existe $f \in L(D)$ tel que $o_P(f) = -n_P + 1$ [appliquer encore f) à $D - P$]; cela signifie qu'il existe un hyperplan de $\mathbf{P}_h(\mathbf{C})$ passant par P et ayant une intersection *simple* avec F(X) en P; donc tout point de F(X) est simple, et F est bien un isomorphisme analytique.

A cause d'un théorème de CHOW, F(X) est une *courbe algébrique* (sans singularités).

§ 2. Application du théorème de Riemann-Roch aux fonctions automorphes

Soient Y le disque unité $|z| < 1$ de $\mathbf{C}$, et G un groupe discret d'automorphismes de Y tel que $X = Y/G$ soit *compact* (nous étudierons un cas plus général au § suivant). Nous noterons π la projection canonique $Y \to X$. Pour tout $y \in Y$ nous noterons G_y le stabilisateur de y dans G, i.e. l'ensemble des $\sigma \in G$ tels que $\sigma(y) = y$.

Lemme. — *Pour tout* $y \in Y$, *le groupe* G_y *est cyclique fini d'ordre* e_y *et il existe une uniformisante locale* z_y *en* y *telle que les éléments de* G_y *soient les homothéties* $z_y \mapsto \varepsilon \cdot z_y$ *où* ε *parcourt le groupe des racines* e_y*-ièmes de l'unité.*

Par une transformation homographique, on est ramené au cas particulier où $y = 0$. Or les transformations de G laissant fixe 0 sont de la forme $z \mapsto e^{2\pi i\varphi} z$

(appliquer le lemme de Schwarz, par exemple) et d'autre part, forment un sous-groupe fini de G. Le lemme résulte immédiatement de là.

(En fait, le lemme précédent n'est pas spécial au disque unité : H. CARTAN a démontré que tout groupe compact d'automorphismes analytiques d'une variété analytique complexe Y admettant un point fixe 0 est localement – au voisinage de 0 – isomorphe à un groupe linéaire.)

Si x est un point de X, les groupes G_y, $y \in \pi^{-1}(x)$, sont conjugués dans G et ont donc le même ordre, que nous noterons e_x et appellerons *l'indice de ramification* de x. Si $e_x > 1$, nous dirons que x est *ramifié* : cela signifie que $x = \pi(y)$ avec $G_y \neq \{1\}$; comme de tels points y sont isolés (à cause du lemme précédent, par exemple), l'ensemble des points ramifiés de X est *fini*.

Nous allons maintenant munir X d'une structure de *variété analytique complexe de dimension* 1; pour cela, il suffit de donner, pour tout point $x \in X$, une uniformisante locale t_x en x, et de vérifier certains axiomes. Si $x = \pi(y)$, $y \in Y$, nous prendrons pour t_x la fonction $(z_y)^{e_y}$, où z_y et e_y ont les propriétés indiquées dans le lemme ci-dessus; cela a un sens, car la fonction $(z_y)^{e_y}$ est évidemment invariante par G_y, donc définit par passage au quotient une fonction sur X, définie au voisinage de x; pour qu'une fonction f, définie au voisinage de x, soit fonction holomorphe de t_x, il faut et il suffit que $\widetilde{f} = f \circ \pi$, définie au voisinage de y, soit holomorphe; ainsi *l'anneau $\mathscr{O}_x$ des fonctions holomorphes en x est isomorphe au sous-anneau de $\mathscr{O}_y$ formé des fonctions invariantes par le groupe* G_y. Ceci montre en particulier que la structure analytique de X ne dépend pas du choix de z_y; quant à la vérification des axiomes des variétés analytiques, elle est immédiate.

L'application $\pi : Y \to X$ est analytique; c'est même localement un isomorphisme en dehors des points ramifiés; s'il n'existe aucun tel point, Y est le revêtement universel de X, et G est isomorphe au groupe fondamental $\pi_1(X)$ de X. Si P est un point de X, nous noterons, comme au § 1, $o_P(f)$, resp. $o_P(\omega)$, l'*ordre* en P d'une fonction méromorphe f, resp. d'une différentielle méromorphe ω. D'autre part, soit h une fonction méromorphe sur Y, automorphe de poids quelconque; si $Q' = \sigma \cdot Q$, avec $\sigma \in G$, on a $o_Q(h) = o_{Q'}(h)$; donc $o_Q(h)$ ne dépend que de la projection $\pi(Q)$ de Q dans X, nous pouvons le noter $\widetilde{o}_P(h)$, si $P = \pi(Q)$.

Les ordres o_P et $\widetilde{o}_P$ ont des relations étroites :

a) *Si f est méromorphe sur* X, *et si $\widetilde{f} = f \circ \pi$ est la fonction automorphe de poids* 0 *définie par f sur* Y, *on a* :

$$\widetilde{o}_P(\widetilde{f}) = e_P \cdot o_P(f), \quad e_P = \text{indice de ramification en P.}$$

b) *Si ω est une différentielle méromorphe sur* X, $\pi^*(\omega)$ *est une différentielle sur* Y *invariante par* G, *donc* (exposé I, n° 3) *égale à $g\cdot dz$, où g est automorphe de poids* 1, *et l'on a*: 3

$$\widetilde{\mathrm{o}}_{\mathrm{P}}(g) = e_{\mathrm{P}} \cdot \mathrm{o}_{\mathrm{P}}(\omega) + e_{\mathrm{P}} - 1.$$

Les propriétés a) et b) se démontrent par un calcul local immédiat. Pour a), on écrit f sous la forme :

$$f = (t_{\mathrm{P}})^{\mathrm{o}_{\mathrm{P}}(f)} \cdot f_1, \quad \text{où } f_1 \text{ est holomorphe} \neq 0 \text{ en P},$$

d'où :

$$\widetilde{f} = (z_{\mathrm{Q}})^{e_{\mathrm{P}}\cdot \mathrm{o}_{\mathrm{P}}(f)} \cdot \widetilde{f}_1 \qquad (\pi(\mathrm{Q}) = \mathrm{P}),$$

ce qui montre bien que l'ordre de $\widetilde{f}$ en Q est $e_{\mathrm{P}}\cdot \mathrm{o}_{\mathrm{P}}(f)$. Démonstration analogue pour b).

Nous choisirons maintenant, une fois pour toutes, une différentielle ω sur X, méromorphe et non identiquement nulle et nous désignerons par g la fonction méromorphe de poids 1 sur Y telle que $\pi^*(\omega) = g \cdot dz$, $\pi^*(\omega)$ désignant, comme ci-dessus, l'image réciproque de la forme ω par l'application π. L'existence d'une telle forme résulte, soit du § 1, b) qui est applicable puisque X est compact, soit plus simplement du théorème 3 de l'exposé I.

La fonction méromorphe g^n, n entier $\geqslant 0$, est donc de poids n ce qui montre que toute fonction méromorphe h de poids n est de la forme :

$$h = f \cdot g^n \text{ avec } \widetilde{f} = f \circ \pi,\ f \text{ méromorphe sur X}.$$

Pour que h soit *holomorphe*, il faut et il suffit que $\widetilde{\mathrm{o}}_{\mathrm{P}}(h) \geqslant 0$ pour tout $\mathrm{P} \in \mathrm{X}$, c'est-à-dire :

$$\widetilde{\mathrm{o}}_{\mathrm{P}}(\widetilde{f}) = e_{\mathrm{P}} \cdot \mathrm{o}_{\mathrm{P}}(f) \geqslant -n \cdot \widetilde{\mathrm{o}}_{\mathrm{P}}(g) = -n \cdot e_{\mathrm{P}} \cdot \mathrm{o}_{\mathrm{P}}(\omega) - n(e_{\mathrm{P}} - 1),$$

ou encore

$$\mathrm{o}_{\mathrm{P}}(f) \geqslant -n \cdot \mathrm{o}_{\mathrm{P}}(\omega) - \Big[n\big(1 - \frac{1}{e_{\mathrm{P}}}\big)\Big],$$

le symbole $[x]$ désignant la partie entière du nombre x.

Soit $\mathrm{K} = \sum \mathrm{o}_{\mathrm{P}}(\omega) \cdot \mathrm{P}$ le diviseur de ω, et posons :

$$\mathrm{E}_n = n \cdot \mathrm{K} + \sum_{\mathrm{P}\in \mathrm{X}} \Big[n\big(1 - \frac{1}{e_{\mathrm{P}}}\big)\Big] \cdot \mathrm{P}\,,$$

le Σ ne portant d'ailleurs que sur les points *ramifiés* de X. L'inégalité ci-dessus équivaut alors à la suivante :

$$(f) \geqslant -\mathrm{E}_n, \quad \text{autrement dit} \quad f \in \mathrm{L}(\mathrm{E}_n).$$

En résumé :

PROPOSITION 1. — *Soit* D_n *l'espace vectoriel des fonctions holomorphes de poids* n *sur* Y. *L'application* $f \mapsto \widetilde{f} \cdot g^n$ *est un isomorphisme de* $\mathrm{L}(\mathrm{E}_n)$ *sur* D_n.

COROLLAIRE. — *Si* $d_n = \dim \mathrm{D}_n$, *on a* $d_n = \ell(\mathrm{E}_n)$.

Pour appliquer le théorème de Riemann-Roch au diviseur E_n, nous avons besoin de connaître le degré de E_n. Mais K étant le diviseur d'une différentielle on a $\deg(\mathrm{K}) = 2g - 2$, g étant le genre de X [§ 1, d)]. Donc :

$$\deg(\mathrm{E}_n) = 2n(g-1) + \sum_{\mathrm{P}\in\mathrm{X}} \Big[n\big(1 - \frac{1}{e_{\mathrm{P}}}\big) \Big].$$

Lemme. — *Le nombre* $\mathrm{A} = 2g - 2 + \sum(1 - 1/e_{\mathrm{P}})$ *est* > 0.

En effet, soit n un entier, multiple de tous les e_{P}, et assez grand pour que $d_n \geqslant 2$ (un tel n existe d'après le théorème 2 de l'exposé I); comme $\ell(\mathrm{E}_n) = d_n \geqslant 2$, on a $\deg(\mathrm{E}_n) > 0$, et puisque n est multiple des e_{P}, $\deg(\mathrm{E}_n) = n\mathrm{A}$, d'où $\mathrm{A} > 0$, c.q.f.d.

(Autre démonstration : $2\pi\mathrm{A}$ est l'aire de X calculée à partir de l'élément d'aire « non-euclidien » de Y, normalisé de telle sorte que la courbure soit -1.)

Comme application du lemme précédent, montrons que $\deg(\mathrm{E}_n) > 2g$ dès que $n \geqslant 2$: on a

$$\deg(\mathrm{E}_n) - (2g-2) = (n-1)(2g-2) + \sum \Big[n\big(1 - \frac{1}{e_{\mathrm{P}}}\big) \Big].$$

Or on vérifie aisément que $\Big[n\big(1 - 1/e_{\mathrm{P}}\big) \Big] \geqslant (n-1)(1 - 1/e_{\mathrm{P}})$. D'où :

$$\deg(\mathrm{E}_n) - (2g-2) \geqslant (n-1)\mathrm{A} > 0 \quad \text{si} \quad n \geqslant 2.$$

On peut donc appliquer la formule (3) du § 1, e), et on l'obtient :

$$d_n = \ell(\mathrm{E}_n) = \deg(\mathrm{E}_n) + 1 - g \quad \text{si} \quad n \geqslant 2,$$

d'où en résumé :

PROPOSITION 2. — *Si* $\mathrm{X} = \mathrm{Y}/\mathrm{G}$ *est compact et de genre* g, *on a* :

$$d_n = (2n-1)(g-1) + \sum_{\mathrm{P}\in\mathrm{X}} \Big[n\big(1 - \frac{1}{e_{\mathrm{P}}}\big) \Big]$$

si $n \geqslant 2$. (Si $n = 0$, $\mathrm{E}_0 = 0$, et $d_0 = 1$; si $n = 1$, $\mathrm{E}_1 = \mathrm{K}$, et $d_1 = g$.)

On peut donner d'autres applications de la proposition 1; par exemple, on peut chercher dans quel cas on a $\deg(\mathrm{E}_n) > 2g$; en appliquant le lemme ci-dessus, on voit que cette condition est réalisée lorsque :

a) $g = 0$, $n \geqslant 2$,
b) $g = 1$, $n \geqslant 6$,
c) $g = 2$, $n \geqslant 3$,
d) $g > 2$, $n \geqslant 2$.

Quand il en est ainsi, le § 1, g) montre que toute base $f_0, \ldots, f_j$ de $\mathrm{L}(\mathrm{E}_n)$ définit un plongement $\mathrm{F} : \mathrm{P} \mapsto \big(f_0(\mathrm{P}), \ldots, f_j(\mathrm{P})\big)$ de X sur une courbe sans singularités de l'espace projectif $\mathbf{P}_j(\mathbf{C})$. Or les fonctions $f_0, \ldots, f_j$ définissent des fonctions holomorphes $g_0, \ldots, g_j$ de poids n; l'application

$$\mathrm{G} : \mathrm{Q} \longmapsto \big(g_0(\mathrm{Q}), \ldots, g_j(\mathrm{Q})\big)$$

de Y dans $\mathbf{P}_j(\mathbf{C})$ est constante sur les classes suivant G et l'on a $\mathrm{G} = \mathrm{F} \circ \pi$. En résumé :

Si n est assez grand [les valeurs précises étant indiquées dans a), b), c), d) ci-dessus] *toute base $g_0, \ldots, g_j$ de l'espace D_n des fonctions holomorphes de poids n définit une application*

$$\mathrm{G} : \mathrm{Q} \longmapsto \big(g_0(\mathrm{Q}), \ldots, g_j(\mathrm{Q})\big) \in \mathbf{P}_j(\mathbf{C})$$

qui, par passage au quotient, définit un isomorphisme analytique de $\mathrm{X} = \mathrm{Y}/\mathrm{G}$ *sur une courbe sans singularités de l'espace projectif complexe* $\mathbf{P}_j(\mathbf{C})$*, où* $j = d_n - 1$.

§ 3. Cas où $\widehat{\mathrm{X}}$ est compact

Conservons les notations du § 2, et soit G un groupe discret d'automorphismes du disque unité Y. Nous ne supposons plus que $\mathrm{X} = \mathrm{Y}/\mathrm{G}$ soit compact; le groupe G peut alors contenir des transformations paraboliques, dont les points doubles (situés sur la circonférence C : $|z| = 1$) sont dits points paraboliques de G. On sait que l'on peut ajouter ces points à Y de façon à obtenir un espace $\widehat{\mathrm{Y}}$ sur lequel opère le groupe G, et que l'espace quotient $\widehat{\mathrm{X}} = \widehat{\mathrm{Y}}/\mathrm{G}$ est une variété analytique complexe de dimension 1 (cf. exposé III); nous noterons encore $\pi : \widehat{\mathrm{Y}} \to \widehat{\mathrm{X}}$ la projection canonique de $\widehat{\mathrm{Y}}$ sur $\widehat{\mathrm{X}}$.

Nous supposerons à partir de maintenant *que* $\widehat{\mathrm{X}}$ *est compact* : cette hypothèse est vérifiée dans les cas particuliers les plus importants, par exemple lorsque G est le groupe modulaire ou un sous-groupe d'indice fini du groupe modulaire. 4

Si $\mathrm{Q} \in \widehat{\mathrm{Y}}$ est un point parabolique de G, nous noterons G_Q le sous-groupe de G formé des $g \in \mathrm{G}$ tels que $g \cdot \mathrm{Q} = \mathrm{Q}$. On sait (exposé III) que G_Q est un

groupe cyclique infini, engendré par une transformation de la forme :

$$\frac{1}{z'-\mathrm{Q}} = \frac{1}{z-\mathrm{Q}} + h, \quad h \in \mathbf{C},$$

où h n'est déterminé qu'au signe près. Soit $\mathrm{P} = \pi(\mathrm{Q}) \in \widehat{\mathrm{X}}$, et soit t_P la fonction :

$$t_\mathrm{P} = \mathrm{e}^{2\pi i/h(z-\mathrm{Q})}.$$

Cette fonction est invariante par $\mathrm{G_Q}$, donc définit une fonction sur $\widehat{\mathrm{X}}$; de plus, si le signe de h est choisi convenablement, on vérifie que t_P est une *uniformisante locale* en P.

Soit g une fonction automorphe de poids n sur Y : la fonction $(z-\mathrm{Q})^{2n} \cdot g(z)$ est alors *invariante* par $\mathrm{G_Q}$. (Rappelons brièvement la démonstration : du fait que g est de poids n, on a $g(z)dz^n = g(z')dz'^n$, et comme $dz/(z-\mathrm{Q})^2 = dz'/(z'-\mathrm{Q})^2$, on en tire bien $g(z) \cdot (z-\mathrm{Q})^{2n} = g(z') \cdot (z'-\mathrm{Q})^{2n}$.) On peut alors parler de *l'ordre au point* P de la fonction $(z-\mathrm{Q})^{2n} \cdot g(z)$, si cette fonction est méromorphe (ce que nous supposerons); cet ordre ne dépend que de g et de P, et sera noté $\widehat{\mathrm{o}}_\mathrm{P}(g)$. Si g_1 et g_2 sont deux fonctions automorphes, on a $\widehat{\mathrm{o}}_\mathrm{P}(g_1 \cdot g_2) = \widehat{\mathrm{o}}_\mathrm{P}(g_1) + \widehat{\mathrm{o}}_\mathrm{P}(g_2)$. Enfin, si $n = 1$, la forme différentielle $g \cdot dz$ est invariante par G, donc est de la forme $\pi^*(\omega)$, où ω est une forme différentielle sur X; dire que g est méromorphe en P équivaut à dire que ω est méromorphe en P, et l'on a la formule :

$$\widehat{\mathrm{o}}_\mathrm{P}(g) = \mathrm{o}_\mathrm{P}(\omega) + 1.$$

(En effet, on a $\omega = \lambda(z-\mathrm{Q})^2 g(z)\ dt_\mathrm{P}/t_\mathrm{P}, \quad \lambda \neq 0.$)

Nous dirons qu'une fonction automorphe g de poids n est *holomorphe en* P si $\widehat{\mathrm{o}}_\mathrm{P}(g) \geqslant 0$, ou, ce qui revient au même, si pour Q se projetant en P, la fonction $(z-\mathrm{Q})^{2n} g(z)$ est fonction holomorphe de l'uniformisante locale t_P. Une fonction de poids n sera dite *holomorphe sur* $\widehat{\mathrm{Y}}$ si elle est holomorphe en tout point de Y et aussi en tout point parabolique. Nous noterons D_n l'espace vectoriel formé par ces fonctions, et d_n la dimension de D_n. S'il n'y a pas de points paraboliques, ces définitions se réduisent à celles du § 2.

Etudions maintenant l'espace D_n. Comme au § 2, nous choisirons une fois pour toutes une fonction g, méromorphe et de poids 1 sur Y, non identiquement nulle, et méromorphe en tous les points paraboliques. Une telle fonction existe : il suffit de prendre un quotient de séries de Poincaré (cf. exposé III). On a $g \cdot dz = \pi^*(\omega)$, où ω est une différentielle méromorphe sur $\widehat{\mathrm{X}}$.

Toute fonction méromorphe h de poids n s'écrit alors :

$h = \widetilde{f} \cdot g^n$, avec $\widetilde{f} = f \circ \pi$, f méromorphe sur $\widehat{\mathrm{X}}$.

Pour que h soit holomorphe en un point $\mathrm{P} \in \mathrm{X}$, il faut et il suffit (cf. § 2) que :

$$\mathrm{o_P}(f) \geqslant -n \cdot \mathrm{o_P}(\omega) - \big[n(1 - 1/e_\mathrm{P})\big],\ e_\mathrm{P} \text{ indice de ramification en P.}$$

De même pour que h soit holomorphe en un point parabolique $\mathrm{P} \in \mathrm{X}$, il faut et il suffit que :

$$\widehat{\mathrm{o}}_\mathrm{P}(\widetilde{f}) \geqslant -n \cdot \widehat{\mathrm{o}}_\mathrm{P}(g),$$

c'est-à-dire :

$$\mathrm{o_P}(f) \geqslant -n \cdot \mathrm{o_P}(\omega) - n.$$

Posons alors $e_\mathrm{P} = \infty$ si P est un point *parabolique* de $\widehat{\mathrm{X}}$. On voit que la formule :

$$\mathrm{o_P}(f) \geqslant -n \cdot \mathrm{o_P}(\omega) - \big[n(1 - 1/e_\mathrm{P})\big] \text{ pour tout } \mathrm{P} \in \widehat{\mathrm{X}}$$

est nécessaire et suffisante pour que h soit holomorphe sur $\widehat{\mathrm{Y}}$.

Soit $\mathrm{K} = (\omega)$ le diviseur de ω, et posons :

$$\mathrm{E}_n = n \cdot \mathrm{K} + \sum_{\mathrm{P} \in \widehat{\mathrm{X}}} \left[n(1 - \frac{1}{e_\mathrm{P}}) \right].$$

On a ainsi obtenu une généralisation de la proposition 1 du § 2 :

PROPOSITION 3. — *L'application* $f \mapsto \widetilde{f} \cdot g^n$ *est un isomorphisme de* $\mathrm{L}(\mathrm{E}_n)$ *sur* D_n.

COROLLAIRE. — $d_n = \ell(\mathrm{E}_n)$.

On peut appliquer le théorème de Riemann-Roch au calcul de $\ell(\mathrm{E}_n)$. Il faut d'abord montrer que le nombre **6**

$$\mathrm{A} = 2g - 2 + \sum \Big(1 - \frac{1}{e_\mathrm{P}}\Big)$$

est > 0, ce qui se fait comme au § 2 (puisque les séries de Poincaré sont holomorphes sur $\widehat{\mathrm{Y}}$, d'après l'exposé III). On en tire que $\deg(\mathrm{E}_n) > 2g - 2$ si $n \geqslant 2$, d'où :

PROPOSITION 4. — *Si* $\widehat{\mathrm{X}} = \widehat{\mathrm{Y}}/\mathrm{G}$ *est compact et de genre* g, *on a* :

$$d_n = (2n - 1)(g - 1) + \sum_{\mathrm{P} \in \widehat{\mathrm{X}}} \Big[n\big(1 - \frac{1}{e_\mathrm{P}}\big) \Big] \quad \textit{si } n \geqslant 2.$$

Si $n = 0$, on a $\mathrm{E}_n = 0$, d'où $d_0 = 1$.

Si $n = 1$, on a $\mathrm{E}_n = \mathrm{K} + \sum_{\mathrm{P} \in \widehat{\mathrm{X}} - \mathrm{X}} \mathrm{P}$; donc, s'il y a *au moins un point parabolique*, on a $\deg(\mathrm{E}_1) > 2g - 2 = \deg(\mathrm{K})$, d'où $d_1 = g - 1 + r$, r étant le nombre de points paraboliques.

Exemple. — On prend pour G le groupe modulaire $z \mapsto \frac{az+b}{cz+d}$, $ad - bc = 1$, a, b, c, d entiers, qui opère sur le demi-plan supérieur. On a $g = 0$ et les e_P sont tous nuls, sauf trois d'entre eux, égaux respectivement à $(2, 3, \infty)$ (« signature » des ramifications). On en déduit la dimension de l'espace des formes modulaires de degré $2n$; on pourra vérifier la formule obtenue en se reportant à l'exposé de GODEMENT au Sém. Bourbaki, n° 74, Février 1953.

Autre exemple : le groupe modulaire *arithmétique*, sous-groupe d'indice 6 du précédent, formé des $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où b et c sont *pairs*. On a encore $g = 0$, et la signature est (∞, ∞, ∞); c'est le groupe qui donne le revêtement universel de la sphère privée de trois points et qui conduit aux théorèmes de Picard.

Plus généralement, en imposant des conditions de congruence aux a, b, c, d, on obtient les « groupes de congruence », qui sont des sous-groupes d'indice fini du groupe modulaire.

Bibliographie

7

[1] H. PETERSSON, Nombreux articles depuis 1930. Notamment : *Zur analytischen Theorie der Grenzkreisgruppen*, II, Math. Annalen **115** (1938), 175–204 (Calcul de d_n au moyen du th. de Riemann-Roch mais sous des hypothèses bien plus larges que celles du présent exposé).

[2] H. POINCARÉ, *Œuvres*, tome II, p. 169, § 6 (on y trouvera notamment la Proposition 2).

[3] A. WEIL, *Généralisation des fonctions abéliennes*, J. de Math. Pures et Appl. **17** (1938), 47–87 (Chap. I) ainsi qu'une Note dans Hamb. Abh. **11** (1935) (extension du théorème de Riemann-Roch aux diviseurs matriciels).

Séminaire Cartan 26 avril 1954
1953-54, exposé n° XVI

DEUX THÉORÈMES SUR LES APPLICATIONS COMPLÈTEMENT CONTINUES

Les théorèmes 1 et 2 démontrés ci-dessous sont dus à L. SCHWARTZ (C.R.A.S. **236** (1953), 2472–2473). Ils seront utilisés dans l'exposé XVII (H. CARTAN) pour démontrer que $H^q(X, \mathscr{F})$ est de dimension finie, si X est une variété analytique compacte, et $\mathscr{F}$ un faisceau analytique cohérent. Ce résultat servira lui-même de base à l'étude des faisceaux analytiques cohérents sur l'espace projectif (exposés XVIII et XIX ci-après).

Dans tout ce qui suit, E et F désignent des espaces vectoriels topologiques, localement convexes, et séparés. Pour tout ce qui concerne les espaces vectoriels topologiques, nous renvoyons à N. BOURBAKI, Livre V, cité EVT dans la suite. 1

DÉFINITION. — *Une application linéaire v de* E *dans* F *est dite complètement continue s'il existe un voisinage* V *de* 0 *dans* E *tel que* $v(V)$ *soit relativement compact dans* F.

(Cette définition est due à J. LERAY, cf. Acta Sci. Math. Szeged **12** (1950), 117–186.)

Une telle application est *continue*; en effet, si W est un voisinage de 0 dans F, il existe un scalaire λ tel que $v(V) \subset \lambda W$ (du fait que $v(V)$ est relativement compacte, donc précompacte), d'où $v(\lambda^{-1}.V) \subset W$.

THÉORÈME 1. — *Soient u et v deux applications linéaires continues de* E *dans* F. *Supposons* :

a) *que u soit un isomorphisme de* E *sur* $u(E)$, *et que* $u(E)$ *soit fermé dans* F,

b) *que v soit complètement continue.*

Alors $w = u + v$ est un homomorphisme[1], *son noyau* N *est de dimension finie, et son image* $w(E)$ *est fermée.* 2

L'hypothèse b) signifie qu'il existe V, voisinage de 0 dans E, tel que $v(V)$ soit relativement compact ; puisque E est localement convexe, on peut supposer que V est l'ensemble des $x \in E$ tels que $p(x) \leqslant 1$, p étant une semi-norme continue sur E (cf. EVT, Chap. II, § 5). Posons $W = V \cap N$; on a $u + v = 0$ sur W, donc $u(W) = -v(W)$ est relativement compact dans F, donc précompact dans F, et aussi dans $u(E)$; puisque $u : E \to u(E)$ est un isomorphisme, W est précompact, et comme c'est un voisinage de 0 dans N, N est de dimension finie[2].

Soit E' un supplémentaire topologique de N dans E (qui existe d'après le théorème de Hahn-Banach, cf. EVT, Chap. II, § 3), et soient u', v', w' les restrictions à E' de u, v, w. On vérifie tout de suite que les conditions a) et b) sont satisfaites pour u' et v' ; supposons le théorème démontré pour u' et v' ; on voit alors facilement qu'il l'est pour u et v (par exemple, $w(E)$ est égal à $w'(E')$, donc fermé — etc.). Il suffit donc de démontrer le théorème pour u' et v', ce qui revient simplement à supposer que $N = 0$, autrement dit que w est *injectif*.

Soit alors $\mathscr{U}$ un ultrafiltre sur E, tel que $w(\mathscr{U})$ converge dans F ; tout revient à montrer que $\mathscr{U}$ converge dans E[3].

Soit a la limite (finie ou infinie) de $p(x)$ suivant $\mathscr{U}$. Montrons d'abord que a est *finie*. Soit H la partie de E formée des x tels que $p(x) \neq 0$. Si l'on avait $a = +\infty$, H appartiendrait à $\mathscr{U}$, et $\mathscr{U}$ induirait sur H un ultrafiltre $\mathscr{U}_H$; puisque $w(x)$ a une limite suivant $\mathscr{U}$, $w(x/p(x))_{x\in H}$ aurait pour limite 0, suivant $\mathscr{U}_H$; d'autre part, $v(x/p(x)) \in v(V)$ a une limite suivant $\mathscr{U}_H$, puisque $v(V)$ est relativement compact. Donc $u(x/p(x))$ aurait une limite, donc aussi $x/p(x)$, d'après l'hypothèse a). Si x_0 désigne cette limite, on aurait $p(x_0) = \lim p(x)/p(x) = 1$, et d'autre part $w(x_0) = \lim w(x/p(x)) = 0$, ce qui est contraire à l'injectivité de w.

Ainsi a est finie ; si l'on pose $V' = (a+1)\cdot V$, V' est l'ensemble des $x \in E$ tels que $p(x) \leqslant a+1$, donc $V' \in \mathscr{U}$; puisque $v(V') = (a+1)\cdot v(V)$ est relativement compact dans F, on en conclut que $v(x)$ converge dans F suivant $\mathscr{U}$, donc aussi $u(x) = w(x) - v(x)$, et l'hypothèse a) entraîne que $\mathscr{U}$ converge dans E, c.q.f.d.

THÉORÈME 2. — *Soient u et v deux applications linéaires continues de* E *dans* F. *Supposons* :

a) *que u soit un homomorphisme faible*[4] *de* E *sur* F,

b) *que v soit complètement continue*

et

(K) *que tout compact convexe de* F *soit l'image par u d'un compact convexe de* E.

Alors $w = u + v$ est un homomorphisme faible de E *sur un sous-espace fermé de codimension finie de* F.

Soit E'_c (resp. F'_c) le dual topologique de E (resp. F), muni de la topologie $\mathscr{T}_c$ de la convergence uniforme sur toute partie compacte convexe de E (resp. F). D'après un théorème de MACKEY[5], le dual de E'_c n'est autre que E, et de même pour F'_c ; autrement dit, la topologie affaiblie[6] de la topologie $\mathscr{T}_c$ sur E' est $\sigma(E', E)$.

Soient ${}^t u$ et ${}^t v$ les transposées de u et v, respectivement ; ce sont des applications linéaires continues de F'_c dans E'_c. Nous allons montrer qu'elles vérifient les hypothèses du théorème 1 :

a) Puisque u applique E *sur* F, ${}^t u$ est injectif ; la condition (K) entraîne que c'est un isomorphisme topologique sur son image; enfin, on sait[7] que l'image de ${}^t u$ est faiblement fermée (donc aussi fermée pour $\mathscr{T}_c$ qui est plus fine), puisque u est un homomorphisme faible.

b) Soit V un voisinage de 0 dans E, tel que $v(V)$ soit relativement compact dans F ; le polaire[8] V^0 de V est une partie équicontinue de E', et, puisque ${}^t v(v(V)^0) \subset V^0$, ${}^t v(v(V)^0)$ est aussi une partie équicontinue de E'_c, donc relativement compacte, d'après le théorème d'Ascoli. D'autre part, $v(V)$ étant relativement compacte, $v(V)^0$ est un voisinage de 0 dans F'_c. Ceci montre que ${}^t v$ est complètement continue.

Appliquons alors le théorème 1 :

i) ${}^t w(F')$ est fermé dans E'_c, donc aussi fermé pour la topologie affaiblie correspondante, qui n'est autre que $\sigma(E', E)$, on l'a vu plus haut. Il en résulte[7] que w est un homomorphisme faible.

ii) ${}^t w$ est aussi un homomorphisme pour les topologies $\mathscr{T}_c$, donc aussi pour les topologies affaiblies correspondantes[9], qui sont $\sigma(E', E)$ et $\sigma(F', F)$. Il en résulte[7] que $w(E)$ est faiblement fermé, donc fermé.

iii) Le noyau N de ${}^t w$ est de dimension finie ; comme N est isomorphe au dual de $F/w(E)$ (parce que $w(E)$ est fermé), on voit que $w(E)$ est un sous-espace de codimension finie de F, c.q.f.d.

COROLLAIRE. — *Soient* E *et* F *deux espaces de Fréchet*[10]*, et soient u et v deux applications linéaires continues de* E *dans* F. *Supposons* :

a) *que u applique* E *sur* F,

b) *que v soit complètement continue.*

Alors $w = u + v$ est un homomorphisme de E *sur un sous-espace fermé de codimension finie de* F.

La condition a) entraîne que u est un homomorphisme (th. de Banach, EVT, Chap. I, § 3), donc un homomorphisme faible[9]. D'autre part, la condition (K)

est vérifiée, du fait que E et F sont des espaces de Fréchet[(11)]. Le théorème 2 montre alors que $w(\mathrm{E})$ est un sous-espace fermé de codimension finie de F, et le théorème de Banach montre que w est un homomorphisme.

Notes

(1) Autrement dit, w transforme tout voisinage de 0 dans E en un voisinage de 0 dans $w(\mathrm{E})$. Cf. N. Bourbaki, Top. Gén., Chap. III, § 2.

(2) Cf. EVT, Chap. I, § 2, n° 4. Rappelons brièvement la démonstration : puisque W est précompact et que $\frac{1}{2}\mathrm{W}$ est un voisinage de 0 dans N, il existe un nombre fini de points a_i tels que W soit contenu dans la réunion des $a_i + \frac{1}{2}\mathrm{W}$; soit M le sous-espace vectoriel de N engendré par les a_i ; puisque M est de dimension finie, M est fermé dans N (EVT, Chap. I, § 2, n° 3), donc N/M est séparé. Soit W′ l'image de W dans N/M ; comme $\mathrm{W} \subset \mathrm{M} + \frac{1}{2}\mathrm{W}$, on a $\mathrm{W}' \subset \frac{1}{2}\mathrm{W}'$, d'où $\mathrm{W}' \supset 2\mathrm{W}'$, $\mathrm{W}' \supset 2^n\mathrm{W}'$ pour tout n, donc $\mathrm{W}' = \mathrm{N/M}$. D'autre part W′ étant image de W est précompact. Donc N/M est précompact, donc nul (car sinon il contiendrait une droite, qui n'est visiblement pas précompacte). Donc $\mathrm{N} = \mathrm{M}$, et N est bien de dimension finie.

(3) Montrons que cette propriété entraîne que $w(\mathrm{E})$ est fermé dans F et que w est un isomorphisme de E sur $w(\mathrm{E})$:

Soit A une partie fermée de E, et soit $y \in \overline{u(\mathrm{A})}$, adhérence de $u(\mathrm{A})$. Il existe un filtre $\mathscr{F}$ sur $w(\mathrm{A})$ qui converge vers y ; si $\mathscr{U}''$ est un ultrafiltre sur $w(\mathrm{A})$ plus fin que $\mathscr{F}$, $\mathscr{U}''$ converge aussi vers y. Puisque w est injectif, il existe un ultrafiltre $\mathscr{U}'$ sur A tel que $w(\mathscr{U}') = \mathscr{U}''$; l'ultrafiltre $\mathscr{U}'$ engendre un ultrafiltre $\mathscr{U}$ sur E, et $w(\mathscr{U})$ converge évidemment vers y. Donc $\mathscr{U}$ converge vers $x \in \mathrm{E}$; puisque $\mathrm{A} \in \mathscr{U}$, et que A est fermé, on a $x \in \mathrm{A}$. D'autre part, w étant continue, on a $w(x) = y$. Ceci montre que $y \in w(\mathrm{A})$, autrement dit que $w(\mathrm{A})$ est fermé dans F.

Appliquant ceci avec $\mathrm{A} = \mathrm{E}$, on voit tout d'abord que $w(\mathrm{E})$ est fermé dans F ; en outre l'application w transforme un fermé de E en un fermé de
3 $w(\mathrm{E})$, donc est un homéomorphisme de E sur $w(\mathrm{E})$, c.q.f.d.

(4) C'est-à-dire un homomorphisme pour E et F munis des topologies affaiblies $\sigma(\mathrm{E}, \mathrm{E}')$ et $\sigma(\mathrm{F}, \mathrm{F}')$. Cf. EVT, Chap. IV, § 2, n° 1.

(5) Cf. EVT, Chap. IV, § 2, n° 3. Rappelons la démonstration :

On sait que le dual de E′, muni de la topologie faible $\sigma(\mathrm{E}', \mathrm{E})$, est égal à E ; comme la topologie $\mathscr{T}_c$ est plus fine que $\sigma(\mathrm{E}', \mathrm{E})$, il en résulte que E est contenu dans E_0, dual de E'_c. Soit $x_0 \in \mathrm{E}_0$; puisque x_0 est une forme linéaire continue sur E'_c, il existe un voisinage V′ de 0 dans E'_c tel que x_0 soit $\leqslant 1$ en

valeur absolue sur V', autrement dit tel que $x_0 \in (V')^0$. Vu la définition de $\mathscr{T}_c$, on peut supposer qu'il existe un ensemble compact convexe K dans E tel que $V' \supset K^0$; on a donc $x_0 \in K^{00}$. Or on sait que K est dense dans K^{00} pour la topologie $\sigma(E_0, E')$; d'autre part, K est compact pour la topologie initiale de E, donc aussi pour $\sigma(E, E')$ qui est moins fine et séparée, donc aussi pour $\sigma(E_0, E')$ qui coïncide visiblement avec $\sigma(E, E')$ sur E. Il s'ensuit que $K = K^{00}$, d'où $x_0 \in E$, et $E_0 = E$, c.q.f.d.

(6) Cf. EVT, Chap. IV, § 2, n° 1.

(7) Pour qu'une application linéaire continue soit un homomorphisme faible, il faut et il suffit que l'image de l'application transposée soit faiblement fermée. Cf. EVT, Chap. IV, § 4, n° 1, ainsi que J. DIEUDONNÉ, *Annales Sci. E.N.S.* **59** (1942), 107–139, th. 14.

(8) Le polaire V^0 de V est l'ensemble des $x' \in E'$ tels que $\mathrm{Re}\langle x', x\rangle \leqslant 1$ pour tout $x \in V$. Cf. EVT, Chap. IV, § 1, n° 3.

(9) Tout homomorphisme est aussi un homomorphisme pour les topologies affaiblies correspondantes, autrement dit, est un homomorphisme faible. Cela résulte immédiatement des deux propriétés suivantes, faciles à démontrer (cf. EVT, Chap. IV, § 1, n° 4) :

a) La topologie faible d'un sous-espace est induite par la topologie faible de l'espace ambiant.

b) La topologie faible d'un quotient (par un sous-espace fermé) est identique à la topologie quotient de la topologie faible de l'espace initial.

(10) Un espace de Fréchet est un espace localement convexe, métrisable et complet. Cf. EVT, Chap. II, § 2, n° 1.

(11) Il suffit de montrer que tout compact de F est l'image par u d'un compact de E, puisque l'enveloppe convexe fermée d'un compact de E est un compact de E (car E est complet, cf. EVT, Chap. II, § 4, n° 1).

D'après le théorème de Banach, F est isomorphe à un espace quotient de E par un sous-espace fermé. Munissons E d'une distance invariante par translation (cf. EVT, Chap. I, § 3, n° 1), notée $d(x, x')$, et munissons F de la distance quotient :

$$d(y, y') = \inf_{u(x)=y,\ u(x')=y'} d(x, x').$$

Soit K un compact de F. Il existe un nombre fini de points $y_i \in K$, tels que, si B_i désigne la boule fermée de centre y_i et rayon $1/2$, les intérieurs des B_i recouvrent K. Choisissons dans E des points x_i tels que $u(x_i) = y_i$. Puisque $B_i \cap K$ est compact, il existe un nombre fini de points $y_{i,j} \in B_i \cap K$ tels que, si B_{ij} désigne la boule fermée de centre y_{ij} et de rayon $1/4$, les intérieurs des B_{ij}

recouvrent $B_i \cap K$. Choisissons dans E des points x_{ij} tels que $u(x_{ij}) = y_{ij}$, et que $d(x_i, x_{ij}) \leqslant 3/4$, ce qui est possible, vu la définition de la distance sur F. Puisque $B_{ij} \cap K$ est compact, il existe un nombre fini de points $y_{ijk} \in B_{ij} \cap K$ tels que, si B_{ijk} désigne la boule fermée de centre y_{ijk} et de rayon $1/8$, les intérieurs des B_{ijk} recouvrent $B_{ij} \cap K$. Choisissons dans E des points x_{ijk} tels que $u(x_{ijk}) = y_{ijk}$, et que $d(x_{ij}, x_{ijk}) \leqslant 3/8$. Etc.

Soit H l'ensemble formé par les $x_i, x_{ij}, x_{ijk}, \dots$ Tout point de H est distant de l'un des x_i de moins de $3/4 + 3/8 + \cdots = 3/2$; de même, tout point de H est distant de l'un des x_{ij} (resp. $x_{ijk} \dots$) de moins de $3/4$ (resp. $3/8, \dots$). Donc H est *précompact*. Comme E est complet, $\overline{H}$ est compact. De plus $u(H) = \{y_i, y_{ij}, y_{ijk}, \dots\}$ est une partie dense de K. Donc $u(\overline{H}) = K$, c.q.f.d.

(On notera que la structure vectorielle n'est pas intervenue dans la démons-
4 tration.)

Séminaire Cartan 10 et 17 mai 1954
1953-54, exposés n^{os} XVIII et XIX

FAISCEAUX ANALYTIQUES SUR L'ESPACE PROJECTIF

§ I. La d''-cohomologie

1. Un lemme.

Lemme 1. — *Soit $f(z)$ une fonction différentiable dans le disque $|z| < \mathrm{R}$. Si $\mathrm{R}' < \mathrm{R}$, il existe une fonction différentiable g telle que*

$$\partial g/\partial \bar{z} = f, \quad \textit{dans le disque } |z| < \mathrm{R}'.$$

Si f est en outre fonction différentiable, ou analytique, de paramètres λ_i, on peut choisir pour g une fonction différentiable, ou analytique, de ces paramètres.

Soit φ une fonction différentiable, égale à 1 pour $|z| \leqslant \mathrm{R}' + \varepsilon$ et à 0 pour $|z| \geqslant \mathrm{R} - \varepsilon$, ε étant assez petit. La fonction $f\varphi$ est à support compact. On peut donc en faire le produit de composition avec la fonction $1/\pi z$, qui est localement sommable. Soit

$$g = \frac{1}{\pi z} * (f\varphi),$$

ce produit de composition, qui est une fonction différentiable sur $\mathbf{C}$. Si l'on considère $1/\pi z$ comme une distribution, on a :

$$\frac{\partial}{\partial \bar{z}}\left(\frac{1}{\pi z}\right) = \delta,$$

mesure de Dirac à l'origine (cf. L. Schwartz, *Théorie des Distributions*, (II, 3; 28)). D'où $\partial g/\partial \bar{z} = f\varphi$, qui est égal à f pour $|z| < \mathrm{R}'$.

En outre, la continuité du produit de composition montre que, si f dépend différentiablement, ou analytiquement, de paramètres, il en est de même de g.

Note. — Un résultat analogue vaut pour les distributions : on remplace f par une distribution sur le produit direct de $|z| < \mathrm{R}$ par l'espace des paramètres,

et l'on fait un produit de composition avec $\frac{1}{\pi z} \times \delta_\lambda$, δ_λ désignant la mesure de Dirac de l'espace des paramètres.

2. La d''-cohomologie locale. — On sait (cf. Séminaire 1951-1952, exposé I) que sur toute variété analytique complexe on a la notion de forme différentielle *de type* (p, q) : c'est une forme dont l'expression au moyen de coordonnées locales complexes z_i fait intervenir p différentielles dz_i et q différentielles $d\bar{z}_j$. Si ω est de type (p, q), $d\omega$ est somme d'une forme de type $(p+1, q)$ et d'une forme de type $(p, q+1)$, que l'on note respectivement $d'\omega$ et $d''\omega$.

On observera que $d'' \circ d'' = 0$; autrement dit d'' peut être considéré comme un opérateur de cobord.

PROPOSITION 1. — *Dans l'espace* $\mathbf{C}^k$*, considérons le polycylindre* D (resp. D′) *défini par les inégalités* $|z_1| < \mathrm{R}_1, \ldots, |z_k| < \mathrm{R}_k$ (resp. $|z_1| < \mathrm{R}'_1, \ldots, |z_k| < \mathrm{R}'_k$, *avec* $|\mathrm{R}'_i| < \mathrm{R}_i$ *pour tout* i).

Soit ω *une forme différentielle, différentiable sur* D*, de type* (p, q) *avec* $q \geqslant 1$*, et telle que* $d''\omega = 0$*. Il existe alors une forme différentielle* α*, différentiable sur* D*, de type* $(p, q-1)$*, telle que* $\omega = d''\alpha$ *sur* D′*.*

Nous montrerons, par récurrence sur i, la proposition suivante qui coïncide avec la proposition 1 pour $i = k$:

(A_i) Soit ω une forme différentielle de type $(p, q), q \geqslant 1$, vérifiant les conditions suivantes :

a) $d''\omega = 0$ pour $|z_j| < \mathrm{R}_j$ $(j \leqslant i)$ et $|z_j| < \mathrm{R}'_j$ $(j > i)$,

b) ω ne contient pas $d\bar{z}_{i+1}, \ldots, d\bar{z}_k$ (pour les valeurs ci-dessus des z_i).

Il existe alors α telle que $d''\alpha = \omega$ sur D′.

Pour $i = 0$, l'hypothèse b) entraîne $\omega = 0$ puisque $q \geqslant 1$. Donc (A_0) est vraie.

Montrons que (A_{i-1}) $\Rightarrow$ (A_i) :

Ecrivons ω sous la forme $\omega = d\bar{z}_i \wedge \beta + \gamma$, où β et γ ne contiennent pas $d\bar{z}_i, \ldots, d\bar{z}_k$. Si f désigne l'un des coefficients de β, on peut, d'après le lemme 1, trouver une fonction g telle que $\partial g / \partial \bar{z}_i = f$ pour $|z_j| < \mathrm{R}_j$ $(j \leqslant i-1)$, $|z_j| < \mathrm{R}'_j$ $(j > i-1)$. En outre, les conditions a) et b) entraînent évidemment que les coefficients de ω, donc de β et γ, sont des fonctions holomorphes de $z_{i+1}, \ldots, z_k$; on pourra donc prendre pour g une fonction holomorphe de ces mêmes variables. Au moyen des fonctions g, on construit de manière évidente une forme ω_i telle que :

$$d''\omega_1 = d\bar{z}_i \wedge \beta + \gamma', \quad \text{pour } |z_j| < \mathrm{R}_j \ (j > i), \ |z_j| < \mathrm{R}'_j \ (j \geqslant i),$$

où γ' ne contient pas $d\bar{z}_i, \ldots, d\bar{z}_k$ (pour les valeurs ci-dessus des z_i).

On a donc $\omega = d''\omega_1 + (\gamma - \gamma')$, et, en appliquant (A_{i-1}) à la forme $\gamma - \gamma'$, on obtient le résultat cherché.

COROLLAIRE. — *Toute forme différentielle de type (p, q), qui est d''-fermée, est localement un d''-cobord si $q \geqslant 1$.*

Remarque. — 1) La proposition 1 et son corollaire sont également valables pour les *courants* de type (p, q), c'est-à-dire pour les formes différentielles à coefficients distributions. La démonstration est la même.

2) Les résultats précédents sont dus à GROTHENDIECK (non publié). On en trouvera une démonstration un peu différente dans une note de DOLBEAULT (C.R.A.S. **236** (1953), 175–177)).

3. Un théorème de DOLBEAULT. — Soit X une variété analytique complexe, de dimension complexe égale à k. Nous désignerons par $\mathscr{A}^{p,q}$ le faisceau des germes de formes de type (p, q) sur X. L'opération d'' étant de type local définit un homomorphisme de $\mathscr{A}^{p,q}$ dans $\mathscr{A}^{p,q+1}$.

Soit d'autre part Ω^p le faisceau des germes de formes holomorphes de degré p sur X; Ω^p est un sous-faisceau de $\mathscr{A}^{p,0}$.

PROPOSITION 2. — *La suite d'homomorphismes de faisceaux :*

$$0 \longrightarrow \Omega^p \longrightarrow \mathscr{A}^{p,0} \xrightarrow{d''} \mathscr{A}^{p,1} \xrightarrow{d''} \cdots \longrightarrow \mathscr{A}^{p,k} \longrightarrow 0.$$

est une suite exacte.

Cela résulte du corollaire à la proposition 1 et du fait évident que les formes de type $(p, 0)$ qui sont d''-fermées sont holomorphes.

Soit maintenant $A^{p,q}$ l'espace vectoriel des formes de type (p, q) définies sur X tout entier [autrement dit, $A^{p,q} = H^0(X, \mathscr{A}^{p,q})$]; l'opération d'' applique $A^{p,q}$ dans $A^{p,q+1}$, et $d'' \circ d'' = 0$. Si l'on désigne par A la somme directe des $A^{p,q}$, on voit que A est un complexe bigradué, l'opérateur cobord étant homogène et de bidegré égal à $(0, 1)$. Nous désignerons le groupe de cohomologie de bidegré (p, q) de A par $H^{p,q}(A)$.

Puisque les $\mathscr{A}^{p,q}$ sont des faisceaux fins, on peut appliquer à la suite exacte de la proposition 2 un résultat élémentaire de théorie des faisceaux (cf. exposé XVII, prop. 1), et l'on obtient ainsi (DOLBEAULT, *loc. cit.*) :

PROPOSITION 3. — $H^q(X, \Omega^p)$ *est isomorphe à* $H^{p,q}(A)$.

Bien entendu, un résultat analogue vaut pour la cohomologie à supports dans une « famille Φ », et pour les formes différentielles à coefficients distributions; on peut également considérer des formes à coefficients dans un espace
1 fibré analytique à fibre vectorielle.

4. Applications. — La proposition 3 a de nombreuses applications. Par exemple, si X est une variété de Stein, on sait que $H^q(X, \Omega^p) = 0$ pour $q \geqslant 1$, puisque Ω^p est un faisceau analytique cohérent; donc $H^{p,q}(A) = 0$. Autrement dit :

Sur une variété de Stein, toute forme de type (p, q), $q \geqslant 1$, *qui est* d''*-fermée, est un* d''*-cobord.*

En particulier, on voit que l'on peut améliorer la proposition 1 en prenant $R'_i = R_i$ pour tout i. A vrai dire, il serait facile d'obtenir cette amélioration sans passer par la théorie des variétés de Stein : il suffirait de faire un « passage à la limite », analogue à celui utilisé dans la démonstration des théorèmes du type Mittag-Leffler.

Mais les applications les plus intéressantes de la proposition 3 concernent les variétés *kählériennes* compactes. On sait en effet (cf. Séminaire 1951-1952, exposé I) que, sur une telle variété, $H^{p,q}(A)$ est isomorphe à l'espace vectoriel des *formes harmoniques de type* (p, q). Il en résulte en particulier que $H^{p,q}(A)$
2 est symétrique en p et q; par exemple, $H^q(X, \mathscr{O}) = H^{0,q}(A)$ est isomorphe à $H^{q,0}(A) = H^0(X, \Omega^q)$, espace des formes holomorphes de degré q (nous avons noté $\mathscr{O}$ le faisceau des germes de fonctions holomorphes sur X, identifié au faisceau Ω^0 des germes de formes holomorphes de degré 0). Si X est l'espace projectif complexe de dimension k, il est immédiat que toute forme différentielle holomorphe sur X, de degré $\geqslant 1$, est identiquement nulle (passer à l'espace vectoriel dont X est un quotient, par exemple). D'où le résultat suivant, qui sera utilisé plus loin :

$H^q(X, \mathscr{O}) = 0$ *pour* $q \geqslant 1$ *si* X *est un espace projectif.*

§ II. Les théorèmes fondamentaux

5. Le faisceau $\mathscr{O}(n)$. — Soit k un entier $\geqslant 0$, et soit Y le complémentaire de l'origine dans l'espace $\mathbf{C}^{k+1}$. Le quotient X de Y par la relation d'équivalence définie dans Y par les homothéties est l'espace projectif complexe $\mathbf{P}_k(\mathbf{C})$. Nous noterons π la projection $Y \to X$; si U est une partie de X, on posera $D_U = \pi^{-1}(U)$; par exemple, si $x \in X$, D_x est une droite (privée de l'origine).

Sur $\mathbf{C}^{k+1}$, les fonctions coordonnées seront notées $z_0, \ldots, z_k$. Pour $0 \leqslant i \leqslant k$, l'ensemble V_i des points de $\mathbf{C}^{k+1}$ où $z_i \neq 0$ est un ouvert contenu dans Y; soit $U_i = \pi(V_i) \subset X$. L'ensemble des points de Y où $z_i = 1$, soit W_i, est un espace

affine analytiquement isomorphe à $\mathbf{C}^k$, et π est un isomorphisme de W_i sur U_i. En particulier les U_i sont des variétés de Stein, et nous avons ainsi défini un recouvrement $\mathscr{U} = \{\mathrm{U}_i\}$ de X par des variétés de Stein, qui est de dimension k (puisqu'il est formé de $k+1$ ouverts d'intersection non vide). Appliquant alors un théorème de LERAY (cf. exposé XVII), on obtient :

PROPOSITION 4. — *Pour tout faisceau analytique cohérent $\mathscr{F}$ sur* X, *on a* $\mathrm{H}^q(\mathscr{U}, \mathscr{F}) = \mathrm{H}^q(\mathrm{X}, \mathscr{F})$ *pour tout* q.

COROLLAIRE. — $\mathrm{H}^q(\mathrm{X}, \mathscr{F}) = 0$ *pour* $q > k$.

Note. — La même démonstration montre que $\mathrm{H}^q(\mathrm{X}, \mathscr{F}) = 0$ pour $q > \dim \mathrm{X}$, si X est une variété projective; j'ignore si ce résultat s'étend à toute variété analytique complexe. 3

Nous allons maintenant définir un faisceau qui jouera dans la suite un rôle important. Soit n un entier (positif ou négatif), et soit U un ouvert de X. Nous désignerons par $\mathscr{O}(n)_\mathrm{U}$ *l'ensemble des fonctions holomorphes sur* D_U *qui sont homogènes de degré* n, c'est-à-dire qui vérifient l'identité :

$$f(tz_0, \ldots, tz_k) = t^n f(z_0, \ldots, z_k) \quad \text{pour } t \in \mathbf{C}^*,\ (z_0, \ldots, z_k) \in \mathrm{D}_\mathrm{U}.$$

L'ensemble $\mathscr{O}(n)_\mathrm{U}$ est un espace vectoriel complexe. Si $\mathrm{V} \subset \mathrm{U}$, la restriction à V d'un élément f de $\mathscr{O}(n)_\mathrm{U}$ est un élément de $\mathscr{O}(n)_\mathrm{V}$, d'où un homomorphisme $\mathscr{O}(n)_\mathrm{U} \to \mathscr{O}(n)_\mathrm{V}$ vérifiant une condition de transitivité évidente. Pour n fixé, les $\mathscr{O}(n)_\mathrm{U}$ définissent donc un faisceau, que nous noterons $\mathscr{O}(n)$. Pour $x \in \mathrm{X}$, un élément de $\mathscr{O}(n)_\mathrm{X}$ peut être identifié à une fonction holomorphe au voisinage de D_x, homogène de degré n. Il est clair que $\mathscr{O}(n)_\mathrm{U}$ est identique à l'espace des sections de $\mathscr{O}(n)$ sur U.

Lorsque $n = 0$, un élément de $\mathscr{O}(n)_\mathrm{U}$ correspond à une fonction holomorphe sur U; autrement dit, le faisceau $\mathscr{O}(0)$ est isomorphe au faisceau $\mathscr{O}$ des germes de fonctions holomorphes sur X.

Si $f \in \mathscr{O}(n)_\mathrm{U}$ et $g \in \mathscr{O}(m)_\mathrm{U}$, on a $f \cdot g \in \mathscr{O}(n+m)_\mathrm{U}$; en particulier, pour $m = 0$, on voit que $\mathscr{O}(n)_\mathrm{U}$ est un module sur $\mathscr{O}(0)_\mathrm{U}$; autrement dit $\mathscr{O}(n)$ est un *faisceau analytique* sur X.

Nous allons préciser ce résultat : notons ${}^i\mathscr{O}$ la restriction du faisceau $\mathscr{O}$ à l'ouvert U_i, et $\theta_i : {}^i\mathscr{O} \to \mathscr{O}(n)$ l'homomorphisme de faisceaux définis par la multiplication par z_i^n (multiplication qui transforme bien une fonction homogène de degré 0 en une fonction homogène de degré n). Il est clair que θ_i est *un isomorphisme de* ${}^i\mathscr{O}$ *sur la restriction de* $\mathscr{O}(n)$ *à* U_i; d'autre part, sur $\mathrm{U}_i \cap \mathrm{U}_j$, $\theta_j^{-1} \circ \theta_i = \mu_{ij}$ est égal à la multiplication par $(z_i/z_j)^n$ (c'est bien un automorphisme de $\mathscr{O}$, puisque z_i/z_j est holomorphe inversible sur $\mathrm{U}_i \cap \mathrm{U}_j$).

Donc :

Le faisceau $\mathscr{O}(n)$ peut être défini à partir des faisceaux ${}^i\mathscr{O}$ par recollement au moyen des isomorphismes $\mu_{ij} : {}^i\mathscr{O} \to {}^j\mathscr{O}$. (Pour la notion de recollement de faisceaux, cf. Séminaire 51-52, exposé XX, n° 13.)

On peut également identifier $\mathscr{O}(n)$ au faisceau des germes de sections holomorphes du fibré à fibre vectorielle de dimension 1, défini par les changements de cartes $(z_i/z_j)^n$ (cf. exposé XVII). Bien entendu, ces diverses définitions montrent que $\mathscr{O}(n)$ est *cohérent.*

Déterminons enfin les sections de $\mathscr{O}(n)$ sur X tout entier, en nous bornant au cas $k \geqslant 1$; une telle section est une fonction holomorphe sur Y, et homogène de degré n; son développement de Laurent montre que c'est *un polynôme homogène de degré n en $z_0, \ldots, z_k$.*

6. Les faisceaux $\mathscr{F}(n)$. — Soit $\mathscr{F}$ un faisceau analytique cohérent sur X, et soit ${}^i\mathscr{F}$ la restriction de $\mathscr{F}$ à U_i. La multiplication par $(z_i/z_j)^n$ est évidemment un isomorphisme $\mu_{ij} : {}^i\mathscr{F} \to {}^j\mathscr{F}$ au-dessus de $\mathrm{U}_i \cap \mathrm{U}_j$.

Nous noterons $\mathscr{F}(n)$ le faisceau obtenu à partir des faisceaux ${}^i\mathscr{F}$ par recollement au moyen des isomorphismes μ_{ij}.

Le faisceau $\mathscr{F}(n)$ est donc isomorphe à $\mathscr{F}$ au-dessus de chaque U_i, et c'est en particulier un faisceau analytique *cohérent.* Pour $\mathscr{F} = \mathscr{O}$, on retrouve évidemment le faisceau $\mathscr{O}(n)$ défini plus haut. Vu la définition de $\mathscr{F}(n)$, une section de $\mathscr{F}(n)$ au-dessus d'un ouvert U de X peut être identifié à un système de $k+1$ sections $s_0, \ldots, s_k$, s_i étant une section de $\mathscr{F}$ au-dessus de $\mathrm{U} \cap \mathrm{U}_i$, qui vérifient les relations : $s_j = (z_i/z_j)^n \cdot s_i$ au-dessus de $\mathrm{U} \cap \mathrm{U}_i \cap \mathrm{U}_j$.

On peut donner une caractérisation commode de $\mathscr{F}(n)$ au moyen de la notion de *produit tensoriel* de deux faisceaux analytiques : soient d'abord $\mathscr{F}$ et $\mathscr{G}$ deux faisceaux analytiques, et posons, pour tout $x \in \mathrm{X}$, $\mathscr{H}_x = \mathscr{F}_x \otimes \mathscr{G}_x$, le produit tensoriel étant pris *sur l'anneau $\mathscr{O}_x$*. Si $\mathscr{H}$ désigne la collection des $\mathscr{H}_x$, on montre facilement qu'il existe une structure de faisceau analytique sur $\mathscr{H}$ et une seule, telle que, si $x \mapsto s(x)$ et $x \mapsto t(x)$ sont des sections de $\mathscr{F}$ et de $\mathscr{G}$ respectivement sur un ouvert $\mathrm{U} \subset \mathrm{X}$, l'application $x \mapsto s(x) \otimes t(x) \in \mathscr{H}_x$ soit une section de $\mathscr{H}$ sur U. Le faisceau $\mathscr{H}$ est appelé *produit tensoriel* des faisceaux $\mathscr{F}$ et $\mathscr{G}$, et noté $\mathscr{F} \otimes_{\mathscr{O}} \mathscr{G}$; il jouit de toutes les propriétés du produit tensoriel usuel. Si $\mathscr{F}$ et $\mathscr{G}$ sont cohérents, $\mathscr{F} \otimes_{\mathscr{O}} \mathscr{G}$ est cohérent. (Pour plus de détails sur cette opération, cf. J-P. Serre, *Un théorème de dualité*, Comm. Math. Helv. **29** (1955), 9–26.)

Proposition 5. — *$\mathscr{F}(n)$ est canoniquement isomorphe à $\mathscr{F} \otimes \mathscr{O}(n)$.*

Sur chaque U_i, on a un isomorphisme canonique $\alpha_i : {}^i\mathscr{F} \to {}^i\mathscr{F} \otimes_{\mathscr{O}} {}^i\mathscr{O}$, et il est clair que $\mu_{ij} \circ \alpha_i = \alpha_j \circ \mu_{ij}$, d'où la proposition.

Signalons également une propriété de l'opération $\mathscr{F}(n)$ qui résulte immédiatement de la définition (ou bien de la prop. 5) :

PROPOSITION 6. — *Si $\mathscr{A} \to \mathscr{B} \to \mathscr{C}$ est une suite exacte de faisceaux analytiques cohérents* (les homomorphismes étant analytiques), *la suite $\mathscr{A}(n) \to$* 4
$\mathscr{B}(n) \to \mathscr{C}(n)$ est exacte pour tout $n \in \mathbf{Z}$.

7. Enoncé des théorèmes fondamentaux. — Voici les théorèmes qui, dans le cas de l'espace projectif, jouent le même rôle que les théorèmes A et B de la théorie des variétés de Stein :

Soit $\mathscr{F}$ un faisceau analytique cohérent sur l'espace projectif X. *Il existe un entier $n_0(\mathscr{F})$ tel que, pour tout $n \geqslant n_0(\mathscr{F})$, on ait* :

THEORÈME A. — $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$ *engendre $\mathscr{F}(n)_x$, considéré comme $\mathscr{O}_x$-module, pour tout $x \in \mathrm{X}$.*

THEORÈME B. — $\mathrm{H}^q(\mathrm{X}, \mathscr{F}(n)) = 0$ *pour tout $q \geqslant 1$.*

La démonstration sera donnée au § III. Nous allons nous borner ici à démontrer un résultat préliminaire :

PROPOSITION 7. — $\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n)) = 0$ *pour $q \geqslant 1$ et $n \geqslant 0$.*

Nous raisonnerons par récurrence sur $k = \dim \mathrm{X}$, le théorème étant trivial pour $k = 0$. Supposons-le démontré pour $k-1$, et démontrons-le pour k. Nous raisonnerons alors par récurrence sur n; pour $n = 0$, on a $\mathscr{O}(0) = \mathscr{O}$, cas qui a été traité au n° 4; supposons le démontré pour $n-1$, et démontrons-le pour n.

Soit H l'hyperplan de $\mathbf{C}^{k+1}$ d'équation $z_0 = 0$, et soit $\mathrm{E} = \pi(\mathrm{H} - \{0\})$ l'image de $\mathrm{H} \cap \mathrm{Y}$ dans X, qui est un hyperplan projectif de X, donc qui peut être considéré comme un espace projectif de dimension $k-1$. On peut définir sur E un faisceau analogue au faisceau $\mathscr{O}(n)$ de X, faisceau que nous noterons $\mathscr{O}_{\mathrm{E}}(n)$; si W est un ouvert de E, une section de $\mathscr{O}_{\mathrm{E}}(n)$ sur W est une fonction holomorphe de $z_1, \ldots, z_k$ sur D_{W}, qui est homogène de degré n. Nous noterons $\mathscr{O}_{\mathrm{E}}(n)'$ le faisceau *sur* X qui coïncide avec $\mathscr{O}_{\mathrm{E}}(n)$ sur E, et est nul sur le complémentaire U_0 de E (cf. Séminaire 50-51, exposé XVII). Soit $\rho : \mathscr{O}(n) \to \mathscr{O}_{\mathrm{E}}(n)'$ l'homomorphisme de faisceaux qui fait correspondre à une fonction holomorphe homogène de degré n sa restriction à $\mathrm{H} \cap \mathrm{Y}$. Soit d'autre part $\sigma : \mathscr{O}(n-1) \to \mathscr{O}(n)$ l'homomorphisme de faisceaux qui fait correspondre à une fonction holomorphe homogène de degré $n-1$ son produit par la fonction z_0.

Lemme 2. — *La suite d'homomorphismes de faisceaux* :

$$0 \longrightarrow \mathscr{O}(n-1) \xrightarrow{\sigma} \mathscr{O}(n) \xrightarrow{\rho} \mathscr{O}_{\mathrm{E}}(n)' \longrightarrow 0,$$

est une suite exacte.

Il est évident que σ est injectif, et que $\sigma \circ \rho = 0$. Si $f \in \mathscr{O}_{\mathrm{E}}(n)'_x$, on peut considérer f comme une fonction f' de $z_0, \ldots, z_k$, indépendante de z_0, et $\rho(f') = f$, ce qui montre que ρ est surjectif. Enfin, si $\rho(f) = 0$, $f \in \mathscr{O}(n)_x$, cela signifie que f s'annule sur H, donc est divisible par z_0, et le quotient est un élément $g \in \mathscr{O}(n-1)_x$ tel que $\sigma(g) = f$ ce qui achève de prouver le lemme.

Appliquant la suite exacte de cohomologie, on obtient alors la suite exacte :

$$\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n-1)) \longrightarrow \mathrm{H}^q(\mathrm{X}, \mathscr{O}(n)) \longrightarrow \mathrm{H}^q(\mathrm{E}, \mathscr{O}_{\mathrm{E}}(n)),$$

puisque l'on sait que $\mathrm{H}^q(\mathrm{X}, \mathscr{O}_{\mathrm{E}}(n)') = \mathrm{H}^q(\mathrm{E}, \mathscr{O}_{\mathrm{E}}(n))$, cf. Séminaire 50-51, *loc. cit.*

Or $\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n-1)) = 0$ d'après l'hypothèse de récurrence sur n, et $\mathrm{H}^q(\mathrm{E}, \mathscr{O}_{\mathrm{E}}(n)) = 0$ d'après l'hypothèse de récurrence sur k. D'où $\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n)) = 0$, c.q.f.d.

Remarques. — 1) Il serait facile de calculer complètement les $\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n))$ ($n \geqslant 0$ ou < 0) par la méthode précédente. On trouve $\mathrm{H}^q(\mathrm{X}, \mathscr{O}(n)) = 0$ pour $q \neq 0$ et $\neq k$, $\dim \mathrm{H}^0(\mathrm{X}, \mathscr{O}(n)) = \binom{n+k}{k}$, et $\dim \mathrm{H}^k(\mathrm{X}, \mathscr{O}(n)) = \binom{-n-1}{k}$.

2) On peut obtenir les résultats précédents par une méthode directe, utilisant la proposition 4 (Frenkel, non publié).

La proposition 7 a la conséquence suivante :

Corollaire. — *Le théorème* B *est vrai pour tout faisceau $\mathscr{F}$ isomorphe à une somme directe d'un nombre fini de faisceaux $\mathscr{O}(m)$.*

On se ramène d'abord au cas d'*un seul faisceau* $\mathscr{O}(m)$ en utilisant le fait que l'opération $\mathscr{F}(n)$ commute à la somme directe (et que les groupes de cohomologie d'une somme directe de faisceaux sont isomorphes à la somme directe des groupes de cohomologie de chaque facteur). Ensuite, on remarque que $\mathscr{O}(m)(n)$ est isomorphe à $\mathscr{O}(m+n)$, donc a des groupes de cohomologie nuls pour $n \geqslant -m$.

[De façon générale, $\mathscr{F}(m)(n)$ est isomorphe à $\mathscr{F}(m+n)$.]

§ III. Démonstration des théorèmes fondamentaux

Nous allons démontrer les théorèmes A et B énoncés au n° 7 du § II. Nous désignerons par (A_r) et (B_r) les propositions suivantes :

(A_r) Si X est un espace projectif complexe de dimension r, et si $\mathscr{F}$ est un faisceau analytique cohérent sur X, $H^0(X, \mathscr{F}(n))$ engendre $\mathscr{F}(n)_x$ pour tout $x \in X$ si n est assez grand.

(B_r) Avec les mêmes hypothèses, $H^q(X, \mathscr{F}(n)) = 0$ pour $q \geqslant 1$ si n est assez grand.

Nous allons démontrer (A_r) et (B_r) par récurrence sur r (le cas $r = 0$ étant trivial). De façon plus précise, nous verrons que (A_{r-1}) et $(B_{r-1}) \Rightarrow (A_r)$ et que $(A_r) \Rightarrow (B_r)$.

8. Démonstration de (A_{r-1}) et $(B_{r-1}) \Rightarrow (A_r)$

On observe d'abord que, si $H^0(X, \mathscr{F}(n_0))$ engendre $\mathscr{F}(n_0)_x$ pour un $x \in X$, alors $H^0(X, \mathscr{F}(n_0+n))$ engendre $\mathscr{F}(n_0+n)_x$ pour tout $n \geqslant 0$. En effet, supposons que $x \in U_0$, par exemple. L'application :

$$m \longmapsto (z_0/z_i)^n \cdot m \quad \text{de } {}^i\mathscr{F} \text{ dans } {}^i\mathscr{F},$$

commute aux identifications qui définissent respectivement les faisceaux $\mathscr{F}(n_0)$ et $\mathscr{F}(n_0 + n)$, donc définit un homomorphisme de faisceaux

$$\varphi : \mathscr{F}(n_0) \longrightarrow \mathscr{F}(n_0 + n),$$

qui est un isomorphisme au-dessus de U_0, donc en particulier en x, ce qui démontre évidemment notre affirmation.

D'autre part, si $H^0(X, \mathscr{F}(n_0))$ engendre $\mathscr{F}(n_0)_x$, alors $H^0(X, \mathscr{F}(n_0))$ engendre $\mathscr{F}(n_0)_y$ pour tout y assez voisin de x, puisque le faisceau $\mathscr{F}(n_0)$ est cohérent.

Ces deux remarques permettent de montrer, par un raisonnement facile de compacité, que (A_r) est entraînée par la proposition en apparence plus faible que voici :

(A'_r) Pour tout faisceau analytique cohérent $\mathscr{F}$ sur X, et tout point $x \in X$, $H^0(X, \mathscr{F}(n))$ engendre $\mathscr{F}(n)_x$ pour n assez grand (i.e., pour $n \geqslant n_0(\mathscr{F}, x)$).

Nous allons maintenant démontrer (A'_r).

Soit donc $x \in X$. Quitte à changer de système de coordonnées dans $\mathbf{C}^{r+1}$, nous pouvons supposer que $z_0 = 0$ en x, autrement dit que $x \in E$, E désignant l'hyperplan d'équation $z_0 = 0$.

Considérons de nouveau l'homomorphisme $\varphi : \mathscr{F}(-1) \to \mathscr{F}$ défini plus haut (sur chaque U_i, c'est la multiplication par z_0/z_i), et soient $\mathscr{H}$ et $\mathscr{G}$ le noyau et le conoyau de φ, respectivement. On a donc la suite exacte :

$$0 \longrightarrow \mathscr{H} \longrightarrow \mathscr{F}(-1) \xrightarrow{\varphi} \mathscr{F} \longrightarrow \mathscr{G} \longrightarrow 0.$$

D'où, en tenant compte de la proposition 6, et du fait que $\mathscr{F}(-1)(n)$ est isomorphe à $\mathscr{F}(n-1)$, la suite exacte :

$$0 \longrightarrow \mathscr{H}(n) \longrightarrow \mathscr{F}(n-1) \xrightarrow{\varphi} \mathscr{F}(n) \longrightarrow \mathscr{G}(n) \longrightarrow 0.$$

Dans cette suite exacte, l'homomorphisme φ est encore donné, sur chaque U_i, par la multiplication par z_0/z_i.

Examinons les propriétés des faisceaux $\mathscr{H}$ et $\mathscr{G}$. Comme φ est évidemment un isomorphisme de $\mathscr{F}(-1)$ sur $\mathscr{F}$ au-dessus de $U_0 = X - E$, on a $\mathscr{H}_y = \mathscr{G}_y = 0$ si $y \notin E$. D'autre part, si $y \in E$, et si f est un élément de $\mathscr{O}_y$ qui induit 0 sur E, on a $f \cdot m = 0$ pour tout $m \in \mathscr{H}_y$ et tout $m \in \mathscr{G}_y$ (en effet, si $y \in U_i$, f est un multiple de z_0/z_i, et notre affirmation résulte de la définition de $\mathscr{H}_y$ et $\mathscr{G}_y$ comme noyau et conoyau de la multiplication par z_0/z_i). Il en résulte que, si l'on note $\mathscr{O}_y(E)$ l'anneau des germes de fonctions holomorphes sur E au point y, $\mathscr{H}_y$ et $\mathscr{G}_y$ sont des $\mathscr{O}_y(E)$-modules. Notons $\mathscr{H}^*$ et $\mathscr{G}^*$ les faisceaux induits par $\mathscr{H}$ et $\mathscr{G}$ sur E; d'après ce qui précède, ce sont des faisceaux analytiques *sur* E, et il est facile de voir qu'ils sont cohérents. D'après le Séminaire 1950-51, exposé XVII, on a $H^q(X, \mathscr{H}) = H^q(E, \mathscr{H}^*)$, et de même pour $\mathscr{G}$.

Tout ceci s'applique également aux faisceaux $\mathscr{H}(n)$ et $\mathscr{G}(n)$: les faisceaux $\mathscr{H}(n)^*$ et $\mathscr{G}(n)^*$ qu'ils induisent sur E sont analytiques cohérents, et d'ailleurs isomorphes aux faisceaux $\mathscr{H}^*(n)$ et $\mathscr{G}^*(n)$ (comme d'habitude, l'isomorphisme est évident sur chaque U_i, et commute aux identifications sur $U_i \cap U_j$).

On a donc, pour $q \geqslant 1$,

$H^q(X, \mathscr{G}(n)) = H^q(E, \mathscr{G}(n)^*) = H^q(E, \mathscr{G}^*(n)) = 0$ pour $n \geqslant n_0$, d'après (B_{r-1}) appliqué au faisceau $\mathscr{G}^*$ sur E.

Résultat identique pour $\mathscr{H}(n)$.

Soit alors $\mathscr{J}_n$ l'image de φ, qui est un sous-faisceau de $\mathscr{F}(n)$. On a les deux suites exactes de faisceaux :

$$0 \longrightarrow \mathscr{H}(n) \longrightarrow \mathscr{F}(n-1) \longrightarrow \mathscr{J}_n \longrightarrow 0,$$
$$0 \longrightarrow \mathscr{J}_n \longrightarrow \mathscr{F}(n) \longrightarrow \mathscr{G}(n) \longrightarrow 0,$$

d'où les deux suites exactes de cohomologie :

$$H^1(X, \mathscr{F}(n-1)) \longrightarrow H^1(X, \mathscr{J}_n) \longrightarrow H^2(X, \mathscr{H}(n)),$$
$$H^1(X, \mathscr{J}_n) \longrightarrow H^1(X, \mathscr{F}(n)) \longrightarrow H^1(X, \mathscr{G}(n)).$$

D'après ce qui précède, $\mathrm{H}^1(\mathrm{X}, \mathscr{G}(n))$ et $\mathrm{H}^2(\mathrm{X}, \mathscr{H}(n))$ sont nuls pour $n \geqslant n_0$, d'où les inégalités :

$$\dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n-1)) \geqslant \dim \mathrm{H}^1(\mathrm{X}, \mathscr{J}_n) \geqslant \dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n)), \quad n \geqslant n_0.$$

Ces inégalités entraînent que $\dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n))$ est une fonction *décroissante* de n pour $n \geqslant n_0$. Comme $\dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n)) < +\infty$, d'après l'exposé XVII, on en conclut que $\dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n))$ est *indépendant* de n, pour $n \geqslant n_1$, d'où :

$$\dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n-1)) = \dim \mathrm{H}^1(\mathrm{X}, \mathscr{J}_n) = \dim \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n)), \quad n \geqslant n_1.$$

Ainsi l'homomorphisme $\mathrm{H}^1(\mathrm{X}, \mathscr{J}_n) \to \mathrm{H}^1(\mathrm{X}, \mathscr{F}(n))$ applique un espace de dimension finie *sur* un espace de même dimension, donc est injectif. La suite exacte de cohomologie montre alors que :

Pour $n \geqslant n_1$, l'homomorphisme $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n)) \to \mathrm{H}^0(\mathrm{X}, \mathscr{G}(n))$ est surjectif.

Mais on sait que $\mathrm{H}^0(\mathrm{X}, \mathscr{G}(n)) = \mathrm{H}^0(\mathrm{E}, \mathscr{G}^*(n))$, et, d'après (A_{r-1}), $\mathrm{H}^0(\mathrm{E}, \mathscr{G}^*(n))$ engendre $\mathscr{G}^*(n)_x = \mathscr{G}(n)_x$, pour $n \geqslant n_2$. On peut supposer que $n_2 \geqslant n_1$. Nous allons voir maintenant que *pour $n \geqslant n_2$, $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$ engendre $\mathscr{F}(n)_x$*, ce qui achèvera de montrer que (A_{r-1}) et $(\mathrm{B}_{r-1}) \Rightarrow (\mathrm{A}_r)$.

Nous supposerons que $x \in \mathrm{U}_i$, ce qui permet d'identifier $\mathscr{F}(n)$ à $\mathscr{F}$ au-dessus de U_i, et en particulier $\mathscr{F}(n)_x$ à $\mathscr{F}_x$. Cette identification transforme, on l'a vu, l'homomorphisme φ en la multiplication par $t_0 = z_0/z_i : \mathscr{F} \to \mathscr{F}$. Donc $\mathscr{G}(n)_x$ se trouve identifié au quotient de $\mathscr{F}_x$ par $t_0 \cdot \mathscr{F}_x$. Soit alors $\mathscr{D}_x \subset \mathscr{F}_x$ le sous-module de $\mathscr{F}_x$ engendré par les éléments de $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$, $n \geqslant n_2$. D'après ce que nous venons de voir, l'image de $\mathscr{D}_x$ dans $\mathscr{F}_x/t_0 \cdot \mathscr{F}_x$ est égale à $\mathscr{F}_x/t_0 \cdot \mathscr{F}_x$ tout entier. Autrement dit, $\mathscr{F}_x = t_0 \cdot \mathscr{F}_x + \mathscr{D}_x$; posons $\mathscr{A}_x = \mathscr{F}_x/\mathscr{D}_x$; l'égalité précédente signifie que $\mathscr{A}_x = t_0 \cdot \mathscr{A}_x$; appliquant alors le lemme de l'exposé VIII-bis-2 (avec $\mathrm{A} = \mathscr{O}_x$, $\mathrm{F} = \mathscr{A}_x$, I=idéal engendré par t_0 dans $\mathscr{O}_x$), on voit que $\mathscr{A}_x = 0$, d'où $\mathscr{F}_x = \mathscr{D}_x$, ce qui achève la démonstration. 5

La démonstration précédente est inspirée d'une démonstration analogue de KODAIRA-SPENCER (*Divisor class groups on algebraic varieties*, Proc. Nat. Acad. Sci. USA **39** (1953), 868–877). Le théorème de finitude de l'exposé XVII y joue un rôle essentiel.

9. Démonstration de $(\mathrm{A}_r) \Rightarrow (\mathrm{B}_r)$

Pour $q > r$, on a $\mathrm{H}^q(\mathrm{X}, \mathscr{F}(n)) = 0$ quel que soit n, d'après le corollaire à la prop. 4. Nous démontrerons alors (B_r) par récurrence descendante sur q, $q \geqslant 1$.

D'après (A_r), il existe un entier m tel que l'espace $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(m))$ engendre $\mathscr{F}(m)_x$ pour tout $x \in \mathrm{X}$. Soit alors $s_1, \ldots, s_p$ une base de l'espace vectoriel

$\mathrm{H}^0(\mathrm{X}, \mathscr{F}(m))$; à tout système $(f_1, \ldots, f_p)$ de p éléments de $\mathscr{O}_x$, faisons correspondre l'élément $\sum f_i \cdot s_i \in \mathscr{F}(m)_x$. On obtient ainsi un homomorphisme analytique $\theta : \mathscr{O}^p \to \mathscr{F}(m)$, qui est *surjectif* puisque $s_1, \ldots, s_p$ engendrent $\mathscr{F}(m)_x$ pour tout $x \in \mathrm{X}$. Si $\mathscr{G}$ est le noyau de θ, on a donc une suite exacte :

$$0 \longrightarrow \mathscr{G} \longrightarrow \mathscr{O}^p \xrightarrow{\theta} \mathscr{F}(m) \longrightarrow 0.$$

D'où, en appliquant la proposition 6, une suite exacte :

$$0 \longrightarrow \mathscr{G}(n) \longrightarrow \mathscr{O}^p(n) \longrightarrow \mathscr{F}(m+n) \longrightarrow 0$$

D'où la suite exacte de cohomologie :

$$\mathrm{H}^q(\mathrm{X}, \mathscr{O}^p(n)) \longrightarrow \mathrm{H}^q(\mathrm{X}, \mathscr{F}(m+n)) \longrightarrow \mathrm{H}^{q+1}(\mathrm{X}, \mathscr{G}(n)).$$

Or, d'après la proposition 7, on a $\mathrm{H}^q(\mathrm{X}, \mathscr{O}^p(n)) = 0$ pour $n \geqslant 0$, et d'après l'hypothèse de récurrence descendante sur q, $\mathrm{H}^{q+1}(\mathrm{X}, \mathscr{G}(n)) = 0$ pour n assez grand.

Donc $\mathrm{H}^q(\mathrm{X}, \mathscr{F}(m+n)) = 0$ pour n assez grand, ce qui achève la démonstration des théorèmes fondamentaux.

Note. — Il serait très facile de montrer directement que $(\mathrm{B}_r) \Rightarrow (\mathrm{A}_r)$; malheureusement, cela ne permettrait de simplifier aucune des démonstrations précédentes. La même situation se retrouve dans la théorie des variétés de Stein : le théorème B entraîne trivialement le théorème A.

§ IV. Faisceaux cohérents d'idéaux

10. Idéaux de polynômes, et faisceaux d'idéaux. — Soit P un polynôme homogène de degré n en les variables $z_0, \ldots, z_r$. Soit $x \in \mathrm{X}$, et soit t une forme linéaire en $z_0, \ldots, z_r$, non nulle en x. Puisque P/t^n est homogène de degré 0, c'est une fonction rationnelle, holomorphe en x, donc c'est un élément de $\mathscr{O}_x$. Si l'on remplace t par une autre forme linéaire t' jouissant des mêmes propriétés, $\mathrm{P}/t'^n = \mathrm{P}/t^n \cdot (t^n/t'^n)$, et t^n/t'^n est un élément *inversible* de $\mathscr{O}_x$. Ainsi l'application $\mathrm{P} \mapsto \mathrm{P}/t^n$ fait correspondre à tout polynôme homogène P un élément de $\mathscr{O}_x$, défini à la multiplication près par un élément inversible de $\mathscr{O}_x$. En particulier, si $\mathscr{F}_x$ est un idéal de $\mathscr{O}_x$, la propriété $\mathrm{P}/t^n \in \mathscr{F}_x$ est indépendante de t. Nous dirons alors, par abus de langage, que P *appartient* à $\mathscr{F}_x$. De même, si $\mathrm{P}_1, \ldots, \mathrm{P}_k$ sont des polynômes homogènes de degrés $n_1, \ldots, n_k$, l'idéal de $\mathscr{O}_x$ engendré par $\mathrm{P}_1/t^{n_1}, \ldots, \mathrm{P}_k/t^{n_k}$ ne dépend pas de t; on dit que c'est l'idéal *engendré par* les $\mathrm{P}_1, \ldots, \mathrm{P}_k$ *en* x.

Si $\mathscr{F} \subset \mathscr{O}$ est un faisceau cohérent d'idéaux sur X, nous dirons qu'un polynôme homogène P *appartient* à $\mathscr{F}$ sur X si P appartient à $\mathscr{F}_x$ pour tout $x \in \mathrm{X}$.

PROPOSITION 8. — *Pour qu'un polynôme homogène* P*, de degré* n*, appartienne au faisceau cohérent d'idéaux* $\mathscr{F}$ *sur* X*, il faut et il suffit que* P *soit une section de* $\mathscr{F}(n)$.

Tout d'abord, puisque $\mathscr{F} \subset \mathscr{O}$, on a $\mathscr{F}(n) \subset \mathscr{O}(n)$; or l'on sait qu'une section de $\mathscr{O}(n)$ n'est pas autre chose qu'un polynôme homogène de degré n en $z_0, \ldots, z_r$; de façon plus précise, un polynôme homogène P de degré n définit sur chaque U_i une fonction holomorphe $f_i = \mathrm{P}/z_i^n$, avec $f_j = (z_i/z_j)^n \cdot f_i$, c'est-à-dire une section de $\mathscr{O}(n)$, et l'on obtient ainsi toutes les sections de $\mathscr{O}(n)$. 6

Donc les sections de $\mathscr{F}(n)$ peuvent s'identifier aux sections de $\mathscr{O}(n)$ qui appartiennent à $\mathscr{F}(n)_x$ pour tout $x \in \mathrm{X}$, c'est-à-dire aux polynômes P, homogènes de degré n, tels que $\mathrm{P}/z_i^n \in \mathscr{F}_x$ pour tout $x \in \mathrm{U}_i$, ce qui signifie bien que P appartient à $\mathscr{F}$, au sens défini plus haut.

PROPOSITION 9. — *Tout faisceau cohérent d'idéaux sur l'espace projectif* X *est engendré par les polynômes homogènes qui lui appartiennent.*

Soit $\mathscr{F}$ le faisceau d'idéaux en question; d'après le théorème A, il existe $n \geqslant 0$ tel que $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$ engendre $\mathscr{F}(n)_x$ pour tout $x \in \mathrm{X}$. D'après ce qui précède, on peut identifier tout élément de $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$ à un polynôme homogène P, de degré n, appartenant à $\mathscr{F}$ sur X. Soit $\mathrm{P}_1, \ldots, \mathrm{P}_k$ une base de l'espace vectoriel de ces polynômes. Si $x \in \mathrm{U}_i$, dire que $\mathrm{H}^0(\mathrm{X}, \mathscr{F}(n))$ engendre $\mathscr{F}_x$ équivaut à dire que $\mathrm{P}_1/z_i^n, \ldots, \mathrm{P}_k/z_i^n$ engendrent $\mathscr{F}_x$ donc $\mathscr{F}$ est bien engendré par les $\mathrm{P}_1, \ldots, \mathrm{P}_k$, au sens défini plus haut, c.q.f.d.

COROLLAIRE (théorème de CHOW). — *Tout sous-ensemble analytique fermé de* X *est algébrique.*

Soient V ce sous-ensemble et $\mathscr{F}(\mathrm{V})$ le faisceau d'idéaux qu'il définit (c'est un faisceau cohérent, d'après un théorème de H. CARTAN — cf. Séminaire 51-52, exposé XVI). D'après la proposition 9, $\mathscr{F}(\mathrm{V})$ est engendré par des polynômes $\mathrm{P}_1, \ldots, \mathrm{P}_k$, ce qui entraîne évidemment que V est le lieu des zéros de ces polynômes, c.q.f.d.

Séminaire Cartan
1953-54, exposé n° XX

24 mai et 14 juin 1954

FONCTIONS AUTOMORPHES

§ I. Faisceaux de fonctions automorphes

1. Le faisceau $\mathscr{A}(J)$. — Dans tout ce qui suit, X désigne une variété analytique complexe de dimension complexe s, et G un groupe d'automorphismes de X vérifiant les hypothèses (I) et (II) de l'exposé XII. On note Y l'espace quotient X/G, et π la projection canonique $X \to Y$. D'après l'hypothèse (I), Y est séparé; d'ailleurs, on a vu dans l'exposé XII que Y est un espace analytique général. 1

Pour tout $x \in X$, on désigne par $G(x)$ le sous-groupe de G formé des $g \in G$ tel que $g \cdot x = x$; d'après l'hypothèse (II), $G(x)$ est un groupe fini. Plus précisément, l'hypothèse (II) permet de ramener toute question locale sur X et G à une question portant sur un groupe $G(x)$.

Soit $g \mapsto J_g$ un *facteur d'automorphie*, au sens de l'exposé I. Nous allons attacher à ce facteur un faisceau $\mathscr{A}(J)$ porté par l'espace Y :

Pour tout ouvert $U \subset Y$, soit $\mathscr{A}(J)_U$ l'ensemble des fonctions holomorphes sur $\pi^{-1}(U)$ qui sont J-automorphes, c'est-à-dire qui vérifient l'identité :

$$f(g \cdot z) = J_g(z) \cdot f(z) \qquad \text{pour tout } z \in \pi^{-1}(U). \tag{1}$$

Si V est un ouvert contenu dans U, on a un homomorphisme évident (la restriction) : $\mathscr{A}(J)_U \to \mathscr{A}(J)_V$; si $W \subset V \subset U$, on a la propriété de transitivité habituelle. Donc, la famille des $\mathscr{A}(J)_U$ définit un faisceau, qui est le faisceau $\mathscr{A}(J)$. Un élément de $\mathscr{A}(J)_y$, $y \in Y$, peut être identifié à une fonction holomorphe sur un voisinage saturé de $\pi^{-1}(y)$ qui vérifie la condition (1). Il est clair que $\mathscr{A}(J)_U$ coïncide avec $H^0(U, \mathscr{A}(J))$.

Lorsque $J_g = 1$ quel que soit $g \in G$, le faisceau $\mathscr{A}(J)$ est le faisceau $\mathscr{O}$ des germes de fonctions holomorphes sur Y (rappelons que, par définition, une fonction holomorphe sur $U \subset Y$ est une fonction holomorphe sur $\pi^{-1}(U)$ qui est invariante par G).

Le produit d'une fonction J-automorphe par une fonction invariante par G étant encore une fonction J-automorphe, on voit que chaque $\mathscr{A}(\mathrm{J})_y$ est muni d'une structure de $\mathscr{O}_y$-module, ce qui définit sur $\mathscr{A}(\mathrm{J})$ une structure de *faisceau analytique* sur Y.

2. Faisceaux analytiques cohérents sur les espaces analytiques. — Nous venons de définir un faisceau analytique sur l'espace analytique général Y. Or, la théorie des faisceaux cohérents peut s'étendre à l'espace Y :

Plus généralement, donnons-nous un espace topologique Y, muni d'un sous-faisceau $\mathscr{O}$ du faisceau des fonctions continues et faisons l'hypothèse que tout $y \in \mathrm{Y}$ possède un voisinage ouvert isomorphe à un sous-ensemble analytique E d'un ouvert U d'un espace $\mathbf{C}^k$; nous dirons alors que Y est un *espace analytique*. Cette définition est plus large que celle de l'exposé VI, qui revient à exiger que, pour tout $y \in \mathrm{Y}$, $\mathscr{O}_y$ soit intégralement clos; un espace analytique vérifiant cette dernière condition sera dit *normal*; par exemple, l'espace $\mathrm{Y} = \mathrm{X}/\mathrm{G}$ du n° 1 est normal.

Soit alors $\mathscr{F}$ un faisceau de $\mathscr{O}$-modules sur Y; on dira que $\mathscr{F}$ est *cohérent* s'il est localement isomorphe au conoyau d'un homomorphisme analytique $\varphi : \mathscr{O}^q \to \mathscr{O}^p$. Si Y est plongé, comme sous-ensemble analytique (avec la structure induite), dans une variété analytique complexe U, soit $\mathscr{F}'$ le faisceau sur U qui coïncide avec $\mathscr{F}$ sur Y, et est nul en dehors de Y; le faisceau $\mathscr{F}'$ est un faisceau analytique sur U, et l'on a :

Lemme 1. — Pour que $\mathscr{F}$ soit cohérent sur Y*, il faut et il suffit que $\mathscr{F}'$ soit cohérent sur* U*.*

On remarque d'abord que le faisceau $\mathscr{O}'$ est cohérent, puisque c'est le quotient du faisceau $\mathscr{O}(\mathrm{U})$ par le faisceau d'idéaux défini par Y (faisceau qui est cohérent d'après un théorème de CARTAN — cf. Sém. 51-52, exposé XVI). Le lemme se déduit immédiatement de là.

Le lemme 1 donne un critère commode pour qu'un faisceau $\mathscr{F}$ sur Y soit cohérent. On en déduit notamment que le noyau, le conoyau et l'image d'un homomorphisme analytique $\mathscr{F} \to \mathscr{G}$ sont des faisceaux cohérents si $\mathscr{F}$ et $\mathscr{G}$ le sont. Bref toutes les propriétés usuelles des faisceaux cohérents sont valables.

3. Cohérence du faisceau $\mathscr{A}(\mathrm{J})$. — Revenons au faisceau $\mathscr{A}(\mathrm{J})$ du n° 1. Nous nous proposons de démontrer le résultat suivant :

THÉORÈME 1. — *Le faisceau analytique $\mathscr{A}(\mathrm{J})$ est cohérent.*

La question est évidemment locale; il faut démontrer que $\mathscr{A}(\mathrm{J})$ est cohérent au voisinage de tout point donné $y_0 \in \mathrm{Y}$. Soit $x_0 \in \mathrm{X}$ avec $\pi(x_0) = y_0$, et

soit $V(x_0)$ un voisinage ouvert de x_0, stable par $G(x_0)$, et vérifiant l'hypothèse (II) de XII-1 (autrement dit, les relations $g \in G$, $x \in V(x_0)$, $g \cdot x \in V(x_0)$ entraînent $g \in G(x_0)$).

Ces propriétés entraînent que $V(x_0)/G(x_0)$ est isomorphe à $\pi(V(x_0)) \subset Y$; d'autre part, il est clair que la restriction de $\mathscr{A}(J)$ à $\pi(V(x_0))$ est isomorphe au faisceau analogue à $\mathscr{A}(J)$ défini à partir de $V(x_0)$ et de $G(x_0)$, à la place de X et de G. On est donc ramené à étudier ce dernier faisceau. Utilisant ensuite le lemme 1 de l'exposé XII, on voit que l'on est finalement ramené à démontrer le théorème 1 dans le cas particulier suivant :

X *est un espace numérique complexe* $\mathbf{C}^s$, *et* G *est un groupe linéaire fini.*

Notons que, si G opère librement sur X, ce qui précède montre que $\mathscr{A}(J)$ est localement isomorphe à $\mathscr{O}$, donc *a fortiori* cohérent.

4. Cohérence du faisceau $\mathscr{A}(J)$; générateurs. — Nous supposons donc que $X = \mathbf{C}^s$, et que G est un groupe linéaire fini, d'ordre n.

Soient S l'algèbre des polynômes $\mathbf{C}[z_1, \ldots, z_s]$, et S^G la sous-algèbre de S formée des polynômes invariants par G. Soit $J_g(z)$ le facteur d'automorphie donné (qui n'est défini que dans un voisinage ouvert V de l'origine dans $\mathbf{C}^s$; nous pouvons évidemment supposer V stable par G). Le faisceau $\mathscr{A}(J)$ est défini sur $\pi(V) = U \subset X/G$, et nous devons montrer qu'il est cohérent sur U.

Si P est un élément de S, nous désignerons par L(P) la fonction :

$$L(P)(z) = \frac{1}{n} \sum_{g \in G} J_g(z)^{-1} \cdot P(g \cdot z).$$

La fonction L(P) est définie et holomorphe dans V. Si $Q \in S^G$, on a évidemment $L(P \cdot Q) = L(P) \cdot Q$.

On sait que S est un module de type fini sur S^G (cf. XII-4, prop. 1-bis); soit $P_1, \ldots, P_k$ un système de générateurs de ce module.

PROPOSITION 1. — *Les fonctions* $L(P_i)$ *engendrent le* $\mathscr{O}_y$*-module* $\mathscr{A}(J)_y$ *pour tout* $y \in U$.

(Cela a un sens, car il est clair que les L(P) sont des fonctions J-automorphes sur $V = \pi^{-1}(U)$.)

La proposition 1 va résulter de la suivante, où le facteur d'automorphie J n'intervient plus :

PROPOSITION 2. — *Soit* $y \in Y = X/G$, *et soit* f *une fonction holomorphe au voisinage de* $\pi^{-1}(y)$. *On peut écrire* f *sous la forme :*

$$f = \sum_{\alpha} h_\alpha \cdot P_\alpha, \qquad \text{avec } P_\alpha \in S, \text{ et } h_\alpha \in \mathscr{O}_y.$$

Montrons que la prop. 2 entraîne la prop. 1. Soit $y \in \mathrm{U}$, et soit $f \in \mathscr{A}(\mathrm{J})_y$; appliquant la prop. 2 à f, on peut écrire $f = \sum_\alpha h_\alpha \cdot \mathrm{P}_\alpha$, comme ci-dessus. Mais chaque P_α peut lui-même s'exprimer comme combinaison linéaire des $\mathrm{P}_1, \ldots, \mathrm{P}_k$, à coefficients dans S^{G}. D'où :

$$f = \sum_{i=1}^{i=k} h_i \cdot \mathrm{P}_i, \quad \text{avec } h_i \in \mathscr{O}_y.$$

Appliquons alors à f l'opération L (qui s'étend évidemment à toute fonction holomorphe définie sur un ouvert de V stable par G). On a $\mathrm{L}(f) = f$ (puisque f est J-automorphe), et $\mathrm{L}(h_i \cdot \mathrm{P}_i) = h_i \cdot \mathrm{L}(\mathrm{P}_i)$, puisque h_i est invariante par G. D'où :

$$f = \sum_{i=1}^{i=k} h_i \cdot \mathrm{L}(\mathrm{P}_i), \qquad \text{c.q.f.d.}$$

5. Cohérence du faisceau $\mathscr{A}(\mathrm{J})$; démonstration de la proposition 2. — Si $x \in \mathrm{X}$, soit $\mathscr{O}_x$ l'anneau des germes de fonctions holomorphes en x; si $y \in \mathrm{Y} = \mathrm{X}/\mathrm{G}$, soit B_y l'anneau des germes de fonctions holomorphes au voisinage de $\pi^{-1}(y)$; l'anneau B_y est un $\mathscr{O}_y$-module puisque $\mathscr{O}_y$ est le sous-anneau de B_y formé des éléments invariants par G. On a :

$$\mathrm{B}_y = \prod_{x \in \pi^{-1}(y)} \mathscr{O}_x,$$

cette décomposition étant compatible avec la structure de $\mathscr{O}_y$-module de B_y.

Si $x \in \pi^{-1}(y)$, $\mathscr{O}_y$ est isomorphe au sous-anneau de $\mathscr{O}_x$ formé des éléments invariants par $\mathrm{G}(x)$. Il s'ensuit (cf. XII-6, th. 2) que $\mathscr{O}_x$ est un $\mathscr{O}_y$-module de type fini, donc que B_y est également *un $\mathscr{O}_y$-module de type fini.*

Soit C_y le sous-$\mathscr{O}_y$-module de B_y engendré par les polynômes. La proposition 2 équivaut à dire que $\mathrm{C}_y = \mathrm{B}_y$.

Puisque $\mathscr{O}_y$ est un anneau local noethérien, d'idéal maximal I_y (I_y étant l'ensemble des éléments de $\mathscr{O}_y$ nuls en y), on peut munir B_y de la I_y-topologie; rappelons (cf. VIII-bis, n° 2) que les sous-modules $(\mathrm{I}_y)^m \cdot \mathrm{B}_y$, $m = 0, 1, \ldots$, forment une base des voisinages de 0 dans cette topologie. Evidemment, la I_y-topologie de $\mathrm{B}_y/\mathrm{C}_y$ est la topologie quotient de la I_y-topologie de B_y; puisque $\mathrm{B}_y/\mathrm{C}_y$ est un module de type fini, le théorème de Krull (VIII-bis, prop. 2) montre que $\mathrm{B}_y/\mathrm{C}_y$ est séparé, donc que C_y *est fermé dans* B_y. Tout revient donc à prouver que C_y est *dense* dans B_y.

Or la topologie de B_y est la topologie produit de celle des $\mathscr{O}_x$, $x \in \pi^{-1}(y)$. Et la I_y-topologie de $\mathscr{O}_x$ coïncide avec la topologie naturelle de l'algèbre locale $\mathscr{O}_x$,

d'après la prop. 4 de VIII-bis. Donc, pour prouver que C_y est dense dans B_y, il suffit de prouver ceci :

Si l'on se donne un entier N, et, pour tout $x \in \pi^{-1}(y)$, un polynôme Q_x, il existe un polynôme Q tel que, pour chaque $x \in \pi^{-1}(y)$, $Q - Q_x$ soit d'ordre $\geqslant N$ en x.

Comme ce dernier énoncé est un cas particulier de celui démontré dans l'Appendice de XII, la démonstration de la prop. 2 est achevée.

6. Cohérence du faisceau $\mathscr{A}(J)$; relations. — Les notations étant celles des n^{os} 4 et 5, soit U′ un ouvert $\subset U$, et soit $V' = \pi^{-1}(U') \subset V$. Soient $f_1, \ldots, f_n$ un nombre fini de fonctions J-automorphes sur V′; par une *relation* entre les f_i nous entendrons un système $h_1, \ldots, h_n$ d'éléments de $\mathscr{O}_y$, $y \in U'$ tel que l'on ait :

$$h_1 \cdot f_1 + \cdots + h_n \cdot f_n = 0.$$

Les relations au point y forment évidemment un *module* sur $\mathscr{O}_y$.

PROPOSITION 3. — *Les relations entre $f_1, \ldots, f_n$ sont engendrées localement par un nombre fini d'entre elles.*

La question étant locale, nous pouvons supposer U′ connexe, puisque X/G est localement connexe.

Si les fonctions $f_1, \ldots, f_n$ sont toutes identiquement nulles, la proposition 3 est évidente. Supposons donc que f_1, par exemple, ne soit pas identiquement nulle. Considérons la fonction H définie par la formule suivante :

$$H(z) = \prod_{h \in G,\ h \neq 1} f_1(h \cdot z).$$

La fonction H est holomorphe dans V′, non identiquement nulle, et le produit $f_1 \cdot H$ est invariant par G. Il s'ensuit que H est J^{-1}-automorphe, donc que les produits $f_2 \cdot H, \ldots, f_n \cdot H$ sont aussi invariants par G. Posons alors $g_1 = f_1 \cdot H$, $\ldots, g_n = f_n \cdot H$. Toute relation entre les f_i :

$$h_1 \cdot f_1 + \cdots + h_n \cdot f_n = 0,$$

conduit à une relation entre les g_i :

$$h_1 \cdot g_1 + \cdots + h_n \cdot g_n = 0,$$

et réciproquement, puisque H n'est pas identiquement nulle et que U′ est connexe. Or, on sait que le faisceau des relations entre un nombre fini de fonctions données est cohérent (th. d'Oka, Sém. 51-52, exposé XV, qui s'étend immédiatement au cas de l'espace analytique Y). D'où la proposition 3.

Les propositions 1 et 3 entraînent évidemment que le faisceau $\mathscr{A}(\mathrm{J})$ est cohérent, ce qui achève la démonstration du théorème 1.

7. Complément : équivalence locale des facteurs d'automorphie. — Si l'on veut étudier de plus près la structure locale des faisceaux $\mathscr{A}(\mathrm{J})$, on est amené à mettre le facteur d'automorphie J sous une forme aussi simple que possible.

La question étant locale, nous pouvons supposer, comme plus haut, que le groupe G est fini, et laisse fixe le point x au voisinage duquel on étudie le faisceau $\mathscr{A}(\mathrm{J})$.

Deux facteurs d'automorphie J_g et J'_g seront dits *équivalents en* x s'il existe une fonction $h(z)$, holomorphe et non nulle au voisinage de x telle que :

$$\mathrm{J}'_g(z) = \mathrm{J}_g(z)\cdot h(g\cdot z)\cdot h(z)^{-1} \quad \text{pour } z \text{ voisin de } x.$$

Dans ce cas, si f est J-automorphe, $f\cdot h$ est J′-automorphe, et la correspondance $f \mapsto f\cdot h$ définit un isomorphisme du faisceau $\mathscr{A}(\mathrm{J})$ sur le faisceau $\mathscr{A}(\mathrm{J}')$, au voisinage de x.

[Dans le langage de la cohomologie des groupes, l'équivalence peut s'interpréter ainsi : soit $\mathscr{O}_x$ le groupe multiplicatif des éléments inversibles de $\mathscr{O}_x$, groupe sur lequel opère G; un facteur d'automorphie J n'est pas autre chose qu'un 1-cocycle de G à valeurs dans le G-module $\mathscr{O}_x$, et deux facteurs J et J′ sont équivalents s'ils sont cohomologues. Autrement dit, le groupe des classes de facteurs d'automorphie locaux n'est pas autre chose que $\mathrm{H}^1(\mathrm{G}, \mathscr{O}_x)$.]

D'autre part, rappelons qu'on appelle *caractère* d'un groupe G, tout homomorphisme $\varepsilon : \mathrm{G} \to \mathbf{C}$ (si l'ordre de G est n, $\varepsilon(g)$ est nécessairement une racine n-ième de l'unité quel que soit $g \in \mathrm{G}$). Tout caractère est un facteur d'automorphie.

THÉORÈME 2. — *Tout facteur d'automorphie* J *est localement équivalent à un caractère, et à un seul.*

Si $\mathrm{J}_g(z)$ est un facteur d'automorphie au voisinage de x, l'application $g \mapsto \mathrm{J}_g(x)$ est un caractère de G; deux facteurs d'automorphie équivalents définissent le même caractère, et tout caractère peut être obtenu ainsi. Il nous suffit donc de prouver que si J_g définit le caractère unité, J_g est équivalent à 1 au voisinage de x. Or, par hypothèse, $\mathrm{J}_g(z)$ est une fonction holomorphe de z qui prend la valeur 1 au point $z = x$; soit $j_g(z) = \log \mathrm{J}_g(z)$, le log étant choisi de telle sorte que $j_g(x) = 0$; on a $j_{gg'}(z) = j_g(g'\cdot z) + j_{g'}(z)$, comme on le voit

aussitôt. Posons $k(z) = \sum_{h\in G} j_h(z)$. On a :

$$k(g\cdot z) = \sum_{h\in G} j_h(g\cdot z) = \sum_{h\in G}(j_{hg}(z) - j_g(z)) = k(z) - n\cdot j_g(z).$$

Si l'on pose alors :

$$h(z) = e^{-k(z)/n},$$

on a $J_g(z) = h(g\cdot z)\cdot h(z)^{-1}$, ce qui montre que J_g est équivalent à 1, c.q.f.d.

[En langage cohomologique : soit I_x l'idéal maximal de $\mathscr{O}_x$; l'application exponentielle montre que $\mathscr{O}_x$ est isomorphe, en tant que G-module, au produit direct de $\mathbf{C}$ sur lequel G opère trivialement, et de I_x; comme I_x est divisible et sans torsion, et que G est fini, on a $H^1(G, I_x) = 0$, d'où $H^1(G, \mathscr{O}_x) = H^1(G, \mathbf{C}) = \mathrm{Hom}(G, \mathbf{C})$, c.q.f.d.]

Remarques. — 1) Pour une variable, le faisceau $\mathscr{A}(J)$ est toujours localement isomorphe à $\mathscr{O}$; mais il est facile de donner des exemples à plusieurs variables où ce n'est pas le cas. C'est naturel, puisqu'un diviseur d'une variété normale n'est pas toujours localement principal.

2) On définit de la même façon que ci-dessus l'équivalence *globale* de deux facteurs d'automorphie. Le groupe des classes de facteurs d'automorphie est encore isomorphe à $H^1(G, \mathscr{O})$, où $\mathscr{O}$ désigne le groupe multiplicatif des fonctions holomorphes inversibles sur X. Mais ce groupe de cohomologie est beaucoup plus difficile à étudier que dans le cas local; pour donner un exemple, si X est un domaine borné contractile, et si G opère librement sur X, $Y = X/G$ étant compact, on peut montrer que $H^1(G, \mathscr{O})$ est isomorphe au groupe des classes de diviseurs de la variété algébrique Y; on peut également donner des résultats précis lorsque X est le disque unité du plan complexe et que Y est compact (cf. PETERSSON, ainsi que GODEMENT, Sém. Bourbaki, Mars 1954), ou bien encore dans le cas des fonctions abéliennes.

§ II. Cas d'un domaine borné

8. Notations. — Nous nous plaçons maintenant dans les hypothèses des exposés I et XV : X est un domaine borné de $\mathbf{C}^s$, et G un groupe discret d'automorphismes de X tel que $Y = X/G$ soit compact. On sait que les conditions (I) et (II) sont alors vérifiées.

On prend pour facteur d'automorphie J_g le jacobien de $x \mapsto g\cdot x$. Les puissances (positives ou négatives) de J sont encore des facteurs d'automorphie, et l'on note $\mathscr{A}_n$ le faisceau $\mathscr{A}(J^{-n})$. Une section du faisceau $\mathscr{A}_n$ est donc *une forme automorphe de poids n* au sens usuel. 2

Comme dans l'exposé XV, on désigne par q le plus petit entier $\geqslant 1$ tel que $J_g(x)^q = 1$, pour tous les couples (g, x) tels que $g \cdot x = x$. On a vu que, si m est un multiple assez grand de l'entier q, toute base $F_0, \ldots, F_r$ de l'espace vectoriel des séries de Poincaré de poids m définit un plongement de Y comme sous-variété normale de l'espace projectif $\mathbf{P}_r(\mathbf{C})$; on désignera par φ_m ce plongement. Si $x \in X$, et si $\pi(x) = y \in Y$, $\varphi_m(y)$ est donc le point de $\mathbf{P}_r(\mathbf{C})$ de coordonnées homogènes $(F_0(x), \ldots, F_r(x))$. Dans les n^{os} suivants, m désignera toujours un entier ayant les propriétés précédentes.

9. Les faisceaux $\mathscr{A}_n$. — Considérons Y comme plongé dans $\mathbf{P}_r(\mathbf{C})$ au moyen de l'application φ_m; si $\mathscr{F}$ est un faisceau cohérent sur Y, soit $\mathscr{F}'$ le faisceau sur $\mathbf{P}_r(\mathbf{C})$ qui coïncide avec $\mathscr{F}$ sur Y et est nul en dehors de Y; d'après le lemme 1, $\mathscr{F}'$ est cohérent. Le faisceau $\mathscr{F}'(n)$, $n \in \mathbf{Z}$, est alors défini par le procédé de l'exposé XVIII, n° 6; il est nul en dehors de Y, et sa restriction à Y est un faisceau que nous noterons $\mathscr{F}(m; n)$ car il dépend non seulement de n *mais aussi de l'entier* m *choisi.* On peut également définir directement $\mathscr{F}(m; n)$ par le procédé suivant :

Soit V_i l'ensemble des points $x \in X$ tels que $F_i(x) \neq 0$; les V_i sont des ouverts saturés de X qui recouvrent X; soit $U_i = \pi(V_i)$; les U_i, $0 \leqslant i \leqslant r$, forment un recouvrement ouvert de $Y = X/G$. Soit maintenant ${}^i\mathscr{F}$ la restriction du faisceau $\mathscr{F}$ à l'ouvert U_i, et soit $m^n_{i,j} : {}^i\mathscr{F} \to {}^i\mathscr{F}$ l'isomorphisme donné par la multiplication par F_i^n/F_j^n au dessus de $U_i \cap U_j$. *Le faisceau obtenu à partir des faisceaux* ${}^i\mathscr{F}$ *par recollement au moyen des isomorphismes* $m^n_{i,j}$ *n'est autre que* $\mathscr{F}(m; n)$*, comme on le voit tout de suite.*

Sous cette forme on voit que $\mathscr{F}(m; n)$ est un faisceau cohérent sur Y.

On peut appliquer ce qui précède au faisceau $\mathscr{A}_p$, $p \in \mathbf{Z}$. On a :

THÉORÈME 3. — *Le faisceau* $\mathscr{A}_p(m; n)$ *est isomorphe à* $\mathscr{A}_{p+nm}$.

L'isomorphisme est défini ainsi : soit f une section de $\mathscr{A}_{p+nm}$ sur un ouvert $U \subset Y$, c'est-à-dire une fonction automorphe de poids $p + nm$ sur $\pi^{-1}(U)$; posons $f_i = f/F_i^n$, qui est une fonction automorphe de poids p sur l'ouvert $\pi^{-1}(U \cap U_i)$, c'est-à-dire une section de $\mathscr{A}_p$ sur $U \cap U_i$; comme $f_j = (F_i/F_j)^n \cdot f_i$ sur $U \cap U_i \cap U_j$, le système des (f_i) est une section de $\mathscr{A}_p(m; n)$ sur U. On vérifie immédiatement que l'on a bien défini ainsi un isomorphisme $\theta : \mathscr{A}_{p+nm} \to \mathscr{A}_p(m; n)$.

COROLLAIRE. — $H^i(Y, \mathscr{A}_n) = 0$ *pour* $i > 0$ *et* n *assez grand.*

Cela résulte du théorème B de l'exposé XVIII, n° 7, appliqué aux faisceaux $\mathscr{A}_p$, $1 \leqslant p \leqslant m$.

Remarque. — Il est très possible que l'on ait, en fait, $\mathrm{H}^i(\mathrm{Y}, \mathscr{A}_n) = 0$ pour $i > 0$ dès que $n \geqslant 2$; c'est en tout cas ce qui se passe dans le cas d'une variable (cf. exposé IV) et, d'après KODAIRA, dans le cas où G opère librement sur X. Malheureusement, la méthode suivie ici ne semble pas pouvoir donner un résultat aussi précis.

10. Première application du théorème 3. — Les notations étant toujours celles du n° 8, soit $\mathscr{A}_{p-m}^{r+1}$ le faisceau somme directe de $r+1$ faisceaux isomorphes au faisceau $\mathscr{A}_{p-m}$, p étant un entier quelconque.

Une section de $\mathscr{A}_{p-m}^{r+1}$ sur un ouvert $\mathrm{U} \subset \mathrm{Y}$ est donc un système de $r+1$ fonctions automorphes de poids $p-m$ sur $\pi^{-1}(\mathrm{U})$, soient $f_0, \ldots, f_r$. Posons :

$$\rho(f_0, \ldots, f_r) = \sum_{i=0}^{i=r} f_i \cdot \mathrm{F}_i;$$

on obtient ainsi une section de $\mathscr{A}_p$ au-dessus de U (c'est-à-dire une fonction automorphe de poids p sur $\pi^{-1}(\mathrm{U})$).

On a ainsi défini un homomorphisme ρ du faisceau $\mathscr{A}_{p-m}^{r+1}$ dans le faisceau $\mathscr{A}_p$, homomorphisme qui est *analytique*. Il est de plus surjectif, du fait que les U_i recouvrent Y.

L'homomorphisme ρ définit des homomorphismes, que nous noterons encore ρ, de $\mathscr{A}_{p-m}^{r+1}(m;n)$ sur $\mathscr{A}_p(m;n)$ ($n \in \mathbf{Z}$ quelconque); si l'on désigne par θ l'isomorphisme $\mathscr{A}_{p+nm} \to \mathscr{A}_p(m;n)$ du théorème 3, on vérifie sans difficulté que $\rho \circ \theta = \theta \circ \rho$.

Or, on a le lemme suivant :

Lemme 2. — Soient $\mathscr{F}$ et $\mathscr{G}$ deux faisceaux analytiques cohérents sur $\mathbf{P}_r(\mathbf{C})$, et soit ρ un homomorphisme analytique de $\mathscr{F}$ sur $\mathscr{G}$. Pour tout n assez grand, l'homomorphisme

$$\rho : \mathrm{H}^0(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n)) \longrightarrow \mathrm{H}^0(\mathbf{P}_r(\mathbf{C}), \mathscr{G}(n)),$$

défini par ρ, est surjectif.

(Si $\mathscr{I}$ désigne le noyau de ρ, le lemme résulte de ce que $\mathrm{H}^1(\mathbf{P}_r(\mathbf{C}), \mathscr{I}(n)) = 0$ pour n assez grand, d'après le théorème B de l'exposé précédent).

En appliquant le lemme 2 à $\mathscr{F} = \mathscr{A}_{p-m}^{r+1}$ et $\mathscr{G} = \mathscr{A}_p$, et tenant compte de ce que $\rho \circ \theta = \theta \circ \rho$, on voit que $\rho : \mathrm{H}^0(\mathrm{Y}, \mathscr{A}_{p+(n-1)m}^{r+1}) \to \mathrm{H}^0(\mathrm{Y}, \mathscr{A}_{p+nm})$ est surjectif, pour n assez grand. En d'autres termes :

THÉORÈME 4. — *Il existe un entier n_0 tel que toute forme automorphe f de poids $\geqslant n_0$ puisse s'écrire $f = \sum_{i=0}^{i=r} f_i \cdot \mathrm{F}_i$, les f_i étant des formes automorphes.*

Autrement dit, toute forme automorphe de poids assez grand appartient à l'idéal engendré par les séries de Poincaré de poids m. D'où (cf. exposé I, prop. 1) :

COROLLAIRE 1. — *Toute forme automorphe de poids assez grand est une série de Poincaré.*

Le théorème 4 entraîne évidemment :

COROLLAIRE 2. — *L'algèbre graduée* M *des formes automorphes est un module de type fini sur l'algèbre des polynômes en les* F_i.

(On peut prendre pour générateurs de ce module une base de l'espace vectoriel des formes de poids $< n_0$.)

COROLLAIRE 3. — *L'algèbre* M *est engendrée par un nombre fini d'éléments.*

D'où :

COROLLAIRE 4. — *Tout idéal de* M *a un nombre fini de générateurs.*

(Dans le cas de 2 variables, ces résultats sont dus à M. HERVÉ, Annales ENS, **69** (1952), 277–302.)

11. Complément. — Les résultats du n° précédent peuvent être étendus à des faisceaux cohérents quelconques.

De façon plus précise, soit $\mathscr{F}$ un faisceau analytique cohérent sur l'espace projectif complexe $\mathbf{P}_r(\mathbf{C})$; le raisonnement du théorème 4 montre que, si n est assez grand, toute section f de $\mathscr{F}(n)$ peut s'écrire $f = \sum_{i=0}^{i=r} f_i.z_i$, où les f_i sont des sections de $\mathscr{F}(n-1)$. Il s'ensuit que $\sum_{n=n_0}^{\infty} \mathrm{H}^0(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ est un module gradué de type fini sur l'algèbre de polynômes $\mathrm{S} = \mathbf{C}[z_0, \ldots, z_r]$.
3 On a ainsi attaché à tout faisceau cohérent $\mathscr{F}$ un S-module gradué de type fini qui le caractérise (comme il résulte tout de suite des théorèmes A et B); ceci généralise la correspondance entre faisceaux cohérents d'idéaux et idéaux homogènes de polynômes rencontrée dans l'exposé précédent.

12. Dimension de l'espace des formes automorphes de poids n. — Si $\mathscr{F}$ est un faisceau analytique cohérent sur Y, nous poserons $h^q(\mathrm{Y}, \mathscr{F}) = \dim \mathrm{H}^q(\mathrm{Y}, \mathscr{F})$, et :

$$\chi(\mathrm{Y}, \mathscr{F}) = \sum_{i=0}^{\infty} (-1)^i h^i(\mathrm{Y}, \mathscr{F}),$$

somme qui est en réalité *finie*. Si $0 \to \mathscr{A} \to \mathscr{B} \to \mathscr{C} \to 0$ est une suite exacte de faisceaux cohérents, la suite exacte de cohomologie montre que $\chi(\mathscr{B}) =$

$\chi(\mathscr{A}) + \chi(\mathscr{C})$. On en déduit que, plus généralement, si l'on a une suite exacte de faisceaux cohérents :

$$0 \longrightarrow \mathscr{C}_0 \longrightarrow \mathscr{C}_1 \longrightarrow \cdots \longrightarrow \mathscr{C}_h \longrightarrow 0,$$

on a :

$$\chi(\mathrm{Y}, \mathscr{C}_0) - \chi(\mathrm{Y}, \mathscr{C}_1) + \cdots + (-1)^h \chi(\mathrm{Y}, \mathscr{C}_h) = 0.$$

Mêmes notations et mêmes résultats si l'on a un faisceau cohérent $\mathscr{F}$ non plus sur Y, mais sur $\mathbf{P}_r(\mathbf{C})$.

PROPOSITION 4. — *Si $\mathscr{F}$ est un faisceau analytique cohérent sur $\mathbf{P}_r(\mathbf{C})$, $\chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ est un polynôme en n, de degré $\leqslant r$.*

On raisonne par récurrence sur $r = \dim \mathbf{P}_r(\mathbf{C})$, le résultat étant évident pour $r = 0$; utilisant la suite exacte du n° 8 de l'exposé précédent, on voit que

$$\begin{aligned} \Delta\chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n)) &= \chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n)) - \chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n-1)) \\ &= \chi(\mathbf{P}_{r-1}(\mathbf{C}), \mathscr{G}(n)) - \chi(\mathbf{P}_{r-1}(\mathbf{C}), \mathscr{H}(n)) \end{aligned}$$

d'où le résultat, grâce à l'hypothèse de récurrence.

COROLLAIRE. — *Pour n assez grand, $h^0(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ est un polynôme en n de degré inférieur ou égal à r.*

En effet, il résulte du théorème B que $h^0(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ est égal à $\chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ pour n assez grand.

On tire tout de suite de la proposition 4 :

PROPOSITION 5. — *Si $\mathscr{F}$ est un faisceau analytique cohérent sur Y, $\chi(\mathrm{Y}, \mathscr{F}(m; n))$ est un polynôme en n (m étant fixé).*

COROLLAIRE. — *Pour n assez grand, $h^0(\mathrm{Y}, \mathscr{F}(m; n))$ est un polynôme en n.*

(Il serait facile de montrer que ce polynôme est de degré inférieur ou égal à $s = \dim \mathrm{Y}$.)

Nous allons maintenant appliquer la proposition 5 et son corollaire aux faisceaux $\mathscr{A}_p$.

Nous noterons d_p la dimension de l'espace vectoriel des formes automorphes de poids p; on a évidemment $d_p = h^0(\mathrm{Y}, \mathscr{A}_p)$. Remarquons que $d_0 = 1$ (toute forme automorphe de poids 0 est constante, comme il résulte tout de suite du principe du maximum et de la compacité de Y), et que $d_p = 0$ pour $p < 0$ (car s'il y avait une forme automorphe de poids < 0 non identiquement nulle, en multipliant une de ses puissances par une forme automorphe de poids opposé, on trouverait une forme automorphe de poids 0 non constante).

Nous poserons $\chi(p) = \chi(\mathrm{Y}, \mathscr{A}_p)$. D'après le corollaire au théorème 3, on a $\chi(p) = d_p$ pour p assez grand. D'après la proposition 5 jointe au théorème 3, $\chi(p + nm)$ est un *polynôme* en n, pour p et m fixés (m vérifiant toujours les hypothèses du n° 8). Nous allons préciser ce résultat :

THÉORÈME 5. — *Il existe des polynômes* $\mathrm{P}_1, \ldots, \mathrm{P}_q$ *vérifiant les propriétés suivantes* :

a) $\chi(n) = \mathrm{P}_i(n)$ *si* $n \equiv i \mod q$;

b) les polynômes P_i *sont de degré* $s = \dim \mathrm{Y}$*, et ont même terme de plus haut degré* $a \cdot n^s/s!$;

c) le coefficient a *est égal à* $\deg \varphi_m(\mathrm{Y})/m^s$*, où* $\deg \varphi_m(\mathrm{Y})$ *désigne le degré de la variété projective* $\varphi_m(\mathrm{Y}) \subset \mathbf{P}_r(\mathbf{C})$.

(Pour la signification de l'entier q, cf. n° 8.)

L'assertion a) peut encore s'écrire :

$$\chi(n) = a \cdot n^s/s! + a_1 \cdot n^{s-1} + \cdots + a_s,$$

où, d'après a) et b), les $a_1, \ldots, a_s$ ne dépendent que de la classe de $n \mod q$.

On notera que la formule précédente est valable pour *tout* n (positif ou négatif); mais pour n assez grand, $\chi(n)$ est égal à d_n; d'où :

COROLLAIRE. — $d_n = a \cdot n^s/s! + a_1 \cdot n^{s-1} + \cdots + a_s$ *pour* n *assez grand.*

Remarques. — 1) Pour calculer $\deg \varphi_m(\mathrm{Y})$, on peut procéder ainsi : on prend s combinaisons linéaires génériques de $\mathrm{F}_0, \ldots, \mathrm{F}_r$, soient $\Phi_1, \ldots, \Phi_s$, et on compte le nombre de points communs (mod G) aux sous-ensembles $\Phi_1 = 0, \ldots, \Phi_s = 0$ du domaine X.

2) Il est facile de donner des exemples où $a_1, \ldots, a_s$ dépendent effectivement de la classe de $n \mod q$: il suffit de faire des produits directs d'exemples à 1 variable.

3) Pour $s = 2$, le théorème 5 est dû à M. HERVÉ (*loc. cit.*).

13. Démonstration du théorème 5. — Soit m un multiple de q suffisamment grand (cf. n° 8); on a vu plus haut que $\chi(p + nm)$ est alors un polynôme en n (dépendant de p); appliquant ceci pour $p = 1, \ldots, m$, on voit qu'il existe m polynômes $\mathrm{P}_1, \ldots, \mathrm{P}_m$ tels que $\chi(n) = \mathrm{P}_i(n)$ si $n \equiv i \bmod m$. L'assertion a) du théorème 5 équivaut à dire que $\mathrm{P}_i = \mathrm{P}_j$ si $i \equiv j \bmod q$.

Soit m' un autre multiple de q, suffisamment grand, tel que $\mathrm{pgcd}(m, m') = q$; nous pouvons recommencer avec m' ce que nous venons de faire avec m, et il existe donc des polynômes $\mathrm{P}'_i, \ldots, \mathrm{P}'_m$, tels que $\chi(n) = \mathrm{P}'_i(n)$ si $n \equiv i \bmod m'$. Supposons que i et i' soient congrus modulo q; puisque $\mathrm{pgcd}(m, m') = q$, il existe une infinité d'entiers qui sont à la fois congrus à $i \bmod m$ et à $i' \bmod m'$;

si n est un tel entier, on a $\mathrm{P}_i(n) = \chi(n) = \mathrm{P}'_{i'}(n)$, ce qui montre que les polynômes P_i et $\mathrm{P}'_{i'}$ sont identiques. Si maintenant $j \equiv i \bmod q$, on a de même $\mathrm{P}_j = \mathrm{P}'_{i'}$, d'où $\mathrm{P}_i = \mathrm{P}_j$, ce qui achève de démontrer l'assertion a).

Montrons maintenant que deux polynômes P_i et P_j ont même terme de plus haut degré. Choisissons une forme automorphe f, non identiquement nulle, et de poids h congru à $j - i \bmod q$ (une telle forme existe, cf. exposé I). Si g est une forme automorphe de poids $n + h$ qui est congrue à $i \bmod q$, $f \cdot g$ est une forme automorphe de poids $n + h$ qui est congrue à $j \bmod q$. D'où $d_{n+h} \geqslant d_n$, ce qui montre que $\mathrm{P}_j(n + h) \geqslant \mathrm{P}_i(n)$ pour n assez grand et congru à $i \bmod q$. Ceci entraîne évidemment (en faisant tendre n vers $+\infty$) que le terme de plus haut degré de P_i est inférieur à celui de P_j, d'où, en permutant i et j, l'égalité de ces termes.

Pour étudier le terme de plus haut degré des polynômes P_i, on peut donc se borner au cas où $i = q$. Si m est un multiple de q vérifiant les hypothèses du n° 8, on a $d_{nm} = \mathrm{P}_q(nm)$ pour n assez grand. Or, on a le résultat suivant :

Lemme 3. — Si n est assez grand, toute forme automorphe de poids nm est un polynôme en les F_i.

Démonstration. — D'après le théorème 3, $\mathscr{A}_{nm}$ est isomorphe à $\mathscr{A}_0(m; n)$. Or $\mathscr{A}_0$ n'est pas autre chose que le faisceau $\mathscr{O}$ des germes de fonctions holomorphes sur Y. Vu que φ_m est un plongement de Y dans $\mathbf{P}_r(\mathbf{C})$, le faisceau $\mathscr{O}$ est un quotient du faisceau $\mathscr{O}(\mathbf{P}_r(\mathbf{C}))$, soit $\mathscr{O}_1$. Appliquant alors le lemme 2 à $\mathscr{O}_1 \to \mathscr{O}$, on voit que toute section de $\mathscr{A}_0(m; n)$ est image d'une section de $\mathscr{O}_1(n)$, si n est assez grand; ceci signifie exactement que toute forme automorphe de poids nm est un polynômes homogène de degré n en les F_i.

(Ce raisonnement montre, plus généralement, que la série linéaire découpée sur une variété normale par les formes de degré assez grand est complète — résultat bien connu.)

Le lemme 3 montre que, pour n assez grand, $\mathrm{P}_q(nm)$ est égal à la dimension de l'espace vectoriel des polynômes homogènes de degré n en les F_i. Si $\mathfrak{a}_m$ désigne l'idéal homogène de $\mathbf{C}[\mathrm{X}_0, \ldots, \mathrm{X}_r]$ formé des polynômes P tels que $\mathrm{P}(\mathrm{F}_0, \ldots, \mathrm{F}_r) = 0$, et si $\chi_{\mathfrak{a}_m}(n)$ désigne le polynôme de Hilbert de cet idéal, on a donc :

$$\mathrm{P}_q(nm) = \chi_{\mathfrak{a}_m}(n) \quad \textit{pour } n \textit{ assez grand.}$$

Or l'idéal $\mathfrak{a}_m$ n'est pas autre chose que l'idéal de la variété $\varphi_m(\mathrm{Y}) \subset \mathbf{P}_r(\mathbf{C})$; d'après un résultat classique (et élémentaire) son terme de plus haut degré est égal à $(\deg \varphi_m(\mathrm{Y})) \cdot n^s / s!$, ce qui achève de démontrer les assertions b) et c) du théorème 5.

14. Compléments divers. — 1) On trouvera dans l'article de HERVÉ des résultats analogues aux précédents, relatifs à des idéaux de fonctions automorphes. Il serait facile de les retrouver par la méthode suivie ici.

2) Il est possible de déduire le théorème 5 de résultats généraux sur les faisceaux cohérents, qui précisent la proposition 4. On définit la *dimension* s et le *degré* d d'un faisceau analytique cohérent $\mathscr{F}$ sur $\mathbf{P}_r(\mathbf{C})$, et l'on montre (en reprenant la démonstration de la proposition 4) que $\chi(\mathbf{P}_r(\mathbf{C}), \mathscr{F}(n))$ est un polynôme en n dont le terme de plus haut degré est égal à $d{\cdot}n^s/s!$.

3) Les faisceaux $\mathscr{A}_p$ sont en rapport étroit avec certains *diviseurs* de la variété Y. Bornons-nous au cas où G opère librement sur X, de telle sorte que Y soit une variété sans singularités. Si D est un diviseur sur Y, notons $\mathscr{L}(\mathrm{D})$ le faisceau défini ainsi : un élément de $\mathscr{L}(\mathrm{D})_y$, $y \in \mathrm{Y}$, est un germe de fonction méromorphe au voisinage de y, soit f, tel que $(f) \geqslant -\mathrm{D}$ au voisinage de y; le faisceau $\mathscr{L}(\mathrm{D})$ est localement isomorphe à $\mathscr{O}$, donc en particulier cohérent. Soit d'autre part K un diviseur « canonique », c'est-à-dire le diviseur d'une forme différentielle méromorphe de degré s sur Y. Le raisonnement de l'exposé IV donne alors :

PROPOSITION 6. — *Le faisceau $\mathscr{A}_p$ est isomorphe au faisceau $\mathscr{L}(p\mathrm{K})$.*

D'où notamment $\chi(k) = \chi(\mathrm{Y}, \mathscr{L}(k\mathrm{K}))$; appliquant alors à la variété algébrique Y les résultats connus sur les $\chi(\mathrm{Y}, \mathscr{L}(\mathrm{D}))$, on obtient sur $\chi(k)$ des renseignements sensiblement plus précis que ceux donnés par le théorème 5. Par exemple, le « théorème de dualité » donne :

COROLLAIRE. — $\chi(1-k) = (-1)^s \chi(k)$.

4 En outre les résultats récents de HIRZEBRUCH permettent d'exprimer les coefficients du polynôme $\chi(n)$ à partir des classes canoniques de la variété Y.

Lorsque l'on ne suppose plus que G opère librement, il faut introduire une notion de « ramification » pour les diviseurs de Y, et l'on peut alors obtenir une proposition analogue à la proposition 6. Nous n'insisterons pas là-dessus.

§ III. Formes E-automorphes

15. Sous-ensembles analytiques stables par G. — Revenons aux hypothèses du n° 1 : soit X une variété analytique complexe de dimension s, et soit G un groupe d'automorphismes de X vérifiant les hypothèses (I) et (II). Considérons un sous-ensemble analytique E de X, stable par G.

PROPOSITION 7. — *L'ensemble* E/G *est un sous-ensemble analytique de* $\mathrm{Y} = \mathrm{X}/\mathrm{G}$.

La question étant locale, nous pouvons supposer que le groupe G est fini, et que E est défini par l'annulation d'un nombre fini de fonctions holomorphes $f_1, \ldots, f_k$. Pour tout $g \in \mathrm{G}$, soit f_i^g la fonction définie par :

$$f_i^g(x) = f_i(g \cdot x) \qquad 1 \leqslant i \leqslant k.$$

Soit r l'ordre de G; pour chaque indice i, soient $\mathrm{F}_i^1, \ldots, \mathrm{F}_i^r$, les fonctions symétriques élémentaires des r fonctions f_i^g, $g \in \mathrm{G}$. On a donc :

$$\mathrm{F}_i^1 = \sum_{g \in \mathrm{G}} f_i^g, \ldots, \quad \mathrm{F}_i^r = \prod_{g \in \mathrm{G}} f_i^g.$$

Les fonctions F_i^j sont invariantes par G, donc peuvent être considérées comme des fonctions holomorphes sur $\mathrm{Y} = \mathrm{X}/\mathrm{G}$. La proposition 7 est donc une conséquence du lemme suivant.

Lemme 4. — E/G *est défini par l'annulation des fonctions* F_i^j, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant r$.

Il est clair que les F_i^j s'annulent sur E; inversement, soit $x \in \mathrm{X}$ tel que $\mathrm{F}_i^j(x) = 0$ quels que soient i et j; ces équations entraînent $f_i(x) = 0$ pour tout i, d'où $x \in \mathrm{E}$, c.q.f.d.

Corollaire. — *Le faisceau d'idéaux défini par* E/G *dans* Y *est cohérent.*

Cela résulte d'un théorème de Cartan, cf. Séminaire 51-52, exposé XVI.

16. Formes E-automorphes. — Par une fonction holomorphe sur E nous entendrons une fonction continue à valeurs complexes sur E qui peut localement se prolonger en une fonction holomorphe sur X; c'est donc une section du faisceau quotient du faisceau $\mathscr{O}(\mathrm{X})$ par le faisceau d'idéaux $\mathscr{I}(\mathrm{E})$ défini par E.

Donnons-nous d'autre part un facteur d'automorphie $g \mapsto \mathrm{J}_g$ sur X. Une fonction f, holomorphe sur E, sera dite E-*automorphe* (relativement à J, ou encore E-J-automorphe) si elle vérifie la relation

$$f(g \cdot x) = \mathrm{J}_g(x) \cdot f(x) \qquad \textit{pour tout } x \in \mathrm{E}. \tag{2}$$

(Cette notion est due à M. Hervé.)

On peut également définir le *faisceau* des germes de formes E-automorphes; si U est un ouvert de $\mathrm{Y} = \mathrm{X}/\mathrm{G}$, on désigne par $\mathscr{A}(\mathrm{J};\mathrm{E})_{\mathrm{U}}$ l'ensemble des fonctions holomorphes sur $\mathrm{E} \cap \pi^{-1}(\mathrm{U})$ qui vérifient la relation (2) pour tout $x \in \mathrm{E} \cap \pi^{-1}(\mathrm{U})$; à partir des $\mathscr{A}(\mathrm{J};\mathrm{E})_{\mathrm{U}}$ on définit le faisceau $\mathscr{A}(\mathrm{J};\mathrm{E})$ de la manière habituelle. C'est un faisceau analytique sur l'espace Y, nul en dehors de E/G.

THÉORÈME 6. — *Le faisceau analytique* $\mathscr{A}(\mathrm{J};\mathrm{E})$ *est un faisceau analytique cohérent sur l'espace* Y.

Avant de démontrer le théorème 6, remarquons que toute forme automorphe vis-à-vis de J (au sens usuel) définit par restriction à E une forme E-automorphe. D'où un homomorphisme de faisceaux

$$\sigma : \mathscr{A}(\mathrm{J}) \longrightarrow \mathscr{A}(\mathrm{J};\mathrm{E}).$$

Il est clair que σ est un homomorphisme analytique.

PROPOSITION 8. — *L'homomorphisme* σ *est surjectif.*

La question étant locale, nous pouvons supposer G fini, d'ordre n. Si l'on a $f \in \mathscr{A}(\mathrm{J};\mathrm{E})_y$, $y \in \mathrm{Y}$, il existe une fonction f_1, holomorphe au voisinage de $\pi^{-1}(y)$, et qui induit f sur E (cela résulte simplement du fait que f est holomorphe sur E). La fonction :

$$\mathrm{L}(f_1) = \frac{1}{n}\sum_{g\in\mathrm{G}} \mathrm{J}_g(x)^{-1} f_1(g\cdot x)$$

appartient alors à $\mathscr{A}(\mathrm{J})_y$, et induit f sur E, c.q.f.d.

COROLLAIRE 1. — *Le faisceau* $\mathscr{A}(\mathrm{J};\mathrm{E})$ *est engendré localement par un nombre fini de ses sections.*

En effet, le faisceau $\mathscr{A}(\mathrm{J})$ possède cette propriété d'après le théorème 1.

La proposition 8 a une autre conséquence intéressante : prenons pour facteur d'automorphie $\mathrm{J}_g = 1$ quel que soit g; le faisceau $\mathscr{A}(\mathrm{J})$ est alors le faisceau $\mathscr{O}$ des germes de fonctions holomorphes sur Y, et le faisceau $\mathscr{A}(\mathrm{J};\mathrm{E})$ est le faisceau des fonctions holomorphes sur E qui sont invariantes par G, autrement dit, c'est le faisceau $\mathscr{O}(\mathrm{E}/\mathrm{G})$ des germes de fonctions holomorphes sur E/G. Le fait que $\sigma : \mathscr{O} \to \mathscr{O}(\mathrm{E}/\mathrm{G})$ soit surjectif signifie alors que le plongement $\mathrm{E}/\mathrm{G} \to \mathrm{Y} = \mathrm{X}/\mathrm{G}$ transforme le faisceau $\mathscr{O}(\mathrm{E}/\mathrm{G})$ en le faisceau *induit* par $\mathscr{O}$ sur E/G; en particulier, puisque E/G est analytique (prop. 7), on a :

COROLLAIRE 2. — *Le faisceau* $\mathscr{O}(\mathrm{E}/\mathrm{G})$ *est cohérent sur* Y.

17. Démonstration du théorème 6 (fin). — Vu le cor. 1 à la prop. 8, il nous reste seulement à démontrer que les *relations* entre un certain nombre de sections $f_1, \ldots, f_n$ de $\mathscr{A}(\mathrm{J};\mathrm{E})$ forment un faisceau cohérent (c'est-à-dire sont engendrées localement par un nombre fini d'entre elles). Nous suivrons la même méthode qu'au n° 6.

Nous supposons que les fonctions $f_1, \ldots, f_n$ sont holomorphes dans un voisinage ouvert d'un point donné x_0. En remplaçant X par $\mathrm{V}(x_0)$, on peut supposer

que le groupe G est fini d'ordre r, laisse le point x_0 fixe, et que $f_1, \ldots, f_n$ sont holomorphes dans E tout entier. Nous voulons étudier le faisceau des relations entre les f_i au voisinage de x_0.

Soit $\mathrm{E} = \mathrm{E}_1 \cup \mathrm{E}_2 \cup \cdots \cup \mathrm{E}_k$ la décomposition de E en sous-ensembles analytiques irréductibles au voisinage de x_0. Soit K l'ensemble des indices i, $1 \leqslant i \leqslant k$, tels qu'il existe au moins une des fonctions $f_1, \ldots, f_n$ qui ne soit pas identiquement nulle sur E_i; il existe des scalaires $a_1, \ldots, a_n$ tels que $a_1 f_1 + \cdots + a_n f_n$ ne s'annule identiquement sur aucun des E_i, $i \in \mathrm{K}$ (il suffit de choisir les a_i en dehors d'un nombre fini de sous-espaces vectoriels de $\mathbf{C}^n$). Posons $f_0 = a_1 f_1 + \cdots + a_n f_n$; c'est encore une fonction E-automorphe relativement à J. Soit H la fonction définie par la formule :

$$\mathrm{H}(x) = \prod_{h \in \mathrm{G},\ h \neq 1} f_0(h \cdot x).$$

La fonction H est holomorphe sur E, et on vérifie facilement qu'elle est J^{-1}-automorphe sur E. En outre, sa restriction à E_i, $i \in \mathrm{K}$, n'est pas identiquement nulle; car sinon, il y aurait $h \in \mathrm{G}$ tel que $f_0(h \cdot x)$ soit identiquement nulle pour $x \in \mathrm{E}_i$, d'où f_0 identiquement nulle pour $x \in h^{-1} \cdot \mathrm{E}_i = \mathrm{E}_j$, d'où $f_1, \ldots, f_n$ identiquement nulles sur E_j, donc aussi sur E_i, contrairement à la définition de K.

Désignons maintenant par $g_1, \ldots, g_n$ les fonctions $f_1 \cdot \mathrm{H}, \ldots, f_n \cdot \mathrm{H}$. Ce sont des fonctions holomorphes sur E et *invariantes par* G, autrement dit des sections du faisceau $\mathscr{O}(\mathrm{E}/\mathrm{G})$.

Toute relation :

$$h_1 \cdot f_1 + \cdots + h_n \cdot f_n = 0, \tag{3}$$

où les h_i appartiennent à $\mathscr{O}_y$, entraîne la relation :

$$h_1 \cdot g_1 + \cdots + h_n \cdot g_n = 0. \tag{4}$$

La réciproque est vraie : la relation (4) peut en effet s'écrire

$$(h_1 \cdot f_1 + \cdots + h_n \cdot f_n) \cdot \mathrm{H} = 0. \tag{5}$$

D'après un résultat connu (cf. Séminaire 51-52, exposés XIV-5 et XVI), la relation (5) entraîne que $h_1 \cdot f_1 + \cdots + h_n \cdot f_n$ est nul sur E_i pour $i \in \mathrm{K}$ [tout au moins pour y assez voisin de $\pi(x_0)$]; d'autre part $h_1 \cdot f_1 + \cdots + h_n \cdot f_n$ est nul sur E_i si $i \notin \mathrm{K}$. Donc (5)$\Rightarrow$(3), ce qui montre bien que (3) et (4) sont équivalents.

Mais, d'après le cor. 2 à la prop. 8, le faisceau $\mathscr{O}(\mathrm{E}/\mathrm{G})$ est cohérent. Donc le faisceau des relations entre les g_i est cohérent, et comme nous venons de voir qu'il coïncide avec le faisceau des relations entre les f_i, la démonstration du théorème 6 est achevée.

18. Application au cas d'un domaine borné. — Faisons maintenant sur X, G, J les hypothèses du n° 8 : X est un domaine borné de $\mathbf{C}^s$, $Y = X/G$ est compact, J_g est le jacobien en x de l'automorphisme $x \mapsto g \cdot x$.

Notons $\mathscr{A}_k(E)$ le faisceau $\mathscr{A}(J^{-k}; E)$.

THÉORÈME 7. — *Le faisceau* $\mathscr{A}_p(E)(m; n)$ *est isomorphe à* $\mathscr{A}_{p+nm}(E)$.

Ce théorème se démontre exactement comme le théorème 3.

COROLLAIRE. — *Toute forme* E*-automorphe de poids assez grand est la restriction à* E *d'une forme automorphe sur* X.

Appliquant le lemme 2 à l'homomorphisme surjectif $\mathscr{A}_p \to \mathscr{A}_p(E)$, on voit que

$$H^0(Y, \mathscr{A}_p(m; n)) \longrightarrow H^0(Y, \mathscr{A}_p(E)(m; n)) = H^0(E, \mathscr{A}_p(E)(m; n))$$

est surjectif pour n assez grand. Compte tenu des théorèmes 3 et 7 (et d'une relation de commutation évidente), ceci signifie que

$$H^0(Y, \mathscr{A}_{p+mn}) \longrightarrow H^0(E, \mathscr{A}_{p+nm}(E))$$

est surjectif pour n assez grand, d'où le corollaire.

Note. — Le résultat ci-dessus avait été obtenu par M. HERVÉ (C.R.A.S. **234** (1952), 41–43) lorsque X est le produit direct de deux disques et que E vérifie certaines hypothèses particulières.

Séminaire Bourbaki mai 1954
1953-54, exposé n° 100

REPRÉSENTATIONS LINÉAIRES ET ESPACES HOMOGÈNES KÄHLÉRIENS DES GROUPES DE LIE COMPACTS

Les résultats qui vont être exposés sont dus à Armand Borel et André Weil (non publiés) 1

1. Espaces homogènes symplectiques

Une variété compacte connexe X est dite *symplectique* si sa dimension est un nombre pair, soit $2n$, et s'il existe $x \in H^2(X)$ tel que $x^n \neq 0$ (dans ce n°, les groupes de cohomologie sont pris à coefficients *réels*). Toute variété *kählérienne* est symplectique. 2

Théorème 1. — *Soient* G *un groupe de Lie compact, connexe, semi-simple, et* U *un sous-groupe fermé de* G. *Si* G/U *est symplectique, il existe un tore* $S \subset G$ *tel que* U *soit égal au commutant* C(S) *de* S *dans* G (autrement dit, $x \in U \iff x \cdot s = s \cdot x$ pour tout $s \in S$).

En particulier (Hopf), U *est un groupe connexe de même rang que* G.

(Un cas particulier de ce théorème se trouve dans une Note de Lichnerowicz [1] ; voir également [2].)

Démonstration. — Soit U_0 la composante connexe de l'élément neutre de U, soit S (resp. S_0) la composante connexe de l'élément neutre du centre de U (resp. du centre de U_0), et soit $V = C(S)$ le commutant de S dans G. On a donc les inclusions :

$$S \subset S_0 \subset U_0 \subset U \subset V \subset G.$$

Considérons le diagramme commutatif suivant :

$$\begin{array}{ccccc} \mathrm{H}^1(\mathrm{V}) & & \xrightarrow{\quad\alpha\quad} & & \mathrm{H}^1(\mathrm{U}_0)^{\mathrm{U}/\mathrm{U}_0} \\ \downarrow{\scriptstyle\tau} & & & & \downarrow{\scriptstyle\tau} \\ \mathrm{H}^2(\mathrm{G}/\mathrm{V}) & \xrightarrow{\gamma} & \mathrm{H}^2(\mathrm{G}/\mathrm{U}) & \xrightarrow{\beta} & \mathrm{H}^2(\mathrm{G}/\mathrm{U}_0)^{\mathrm{U}/\mathrm{U}_0} \end{array},$$

où τ désigne la *transgression*, et où $\mathrm{H}^1(\mathrm{U}_0)^{\mathrm{U}/\mathrm{U}_0}$ (resp. $\mathrm{H}^2(\mathrm{G}/\mathrm{U}_0)^{\mathrm{U}/\mathrm{U}_0}$) désigne le sous-groupe de $\mathrm{H}^1(\mathrm{U}_0)$ (resp. de $\mathrm{H}^2(\mathrm{G}/\mathrm{U}_0)$) formé des éléments invariants par U/U_0.

Puisque G est semi-simple, $\mathrm{H}^1(\mathrm{G}) = \mathrm{H}^2(\mathrm{G}) = 0$, d'où il résulte tout de suite que τ est une bijection (noter que V est connexe, d'après un résultat bien connu, dû à HOPF). D'autre part, la définition même de V montre que α est surjectif, et un théorème élémentaire sur les revêtements finis montre que β est bijectif. Donc γ est surjectif.

S'il existe $x \in \mathrm{H}^2(\mathrm{G}/\mathrm{U})$ avec $x^n \neq 0$ ($2n = \dim \mathrm{G}/\mathrm{U}$), il existe alors aussi $x' \in \mathrm{H}^2(\mathrm{G}/\mathrm{V})$ avec $x'^n \neq 0$, ce qui entraîne évidemment $\dim \mathrm{G}/\mathrm{V} \geqslant 2n$, d'où $\dim \mathrm{V} \leqslant \dim \mathrm{U}$, d'où $\mathrm{V} = \mathrm{U}$ puisque V est connexe, et l'on a bien $\mathrm{U} = \mathrm{C}(\mathrm{S})$, c.q.f.d.

Remarques. — 1) Réciproquement, si $\mathrm{U} = \mathrm{C}(\mathrm{G})$, on peut construire sur G/U une métrique kählérienne telle que G/U soit une variété de Hodge. Cela peut se voir par une méthode « infinitésimale ». Mais nous obtiendrons au n° 3 un résultat plus précis, en exhibant un plongement de G/U dans un espace projectif.
2) On notera que, parmi les sous-groupes U du type C(S), se trouvent en particulier les *tores maximaux* de G.

2. Structure complexe sur G/U

Soit T un tore maximal de G, $\mathfrak{t}$ (resp. $\mathfrak{g}$) l'algèbre de Lie de T (resp. G). Nous écrirons les racines de $\mathfrak{g}$ (relativement à $\mathfrak{t}$) sous la forme $2\pi i \cdot a_i(x)$, où $a_i(x)$ est une forme linéaire réelle sur $\mathfrak{t}$. Si a est une racine, on désignera par e_a l'élément de $\mathfrak{g}_{\mathbf{C}}$, algèbre de Lie complexifiée de $\mathfrak{g}$, tel que $[t, e_a] = 2\pi i \cdot a(t) \cdot e_a$ pour tout $t \in \mathfrak{t}_{\mathbf{C}}$ (e_a est défini à une homothétie près). Si $a_1, \ldots, a_r$ est un système simple de racines de $\mathfrak{g}$, on notera W la partie de $\mathfrak{t}$ définie par les inégalités $a_i(t) \geqslant 0$, $1 \leqslant i \leqslant r$ (« chambre de Weyl »).

Le produit scalaire (x, y) défini par l'opposé de la forme de Killing de $\mathfrak{g}$ permet d'identifier $\mathfrak{t}$ et $\mathfrak{t}_{\mathbf{C}}$ à leurs duaux; en particulier, les a_i peuvent être considérés comme des éléments de $\mathfrak{t}$.

Nous désignerons par $\mathfrak{h}$ le sous-espace vectoriel de $\mathfrak{g}_{\mathbf{C}}$ engendré par $\mathfrak{t}_{\mathbf{C}}$ et les e_a, où a parcourt l'ensemble des racines $\geqslant 0$ de $\mathfrak{g}$. C'est une sous-algèbre résoluble de $\mathfrak{g}_{\mathbf{C}}$.

Si b est un élément de W, soit P_b l'ensemble des racines $\geqslant 0$ orthogonales à b ; le sous-espace vectoriel de $\mathfrak{g}_{\mathbf{C}}$ engendré par $\mathfrak{h}$ et les e_{-a}, $a \in \mathrm{P}_b$, est une sous-algèbre $\mathfrak{l}_b$ de $\mathfrak{g}_{\mathbf{C}}$ (en effet, $\mathfrak{l}_b$ est engendrée par $\mathfrak{t}_{\mathbf{C}}$ et les e_a où $(a, b) \geqslant 0$, puisque $b \in \mathrm{W}$). Si b est intérieur à W, on a $\mathfrak{l}_b = \mathfrak{h}$; si $b = 0$, $\mathfrak{l}_b = \mathfrak{g}_{\mathbf{C}}$. On voit tout de suite que $\mathfrak{l}_b \cap \mathfrak{g} = \mathfrak{c}(b)$, en désignant par $\mathfrak{c}(b)$ l'ensemble des $x \in \mathfrak{g}$ tels que $[x, b] = 0$. Si S est un tore de T, on peut trouver dans S un sous-groupe à 1 paramètre partout dense, d'où un élément $b \in \mathfrak{t}$ tel que $\mathfrak{c}(b) = \mathfrak{c}(\mathrm{S})$; en outre, en effectuant un automorphisme intérieur, on peut supposer que $b \in \mathrm{W}$.

Nous supposerons à partir de maintenant que G est simplement connexe ; il est clair que cela ne restreint pas la généralité. Soit alors $\mathrm{G}_{\mathbf{C}}$ le groupe complexe simplement connexe d'algèbre de Lie $\mathfrak{g}_{\mathbf{C}}$, qui contient G comme sous-groupe 3
fermé, comme on sait ; soient $\mathrm{T}_{\mathbf{C}}$, H, L_b, $\mathrm{C}(b)$, les sous-groupes fermés de $\mathrm{G}_{\mathbf{C}}$ d'algèbres de Lie $\mathfrak{t}_{\mathbf{C}}$, $\mathfrak{h}$, $\mathfrak{l}_b$, $\mathfrak{c}_b$; ce sont des sous-groupes fermés de $\mathrm{G}_{\mathbf{C}}$ (c'est évident pour $\mathrm{T}_{\mathbf{C}}$ et $\mathrm{C}(b)$; pour L_b, cela résulte de ce que $\mathfrak{l}_b$ est son propre normalisateur dans $\mathfrak{g}_{\mathbf{C}}$, et de même pour H). De plus, on peut montrer que $\mathrm{L}_b \cap \mathrm{G} = \mathrm{C}(b)$ (Borel et Weil utilisent un raisonnement direct, mais cela résulte également du théorème 1 et de la construction du n° 3). On en déduit que $\mathrm{G}/\mathrm{C}(b) = \mathrm{G}_{\mathbf{C}}/\mathrm{L}_b$, et comme on a vu que tout $\mathrm{C}(\mathrm{S})$ est égal à un $\mathrm{C}(b)$, on obtient finalement :

Théorème 2. — *Les espaces homogènes* G/U*, où* $\mathrm{U} = \mathrm{C}(\mathrm{S})$ (S étant un tore de G) *sont des espaces homogènes complexes.*

En particulier, $\mathrm{G}/\mathrm{T} = \mathrm{G}_{\mathbf{C}}/\mathrm{H}$ est un espace homogène complexe, comme l'avait observé Borel dans sa thèse.

(On notera toutefois que la structure complexe de G/U ainsi obtenue *dépend* du système simple de racines choisi.) 4

3. Plongement associé à une représentation irréductible de $\mathrm{G}_{\mathbf{C}}$

Soit $x \mapsto \mathfrak{a}_x$ une représentation linéaire complexe de $\mathfrak{g}_{\mathbf{C}}$ dans un espace vectoriel complexe E de dimension finie. Une forme linéaire b sur $\mathfrak{t}_{\mathbf{C}}$ est dite un *poids* de la représentation, s'il existe $e \neq 0$, $e \in \mathrm{E}$, tel que $\mathfrak{a}_t(e) = 2\pi i \cdot b(t) \cdot e$ pour tout $t \in \mathfrak{t}_{\mathbf{C}}$; un poids est dit *dominant* si $b + a_i$ n'est un poids pour aucune 5
valeur de i $(1 \leqslant i \leqslant r)$; toute représentation possède un poids dominant ; si la représentation est irréductible, ce poids dominant est unique et l'élément e correspondant est bien déterminé (à homothétie près) ; inversement, si E

est engendré par les transformés d'un élément e correspondant à un poids dominant, la représentation est irréductible. Enfin, les poids dominants des diverses représentations de $\mathfrak{g}_{\mathbf{C}}$ sont caractérisés par les formules :

$$(a_i, b) = k_i \cdot (a_i, a_i)/2, \quad k_i \text{ entier} \geqslant 0, \quad 1 \leqslant i \leqslant r.$$

A tout poids dominant b, on peut faire correspondre l'algèbre $\mathfrak{l}_b$, comme au n° 2 (c'est licite, car $b \in \mathrm{W}$, d'après les formules que l'on vient d'écrire) ; l'espace homogène $\mathrm{G/U} = \mathrm{G}_{\mathbf{C}}/\mathrm{L}_{b'}$ sera dit *strictement associé* à la représentation irréductible de poids dominant b ; tout espace $\mathrm{G/U} = \mathrm{G}_{\mathbf{C}}/\mathrm{L}_b$, où $\mathrm{L}_{b'} \subset \mathrm{L}_b$ sera dit *associé* à cette représentation. On observera que, si b' est un élément quelconque de W, il existe toujours un poids dominant b tel que $\mathrm{L}_b = \mathrm{L}_{b'}$; il suffit de prendre b orthogonal aux mêmes a_i que b', ce qui est évidemment possible. Donc *tout espace* G/U *du type étudié plus haut est strictement associé à une représentation irréductible de* $\mathrm{G}_{\mathbf{C}}$.

Soit alors $x \mapsto \mathfrak{a}_x$ une telle représentation de $\mathfrak{g}_{\mathbf{C}}$ dans un espace vectoriel E, et prolongeons-la en une représentation analytique $x \mapsto \mathrm{A}_x$ de $\mathrm{G}_{\mathbf{C}}$. Si e est un élément $\neq 0$ de E correspondant au poids dominant b, e est un vecteur propre de L_b ; inversement, si $x \in \mathrm{G}_{\mathbf{C}}$ est tel que A_x admette e pour vecteur propre, on a $x \in \mathrm{L}_b$ (on vérifie d'abord, par la théorie infinitésimale, que, si e est vecteur propre de $\mathfrak{a}_x$, on a $x \in \mathfrak{l}_b$; il en résulte évidemment que, si e est vecteur propre de A_x, x est contenu dans le normalisateur de L_b ; tout revient donc à prouver que L_b est son propre normalisateur dans $\mathrm{G}_{\mathbf{C}}$, ce que Borel et Weil démontrent par un raisonnement direct, utilisant un résultat de Gantmacher ; mais cela résulte aussi du théorème 1 et des résultats établis ci-dessous).

Soit P l'espace projectif complexe quotient de $\mathrm{E} - \{0\}$ par la relation d'équivalence définie par les homothéties, et soit π la projection canonique de $\mathrm{E} - \{0\}$ sur P. A tout $x \in \mathrm{G}_{\mathbf{C}}$ nous ferons correspondre l'élément $\pi(\mathrm{A}_x \cdot e) \in \mathrm{P}$; on obtient ainsi une application analytique $\varphi_b : \mathrm{G}_{\mathbf{C}} \to \mathrm{P}$, constante sur les classes mod L_b, donc qui définit $\widetilde{\varphi}_b : \mathrm{G}_{\mathbf{C}}/\mathrm{L}_b \to \mathrm{P}$; d'après ce qui précède, $\widetilde{\varphi}_b$ est injectif. On vérifie par un raisonnement infinitésimal que $\widetilde{\varphi}_b$ est une immersion (il suffit de le voir à l'élément neutre de $\mathrm{G}_{\mathbf{C}}$), donc :

Théorème 3. — *Toute représentation irréductible de* $\mathrm{G}_{\mathbf{C}}$*, de poids dominant* b*, définit un plongement* $\widetilde{\varphi}_b$ *de* $\mathrm{G}_b/\mathrm{L}_b = \mathrm{G/U}$ *comme sous-variété analytique sans singularité* (donc algébrique, d'après Chow) *de l'espace projectif complexe associé à l'espace de la représentation.*

En particulier, les variétés G/U *sont des variétés algébriques projectives.*

Si G/U est simplement associé à la représentation A_x, on obtient par composition : $G/U \longrightarrow G_{\mathbf{C}}/L_b \xrightarrow{\widetilde{\varphi}_b} P$ une application analytique de G/U dans P, d'où un *système linéaire* de diviseurs sur G/U : l'image réciproque des sections hyperplanes de $\widetilde{\varphi}_b(G_{\mathbf{C}}/L_b)$. Nous verrons au n° 4 que ce système est complet ; notons dès maintenant qu'en tout cas l'image de G/U dans P n'est contenue dans aucun sous-espace projectif de P, vu l'irréductibilité de A_x.

Les diviseurs du système linéaire précédent définissent une classe de cohomologie $h \in H^2(G/U, \mathbf{Z})$; d'autre part, le poids b peut être identifié à un élément de $H^1(U, \mathbf{Z})$, donc de $H^2(G/U, \mathbf{Z})$, par transgression. On peut montrer que les éléments h et b *coïncident* (au signe près, dépendant des conventions d'orientation choisies).

4. Représentation irréductible associée à une classe de diviseurs sur G/U

Soit $G/U = G_{\mathbf{C}}/L$ un espace homogène du type étudié ci-dessus. Considérons une classe d de diviseurs sur G/U contenant au moins un diviseur $D > 0$ (rappelons que deux diviseurs sont dans la même classe, ou sont linéairement équivalents, si leur différence est égale au diviseur d'une fonction méromorphe). Soit $|D|$ l'ensemble des diviseurs $\geqslant 0$ équivalents à D, et L(D) l'ensemble des fonctions méromorphes f telles que $(f) \geqslant -D$; l'application $f \mapsto (f) + D$ définit une bijection de l'espace projectif P^* associé à L(D) sur l'ensemble $|D|$ (qui se trouve ainsi muni d'une structure projective, d'ailleurs indépendante du diviseur D choisi dans d). Si $x \in G_{\mathbf{C}}$, $x \cdot D$ est un diviseur de G/U, évidemment $\geqslant 0$, et qui est *linéairement équivalent* à D (en effet, G/U est kählérien, puisque algébrique, et de plus simplement connexe, puisque U a même rang que G ; donc le groupe des classes de diviseurs de G/U est isomorphe à un sous-groupe de $H^2(G/U, \mathbf{Z})$ sur lequel $G_{\mathbf{C}}$ ne peut qu'opérer trivialement, puisque $G_{\mathbf{C}}$ est connexe). On a donc $x \cdot D \in |D|$.

Soit $F_0, \ldots, F_r$ une base de L(D). Si l'on fait correspondre à tout $x \in G/U$ le point d'un espace projectif P de coordonnées homogènes $F_0(x), \ldots, F_r(x)$, on obtient une application σ, a priori « méromorphe », de G/U dans P ; en fait cette application est partout holomorphe : cela résulte de ce que la série linéaire complète $|D|$ n'a pas de « points de base » (autrement dit, pour tout $x \in G/U$, il existe $D' \in |D|$ tel que $x \notin D'$ à cause de l'invariance de $|D|$ par translation). L'espace projectif P peut être considéré comme « *dual* » de l'espace P^* associé à L(D) ; les éléments de $|D|$ sont les images réciproques des sections hyperplanes de $\sigma(G/U)$ dans P. De par sa construction même, $\sigma(G/U)$ n'est contenu dans aucune sous-variété projective de P.

Nous allons maintenant montrer que l'on peut associer à tout $x \in \mathrm{G}_{\mathbf{C}}$ un automorphisme $\tilde{x}$ de P tel que :

$$(*) \qquad \sigma(x \cdot y) = \tilde{x} \cdot \sigma(y) \text{ pour tout } y \in \mathrm{G/U}.$$

Puisque $x^{-1} \cdot \mathrm{D} \in |\mathrm{D}|$, et que l'on a évidemment $\mathrm{F}_i(x \cdot y) \geqslant -x^{-1} \cdot \mathrm{D}$ ($\mathrm{F}_i(x \cdot y)$ étant considérée comme fonction de $y \in \mathrm{G/U}$), il existe une fonction g_x, définie à une homothétie près, telle que :

$$\mathrm{F}_i(x \cdot y) \cdot g_x(y) = \sum_{j=0}^{r} \mathrm{A}_{ij}(x) \cdot \mathrm{F}_j(y),$$

où $\mathrm{A}_{ij}(x)$ est une matrice inversible attachée à x, et qui définit donc un automorphisme $\tilde{x}$ de P vérifiant évidemment la condition $(*)$ écrite plus haut. En outre, la condition $(*)$ détermine uniquement $\tilde{x}$, puisque $\sigma(\mathrm{G/U})$ n'est contenu dans aucune sous-variété projective de P ; la même raison montre que $\tilde{x}$ dépend analytiquement de x, donc définit une représentation projective de $\mathrm{G}_{\mathbf{C}}$. Soit alors E l'espace vectoriel dual de L(D), espace dont le projectif associé n'est autre que P ; du fait que $\mathrm{G}_{\mathbf{C}}$ est simplement connexe, on peut trouver une représentation linéaire $x \mapsto \mathrm{A}_x$ de $\mathrm{G}_{\mathbf{C}}$ dans GL(E) qui donne $x \mapsto \tilde{x}$ par passage au quotient. Montrons maintenant que E est *irréductible*, et associée à un poids dominant b tel que $\mathrm{L}_b \supset \mathrm{L}$. Soit y_0 l'image dans G/U de l'élément neutre de G, et soit $e \in \mathrm{E}$ un élément $\neq 0$ dont l'image dans P soit égale à $\sigma(y_0)$. La formule $(*)$ montre alors que e est un vecteur propre de L (dans la représentation $x \mapsto \mathrm{A}_x$), donc de $\mathrm{H} \subset \mathrm{L}$, donc correspond à un poids dominant b tel que $\mathrm{L}_b \supset \mathrm{L}$. Les transformés de e par les opérations A_x, $x \in \mathrm{G}_{\mathbf{C}}$, engendrent dans E un sous-espace vectoriel E' dont l'image dans P contient $\sigma(\mathrm{G/U})$ d'après la formule $(*)$, donc est égale à P, ce qui montre que $\mathrm{E}' = \mathrm{E}$, et que E est irréductible d'après ce qui a été rappelé au n° 3. Nous avons ainsi complètement reconstitué la situation du n° 3. Résumons les résultats obtenus :

THÉORÈME 4. — *Un élément de* $\mathrm{H}^2(\mathrm{G/U}, \mathbf{Z})$ *est dual d'un diviseur* $\mathrm{D} \geqslant 0$ *si et seulement si c'est le poids dominant d'une représentation de* $\mathrm{G}_{\mathbf{C}}$ *associée à* G/U. *Le système linéaire complet* $|\mathrm{D}|$ *est alors dual de l'espace de la représentation*; *il est ample si et seulement si la représentation est strictement associée à* G/U.

6 (Rappelons qu'un système linéaire de diviseurs est dit *ample* s'il n'a pas de composante fixe, et si l'application de la variété dans un espace projectif qu'il définit est un plongement.)

Par exemple, si U = T, tous les poids dominants $b = \sum k_i \cdot b_i$ (les b_i étant les poids fondamentaux) correspondent à des diviseurs > 0 de G/T ; pour que

le système linéaire complet contenant ce diviseur soit ample, il faut et il suffit que tous les k_i soient > 0.

Une conséquence intéressante de ce qui précède est que la dimension de la représentation irréductible de poids dominant b est égale à la dimension de L(D), D associé à b comme plus haut, dimension qui peut être calculée grâce au théorème de Riemann-Roch au moyen de la classe de cohomologie de D, c'est-à-dire justement de b. On retrouve ainsi la formule classique de H. WEYL.

5. Compléments

D'après GOTO, les variétés G/U sont des variétés *rationnelles*. Il est même probable (et peut-être démontré) qu'elles admettent des décompositions « cellulaires » complexes, analogues à celles des grassmanniennes complexes ; autrement dit, il existerait une famille de sous-variétés de G/U emboîtées, telles que la différence entre deux sous-variétés consécutives soit algébriquement isomorphe à un espace affine. C'est en tout cas ce que l'on vérifie pour les groupes classiques, et ce que WEIL a pu démontrer pour $G = E_6$, et U convenable.

Il en résulterait notamment que les espaces G/U (et en particulier G/T) n'ont pas de torsion, conformément à une conjecture émise par BOREL dans sa thèse (et qu'il avait pu vérifier pour les groupes classiques, pour G_2 et pour F_4, au moyen des fibrations de ces groupes).

Bibliographie

[1] A. LICHNEROWICZ, *Sur les espaces homogènes kählériens*, C.R.A.S. **237** (1953), 695–697.

[2] *Colloque de géométrie différentielle, Strasbourg 1953*, Colloques internationaux du C.N.R.S., n° **52** (1953), Paris.

Additif (Avril 1957)

Les questions mentionnées ci-dessus ont été résolues par BOREL, BOTT, CHEVALLEY, GOTO, TITS. On en trouvera une bibliographie dans :

A. BOREL, *Topology of Lie groups and characteristic classes*, Bull. A.M.S. **61** (1955), 397–432.

J. TITS, *Sur certaines classes d'espaces homogènes de groupes de Lie*, Mém. Acad. roy. Belg. **29** (1955), 1–268.

Séminaire Cartan
1954-55, exposé n° 1

10 novembre 1954

LES ESPACES $K(\Pi, n)$

Dans cet exposé, nous allons indiquer les principales propriétés des espaces $K(\Pi, n)$, introduits par EILENBERG-MAC LANE [4]; nous nous placerons à un point de vue purement « topologique » (cf. [20], [15], [17]). Le point de vue « algébrique » (cf. [4], [5], [1]) fera l'objet des exposés suivants.

1. Rappels

Soit $f : X \to Y$ une application continue d'un espace X dans un espace Y. Le « mapping-cylinder » X_f de f est défini ainsi : si Z désigne l'espace somme de Y et de $X \times I$ ($I = [0, 1]$), X_f est l'espace obtenu à partir de Z en identifiant $(x, 1)$ avec $f(x)$ pour tout $x \in X$.

L'espace X_f contient X et Y, et Y est un rétracte de déformation de X_f; de plus l'application composée $X \to X_f \to Y$ est égale à f. Si l'on convient d'identifier X_f et Y (ce qui est naturel, vu qu'ils ont même type d'homotopie), on voit que *f se trouve ainsi identifiée à l'injection de* X *dans* X_f.

A titre d'application, supposons que les homomorphismes

$$f_0 : \pi_i(X) \longrightarrow \pi_i(Y)$$

définis par f soient bijectifs pour tout i; on en conclut que $\pi_i(X_f, X) = 0$ pour tout i, d'où, par un raisonnement élémentaire de déformation, $H_i(X_f, X) = 0$ pour tout i, ce qui montre que

$$f_* : H_i(X) \longrightarrow H_i(Y)$$

est bijectif pour tout i.

De façon analogue, *toute application continue peut être remplacée par une fibration.* D'après ce qui précède, on peut se borner à le montrer pour une injection $X \to Y$. Soit alors X' l'espace des chemins de Y dont l'origine appartient à X; l'espace X est un rétracte de déformation de X'; l'application π qui fait correspondre à tout chemin de Y son extrémité fait de X' un espace fibré de base Y (au sens de [15]), et l'application composée $X \to X' \xrightarrow{\pi} Y$ n'est autre

que l'injection de X dans Y. Si, comme précédemment, on identifie X à X′, on voit que l'injection de X vers Y est remplacée par la projection $\pi : X' \to Y$.

Ces deux procédés sont souvent utilisés dans les questions relatives aux groupes d'homotopie. Cf. notamment [9], [10], [16].

2. Les espaces $K(\Pi, n)$ — définition et construction

Soit n un entier $\geqslant 1$, et soit Π un groupe, supposé abélien si $n \geqslant 2$. Un espace X est appelé un *espace* $K(\Pi, n)$ si l'on a :

$$\begin{cases} \pi_i(X) = 0 & \text{pour } i \neq n \\ \pi_n(X) = \Pi. \end{cases}$$

En particulier, $\pi_0(X) = 0$, ce qui signifie que X est connexe par arcs.

Exemple. — Le cercle $\mathbf{S}_1$ est un espace $K(\mathbf{Z}, 1)$; le tore $\mathbf{T}^d$ est un espace $K(\mathbf{Z}^d, 1)$; plus généralement, si X est un espace $K(\Pi, n)$, et X′ est un espace $K(\Pi', n)$, il est clair que $X \times X'$ est un espace $K(\Pi \times \Pi', n)$.

L'espace projectif réel de dimension infinie, $\mathbf{P}_\infty(\mathbf{R})$, est un espace $K(\mathbf{Z}/2\mathbf{Z}, 1)$; de même un espace lenticulaire de dimension infinie est un espace $K(\mathbf{Z}/p\mathbf{Z}, 1)$.

L'espace projectif complexe de dimension infinie, $\mathbf{P}_\infty(\mathbf{C})$, est un espace $K(\mathbf{Z}, 2)$.

Construction d'espaces $K(\Pi, n)$. Donnons-nous n et Π (abélien, si $n \geqslant 2$). Le procédé décrit dans [22] permet de construire un *complexe cellulaire* qui soit un espace $K(\Pi, n)$; on définit par récurrence le q-squelette K_q de ce complexe, de la façon suivante :

pour $q < n$, K_q est réduit à un point x_0.

K_n s'obtient en attachant à x_0 des cellules de dimension n, correspondant chacune à un générateur du groupe Π.

K_{n+1} s'obtient en attachant à K_n des cellules de dimension $n+1$,de telle sorte que leurs bords fournissent les relations nécessaires entre les générateurs précédents.

...

$K_{q+1}, q > n$, s'obtient en attachant à K_q des cellules de dimension $q+1$,de telle sorte que leurs bords engendrent le groupe $\pi_q(K_q)$.

On constate alors que $\pi_i(K_q) = 0$ pour $i < q$, et $i \neq n$, tandis que, si $q > n+1$, on a $\pi_n(K_q) = \Pi$. Le complexe K, réunion des K_q, est donc bien un espace $K(\Pi, n)$.

De plus, si Π est un *groupe abélien de type fini,* on peut faire en sorte que les K_q soient des complexes *finis* (cf. [18], 36–37) : on raisonne par récurrence sur q ; si K_q est un complexe fini, $\pi_q(K_q)$ est un groupe de type fini, ([15], 491, ou [16], 271–274), donc K_{q+1} peut être obtenu en attachant à K_q un nombre fini de cellules.

3. Espaces $K(\Pi, n)$ et classes de cohomologie

A partir de maintenant, nous nous bornerons au cas où Π est un groupe abélien (ce n'est une restriction que si $n = 1$). Si Y est un espace $K(\Pi, n)$, on a alors $H_n(Y) = \Pi$ et $H_{n-1}(Y) = 0$, ce qui montre que $H^n(Y, G) = \mathrm{Hom}(\Pi, G)$; en particulier, le groupe $H^n(Y, \Pi)$ contient une *classe fondamentale* ι, correspondant à l'application identique de Π sur Π.

Soit $f : X \to Y$ une application continue d'un espace X dans l'espace Y ; l'élément $f^*(\iota)$ est un élément bien déterminé de $H^n(X, \Pi)$, qui ne dépend que de la classe d'homotopie de f.

THÉORÈME. — *Si* X *est un complexe cellulaire, l'application* $f \mapsto f^*(\iota)$ *met en correspondance bijective les classes d'homotopie d'applications* (continues) *de* X *dans* Y *et les éléments de* $H^n(X, \Pi)$.

(Cf. [5], Note IV, [6], III, ainsi que [17].)

Le théorème précédent est une simple conséquence de la théorie des obstructions de S. EILENBERG : par exemple, pour montrer qu'il existe une application $f : X \to Y$ telle que $f^*(\iota)$ soit une classe de cohomologie donnée $x \in H^n(X, \Pi)$, on commence par définir f sur le $n+1$-squelette de X (ce qui est toujours possible, comme on sait), puis on prolonge f sur les squelettes successifs en utilisant le fait que les $\pi_i(Y)$ sont nuls pour $i > n$. On procède de la même façon pour construire une homotopie entre deux applications f et g telles que $f^*(\iota) = g^*(\iota)$.

On peut appliquer le théorème précédent au cas où X est lui-même un espace $K(\Pi, n)$; on en conclut qu'il existe une application $f : X \to Y$ telle que $f_0 : \pi_n(X) \to \pi_n(Y)$ soit l'application identique de Π sur Π. D'après ce qui a été rappelé au n° 1, f induit donc un isomorphisme des groupes d'homologie de X sur ceux de l'espace Y. Donc, *les groupes d'homologie d'un espace* $K(\Pi, n)$ *ne dépendent que de* Π *et de* n (cf. [4]) ; on les note $H_q(\Pi, n; G)$, ce sont les *groupes d'Eilenberg-Mac Lane.* Pour $n = 1$, ils se réduisent aux groupes d'homologie du groupe Π, au sens de HOPF et de EILENBERG-MAC LANE. Le calcul des $H_q(\Pi, n; G)$, pour n quelconque, fera l'objet des exposés suivants.

4. Les espaces $K(\Pi, n)$, comme foncteurs de Π

Soit X un complexe cellulaire qui soit un espace $K(\Pi, n)$, et soit Y un espace $K(\Pi', n)$. On a que $H^n(X, \Pi') = \mathrm{Hom}(\Pi, \Pi')$, et le théorème du numéro précédent montre donc que *les classes d'applications de* X *dans* Y *correspondent bijectivement aux homomorphismes de* Π *dans* Π'. En appliquant le procédé du n° 1 on peut en déduire diverses fibrations (cf. [17], n° 6.)

Appliquons ce qui précède à l'homomorphisme $\Pi \times \Pi \to \Pi$ qui fait correspondre à tout couple (α, β) l'élément $\alpha + \beta$: si X est un complexe cellulaire qui est un espace $K(\Pi, n)$, l'espace $X \times X$ est un espace $K(\Pi \times \Pi, n)$, et c'est aussi un complexe cellulaire (du moins si X à un nombre fini de cellules en toute dimension) ; il existe donc une application $\varepsilon : X \times X \to X$ telle que $\varepsilon_0 : \pi_n(X \times X) \to \pi_n(X)$ soit l'homomorphisme ci-dessus. D'où une structure d'*algèbre* sur $H_*(X) = \oplus H_q(X)$. Si l'on note $(x, y) \mapsto x \cdot y$ l'application qui vient d'être définie (et qui est unique à homotopie près), on voit que cette application est homotope à l'application $(x, y) \mapsto y \cdot x$ (car les deux application ont le même effet sur π_n) ; le même raisonnement montre que $(x, y) \cdot z$ et $x \cdot (y, z)$ sont des applications homotopes de $X \times X \times X$ dans X. Donc $H_*(\Pi, n)$ est une algèbre *associative* et *anticommutative*. On démontre de même l'existence dans X d'un « inverse à homotopie près ».

5. Relations entre $K(\Pi, n-1)$ et $K(\Pi, n)$

Soit X un espace $K(\Pi, n)$, et notons $\Omega(X)$ l'espace des lacets sur X (ayant leur origine et leur extrémité en un point fixé de X). Puisque $\pi_i(\Omega(X)) = \pi_{i+1}(X)$, l'espace $\Omega(X)$ est un espace $K(\Pi, n-1)$. En considérant l'espace fibré E des chemins sur X d'origine fixée, on voit (cf. [15], chap. VI) qu'*il existe un espace fibré contractile dont la base est un* $K(\Pi, n)$ *et la fibre un* $K(\Pi, n-1)$.

Une telle fibration fournit des relations très précises entre les espaces $K(\Pi, n)$ et $K(\Pi, n-1)$; d'où la possibilité d'une étude des $K(\Pi, n)$ par récurrence sur n (le cas $n = 1$ étant bien connu) ; c'est ainsi que, par des calculs de suites spectrales, on peut déterminer les algèbres de cohomologie $H^*(\Pi, n; \mathbf{R})$ et $H^*(\Pi, n; \mathbf{F}_2)$, cf. [15], [17]. Lorsqu'on se place au point de vue algébrique, cette fibration est remplacée par la notion de « construction » de H. Cartan [1].

Le produit de deux lacets définit une multiplication dans $\Omega(X)$, qui est un espace $K(\Pi, n-1)$; d'où une structure d'algèbre sur $H_*(\Pi, n-1)$. Cette structure *coïncide* avec celle définie au n° précédent, comme on le voit en écrivant un diagramme (voir aussi [7]). L'espace fibré E joue, pour le « groupe »

$K(\Pi, n-1)$, le rôle d'un espace fibré principal universel, dont l'espace classifiant est $K(\Pi, n)$.

6. Espaces $K(\Pi, n)$ et opérations cohomologiques

Le théorème du n° 3 joue un rôle essentiel dans l'étude des opérations cohomologiques (cf. [6], III, ainsi que [17], § 4). Par exemple, supposons que l'on veuille prouver la formule suivante, due à ADEM :

$$Sq^2Sq^2(x) = Sq^3Sq^1(x) \qquad \textit{pour tout } x \in H^n(X, \mathbf{F}_2).$$

On peut supposer que X est un complexe cellulaire. Dans ce cas, d'après le n° 3, on a $x = f^*(\iota)$, f étant une application continue convenable de X dans un espace $K(\mathbf{F}_2, n)$, et tout revient à démontrer que $Sq^2Sq^2(\iota) = Sq^3Sq^1(\iota)$ dans $H^{n+4}(\mathbf{F}_2, n; \mathbf{F}_2)$. On peut même éviter de vérifier cette dernière formule : supposons seulement démontré que $H^{n+4}(\mathbf{F}_2, n; \mathbf{F}_2)$ est un espace vectoriel de dimension 2 sur le corps $\mathbf{F}_2$ (n étant $\geqslant 4$) ; alors les trois éléments $Sq^4(\iota), Sq^3Sq^1(\iota), Sq^2Sq^2(\iota)$ sont liés par au moins une relation linéaire ; mais il est facile de construire une autre classe de cohomologie x particulière (dans un produit d'espaces projectifs réels, par exemple) telle que $Sq^2Sq^2(x) = Sq^3Sq^1(x)$ et que $Sq^4(x)$ et $Sq^3Sq^1(x)$ soient linéairement indépendantes sur $\mathbf{F}_2$; il en résulte que la seule relation linéaire possible entre $Sq^4(\iota), Sq^3Sq^1(\iota)$ et $Sq^2Sq^2(\iota)$ est la relation $Sq^3Sq^1(\iota) = Sq^2Sq^2(\iota)$, c.q.f.d.

La même méthode permet de retrouver les résultats d'ADEM relatifs aux puissances réduites de Steenrod (cf. [2]) ; le seul résultat que l'on utilise est la dimension de $H^q(\mathbf{F}_p, n; \mathbf{F}_p)$ sur le corps $\mathbf{F}_p$.

7. Espaces $K(\Pi, n)$ et type d'homotopie

Soit $\pi_1, \ldots, \pi_n, \ldots$ une suite de groupes, et essayons de construire un espace X dont le i-ième groupe d'homotopie soit π_i. Soit d'abord X_1 un espace $K(\pi_1, 1)$. Nous allons déterminer un espace X_2, fibré de base X_1, et de fibre un espace $K(\pi_2, 2)$; il est clair qu'un tel espace a pour groupes d'homotopie $\pi_1, \pi_2, 0, \ldots$. Soit E un espace fibré contractile de base $K(\pi_2, 3)$ et de fibre $K(\pi_2, 2)$; si f est une application continue de X_1 dans $K(\pi_2, 3)$, l'espace fibré image réciproque de E par f est un espace fibré de base X_1 et de fibre $K(\pi_2, 2)$. Si X_1 est un complexe cellulaire, on sait que la classe d'homotopie de f correspond biunivoquement à une classe de cohomologie $k^3 \in H^3(\pi_1, 1; \pi_2)$. On voit donc que, à tout élément $k^3 \in H^3(\pi_1, 1; \pi_2)$, est associé un espace X_2 que nous appellerons un espace $K(\pi_1, 1, \pi_2, 2, k^3)$. De la même façon, toute classe de cohomologie $k^4 \in H^4(X_2; \pi_3)$ définit un espace

fibré $X_3 = K(\pi_1, 1, \pi_2, 2, k^3, \pi_3, 3, k^4)$ de base X_2 et de fibre $K(\pi_3, 3)$. Et ainsi de suite.

La construction précédente a été introduite, d'un point de vue purement algébrique, par POSTNIKOV ([13], [14]) et ZILBER (non publié) ; voir aussi [8]. Signalons que l'on peut démontrer que tout espace X a même type d'homotopie (au point de vue singulier) que la limite d'une suite $(X_1, \dots, X_n, \dots)$ définie comme ci-dessus ; les groupes d'homotopie $\pi_1, \dots$ et les invariants $k^3, \dots$ constituent un système complet d'invariants du type d'homotopie.

Les espaces $K(\pi_1, 1, \pi_2, 2, k^3, \dots)$ jouent un rôle « universel » pour les opérations cohomologiques non partout définies (par exemple les opérations introduites par MASSEY et ADEM), de même que les espaces $K(\Pi, n)$ jouent un rôle universel pour les opérations cohomologiques partout définies.

8. Autres applications des $K(\Pi, n)$

Les espaces $K(\Pi, n)$ sont en relation étroite avec les problèmes d'obstructions ; cf. [5], Note IV, [5], III, II, [12].

Ils peuvent également être utilisés dans le *calcul des groupes d'homotopie* d'un espace donné X : on construit des espaces (X, i) qui « tuent » les groupes d'homotopie de X jusqu'au i-ième, et qui sont reliés entre eux par des fibrations faisant intervenir des espaces $K(\Pi, n)$ (cf. [3], Note I, et [21]). On trouvera des applications de cette méthode dans [3], Note II, [9], [10], [16], [17], [18].

Pour une construction explicite d'un complexe cellulaire $K(\mathbf{Z}, n)$ (en dimensions assez basses), cf. [19].

Bibliographie

[1] H. CARTAN, *Sur les groupes d'Eilenberg-Mac Lane* $H(\Pi, n)$ I, Proc. Nat. Acad. Sci. USA **40** (1954), 467–471; II, *ibid.* 704–707.

[2] H. CARTAN, *Sur l'itération des opérations de Steenrod.* Comm. Math. Helv. **29** (1955), 40–58.

[3] H. CARTAN et J-P. SERRE, *Espaces fibrés et groupes d'homotopie.* I, C.R.A.S **234** (1952), 288–290; II, *ibid.* 393–395.

[4] S. EILENBERG and S. MAC LANE, *Relations between homology and homotopy groups of spaces.* I, Ann. of Math. **46** (1945), 480–509; II, *ibid.* **51** (1950), 514–533.

[5] S. EILENBERG and S. MAC LANE, *Cohomology theory of abelian groups and homotopy theory* I, Proc. Nat. Acad. Sci. USA **36** (1950), 443–447; II, *ibid.* 657–663; III, *ibid.* **37** (1951), 307–310; IV, *ibid.* **38** (1952), 1340–1342.

[6] S. Eilenberg and S. Mac Lane, *On the groups* H(Π, n) I, Ann. of Math. **58** (1953), 55–106; II, *ibid.* **60** (1954), 49–139; III, *ibid.* **60** (1954), 513–557.

[7] S. Mac Lane, *The homology products in* K(Π, n), Proc. A.M.S. **5** (1954), 642–651.

[8] K. Mizuno, *On the minimal complexes,* J. Inst. Polyt. Osaka City Univ. **5** (1954), 41–51.

[9] J.C. Moore, *Some applications of homology theory to homotopy problems,* Ann. of Math. **58** (1953), 325–350.

[10] J.C. Moore, *On homotopy groups of spaces with a single non-vanishing homology group,* Ann. of Math. **59** (1954), 549–557.

[11] M. Nakaoka, *Classification of mappings of a complex into a special kind of complex,* J. Inst. Polyt. Osaka City Univ. **3** (1952), 101–143.

[12] M. Nakaoka, *On homotopy classification and extension,* Proc. Japan Acad. **29** (1953), 6–9.

[13] M.M. Postnikov, *Determination of the homology groups of a space by means of the homotopy invariants* (en russe), Doklady Akad. Nauk SSSR **76** (1951), 359–362.

[14] M.M. Postnikov, *On the homotopy type of polyedra* (en russe). Doklady Akad. Nauk SSSR **76** (1951), 789–791.

[15] J-P. Serre, *Homologie singulière des espaces fibrés. Applications,* Ann. of Math. **54** (1951), 425–505.

[16] J-P. Serre, *Groupes d'homotopie et classes de groupes abéliens,* Ann. of Math. **58** (1953), 258–294.

[17] J-P. Serre, *Cohomologie modulo 2 des complexes d'Eilenberg-Mac Lane,* Comm. Math. Helv. **27** (1953), 198–232.

[18] R. Thom, *Quelques propriétés globales des variétés différentiables,* Comm. Math. Helv. **28** (1954), 17–86.

[19] H. Toda, *Generalized Whitehead products and homotopy groups of spheres,* J. Inst. Polyt. Osaka City Univ. **3** (1952), 43–82.

[20] G.W. Whitehead, *On spaces with vanishing low-dimensional homotopy groups,* Proc. Nat. Acad. Sci. USA **34** (1948), 207–211.

[21] G.W. Whitehead, *Fibre spaces and the Eilenberg homology groups,* Proc. Nat. Acad. Sci. USA **38** (1952), 426–430.

[22] J.H.C. Whitehead, *On the realizability of homotopy groups,* Ann. of Math. **50** (1949), 261–263.

Séminaire Cartan
1954-55, exposé n° 20

2 et 9 mai 1955

GROUPES D'HOMOTOPIE DES BOUQUETS DE SPHÈRES

§ 1. Opérations homotopiques

Soient n et p deux entiers. Pour tout espace X, donnons-nous une application

$$f : \pi_n(\mathrm{X}) \longrightarrow \pi_p(\mathrm{X}),$$

commutant avec les applications continues $\mathrm{X} \to \mathrm{Y}$. La collection des applications f est appelée une *opération homotopique à une variable* (cf. [1]) ; c'est une notion analogue à celle d'opération cohomologique étudiée dans les exposés 14 à 16.

Il est facile de déterminer toutes les opérations homotopiques à une variable. En effet, soit $i_n \in \pi_n(\mathbf{S}_n)$ la classe d'homotopie de l'application identique $\mathbf{S}_n \to \mathbf{S}_n$; si f est une opération homotopique, $f(i_n) = \alpha$ est un élément bien déterminé de $\pi_p(\mathbf{S}_n)$, et si β est un élément quelconque de $\pi_n(\mathrm{X})$, on a :

$$f(\beta) = f \circ \beta(i_n) = \beta \circ f(i_n) = \beta \circ \alpha.$$

Inversement, si α est un élément de $\pi_p(\mathbf{S}_n)$, l'application $\beta \mapsto \beta \circ \alpha$ est une opération homotopique à une variable. Ainsi, l'ensemble des opérations homotopiques à une variable est en correspondance naturelle avec l'ensemble des éléments du groupe $\pi_p(\mathbf{S}_n)$; la sphère $\mathbf{S}_n$ joue donc un rôle *universel* pour ces opérations (de même que $\mathrm{K}(\Pi, n)$ joue un rôle universel pour les opérations cohomologiques à une variable).

On définit de la même manière les *opérations homotopiques à plusieurs variables*. Par exemple, une opération à 2 variables est la donnée, pour tout espace X, d'une application f de $\pi_n(\mathrm{X}) \times \pi_m(\mathrm{X})$ dans $\pi_p(\mathrm{X})$, commutant aux applications continues (n, m et p étant des entiers donnés). Ici, l'espace universel est l'espace $\mathbf{S}_n \vee \mathbf{S}_m$ qui est réunion de deux sphères $\mathbf{S}_n$ et $\mathbf{S}_m$ ayant un point commun (« bouquet » de sphères). En effet, la donnée d'un couple d'éléments

$\beta \in \pi_n(\mathrm{X})$, $\gamma \in \pi_m(\mathrm{X})$ équivaut à la donnée d'une classe d'applications

$$\beta \vee \gamma \colon \mathbf{S}_n \vee \mathbf{S}_m \longrightarrow \mathrm{X};$$

d'autre part, les injections canoniques $i_n \colon \mathbf{S}_n \to \mathbf{S}_n \vee \mathbf{S}_m$ et $i_m \colon \mathbf{S}_m \to \mathbf{S}_n \vee \mathbf{S}_m$ peuvent être regardées comme des éléments de $\pi_n(\mathbf{S}_n \vee \mathbf{S}_m)$ et de $\pi_m(\mathbf{S}_n \vee \mathbf{S}_m)$ respectivement ; il s'ensuit que $f(i_n, i_m)$ est un élément bien défini

$$\alpha \in \pi_p(\mathbf{S}_n \vee \mathbf{S}_m),$$

et que, pour tout couple $\beta \in \pi_n(\mathrm{X})$, $\gamma \in \pi_m(\mathrm{X})$, on a :

$$f(\beta, \gamma) = (\beta \vee \gamma) \circ \alpha.$$

Plus généralement, les opérations homotopiques à k variables

$$f : \pi_{n_1}(\mathrm{X}) \times \cdots \times \pi_{n_k}(\mathrm{X}) \longrightarrow \pi_p(\mathrm{X})$$

sont en correspondance bijective avec les éléments de $\pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$. Nous verrons au § 2 comment ce dernier groupe peut être calculé en fonction des groupes d'homotopie de sphères.

Exemple d'opération homotopique : le produit de Whitehead

Considérons $\mathbf{S}_n \vee \mathbf{S}_m$ comme plongé dans le produit direct $\mathbf{S}_n \times \mathbf{S}_m$; nous obtenons ainsi une suite exacte :

$$\cdots \longrightarrow \pi_p(\mathbf{S}_n \vee \mathbf{S}_m) \longrightarrow \pi_p(\mathbf{S}_n \times \mathbf{S}_m) \longrightarrow \pi_p(\mathbf{S}_n \times \mathbf{S}_m, \mathbf{S}_n \vee \mathbf{S}_m) \longrightarrow \cdots$$

En fait, en tenant compte de ce que $\pi_p(\mathbf{S}_n \times \mathbf{S}_m) = \pi_p(\mathbf{S}_n) \oplus \pi_p(\mathbf{S}_m)$, on voit facilement que la suite exacte précédente se décompose, et l'on obtient un isomorphisme :

$$\pi_p(\mathbf{S}_n \vee \mathbf{S}_m) = \pi_p(\mathbf{S}_n) \oplus \pi_p(\mathbf{S}_m) \oplus \pi_{p+1}(\mathbf{S}_n \times \mathbf{S}_m, \mathbf{S}_n \vee \mathbf{S}_m).$$

Les deux premiers facteurs sont plongés par les injections i_n et i_m ; le troisième facteur est plongé par l'opérateur bord

$$d \colon \pi_{p+1}(\mathbf{S}_n \times \mathbf{S}_m, \mathbf{S}_n \vee \mathbf{S}_m) \longrightarrow \pi_p(\mathbf{S}_n \vee \mathbf{S}_m).$$

Mais le théorème d'Hurewicz relatif montre que $\pi_p(\mathbf{S}_n \times \mathbf{S}_m, \mathbf{S}_n \vee \mathbf{S}_m)$ est nul pour $q < n + m$, et que $\pi_{n+m}(\mathbf{S}_n \times \mathbf{S}_m, \mathbf{S}_n \vee \mathbf{S}_m)$ est cyclique infini, engendré par $i_n \times i_m$; en appliquant l'opérateur d à $i_n \times i_m$, on trouve un élément de $\pi_{n+m-1}(\mathbf{S}_n \vee \mathbf{S}_m)$ que nous noterons $[i_n, i_m]$. D'après ce qui a été dit plus haut, l'élément $[i_n, i_m]$ définit une opération homotopique à deux variables, que nous noterons

$$(\beta, \gamma) \longmapsto [\beta, \gamma];$$

c'est le *produit de Whitehead*. Par définition, on a $[\beta, \gamma] \in \pi_{n+m-1}(\mathrm{X})$ si $\beta \in \pi_n(\mathrm{X})$, $\gamma \in \pi_m(\mathrm{X})$. Si β est représenté par $b \colon \mathrm{I}^n \to \mathrm{X}$ tel que $b(\dot{\mathrm{I}}^n) = x_0$, et si

γ est représenté par $c\colon \mathrm{I}^m \to \mathrm{X}$, alors $[\beta, \gamma]$ est représenté par l'application u de $\dot{\mathrm{I}}^{n+m} = \mathbf{S}_{n+m-1}$ dans X définie par la formule :

$$u(x,y) = \begin{cases} b(x) & \text{si } x \in \mathrm{I}^n \text{ et } y \in \dot{\mathrm{I}}^m, \\ c(y) & \text{si } x \in \dot{\mathrm{I}}^n \text{ et } y \in \mathrm{I}^m. \end{cases}$$

Il en résulte aisément que $[\beta, \gamma]$ est *bilinéaire*. De plus, un calcul d'orientations montre que $[\beta, \gamma] = (-1)^{nm}[\gamma, \beta]$, et nous verrons plus loin que $[\beta, \gamma]$ vérifie *l'identité de Jacobi* (modifiée par des signes convenables). Le produit de Whitehead possède donc des propriétés tout à fait analogues à celles du crochet d'une algèbre de Lie.

§ 2. Le théorème de Hilton

Ce théorème (démontré dans [3]) exprime $\pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$, $n_1 \geqslant 2, \ldots,$ $n_k \geqslant 2$, comme une somme directe de groupes d'homotopie de sphères $\pi_p(\mathbf{S}_m)$. Chaque facteur se trouve plongé par un certain produit de Whitehead multiple. Nous allons d'abord décrire ces produits.

Définition des produits basiques

Nous définirons par récurrence sur w les produits basiques de poids w ; les 1
produits basiques de poids 1 sont les éléments $i_1, \ldots, i_k$, classes d'homotopie des injections canoniques

$$\mathbf{S}_{n_1} \longrightarrow \mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k}, \ldots, \quad \mathbf{S}_{n_k} \longrightarrow \mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k};$$

nous les ordonnons par la relation d'ordre $i_1 < i_2 < \cdots < i_k$. Supposons maintenant définis et ordonnés les produits basiques de poids $< w$. Un produit basique de poids w sera alors un produit de Whitehead $[a, b]$, où a (resp. b) est un produit basique de poids u (resp. v), avec $u + v = w$, $a < b$, et si b est lui-même défini comme $[c, d]$, on doit avoir $c \leqslant a$. Les produits de poids w sont ordonnés arbitrairement entre eux, et sont considérés comme strictement supérieurs aux produits basiques de poids $< w$.

Exemple. — Si $k = 2$, et si l'on pose $x = i_1$, $y = i_2$, les produits basiques de poids $\leqslant 4$ sont les suivants :

poids 1 : x, y

poids 2 : $[x, y]$

poids 3 : $[x, [x, y]]$, $[y, [x, y]]$

poids 4 : $[x, [x, [x, y]]]$, $[y, [x, [x, y]]]$, $[y, [y, [x, y]]]$.

Chaque produit basique a peut être considéré comme un élément du groupe $\pi_{n_a}(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$, n_a désignant un entier facile à déterminer. L'application $\beta \mapsto a \circ \beta$ est donc un homomorphisme f_a de $\pi_p(\mathbf{S}_{n_a})$ dans $\pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$; d'où un homomorphisme f de la somme directe $\bigoplus_a \pi_p(\mathbf{S}_{n_a})$ dans le groupe $\pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$. Le résultat de HILTON s'énonce alors :

THÉORÈME. — *Pour tout entier p, l'homomorphisme f est un isomorphisme de $\bigoplus_a \pi_p(\mathbf{S}_{n_a})$ sur $\pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$.*

On observera que les entiers n_a tendent vers $+\infty$; il s'ensuit que, pour chaque entier p, la somme directe $\bigoplus_a \pi_p(\mathbf{S}_{n_a})$ est *finie*. On a par exemple :

$$\pi_p(\mathbf{S}_n \vee \mathbf{S}_n) = \pi_p(\mathbf{S}_n) \oplus \pi_p(\mathbf{S}_n) \oplus \pi_p(\mathbf{S}_{2n-1}) \oplus \pi_p(\mathbf{S}_{3n-2}) \oplus \pi_p(\mathbf{S}_{3n-2}) \text{ si } p < 4n-3.$$

[Des résultats partiels de ce genre avaient d'ailleurs été déjà obtenus par G. WHITEHEAD, J.H.C. WHITEHEAD, BLAKERS-MASSEY, MOORE, CHANG, etc.]

Démonstration du théorème de Hilton

Soit Ω l'espace des lacets sur l'espace $\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k}$; d'après un résultat de BOTT et SAMELSON [2], $\mathrm{H}_*(\Omega)$, munie de la structure d'algèbre définie par le produit de Pontrjagin, est *l'algèbre associative libre* engendrée par les éléments $x_1, \ldots, x_k$ correspondant aux sphères $\mathbf{S}_{n_1}, \ldots, \mathbf{S}_{n_k}$ par transgression. (La démonstration de BOTT et SAMELSON consiste à expliciter la suite spectrale de l'espace des chemins sur $\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k}$; on pourrait également utiliser le théorème de MOORE démontré dans l'exposé 3.) Soit de même Ω_a l'espace des lacets sur $\mathbf{S}_{n_a}$; l'algèbre $\mathrm{H}_*(\Omega_a)$ est une algèbre de polynômes à 1 générateur y_a de dimension $n_a - 1$. Si l'on désigne par T la limite inductive des produits finis des Ω_a, a parcourant l'ensemble des produits basiques, on voit que $\mathrm{H}_*(\mathrm{T})$ admet pour base l'ensemble des éléments de la forme :

$$y_{a_1}^{m_1} \otimes \cdots \otimes y_{a_i}^{m_i}.$$

Chaque produit basique a définit, par passage aux espaces de lacets, une application multiplicative $g_a \colon \Omega_a \to \Omega$; nous désignerons par x_a l'image de y_a par g_a. Puisque g_a est multiplicative, l'image de y_a^m par g_a est égale à x_a^m. Soit alors $g \colon \mathrm{T} \to \Omega$ l'application produit des applications g_a ; par passage à l'homologie, g transforme les $y_{a_1}^{m_1} \otimes \cdots \otimes y_{a_i}^{m_i}$ en les *monômes* $x_{a_1}^{m_1} \cdots x_{a_i}^{m_i}$. Admettons provisoirement que ces monômes forment une *base* de $\mathrm{H}_*(\Omega)$. Alors $g_* \colon \mathrm{H}_*(\mathrm{T}) \to \mathrm{H}_*(\Omega)$ est une bijection ; comme les espaces T et Ω sont des H-espaces, ceci entraîne, en vertu du théorème de Moore, que $\widetilde{g}_* \colon \mathrm{H}_*(\widetilde{\mathrm{T}}) \to \mathrm{H}_*(\widetilde{\Omega})$ est bijectif, $\widetilde{\mathrm{T}}$ et $\widetilde{\Omega}$ désignant les revêtements universels de T et de Ω respectivement (pour une démonstration directe, cf. [3]) ; appliquant alors le

théorème d'Hurewicz relatif au mapping-cylinder de $\widetilde{g}$, on en conclut que $g_0 : \pi_{p-1}(\mathrm{T}) \to \pi_{p-1}(\Omega)$ est bijectif pour tout p. Mais, $\pi_{p-1}(\mathrm{T}) = \bigoplus_a \pi_p(\mathbf{S}_{n_a})$, $\pi_{p-1}(\Omega) = \pi_p(\mathbf{S}_{n_1} \vee \cdots \vee \mathbf{S}_{n_k})$, et ces isomorphismes transforment g_0 en f, comme on le vérifie immédiatement ; donc f est bijectif.

Ainsi, la démonstration sera achevée si nous montrons que les monômes $x_{a_1}^{m_1} \cdots x_{a_i}^{m_i}$ forment une base de $\mathrm{H}_*(\Omega)$.

Calculons d'abord les x_a en fonction des générateurs $x_1, \ldots, x_k$ de $\mathrm{H}_*(\Omega)$. De façon générale, soit X un espace quelconque, soit Ω son espace des lacets, et soit τ l'application composée des homomorphismes canoniques :

$$\pi_{p+1}(\mathrm{X}) \longrightarrow \pi_p(\Omega) \longrightarrow \mathrm{H}_p(\Omega).$$

D'après une formule de SAMELSON [4], on a :

$$\tau[\beta, \gamma] = (-1)^p(\tau\beta \cdot \tau\gamma - (-1)^{pq}\tau\gamma \cdot \tau\beta) \text{ si } \beta \in \pi_{p+1}(\mathrm{X}),\ \gamma \in \pi_{q+1}(\mathrm{X}).$$

Ceci nous fournit la valeur des x_a : si l'on munit $\mathrm{H}_*(\Omega)$ de l'opération

$$[x, y] = (-1)^p(x \cdot y - (-1)^{pq} y \cdot x),$$

x_a n'est autre que le a-ième produit basique des $x_1, \ldots, x_k$.

Nous sommes ainsi ramenés à un problème purement algébrique : montrer que, si l'on forme les produits basiques x_a des générateurs d'une algèbre associative libre A, les monômes en les x_a forment une *base* de A. Dans le cas où le crochet $[x, y]$ est égal à $x \cdot y - y \cdot x$ (ce qui se produit si toutes les sphères considérées sont de dimension impaire), le résultat précédent est un théorème bien connu de WITT ; ceci montre que le nombre des monômes en les x_a de **2**
degré r donné est égal au rang du groupe formé des éléments homogènes de degré r de A. Il suffit donc, dans le cas où les n_i sont quelconques, de montrer que les monômes en question *engendrent* A ; c'est ce que fait HILTON [3], par un raisonnement direct, inspiré de raisonnements analogues de P. HALL et MAGNUS.

§ 3. Applications

Le théorème de Hilton détermine complètement la forme des opérations homotopiques à plusieurs variables ; il montre en particulier que ces opérations sont engendrées par les trois opérations élémentaires suivantes : addition, composition, produit de Whitehead.

Il fournit également une démonstration de l'*identité de Jacobi* :

$$(-1)^{pq}[[\beta, \gamma], \alpha] + (-1)^{qr}[[\gamma, \alpha], \beta] + (-1)^{rp}[[\alpha, \beta], \gamma] = 0$$

si $\alpha \in \pi_p(\mathrm{X})$, $\beta \in \pi_q(\mathrm{X})$, $\gamma \in \pi_r(\mathrm{X})$.

En effet, d'après le § 1, il suffit de démontrer cette identité lorsque α, β, γ sont respectivement égaux aux éléments i_p, i_q, i_r de $\pi_*(\mathbf{S}_p \vee \mathbf{S}_q \vee \mathbf{S}_r)$. Comme $[i_p, [i_q, i_r]]$ n'est pas un produit basique, il peut s'écrire sous la forme :

$$[i_p, [i_q, i_r]] = a[i_q, [i_p, i_r]] + b[i_r, [i_p, i_q]] + \delta,$$

où a et b sont des entiers, et où δ est une somme d'opérations homotopiques ne portant que sur deux des trois éléments i_p, i_q, i_r. La formule précédente étant universelle, on en déduit facilement que $\delta = 0$, et l'on détermine les valeurs de a et de b par un raisonnement homologique.

[D'autres démonstrations de l'identité de Jacobi ont été données par Nakaoka et Toda, Massey et Uehara, G. Whitehead.]

Une autre application importante du théorème de Hilton est la définition des *invariants de Hopf généralisés* (cf. [3]) : soit

$$\Phi\colon \pi_p(\mathbf{S}_n) \longrightarrow \pi_p(\mathbf{S}_n \vee \mathbf{S}_n)$$

l'application obtenue en identifiant en un point l'équateur de $\mathbf{S}_n$. Si l'on compose Φ avec les projections de $\pi_p(\mathbf{S}_n \vee \mathbf{S}_n)$ sur ses différents facteurs $\pi_p(\mathbf{S}_{2n-1})$, $\pi_p(\mathbf{S}_{3n-2}), \ldots$, on obtient des homomorphismes :

$$\begin{aligned} \mathrm{H}_0\colon \pi_p(\mathbf{S}_n) &\longrightarrow \pi_p(\mathbf{S}_{2n-1}) \\ \mathrm{H}_1,\ \mathrm{H}_2\colon \pi_p(\mathbf{S}_n) &\longrightarrow \pi_p(\mathbf{S}_{3n-2}) \\ &\cdots, \end{aligned}$$

et l'on a, pour tout $\alpha \in \pi_p(\mathbf{S}_n)$:

$$\Phi(\alpha) = i_1 \circ \alpha + i_2 \circ \alpha + [i_1, i_2] \circ \mathrm{H}_0\alpha + [i_1, [i_1, i_2]] \circ \mathrm{H}_1\alpha + \cdots$$

Si X est un espace quelconque, et si β et γ sont deux éléments de $\pi_n(\mathrm{X})$, on déduit de la formule précédente que l'on a :

$$(\beta + \gamma) \circ \alpha = \beta \circ \alpha + \gamma \circ \alpha + [\beta, \gamma] \circ \mathrm{H}_0\alpha + [\beta, [\beta, \gamma]] \circ \mathrm{H}_1\alpha + \cdots$$

On voit ainsi quelle est la « déviation de l'additivité » de l'opération $\beta \mapsto \beta \circ \alpha$.

On trouvera dans [3] diverses propriétés des H_i ; le plus intéressant de ces opérateurs est H_0, qui généralise directement l'invariant de Hopf classique. On verra d'ailleurs, dans un exposé ultérieur de Moore (exposé 22), qu'il est en rapport étroit avec la suspension de Freudenthal.

Références

[1] A. L. Blakers et W. S. Massey, *Products in homotopy theory*, Ann. of Math. **58** (1953), 295–324.

[2] R. Bott et H. Samelson, *On the Pontrjagin product in spaces of paths*, Comm. Math. Helv. **27** (1953), 320–337.

[3] P. J. Hilton, *On the homotopy groups of the union of spheres*, J. London Math. Soc. **30** (1955), 154-172.

[4] H. Samelson, *A connection between the Whitehead and the Pontrjagin product*, Amer. J. of Math. **75** (1953), 744–752.

Séminaire Chevalley 21 avril 1958
1958, exposé n° 1

ESPACES FIBRÉS ALGÉBRIQUES

Le texte qui suit, rédigé en septembre 1958, diffère sensiblement de l'exposé oral, ne serait-ce que par sa longueur.

Sommaire

Introduction

La définition des espaces fibrés algébriques donnée par Weil [19] suppose ceux-ci *localement triviaux*. Cette hypothèse a certaines conséquences fâcheuses : un revêtement non ramifié n'est pas un espace fibré; un groupe algébrique n'est pas nécessairement fibré par un sous-groupe. Le but de cet exposé est de proposer une définition plus large, celle des espaces fibrés *localement isotriviaux*, qui échappe à ces inconvénients.

Dans tout ce qui suit, le corps de base k est supposé algébriquement clos, de caractéristique quelconque. Nous suivons la terminologie et les notations de FAC [15], à cela près que nous appelons « espaces algébriques » (resp. « morphismes ») les « variétés algébriques » (resp. « applications régulières ») de FAC ; pour nous conformer à l'usage du séminaire Chevalley, nous réservons le terme de « variété » au cas irréductible.

Il ne serait pas bien difficile d'étendre les résultats de cet exposé au cas d'un corps de base quelconque ; pour une base réduite à un point on retrouverait la situation étudiée dans LANG-TATE [13]. Il serait plus intéressant de se placer
1 dans le cadre de la théorie générale des *schémas* de GROTHENDIECK (cf. [12]) ; pour la théorie des revêtements (§ 1), c'est facile ; par contre, dès que l'on aborde les espaces fibrés proprement dits, on se heurte à des difficultés sérieuses (en voici un exemple typique : si G est un schéma en groupes sur un schéma donné, et si H est un schéma de sous-groupes de G, peut-on définir un schéma
2 quotient G/H ?).

§ 1. Revêtements non ramifiés

1.1. Définition d'un espace entier sur un autre. — Soit $\pi : Y \to X$ un morphisme d'un espace algébrique Y dans un espace algébrique X. Nous dirons que Y est *entier* sur X si la condition suivante est réalisée :

(E) *Il existe un recouvrement ouvert affine* X_i *de* X *tel que les* $Y_i = \pi^{-1}(X_i)$ *soient des ouverts affines de* Y*, et que, si* A_i (resp. B_i) *désigne l'anneau de coordonnées de* X_i (resp. Y_i)*, l'anneau* B_i *soit un* A_i*-module de type fini.*

(On dit aussi que $\pi : Y \to X$ est un morphisme *fini*.)

Si Y est entier sur X, l'image directe $\pi(\mathscr{O}_Y)$ du faisceau des anneaux locaux de Y est un faisceau cohérent de $\mathscr{O}_X$-algèbres : c'est évident localement (avec les notations de (E), le faisceau $\pi(\mathscr{O}_Y)$ est défini, sur la variété affine X_i par le A_i-module B_i). Inversement, tout faisceau cohérent de $\mathscr{O}_X$-algèbres, dépourvu
3 d'éléments nilpotents, correspond à un Y et à un seul. Si $x \in X$, les points de Y au-dessus de x correspondent aux idéaux premiers maximaux de l'anneau semi-local $\pi(\mathscr{O}_Y)_x$, et leurs anneaux locaux ne sont autres que les localisés de cet anneau semi-local.

Si Y est entier sur X et si X est *affine*, il en est de même de Y. En effet, soit A l'anneau de coordonnées affines de X, et soit B l'ensemble des sections de $\pi(\mathscr{O}_Y)$; d'après les propriétés élémentaires des variétés affines, B est un A-module de type fini, donc est une algèbre affine. L'algèbre B correspond donc à une variété affine Y′, entière sur X, et on vérifie facilement que Y′ coïncide avec Y [par exemple à cause du fait que $\pi(\mathscr{O}_Y) = \pi(\mathscr{O}_{Y'})$].

Le résultat précédent montre que si Z est entier sur Y et Y entier sur X, alors Z est entier sur X.

Remarque. — La condition (E) entraîne que π est un morphisme *propre* (au sens de CHEVALLEY [8]) et que $\pi^{-1}(x)$ est *fini* pour tout $x \in X$. Inversement, ces deux conditions entraînent (E) (CHEVALLEY, non publié) ; comme nous

n'aurons pas besoin de ce fait, nous nous bornerons à signaler qu'on peut le démontrer en utilisant le théorème des fonctions holomorphes de Zariski, sous la forme de GROTHENDIECK ([12], th. 4).

1.2. Définition d'un revêtement non ramifié. — Soit $\pi : Y \to X$ un morphisme fini. On dit que π est *non ramifié* en un point $y \in Y$ ayant pour image $x = \pi(y)$ si la condition suivante est satisfaite :

(NR) *L'homomorphisme* $\widehat{\pi} : \widehat{\mathscr{O}_x} \to \widehat{\mathscr{O}_y}$ *défini par* π *est un isomorphisme.*

(De façon générale, on note $\widehat{A}$ le complété d'un anneau local A pour la topologie définie par les puissances de l'idéal maximal.)

La condition (NR) se décompose en deux ; tout d'abord, $\widehat{\pi}$ doit être *injectif* (condition très large, vérifiée par exemple si X et Y sont normales et de même dimension) ; ensuite, $\widehat{\pi}$ doit être *surjectif*, ce qui équivaut à dire que l'idéal maximal $\mathfrak{m}_y$ de $\mathscr{O}_y$ est *engendré* par l'idéal maximal $\mathfrak{m}_x$ de $\mathscr{O}_x$. Lorsque X et Y sont irréductibles, et de même dimension, on retrouve la définition de la non-ramification du séminaire CHEVALLEY [7], page 5-15.

[La condition (NR) n'est « raisonnable » que parce que le corps de base k est supposé algébriquement clos. Dans le cas général, il faudrait supposer que $\widehat{\mathscr{O}_y}$ est un $\widehat{\mathscr{O}_x}$-module libre de type fini et que son *discriminant* est inversible dans $\widehat{\mathscr{O}_x}$. Cette définition peut se mettre sous plusieurs formes équivalentes, mais nous n'insisterons pas là-dessus.] 4

Si x est un point de X, on dit que π est *non ramifié en* x s'il est non ramifié en tous les points de Y se projetant sur x. Si ces points sont en nombre de n, le complété de l'anneau semi-local $\pi(\mathscr{O}_Y)_x$ est isomorphe à $(\widehat{\mathscr{O}_x})^n$; c'est donc un $\widehat{\mathscr{O}_x}$-module libre de rang n, et son radical est engendré par $\mathfrak{m}_x$. En utilisant les propriétés agréables de la complétion d'un anneau local (cf. par exemple [4], exposé 18, ou GAGA [16], Annexe), on voit qu'il en est de même pour $\pi(\mathscr{O}_Y)_x$. En d'autres termes :

(NR)′ *L'anneau semi-local* $\pi(\mathscr{O}_Y)_x$ *est un* $\mathscr{O}_x$*-module libre de type fini, et son radical est engendré par* $\mathfrak{m}_x$.

Inversement, il est immédiat que (NR)′ entraîne que Y est non ramifié en x.

Enfin, on dira que $\pi : Y \to X$ est un *revêtement non ramifié* s'il est fini et non ramifié en tout point (de X ou de Y, c'est la même chose).

Si c'est le cas, le faisceau $\pi(\mathscr{O}_Y)$ est localement libre (la réciproque étant bien entendu inexacte); son rang est donc constant sur toute composante connexe de X ; on l'appelle le *degré* du revêtement (sur la composante connexe en question) ; en vertu de ce qui précède, c'est aussi le nombre de points de Y ayant

pour image un point donné de X. Si ce rang est partout égal à 1, l'application π est un isomorphisme : c'est évident sur la condition (NR)′.

Si $\pi : Y \to X$ est un morphisme fini quelconque, l'ensemble des points de X au-dessus desquels Y est non ramifié forme un *ouvert*. Si X et Y sont irréductibles et de même dimension, cet ouvert est non vide si et seulement si l'extension $k(Y)/k(X)$ est séparable (cf. [7], *loc. cit.*).

1.3. Opérations sur les revêtements non ramifiés. — Toutes les propriétés formelles des revêtements topologiques se laissent transposer. De façon précise :

(a) *Transitivité des revêtements.* — Si $Z \to Y$ et $Y \to X$ sont des revêtements non ramifiés, le composé $Z \to X$ est un revêtement non ramifié.

C'est évident, puisque l'on sait déjà que Z est entier sur X (n° 1.1).

(b) *Produit de deux revêtements.* — Si $Y \to X$ et $Y' \to X'$ sont des revêtements non ramifiés, le produit $Y \times Y' \to X \times X'$ est un revêtement non ramifié.

C'est évident.

(c) *Revêtement induit sur un sous-espace.* — Soit $Y \to X$ un revêtement non ramifié, soit $X' \subset X$, et soit Y' son image réciproque. Alors $Y' \to X'$ est un revêtement non ramifié ; de plus, pour tout point $y \in Y'$ se projetant en $x \in X'$, l'idéal de Y' dans $\mathscr{O}_y$ est engendré par l'idéal de X' dans $\mathscr{O}_x$.

Soit $\mathfrak{a}$ l'idéal de X' dans $\mathscr{O}_x$; posons $A_x = \pi(\mathscr{O}_Y)_x$, anneau semi-local de $\pi^{-1}(x)$ dans l'espace algébrique Y. D'après (NR)′ l'anneau A_x est un $\mathscr{O}_x$-module libre, et son radical est engendré par $\mathfrak{m}_x$; il en est donc de même de l'anneau quotient $A_x/\mathfrak{a}A_x$, considéré comme $\mathscr{O}_x/\mathfrak{a}$-module. En particulier, le complété de cet anneau est isomorphe à $(\widehat{\mathscr{O}_x}/\widehat{\mathfrak{a}})^n$, en notant n le degré en x du revêtement. D'après un théorème de Chevalley [6] (voir aussi [4], exposé 19), cet anneau complété n'a pas d'éléments nilpotents, et il en est *a fortiori* de même de $A_x/\mathfrak{a}A_x$. Ceci montre que $\mathfrak{a}A_x$ n'est autre que l'idéal défini par Y' dans A_x, d'où le résultat cherché.

[On pourrait éviter d'employer le théorème de Chevalley (qui est spécial aux anneaux locaux de la géométrie algébrique), en montrant que tout anneau semi-local qui est non ramifié sur un anneau local sans éléments nilpotents n'a pas non plus d'éléments nilpotents.]

(d) *Image réciproque d'un revêtement.* — Soit $Y \to X$ un revêtement non ramifié, soit $f : Z \to X$ un morphisme, et soit $Z \times_X Y$ l'image réciproque (« pull-back ») de Y par f. Alors $Z \times_X Y \to Z$ est un revêtement non ramifié.

D'après (b), le produit $Z \times Y$ est un revêtement non ramifié de $Z \times X$. On applique alors (c) au graphe de f plongé dans $Z \times X$. (On peut d'ailleurs préciser (d) comme on l'a fait pour (c) ; nous laissons l'énoncé au lecteur.)

(e) *Sections.* — Soit $Y \to X$ un revêtement non ramifié et soit $s : X \to Y$ une section de ce revêtement. L'image $s(X)$ de s est alors ouverte et fermée dans Y, et la projection $s(X) \to X$ est un isomorphisme.

Le morphisme s est propre d'après [8], prop. 1. Son image $s(X)$ est donc fermée, et il est clair que $s(X) \to X$ est un isomorphisme. Si $y \in s(X)$ les anneaux locaux de Y et de $s(X)$ en y ont même complété (à savoir $\widehat{\mathscr{O}_x}$) ; comme celui de $s(X)$ est quotient de celui de Y, ils coïncident, ce qui montre que $s(X)$ est égal à Y dans un voisinage de y, autrement dit que $s(X)$ est ouvert.

(f) *Unicité des relèvements.* — Soit $Y \to X$ un revêtement non ramifié, soit Z un espace algébrique, et soient g_1, g_2 deux morphismes de Z dans Y. Si ces deux morphismes ont la même projection $f : Z \to X$, et s'ils prennent la même valeur en un point $z \in Z$, ils coïncident en tout point de la composante connexe de z.

En prenant l'image réciproque de Y par $f : Z \to X$, on se ramène au cas où g_1 et g_2 sont deux *sections* ; on applique alors (e).

1.4. Revêtements galoisiens non ramifiés. — Soit Y un espace algébrique, et soit $\mathfrak{g}$ un groupe fini d'automorphismes de Y. L'espace quotient $Y/\mathfrak{g}$ est muni de façon naturelle d'une structure d'espace annelé ; on sait (cf. par exemple [17], § 3, ou [18], chapitre III, n° 12) que c'est même un espace algébrique si (et seulement si, d'après le théorème de Chevalley cité au n° 1.1) la condition suivante est satisfaite :

(∗) *Toute orbite de* $\mathfrak{g}$ *est contenue dans un ouvert affine de* Y.

Cette hypothèse montre que l'on peut recouvrir Y par des ouverts affines Y_i stables par $\mathfrak{g}$; si B_i désigne l'anneau de coordonnées de Y_i, le groupe $\mathfrak{g}$ opère sur B_i, et l'anneau A_i des invariants de B_i est une algèbre affine. La structure d'espace algébrique de $Y/\mathfrak{g}$ peut alors être définie en « recollant » les variétés affines X_i correspondant aux A_i.

Comme de plus les B_i sont des A_i-modules de type fini ([18], *loc. cit.*, lemme 10) on voit que Y *est entier sur* $Y/\mathfrak{g}$.

Posons $X = Y/\mathfrak{g}$, et soit $x \in X$. Soit $A_x = \pi(\mathscr{O}_Y)_x$ l'anneau semi-local de $\pi^{-1}(x)$ dans Y. Le groupe $\mathfrak{g}$ opère sur A_x, et on peut donc définir ses *groupes de cohomologie* $H^q(\mathfrak{g}, A_x)$; par définition, on a $H^0(\mathfrak{g}, A_x) = \mathscr{O}_x$.

Du fait que le couple $(\mathscr{O}_x, \widehat{\mathscr{O}_x})$ est plat (GAGA, Annexe), on déduit facilement :

$$\mathrm{H}^q(\mathfrak{g}, \mathrm{M} \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x}) = \mathrm{H}^q(\mathfrak{g}, \mathrm{M}) \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x},$$

pour tout $\mathscr{O}_x$-module de type fini M sur lequel opère $\mathfrak{g}$. En appliquant ceci à $\mathrm{M} = \mathrm{A}_x$, et en remarquant que $\mathrm{M} \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x} = \widehat{\mathrm{M}} = \prod_{y \mapsto x} \widehat{\mathscr{O}_y}$, on obtient :

$$\mathrm{H}^q(\mathfrak{g}, \mathrm{A}_x) \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x} = \mathrm{H}^q(\mathfrak{g}, \prod \widehat{\mathscr{O}_y}),$$

le produit étant étendu aux y se projetant sur x. Comme $\mathfrak{g}$ permute les $\widehat{\mathscr{O}_y}$, un
6 résultat bien connu montre que le membre de droite s'identifie à $\mathrm{H}^q(\mathfrak{g}_y, \widehat{\mathscr{O}_y})$, où $\mathfrak{g}_y$ désigne le sous-groupe de $\mathfrak{g}$ laissant fixe le point y choisi. On obtient donc :

(a) *Pour tout $y \in \mathrm{Y}$ se projetant en $x \in \mathrm{X}$, on a un isomorphisme*

$$\mathrm{H}^q(\mathfrak{g}_y, \widehat{\mathscr{O}_y}) = \mathrm{H}^q(\mathfrak{g}, \mathrm{A}_x) \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x}, \quad q = 0, 1, \ldots$$

Supposons alors que le groupe $\mathfrak{g}$ opère *librement*, c'est-à-dire que $\mathfrak{g}_y = \{1\}$ pour tout $y \in \mathrm{Y}$. En appliquant (a) avec $q = 0$, on obtient $\widehat{\mathscr{O}_y} = \widehat{\mathscr{O}_x}$, et $\mathrm{H}^q(\mathfrak{g}, \mathrm{A}_x) \otimes_{\mathscr{O}_x} \widehat{\mathscr{O}_x} = 0$ pour $q \geqslant 1$, d'où $\mathrm{H}^q(\mathfrak{g}, \mathrm{A}_x) = 0$ puisque le couple $(\mathscr{O}_x, \widehat{\mathscr{O}_x})$ est plat. Autrement dit :

(b) *Si $\mathfrak{g}$ opère librement sur* Y*, le morphisme* $\mathrm{Y} \to \mathrm{Y}/\mathfrak{g}$ *est un revêtement non ramifié et l'on a* $\mathrm{H}^q(\mathfrak{g}, \mathrm{A}_x) = 0$ *pour* $q \geqslant 1$ *et* $x \in \mathrm{Y}/\mathfrak{g}$.

7 On dit alors que le morphisme $\mathrm{Y} \to \mathrm{Y}/\mathfrak{g}$ est un revêtement *galoisien* non ramifié de groupe de Galois $\mathfrak{g}$. Les éléments de $\mathfrak{g}$ définissent des automorphismes de ce revêtement ; si X est connexe, la propriété d'unicité 1.3 (f) montre que ce sont les seuls.

On notera que, même si X est connexe, l'espace Y n'est pas nécessairement connexe. Si Y_0 est une composante connexe de Y le sous-groupe $\mathfrak{g}_0$ de $\mathfrak{g}$ formé des éléments laissant stable Y_0 fait de Y_0 un revêtement galoisien non ramifié de X, de groupe de Galois $\mathfrak{g}_0$.

1.5. Construction du revêtement galoisien associé à un revêtement non ramifié quelconque. — Soit X un espace connexe, et soit $\pi : \mathrm{Y} \to \mathrm{X}$ un revêtement non ramifié de X de degré n. Nous nous proposons de construire un revêtement *galoisien* non ramifié de X, dont Y soit le quotient.

Pour cela, soit $\mathrm{Y}^n_{\mathrm{X}}$ l'image réciproque dans Y^n de la diagonale de X^n ; d'après 1.3, on obtient ainsi un revêtement non ramifié $\mathrm{Y}^n_{\mathrm{X}} \to \mathrm{X}$ de degré égal à n^n. De plus, le groupe symétrique $\mathfrak{S}_n$ opère sur ce revêtement. Soit T l'ensemble des points de $\mathrm{Y}^n_{\mathrm{X}}$ laissés fixes par au moins une permutation $\sigma \in \mathfrak{S}_n$ distincte de l'identité ; d'après 1.3 (f), l'ensemble T est à la fois ouvert et fermé

dans Y^n_X. Soit Z son complémentaire ; c'est un revêtement non ramifié de X dont les points sont les familles $(y_1, \ldots, y_n)$ de n points de Y, ayant même image dans X, et tous distincts ; le degré de Z est donc $n!$. Le groupe $\mathfrak{S}_n$ opère librement sur Z ; par passage au quotient, on en déduit un revêtement non ramifié $Z/\mathfrak{S}_n \to X$, de degré 1, c'est-à-dire un isomorphisme d'après 1.2. Ainsi, Z *est un revêtement galoisien non ramifié de* X, de groupe de Galois $\mathfrak{S}_n$; on constate tout de suite que Y *s'identifie au quotient* $Z/\mathfrak{S}_{n-1}$. Le revêtement Z est donc le revêtement cherché.

Si Y est connexe, on peut prendre une composante connexe Z_0 de Z de groupe de Galois $\mathfrak{g} \subset \mathfrak{S}_n$; on constate alors que Y s'identifie à $Z_0/\mathfrak{h}$, avec $\mathfrak{h} = \mathfrak{g} \cap \mathfrak{S}_{n-1}$. Le revêtement Z_0 est le « plus petit » revêtement galoisien non ramifié de X dominant le revêtement Y ; on laisse au lecteur le soin de préciser cet énoncé.

[Lorsque X et Y sont des variétés normales, le revêtement Z_0 n'est autre que le normalisé de X dans la plus petite extension galoisienne de $k(X)$ contenant $k(Y)$.]

§ 2. Espaces fibrés principaux

2.1. Système fibré. — Soit G un groupe algébrique (non nécessairement connexe), et soit E un espace algébrique. Nous dirons que G *opère à droite* sur E si l'on s'est donné un morphisme $F : E \times G \to E$ vérifiant les deux identités :

a) $F(x, 1) = x$ pour tout $x \in E$.

b) $F(x, gg') = F(F(x, g), g')$ pour $x \in E$, $g \in G$, $g' \in G$.

On écrit d'ordinaire $F(x, g)$ sous la forme $x \cdot g$ de telle sorte que les identités ci-dessus s'écrivent $x \cdot 1 = x$ et $x \cdot (g \cdot g') = (x \cdot g) \cdot g'$. On notera que les translations $x \mapsto x \cdot g$ (g fixé dans G) sont des *automorphismes* de E.

On définit de même la notion de groupe *opérant à gauche* sur un espace.

Soit P un espace algébrique sur lequel le groupe G opère à droite, et soit $\pi : P \to X$ un morphisme de P dans un espace X. Nous dirons que (G, P, X) est un *système fibré* si l'on a $\pi(x \cdot g) = \pi(x)$ pour tout $x \in P$. La notion d'*isomorphisme* de système fibré est claire (pour X et G fixés). Il en est de même de la notion d'*image réciproque* par un morphisme $f : X' \to X$: on définit P′ comme le sous-espace de $X' \times P$ formé des couples ayant même image dans X (i.e. $P' = X' \times_X P$), et on définit $\pi' : P' \to X'$ et $F' : P' \times G \to P'$ de façon évidente.

2.2. Définitions. — Soient X un espace algébrique, G un groupe algébrique, et (G, P, X) un système fibré. Nous dirons que ce système (ou, par abus de langage, P lui-même) est *trivial* s'il est isomorphe à $X \times G$ muni des opérations $(x, g) \cdot g' = (x, gg')$ et de la projection canonique $X \times G \to X$. Nous dirons qu'il est *isotrivial* s'il existe un revêtement non ramifié $f : X' \to X$ tel que l'image réciproque de P par f soit un système trivial (de base X').

Nous dirons enfin que P est *localement trivial* (resp. *localement isotrivial*) si tout $x \in X$ possède un voisinage U au-dessus duquel P est trivial (resp. iso-
8 trivial). Un système fibré (G, P, X) localement isotrivial sera aussi appelé un *espace fibré principal de base* X *et de groupe* G. Cette terminologie est une extension de celle de WEIL [19], qui se bornait au cas localement trivial.

2.3. Construction d'espaces fibrés isotriviaux au moyen de cocycles Soit X un espace algébrique, et soit P un espace fibré principal de base X qui soit isotrivial. Ceci signifie qu'il existe un revêtement non ramifié $X' \to X$ sur lequel P devient trivial. Vu 1.5, on peut supposer que X' est *galoisien* sur X ; soit $\mathfrak{g}$ son groupe de Galois.

Notons $\Gamma(X', G)$ le groupe des *morphismes* de X' dans G ; le groupe $\mathfrak{g}$ opère sur $\Gamma(X', G)$ par la règle :

$$(\sigma f)(x') = f(x' \cdot \sigma) \quad \text{(on fait opérer } \mathfrak{g} \text{ à droite sur } X').$$

On peut donc définir $H^0(\mathfrak{g}, \Gamma(X', G))$, qui est un groupe, et $H^1(\mathfrak{g}, \Gamma(X', G))$ qui est un ensemble pointé avec un point marqué (cf. FRENKEL [9], ou GROTHENDIECK [10]).

PROPOSITION 1. — *Les classes d'espaces fibrés principaux de base* X *et groupe* G *dont l'image réciproque sur* X' *est triviale correspondent bijectivement aux éléments de* $H^1(\mathfrak{g}, \Gamma(X', G))$.

Soit P un tel espace fibré, et soit $P' \subset X' \times P$ son image réciproque par $f : X' \to X$. Par hypothèse, P' est isomorphe à $X' \times G$. On a donc un diagramme commutatif :

$$\begin{array}{ccc} X' \times G & \longrightarrow & P \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ X' & \xrightarrow{f} & X. \end{array}$$

L'espace P' peut être considéré comme l'image réciproque par π du revêtement $X' \to X$. D'après 1.3, c'est donc un *revêtement non ramifié de* P*, évidement galoisien de groupe* $\mathfrak{g}$. Ainsi, P s'identifie à $P'/\mathfrak{g}$, et tout revient à déterminer les actions de $\mathfrak{g}$ sur $P' = X' \times G$. Ces opérations doivent être compatibles avec

la projection π' de $X' \times G$ sur X', et doivent commuter aux opérations de G. On en déduit leur expression :

$$(x', g) \cdot \sigma = (x' \cdot \sigma, \varphi_\sigma(x') \cdot g), \quad \sigma \in \mathfrak{g},$$

où φ_σ est un morphisme de X' dans G dépendant de σ, c'est-à-dire une 1-cochaîne de $\mathfrak{g}$ à valeur dans $\Gamma(X', G)$. En exprimant l'associativité :

$$(x', g) \cdot \sigma\tau = \big((x', g) \cdot \sigma\big) \cdot \tau, \quad \sigma, \tau \in \mathfrak{g},$$

on obtient l'identité :

$$\varphi_{\sigma\tau}(x') = \varphi_\tau(x' \cdot \sigma) \cdot \varphi_\sigma(x'), \quad \text{i.e. } \varphi_{\sigma\tau} = (\varphi_\tau)^\sigma \cdot \varphi_\sigma,$$

ce qui signifie que $\sigma \mapsto \varphi_\sigma$ est un 1-*cocycle*. Inversement, la donnée d'un tel cocycle permet de faire opérer $\mathfrak{g}$ sur $X' \times G$, et de définir P comme le quotient $(X' \times G)/\mathfrak{g}$ (la propriété $(*)$ du n° 1.4 est bien vérifiée, car tout sous-ensemble fini d'un groupe algébrique est contenu dans un ouvert affine). Enfin, on vérifie immédiatement que deux cocycles φ_σ et φ'_σ correspondent à des espaces fibrés principaux isomorphes si et seulement s'ils sont cohomologues.

En appliquant la proposition 1 aux ouverts de X, et en passant à la limite (suivant différentes bases de filtre), on obtient :

a) Soit $x \in X$ un point fixé. Les classes d'espaces fibrés principaux de base un *voisinage de* x qui deviennent triviaux sur un voisinage de $f^{-1}(x)$ dans X' correspondent aux éléments de l'ensemble $H^1(\mathfrak{g}, \Gamma_x(X', G))$, en notant $\Gamma_x(X', G)$ le groupe des germes de morphismes de voisinages de $f^{-1}(x)$ dans G.

Exemple. — Prenons $G = \mathbf{G}_a$ le groupe additif. Le groupe $\Gamma_x(X', G)$ n'est autre que l'anneau semi-local de $f^{-1}(x)$, noté A_x dans 1.4. En appliquant 1.4 (b), on voit donc que $H^1(\mathfrak{g}, A_x) = 0$, autrement dit *que tout espace fibré principal de groupe* $\mathbf{G}_a$ *est localement trivial*. Nous donnerons plus loin une autre démonstration de ce fait.

b) Supposons X' et X irréductibles. Les classes d'espaces fibrés principaux de base un ouvert non vide de X (non précisé) qui deviennent triviaux sur un ouvert non vide de X' stable par $\mathfrak{g}$ correspondent aux éléments de $H^1(\mathfrak{g}, k(X', G))$, où $k(X', G)$ désigne *le groupe des applications rationnelles de* X' *dans* G. On notera que $H^1(\mathfrak{g}, k(X', G))$ est aussi l'ensemble des classes *d'espaces homogènes principaux* sur G, qui sont définis sur $k(X)$, et qui ont un point rationnel dans $k(X')$ (cf. LANG-TATE [13]) ; cela provient de ce que la « fibre générique » d'un fibré principal est un tel espace homogène.

2.4. Critère d'isotrivialité locale. — Soit (G, P, X) un système fibré. Considérons les deux propriétés suivantes :

(FP) Si y et y' sont deux éléments de P ayant même projection sur X, il existe un élément g de G et un seul tel que $y' = y \cdot g$; l'application qui, à un tel couple (y, y'), fait correspondre g, est un morphisme du sous-espace T de $P \times P$ où elle est définie dans le groupe G.

(En topologie générale, cette propriété est souvent prise comme définition des espaces fibrés principaux.)

(SL) Pour tout $x \in X$, il existe un revêtement non ramifié $f : U' \to U$, où U est un voisinage de x, et un morphisme $s : U' \to P$ tel que $\pi \circ s = f$ sur U.

(On peut considérer s comme une « section locale multiforme », non ramifiée au voisinage de x.)

PROPOSITION 2. — *Pour qu'un système fibré soit localement isotrivial, il faut et il suffit qu'il vérifie* (FP) *et* (SL).

Supposons que P soit localement isotrivial. Si P devient trivial sur le revêtement $U' \to U$, la propriété (SL) est évidemment satisfaite. Pour vérifier (FP), on peut raisonner localement, c'est-à-dire supposer que $P = (X' \times G)/\mathfrak{g}$, $\mathfrak{g}$ opérant sur $X' \times G$ au moyen d'un cocycle φ_σ. Soit T' le sous-espace de $X' \times G \times X' \times G$ formé des couples $t' = \big((x, g), (x', g')\big)$ tels que $x = x'$; ce sous-espace est stable par $\mathfrak{g}$, et son image dans P est le sous-espace T défini dans (FP). Si $t' \in T'$ posons $\theta'(t') = g^{-1}g'$; un calcul immédiat montre que le morphisme $\theta' : T' \to G$ vérifie $\theta' \circ \sigma = \theta'$ pour tout $\sigma \in \mathfrak{g}$, dont définit par passage au quotient un morphisme $\theta : T \to G$. On a évidemment $y' = y \cdot \theta(y, y')$ pour tout $(y, y') \in T$, ce qui montre que (FP) est vérifié.

Réciproquement, supposons (FP) et (SL) vérifiés. Si $f : U' \to U$ est un revêtement ayant les propriétés postulées dans (SL) nous allons montrer que l'image réciproque P′ de P sur U′ est triviale. En effet, cette image réciproque possède une section s' (correspondant à s), et vérifie (FP). Soit $\theta : T \to G$ le morphisme de T dans G tel que $y' = y \cdot \theta(y, y')$ pour $(y, y') \in T$. On définit alors deux morphismes réciproques :

$$\Phi : X' \times G \longrightarrow P' \quad \text{et} \quad \Psi : P' \longrightarrow X' \times G,$$

par les formules :

$$\Phi(x', g) = s(x') \cdot g \quad \text{et} \quad \Psi(y) = \big(\pi(y), \theta(y, s(\pi(y)))\big).$$

On en déduit bien que P′ est isomorphe à $X' \times G$, c.q.f.d.

9 *Questions.* — 1°) Est-il possible de remplacer la propriété (SL) par la propriété (plus faible) suivante :

(SLF) Pour tout $x \in X$, et tout $y \in P$ se projetant en x, il existe un homomorphisme $\widehat{s} : \widehat{\mathscr{O}_y} \to \widehat{\mathscr{O}_x}$ tel que le composé $\widehat{s} \circ \widehat{\pi}$ soit l'identité sur $\widehat{\mathscr{O}_x}$.

Cette propriété signifie que le système fibré P possède une « section locale formelle » en chaque point de la base.

2°) On peut même se demander si la propriété (FP) n'est pas suffisante à elle seule pour assurer que P est localement isotrivial (X étant défini comme le quotient P/G ; bien entendu, il faudrait démontrer que ce quotient est un espace algébrique, sous des hypothèses raisonnables).

2.5. Premiers exemples d'espaces fibrés principaux. — Les plus importants sont :

a) Les espaces fibrés *localement triviaux*, considérés par WEIL [19], et classifiés par lui dans certains cas (notamment lorsque $G = \mathbf{G}_m$, groupe multiplicatif).

b) Les *revêtements non ramifiés* $X' \to X$ qui sont galoisiens de groupe de Galois $\mathfrak{g}$. En effet, un tel revêtement définit un système fibré qui devient évidemment trivial sur X' lui-même ; c'est donc un espace fibré principal *isotrivial* de groupe $\mathfrak{g}$.

[La définition des espaces fibrés principaux que nous avons adoptée est, en somme, la plus restrictive qui contienne comme cas particuliers les fibrés du type (a) et ceux du type (b), et qui soit stable par les opérations usuelles (cf. n° 2.6).]

c) Un groupe, fibré par un sous-groupe. De façon précise :

PROPOSITION 3. — *Soient* G_1 *un groupe algébrique,* G *un sous-groupe algébrique de* G_1*, et* $H = G_1/G$ *l'espace homogène quotient, muni de la structure d'espace algébrique défini dans* [7]*, exposé 8. Si l'on fait opérer* G *sur* G_1 *par translations à droite, le système* (G, G_1, H) *est un espace fibré principal de base* H *et de groupe* G*.*

D'après la proposition 2, il suffit de montrer que (G, G_1, H) vérifie les axiomes (FP) et (SL). Si $y, y' \in G_1$ ont même image dans $H = G_1/G$, il existe $g \in G$ tel que $y' = y \cdot g$, et cet élément g s'écrit $g = y' \cdot y^{-1}$. Puisque la loi de composition est un morphisme de $G_1 \times G_1$ dans G_1, on voit bien que l'axiome (FP) est vérifié. Reste à construire une « section locale multiforme », régulière en un point donné de H. Soit $(G_1)_0$ la composante connexe de l'élément neutre de G_1, soit $G_0 = (G_1)_0 \cap G$, et $H_0 = (G_1)_0/G_0$; les variétés $(G_1)_0$ et H_0 sont irréductibles, et H_0 est la composante connexe de l'élément origine de H. On sait ([7], *loc. cit.*) que l'extension $k((G_1)_0)/k(H_0)$ des corps de fonctions rationnelles est séparable ; il s'ensuit aussitôt qu'il existe une

sous-variété irréductible X' de $(G_1)_0$, de même dimension que H, et telle que la projection $X' \to H_0$ définisse une extension finie *séparable* $k(X')/k(H_0)$. (Il suffit de prendre pour X' une sous-variété de G_1 passant par l'élément neutre et ayant en ce point une variété tangente transversale à celle de G). D'après
10 1.2, il existe alors un ouvert non vide U de H_0 dont l'image réciproque U' dans X' constitue un revêtement non ramifié $U' \to U$. La propriété (SL) est donc vérifiée au-dessus de U puisque $U' \subset X' \subset G_1$. Par translation, on en déduit qu'elle est vérifiée partout, c.q.f.d.

Remarque. — Soit (G, P, X) un système fibré. Supposons pour simplifier que X soit irréductible et que $P \to X$ soit surjectif. Le raisonnement fait ci-dessus montre alors que, *si l'extension* $k(P)/k(X)$ *est séparable, et si la propriété* (FP) *est vérifiée*, il existe un ouvert non vide de X au-dessus duquel P est isotrivial.

2.6. Systèmes fibrés définis par des revêtements radiciels. — Au lieu de définir les espaces fibrés principaux au moyen des revêtements non ramifiés au sens du § 1, on peut songer à utiliser des revêtements *radiciels*. La difficulté est que l'on ne sait pas définir en général ceux de ces revêtements qui sont « bons », c'est-à-dire ceux qui doivent jouer le rôle des revêtements non ramifiés. On ne le sait, grâce à CARTIER [5], que dans le cas des *variétés non singulières* : si Y est une telle variété, on se donne un sous-fibré vectoriel E du fibré tangent T_Y, et on suppose que les sections rationnelles S(E) de E forment une p-algèbre de Lie restreinte (c'est-à-dire sont stables pour le crochet et la puissance p-ième) ; on définit alors sur Y une nouvelle structure de variété en prenant comme fonctions régulières celles qui sont annulées par les dérivations $D \in S(E)$. Si $X = Y/E$ est la variété ainsi obtenue, l'application canonique $Y \to X$ fait de Y un « bon » revêtement radiciel de X, de hauteur 1. Pour $E = T_Y$, on obtient $X = Y^p$.

Soit maintenant G un groupe algébrique. Sur $Y \times G$ donnons-nous un fibré E comme ci-dessus, en exigeant que E soit invariant par translation, et qu'en chaque point E soit supplémentaire de T_G dans $T_{Y \times G}$; dans le langage de la géométrie différentielle, E est une *connexion intégrable*. (cf. [5], n° 6). Si l'on pose $P = (Y \times G)/E$ et $X = Y^p$, on constate que (G, P, X) est un système
11 fibré, qui devient trivial sur Y. *Un tel système fibré est-il localement isotrivial*? D'après les résultats de CARTIER, il est très vraisemblable que la réponse est affirmative ; il en est en tout cas ainsi, comme il l'a montré, lorsque $G = \mathbf{G}_a$, ou $\mathbf{G}_m$. Il ne devrait pas être difficile de traiter de même le cas du groupe $\mathbf{GL}_n$, d'où, sans doute, tous les groupes linéaires ; peut-être pourra-t-on passer de là au cas général.

§ 3. Opérations sur les espaces fibrés principaux

Nous allons voir que les espaces fibrés principaux (localement isotriviaux) jouissent de propriétés tout analogues à celles dont on a l'habitude en topologie (cf. par exemple GROTHENDIECK [10]). Comme les démonstrations ne présentent aucune difficulté, nous nous bornerons à de brèves indications.

3.1. Caractère fonctoriel en X de $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$. — Soient X un espace algébrique, et G un groupe algébrique. L'ensemble des classes d'espaces fibrés principaux de base X et groupe G sera noté $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$. Les classes d'espaces fibrés localement triviaux forment dans $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$ un sous-ensemble qui n'est autre que le premier « ensemble de cohomologie » $\mathrm{H}^1(\mathrm{X}, \underline{\mathrm{G}})$, en notant $\underline{\mathrm{G}}$ le faisceau des germes de morphismes de X dans G. (cf. [10], n° 5.1 ou [9], n° 3). Le groupe $\mathrm{H}^0(\mathrm{X}, \underline{\mathrm{G}})$ sera également noté $\Gamma(\mathrm{X}, \mathrm{G})$; c'est le groupe des morphismes de X dans G.

Soit $f : \mathrm{X}' \to \mathrm{X}$ un morphisme. Si P est un espace fibré principal de base X et de groupe G, l'image réciproque P' de P par f est encore un espace fibré principal. En effet, il faut vérifier que le système fibré $\mathrm{P}' = \mathrm{P} \times_{\mathrm{X}} \mathrm{X}'$ est localement isotrivial ; la question étant locale, on peut supposer que P est isotrivial, i.e. qu'il existe un revêtement non ramifié $\mathrm{Y} \to \mathrm{X}$ sur lequel P devient trivial ; mais alors P' devient trivial (transitivité des images réciproques) sur $\mathrm{Y}' = \mathrm{Y} \times_{\mathrm{X}} \mathrm{X}'$, qui est un revêtement non ramifié de X' d'après 1.3 ; donc P' est bien localement isotrivial.

On déduit de là une application $f^* : \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}}) \to \widetilde{\mathrm{H}}^1(\mathrm{X}', \underline{\mathrm{G}})$ qui fait de $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$ un *foncteur contravariant* en X (nous verrons plus loin que c'est aussi un foncteur covariant en G).

Soient P et P' deux fibrés principaux de base X et X'. *Pour que* P' *soit isomorphe à* $f^*(\mathrm{P})$, *il faut et il suffit qu'il existe un diagramme commutatif* :

$$\begin{array}{ccc} \mathrm{P}' & \xrightarrow{\mathrm{F}} & \mathrm{P} \\ \downarrow & & \downarrow \\ \mathrm{X}' & \xrightarrow{f} & \mathrm{X} \end{array}$$

(F commutant aux opérations de G).

En effet, l'application F définit un morphisme $\mathrm{P}' \to f^*(\mathrm{P})$, ce qui nous ramène à démontrer notre assertion lorsque $\mathrm{X}' = \mathrm{X}$, f étant l'identité. De plus, on peut supposer que P et P' deviennent triviaux sur un revêtement $\mathrm{Y} \to \mathrm{X}$ non ramifié, galoisien de groupe $\mathfrak{g}$. Ces deux espaces s'identifient donc à $(\mathrm{Y} \times \mathrm{G})/\mathfrak{g}$ et $(\mathrm{Y} \times \mathrm{G})/\mathfrak{g}$ le groupe $\mathfrak{g}$ opérant sur $\mathrm{Y} \times \mathrm{G}$ au moyen de cocycles φ_σ et φ'_σ. Le morphisme F définit un morphisme $\mathrm{F}' : \mathrm{Y} \times \mathrm{G} \to \mathrm{Y} \times \mathrm{G}$, et il

est clair qu'un tel morphisme est nécessairement un isomorphisme. D'où, par passage au quotient par $\mathfrak{g}$, le fait que F lui-même est un isomorphisme.

On voit en particulier qu'un espace fibré principal est *trivial* s'il a une section.

3.2. Construction des espaces fibrés associés. — Soit P un espace fibré principal de base X et groupe G, et soit F un espace algébrique sur lequel le groupe G opère à gauche. Nous nous proposons de construire *l'espace fibré associé à* P*, de base* X*, et de fibre* F. Nous devrons toutefois faire une hypothèse sur F :

(∗∗) *Tout sous-ensemble fini de* F *est contenu dans un ouvert affine de* F.

J'ignore si cette hypothèse (ou une hypothèse analogue) est nécessaire ; de toutes façons, elle est automatiquement remplie si F est quasi-projective.

PROPOSITION 4. — *Faisons opérer* G *à droite sur* $P \times F$ *par la formule* :

$$(y, f) \cdot g = (y \cdot g, g^{-1} \cdot f).$$

Il existe alors un espace algébrique Q *et un seul tel que* $P \times F$ *soit un espace fibré principal de base* Q *et de groupe* G.

L'espace Q est l'espace fibré associé cherché. On le notera $P \times^G F$. Son unicité est évidente [de façon générale, la connaissance d'un fibré principal P et de son groupe structural G détermine la base : c'est le quotient P/G, munie de la structure annelée quotient (vérification immédiate sur les modèles locaux 2.3)]. Son existence est un problème local. On peut donc supposer que $P = (X' \times G)/\mathfrak{g}$ où $X' \to X$ est un revêtement galoisien non ramifié, de groupe de Galois $\mathfrak{g}$ opérant au moyen d'un cocycle φ_σ (cf. n° 2.3). On construit alors Q comme quotient $(X' \times F)/\mathfrak{g}$, où $\mathfrak{g}$ opère sur $X' \times F$ par la formule :

$$(x', f) \cdot \sigma = (x' \cdot \sigma \ , \ \varphi_\sigma(x') \cdot f).$$

La condition (∗) de 1.4 est vérifiée, grâce à l'hypothèse (∗∗) ci-dessus. L'image réciproque sur $X' \times F$ du système fibré $(G, P \times F, Q)$ est isomorphe à $X' \times F \times G$ (calcul facile), d'où la proposition.

Exemples. — a) Si F est un ensemble fini, l'espace fibré $P \times^G F$ est un *revêtement non ramifié* de X. Inversement, si X est connexe, tout revêtement non ramifié de X peut s'obtenir ainsi, d'après 1.5.

b) Si $\alpha : F \to F'$ est un morphisme compatible à l'action de G, on en déduit un morphisme : $P \times^G F \to P \times^G F'$.

c) Si $f : X' \to X$ est un morphisme, l'image réciproque de $P \times^G F$ par f est isomorphe à $P' \times^G F$, où $P' = f^*(P)$. En particulier, on voit que les fibrés

associés $P \times^G F \to X$ deviennent triviaux (localement) sur des revêtements non ramifiés.

3.3. Extension du groupe structural. — Soit $\theta : G \to G'$ un homomorphisme du groupe G dans un groupe G'. On peut faire opérer G à gauche sur G' par la formule :

$$g \cdot g' = \theta(g) \cdot g'.$$

Comme G' vérifie évidemment la condition $(**)$, l'espace fibré associé $P \times^G G'$ est défini. De plus, comme G' opère sur lui-même par translations à droite, et que ces actions commutent aux opérations de G, le groupe G' opère à droite sur $P \times^G G'$.

PROPOSITION 5. — *Si* P *est un espace fibré principal de base* X *et groupe* G, *le fibré associé* $P \times^G G'$ *est un espace fibré principal de base* X *et groupe* G'.

La question étant locale, on peut supposer qu'il existe un revêtement non ramifié $f : X' \to X$ tel que $f^*(P)$ soit trivial. Il en est alors de même de $f^*(P \times^G G')$, c.q.f.d.

Nous noterons $\theta_*(P)$ l'espace fibré principal $P \times^G G'$. On obtient ainsi une application $\theta_* : \widetilde{H}^1(X, \underline{G}) \to \widetilde{H}^1(X, \underline{G'})$, qui fait de $\widetilde{H}^1(X, \underline{G})$ un bifoncteur.

On peut donner de $\theta_*(P)$ une caractérisation analogue à celle donnée dans 3.1 pour l'image réciproque.

3.4. Produits. Cas où G est commutatif. — Soit I un ensemble fini, et, pour tout $i \in I$, soit P_i un espace fibré principal de base X_i et groupe G_i. Il est clair que $\prod P_i$ est alors un espace fibré principal de base $\prod X_i$ et de groupe $\prod G_i$, d'où une application canonique :

$$\prod \widetilde{H}^1(X_i, \underline{G}_i) \to \widetilde{H}^1(\prod X_i, \prod \underline{G}_i).$$

Si tous les X_i sont égaux à un même espace X, l'application diagonale permet d'appliquer $\widetilde{H}^1(\prod X_i, \underline{G})$ dans $\widetilde{H}^1(X, \underline{G})$ (en posant $G = \prod G_i$, pour simplifier les notations).

PROPOSITION 6. — *L'application canonique* $\prod \widetilde{H}^1(X, \underline{G}_i) \to \widetilde{H}^1(X, \underline{G})$ *est bijective.*

Les homomorphismes de projection $G \to G_i$ définissent une application en sens inverse, et on vérifie tout de suite que les deux composés sont égaux à l'identité.

Supposons maintenant que G soit *commutatif*. L'application somme $s : G \times G \to G$ étant un homomorphisme, on a une application

$$s_* : \widetilde{H}^1(X, \underline{G} \times \underline{G}) = \widetilde{H}^1(X, \underline{G}) \times \widetilde{H}^1(X, \underline{G}) \longrightarrow \widetilde{H}^1(X, \underline{G}),$$

c'est-à-dire une loi de composition dans $\widetilde{H}^1(X, \underline{G})$.

PROPOSITION 7. — *La loi de composition définie ci-dessus fait de* $\widetilde{H}^1(X, \underline{G})$ *un groupe commutatif.*

C'est immédiat.

Bien entendu, les applications f^* sont compatibles avec la structure de groupe de $\widetilde{H}^1(X, \underline{G})$. De plus cette structure induit sur $H^1(X, \underline{G})$ sa structure naturelle de groupe de cohomologie.

3.5. Restriction du groupe structural. — Soit G un groupe et soit H un sous-groupe de G. Soit d'autre part P un espace fibré principal de base X et de groupe G. Puisque $H \subset G$, le groupe H opère à droite sur P.

PROPOSITION 8. — *L'espace* P *est un espace fibré principal de groupe* H *et de base* $P \times^G (G/H)$. *Si de plus la fibration de* G *par* H (cf. prop. 3) *est localement triviale, et si* P *est lui-même localement trivial* (comme G-espace fibré principal)*, cette fibration est localement triviale.*

(Noter que l'espace fibré associé $P \times^G (G/H)$ est bien défini, puisque G/H vérifie la condition (∗∗) d'après [18], Chapitre V, n° 20.)

La question étant locale, on peut supposer que l'image réciproque P' de P sur un revêtement non ramifié $X' \to X$ est triviale. On a alors $P' = X' \times G$, et il est clair que P' est un espace fibré principal de base $X' \times (G/H)$ et groupe H, d'où la première partie de la proposition. La seconde partie se démontre de même.

PROPOSITION 9. — *La donnée d'un espace fibré principal de groupe* H *est équivalente à celle d'un espace fibré principal de groupe* G*, muni d'une section du fibré associé en fibre* G/H.

(C'est le critère habituel de « restriction du groupe structural », convenablement précisé.)

Soit Q un fibré principal de groupe H et base X. L'injection $i : H \to G$ permet de lui associer un fibré principal $i_*(Q) = Q \times^H G$ de groupe G ; le fibré associé à $i_*(Q)$ et de fibre G/H est canoniquement isomorphe au fibré associé à H de même fibre ; comme H opère sur G/H en laissant fixe l'origine, ceci définit une section canonique de ce fibré.

Inversement, partons d'un fibré principal P de base X et groupe G, et d'une section $s : X \to P \times^G (G/H)$ du fibré associé en fibres G/H. D'après la proposition 8, P est un espace fibré principal de base $P \times^G G/H$ et de groupe H ; on peut donc définir $s^*(P) = Q$, l'image réciproque de ce fibré par s, et c'est un fibré principal, de base X et de groupe H.

En écrivant quelques diagrammes, on vérifie que les applications que nous venons de définir sont réciproques l'une de l'autre.

PROPOSITION 10. — *Soit* Q *un espace fibré principal de base* X *et groupe* H. *Supposons que le* G*-espace fibré* $P = i_*(Q) = Q \times^H G$ *soit localement trivial, et que la fibration de* G *par* H *soit localement triviale. Alors* Q *est localement trivial.*

En effet, la démonstration de la proposition 9 montre que Q est image réciproque de P considéré comme fibré principal de groupe H et base $P \times^H G/H$; d'après la proposition 8, cet espace fibré est localement trivial, et il en est donc de même de Q.

Exemple. — Isomorphismes de deux fibrés principaux. Soient P et P′ deux fibrés principaux de même groupe G. Ils définissent un fibré $P \times_X P'$ de groupe $G \times G$. Si l'on fait opérer $G \times G$ sur G par translations à droite et à gauche, on en déduit un fibré associé (la fibre étant $(G \times G)/\Delta$, où Δ désigne la diagonale). Les *sections* de ce fibré correspondent aux *isomorphismes* de P sur P′, ou, ce qui revient au même, aux *restrictions du groupe structural* $G \times G$ *à* Δ.

3.6. Suites exactes associées à un sous-groupe. — Tous les résultats du Chapitre V du rapport de GROTHENDIECK [10] qui ne font pas intervenir des groupes de cohomologie de dimension $\geqslant 2$ sont valables pour les fibrés considérés ici. Nous nous bornons à mentionner les plus importants.

Reprenons d'abord la situation du n° précédent, et soit H un sous-groupe algébrique d'un groupe algébrique G. On a alors (cf. [10], p. 71, corollaire à la prop. 5.2.1, voir aussi FRENKEL [9], n° 16) :

PROPOSITION 11. — *On a une suite exacte* :

$$\{e\} \longrightarrow \Gamma(X, H) \longrightarrow \Gamma(X, G) \longrightarrow \Gamma(X, G/H) \xrightarrow{d} \widetilde{H}^1(X, \underline{H}) \longrightarrow \widetilde{H}^1(X, \underline{G}).$$

(Noter que le groupe $\Gamma(X, G)$ opère sur $\Gamma(X, G/H)$, et que l'on a $u(g) = g \cdot 1$. L'exactitude en $\Gamma(X, G/H)$ signifie que $d(f) = d(f')$ si et seulement s'il existe $g \in \Gamma(X, G)$ avec $f' = g \cdot f$, cf. [10].)

La définition de $d : \Gamma(X, G/H) \to \widetilde{H}^1(X, \underline{H})$ est la suivante : un élément $f \in \Gamma(X, G/H)$ définit une section du fibré trivial $(X \times G)/H$, donc (prop. 9)

un espace fibré principal de groupe H dont l'extension à G est triviale ; de plus la proposition 9 montre que l'on obtient par ce procédé tous les espaces fibrés jouissant de cette propriété, c'est-à-dire justement le noyau de $\widetilde{H}^1(X, \underline{H}) \to \widetilde{H}^1(X, \underline{G})$. Le fait que $d(f) = d(f')$ équivaut à l'existence de $g \in \Gamma(X, G)$ tel que $f' = g \cdot f$ se vérifie sans difficulté.

PROPOSITION 12 ([10], prop. 5.3.1). — *Si* H *est un sous-groupe invariant dans* G*, la suite* $\widetilde{H}^1(X, \underline{H}) \to \widetilde{H}^1(X, \underline{G}) \to \widetilde{H}^1(X, \underline{G/H})$ *est exacte. De plus, le groupe* $\Gamma(X, G/H)$ *opère sur* $\widetilde{H}^1(X, \underline{G})$ *et deux éléments de* $\widetilde{H}^1(X, \underline{H})$ *ont même image dans* $\widetilde{H}^1(X, \underline{G})$ *si et seulement s'ils sont congruents suivant ce groupe de permutations.*

L'exactitude résulte immédiatement de la proposition 9. Les opérations de $\Gamma(X, G/H)$ sur $\widetilde{H}^1(X, \underline{H})$ se définissent de la façon suivante :

Soit P un espace fibré principal de groupe H ; l'espace fibré associé de fibre G/H est trivial (en tant qu'espace fibré principal de groupe G/H). Si on l'identifie à $X \times (G/H)$, on voit que tout élément g du groupe $\Gamma(X, G/H)$ en définit une section, donc aussi (prop. 9) un autre fibré P' de groupe H et ayant même image que P dans $\widetilde{H}^1(X, \underline{G})$. L'élément P' est le transformé de P par g, et la proposition 9 montre bien que deux éléments de $\widetilde{H}^1(X, \underline{H})$ ont même image dans $\widetilde{H}^1(X, \underline{G})$ si et seulement s'ils sont transformés l'un de l'autre par un élément du groupe $\Gamma(X, G/H)$.

On peut dire des choses plus précises lorsque H est commutatif ou mieux lorsqu'il est *contenu dans le centre* de G. Dans ce dernier cas, $\widetilde{H}^1(X, \underline{H})$ opère sur $\widetilde{H}^1(X, \underline{G})$, deux éléments de ce dernier ensemble étant congrus suivant ce groupe si et seulement s'ils ont même image dans $\widetilde{H}^1(X, \underline{G/H})$ (cf. [10], prop. 5.5.2 ou [9], n° 18). Enfin, si G lui-même est commutatif, on a :

PROPOSITION 13. — *Si* H *est un sous-groupe d'un groupe commutatif* G*, on a une suite exacte de groupes abéliens* :

$$\{1\} \longrightarrow \Gamma(X, H) \longrightarrow \Gamma(X, G) \longrightarrow \Gamma(X, G/H) \longrightarrow \widetilde{H}^1(X, \underline{H}) \longrightarrow \widetilde{H}^1(X, \underline{G}) \longrightarrow \widetilde{H}^1(X, \underline{G/H})$$

Remarques. — 1°) Si la fibration de G est localement triviale, on peut écrire une suite exacte analogue à celle de la prop. 13, où les H^1 usuels remplacent les $\widetilde{H}^1$. Cela se voit, soit en utilisant la prop. 10, soit directement en remarquant que l'on a *dans ce cas* (et seulement dans ce cas) une suite exacte de faisceaux :

$$0 \longrightarrow \underline{H} \longrightarrow \underline{G} \longrightarrow \underline{G/H} \longrightarrow 0\,.$$

2°) On peut se demander s'il est possible de définir des groupes de cohomologie supérieurs $\widetilde{H}^q(X, \underline{G})$ qui permettent d'étendre la suite exacte de la proposition 13 en toute dimension. GROTHENDIECK a montré que c'est bien le cas (non publié), et il semble même que ces nouveaux groupes de cohomologie, lorsque G est fini, fournissent la « vraie cohomologie » nécessaire pour la 12
démonstration des conjectures de Weil. Voir à ce sujet l'introduction de [12].

§ 4. Critères de trivialité locale. Groupes spéciaux.

4.1. Groupes spéciaux. — Soit G un groupe algébrique. Nous dirons qu'il est *spécial* si tout fibré principal de groupe G est *localement trivial.*

THÉORÈME 1. — *Tout groupe spécial est connexe et linéaire.*

La démonstration sera donnée au n° suivant. Nous allons commencer par démontrer quelques lemmes.

Lemme 1. — Soit G *un groupe algébrique spécial, et soit* H *un sous-groupe de* G. *Pour que* H *soit spécial, il faut et il suffit que la fibration de* G *par* H *soit localement triviale.*

La nécessité est évidente. Pour démontrer la suffisance, soit Q un espace fibré principal, de base X et de groupe H. L'espace fibré $P = Q \times^H G$ est localement trivial, puisque G est spécial. Il en est donc de même de P, d'après la prop. 10.

Lemme 2. — Soit $\varphi : G \to A$ *un homomorphisme d'un groupe algébrique* G *sur une variété abélienne* A. *La restriction de* φ *au centre* C *de* G *est alors surjective.*

Le quotient G/C est un groupe *linéaire* (cf. ROSENLICHT [14], th. 13 ; la démonstration n'est pas difficile : on fait opérer G par automorphismes intérieurs sur les quotients $\mathscr{O}_e/\mathfrak{m}^n$, où $\mathscr{O}_e$ désigne l'anneau local de l'élément neutre, et l'on montre qu'on obtient ainsi une représentation linéaire fidèle de G/C). L'homomorphisme $G/C \to A/\varphi(C)$ est donc trivial (puisque $A/\varphi(C)$ est une variété abélienne), d'où $A = \varphi(C)$.

Lemme 3. — Les hypothèses étant celles du lemme 2, *il existe une famille finie de nombres premiers* p_i *telle que, pour tout nombre premier* $\ell \neq p_i$, *tout élément de* A *d'ordre* ℓ *soit image d'un élément de* G *d'ordre* ℓ.

Le lemme 2 permet de remplacer G par son centre, c'est-à-dire de supposer G *commutatif*. Soit R le noyau de $\varphi : G \to A$, et soit R_0 la composante connexe de l'élément neutre dans R. Le groupe R/R_0 est un groupe fini ; nous prendrons pour p_i les nombres premiers divisant l'ordre de R/R_0, augmentés éventuellement de la caractéristique. Si $\ell \neq p_i$, la multiplication par ℓ est surjective dans R_0 (son application tangente est surjective, et c'est un homomorphisme), donc aussi dans R. Il en résulte bien que tout élément d'ordre ℓ de A est image d'un élément d'ordre ℓ de G.

Lemme 4. — *Soit* X *une variété non singulière, soit* A *une variété abélienne, et soit* P *un espace fibré principal de base* X *et de groupe* A. *Les trois propriétés suivantes sont équivalentes* :

(i) *P est trivial.*

(ii) *P est localement trivial.*

(iii) *P a une section rationnelle.*

Les implications (i)⇒(ii)⇒ (iii) sont claires. Montrons (iii)⇒(i). Il suffit pour cela de prouver que toute *section rationnelle de* P *est régulière* (i.e. est un morphisme). La question étant locale, on peut supposer P de la forme $(X' \times A)/\mathfrak{g}$, où X' est un revêtement galoisien non ramifié de X, de groupe de Galois $\mathfrak{g}$. La section s de P correspond à une section s' de $X' \times A \to X'$ invariante par $\mathfrak{g}$, c'est-à-dire à une application rationnelle de X' dans A. Mais X' est non singulière (puisque X l'est et que le revêtement $X' \to X$ est non ramifié) ; d'après une propriété bien connue des variétés abéliennes (cf. Weil [20], th. 6) l'application s' est partout régulière, et il en est de même de s,

c.q.f.d.

4.2. Démonstration du théorème 1

a) Nous allons d'abord montrer que *tout groupe spécial* G *qui est connexe est linéaire*

D'après le « théorème de Chevalley » (voir Barsotti [1] ou Rosenlicht [14]), le groupe G contient un sous-groupe linéaire R invariant tel que le quotient $G/R = A$ soit une variété abélienne. Il nous faut montrer que A est réduite à 0. Sinon, d'après Weil ([20], p. 127), A possèderait des éléments d'ordre premier ℓ pour tout ℓ distinct de la caractéristique. D'après le lemme 3, il existerait donc un élément $a \in A$ d'ordre premier ℓ qui serait image d'un élément $g \in G$ d'ordre ℓ. Si l'on désigne par N le groupe cyclique $\mathbf{Z}/\ell\mathbf{Z}$, on aurait donc un homomorphisme $\varepsilon : N \to G$ tel que le composé $N \to G \to A$ soit injectif. Nous allons utiliser ε pour construire un espace fibré principal de groupe G qui ne soit pas localement trivial. Pour cela, nous ferons choix d'une

variété algébrique X vérifiant les trois conditions suivantes :

1°) X est *non singulière.*
2°) $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}}) \neq 0$.
3°) *Toute application rationnelle de* X *dans* A/N *est constante.*

[Exemples de telle variété : la droite affine privée d'un point, une courbe elliptique qui n'est pas isogène à aucun facteur simple de A.]

Soit alors $x \in \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}})$, avec $x \neq 0$. Je dis que $\varepsilon_*(x) \in \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$ n'est pas localement trivial (ce qui contredit l'hypothèse faite sur G). En effet, si $\varepsilon_*(x)$ était localement trivial, il en serait *a fortiori* de même de l'image de $\varepsilon_*(x)$ dans $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}})$. D'après le lemme 4, cette image serait nulle. Mais on peut appliquer la suite exacte de la prop. 13 au sous-groupe N de A. On en déduit la suite exacte :

$$\Gamma(\mathrm{X}, \mathrm{A}) \longrightarrow \Gamma(\mathrm{X}, \mathrm{A/N}) \longrightarrow \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}}) \longrightarrow \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}}).$$

Vu l'hypothèse du 3°) ci-dessus, tout morphisme de X dans A/N est constant, donc est image d'un morphisme de X dans A. On en conclut que l'homomorphisme $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}}) \to \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}})$ est injectif, d'où une contradiction, puisque $x \neq 0$.

b) Montrons maintenant que *tout groupe spécial est linéaire*

Soit G un groupe spécial, et soit G_0 sa composante connexe de l'élément neutre. La fibration de G par G_0 est évidemment triviale (l'espace de base étant fini), et le lemme 1 montre que G_0 est spécial. D'après (a), G_0 est donc linéaire, et, en particulier, c'est une variété affine ; comme G est réunion disjointe de composantes connexes toutes isomorphes à G_0, on voit que G est une variété affine, donc est un groupe linéaire ([7], exposé 4, prop. 1).

c) Il reste à montrer que *tout groupe spécial est connexe*

Soit G un tel groupe ; d'après (b), on peut le supposer plongé dans le groupe linéaire $\mathbf{GL}_n$. Soit G_0 la composante connexe de l'élément neutre de G, et soit $\mathrm{N} = \mathrm{G}/\mathrm{G}_0$; c'est un groupe fini. Le groupe $\mathbf{GL}_n$, fibré par G, est localement trivial (puisque G est spécial) ; il en est de même du fibré associé de groupe N, qui n'est autre que $\mathbf{GL}_n/\mathrm{G}_0$. Autrement dit, le revêtement $\mathbf{GL}_n/\mathrm{G}_0 \to \mathbf{GL}_n/\mathrm{G}$, qui est galoisien de groupe N, est à la fois *localement trivial et connexe.* Ce n'est possible que si $\mathrm{N} = \{1\}$, du fait que les variétés $\mathbf{GL}_n/\mathrm{G}_0$ et $\mathbf{GL}_n/\mathrm{G}$ sont normales.

4.3. Caractérisation des groupes spéciaux. — Vu le théorème 1, tout groupe spécial est linéaire. Il nous faut donc donner un critère permettant de reconnaître si un sous-groupe G du groupe linéaire $\mathbf{GL}_n$ est spécial.

THÉORÈME 2. — *Pour qu'un sous-groupe algébrique* G *de* $\mathbf{GL}_n$ *soit spécial, il faut et il suffit que la fibration de* $\mathbf{GL}_n$ *par* G *soit localement triviale.*

(Condition équivalente : il doit exister une *section rationnelle* $\mathbf{GL}_n/\mathrm{G} \to \mathbf{GL}_n$; en effet, on en déduit par translation l'existence d'une section régulière en un point donné de $\mathbf{GL}_n/\mathrm{G}$, cf. la démonstration de la prop. 3.)

COROLLAIRE. — *Soit* G *un groupe linéaire. Si, pour un plongement particulier de* G *dans un groupe* $\mathbf{GL}_n$*, la fibration de* $\mathbf{GL}_n$ *par* G *est localement triviale, ceci a lieu pour tout plongement.*

Démonstration du théorème 2. — Compte tenu du lemme 1, il nous suffit de prouver que le *groupe linéaire général* $\mathbf{GL}_n$ *est spécial.* Soit donc P un espace fibré principal de base X, et de groupe $\mathbf{GL}_n$; si $x \in \mathrm{X}$, nous devons montrer qu'il existe un voisinage de x sur lequel P est trivial. Puisque P est localement isotrivial, il existe en tout cas un ouvert U contenant x, et un revêtement galoisien non ramifié U′ de U, de groupe de Galois $\mathfrak{g}$, tel que l'image réciproque P′ de P sur U′ soit localement triviale. Notons π la projection de U′ sur U, et soit A_x l'anneau semi-local de $\pi^{-1}(x)$ sur U′. Le groupe $\Gamma_x(\mathrm{U}', \mathbf{GL}_n)$ des germes de morphismes des voisinages de $\pi^{-1}(x)$ dans $\mathbf{GL}_n$ peut s'identifier à $\mathbf{GL}_n(\mathrm{A}_x)$. D'après 2.3, l'espace fibré P définit un élément $p_x \in \mathrm{H}^1(\mathfrak{g}, \mathbf{GL}_n(\mathrm{A}_x))$, et P est localement trivial en x si et seulement si p_x est trivial. Nous sommes donc ramenés à démontrer :

Lemme 5. — *On a* $\mathrm{H}^1(\mathfrak{g}, \mathbf{GL}_n(\mathrm{A}_x)) = 0$.

La démonstration est standard (cf. [17], n° 15) : si y_1 est l'un des points de U′ qui se projettent en x, on choisit une matrice $h \in \mathrm{M}_n(\mathrm{A}_x)$ qui prend la valeur 1 en y_1, et 0 aux autres points de $\pi^{-1}(x)$. Si φ_σ est un 1-cocycle de $\mathfrak{g}$ à valeur dans $\mathbf{GL}_n(\mathrm{A}_x)$, on pose :

$$a = \sum_{\tau \in \mathfrak{g}} \tau(h) \cdot \varphi_\tau.$$

On vérifie tout de suite que a est inversible en chacun des points de $\pi^{-1}(x)$, donc appartient à $\mathbf{GL}_n(\mathrm{A}_x)$. On a de plus :

$$\sigma(a)\varphi_\sigma = \sum \sigma\tau(h) \cdot \sigma(\varphi_\tau)\varphi_\sigma = \sum \sigma\tau(h) \cdot \varphi_{\sigma\tau} = a,$$

ce qui montre que φ_σ est un cobord et achève la démonstration.

4.4. Exemples de groupes spéciaux.

a) *Le groupe* $\mathbf{G}_m$ *est spécial.* — En effet, c'est $\mathbf{GL}_1$.

Le groupe $\mathbf{G}_a$ *est spécial*; en effet, on le plonge dans $\mathbf{GL}_2$ comme groupe triangulaire inférieur avec des 1 sur la diagonale : $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, et le groupe triangulaire supérieur forme une section rationnelle. Plus généralement (ROSENLICHT [14], théorème 10) :

PROPOSITION 14. — *Tout groupe linéaire connexe résoluble est spécial.*

Un tel groupe est en effet extension multiple de groupes isomorphes à $\mathbf{G}_m$ ou à $\mathbf{G}_a$ (cf. par exemple [7]), et il suffit d'appliquer le lemme suivant :

Lemme 6. — *Soit* G *un groupe algébrique et soit* H *un sous-groupe invariant de* G. *Si* H *et* G/H *sont spéciaux, le groupe* G *est spécial.*

La démonstration est immédiate (utiliser par exemple la suite exacte de la prop. 12).

b) *Le groupe* $\mathbf{SL}_n$ *est spécial.* — En effet, il admet comme supplémentaire dans $\mathbf{GL}_n$ le groupe des matrices de la forme :

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

c) *Le groupe symplectique* $\mathbf{Sp}_{2n}$ *est spécial.* — En effet, l'espace homogène $\mathbf{GL}_{2n}/\mathbf{Sp}_{2n}$ s'identifie à l'espace des formes bilinéaires alternées non dégénérées. Dire que la fibration $\mathbf{GL}_{2n}/\mathbf{Sp}_{2n}$ admet une section rationnelle revient à dire que la forme alternée *générique*

$$\sum_{i<j} u_{ij}\, x_i \wedge x_j$$

peut être ramenée à la forme canonique $\sum x_{2i-1} \wedge x_{2i}$ par une matrice à coefficients dans $k(u_{ij})$; or c'est effectivement possible, d'après la théorie élémentaire des formes alternées.

d) On peut montrer en utilisant le théorème 2, que le *groupe orthogonal unimodulaire* $\mathbf{SO}_n$ *n'est pas spécial pour* $n \geqslant 3$. — Cela revient à prouver que la forme quadratique générique

$$\sum_{i<j} u_{ij}\, x_i x_j$$

ne peut pas se mettre sous la forme $\sum x_i^2$ par un changement linéaire de variables à coefficients dans le corps engendré sur k par les u_{ij} et par la racine carrée du discriminant $\det(u_{ij})$.

Nous ne donnerons pas la démonstration car le résultat en question est un cas très particulier de la *caractérisation des groupes spéciaux donnée par* GROTHENDIECK (voir le dernier exposé de ce séminaire). Cette caractérisation montre notamment que *les seuls groupes semi-simples spéciaux sont les produits des groupes* $\mathbf{SL}_n$ *et* $\mathbf{Sp}_{2n}$. En particulier, *les groupes projectifs* $\mathbf{PGL}_n$, $n \geqslant 2$, *ne sont pas spéciaux, non plus que les groupes de spineurs* $\mathbf{Spin}_n$ *pour* $n \geqslant 7$ (ce dernier exemple contredit la conjecture faite dans GAGA, p. 34).

§ 5. Classification des espaces fibrés principaux dans quelques cas particuliers

5.1. Groupes $\mathbf{G}_a$ et $\mathbf{G}_m$. — Comme ces groupes sont spéciaux (4.4), les groupes de classes de fibrés $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathbf{G}}_a)$ et $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathbf{G}}_m)$ s'identifient simplement aux groupes de cohomologie $\mathrm{H}^1(\mathrm{X}, \mathscr{O}_x)$ et $\mathrm{H}^1(\mathrm{X}, \mathscr{O}_x^*)$; lorsque X est non singulière, ce dernier groupe s'identifie lui-même au groupe des *classes de diviseurs* sur X, pour l'équivalence linéaire (cf. WEIL [19]).

5.2. Groupes abéliens finis. — Soit d'abord G un groupe cyclique d'ordre n premier à la caractéristique. Si $\theta : \mathbf{G}_m \to \mathbf{G}_m$ est définie par $\theta(\lambda) = \lambda^n$, on a la suite exacte :

$$0 \longrightarrow \mathrm{G} \longrightarrow \mathbf{G}_m \xrightarrow{\theta} \mathbf{G}_m \longrightarrow 0.$$

En appliquant la proposition 13, on en déduit :

PROPOSITION 15. — *On a une suite exacte* :

$$0 \longrightarrow \Gamma(\mathrm{X}, \mathbf{G}_m)_n \longrightarrow \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}}) \longrightarrow {}_n\mathrm{H}^1(\mathrm{X}, \mathscr{O}^*) \longrightarrow 0$$

(Pour tout groupe commutatif H, on note H_n le quotient $\mathrm{H}/n\mathrm{H}$ et ${}_n\mathrm{H}$ le sous-groupe de H formé des éléments d'ordre divisant n.)

Lorsque X est complète et connexe, on a $\Gamma(\mathrm{X}, \mathbf{G}_m) = k^*$, et $\Gamma(\mathrm{X}, \mathbf{G}_m)_n = 0$. On en déduit (cf. [17], n° 15) :

COROLLAIRE. — *Lorsque* X *est non singulière et complète, le groupe des classes de revêtements non ramifiés de* X*, de groupe de Galois cyclique d'ordre* n*, est isomorphe au groupe des classes de diviseurs de* X *d'ordre divisant* n.

Si G est cyclique d'ordre p, on utilise la suite exacte :

$$0 \longrightarrow \mathrm{G} \longrightarrow \mathbf{G}_a \xrightarrow{\wp} \mathbf{G}_a \longrightarrow 0 \qquad (\wp(\lambda) = \lambda^p - \lambda),$$

et l'on obtient (cf. [17], n° 16) :

PROPOSITION 16. — *Lorsque* X *est complète, le groupe des classes de revêtements non ramifiés de* X*, de groupe de Galois cyclique d'ordre* p *égal à la caractéristique, est isomorphe au sous-groupe de* $\mathrm{H}^1(\mathrm{X}, \mathscr{O}_\mathrm{X})$ *formé des éléments annulés par* $\wp$.

On retrouverait de même la classification des revêtements cycliques d'ordre p^n donnée dans [17], n° 18, en utilisant les vecteurs de Witt.

5.3. Variétés abéliennes. — Soit X une variété *non singulière*, et soit A une variété abélienne.

Lemme 7. — Le groupe $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}})$ *est un groupe de torsion.*

Soit P un espace fibré principal de base X et de groupe A. Il existe un ouvert non vide U de X et un revêtement galoisien non ramifié $\mathrm{U}' \to \mathrm{U}$ tels que l'image réciproque P' de P sur U soit triviale. Soit n l'ordre de ce revêtement, et soit $\mathfrak{g}$ son groupe de Galois. D'après 2.3, l'espace fibré P définit un élément p_U d'un certain groupe de cohomologie de $\mathfrak{g}$; puisque $\mathfrak{g}$ est d'ordre égal à n, on a $n \cdot p_\mathrm{U} = 0$, ce qui signifie que n·P est trivial sur U. D'après le lemme 4, l'espace fibré n·P est trivial sur X tout entier, c.q.f.d.

[Ce résultat est spécial aux variétés non singulières. Si l'on prend par exemple pour X deux droites ayant un point en commun, on trouve que $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}})$ s'identifie à A elle-même.] 13

PROPOSITION 17. — *Supposons que la caractéristique du corps de base soit nulle. Alors tout espace fibré principal de base* X *non singulière et de groupe* A *s'obtient par extension du groupe structural à partir d'un revêtement abélien non ramifié* $\mathrm{X}' \to \mathrm{X}$*, de groupe de Galois un sous-groupe de* A.

Soit $p_\mathrm{X} \in \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}})$. D'après le lemme 7, il existe n tel que $n \cdot p_\mathrm{X} = 0$. Soit θ l'homothétie de rapport n dans A, et soit N son noyau. On a la suite exacte $0 \to \mathrm{N} \to \mathrm{A} \xrightarrow{\theta} \mathrm{A} \to 0$, d'où (prop. 13) la suite exacte :

$$\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}}) \longrightarrow \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}}) \xrightarrow{\theta} \widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{A}}).$$

Comme le foncteur $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{G}})$ est additif en G (cf. 3.4), l'homomorphisme θ n'est autre que la multiplication par n, et p_X appartient à son noyau. Donc p_X est image d'un élément de $\widetilde{\mathrm{H}}^1(\mathrm{X}, \underline{\mathrm{N}})$, c.q.f.d.

COROLLAIRE 1. — *Tout espace fibré principal de base une variété abélienne et de groupe une variété abélienne peut être muni d'une structure de variété abélienne.*

En effet, on sait que c'est vrai pour les revêtements abéliens non ramifiés.

COROLLAIRE 2. — *Tout espace fibré principal de base* X *non singulière et de groupe* G *connexe s'obtient par extension du groupe structural à partir d'un espace fibré principal de groupe un groupe linéaire.*

Soit $G/R = A$ le plus grand quotient de G qui soit une variété abélienne. Si $x \in \widetilde{H}^1(X, \underline{G})$, soit p_X l'image de x dans $\widetilde{H}^1(X, \underline{A})$; d'après la proposition 17, il existe un sous-groupe fini N de A tel que l'image de p_X dans $\widetilde{H}^1(X, \underline{A/N})$ soit triviale. Soit S l'image réciproque de N dans G ; on a $G/S = A/N$, ce qui montre que x est image d'un élément $y \in \widetilde{H}^1(X, \underline{S})$. Comme $S/R = N$, le groupe S est une variété affine, donc est linéaire, c.q.f.d.

Remarque. — On voit pourquoi la proposition 17 n'est pas valable en caractéristique p ; c'est qu'il se peut que p_X soit, par exemple, d'ordre égal à p, et la multiplication par p dans A *n'est pas une isogénie séparable*, donc ne permet pas de définir un isomorphisme $A/N \to A$. Il est d'ailleurs facile de construire des exemples (avec X variété abélienne) montrant que *la proposition 17 et son corollaire 2 peuvent être inexacts en caractéristique* $p > 0$. Pour les rétablir, il faudrait élargir le cadre que nous avons adopté, et accepter des *revêtements radiciels* ainsi que des espaces algébriques dont le faisceau d'anneaux possède
14 des *éléments nilpotents*. Le groupe fini N serait remplacé par une « hyperalgèbre » finie, au sens de Cartier. Il est vraisemblable que l'on récupèrerait alors le corollaire 1.

5.4. Groupe linéaire général et groupe linéaire unimodulaire. — Ces deux groupes sont spéciaux. Un fibré principal de base X et de groupe $\mathbf{GL}_n$ est donc localement trivial ; comme $\mathbf{GL}_n$ est le groupe des automorphismes d'un espace vectoriel de dimension n, on en déduit facilement qu'un tel espace correspond biunivoquement à un *fibré à fibre vectorielle de rang* n, ou encore à un *faisceau algébrique localement libre de rang* n (cf. FAC, n° 50). La classification de ces fibrés est d'ailleurs un problème difficile, qui n'est résolu que pour des espaces X très particuliers [plan affine (SESHADRI), courbe de genre 0 (GROTHENDIECK), courbe de genre 1 (ATIYAH)].

D'après la prop. 9, un fibré principal de groupe $\mathbf{SL}_n$ est déterminé par la donnée d'un fibré principal de groupe $\mathbf{GL}_n$ et d'une section du fibré associé de fibre $\mathbf{GL}_n/\mathbf{SL}_n$; cela revient à se donner un fibré E à fibre vectorielle de rang n, et une section du fibré $\wedge^n E$ partout non nulle.

5.5. Groupe projectif. — Soit $\mathbf{PGL}_n = \mathbf{GL}_n/\mathbf{G}_m$ le groupe projectif de dimension n (groupe des automorphismes de l'espace projectif $\mathbf{P}_{n-1}$). Ce n'est

pas un groupe spécial ; introduisons donc l'ensemble $\mathrm{H}^1_x(\mathbf{PGL}_n)$ des classes d'espaces fibrés principaux *locaux* de groupe $\mathbf{PGL}_n$, définis au voisinage d'un point fixé $x \in \mathrm{X}$. La suite exacte associée à l'extension $\mathbf{GL}_n/\mathbf{G}_m = \mathbf{PGL}_n$ montre que $\mathrm{H}^1_x(\mathbf{PGL}_n)$ *se plonge dans* $\mathrm{H}^2_x(\mathbf{G}_m)$ (qui est un groupe abélien) ; on obtient ainsi ceux des éléments de $\mathrm{H}^2_x(\mathbf{G}_m)$ qui sont « décomposés » par un revêtement non ramifié de degré n. On est ici dans une situation qui généralise celle du « groupe de Brauer ». D'ailleurs, si l'on considérait des fibrés de groupe $\mathbf{PGL}_n$ du point de vue birationnel, on verrait qu'ils correspondent biunivoquement aux classes d'algèbres simples sur $k(\mathrm{X})$ qui contiennent une algèbre de degré n^2 (ou, ce qui revient au même, qui sont décomposées par une extension de $k(\mathrm{X})$ dont le degré divise n). [Pour définir une algèbre simple à partir d'un fibré, utiliser le fait que $\mathbf{PGL}_n$ est le groupe des automorphismes de l'algèbre de matrices $\mathrm{M}_n(k)$.]

Nous n'insisteront pas là-dessus, et nous nous bornerons à mentionner le résultat suivant (dû à GROTHENDIECK) :

PROPOSITION 18. — *Soit* X *une variété non singulière, et soit* P *un espace fibré principal de base* X *et de groupe* $\mathbf{PGL}_n$. *Les trois propriétés suivantes sont équivalentes* :

(i) P *est image d'un fibré de groupe* $\mathbf{GL}_n$.
(ii) P *est localement trivial.*
(iii) P *possède une section rationnelle.*

Les implications (i)⇒(ii)⇒(iii) sont triviales. Pour montrer que (iii)⇒(i) on construit le fibré Y en espaces projectifs associés à P. Grâce à (iii) et au fait que Y est non singulier, on peut trouver un fibré à fibre vectorielle de rang 1 sur Y qui induit sur chaque fibre projective le fibré standard (correspondant à une section hyperplane). Sur chaque fibre, les sections de ce fibré forment un espace vectoriel de dimension n ; et l'on obtient ainsi le fibré vectoriel cherché.

On peut aussi démontrer directement que (i)⇔(ii) (cf. [11], n° 3.4) et que (ii)⇔(iii) (en comparant, au moyen d'une suite exacte, le groupe de Brauer local $\mathrm{H}^2_x(\mathbf{G}_m)$, et le véritable groupe de Brauer).

COROLLAIRE. — *Si* X *est une courbe non singulière, tout espace fibré principal de base* X *et de groupe* $\mathbf{PGL}_n$ *est localement trivial.*

Soit P un tel espace fibré. D'après le théorème de Tsen, le groupe de Brauer de $k(\mathrm{X})$ est réduit à 0 ; donc P possède une section rationnelle, et on applique la prop. 18.

Remarque. — La comparaison du lemme 4 et de la prop. 18 suggère la question suivante ; soit X une variété non singulière, soit G un groupe algébrique

connexe, et soit P un espace fibré principal de base X et de groupe G. Est-il
15 vrai que, si P possède une section rationnelle, P est localement trivial ?

5.6. Groupe orthogonal. — (Nous supposons pour simplifier que la caractéristique p du corps k est $\neq 2$; lorsque $p = 2$, il faudrait modifier légèrement ce qui suit, et utiliser notamment l'invariant d'Arf à la place du discriminant.)

Soit $\mathbf{O}_n$ le groupe orthogonal de dimension n. L'espace homogène $\mathbf{GL}_n/\mathbf{O}_n$ s'identifie au point de vue ensembliste à l'espace Q_n des formes quadratiques non dégénérées $\sum_{i\leqslant j} u_{i,j}\, x_i x_j$, $\det(u_{i,j}) \neq 0$. Si l'on munit Q_n de sa structure évidente de variété algébrique (ouvert dans l'espace affine de dimension $n(n+1)/2$), on vérifie que l'application tangente à $\mathbf{GL}_n/\mathbf{O}_n \to \mathrm{Q}_n$ est partout surjective, donc que c'est un *isomorphisme*. D'après la prop. 9, un fibré principal de groupe $\mathbf{O}_n$ correspond biunivoquement à un *fibré à fibre vectorielle dont chaque fibre est munie d'une forme quadratique non dégénérée*, les coefficients de cette forme étant fonctions régulières du point (ce qui a un sens localement). Un tel fibré est *localement trivial* en $x \in \mathrm{X}$ si l'on peut trouver, au voisinage de x, n sections formant en chaque point voisin de x une base orthonormale.

De même, un fibré principal de groupe $\mathbf{SO}_n$ correspond à un fibré orthogonal E dont chaque fibre est « orientée » (cela signifie qu'on s'est donné une section s de $\wedge^n \mathrm{E}$ de carré égal à 1). On voit immédiatement quand un tel fibré est trivial (resp. localement trivial). On montre en particulier que *tout fibré principal de groupe* $\mathbf{SO}_n$ *et de base une courbe non singulière est localement trivial* (cette
16 propriété est-elle vraie pour tous les groupes linéaires connexes ?).

§ 6. Comparaison avec les espaces fibrés analytiques

Dans tout ce §, on suppose $k = \mathbf{C}$, corps des nombres complexes. On rappelle que tout espace algébrique définit fonctoriellement un espace analytique X^h, et tout faisceau algébrique cohérent $\mathscr{F}$ sur X définit un faisceau analytique cohérent $\mathscr{F}^h$; le faisceau $(\mathscr{O}_\mathrm{X})^h$ sera noté $\mathscr{H}_\mathrm{X}$, c'est le faisceau des germes de fonctions holomorphes sur X. Pour plus de détails voir GAGA et Grothendieck ([3], exposé n° 2)

6.1. Revêtements non ramifiés. — Soit T un espace analytique. Nous dirons qu'un morphisme (analytique) $f : \mathrm{Z} \to \mathrm{T}$ est un revêtement fini non ramifié s'il est propre, et si c'est un isomorphisme local en chaque point $z \in \mathrm{Z}$.

Proposition 19. — *Si* $\pi : \mathrm{Y} \to \mathrm{X}$ *est un revêtement algébrique non ramifié,* $\pi^h : \mathrm{Y}^h \to \mathrm{X}^h$ *est un revêtement non ramifié.*

Puisque π est propre, il en est de même de π^h (GROTHENDIECK [3], p. 2.08) ; de plus, l'image directe du faisceau $\mathscr{H}_Y$ est un faisceau cohérent sur X^h ([3], *loc. cit.*). Or, si $x \in X$, le module ponctuel $\pi(\mathscr{H}_Y)_x$ n'est autre que le produit direct $\prod \mathscr{H}_y$, pour les y se projetant en x. Il s'ensuit que chacun des $\mathscr{H}_Y$ est un $\mathscr{H}_x$-module de *type fini*. Mais on sait que $\widehat{\mathscr{H}_x} = \widehat{\mathscr{O}}_x$ et de même pour y (cf. GAGA) ; comme le revêtement $Y \to X$ est non ramifié, on en déduit $\widehat{\mathscr{H}_y} = \widehat{\mathscr{H}_x}$, d'où $\mathscr{H}_y = \mathscr{H}_x$ d'après les propriétés bien connues des complétions des modules de type fini. Ceci signifie que π^h est un isomorphisme local en y, c.q.f.d.

[On peut donner une démonstration plus élémentaire, en remarquant que Y peut s'obtenir localement par une équation du type :

$$(*) \qquad z^n + a_1 z^{n-1} + \cdots + a_n = 0, \ a_i \in \mathscr{O}_x,$$

qui est *non ramifiée* au sens suivant : les valeurs α_i des a_i en x sont telles que l'équation réduite $z^n + \alpha_1 z^{n-1} + \cdots + \alpha_n = 0$ aient toutes ses racines *distinctes*. L'espace Y^h est défini localement par la même équation $(*)$, et on doit montrer que celle-ci se décompose en produit $\prod_{1 \leqslant i \leqslant n}(z - z_i)$, avec $z_i \in \mathscr{H}_x$, ce qui est immédiat.]

PROPOSITION 20. — *Soit $\pi : Y \to X$ un revêtement algébrique non ramifié, soit Z un espace algébrique, soit $f : Z \to X$ un morphisme algébrique, et soit $g : Z^h \to Y^h$ un morphisme analytique tel que $\pi^h \circ g = f^h$. Alors g est algébrique.*

En prenant l'image réciproque $Z \times_X Y$, on se ramène au cas $Z = X$, autrement dit au cas d'une *section holomorphe* $s : X^h \to Y^h$. On doit prouver que cette section est algébrique. On peut supposer X connexe ; $s(X^h)$ est alors une composante connexe de Y^h. Mais on sait (cf. par exemple WEIL [21], p. 166) que les composantes connexes de l'espace analytique Y^h ne sont autres que les composantes connexes de l'espace algébrique Y. Il s'ensuit bien que s est algébrique.

COROLLAIRE. — *Si Y et Y' sont deux revêtements algébriques non ramifiés de X, tout isomorphisme analytique de ces revêtements est algébrique.*

Soit alors $T \to X^h$ un revêtement fini analytique non ramifié X^h ; d'après le corollaire précédent, la phrase « T est un revêtement algébrique » a un sens précis. On peut se demander si c'est toujours le cas. C'est vrai lorsque X est *complète* (voir plus loin), ou *normale* (d'après GRAUERT-REMMERT) ; j'ignore ce qu'il en est en général. 17

6.2. Espace fibré analytique défini par un espace fibré algébrique

PROPOSITION 21. — *Soient* X *un espace algébrique,* G *un groupe algébrique et* P *un espace fibré principal* (localement isotrivial) *de base* X *et de groupe* G. *L'espace analytique* P^h *est alors un espace fibré principal analytique* (localement trivial) *de base* X^h *et de groupe* G^h.

En effet, P^h devient localement trivial sur un revêtement non ramifié $U'^h \to U^h$, où U est un voisinage d'un point x donné dans X. Comme un revêtement non ramifié est localement un produit (au point de vue analytique), on en déduit que P^h est localement trivial.

6.3. Cas où la base est complète. — Lorsque X est complète, les raisonnements de GAGA, n° 20 s'appliquent sans modifications. Nous nous bornerons à énoncer les résultats que l'on obtient ainsi :

PROPOSITION 22. — *Tout isomorphisme analytique entre deux espaces fibrés algébriques principaux de base* X *et de groupe* G *est algébrique.*

PROPOSITION 23. — *Soit* H *un sous-groupe algébrique de* G, *et soit* P *un espace fibré principal analytique, de base* X^h *et de groupe* H^h. *Pour que* P *soit algébrique, il faut et il suffit qu'il en soit ainsi de l'espace* $P \times^H G$ *déduit de* P *par extension du groupe structural de* H *à* G.

De plus, tout espace fibré principal analytique de groupe $\mathbf{GL}_n$ est algébrique (cf. GAGA, prop. 18). En combinant ce résultat avec la prop. 23, on obtient :

THÉORÈME 3. — *Si* G *est un groupe algébrique linéaire, tout espace fibré analytique principal de base* X^h *et groupe* G^h *est algébrique.*

En général, cet espace fibré algébrique n'est que *localement isotrivial*; toutefois, si G est *spécial*, il est localement trivial : c'est le cas traité dans GAGA.

COROLLAIRE. — *Tout revêtement analytique fini non ramifié de* X^h *est algébrique.*

En effet un groupe fini est linéaire.

Le théorème 3 ne s'étend par au cas d'un groupe G qui n'est pas linéaire. On a toutefois le résultat suivant :

THÉORÈME 4. — *Soit* G *un groupe algébrique connexe, et soit* A *le plus grand quotient de* G *qui soit une variété abélienne. Soit* P *un espace fibré analytique principal de base une variété algébrique non singulière complète* X^h, *et de groupe* G^h ; *soit* $p_A \in H^1(X^h, \underline{A}^h)$ *la classe de l'espace fibré analytique de*

groupe A^h *déduit de* P *par extension du groupe structural de* G^h *à* A^h. *Pour que* P *soit algébrique, il faut et il suffit que* p_A *soit un élément d'ordre fini dans* $H^1(X^h, \underline{A}^h)$.

La condition est nécessaire, d'après le lemme 7 du n° 5.3. Inversement, soit n un entier $\geqslant 1$ tel que $n \cdot p_A = 0$, et soit N le noyau de l'homothétie de rapport n dans A; l'espace fibré principal de groupe A/N déduit de P par extension du groupe structural est donc analytiquement trivial. Soit S l'image réciproque de N dans G ; comme $G/S = A/N$, l'analogue analytique de la proposition 12 montre que p_A est image d'un élément $y \in H^1(X^h, \underline{S}^h)$. Puisque le groupe S est linéaire, l'espace fibré principal correspondant à y est algébrique, et il en est de même de P, c.q.f.d.

Remarque. — Lorsque $G = A$, on voit que les éléments algébriques du groupe $H^1(X^h, \underline{A}^h)$ sont exactement *les éléments de torsion*, ou, ce qui revient au même, les éléments qui deviennent triviaux sur une extension abélienne non ramifiée de X^h. On comparera avec les résultats de BLANCHARD [2], donnant des critères pour que P soit *kählérien* ou *projectif* (lorsque X est elle-même supposée projective).

6.4. Un exemple d'espace fibré projectif qui ne provient pas d'un espace fibré linéaire. — Il est facile de donner de tels exemples lorsqu'on se place à un point de vue « birationnel », c'est-à-dire lorsqu'on n'exige aucune propriété particulière de la base : en effet, on sait que le groupe de Brauer de $k(X)$ est $\neq 0$ si $\dim(X) \geqslant 2$. Nous nous proposons ici de construire un exemple où la base est une *variété projective*, définie sur $\mathbf{C}$.

Soit $\pi : Y \to X$ un revêtement galoisien non ramifié, de groupe de Galois $\mathfrak{g}$, les variétés X et Y étant projectives non singulières (nous les choisirons de façon plus précise ultérieurement). Soit $\varphi : \mathfrak{g} \to \mathbf{PGL}_n$ un homomorphisme de $\mathfrak{g}$ dans le groupe projectif $\mathbf{PGL}_n$; par extension du groupe structural, on déduit de Y un espace fibré principal isotrivial P, de base X, et de groupe $\mathbf{PGL}_n$. Nous allons voir qu'on peut choisir Y, X, $\mathfrak{g}$, φ de telle sorte que *cet espace fibré ne provienne pas d'un fibré de groupe* $\mathbf{GL}_n$, *même du point de vue topologique* (et *a fortiori* du point de vue analytique, ou, ce qui revient au même, algébrique).

La suite exacte $1 \to \mathbf{G}_m \to \mathbf{GL}_n \to \mathbf{PGL}_n \to 1$ montre que l'obstruction au « relèvement » de P est un élément du groupe de cohomologie $H^2(X, \mathscr{C}^*)$ où $\mathscr{C}^*$ désigne le faisceau des germes d'applications continues de X dans $\mathbf{G}_m$; ce groupe est lui-même isomorphe à $H^3(X, \mathbf{Z})$, comme on le voit tout de suite. Nous désignerons par $\alpha \in H^3(X, \mathbf{Z})$ l'obstruction en question.

D'autre part, l'image réciproque de $\mathbf{GL}_n$ par φ définit une extension E_φ de $\mathfrak{g}$ par $\mathbf{G}_m$, donc un élément de $\mathrm{H}^2(\mathfrak{g}, \mathbf{G}_m) = \mathrm{H}^3(\mathfrak{g}, \mathbf{Z})$; nous désignerons par β cet élément. Le revêtement Y définit, comme on sait, un homomorphisme
18 $\theta_\mathrm{Y} : \mathrm{H}^q(\mathfrak{g}, \mathbf{Z}) \to \mathrm{H}^q(\mathrm{X}, \mathbf{Z})$ pour tout entier $q \geqslant 0$; un calcul explicite montre que *l'image par θ_Y de l'élément β n'est autre que l'obstruction α définie ci-dessus.* Nous aurons donc l'exemple cherché si nous choisissons les données de telle sorte que les deux conditions suivantes soient satisfaites :

(i) L'élément $\beta \in \mathrm{H}^3(\mathfrak{g}, \mathbf{Z})$ n'est pas nul.

(ii) L'homomorphisme $\theta_\mathrm{Y} : \mathrm{H}^3(\mathfrak{g}, \mathbf{Z}) \to \mathrm{H}^3(\mathrm{X}, \mathbf{Z})$ est injectif.

La condition (i) signifie que l'extension E_φ de $\mathfrak{g}$ par $\mathbf{G}_m$ n'est pas triviale. Nous la vérifierons en prenant pour $\mathfrak{g}$ le « Viergruppe » $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, plongé dans le groupe projectif $\mathbf{PGL}_2$ au moyen des matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; le groupe E_φ n'est pas commutatif (les matrices ci-dessus ne commutent pas dans $\mathbf{GL}_2$, mais seulement dans $\mathbf{PGL}_2$), donc $\beta \neq 0$.

Pour la condition (ii), nous utiliserons la construction donnée dans [17], n° 20 ; on obtient ainsi un revêtement $\mathrm{Y} \to \mathrm{X}$ ayant pour groupe de Galois $\mathfrak{g}$, Y étant une intersection complète non singulière de dimension r arbitraire (nous prendrons $r \geqslant 3$) ; le groupe $\mathfrak{g}$ opère sur l'espace projectif contenant Y au moyen d'une représentation linéaire convenable. On écrit la suite spectrale de Cartan-Leray du revêtement $\mathrm{Y} \to \mathrm{X}$; le terme E_2 est $\mathrm{H}^*(\mathfrak{g}, \mathrm{H}^*(\mathrm{Y}, \mathbf{Z}))$. Les propriétés connues des intersections complètes, et l'hypothèse $r \geqslant 3$ montrent que $\mathrm{H}^1(\mathrm{Y}, \mathbf{Z}) = 0$ et que $\mathrm{H}^2(\mathrm{Y}, \mathbf{Z}) = \mathbf{Z}$, un générateur étant fourni par une section hyperplane de Y. Dans la suite spectrale, on voit que le noyau de $\theta_\mathrm{Y} : \mathrm{H}^3(\mathfrak{g}, \mathbf{Z}) \to \mathrm{H}^3(\mathrm{X}, \mathbf{Z})$ est égal à l'image de $d_3 : \mathrm{H}^2(\mathrm{Y}, \mathbf{Z}) \to \mathrm{H}^3(\mathfrak{g}, \mathbf{Z})$, et on doit montrer que ce dernier homomorphisme est nul, autrement dit que le générateur de $\mathrm{H}^2(\mathrm{Y}, \mathbf{Z})$ provient de $\mathrm{H}^2(\mathrm{X}, \mathbf{Z})$. En fait, on va voir qu'il existe un diviseur D de Y, dont la classe est celle de la section hyperplane, et qui est stable par $\mathfrak{g}$, donc qui provient d'un diviseur de X par image réciproque ; cela démontrera notre assertion. Soit t l'une des coordonnées projectives ; le groupe $\mathfrak{g}$ opère sur ces coordonnées par construction ; on peut donc faire le quotient t^σ/t, $\sigma \in \mathfrak{g}$, qui est une fonction rationnelle sur Y dépendant de σ, soit φ_σ. Il est clair que φ_σ est un 1-cocycle de $\mathfrak{g}$ à valeur dans $k(\mathrm{Y})^*$; d'après le « théorème 90 » (ou bien 4.4 (a) ; c'est la même chose), ce cocycle est un cobord, i.e. s'écrit $\varphi_\sigma = g^\sigma/g$, avec $g \in k(\mathrm{Y})^*$. Le diviseur de tg^{-1} est alors le diviseur cherché.

Bibliographie

[1] I. Barsotti, *Structure theorems for group-varieties*, Ann. Mat. pura ed appl., Série 4, **38** (1955), 77–119.

[2] A. Blanchard, *Sur les variétés analytiques complexes*, Ann. scient. Ec. Norm. Sup., Série 3, **73** (1956), 157–202.

[3] H. Cartan, Séminaire 1956/57, *Topologie.*

[4] H. Cartan et C. Chevalley, Séminaire 1955/56, *Géométrie algébrique.*

[5] P. Cartier, *Calcul différentiel sur les variétés algébriques en caractéristique non nulle*, C.R.A.S. **245** (1957), 1109–1111.

[6] C. Chevalley, *Intersections of algebraic and algebroid varieties*, Trans. Amer. math. Soc. **57** (1945), 1–85.

[7] C. Chevalley, Séminaire 1956-1958, *Classification des groupes de Lie algébriques.*

[8] C. Chevalley, *La notion de correspondance propre en géométrie algébrique*, Séminaire Bourbaki 1957/58, exposé n° 152.

[9] J. Frenkel, *Cohomologie non abélienne et espaces fibrés*, Bull. Soc. math. France **85** (1957), 135–220.

[10] A. Grothendieck, *A general theory of fibre spaces with structure sheaf.* Lawrence, University of Kansas, 1955 (Report n° 4).

[11] A. Grothendieck, *Sur quelques points d'algèbre homologique*, Tôhoku math. J. **9** (1957), 119–221.

[12] A. Grothendieck, *The cohomology theory of abstract algebraic varieties*, Congrès international des Mathématiciens [1958. Edinburgh], 103–118

[13] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. of Math. **80** (1958), 659–684.

[14] M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. of Math. **78** (1956), 401–443.

[15] J-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math. **61** (1955), 197–278 (cité FAC).

[16] J-P. Serre, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier **6** (1956) 1–42 (cité GAGA).

[17] J-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium de Topologie algébrique [1956. Mexico], 24–53.

[18] J-P. Serre, *Groupes Algébriques et Corps de Classes*, Cours au Collège de France 1957. Paris, Hermann, 1959.

[19] A. Weil, *Fibre spaces in algebraic geometry*, Notes rédigées par A. Wallace d'après un cours de 1952. University of Chicago, Dept of Math., 1955 (multigraphié). 19

[20] A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, Hermann, 1948.

[21] A. Weil, *Introduction à l'étude des variétés kählériennes*, Paris, Hermann, 1958.

Séminaire Chevalley
1958-59, exposé n° 10

MORPHISMES UNIVERSELS ET VARIÉTÉS D'ALBANESE

1. Morphismes maximaux

Soit V une variété, et soit $f : V \to A$ un morphisme de V dans un groupe commutatif A. Soit A' le sous-groupe de A engendré par les $f(x) - f(y)$, pour x et y parcourant V ; c'est un sous-groupe *algébrique* (c'est-à-dire fermé) et *irréductible* de A. En effet, notons f^n le morphisme de V^{2n} dans A défini par la formule : 1

$$f^n(x_1, \ldots, x_n; y_1, \ldots, y_n) = f(x_1) + \cdots + f(x_n) - f(y_1) - \cdots - f(y_n) \ ,$$

et soit W_n l'image de V^{2n} par f^n. Les ensembles W_n sont constructibles, irréductibles, et croissent avec n ; il existe donc un entier m tel que l'adhérence $\overline{W}_n$ de W_n soit indépendante de n pour $n \geqslant m$. On a $W_n + W_n = W_{2n}$, ce qui montre que $\overline{W}_m$ est un sous-groupe (évidemment connexe et fermé) de A. Mais W_m étant constructible, contient un ouvert de son adhérence $\overline{W}_m$ et il en résulte aussitôt que $W_m + W_m = \overline{W}_m$, d'où $W_{2m} = \overline{W}_m$, ce qui prouve que $\overline{W}_m$ n'est autre que A'.

Le même raisonnement montre que A' ne change pas lorsqu'on remplace V par un ouvert non vide $U \subset V$, et f par $f|_U$ [autrement dit, A' a un caractère « birationnel »].

Définition 1. — *On dit que le morphisme* $f : V \to A$ *engendre* A *si l'on a* $A' = A$.

Il revient au même de dire que l'image de V par f n'est contenue dans aucun ensemble de la forme $a + B$, $a \in A$, B étant un sous-groupe algébrique de A distinct de A.

Rappelons maintenant qu'un homomorphisme $g : B \to A$ de groupes algébriques (irréductibles, comme toujours dans ce séminaire) est appelé une

isogénie si g est surjectif, et si son noyau est fini. Cette isogénie est dite *séparable* (resp. *radicielle*) si l'extension correspondante $R(B)/R(A)$ est séparable (resp. radicielle).

DÉFINITION 2. — *On dit que le morphisme $f : V \to A$ est maximal (resp. radiciellement maximal) s'il engendre* A*, et si toute factorisation de f sous la forme* :

$$V \xrightarrow{h} B \xrightarrow{g} A ,$$

où h est un morphisme, et où g est une isogénie (resp. une isogénie radicielle), entraîne que g est un isomorphisme.

[En termes plus imagés, on ne peut « relever » f à aucune isogénie non triviale (resp. . . . , etc.)]

Exemples. — 1^0 Si $A = 0$, tout morphisme $f : V \to A$ est maximal.

2^0 Si V est une courbe non singulière, et si $f : V \to J$ est son application canonique dans sa jacobienne, l'application f est maximale.

Remarque. — Dans les définitions 1 et 2, ce n'est pas vraiment la structure de groupe de A qui intervient, mais seulement sa structure « affine », c'est-à-dire sa structure d'espace homogène principal sur lui-même ; il en est de même dans les n^{os} ci-dessous.

2. Factorisation des morphismes d'une variété dans un groupe algébrique commutatif

Si A et B sont deux groupes algébriques commutatifs, nous dirons qu'une application $h : B \to A$ est un *homomorphisme affine* si c'est la composée d'un homomorphisme du groupe algébrique B dans le groupe algébrique A et d'une translation de A. Le noyau de la composante homogène de h est appelé simplement le *noyau* de h. Dire qu'un morphisme $f : V \to A$ est maximal équivaut à dire que toute factorisation de f sous la forme $V \to B \xrightarrow{h} A$ où h est un homomorphisme affine surjectif *à noyau fini* entraîne que h est un isomorphisme (affine, bien entendu).

THÉORÈME 1. — *Soit $f : V \to A$ un morphisme d'une variété* V *dans un groupe algébrique commutatif* A*. On peut factoriser f sous la forme* :

$$V \xrightarrow{g} B \xrightarrow{h} A ,$$

où g est un morphisme maximal, et où h est un homomorphisme affine à noyau fini.

[On peut montrer que cette factorisation est unique, à isomorphisme unique près.]

Soit A' le sous-groupe de A engendré par les $f(x) - f(y)$, $x, y \in V$. Le morphisme f se factorise en $V \xrightarrow{f'} A' \xrightarrow{i} A$ en posant $f'(x) = f(x) - f(x_0)$, $i(a') = a' + f(x_0)$, x_0 étant un point choisi arbitrairement dans V. Quitte à remplacer A par A', on voit donc que l'on peut supposer que $A' = A$, c'est-à-dire que f *engendre* A. Si f est maximale, le théorème est démontré. Sinon, il existe une isogénie non triviale $h_1 : A_1 \to A$ telle que f se factorise en $f = h_1 \circ f_1$ où f_1 est un morphisme de V dans A_1. Il est clair que f_1 engendre A_1 ; si f_1 est maximale, le théorème est démontré (en posant $B = A_1$, $g = f_1$, $h = h_1$). Sinon, il existe une isogénie non triviale $h_2 : A_2 \to A_1$ telle que f_1 se factorise en $f_1 = h_2 \circ f_2$, etc. Tout revient à montrer que cette suite d'opérations ne peut se poursuivre indéfiniment. Supposons que ce soit le cas, et choisissons un entier n assez grand pour que l'application $f^n : V^{2n} \to A$ définie au n° 1 soit dominante. On voit tout de suite qu'il en est alors de même des applications f_i^n, $i = 1, 2, \ldots$ Comme ces applications sont dominantes, leurs cohomomorphismes identifient les corps de fonctions rationnelles $R(A)$, $R(A_1)$, $R(A_2), \ldots$ à des sous-corps de $R(V^{2n})$; on obtient ainsi une suite strictement croissante de sous-corps de $R(V^{2n})$, et la réunion de ces corps n'est pas une extension de type fini de $R(A)$; comme $R(V^{2n})$ est une extension de type fini de $R(A)$, on obtient un résultat en contradiction avec le lemme suivant :

Lemme 1. — Soit M *une extension de type fini d'un corps* E. *Toute sous-extension* F *de* M *est de type fini sur* E. **2**

Soit $(x_1, \ldots, x_s)$ une base de transcendance de F sur E et complétons-la en une base de transcendance $(x_1, \ldots, x_s, y_1, \ldots, y_r)$ de M sur E. Alors F est une extension algébrique de $E(x)$, et, puisque $E(x, y)$ est pure sur $E(x)$, les extensions $F/E(x)$ et $E(x, y)/E(x)$ sont linéairement disjointes. On a donc

$$[F : E(x)] = [F(y) : E(x, y)] \leqslant [M : E(x, y)] .$$

Comme M est de type fini sur $E(x, y)$, on a $[M : E(x, y)] < +\infty$, d'où le même résultat pour $[F : E(x)]$, ce qui montre que F est de type fini sur $E(x)$, donc sur E.

Ceci achève la démonstration du théorème 1.

Soit maintenant $\mathscr{C}$ une catégorie de groupes algébriques commutatifs vérifiant les deux propriétés suivantes :

(I) Si A_1 et A_2 appartiennent à $\mathscr{C}$, on a $A_1 \times A_2 \in \mathscr{C}$.

(II) Si $f : A \to B$ est un homomorphisme à noyau fini, et si $B \in \mathscr{C}$, alors $A \in \mathscr{C}$.
La condition (II) entraîne en particulier qu'un sous-groupe fermé d'un groupe de la catégorie appartient à la catégorie.

DÉFINITION 3. — *Soit $f : V \to A$ un morphisme. On dit que f est universel pour $\mathscr{C}$ si l'on a $A \in \mathscr{C}$, et si, pour tout morphisme $f' : V \to A'$, où $A' \in \mathscr{C}$, il existe un homomorphisme affine $h : A \to A'$ et un seul tel que $f' = h \circ f$.*

[Autrement dit, f résout un problème universel, au sens de [2], chap. V, n° 3.]

Il est clair que, s'il existe un morphisme universel $f : V \to A$ pour la catégorie $\mathscr{C}$, il est unique, à isomorphisme unique près.

THÉORÈME 2. — *Supposons que $\mathscr{C}$ vérifie les axiomes* (I) *et* (II) *ci-dessus. Soit $f : V \to A$ un morphisme, avec $A \in \mathscr{C}$. Pour que f soit universel, il faut et il suffit qu'il soit maximal, et que, pour tout morphisme maximal $f' : V \to A'$, avec $A' \in \mathscr{C}$ on ait* $\dim A' \leqslant \dim A$.

a) Supposons f universel, et supposons que l'on ait factorisé f en

$$V \xrightarrow{k} B \xrightarrow{i} A ,$$

où i a un noyau fini ; on a donc $B \in \mathscr{C}$, et la propriété universelle de f montre qu'il existe un homomorphisme affine $h : A \to B$ tel que $k = h \circ f$. Comme $f = i \circ k$, on en tire $i \circ h \circ f = f$, d'où $i \circ h = 1$ d'après l'unicité postulée dans la définition 3. Il s'ensuit que h est injectif, ce qui montre que A et B ont même dimension ; comme h est surjectif, il est bijectif, et de même pour i, donc i et h sont des isomorphismes réciproques, ce qui montre que f est maximal. Enfin, si $f' : V \to A'$ est maximal, avec $A' \in \mathscr{C}$, il existe $h : A \to A'$ tel que $f' = h \circ f$, et h est nécessairement surjectif, puisque f' engendre A' ; d'où $\dim A' \leqslant \dim A$.

b) Réciproquement, supposons ces propriétés vérifiées, et montrons que f est universel. Soit $f' : V \to A'$ un morphisme, avec $A' \in \mathscr{C}$, et soit $g : V \to A \times A'$ l'application produit des applications f et f'. D'après le théorème 1, on peut factoriser g en

$$V \xrightarrow{k} B \xrightarrow{i} A \times A'$$

où k est maximale, et où i est un homomorphisme à noyau fini. D'après (I) et (II), on a $B \in \mathscr{C}$, d'où $\dim B \leqslant \dim A$. Mais, si l'on note p (resp. p') la projection de $A \times A'$ sur A (resp. A'), on a $p \circ g = f$, d'où $p \circ i \circ k = f$. Comme f engendre A, il s'ensuit que $p \circ i$ est surjectif, et comme $\dim B \leqslant \dim A$, le noyau de $p \circ i$ est fini ; mais f est maximale, donc $p \circ i$ est un isomorphisme. Notons r

l'isomorphisme réciproque, et posons $h = p' \circ i \circ r$; c'est un homomorphisme affine de A dans A′, et l'on a

$$h \circ f = p' \circ i \circ r \circ p \circ i \circ k = p' \circ i \circ k = f' \ .$$

Tout homomorphisme h' tel que $h' \circ f = f'$ coïncide nécessairement avec h, puisque f engendre A, c.q.f.d.

COROLLAIRE. — *Pour qu'il existe un morphisme universel* $f : \mathrm{V} \to \mathrm{A}$ *pour la variété* V *et pour la catégorie* $\mathscr{C}$*, il faut et il suffit que les dimensions des groupes* $\mathrm{A}' \in \mathscr{C}$ *pour lesquels il existe une application maximale* $f' : \mathrm{V} \to \mathrm{A}'$ *soient bornées.*

Caractère fonctoriel des morphismes universels. — Lorsqu'il existe, le morphisme universel $f : \mathrm{V} \to \mathrm{A}$ est un foncteur en V et en $\mathscr{C}$. De façon précise :

a) *Variation avec* V : Soit $\varphi : \mathrm{V} \to \mathrm{V}'$ un morphisme, et supposons que, pour une catégorie $\mathscr{C}$ fixée, les morphismes universels pour $\mathscr{C}$ $f : \mathrm{V} \to \mathrm{A}$ et $f' : \mathrm{V}' \to \mathrm{A}'$ existent. Il existe alors un homomorphisme affine $\varphi_{\mathscr{C}} : \mathrm{A} \to \mathrm{A}'$ et un seul tel que $\varphi_{\mathscr{C}} \circ f = f' \circ \varphi$; cela résulte de la propriété universelle de f.

Supposons en outre que φ soit *dominant.* Alors l'existence de f *entraîne* celle de f' ; en effet, si $g : \mathrm{V} \to \mathrm{A}'$ est un morphisme maximal, on peut factoriser $g \circ \varphi$ en $h \circ f$, où $h : \mathrm{A} \to \mathrm{A}'$ est un homomorphisme affine ; du fait que φ est dominant, le raisonnement du n° 1 montre que h est surjectif et l'on a $\dim \mathrm{A}' \leqslant \dim \mathrm{A}$; on applique alors le corollaire ci-dessus.

Indiquons également, sans démonstration cette fois, deux autres propriétés des morphismes universels :

Variation en fonction d'un paramètre. Soit $f : \mathrm{V} \to \mathrm{A}$ un morphisme universel pour une catégorie $\mathscr{C}$, et soit T une variété. soit $\mathrm{A}' \in \mathscr{C}$ et soit $f' : \mathrm{V} \times \mathrm{T} \to \mathrm{A}'$ un morphisme. Pour chaque $t \in \mathrm{T}$, il existe un homomorphisme affine $h_t : \mathrm{A} \to \mathrm{A}'$ tel que $h_t \circ f(x) = f'(x, t)$ pour $x \in \mathrm{V}$. *L'application* $h : \mathrm{A} \times \mathrm{T} \to a'$ *définie par les* $\{h_t\}_{t \in \mathrm{T}}$ *est un morphisme.*

Produits. Si $f : \mathrm{V} \to \mathrm{A}$ et $f' : \mathrm{V}' \to \mathrm{A}'$ sont des morphismes universels pour une catégorie $\mathscr{C}$, l'application produit

$$f \times f' : \mathrm{V} \times \mathrm{V}' \longrightarrow \mathrm{A} \times \mathrm{A}'$$

est un morphisme universel pour la catégorie $\mathscr{C}$.

b) *Variation avec* $\mathscr{C}$. Soit V une variété, et soient $\mathscr{C}$ et $\mathscr{C}'$ deux catégories vérifiant (I) et (II), et telles que $\mathscr{C} \subset \mathscr{C}'$. Supposons qu'il existe un morphisme universel $f : \mathrm{V} \to \mathrm{A}'$ pour $\mathscr{C}'$. Il existe alors un morphisme universel $f : \mathrm{V} \to \mathrm{A}$

pour $\mathscr{C}$ (cela résulte du corollaire ci-dessus), et un homomorphisme affine unique $h : A' \to A$ tel que $h \circ f' = f$ (d'après la propriété universelle de f'). En outre, le noyau N de h est *connexe*, et h définit par passage au quotient un isomorphisme de A'/N sur A ; en effet, si l'on note N_0 la composante connexe du noyau N de h, l'homomorphisme h définit par passage au quotient un homomorphisme affine $i : A'/N_0 \to A$ à noyau fini ; comme f est maximal, l'homomorphisme i est un isomorphisme, d'où nos deux assertions.

Exemples. — Nous donnerons plus loin une condition nécessaire et suffisante simple pour qu'une variété admette un morphisme universel. Indiquons dès maintenant quelques cas particuliers :

1^0) Si $\mathscr{C}$ est la catégorie des *variétés abéliennes*, il existe des morphismes universels pour toute variété V (cf. n° 4). Il en est de même lorsque $\mathscr{C}$ est la catégorie des extensions d'une variété abélienne par un tore (cf. n° 5).

2^0) Si V est *complète*, il existe des morphismes universels $f : V \to A$ pour toute catégorie $\mathscr{C}$ (cf. n° 4).

3^0) Si V est une courbe *non complète*, et si $\mathscr{C}$ est la catégorie des groupes isomorphes à un produit de groupes additifs $\mathbf{G}_a$, *il n'existe pas* de morphisme universel $f : V \to A$ pour $\mathscr{C}$. Cela se voit, soit en appliquant le théorème 8 du n° 6 (et en remarquant que, d'après le théorème de Riemann-Roch, il existe des fonctions régulières non constantes sur V), soit en appliquant la théorie des jacobiennes généralisées de ROSENLICHT (cf. [7], chap. V).

3. Un critère pour les morphismes radiciellement maximaux

Soit A un groupe algébrique commutatif. Nous noterons t_A l'espace vectoriel des champs de vecteurs invariants sur A ; muni du crochet, c'est une *algèbre de Lie*.

Lemme 2. — *L'algèbre de Lie t_A est commutative* (i.e. $[X, Y] = 0$ pour tout couple X, Y).

C'est « évident », mas on va tout de même en donner une démonstration, basée sur le fait que t_A est fonctoriel et commute aux produits. Puisque A est commutatif, l'application $r : A \times A \to A$ donnée par $r(x, y) = x + y$ est un homomorphisme, donc définit un homomorphisme de l'algèbre de Lie $t_A \times t_A$ dans t_A. On constate aussitôt que cet homomorphisme applique le couple (X, Y) sur $X + Y$. Si X et Y sont deux éléments de t_A, ce sont les images de $(X, 0)$ et de $(0, Y)$. Mais le crochet de $(X, 0)$ et de $(0, Y)$ est nul. Donc $[X, Y] = 0$, c.q.f.d.

Lorsque la caractéristique est $p \neq 0$, t_A est stable par l'opération $X \mapsto X^p$; en vertu du lemme 2 et de la formule du binôme, l'opération $X \mapsto X^p$ est semi-linéaire :

$$(\lambda X + \mu Y)^p = \lambda^p X^p + \mu^p Y^p \ .$$

Nous noterons s_A l'espace dual de t_A ; c'est aussi (voir par exemple [7], chap. III, n° 11) l'espace vectoriel des formes différentielles de degré 1 invariantes sur A.

Lemme 3. — *Pour toute forme invariante $\omega \in s_A$, on a $d\omega = 0$.*

On applique la formule standard :

$$\langle X \wedge Y, d\omega \rangle = X(\langle Y, \omega \rangle) - Y(\langle X, \omega \rangle) - \langle [X, Y], \omega \rangle \ ,$$

en prenant $X, Y \in t_A$. Les termes $\langle Y, \omega \rangle$ et $\langle X, \omega \rangle$ sont des constantes et le lemme 2 montre que $[X, Y] = 0$; on en déduit $\langle X \wedge Y, d\omega \rangle = 0$ pour tout couple X, Y d'où $d\omega = 0$.

Supposons maintenant que la caractéristique du corps de base soit $p \neq 0$. Puisque $d\omega = 0$ pour tout $\omega \in s_A$, l'*opération de Cartier* (cf. exposé 6) est définie pour une telle forme ; si on la note C, on a le lemme suivant :

Lemme 4. — *Pour tout $X \in t_A$ et tout $\omega \in s_A$, $\langle X^p, \omega \rangle = \langle X, C\omega \rangle^p$.*

[En d'autres termes, l'opération C est la *transposée* (au sens des applications semi-linéaires) de l'opération $X \mapsto X^p$.]

Cela résulte de la formule (démontrée dans l'exposé 6) :

$$\langle X^p, \omega \rangle = \langle X, C\omega \rangle^p + X^{p-1}(\langle X, \omega \rangle) \ ,$$

compte tenu de ce que $\langle X, \omega \rangle$ est une constante.

Enfin, si V est une variété quelconque, nous noterons D(V) l'ensemble des formes différentielles de degré 1 (rationnelles) de V, c'est-à-dire le R(V)-espace vectoriel des différentielles de R(V). Pour toute fonction $f : V \to A$, et toute forme $\omega \in s_A$, *l'image réciproque* $f^*\omega$ de ω par f est définie, et c'est un élément de D(V).

THÉORÈME 3. — *Soit* V *une variété, soit* A *un groupe algébrique commutatif, et soit $f : V \to A$ un morphisme. Si $f^* : s_A \to D(V)$ est injectif, f est radiciellement maximal. Inversement, si f est radiciellement maximal, et si* V *est normale, f^* est injectif* (*cf.* [5]).

a) Supposons f factorisé en $V \to B \xrightarrow{i} A$, où i est un homomorphisme affine injectif. Si f^* est injectif, il en est *a fortiori* de même de $i^* : s_A \to s_B$, ce qui entraîne que A et B ont même dimension et que i est un isomorphisme (voir par exemple [5, p. 56]). Donc f est radiciellement maximal.

b) Supposons maintenant que f soit radiciellement maximal. Distinguons deux cas :

b-1) *La caractéristique est* 0. — Choisissons un entier m assez grand pour que le morphisme $f^m : V^{2m} \to A$ du numéro 1 soit dominant, donc définisse une extension de corps $R(V^{2m})/R(A)$. Vu l'hypothèse sur la caractéristique, cette extension est séparable, et si $\omega \in s_A$ est telle que $(f^{2m})^*\omega = 0$, on a nécessairement $\omega = 0$. Mais on peut calculer la forme $(f^{2m})^*\omega$ à partir de la forme $f^*\omega$: si l'on note $p_1, \ldots, p_m, q_1, \ldots, q_m$ les $2m$ projections de V^{2m} sur V, on a la formule :

$$(f^{2m})^*\omega = p_1^* f^*\omega + \cdots + p_m^* f^*\omega - q_1^* f^*\omega - \cdots - q_m^* f^*\omega.$$

(Cette formule se démontre en factorisant f^{2m} en $V^{2m} \to A^{2m} \to A$, et en appliquant à $A^{2m} \to A$ la proposition 17 de [7], *loc. cit.*) Si donc $f^*\omega = 0$, on a aussi $(f^{2m})^*\omega = 0$, d'où $\omega = 0$, et f^* est bien injectif.

b-2) *La caractéristique est* $p \neq 0$. — Soit n^* le noyau de l'application $f^* : s_A \to D(V)$. La formule $Cf^* = f^*C$ montre que n^* est stable par C; en vertu du lemme 4, l'orthogonal n de n^* dans t_A est stable par l'opération de puissance p-ième. La théorie des isogénies radicielles de hauteur 1 (cf. [5], § 2) permet alors de construire une isogénie radicielle

$$h : A \longrightarrow B,$$

qui soit de hauteur 1 (i.e. $R(B) \supset R(A)^p$), et telle que le noyau de $t_A \to t_B$ soit n. L'application $h \circ f : V \to B$ vérifie la formule : $(h \circ f)^*\omega = 0$ pour toute $\omega \in s_B$. En d'autres termes, *l'application tangente à* $h \circ f$ est identiquement nulle (en tout point simple de V, pour fixer les idées). Il en résulte facilement que le morphisme $h \circ f$ peut se factoriser en $V \xrightarrow{g} B^{1/p} \to B$, où g est une
3 *fonction*; comme V est normale, le « théorème principal » montre que g est
4 un morphisme. De plus, comme h est de hauteur 1, l'application $B^{1/p} \to B$ se factorise en $B^{1/p} \to A \to B$. Du fait que f est radiciellement maximal, ceci implique que $B^{1/p} \to A$ est un isomorphisme donc que $B \to A^p$ est un isomorphisme, c'est-à-dire que $n = t_A$, d'où $n^* = 0$, ce qui montre bien que f^* est injectif.

COROLLAIRE. — *Soit* V *une variété normale, et soit* $\Omega(V)$ *l'espace vectoriel des formes différentielles de degré* 1 *sur* V *qui sont régulières en tout point simple de* V. *Si* $f : V \to A$ *engendre* A, *on a* $\dim A \leqslant \dim \Omega(V)$.

D'après le théorème 1, on peut factoriser f en $V \xrightarrow{g} B \to A$, où g est maximal, et où $B \to A$ est une isogénie. Pour toute forme $\omega \in \Omega(B)$, on a $g^*\omega \in \Omega(V)$ puisque g est un morphisme, et ceci vaut notamment pour $\omega \in s_B$. En appliquant le théorème 3 à g, on voit que $\dim s_B \leqslant \dim \Omega(V)$, d'où le corollaire puisque $\dim s_B = \dim B = \dim A$.

Remarques. — 1^0) Dans les énoncés ci-dessus, l'hypothèse de normalité peut être remplacée par l'hypothèse plus faible suivante : pour tout point $P \in V$, on a $\mathscr{O}(P) \cap R(V)^p = \mathscr{O}(P)^p$, en notant $\mathscr{O}(P)$ l'anneau local de P, et p l'exposant caractéristique du corps de base.

2^0) Dire que $f^* : s_A \to D(V)$ est injectif équivaut à dire que, pour tout n assez grand, l'application $f^n : V^{2n} \to A$ est surjective et *séparable* (i.e. son cohomomorphisme définit une extension de corps $R(V^{2n})/R(A)$ qui est séparable). Cela se voit en déterminant l'application tangente à f^n en un point $(P_1, \ldots, P_n, Q_1, \ldots, Q_n)$ de V^{2n}.

4. La variété d'Albanese

Nous utiliserons le lemme suivant :

Lemme 5. — *Soit* V *une variété complète, soit* F *un sous-ensemble fermé de* V*, et soit* $X = V - F$. *Supposons que* X *soit non singulier et que* $\dim F \leqslant \dim V - 2$. *Si* Ω_X *désigne le faisceau des germes de formes différentielles régulières de degré* 1 *sur* X*, l'espace vectoriel* $H^0(X, \Omega_X)$ *est de dimension finie.*

En effet, Ω_X est un faisceau cohérent localement libre, donc sans torsion, et l'on applique un résultat général sur les faisceaux cohérents sans torsion (Annexe I, corollaire au th. 9).

On notera que l'espace $H^0(X, \Omega_X)$ n'est autre que l'espace $\Omega(X)$ des différentielles régulières en tout point de X.

THÉORÈME 4. — *Soit* V *une variété. Supposons qu'il existe une variété complète* W *et un sous-ensemble fermé* F *de* W*, avec* $\dim F \leqslant \dim W - 2$*, tels que* V *soit isomorphe à* $W - F$. *Alors, pour toute catégorie* $\mathscr{C}$*, il existe un morphisme universel* $f : V \to A$ *pour* $\mathscr{C}$.

Identifions V à $W - F$. Soit W^* la normalisée de W; c'est une variété complète. Soit F' l'ensemble des points singuliers de W^*; soit F'' l'image réciproque de F par la projection $W^* \to W$, et soit $F^* = F' \cup F''$. On a $\dim F^* \leqslant \dim W^* - 2$, et le lemme 5, appliqué à W^* et F^*, montre que l'espace

$\Omega(W^* - F^*)$ est de dimension finie. Le corollaire au th. 3, joint au corollaire au th. 2, montre alors qu'il existe un morphisme universel

$$f^* : W^* - F^* \longrightarrow A^*$$

pour la catégorie $\mathscr{C}$. Mais la projection $W^* \to W$ induit par restriction un morphisme $\varphi : W^* - F^* \to V = W - F$, et ce morphisme est évidemment dominant. D'après le caractère fonctoriel des morphismes universels (cf. n° 2), il existe donc aussi un morphisme universel $f : V \to A$, c.q.f.d.

Remarque. — Les hypothèses étant celles du théorème 4, soit $f : V \to A$ un morphisme qui engendre A; il est vraisemblable que A est alors nécessairement une *variété abélienne*. C'est en tout cas vrai si V est *complète* (car A est image de V^{2n} pour n assez grand), ou bien si W est *projective* (en effet, on se ramène tout de suite au cas où A ne contient aucune variété abélienne; si C est une courbe sur W qui ne rencontre pas F, la restriction de f à C est constante, d'après ce qui précède; en utilisant le fait que W est projective, et $\dim F \leqslant \dim W - 2$ on montre alors qu'il y a « suffisamment » de telles courbes pour que la propriété précédente entraîne que f soit constante).

THÉORÈME 5. — *Soit $\mathscr{A}$ la catégorie des variétés abéliennes. Pour toute variété* V*, il existe un morphisme $f : V \to A$ universel pour $\mathscr{A}$.*

Soit V_1 un ouvert affine non singulier de V; puisque V_1 est affine, on peut le plonger comme ouvert dans une variété projective V_2; quitte à normaliser V_2, on peut supposer que V_2 est normale. Soit F l'ensemble des points singuliers de V_2, et soit $V_3 = V_2 - F$. La variété V_3 possède un morphisme universel $f : V_3 \to A$, d'après le théorème 4. D'autre part, d'après une propriété fondamentale des variétés abéliennes (voir exposé 9), toute fonction de V_2 dans une variété abélienne est un morphisme sur V_3; donc les morphismes de V_1 et V_3 dans les variétés abéliennes coïncident. Il s'ensuit que la restriction de f à V_1 est un morphisme universel pour $\mathscr{A}$. Comme l'injection de V_1 dans V est un morphisme dominant, l'argument fonctoriel utilisé plus haut montre l'existence d'un morphisme universel de V pour $\mathscr{A}$, c.q.f.d.

La variété abélienne A ainsi associée à V est appelée la *variété d'Albanese* (au sens morphique) de V, et f est l'application canonique de V dans sa variété d'Albanese. Comme on l'a vu plus haut, la variété d'Albanese est un *foncteur* en V, compatible avec les produits; ce dernier résultat est ici immédiat, puisqu'on sait que tout morphisme d'un produit $V \times V'$ dans une variété abélienne A est somme d'un morphisme de V dans A et d'un morphisme de V' dans A (cf. exposé 9).

Il faut signaler que, dans la littérature (cf. [3], par exemple), la variété d'Albanese est définie par une propriété universelle portant sur les *fonctions* (rationnelles) et non sur les *morphismes*. Le théorème suivant indique les relations entre ces deux définitions :

THÉORÈME 6. — *Soit* V *une variété. Soit* $f_r : V \to A_r$ *la fonction canonique de* V *à valeurs dans sa variété d'Albanese* (au sens fonctions). *Soit* $f : V \to A$ *le morphisme canonique de* V *dans sa variété d'Albanese* (au sens du texte, c'est-à-dire des morphismes) .

(i) *Il existe alors un homomorphisme affine* $g : A_r \to A$ *et un seul tel que* $g \circ f_r = f$. *Cet homomorphisme est surjectif.*

(ii) *Si* V *est normale, le noyau* N *de* g *est connexe, et* g *définit par passage au quotient un isomorphisme de* A_r/N *sur* A.

(iii) *Si* V *est non singulière,* g *est un isomorphisme.*

Comme tout morphisme est une fonction, l'assertion (i) résulte du caractère universel de f_r et du fait que f engendre A. Supposons maintenant V normale, et soit N_0 la composante connexe du noyau N de g. En composant $V \to A_r \to A_r/N_0$ on obtient une fonction $f_0 : V \to A_r/N_0$; mais le composé $V \to A_r/N_0 \to A$ est un morphisme, et l'homomorphisme $A_r/N_0 \to A$ a un noyau fini. En appliquant le « théorème principal », on voit que f_0 est un morphisme, et comme f est maximal, l'homomorphisme $A_r/N_0 \to A$ est un isomorphisme, ce qui démontre (ii). Enfin, si V est non singulière, toute fonction de V dans une variété abélienne est un morphisme, d'où évidemment (iii).

Exemples. — i) Soit C une courbe elliptique, en caractéristique p, et soit $P \in C$. Soit $\mathscr{O}'(P)$ le sous-anneau de l'anneau local $\mathscr{O}(P)$ formé des fonctions dont la différentielle s'annule en P ; soit C' la courbe dont les anneaux locaux sont les mêmes que ceux de C, sauf en P où $\mathscr{O}(P)$ est remplacé par $\mathscr{O}'(P)$ (C' a un « point de rebroussement ordinaire » en P, cf. [7], p. 70). Si l'on note C^p la puissance p-ième de C, on a des morphismes $C \to C' \to C^p$, et on vérifie facilement que C^p (resp. C) est la variété d'Albanese au sens morphique (resp. au sens des fonctions) de C'. L'hypothèse de normalité est donc essentielle dans la partie (ii) du théorème.

ii) Soit encore C une courbe elliptique plongée sans singularités dans le plan $\mathbf{P}_2$ et soit E le cône correspondant ; c'est une variété normale. On voit facilement que C est la variété d'Albanese (au sens des fonctions) de E, alors que la variété d'Albanese morphique est réduite à 0. L'hypothèse de non singularité est donc essentielle dans la partie (iii) du théorème.

Remarque. — Comme toute variété est birationnellement équivalente à une variété non singulière (enlever les points singuliers !), le théorème 6 montre

que la variété d'Albanese au sens des fonctions est un cas particulier de la variété d'Albanese morphique.

5. Existence de morphismes universels. Premier cas

THÉORÈME 7. — *Soit $\mathscr{C}$ une catégorie* (vérifiant, comme toujours, les conditions (I) et (II) du n° 2). *Supposons que $\mathscr{C}$ ne contienne pas le groupe additif $\mathbf{G}_a$. Toute variété* V *possède alors un morphisme universel pour $\mathscr{C}$.*

Vu les théorèmes de structure pour les groupes algébriques (cf. [7], p. 50), le fait pour un groupe algébrique commutatif de ne contenir aucun sous-groupe isomorphe à $\mathbf{G}_a$ équivaut au fait d'être extension d'une variété abélienne par un tore (c'est-à-dire un produit de groupes multiplicatifs $\mathbf{G}_m$). Si l'on note $\mathscr{S}$ la catégorie formée par ces extensions, l'hypothèse faite sur $\mathscr{C}$ signifie donc que $\mathscr{C} \subset \mathscr{S}$, et l'on est ramené à démontrer l'existence de morphismes universels pour $\mathscr{S}$.

Soit donc V une variété, et soit V_1 un ouvert affine non singulier de V ; plongeons V_1 comme ouvert d'une variété projective normale V_2, et soit F l'ensemble des points singuliers de V_2 ; soit $V_3 = V_2 - F$ et soit $\Delta = V_3 - V_1$. Les composantes irréductibles $\Delta_1, \ldots, \Delta_k$ de Δ sont *toutes de codimension* 1 ; en effet, Δ est l'ensemble des points où la fonction $V_3 \to V_1$ n'est pas définie, et puisque V_3 est normale et V_1 affine, on sait que toutes les composantes d'un tel ensemble sont de codimension 1.

Lemme 6. — Soit $f : V_1 \to G$ un morphisme de V_1 dans un groupe $G \in \mathscr{S}$ et soit $\omega \in s_G$. Alors la forme différentielle $f^*\omega$, considérée comme une forme différentielle sur V_3, est régulière sur V_1, et a au plus des pôles simples sur les Δ_i.

Admettons pour un moment ce lemme, et achevons la démonstration du théorème 7. Soit D le diviseur sur V_3 somme des diviseurs irréductibles Δ_i, et soit L(D) le faisceau des germes de fonctions rationnelles φ vérifiant localement $(\varphi) \geqslant -D$. Il est bien connu que ce faisceau est un faisceau localement libre de rang 1 (il est isomorphe au faisceau des sections de l'espace fibré vectoriel associé à D) ; si l'on note Ω le faisceau des germes de formes différentielles régulières de degré 1 sur V_3, le lemme 6 signifie que $f^*\omega \in H^0(V_3, L(D) \otimes \Omega)$. Mais $V_3 = V_2 - F$, avec $\dim F \leqslant \dim V_2 - 2$, et le résultat démontré dans l'Annexe I (corollaire au th. 9) montre que $H^0(V_3, L(D) \otimes \Omega)$ est un espace vectoriel de dimension finie, soit N. D'après le th. 3, on a donc $\dim G \leqslant N$, et d'après le corollaire au th. 2, la variété V_1 admet un morphisme universel pour $\mathscr{S}$. Puisque $V_1 \to V$ est dominant, il en est de même de V, c.q.f.d.

Démonstration du lemme 6. — D'après le théorème de structure rappelé plus haut, le groupe G contient un sous-groupe T isomorphe à un produit $(\mathbf{G}_m)^n$ de groupes multiplicatifs, le quotient $A = G/T$ étant une variété abélienne ; nous désignerons par $\pi : G \to A$ la projection canonique de G sur A. Puisque V_3 est non singulière, le morphisme $\pi \circ f$ de V_1 dans A se prolonge en un morphisme $G : V_3 \to A$.

Soit $P \in V_3$, et soit $Q = g(P) \in A$. On sait (cf. par exemple [7], p. 170, prop. 6) que les translations par les éléments de T munissent G d'une structure d'espace fibré principal *localement trivial* de base A. Il existe donc un voisinage U de Q au-dessus duquel existe une section $s : U \to G$; cette section permet d'identifier l'espace fibré $\pi^{-1}(U)$ au produit $U \times T$. Notons ω_U la restriction de ω à $\pi^{-1}U$; c'est une forme fermée partout régulière, et invariante par les translations définies par les éléments de T. Si l'on note $(x_1, \ldots, x_n)$ les coordonnées naturelles dans $(\mathbf{G}_m)^n$, on voit aisément qu'une telle forme peut s'écrire d'une façon unique comme une somme :

$$\omega_U = \pi^*\alpha_U + c_1 dx_1/x_1 + \cdots + c_n dx_n/x_n \ ,$$

où les c_i sont des constantes, et où α_U est une forme différentielle régulière sur U (cette écriture dépend évidemment de la section s choisie : on a $\alpha_U = s^*\omega_U$ — par contre les coefficients c_i ne dépendent pas du choix de s).

Soit $U' = g^{-1}(U)$; c'est un voisinage de P dans V_3. La restriction de $f^*\omega$ à U' est donné par la formule :

$$(*) \qquad \begin{aligned} f^*\omega|U' &= f^*\pi^*\alpha_U + c_1 d\varphi_1/\varphi_1 + \cdots + c_n d\varphi_n/\varphi_n \\ &= g^*\alpha_U + c_1 d\varphi_1/\varphi_1 + \cdots + c_n d\varphi_n/\varphi_n \ , \end{aligned}$$

où les φ_i désignent les fonctions rationnelles $x_i \circ f$ (en dépit de la notation, ces fonctions dépendent du choix de s).

Comme g est un morphisme, la formule $(*)$ montre que la forme $f^*\omega$ peut s'écrire, au voisinage de tout point, comme la somme d'une différentielle régulière et de n « différentielles logarithmiques ». Or, il est clair qu'une différentielle logarithmique n'a que des pôles d'ordre 1; d'autre part, on sait que $f^*\omega$ n'a pas de pôle sur V_1, puisque f est un morphisme sur V_1 ; le lemme 6 est donc démontré.

Remarques. — 1^0) Le théorème 7 contient le théorème 5 (existence de la variété d'Albanese) comme cas particulier.

2^0) Avec les notations de la démonstration faite ci-dessus, soit $f : V_1 \to G$ un morphisme universel pour $\mathscr{S}$; soit T le plus grand tore contenu dans G, et soit $A = G/T$ la variété abélienne quotient. On voit facilement que $V_1 \to G \to A$ n'est autre que l'application canonique de V_1 dans sa variété

d'Albanese ; pour déterminer G il faut donc déterminer une certaine extension de A par un tore ; dans certain cas, ceci peut se faire explicitement, comme nous le verrons dans l'exposé suivant.

6. Existence de morphismes universels. Second cas

THÉORÈME 8. — *Soit $\mathscr{C}$ une catégorie* (vérifiant, comme toujours, les conditions (I) et (II) du n° 2). *Supposons que $\mathscr{C}$ contienne le groupe additif $\mathbf{G}_a$, et soit* V *une variété. Les deux conditions suivantes sont équivalentes* :

(i) *La variété* V *possède un morphisme universel pour $\mathscr{C}$.*

(ii) *Toute fonction numérique régulière sur* V *est constante.*

Montrons que (i) ⇒ (ii). Une fonction numérique régulière sur V n'est pas autre chose qu'un morphisme de V dans le groupe additif $\mathbf{G}_a$. Supposons donc qu'il existe un morphisme non constant $f : \mathrm{V} \to \mathbf{G}_a$; ce morphisme engendre $\mathbf{G}_a$. Considérons le morphisme

$$\varphi : \mathbf{G}_a \longrightarrow \mathbf{G}_a \times \mathbf{G}_a$$

défini en caractéristique $\neq 2$ par $\varphi(t) = (t, t^2)$, et en caractéristique 2 par $\varphi(t) = (t, t^3)$. On voit tout de suite que φ engendre $(\mathbf{G}_a)^2$. Le morphisme $\varphi \circ f : \mathrm{V} \to (\mathbf{G}_a)^2$ engendre donc le groupe $(\mathbf{G}_a)^2$. Mais le morphisme $\varphi \times \varphi : (\mathbf{G}_a)^2 \to (\mathbf{G}_a)^4$ engendre $(\mathbf{G}_a)^4$; il en est donc de même de $(\varphi \times \varphi) \circ \varphi \circ f : \mathrm{V} \to (\mathbf{G}_a)^4$, et l'on peut continuer indéfiniment ; on obtient pour tout entier k un morphisme $f_k : \mathrm{V} \to (\mathbf{G}_a)^{2^k}$ qui engendre $(\mathbf{G}_a)^{2^k}$, et comme ce groupe appartient à $\mathscr{C}$, il est clair que V ne possède pas de morphisme universel pour $\mathscr{C}$.

Montrons que (ii) ⇒ (i). Soit $f : \mathrm{V} \to \mathrm{G}$ un morphisme qui engendre G. D'après les théorèmes de structure déjà cités, G contient un sous-groupe connexe linéaire R tel que le quotient G/R = A soit une variété abélienne ; de plus, R = T × U, où T est un tore et U un groupe unipotent. Le groupe G/U est extension de A par R, donc appartient à la catégorie $\mathscr{S}$ considérée au numéro précédent ; vu le théorème 7, la dimension de G/U est bornée, et tout revient donc à montrer que la dimension de U est bornée si V vérifie (ii). Distinguons deux cas :

a) *Si la caractéristique est $p \neq 0$, on a* U = 0. En effet, le groupe G/pG, étant annulé par p, est un groupe unipotent, donc est une variété affine. Vu la condition (ii), le morphisme V → G → G/pG est constant ; mais d'autre part, ce morphisme engendre G/pG ; donc G/pG = 0. La multiplication par p a donc un noyau fini dans G, donc aussi dans U, et ceci entraîne U = 0 (car sinon U contiendrait un sous-groupe isomorphe à $\mathbf{G}_a$).

b) *Si la caractéristique est* 0*, on a* $\dim \mathrm{U} \leqslant \dim \mathrm{A}$. En effet, le groupe U est alors isomorphe à $(\mathbf{G}_a)^n$. Soit $\mathrm{E} = \mathrm{G}/\mathrm{T}$; c'est une extension de A par U; elle est donc définie par n éléments $x_1, \ldots, x_n$ de $\mathrm{Ext}(\mathrm{A}, \mathbf{G}_a)$ (cf. [7], chap. VII). Soit $g = \dim \mathrm{A}$; on sait (*loc. cit.*, th. 10) que $\mathrm{Ext}(\mathrm{A}, \mathbf{G}_a)$ est un espace vectoriel de dimension g sur le corps de base. Si l'on avait $n > g$, il existerait des constantes c_i, non toutes nulles, telles que $\sum c_i x_i = 0$. Les c_i définissent un homomorphisme $c : (\mathbf{G}_a)^n \to \mathbf{G}_a$ non trivial ; soit E_c l'extension de A par $\mathbf{G}_a$ déduite de G au moyen de c (*loc. cit.*, § 1). On a un homomorphisme surjectif $\mathrm{E} \to \mathrm{E}_c$; d'autre part, la relation $\sum c_i x_i = 0$ signifie que E_c est une extension triviale de A par $\mathbf{G}_a$, d'où l'existence d'un homomorphisme non trivial $\mathrm{E}_c \to \mathbf{G}_a$. En composant

$$\mathrm{V} \longrightarrow \mathrm{E} \longrightarrow \mathrm{E}_c \longrightarrow \mathbf{G}_a \ ,$$

on obtient un morphisme non constant de V dans $\mathbf{G}_a$, ce qui contredit (ii). On a donc bien $n \leqslant g$, ce qui achève la démonstration.

Remarque. — Si V est de la forme $\mathrm{W} - \mathrm{F}$, avec W complète, et $\dim \mathrm{F} \leqslant \dim \mathrm{W} - 2$, on voit facilement (cf. Annexe I) que toute fonction régulière sur V est constante. Le théorème 8 contient donc le théorème 4 comme cas particulier.

Exemples. — Soit G un groupe vérifiant la condition (ii) du théorème 8. *L'application identique* $i : \mathrm{G} \to \mathrm{G}$ *est alors un morphisme universel*, autrement dit tout morphisme $f : \mathrm{G} \to \mathrm{H}$ de G dans un groupe algébrique (l'hypothèse de commutativité est même superflue) est un homomorphisme affine. On peut en effet supposer que $f(0) = 0$, et en formant $f(x + y) - f(x) - f(y)$, on obtient un morphisme de $\mathrm{G} \times \mathrm{G}$ dans H qui est nul sur $\mathrm{G} \times 0$ et $0 \times \mathrm{G}$. Soit R le plus grand sous-groupe linéaire de H, et soit $\mathrm{A} = \mathrm{H}/\mathrm{R}$ la variété abélienne quotient. On sait (exposé 9) que le composé $\mathrm{G} \times \mathrm{G} \to \mathrm{H} \to \mathrm{A}$ est nul. Le morphisme $\mathrm{G} \times \mathrm{G} \to \mathrm{H}$ applique donc $\mathrm{G} \times \mathrm{G}$ dans R et il est constant et égal à 0 d'après (ii), c.q.f.d.

On peut former un tel groupe G en prenant une extension non triviale d'une courbe elliptique A par le groupe $\mathbf{G}_a$ (en caractéristique zéro), ou bien une extension de A par $\mathbf{G}_m$ correspondant à un point de A qui ne soit pas d'ordre fini (en toute caractéristique). On montre que le groupe G ainsi obtenu *n'est pas* de la forme $\mathrm{W} - \mathrm{F}$, avec W complète et $\dim \mathrm{F} \leqslant \dim \mathrm{W} - 2$ (le théorème 8 est donc « plus fort » que le théorème 4).

Annexe I

Prolongement de certains faisceaux algébriques cohérents

On se propose de démontrer le résultat suivant :

THÉORÈME 9. — *Soit* Y *une variété, soit* F *un sous-ensemble fermé de* Y*, et soit* $X = Y - F$*. Supposons que* $\dim F \leqslant \dim Y - 2$*. Soit d'autre part* M *un faisceau algébrique cohérent sans torsion sur* X*, et soit* M^* *son image directe par l'injection* $i : X \to Y$ (cf. exposé 3, § 2)*. Le faisceau* M^* *est alors un faisceau algébrique cohérent sur* Y*.*

Avant de donner la démonstration, indiquons une conséquence du théorème précédent (cf. [4]) ;

COROLLAIRE. — *Les hypothèses étant celles du théorème* 9*, si l'on suppose en outre que* Y *est une variété complète, alors* $H^0(X, M)$ *est un espace vectoriel de dimension finie sur le corps de base.*

En effet, on a $H^0(X, M)) = H^0(Y, i_*M)$ d'après la définition de l'image directe, et le faisceau $i_*M = M^*$ est cohérent ; d'après un résultat connu (cf. exposé 4, corollaire au théorème de dévissage), l'espace vectoriel $H^0(Y, M^*)$ est de dimension finie, c.q.f.d.

[Le corollaire ci-dessus ne s'étend pas aux $H^q(X, M)$, $q \geqslant 1$. Contre-exemple : $Y = \mathbf{P}_2$ (plan projectif), F réduit à un point, M = faisceau des anneaux locaux.]

On utilisera le lemme suivant :

Lemme 7. — Soit V *une variété affine d'anneau de coordonnées* A*, et soit* f *une fonction numérique sur* V*. On suppose que* $f \in A_{\mathfrak{p}}$ *pour tout idéal premier* $\mathfrak{p}$ *de hauteur* 1 *de* A (« de hauteur 1 » = « minimal parmi les idéaux premiers $\neq 0$ »)*. Alors* f *est entière sur* A*.*

Soit A' la clôture intégrale de A dans son corps des fractions R(V). Si $\mathfrak{q}$ est un idéal premier de hauteur 1 dans A', l'idéal premier $\mathfrak{p} = \mathfrak{q} \cap A$ est de hauteur 1 dans A ; en effet, si l'on pose $n = \dim V$, on sait que $\dim A'/\mathfrak{q} = n-1$, et comme $A'/\mathfrak{q}$ est entier sur $A/\mathfrak{p}$, cela donne $\dim A/\mathfrak{p} = \dim A'/\mathfrak{q} = n - 1$, et la hauteur de $\mathfrak{p}$ est bien égale à 1. Comme $f \in A_{\mathfrak{p}}$, on a *a fortiori* $f \in A'_{\mathfrak{q}}$. Mais on sait que $A' = \cap A'_{\mathfrak{q}}$ lorsque $\mathfrak{q}$ parcourt les idéaux premiers de hauteur 1 de A' (car A' est noethérien et intégralement clos). On a donc bien $f \in A'$.

Démonstration du théorème 9. — La question étant locale on peut supposer que Y est une variété affine. Soit N un faisceau cohérent sur Y dont la restriction à X coïncide avec M ; un tel faisceau existe d'après [1], prop. 2 ; quitte à diviser N par son faisceau de torsion, on peut supposer que N est sans torsion.

Le module sur l'anneau de coordonnées A de Y correspondant à N est donc sans torsion; il est isomorphe à un sous-module d'un module libre A^n. Cela revient à dire que M est isomorphe à un sous-faisceau de $\mathscr{O}^n$, où $\mathscr{O}$ désigne le faisceau des anneaux locaux. Le faisceau i_*M est donc un sous-faisceau du faisceau $(i_*\mathscr{O})^n$; comme on sait déjà que i_*M est quasi-cohérent (cf. 3-04), pour voir que c'est un faisceau cohérent, il suffit de montrer que $i_*\mathscr{O}$ est cohérent, ou encore que $H^0(Y, i_*\mathscr{O})$ est un A-module de type fini. Mais on a $H^0(Y, i_*\mathscr{O}) = H^0(X, \mathscr{O})$; c'est donc l'ensemble des fonctions f sur Y qui sont régulières en tout point de X. Comme $\dim F \leqslant \dim V - 2$, une telle fonction appartient à l'anneau local $A_\mathfrak{p}$ de toute sous-variété irréductible de Y de codimension 1 ; d'après le lemme 7, cela entraîne que $H^0(X, \mathscr{O})$ est contenu dans la clôture intégrale A′ de A dans son corps des fractions. Comme cette clôture intégrale est un A-module de type fini, ceci achève la démonstration.

Remarque. — Si Y est complète et si $\dim F \leqslant \dim Y - 2$, le corollaire ci-dessus montre que l'algèbre des fonctions régulières sur $X = Y - F$ est de dimension finie. Comme cette algèbre n'a pas de diviseurs de zéro et que le corps de base est algébriquement clos, elle est réduite aux scalaires. On retrouve donc le fait que toute fonction régulière sur X est constante.

Annexe II

Morphismes maximaux et homologie ℓ-adique

Nous commencerons par « rappeler » la définition du groupe d'homologie ℓ-adique *de dimension* 1 d'une variété V (ℓ étant un nombre premier différent de la caractéristique) :

Considérons tous les revêtements connexes non ramifiés $W \to V$ qui sont galoisiens (cf. [6]), et dont le groupe de Galois $G(W/V)$ est un *ℓ-groupe commutatif.* Ces revêtements forment de façon naturelle un ensemble filtrant, et la limite projective $H_1(V; \ell)$ des groupes $G(W/V)$ suivant cet ensemble est le groupe d'homologie que nous voulions définir. C'est un ℓ-groupe compact totalement discontinu commutatif et comme tel c'est un $\mathbf{Z}_\ell$-module, $\mathbf{Z}_\ell$ désignant l'anneau des entiers ℓ-adiques. C'est un foncteur covariant en V. Il est *vraisemblable* qu'il jouit des propriétés suivantes : 5

(i) $H_1(V; \ell)$ *est un $\mathbf{Z}_\ell$-module de type fini.*

(ii) *Pour* V *fixée, le rang de* $H_1(V;\ell)$ *ne dépend pas de* ℓ ; *pour presque tout* ℓ, $H_1(V;\ell)$ *est un* $\mathbf{Z}_\ell$*-module libre.*

(iii) *Si* $f : V \to V'$ *est un morphisme, le rang de l'homomorphisme*

$$f_{*;\ell} : H_1(V;\ell) \longrightarrow H_1(V';\ell)$$

ne dépend pas de ℓ; *pour presque tout* ℓ, *le conoyau de* $f_{*;\ell}$ *est* $\mathbf{Z}_\ell$*-libre.*

(iv) *On a* $H_1(V \times V';\ell) = H_1(V;\ell) \times H_1(V';\ell)$.

[Lorsque le corps de base est $\mathbf{C}$, et que V est normale, GRAUERT et REMMERT ont montré que $H_1(V;\ell)$ est le complété ℓ-adique du groupe d'homologie usuel
6 $H_1(V,\mathbf{Z})$; GROTHENDIECK aurait réussi à supprimer l'hypothèse de normalité, ce qui démontrerait (i), ..., (iv) dans ce cas. En caractéristique $p \neq 0$, on a des résultats partiels ; par exemple, on peut démontrer (i) si V est normale et (ii) si V est projective non singulière (appliquer le théorème de Néron-Severi), ainsi que (iv) si V est complète (LANG-SERRE dans le cas normal, GROTHENDIECK dans le cas général).]

Soit maintenant G un groupe algébrique commutatif. L'application $x \mapsto \ell^n \cdot x$ fait de G un revêtement non ramifié de lui-même, dont le groupe de Galois $G(\ell^n)$ est le sous-groupe formé par les x tels que $\ell^n \cdot x = 0$. Si l'on note $T_\ell(G)$ la limite projective des groupes $G(\ell^n)$, on a donc un homomorphisme canonique :

$$\varepsilon : H_1(G;\ell) \longrightarrow T_\ell(G)\,.$$

7 Il est *vraisemblable* que ε est un isomorphisme [ce serait en tout cas une conséquence de (iv)]; c'est vrai si G est une variété abélienne.

Soit maintenant $f : V \to G$ un morphisme de la variété V dans le groupe G ; en composant $f_{*,\ell}$ et ε on obtient pour tout ℓ un homomorphisme : $H_1(V;\ell) \to T_\ell(G)$.

THÉORÈME 10. — *Si* $f : V \to G$ *est maximal, l'homomorphisme*

$$H_1(V;\ell) \longrightarrow T_\ell(G).$$

est surjectif pour tout ℓ.

Soit I l'image de cet homomorphisme. Si l'on avait $I \neq T_\ell(G)$, il existerait un sous-groupe I' fermé, contenant I, et d'indice ℓ dans $T_\ell(G)$. Ce sous-groupe I' correspondrait à une isogénie $g : A' \to A$ séparable, et de noyau cyclique d'ordre ℓ. Le fait que I' contient I signifie que l'image réciproque par f de A', considéré comme revêtement de A, est un revêtement *trivial* de V; en d'autres termes, on peut factoriser f en $g \circ h$, où $h : V \to A'$ est un morphisme ; c'est contraire au caractère maximal de f.

Remarque. — Soit t la dimension du plus grand tore contenu dans G, et soit g la dimension de la plus grande variété abélienne quotient de G. D'après un résultat de WEIL, $T_\ell(G)$ est un $\mathbf{Z}_\ell$-module libre de rang $2g+t$. On a donc $2g+t \leqslant \text{rang } (H_1(V;\ell))$, et cette majoration fournit une autre démonstration du théorème 7 (*à condition d'admettre la conjecture* (i)).

Soit maintenant $\mathscr{S}$ la catégorie des extensions d'une variété abélienne par un tore, et soit $f : V \to G$ un morphisme universel pour cette catégorie. D'après le théorème 10, l'homomorphisme

$$H_1(V;\ell) \longrightarrow T_l(G).$$

est surjectif pour tout ℓ. *Dans quel cas son noyau est-il fini*? C'est vrai si V est projective non singulière (d'après NÉRON-SEVERI), ou si V est une courbe non singulière (cf. [7], chapitre VI) ; c'est faux si V est une courbe avant un point double à tangentes distinctes; peut-être est-ce toujours vrai si V est *normale*?

Dans le cas complexe, la question précédente se reformule ainsi : *Dans quel cas l'homomorphisme* $H_1(V,\mathbf{Z}) \to H_1(G;\mathbf{Z})$, *qui est toujours surjectif, a-t-il un noyau fini*? C'est vrai lorsque V est projective non singulière, soit d'après la théorie kählérienne, soit d'après ce qui a été dit plus haut. La question est en relation avec la suivante : dans quel cas l'image réciproque des formes différentielles invariantes de G donne-t-elle toutes les formes différentielles régulières sur V (supposée complète)? Ici encore la théorie kählérienne donne une réponse affirmative lorsque V est projective non singulière ; il serait intéressant d'aller plus loin

Annexe III

La réduction au cas des courbes

L'existence de la variété d'Albanese d'une courbe résulte tout de suite (par normalisation) des propriétés de la jacobienne. Le cas d'une variété de dimension quelconque se ramène à celui des courbes par le procédé suivant :

Soit V une variété projective de dimension n plongée dans un espace projectif $\mathbf{P}_{n+r}$; soit F l'ensemble des points singuliers de V; *on suppose* que $\dim F \leqslant \dim V - 2$ (cf. n° 4).

THÉORÈME 11. — *Soit* $f : V \to G$ *un morphisme qui engendre le groupe* G. *Soit* L *une sous-variété linéaire de* $\mathbf{P}_{n+r}$ *de dimension* $\geqslant r+1$ *et supposons que* $L \cap F = \varnothing$. *La restriction de* f *à* $V \cap L$ *engendre alors* G.

Indiquons brièvement la démonstration. Soit H le sous-groupe de G engendré par $L \cap V$; quitte à remplacer G par G/H, on peut supposer que $H = 0$, c'est-à-dire que la restriction de f à $V \cap L$ applique $V \cap L$ en un seul point $e \in G$. Soit U un voisinage affine de l'élément neutre de G. On voit aisément que, pour toute sous-variété linéaire L' de $\mathbf{P}_{n+r}$ de même dimension que L, et assez voisine de L, f applique $L' \cap V$ dans U; mais $L' \cap V$ est connexe (théorème de connexion), et complète ; comme U est affine, on en conclut que la restriction de f à $V \cap L'$ est constante. Soit $Q \in V \cap L$; si l'on se borne aux L' qui passent par Q, on montre aisément que la réunion des $V \cap L'$ correspondant est un voisinage de Q. Il s'ensuit que f est constante sur ce voisinage, donc partout, c.q.f.d.

Noter que l'on peut choisir L de telle sorte que $V \cap L$ soit une courbe (et même, si l'on y tient, une courbe irréductible et non singulière) ; le théorème 11 montre alors que $\dim G$ est borné par le genre de cette courbe, et cette majoration démontre l'existence d'un morphisme universel pour $V - F$. C'est la méthode de MATSUSAKA et CHOW, (cf. [3], Chap. II), à cela près que ces auteurs se servaient d'une courbe « générique » et obtenaient donc un résultat un peu moins précis.

Bibliographie

[1] A. BOREL et J-P. SERRE, *Le théorème de Riemann-Roch* (*d'après des résultats inédits de A. Grothendieck*), Bull. Soc. math. France **86** (1958), 97–136.

[2] N. BOURBAKI, *Théorie des Ensembles*, chap. 4 : Structures, Paris, Hermann, 1957.

[3] S. LANG, *Abelian Varieties*, New York, London, Interscience Publishers (1959) (Interscience Tracts in pure and applied Mathematics, **7**).

[4] D. REES, *On the sections of coherent algebraic sheaves* (non publié).

[5] J-P. SERRE, *Quelques propriétés des variétés abéliennes en caractéristique p*, Amer. J. of Math. **80** (1958), 715–739.

[6] J-P. SERRE, *Espaces fibrés algébriques*, Séminaire Chevalley 1958 : *Anneaux de Chow et applications*, exposé n° 1.

[7] J-P. SERRE, *Groupes Algébriques et Corps de Classes*, Paris, Hermann, 1959.

Séminaire Chevalley
1958-59, exposé n° 11

MORPHISMES UNIVERSELS ET DIFFÉRENTIELLES DE TROISIÈME ESPÈCE

Dans ce qui suit, X désigne une variété *projective non singulière* sur le corps K. On se donne sur X un nombre fini de sous-variétés de codimension 1, soient $D_i, \ldots, D_r$; on note Y la sous-variété $X - D$, où $D = \cup D_i$. Si $\mathscr{S}$ désigne la catégorie des groupes algébriques qui sont extension d'une variété abélienne par un tore, on sait (cf. exposé 10, th. 7) qu'il existe un morphisme $f : Y \to G$, $G \in \mathscr{S}$, qui est universel pour $\mathscr{S}$; le problème consiste à construire explicitement ce morphisme ; c'est ce qu'on fera au § 1 en utilisant la théorie des variétés de Picard. De plus, les formes différentielles sur X qui sont images réciproques par f de formes invariantes sur G ne sont autres (dans le cas classique) que les formes dites « de troisième espèce », admettant pour « résidu » une combinaison linéaire des D_i ; de ce point de vue, la construction du § 1 est essentiellement équivalente à un théorème classique de Severi ([8], p. 91 ; voir aussi [6]).

§ 1. Construction du morphisme universel

Soit D(X) le groupe des diviseurs de X ; puisque X est non singulière, chacun des D_i définit un élément de D(X), que l'on note encore D_i. Le sous-groupe de D(X) engendré par les D_i est isomorphe à $\mathbf{Z}^r$; nous le noterons I.

Soit C(X) le groupe des classes de diviseurs de X, et soit P la *variété de Picard* de X, identifiée à un sous-groupe de C(X). Le noyau de l'homomorphisme

$$I \longrightarrow D(X) \longrightarrow C(X) \longrightarrow C(X)/P$$

sera désigné par J ; on a donc un homomorphisme canonique $\theta : J \to P$ obtenu par restriction de $I \to C(X)$. Le groupe J est un groupe abélien libre de type fini.

On note T le tore dont le groupe des caractères (cf. [1]) est J. On a donc $T = \mathrm{Hom}(J, \mathbf{G}_m)$, $J = \mathrm{Hom}(T, \mathbf{G}_m)$, le premier « Hom » étant pris sur $\mathbf{Z}$, le second étant pris au sens des groupes algébriques.

On note $\varphi : X \to A$ le morphisme canonique de X dans sa *variété d'Albanese*; on sait que la variété de Picard de A s'identifie à celle de X, c'est-à-dire à P. D'autres part, on sait (cf. [4], chapitre VII, n° 16) que le groupe $\mathrm{Ext}(A, \mathbf{G}_m)$ des extensions de A par $\mathbf{G}_m$ s'identifie au groupe P. On en déduit facilement que le groupe $\mathrm{Ext}(A, T)$ s'identifie à $\mathrm{Hom}(J, P)$, et comme on a défini plus haut un élément canonique θ dans ce groupe, on trouve ainsi une *extension canonique* G *de* A *par* T.

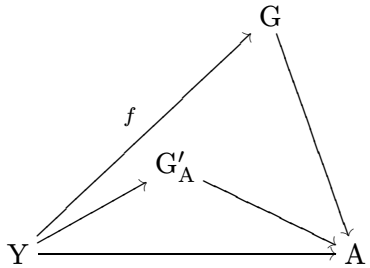
On peut considérer G comme un espace fibré principal de base A et de groupe T; soit $E = X \times_A G$ l'image réciproque par $\varphi : X \to A$ de cet espace fibré : c'est un espace fibré principal de base X et de groupe T. Pour tout j de $\mathrm{Hom}(T, \mathbf{G}_m) = J$, soit E_j l'espace fibré principal de base X et de groupe $\mathbf{G}_m$ déduit de E au moyen de j; un tel espace fibré correspond à un élément de C(X), on le sait; ici, par construction même de E, cet élément n'est autre que l'*image canonique* de j dans C(X). Or, si M est un espace fibré de base X et de groupe $\mathbf{G}_m$, correspondant à une classe de diviseurs $m \in C(X)$, et si Δ est un diviseur de classe m, il existe une section s de M (au sens fonctions) dont le « diviseur » est Δ; de plus, cette section est unique, à multiplication près par un élément de $\mathbf{G}_m$ (cela tient au fait que X est complète). En appliquant ce résultat à E_j, on voit qu'il existe une section $g_j : X \to E_j$ dont le diviseur est j lui-même. En prenant une base $j_1, \ldots, j_k$ de J sur $\mathbf{Z}$, on déduit de là l'existence d'une section $g : X \to E$ qui, pour tout j, donne g_j par composition avec $E \to E_j$; cette propriété caractérise g à une translation près par un élément de T. Mais une section de E correspond canoniquement à une fonction de X dans G relevant φ. La fonction g définit donc une fonction $f : X \to G$ déterminée à une translation près par un élément de T. Comme g est régulière en dehors de D, la restriction de f à $Y = X - D$ est un *morphisme* de Y dans G.

THÉORÈME 1. — *Le morphisme* $f|Y : Y \to G$ *défini ci-dessus est universel pour la catégorie* $\mathscr{S}$.

Nous désignerons par π la projection de G sur A; on a $\pi \circ f = \varphi$ par construction même de f.

Soit $k : Y \to G'$ un morphisme de Y dans un groupe G' de la catégorie $\mathscr{S}$; le groupe G' est extension d'une variété abélienne A' par un tore T'. Si l'on compose $Y \to G' \to A'$, on trouve un morphisme $Y \to A'$, et comme A est la variété d'Albanese de Y, on peut factoriser en $Y \to A \to A'$; quitte à faire une translation, on peut supposer que $A \to A'$ est un homomorphisme de groupes. Soit alors G'_A l'extension de A par T' image réciproque de G' par l'homomorphisme $A \to A'$. Les morphismes $Y \to G'$ et $Y \to A$ définissent un

morphisme $k_{\mathrm{A}} : \mathrm{Y} \to \mathrm{G}'_{\mathrm{A}}$, et l'on a un diagramme commutatif :

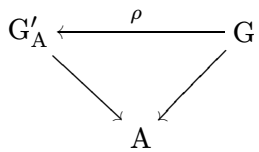


Tout revient à démontrer qu'il existe un homomorphisme unique ρ de G dans G'_{A} laissant commutatif le diagramme précédent.

Désignons par J' le groupe des caractères de T' ; à tout élément j' de $\mathrm{Hom}(\mathrm{T}', \mathbf{G}_m)$ est associée une extension $j'(\mathrm{G}'_{\mathrm{A}})$ de A par $\mathbf{G}_m$, et un morphisme $k(j')$ de Y dans cette extension. Si l'on considère $k(j')$ comme une fonction sur X, on peut parler du *diviseur* de cette fonction (car c'est localement une fonction à valeurs dans $\mathbf{G}_m$), et ce diviseur est nécessairement une combinaison linéaire des D_i, c'est-à-dire un élément de I. On a donc obtenu un homomorphisme de J' dans I. En fait, cet homomorphisme applique J' *dans* J, car la classe du diviseur $k(j')$ est image réciproque par φ de la classe de diviseurs sur A associée à l'extension $j'(\mathrm{G}'_{\mathrm{A}})$, et on sait que cette dernière appartient à P (cf. [4], *loc. cit.*). On a donc un morphisme

$$\lambda : \mathrm{J}' \longrightarrow \mathrm{J} \quad .$$

Par transposition, cet homomorphisme définit un homomorphisme $\mu : \mathrm{T} \to \mathrm{T}'$ d'où un homomorphisme $\mu_* : \mathrm{Ext}(\mathrm{A}, \mathrm{T}) \to \mathrm{Ext}(\mathrm{A}, \mathrm{T}')$. Cet homomorphisme μ_* transforme $\mathrm{G} \in \mathrm{Ext}(\mathrm{A}, \mathrm{T})$ en $\mathrm{G}'_{\mathrm{A}} \in \mathrm{Ext}(\mathrm{A}, \mathrm{T}')$: cela se voit en identifiant ces deux groupes à $\mathrm{Hom}(\mathrm{J}, \mathrm{P})$ et $\mathrm{Hom}(\mathrm{J}', \mathrm{P})$, respectivement. Il s'ensuit qu'il existe un homomorphisme $\rho : \mathrm{G} \to \mathrm{G}'_{\mathrm{A}}$ qui coïncide avec μ sur T, et qui rend commutatif le diagramme



Il reste à comparer $\rho \circ f$ et k_{A}. Cela se fait en remarquant que ces morphismes définissent deux sections (fonctions) au-dessus de X d'un même espace fibré de groupe T' et que ces deux sections ont même diviseur (pour tout $j' \in \mathrm{J}'$) ; elles coïncident donc à la multiplication près par un élément de T'. Quitte à effectuer une translation sur ρ, on peut supposer que $\rho \circ f = k_{\mathrm{A}}$. Enfin, si $\rho' \circ f = k_{\mathrm{A}}$,

ρ' étant un autre homomorphisme affine, ρ' doit appliquer T dans T′, et le raisonnement précédent, pris en sens inverse, montre qu'il coïncide avec ρ sur T ; on a alors nécessairement $\rho = \rho'$, ce qui achève de démontrer la propriété universelle de $f|Y$.

Exemple. — Si X est une *courbe*, les D_i sont des points, et J est formé des combinaisons linéaires $\sum n_i D_i$, avec $\sum n_i = 0$; c'est un groupe libre de rang $r - 1$. Le groupe G construit ci-dessus est la jacobienne généralisée de X pour le module $\mathfrak{m} = \sum D_i$, (cf. [4], Chap. V, n° 17).

§ 2. Images réciproques des différentielles invariantes sur G

Rappelons d'abord la définition des *formes de troisième espèce* :

Soit α une forme différentielle de degré 1 sur X. On dit que α est de troisième espèce si, au voisinage de tout point $P \in X$, il est possible d'écrire α sous la forme

$$\alpha = \sum c_i df_i/f_i + \beta \ ,$$

où les f_i sont des fonctions numériques, les c_i des constantes, et la forme β est régulière en P.

La décomposition ci-dessus n'est évidemment pas unique ; toutefois, on montre que le diviseur local (à coefficients dans K) $\sum c_i(f_i)$ est bien déterminé ; en faisant varier P, on obtient un diviseur sur X à coefficients dans K [c'est-à-dire un élément de $K \otimes D(X)$] ; on l'appelle le *résidu* de α, et on le note $\mathrm{Res}(\alpha)$. Pour qu'une sous-variété irréductible Δ de X soit variété polaire de α, il faut et il suffit que le coefficient de Δ dans $\mathrm{Res}(\alpha)$ soit non nul. En particulier, α est régulière sur X (« de première espèce ») si et seulement si $\mathrm{Res}(\alpha) = 0$.

Soit maintenant $\omega \in s_G$ une forme différentielle de degré 1 invariante sur le groupe G construit au § 1. La restriction ω_T de ω à T est une forme invariante sur T, et l'on obtient ainsi toutes les formes invariantes sur T. D'autre part, T a pour groupe de caractères J, qui est un sous-groupe de I ; donc T est image du tore correspondant à I, tore qui n'est autre que $(\mathbf{G}_m)^r$. L'image réciproque dans $(\mathbf{G}_m)^r$ de ω_T sera notée $P\omega$; on peut l'écrire $P\omega = \sum c_i dx_i/x_i$, où les x_i désignent les coordonnées naturelles de $(\mathbf{G}_m)^r$. On vérifie tout de suite que l'on obtient ainsi tous les systèmes (c_i) qui sont combinaisons linéaires à coefficients dans K de systèmes $(n_i) \in J$; nous noterons KJ l'ensemble de ces systèmes. Avec ces notations, on a le théorème suivant

THÉORÈME 2. — *Si ω est une forme différentielle invariante de degré* 1 *sur* G, *la forme $f^*\omega$ est une forme de troisième espèce sur* X. *De plus, si* $\mathrm{P}\omega = \sum c_i dx_i/x_i$, *on a* $\mathrm{Res}(f^*\omega) = \sum c_i \mathrm{D}_i$.

COROLLAIRE. — *Pour qu'un diviseur sur* X *à coefficients dans* K *soit résidu d'une forme différentielle de la forme $f^*\omega$, $\omega \in s_{\mathrm{G}}$, il faut et il suffit qu'il appartienne à* KJ.

On sait (exposé 10, démonstration du lemme 6) que $f^*\omega$ est une forme différentielle de troisième espèce. Il reste à calculer son résidu. Par linéarité, on peut supposer que ω est image réciproque d'une forme invariante π_j du groupe G_j déduit de G par $j : \mathrm{T} \to \mathbf{G}_m$, et que cette forme π_j induit sur $\mathbf{G}_m \subset \mathrm{G}_j$ la forme dx/x. On a donc $f^*\omega = f_j^*(\pi_j)$, en notant $f_j : \mathrm{X} \to \mathrm{G}_j$ la fonction canonique de X dans G_j. Si l'on se place au voisinage d'un point $\mathrm{P} \in \mathrm{X}$, on peut identifier G_j à un produit $\mathrm{U} \times \mathbf{G}_m$, U étant un ouvert de A (cf. la démonstration du lemme 6, exposé 10, citée plus haut), et la forme π_j s'écrit alors $\gamma_j + dx/x$, où γ_j est image réciproque d'une forme régulière sur U. La fonction f_j peut être considérée comme un couple (φ, h_j), où $\varphi : \mathrm{X} \to \mathrm{A}$ est l'application canonique de X dans sa variété d'Albanese, et où $h_j : \mathrm{X} \to \mathbf{G}_m$ est une fonction numérique. De plus, d'après la construction même de f, le diviseur de h_j est égal à j. Il s'ensuit que dh_j/h_j a pour résidu j, et comme dh_j/h_j est égal à $f_j^*(\pi_j)$ à une forme régulière près, cela démontre le théorème.

Exemple. — Supposons que X soit une courbe de genre g ; les D_i $(i = 1, \ldots, r)$ sont des points $\mathrm{P}_i \in \mathrm{X}$. D'après le corollaire ci-dessus, un diviseur $\sum c_i \mathrm{P}_i$ est résidu d'une différentielle $f^*\omega$ si et seulement si $\sum c_i = 0$, condition qui était de toute façon nécessaire d'après la formule des résidus. Soit alors α une forme de troisième espèce sur X, régulière en dehors des P_i ; d'après ce qui précède, il existe $\omega_0 \in s_{\mathrm{G}}$ telle que $\mathrm{Res}(\alpha) = \mathrm{Res}(f^*\omega_0)$; la forme $\alpha - f^*\omega_0$ est donc une forme de première espèce, donc provient de la variété d'Albanese (jacobienne) de X. On en conclut que α est de la forme $f^*\omega$, avec $\omega \in s_{\mathrm{G}}$ (pour une autre démonstration, voir [4], p. 97).

Nous verrons au § 3 que ce résultat s'étend aux variétés de dimension arbitraire pourvu que la caractéristique du corps K soit zéro (il y a des contre-exemples d'IGUSA en caractéristique p, cf. [2]).

§ 3. Le cas classique

Nous supposons maintenant que le corps de base K est le corps $\mathbf{C}$ des nombres complexes; la variété X est donc une variété *kählérienne.*

Si Δ est un diviseur sur X, nous noterons $h(\Delta)$ la classe de cohomologie entière de degré 2 qui lui est attachée (cf. par exemple [7], chapitre V). Si l'on note $\mathscr{O}$ (resp. $\mathscr{O}^*$) le faisceau des fonctions holomorphes (resp. holomorphes non nulles) sur X, on a une suite exacte :

$$0 \longrightarrow \mathbf{Z} \xrightarrow{2i\pi} \mathscr{O} \xrightarrow{\exp} \mathscr{O}^* \longrightarrow 0,$$

et si $\Delta \in \mathrm{H}^1(\mathrm{X}, \mathscr{O}^*)$, on a $h(\Delta) = \delta(\Delta) \in \mathrm{H}^2(\mathrm{X}, \mathbf{Z})$, le cobord étant pris par rapport à la suite exacte précédente.

THÉORÈME 3. — *Pour que Δ soit algébriquement équivalent à zéro, il faut et il suffit que $h(\Delta)$ soit nul.*

(On dit qu'un diviseur est algébriquement équivalent à zéro si son image dans le groupe des classes de diviseurs appartient à la variété de Picard.)

Vu la suite exacte $\mathrm{H}^1(\mathrm{X}, \mathscr{O}) \to \mathrm{H}^1(\mathrm{X}, \mathscr{O}^*) \to \mathrm{H}^2(\mathrm{X}, \mathbf{Z})$, le théorème 3 revient à dire que l'image de $\mathrm{H}^1(\mathrm{X}, \mathscr{O})$ dans $\mathrm{H}^1(\mathrm{X}, \mathscr{O}^*)$ n'est autre que la variété de Picard de X, résultat bien connu (voir par exemple [3]).

Soit $\varepsilon : \mathrm{H}^2(\mathrm{X}, \mathbf{Z}) \to \mathrm{H}^2(\mathrm{X}, \mathbf{C})$ l'homomorphisme induit par la multiplication par $2i\pi$ sur les coefficients. Nous noterons $c(\Delta)$ l'image de $h(\Delta)$ par ε. L'application c se prolonge par linéarité aux diviseurs *à coefficients complexes.*

THÉORÈME 4 (WEIL, [5]). — *Soit $\Delta = \sum c_i \mathrm{D}_i$ un diviseur à coefficients complexes. Pour qu'il existe une forme α de troisième espèce sur* X *telle que* $\mathrm{Res}(\alpha) = \Delta$*, il faut et il suffit que $c(\Delta) = 0$.*

Rappelons brièvement la démonstration. Soit Ω^1 le faisceau des germes de formes holomorphes sur X. On sait (théorème de Dolbeault) que $\mathrm{H}^1(\mathrm{X}, \Omega^1)$ s'identifie à la composante $\mathrm{H}^{1,1}(\mathrm{X}, \mathbf{C})$ de $\mathrm{H}^2(\mathrm{X}, \mathbf{C})$. D'autre part, l'homomorphisme de faisceaux défini par $f \mapsto df/f$ envoie $\mathrm{H}^1(\mathrm{X}, \mathscr{O}^*)$ dans $\mathrm{H}^1(\mathrm{X}, \Omega^1)$. On en déduit par composition un homomorphisme $\mathrm{H}^1(\mathrm{X}, \mathscr{O}^*) \to \mathrm{H}^2(\mathrm{X}, \mathbf{C})$ *qui coïncide avec l'homomorphisme c défini plus haut* (cf. [7], *loc. cit.*). Dire que $c(\Delta) = 0$ revient donc à dire que l'image de Δ dans $\mathrm{H}^1(\mathrm{X}, \Omega^1)$ est nulle. Or, si l'on recouvre X par des ouverts U_λ et si sur chaque U_λ on représente Δ par $\sum c_i(f_i^\lambda)$, on peut trouver des formes π_λ holomorphes sur U_λ, telles que

$$\sum c_i \, df_i^\lambda / f_i^\lambda - \sum c_i \, df_i^\mu / f_i^\mu = \pi_\lambda - \pi_\mu \qquad \text{sur} \quad \mathrm{U}_\lambda \cap \mathrm{U}_\mu.$$

Mais alors la forme

$$\alpha = \sum c_i \, df_i^\lambda / f_i^\lambda - \pi_\lambda = \sum c_i \, df_i^\mu / f_i^\mu - \pi_\mu$$

est une forme de troisième espèce (au sens analytique, donc aussi algébrique) admettant Δ pour résidu. Le même raisonnement, pris en sens inverse, montre que l'existence d'une telle forme implique la nullité de $c(\Delta)$.

COROLLAIRE 1. — *Pour qu'il existe une forme de troisième espèce sur* X *admettant* Δ *pour résidu, il faut et il suffit que* $\Delta \in \mathrm{KJ}$ (les notations étant celles du § 1).

En effet, le théorème 3 montre que J est l'ensemble des $\Delta = \sum n_i \mathrm{D}_i$ tels que $h(\Delta) = 0$, donc KJ est l'ensemble des Δ tels que $c(\Delta) = 0$.

COROLLAIRE 2. — *Toute forme de troisième espèce sur* X *qui est régulière sur* Y *est de la forme* $f^*\omega$, *avec* $\omega \in s_{\mathrm{G}}$.

Soit α une telle forme. D'après le corollaire au th. 2 et le corollaire 1 au th. 4, il existe $\omega_0 \in s_{\mathrm{G}}$ telle que $\mathrm{Res}(\alpha) = \mathrm{Res}(\omega_0)$. La forme $\alpha - \omega_0$ est donc partout régulière, et l'on sait qu'une telle forme est image réciproque d'un élément de s_{A}, donc aussi d'un élément de s_{G}. D'où le résultat.

COROLLAIRE 3. — *Toute forme de troisième espèce sur* X *est fermée*

En effet, il en est ainsi des formes $f^*\omega$, avec $\omega \in s_{\mathrm{G}}$.

Remarque. — Les corollaires ci-dessus s'énoncent de façon purement algébrique. Comme ils sont vrais sur le corps $\mathbf{C}$, le « principe de Lefschetz » montre qu'ils sont vrais sur tout corps algébriquement clos de caractéristique 0. En caractéristique p, les corollaires 1 et 2 peuvent être en défaut, comme on l'a signalé plus haut ; j'ignore ce qu'il en est du corollaire 3. **1**

Bibliographie

[1] A. GROTHENDIECK, *Généralités sur les groupes algébriques affines, Groupes algébriques affines commutatifs*, Séminaire Chevalley 1956-57 : Classification des groupes de Lie algébriques, exposé n° 4.

[2] J-I. IGUSA, *On some problems in abstract algebraic geometry*, Proc. Nat. Acad. Sci. USA **41** (1955), 964–967.

[3] K. KODAIRA and D. SPENCER, *Groups of complex line bundles over compact Kähler varieties, Divisor class groups on algebraic varieties*, Proc. Nat. Acad. Sci. USA **39** (1953), 868–877.

[4] J-P. SERRE, *Groupes Algébriques et Corps de Classes*, Paris, Hermann, 1959.

[5] A. WEIL, *Sur la théorie des formes différentielles attachées à une variété analytique complexe*, Comm. Math. Helv. **20**, 1947, 110–116.

[6] A. Weil, *Variétés abéliennes*, Algèbre et Théorie des Nombres. [1949, Paris] ; 124–127, Paris, Centre National de la Recherche scientifique (1950) (Colloque intern. C.N.R.S. **24**).

[7] A. Weil, *Introduction à l'Étude des Variétés Kählériennes*, Paris, Hermann, 1958.

[8] O. Zariski, *Algebraic Surfaces*, New York, Chelsea publishing Company (1948) (Ergebnisse der Mathematik, Band 3, Heft 5).

Séminaire Bourbaki
1959-60, exposé n° 198

février 1960

RATIONALITÉ DES FONCTIONS ζ DES VARIÉTÉS ALGÉBRIQUES

d'après B. Dwork

§ 1. Introduction

La fonction ζ d'un *schéma* S *de type fini sur* $\mathbf{Z}$ est définie par le produit eulérien :

$$\zeta_S(s) = \prod_P \frac{1}{(1 - 1/N(P)^s)}, \tag{1}$$

où P parcourt l'ensemble des points fermés de S, et où N(P) est le nombre d'éléments du corps résiduel $\kappa(P)$ correspondant. Ce produit converge pour $\mathrm{Re}(s)$ assez grand, et on conjecture qu'il se prolonge en une fonction méromorphe dans tout le plan complexe. Considérons en particulier, un *schéma* V *de type fini sur* $\mathbf{F}_q$, corps fini à q éléments (c'est ce que certains appellent une « variété algébrique définie sur $\mathbf{F}_q$ »). On a alors $\mathbf{F}_q \subset \kappa(P)$, et si $\deg(P)$ désigne le degré de cette extension, on a :

$$N(P) = q^{\deg(P)}, \tag{2}$$

ce qui conduit à changer de variable, et à poser $t = q^{-s}$. On obtient ainsi la fonction :

$$Z_V(t) = \prod_P \frac{1}{1 - t^{\deg(P)}}, \tag{3}$$

qui est une série formelle en t, à coefficients dans $\mathbf{Z}$. Notons N_s le nombre de points du $\mathbf{F}_q$-schéma V à valeurs dans l'extension $\mathbf{F}_{q^s}$ de $\mathbf{F}_q$. Un calcul simple donne :

$$Z_V(t) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{t^s}{s}\right). \tag{4}$$

WEIL, à qui ces définitions sont dues, avait conjecturé que Z_V est une fonction rationnelle de t, et l'avait vérifié dans certains cas (cf. [5] ainsi que l'exposé de DELSARTE [2]). DWORK vient de résoudre la question :

THÉORÈME ([4]). — *Pour tout schéma* V *de type fini sur le corps* $\mathbf{F}_q$*, la série* $Z_V(t)$ *est une fonction rationnelle de* t*.*

On peut se borner au cas où q est un nombre premier p, puisque $\mathbf{F}_q$ est de type fini sur $\mathbf{F}_p$. De plus, si V' et V'' sont des sous-schémas de V, avec $V' \cup V'' = V$ et $V' \cap V'' = W$, on a :

$$Z_V = Z_{V'} \cdot Z_{V''} \cdot Z_W^{-1}. \tag{5}$$

Cette formule permet, par un argument combinatoire facile, de ramener le théorème au cas où V est affine, et même au cas où V est défini par une seule équation

$$f(X_1, \ldots, X_n) = 0, \text{ à coefficients dans } \mathbf{F}_p. \tag{6}$$

Dans ce cas, N_s est simplement *le nombre de solutions de l'équation* (6) *dans le corps à* p^s *éléments.*

§ 2. Un critère de rationalité

On va d'abord rappeler un critère classique :
Soit k un corps, et soit

$$F(t) = \sum_{s=0}^{\infty} A_s t^s, \ A_s \in k \tag{7}$$

une série formelle. Si s et m sont deux entiers $\geqslant 0$, posons

$$N_{s,m} = \det(A_{s+i+j}), \ 0 \leqslant i \leqslant m, \ 0 \leqslant j \leqslant m. \tag{8}$$

PROPOSITION 1. — *Pour que* F *soit quotient de deux polynômes en* t *à coefficients dans* k (i.e. pour que F soit rationnelle)*, il faut et il suffit qu'il existe un entier* $m \geqslant 0$ *tel que* $N_{s,m} = 0$ *pour tout* s *assez grand.*

Pour la démonstration, voir [1], ainsi que BOURBAKI, A IV.85, exerc. 1.

Supposons maintenant que les A_s soient *entiers.* On pourra donc parler à la fois de leur valeur absolue *usuelle* (induite par le plongement dans $\mathbf{C}$), notée $|A|$, et de leur valeur absolue *p-adique*, notée $|A|_p$; comme d'habitude, on suppose cette dernière normalisée par la formule du produit, i.e. $|p^a|_p =$

p^{-a}. De plus, on se donne un corps valué complet Ω, algébriquement clos, contenant $\mathbf{Q}_p$, et dont la valeur absolue prolonge celle de $\mathbf{Q}_p$. Une série

$$f = \sum_{i=0}^{\infty} a_i\, t^i, \quad a_i \in \Omega,$$

sera dite *holomorphe* dans le disque $|t|_p < r$ si elle converge absolument dans ce disque; un quotient de deux telles séries sera appelé *méromorphe*. Si f est holomorphe pour $|t|_p < r$, et si $r' < r$, on démontre qu'on peut écrire f sous la forme $\mathrm{P}\cdot f'$, où P est un polynôme, et où f' est une série holomorphe ainsi que son inverse dans le disque $|t|_p < r'$ (on ne peut plus, ici, se servir de l'intégrale de Cauchy, il faut raisonner directement, en se servant du « polygone de Newton » de f, ce n'est pas difficile). 1

PROPOSITION 2. — *Soit* $\mathrm{F} = \sum_{s=0}^{\infty} \mathrm{A}_s t^s$ *une série à coefficients entiers, et soit* p *un nombre premier. Supposons qu'il existe deux nombres réels positifs* R *et* r*, avec* $\mathrm{R}r > 1$*, tels que* F *soit méromorphe dans le disque* $|z| < \mathrm{R}$ *de* $\mathbf{C}$ *ainsi que dans le disque* $|z|_p < r$ *de* Ω*. Alors* F *est rationnelle.*

Lorsque $\mathrm{R} > 1$, on retrouve un résultat d'Emile BOREL ([1]). Supposons donc $\mathrm{R} \leqslant 1$, d'où $r > 1$. Par hypothèse, il existe des séries entières :

$$\mathrm{A}(t) = \sum_{i=0}^{\infty} a_i\, t^i, \quad \mathrm{B}(t) = \sum_{i=0}^{\infty} \mathrm{B}_i\, t^i, \quad a_i, \mathrm{B}_i \in \Omega, \tag{9}$$

holomorphes dans $|z|_p < r$, et telles que $\mathrm{B} = \mathrm{A}\cdot\mathrm{F}$. D'après ce qui a été dit ci-dessus, on peut même supposer que A est un polynôme (quitte à diminuer un peu r), et aussi que $a_0 = 1$. Quitte a diminuer encore un peu r et R, on a des inégalités :

$$|\mathrm{B}_s|_p \leqslant r^{-s}, \quad \text{pour } s \text{ assez grand}, \tag{10}$$

$$|\mathrm{A}_s| \leqslant \mathrm{R}^{-s}, \quad \text{pour } s \text{ assez grand}. \tag{11}$$

Soit e le degré de A, et choisissons un entier m tel que $\mathrm{R}^{m+1} r^{m+1-e} = k$ soit > 1, ce qui est possible puisque $\mathrm{R}r > 1$. On va appliquer le critère de la prop. 1. Puisque $\mathrm{B} = \mathrm{A}\cdot\mathrm{F}$, on a :

$$\mathrm{B}_{s+e} = \mathrm{A}_{s+e} + a_1 \mathrm{A}_{s+e-1} + \cdots + a_e \mathrm{A}_s. \tag{12}$$

Dans le déterminant $\mathrm{N}_{s,m} = \det(\mathrm{A}_{s+i+j}), 0 \leqslant i, j \leqslant m$, on peut donc remplacer les A_{s+i+j}, $j \geqslant e$, par les B_{s+i+j}. En appliquant (10) et en tenant compte du fait que $|\mathrm{A}_s|_p \leqslant 1$, on en déduit :

$$|\mathrm{N}_{s,m}|_p \leqslant r^{-(m+1-e)s}, \text{ pour } s \text{ assez grand}. \tag{13}$$

D'autre part, on tire de (11) l'inégalité :

$$|\mathrm{N}_{s,m}| \leqslant (m+1)!\mathrm{R}^{-(m+1)(s+m)}, \text{ pour } s \text{ assez grand.} \tag{14}$$

D'où :

$$|\mathrm{N}_{s,m}|\cdot|\mathrm{N}_{s,m}|_p \leqslant k_1 \cdot k^{-s}, \quad \text{avec } k_1 \text{ indépendant de } s. \tag{15}$$

Comme $k > 1$, ceci entraîne $|\mathrm{N}_{s,m}|\cdot|\mathrm{N}_{s,m}|_p < 1$ pour s assez grand, et comme $\mathrm{N}_{s,m}$ est un entier, ceci entraîne $\mathrm{N}_{s,m} = 0$, c.q.f.d.

Remarque. — On trouvera dans [4] un énoncé généralisant la proposition 2 au cas où l'on prend les A_i dans un corps de nombres K, et où l'on fait des hypothèses de méromorphie pour un nombre fini de places de K.

Application à la fonction $\mathrm{Z_V}(t)$. — Si V est plongé dans l'espace affine à n dimensions, la série $\mathrm{Z_V}(t)$ admet comme majorante la série $1/(1-p^n t)$, ce qui montre qu'elle est holomorphe dans le disque de rayon p^{-n}. Pour pouvoir lui appliquer la proposition 2, il faut donc montrer qu'elle est méromorphe au sens p-adique dans un disque de rayon $> p^n$. En fait, on verra que $\mathrm{Z_V}(t)$ est même *méromorphe dans tout* Ω, autrement dit est quotient de deux séries à coefficients dans Ω, ayant chacune un rayon de convergence infini; ces séries seront construites explicitement, à partir de l'équation f définissant le schéma V. Ceci sera fait au § 5; les §§ 3 et 4 sont consacrés à des constructions préliminaires.

§ 3. Factorisation des caractères additifs des corps finis

On note K le corps résiduel de Ω; c'est un corps algébriquement clos de caractéristique p; il contient donc les $\mathbf{F}_{p^s}$. Tout élément de K a un unique « représentant multiplicatif » dans Ω. Les représentants multiplicatifs des éléments de $\mathbf{F}_{p^s}$ sont les racines (p^s-1)-ièmes de l'unité et 0. On note Λ l'anneau des entiers de Ω; on a $\Lambda \cap \mathbf{Q}_p = \mathbf{Z}_p$, anneau des entiers p-adiques. Enfin, on pose

$$|x|_p = p^{-\mathrm{ord}(x)}, \quad x \in \Omega.$$

On a $\mathrm{ord}(p) = 1$.

Soient t et Y deux indéterminées. Considérons la série formelle

$$\mathrm{H}(t,\mathrm{Y}) = (1+\mathrm{Y})^t = \sum_{m=0}^{\infty} \binom{t}{m} \mathrm{Y}^m, \text{ où } \binom{t}{m} = \frac{t(t-1)\cdots(t-m+1)}{m!}. \tag{16}$$

C'est un élément de $\mathbf{Q}[[t, \mathrm{Y}]]$: ses coefficients sont des nombres rationnels. Lorsque $t \in \mathbf{Z}_p$, les $\binom{t}{m}$ appartiennent aussi à $\mathbf{Z}_p$, et $(1+\mathrm{Y})^t$ converge pour $\mathrm{ord}(\mathrm{Y}) > 0$; c'est d'ailleurs la puissance « t-ième » de $1+\mathrm{Y}$ en un sens évident.

Formons maintenant le produit infini :

$$\mathrm{F}(t, \mathrm{Y}) = \mathrm{H}(t, \mathrm{Y}) \cdot \mathrm{H}\left(\frac{t^p - 1}{p}, \mathrm{Y}^p\right) \cdot \mathrm{H}\left(\frac{t^{p^2} - t^p}{p^2}, \mathrm{Y}^{p^2}\right) \cdots \tag{17}$$

c'est-à-dire :

$$\mathrm{F}(t, \mathrm{Y}) = (1+\mathrm{Y})^t (1+\mathrm{Y}^p)^{\frac{t^p - t}{p}} (1+\mathrm{Y}^{p^2})^{\frac{t^{p^2} - t^p}{p^2}} \cdots \tag{18}$$

On voit tout de suite que ce produit infini converge dans $\mathbf{Q}[[t, \mathrm{Y}]]$.

Lemme. — Les coefficients de la série formelle F *sont dans* $\mathbf{Z}_p$.

On calcule $\mathrm{F}(t^p, \mathrm{Y}^p)/\mathrm{F}(t, \mathrm{Y})^p$, et l'on trouve $(1+\mathrm{Y}^p)^t/(1+\mathrm{Y})^{pt}$. Mais on voit facilement que $(1+\mathrm{Y}^p)/(1+\mathrm{Y})^p$ est de la forme $1+p\mathrm{Z}$ où Z est une série sans terme constant à coefficients dans $\mathbf{Z}_p$; on en déduit que $(1+p\mathrm{Z})^t$ est du même type $1+p\mathrm{Z}'$ (utiliser les propriétés de divisibilité des coefficients binomiaux). La relation $\mathrm{F}(t^p, \mathrm{Y}^p)/\mathrm{F}(t, \mathrm{Y})^p = 1 + p\mathrm{Z}'$ montre alors que les coefficients de F appartiennent à $\mathbf{Z}_p$ d'après un critère de Dwork ([3, lemme 1]).
[On peut aussi démontrer le lemme en exprimant la fonction F au moyen de l'exponentielle de Artin-Hasse.]

Développons F en série par rapport à Y :

$$\mathrm{F}(t, \mathrm{Y}) = \sum_{m=0}^{\infty} \mathrm{B}_m(t) \cdot \mathrm{Y}^m. \tag{19}$$

On voit tout de suite que B_m est un polynôme de degré $\leqslant m$ en t. On a donc :

$$\mathrm{F}(t, \mathrm{Y}) = \sum_{m=0}^{\infty} t^m \alpha_m(\mathrm{Y}), \tag{20}$$

où $\alpha_m(\mathrm{Y})$ est une série formelle commençant par un terme de degré $\geqslant m$ et à coefficients dans $\mathbf{Z}_p$.
Choisissons une racine primitive p-ième de l'unité $\varepsilon = 1+\lambda$. On a $\mathrm{ord}(\lambda) = \frac{1}{p-1}$, on le sait. Posons :

$$\Theta(t) = \mathrm{F}(t, \lambda) = \sum_{m=0}^{\infty} \beta_m t^m, \text{ avec } \beta_m = \alpha_m(\lambda). \tag{21}$$

On a :

$$\mathrm{ord}(\beta_m) \geqslant \frac{m}{p-1}, \tag{22}$$

puisque $\alpha_m(\mathrm{Y})$ commence par Y^m. La série Θ converge donc dans le disque $\mathrm{ord}(t) > -\frac{1}{p-1}$.

Soit maintenant $t' \in \mathbf{F}_{p^s} \subset \mathrm{K}$, et soit t le représentant multiplicatif de t' dans Ω. On a $t^{p^s} = t$. Si l'on pose $t + t^p + \cdots + t^{p^{s-1}} = \mathrm{Tr}(t)$, l'élément $\mathrm{Tr}(t)$ appartient à $\mathbf{Z}_p$. De plus, on a l'égalité :

$$(1+\mathrm{Y})^{\mathrm{Tr}(t)} = \mathrm{F}(t,\mathrm{Y})\cdot\mathrm{F}(t^p,\mathrm{Y})\cdots\mathrm{F}(t^{p^{s-1}},\mathrm{Y}), \tag{23}$$

comme on le constate tout de suite. Les deux membres de cette égalité sont des séries à coefficients dans Λ; on peut donc substituer λ à Y, et on l'on trouve l'égalité :

$$\varepsilon^{\mathrm{Tr}(t)} = \Theta(t)\cdot\Theta(t^p)\cdots\Theta(t^{p^{s-1}}), \tag{24}$$

où le membre de gauche signifie que l'on élève ε à la puissance $\mathrm{Tr}(t)$-ième, ce qui a un sens puisque $\mathrm{Tr}(t) \in \mathbf{Z}_p$. Comme $\varepsilon^p = 1$, on peut réduire $\mathrm{Tr}(t)$ mod p, et l'on obtient

$$\mathrm{Tr}(t') = t' + t'^p + \cdots + t'^{p^{s-1}}, \tag{25}$$

la trace étant celle définie par l'extension $\mathbf{F}_{p^s}/\mathbf{F}_p$. L'application $t' \mapsto \varepsilon^{\mathrm{Tr}(t')}$ est *un caractère additif non trivial* du corps $\mathbf{F}_{p^s}$. En résumé :

PROPOSITION 3. — *Pour tout entier $s \geqslant 1$, le caractère additif $t' \mapsto \varepsilon^{\mathrm{Tr}(t')}$ peut s'écrire sous la forme $t' \mapsto \Theta(t)\cdot\Theta(t^p)\cdots\Theta(t^{p^{s-1}})$, où t est le représentant multiplicatif de t', et où Θ est une série à coefficients dans Ω vérifiant* (22).

En fait, les coefficients de Θ appartiennent à l'anneau $\mathbf{Z}_p[\varepsilon]$.

§ 4. Traces et déterminants de certaines matrices infinies

Soit L un corps, et soit n un entier. Si $u = (u_1, \ldots, u_n)$ est un élément de $\mathbf{Z}^n$, on notera X^u le monôme $\mathrm{X}_1^{u_1} \ldots \mathrm{X}_n^{u_n}$ en les n indéterminées $\mathrm{X} = (\mathrm{X}_1, \ldots, \mathrm{X}_n)$; on dira que u est $\geqslant 0$ si $u_i \geqslant 0$ pour tout i; on posera $c(u) = \sum u_i$.

Soit $\mathrm{E} = \mathrm{L}[[\mathrm{X}]]$ l'anneau des séries formelles en $\mathrm{X}_1, \ldots, \mathrm{X}_n$ à coefficients dans L; à tout $\mathrm{G} \in \mathrm{E}$, on associe l'endomorphisme $\varphi \mapsto \mathrm{G}\cdot\varphi$ de E qu'on notera encore G. D'autre part, si q est un entier $\geqslant 2$, on définit un endomorphisme Ψ_q de E par la formule :

$$\Psi_q\Big(\sum_{u\geqslant 0} a_u \mathrm{X}^u\Big) = \sum_{u\geqslant 0} a_{qu}\mathrm{X}^u. \tag{26}$$

Si $G = \sum_{v \geqslant 0} g_v X^v$, l'endomorphisme $\Psi_q \circ G$ de E est représenté par la *matrice infinie* $\Psi_{q,G}(u,v) = g_{qv-u}$. On notera les formules :

$$\Psi_q \circ \Psi_{q'} = \Psi_{qq'} \tag{27}$$

$$G \circ \Psi_q = \Psi_q \circ G_q, \quad \text{avec } G_q(X) = G(X^q). \tag{28}$$

On va appliquer ce qui précède *au cas où* $L = \Omega$, *et où la série* $G = \sum_{v \geqslant 0} g_v X^v$ *vérifie la condition suivante* :

(29) *Il existe une constante* $M > 0$ *telle que* $\operatorname{ord}(g_v) \geqslant M \cdot c(v)$ *pour tout* v.

Si G_1 et G_2 vérifient (29), il en est de même de leur produit, ainsi que de $G_1(X^h)$ pour tout entier $h \geqslant 1$.

Proposition 4. — *Supposons que* G *vérifie* (29). *Alors, pour tout entier* $s \geqslant 1$, *la série qui donne la trace de la matrice* $(\Psi_{q,G})^s$ *est convergente, et si l'on désigne sa somme par* $\operatorname{Tr}(\Psi^s)$, *on a* :

$$(q^s - 1)^n \cdot \operatorname{Tr}(\Psi^s) = \sum_{x^{q^s-1}=1} G(x) \cdot G(x^q) \cdots G(x^{q^{s-1}}). \tag{30}$$

[Ici encore x désigne un système $(x_1, \ldots, x_n)$, $x_i \in \Omega$, et la condition $x^{q^s-1} = 1$ signifie que chacun des x_i est une racine $(q^s - 1)$-ième de l'unité.]

Quitte à remplacer q par q^s, et $G(X)$ par $G(X) \cdot G(X^q) \cdots G(X^{q^{s-1}})$, on peut supposer que $s = 1$ (utiliser les formules (27) et (28)). On a alors $\operatorname{Tr}(\Psi) = \sum_{u \geqslant 0} g_{(q-1)u}$, série qui est convergente d'après (29). D'autre part, on vérifie aisément que l'on a :

$$\sum_{x^{q-1}=1} x^v = \begin{cases} (q-1)^n & \text{si } q-1 \text{ divise } v, \\ 0 & \text{sinon.} \end{cases} \tag{31}$$

On a donc bien $\sum_{x^{q-1}=1} G(x) = (q-1)^n \sum_{u \geqslant 0} g_{(q-1)u}$, c.q.f.d.

Considérons maintenant le *déterminant* de la matrice $1 - t\Psi$, où t est une indéterminée. Il est défini par le développement usuel :

$$\det(1 - t\Psi) = \sum_{m=0}^{\infty} \gamma_m t^m, \tag{32}$$

avec :

$$\gamma_m = (-1)^m \sum \varepsilon(u,v) \Psi(u_1, v_1) \cdots \Psi(u_m, v_m), \tag{33}$$

les $u_1, \ldots, u_m$ étant distincts, les $v_1, \ldots, v_m$ formant une permutation des u_i, et $\varepsilon(u, v)$ désignant la signature de cette permutation. Si l'on désigne par $\psi(\mathrm{U})$ l'un des termes de la somme (33), on a, en utilisant (29) :

$$\operatorname{ord}(\psi(\mathrm{U})) \geqslant (q-1)\mathrm{M}\sum_{i=1}^{i=m} c(u_i), \tag{34}$$

ce qui montre que $\operatorname{ord}(\psi(\mathrm{U}))$ tend vers $+\infty$, et la série (33) est convergente.

PROPOSITION 5. — *Supposons que* G *vérifie* (29). *Alors* :
(i) $\det(1 - t\Psi) = \exp(-\sum_{s=1}^{\infty} \operatorname{Tr}(\Psi^s)t^s/s)$;
(ii) *La série* $\det(1 - t\Psi)$ *a un rayon de convergence infini.*

La formule (i) est bien connue pour les matrices finies; on se ramène à ce cas en tronquant Ψ à un ordre r, et en montrant que, si Ψ_r désigne la matrice $r \times r$ ainsi obtenue, le polynôme $\det(1 - t\Psi_r)$ tend vers $\det(1 - t\Psi)$ pour la topologie de la convergence simple des coefficients.
Pour démontrer (ii), il faut prouver que :

$$\operatorname{ord}(\gamma_m)/m \longrightarrow +\infty \text{ lorsque } m \longrightarrow +\infty. \tag{35}$$

Or d'après (34), on a :

$$\operatorname{ord}(\gamma_m) \geqslant \mathrm{M}(q-1) \cdot \inf\Big(\sum_{i=1}^{i=m} c(u_i)\Big), \tag{36}$$

la borne inférieure étant prise sur toutes les suites $u_1, \ldots, u_m$ formés d'éléments positifs et distincts. Si l'on pose :

$$d_m = \inf\Big(\sum_{i=1}^{i=m} c(u_i)\Big), \tag{37}$$

tout revient donc à montrer que $d_m/m \to +\infty$. Mais on peut ranger les $u \geqslant 0$ en une suite $u_1, \ldots, u_n, \ldots$ de telle sorte sorte que $c(u_i) \leqslant c(u_{i+1})$, et il est alors clair que $d_m = \sum_{i=1}^{i=m} c(u_i)$. Comme les $c(u_i)$ tendent vers $+\infty$, il en est de même de leur moyenne arithmétique, ce qui signifie bien que d_m/m tend vers $+\infty$, c.q.f.d.

§ 5. Expression analytique des fonctions $\mathrm{Z_V}$

On a vu au § 1 qu'il suffit de considérer le cas où V est une hypersurface dans l'espace affine de dimension n, définie par une seule équation $f(x) = 0$, avec $f \in \mathbf{F}_p[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. On peut en outre retrancher de V les points où l'une des coordonnées est nulle. Le nombre N_s est alors simplement le nombre de

solutions communes des équations $f(x) = 0$ et $x^{p^s-1} = 1$. Fixons un entier $s \geqslant 1$; pour tout $t' \in \mathrm{F}_{p^s}$, soit $\Theta_s(t')$ la racine p-ième de l'unité définie par :

$$\Theta_s(t') = \varepsilon^{\mathrm{Tr}(t')} = \Theta(t) \cdot \Theta(t^p) \cdots \Theta(t^{p^{s-1}}), \tag{38}$$

(cf. prop. 3). Ecrivons k_s au lieu de $\mathbf{F}_{p^s}$ pour simplifier l'écriture. Du fait que Θ_s est un caractère non trivial de k_s, on a :

$$\sum_{x_0 \in k_s} \Theta_s(x_0.u) = \begin{cases} p^s & \text{si } u = 0, \\ 0 & \text{si } u \neq 0. \end{cases} \tag{39}$$

En appliquant ceci à $u = f(x)$, et en sommant, il vient :

$$p^s \mathrm{N}_s = (p^s - 1)^n + \sum \Theta_s(x_0 f(x)), \tag{40}$$

la somme étant étendue aux $x_0 \in k_s^*$ et aux $x \in (k_s^*)^n$.

Ecrivons alors $\mathrm{X}_0 f(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ comme somme de monômes $\sum_{i=1}^{j} a_i \mathrm{X}^{w_i}$, où X désigne maintenant $(\mathrm{X}_0, \ldots, \mathrm{X}_n)$, et où les a_i appartiennent à $\mathbf{F}_p$. On peut écrire (40) sous la forme :

$$p^s \mathrm{N}_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} \prod_{i=1}^{j} \Theta_s(a_i x^{w_i}). \tag{41}$$

Soit $\mathrm{A}_i \in \mathbf{Z}_p$ le représentant multiplicatif de a_i. Si celui de x est y, celui de $a_i x^{w_i}$ est $\mathrm{A}_i y^{w_i}$. En combinant (38) et (41) on peut donc écrire :

$$p^s \mathrm{N}_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} \prod_{i=1}^{j} \prod_{j=0}^{s-1} \Theta(\mathrm{A}_i x^{p^j w_i}). \tag{42}$$

Posons maintenant :

$$\mathrm{G}(\mathrm{X}) = \prod_{i=1}^{j} \Theta(\mathrm{A}_i \mathrm{X}^{w_i}). \tag{43}$$

En portant dans (42), on trouve :

$$p^s \mathrm{N}_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} \mathrm{G}(x) \cdot \mathrm{G}(x^p) \cdots \mathrm{G}(x^{p^{s-1}}). \tag{44}$$

En utilisant l'inégalité (22) on voit tout de suite que $\Theta(\mathrm{A}_i \mathrm{X}^{w_i})$ vérifie la condition (29) du § 4, et il en est donc de même de la série G. En lui appliquant la proposition 4, avec $q = p$, et en portant dans (44), on obtient :

$$p^s \mathrm{N}_s = (p^s - 1)^n + (p^s - 1)^{n+1} \mathrm{Tr}(\Psi^s), \tag{45}$$

ou encore :

$$p^s \mathrm{N}_s = \sum_{i=0}^{n} (-1)^i \binom{n}{i} p^{s(n-i)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} p^{s(n+1-i)} \mathrm{Tr}(\Psi^s). \tag{46}$$

Posons alors :

$$\Delta(t) = \det(1 - t\Psi) = \exp\Big(-\sum_{s=1}^{\infty} \mathrm{Tr}(\Psi^s) \frac{t^s}{s}\Big), \tag{47}$$

cf. prop. 5.

En multipliant (46) par t^s/s et en ajoutant les équations ainsi obtenues, on obtient finalement :

$$\mathrm{Z_V}(pt) = \prod_{i=0}^{i=n} (1 - p^{n-i}t)^{(-1)^{i+1}\binom{n}{i}} \prod_{i=0}^{i=n+1} \Delta(p^{n+1-i}t)^{(-1)^{i+1}\binom{n+1}{i}} \tag{48}$$

Comme la série Δ converge dans tout le plan Ω (prop. 5), la formule (48) montre bien que $\mathrm{Z_V}(t)$ est méromorphe dans tout le plan, ce qui achève la démonstration.

Bibliographie

[1] E. Borel, *Sur une application d'un théorème de M. Hadamard*, Bull. Sc. Math., 2e série **18** (1894), 22–25.

[2] J. Delsarte, *Nombre de solutions des équations polynomiales sur un corps fini*, Sém. Bourbaki 1950/51, exposé n° 39.

[3] B. Dwork, *Norm residue symbol in local number fields*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 180–190.

[4] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. of Math. **82** (1960), 631–648.

[5] A. Weil, *Number of solutions of equations in finite fields*, Bull. A.M.S. **55** (1949), 497–508.

Séminaire Bourbaki mai 1960
1959-60, exposé n° 204

REVÊTEMENTS RAMIFIÉS DU PLAN PROJECTIF

d'après S. Abhyankar

§ 1. Résultats classiques

Commençons par rappeler l'énoncé du « théorème d'existence de Riemann-Enriques » :

Théorème 1. — *Soit* V *une variété algébrique, définie sur le corps* **C** *des nombres complexes, et soit* $\pi : V' \to V$ *un revêtement fini* (au sens topologique) *de* V. *Il existe alors sur* V' *une structure algébrique et une seule qui soit compatible avec la structure analytique de* V', *et qui soit telle que* π *soit un morphisme* (algébrique).

(De façon plus imagée : tout revêtement fini d'une variété algébrique est algébrique.)

Noter que *l'on ne suppose* pas V projective ; au contraire, on s'intéresse particulièrement au cas où $V = W - F$, W étant projective et F une sous-variété de W ; le théorème 1 montre alors que les sous-groupes d'indice fini de $\pi_1(W - F)$ correspondent aux revêtements connexes $W' \to W$ qui sont non ramifiés en dehors de F. Lorsque W est la droite projective (resp. le plan projectif), c'est bien là le théorème d'existence de Riemann (resp. d'Enriques).

Il n'est pas question d'exposer ici la démonstration du théorème 1. Indiquons seulement que, si V est normale, il se déduit de deux résultats de Grauert-Remmert ([3], th. 1, et [4], th. 32), et que le cas général se ramène au cas normal grâce à la théorie de la descente de Grothendieck (cf. [5], p. 10 et p. 11).

Le théorème 1 montre quel intérêt il y a (même d'un point de vue purement algébrique) à déterminer le groupe $\pi_1(V)$. Cette détermination est facile lorsque $\dim(V) = 1$. Il n'en est plus de même en dimension 2. Le cas le plus

étudié est celui où $V = \mathbf{P}_2 - C$, C étant une courbe du plan $\mathbf{P}_2$. Une méthode générale permettant d'obtenir générateurs et relations pour $\pi_1(\mathbf{P}_2 - C)$ a été donnée par VAN KAMPEN (cf. ZARISKI, [8], Chap. VIII). De nombreux cas particuliers ont été étudiés par ZARISKI, CHISINI, etc. Le résultat le plus frappant est sans doute le suivant, dû à ZARISKI ([8], p. 163).

THÉORÈME 2. — *Si la courbe* C *n'a que des points simples ou des points doubles à tangentes distinctes, le groupe* $\pi_1(\mathbf{P}_2 - C)$ *est commutatif.*

[Noter que, une fois que l'on sait que $\pi_1(\mathbf{P}_2 - C)$ est commutatif, des arguments homologiques donnent immédiatement sa structure : si C est réunion de courbes irréductibles de degré $d_1, \ldots, d_r$, le groupe $\pi_1(\mathbf{P}_2 - C)$ est quotient de $\mathbf{Z}^r$ par le sous-groupe engendré par l'élément $(d_1, \ldots, d_r)$.]

ZARISKI commence par vérifier cet énoncé lorsque C et formé d'un certain nombre de droites (ce n'est pas aussi facile que l'on pense !), et passe de là au
1 cas général par un argument de « dégénérescence » ; j'ignore quel travail serait nécessaire pour rendre sa démonstration complète.

L'un des objectifs du mémoire d'ABHYANKAR [2] est de démontrer un résultat analogue au théorème 2 en géométrie algébrique de caractéristique quelconque ; on verra d'ailleurs qu'il n'y parvient que partiellement.

§ 2. Revêtements modérément ramifiés

A partir de maintenant, nous nous plaçons en géométrie algébrique sur un corps algébriquement clos k de caractéristique quelconque ; on désigne par p l'exposant caractéristique de k (au sens de BOURBAKI).

2 Soit V une variété normale ; nous appellerons *revêtement* de V tout morphisme $\pi : V' \to V$, où V' est normale, de même dimension que V, le morphisme π étant « fini » au sens de Grothendieck (c'est-à-dire propre, et à fibres finies). Si R(V) et R(V') sont les corps de fonctions rationnelles de V et V', R(V') est extension finie de R(V) ; le degré [R(V') : R(V)] est appelé le degré du revêtement. Inversement, toute extension finie K de R(V) est de la forme R(V') comme on le voit en prenant pour V' la normalisée de V dans K.

Un revêtement $\pi : V' \to V$ est dit *galoisien* si R(V') est extension galoisienne de R(V) ; le groupe de Galois G de R(V')/R(V) opère alors sur V', et V s'identifie à V'/G. Dans la suite, nous ne considérerons *que des revêtements galoisiens.*

Soit donc $\pi : V' \to V$ un tel revêtement, et soit n son degré. On dit que V' est *non ramifié* en un point $P \in V$ si $\pi^{-1}(P)$ est formé de n points distincts.

L'ensemble des points de ramification de V' est une sous-variété Δ de V distincte de V. Lorsque V est *non singulière*, toutes les composantes irréductibles de Δ sont de codimension 1 : c'est le « théorème de pureté », voir plus loin, n° 4.1.

Soit C une sous-variété irréductible de codimension 1 de V et soit C' une composante irréductible de $\pi^{-1}(C)$; les anneaux locaux A et A' de C et C' sont des anneaux de valuation discrète, et la théorie de la ramification (cf. [7], chapitre V, par exemple) s'applique. En particulier, on peut définir le *sous-groupe d'inertie* $I_{C'}$ du groupe de Galois G ; c'est l'ensemble des $s \in G$ tels que $s(Q) = Q$ pour tout $Q \in C'$. Nous dirons que le revêtement considéré est *modérément ramifié* (« tamely ramified ») en C si $I_{C'}$ est d'ordre premier à p (condition indépendante du choix de C' au-dessus de C). D'après la théorie de la ramification, le groupe $I_{C'}$ est alors *cyclique*.

Soit C une sous-variété irréductible de V. Un revêtement $V' \to V$ sera dit modérément ramifié sur (V, C) si V' est non ramifié en dehors de C, et est modérément ramifié pour toute sous-variété irréductible de codimension 1 de V (il suffit d'ailleurs de le vérifier pour celles qui sont contenues dans C). Soit Ω une extension algébriquement close de R(V) ; les sous-corps K de Ω, finis sur V, et tels que le revêtement correspondant soit modérément ramifié sur (V, C) forment une famille filtrante croissante ; leur réunion est une extension galoisienne (infinie en général) de R(V), dont le groupe de Galois sera noté $\pi_1^t(V, C)$. Lorsque $C = \varnothing$, on retrouve le groupe fondamental de V, au sens de GROTHENDIECK ; lorsque le corps est le corps $\mathbf{C}$ des complexes, le théorème 1 montre que le groupe $\pi_1^t(V, C)$ n'est autre que le *complété* du groupe fondamental usuel $\pi_1(V - C)$ pour la topologie des sous-groupes d'indice fini.

§ 3. Revêtements modérément ramifiés de certaines surfaces

Nous allons maintenant faire une série d'hypothèses restrictives sur le couple (V, C).

(i) V *est une surface non singulière.*

(Le cas général peut souvent se ramener à celui-là, en coupant par des hyperplans et en appliquant le théorème de Bertini. Cette hypothèse n'est donc pas aussi restrictive qu'elle le paraît.)

(ii) *La sous-variété* C *est une courbe dont tous les points sont, ou bien des points simples, ou bien des points doubles ordinaires. De plus, toutes les composantes irréductibles de* C *sont non singulières.*

(Cette hypothèse est *plus forte* que celle du théorème 2. Par exemple, si C est irréductible, elle signifie que C est non singulière.)

Soit $\pi : V' \to V$ un revêtement modérément ramifié sur (V, C). Soient C_α les composantes irréductibles de C, et soient C'_α leurs images réciproques par π. Une étude locale des revêtements modérément ramifiés (cf. n° 4.2) montre que les C'_α sont des courbes *non singulières*, éventuellement réductibles.

(iii) *La variété* V *est projective, et, pour toute composante irréductible* C_α *de* C*, la dimension de la série linéaire complète* $|C_\alpha|$ *est* $\geqslant 2$.

Le fait que $|C_\alpha|$ soit de dimension $\geqslant 2$ et contienne un diviseur irréductible entraîne qu'elle n'a pas de composante fixe, et qu'elle n'est pas « composée avec un pinceau » (autrement dit, elle définit une application rationnelle de V dans un espace projectif dont l'image est de dimension 2). Il en est donc de même de la série formée des $\pi^{-1}(D)$, $D \in |C_\alpha|$. En appliquant à cette série linéaire le théorème de Bertini et le théorème de connexion, on voit que tous les $\pi^{-1}(D)$ sont connexes. Ceci s'applique notamment à $D = C_\alpha$, et comme $\pi^{-1}(C_\alpha)$ a pour support C'_α, on voit que C'_α est connexe. Comme on sait d'autre part que c'est une courbe non singulière, on en conclut que c'est une *courbe irréductible*. Soit I_α le groupe d'inertie de C'_α dans le groupe de Galois G ; c'est un sous-groupe cyclique invariant de G. Si $\alpha \neq \beta$, les hypothèses faites sur $|C_\alpha|$ et $|C_\beta|$ montrent que C_α et C_β se rencontrent en un point au moins ; une étude locale du revêtement en ce point (cf. n° 4.2) montre alors que I_α et I_β *commutent*. Soit I le sous-groupe de G engendré par les I_α ; c'est un sous-groupe commutatif, et invariant, du groupe G. Soit $V'' = V'/I$; c'est un revêtement modérément ramifié sur (V, C), de groupe de Galois G/I ; de plus, la construction même de V'' montre que les groupes d'inertie des C_α dans V'' sont nuls, c'est-à-dire qu'aucun des C_α n'est contenu dans le lieu de ramification Δ de $V'' \to V$. D'après le théorème de pureté, on a $\Delta = \varnothing$, autrement dit $V'' \to V$ est *non ramifié*. En passant à la limite sur V', on obtient le résultat suivant :

THÉORÈME 3. — *Si le couple* (V, C) *vérifie les hypothèses* (i), (i), (iii)*, le quotient de* $\pi_1^t(V, C)$ *par le sous-groupe commutatif invariant* I *est isomorphe au groupe* $\pi_1^t(V, \varnothing)$.

(Ce théorème est essentiellement celui que démontre ABHYANKAR dans [2], bien qu'il ne l'énonce pas.)

COROLLAIRE. — *Si l'on suppose en outre que* V *est simplement connexe* (c'est-à-dire ne possède aucun revêtement non ramifié de degré > 1)*, le groupe* $\pi_1^t(V, C)$ *est commutatif.*

En effet, l'hypothèse « V simplement connexe » signifie que le groupe $\pi_1^t(V, \varnothing)$ est trivial.

Le corollaire ci-dessus s'applique notamment au couple $(\mathbf{P}_2, \mathrm{C})$, *où* $\mathbf{P}_2$ *désigne le plan projectif, et* C *une courbe vérifiant la condition* (ii). En effet, tout espace projectif est simplement connexe (voir n° 4.3), et si C_α est une composante connexe de C de degré d_α, la dimension de la série linéaire $|\mathrm{C}_\alpha|$ est égale à $d_\alpha(d_\alpha+3)/2$ qui est $\geqslant 2$.

Remarque. — 1) Une fois que l'on sait que $\pi_1^t(\mathrm{V}, \mathrm{C})$ est commutatif, il n'est pas difficile de le déterminer complètement, au moyen de la théorie de Kummer. Lorsque $\mathrm{V} = \mathbf{P}_2$, on trouve, comme on pouvait s'y attendre, le complété du groupe analogue sur $\mathbf{C}$ pour la topologie des sous-groupes d'indice fini et premier à p.

2) Le corollaire au théorème 3 est démontré dans [2] sans supposer que les C_α soient non singulières, mais la démonstration est incorrecte. Il ne semble donc pas que l'on puisse obtenir une véritable généralisation du théorème 2 par les méthodes d'Abhyankar; c'est bien dommage. [On peut toutefois traiter le 3
cas où les C_α n'ont « pas trop » de points multiples, grâce à des éclatements convenables. Cf. une série de mémoires d'Abhyankar en cours de publication.]

§ 4. Indications sur les démonstrations

4.1. Théorème de pureté. — Il a été énoncé tout d'abord par Abhyankar [1], avec une démonstration incorrecte, attribuée à Zariski. Une démonstration simple (et correcte) a été publiée ensuite par Zariski [9].

Le théorème garde un sens pour des *schémas* quelconques. Sous cette forme, 4
il vient d'être démontré par Nagata [6], s'appuyant lui-même sur un résultat de Chow.

4.2. Étude locale des revêtements modérément ramifiés. — On s'appuie sur le :

Lemme d'Abhyankar. — *Soient* V' *et* W *deux revêtements modérément ramifiés de* (V, C) ; *pour toute composante irréductible* C_α *de codimension* 1 *de* C, *soit* i_α (*resp.* j_α) *l'ordre du groupe d'inertie d'une composante irréductible* C'_α (*resp.* D_α) *de l'image réciproque de* C_α ; *supposons* : 5

a) *que* W *est non singulière,*

b) *que* j_α *est multiple de* i_α *pour tout* α.

Si alors on note W' *le revêtement commun de* V' *et* W *correspondant au composé des corps* $\mathrm{R}(\mathrm{V}')$ *et* $\mathrm{R}(\mathrm{W})$, W' *est un revêtement non ramifié de* W.

Soit G le groupe de Galois de $\mathrm{V}' \to \mathrm{V}$, soit H celui de $\mathrm{W} \to \mathrm{V}$, et soit S celui de $\mathrm{W}' \to \mathrm{V}$; le groupe S contient deux sous-groupes invariants T et T'

tels que $S/T = G$, $S/T' = H$, et l'on a $T \cap T' = \{e\}$. Soit I_α le groupe d'inertie d'une composante irréductible E_α de l'image réciproque de C_α dans W' ; le groupe I_α se plonge dans le produit des groupes correspondants dans V' et W, groupes qui sont cycliques d'ordre i_α et j_α respectivement. Il en résulte que I_α est d'ordre premier à p, donc cyclique, et comme il se projette *sur* le groupe d'inertie de $W \to V$, la condition (b) montre qu'il est isomorphe à ce dernier. On a donc $I_\alpha \cap T' = \{e\}$, ce qui montre qu'aucun des D_α n'est contenu dans l'ensemble de ramification de $W' \to W$; en appliquant le théorème de pureté, on en conclut bien que $W' \to W$ est non ramifié.

Revenons maintenant à la situation du § 3 ; on va étudier $V' \to V$ au voisinage d'un point $P \in C$. Traitons le cas où P est un point double de C (le cas d'un point simple étant analogue). La question étant locale, on peut supposer que C est défini en P par l'équation $xy = 0$, où x, y forment un système régulier de paramètres. On prendra alors pour W la sous-variété de $V \times k^2$ définie par les équations $x'^n = x$, $y'^m = y$, n, m étant deux entiers premiers à p. On constate facilement que, quitte à restreindre encore V, on trouve pour W une variété non singulière, formant un revêtement modérément ramifié sur (V, C), les ordres des groupes d'inertie étant respectivement n et m, et le groupe de Galois étant $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} = H$. On peut donc appliquer le lemme d'Abhyankar à V' et W, pourvu que n et m soient choisis assez grands. On en tire :

Si $P \in V$, $P' \in V'$, $Q \in W$, $Q' \in W'$ sont des points qui se correspondent, le complété de l'anneau local $\mathscr{O}_Q$ s'identifie à celui de l'anneau local $\mathscr{O}_{Q'}$. Comme on a :

$$\widehat{\mathscr{O}}_{Q'} \supset \widehat{\mathscr{O}}_{P'} \supset \widehat{\mathscr{O}}_P,$$

et que tous ces anneaux sont intégralement clos, on voit que $\widehat{\mathscr{O}}_{P'}$ *s'identifie au sous-anneau de* $\widehat{\mathscr{O}}_Q = k[\![x', y']\!]$ fixé par un certain sous-groupe du groupe $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ (ce dernier opérant par $x' \mapsto \varepsilon x'$, $y' \mapsto \zeta y'$, où $\varepsilon^n = \zeta^m = 1$). On obtient ainsi une description complète (du point de vue « formel ») du revêtement $V' \to V$, description qui permet de vérifier sans difficultés les assertions du § 3.

4.3. $\pi_1(\mathbf{P}_n) = 0$**.** — Le théorème de Bertini permet de se ramener au cas $n = 1$. Dans ce cas, si $X \to \mathbf{P}_1$ est un revêtement non ramifié, de degré d, le genre de X étant g, la formule de Hurwitz montre que

$$1 - g = d,$$

d'où $g = 1 - d$, ce qui entraîne nécessairement $d = 1$.

[Variante : montrer qu'un revêtement non ramifié de $\mathbf{P}_n$ définit un revêtement de k^{n+1} ramifié seulement à l'origine, et appliquer le théorème de pureté.]

Bibliographie

[1] S. Abhyankar, *On the ramification of algebraic functions*, Amer. J. of Math. **77** (1955), 575–592.

[2] S. Abhyankar, *Tame coverings and fundamental groups of algebraic varieties, Part I : Branch loci with normal crossings, Applications : theorems of Zariski and Picard*, Amer. J. of Math. **81** (1959), 46–94.

[3] H. Grauert et R. Remmert, *Espaces analytiquement complets*, C.R.A.S. **245** (1957), 882–885.

[4] H. Grauert et R. Remmert, *Komplexe Raüme*, Math. Annalen **136** (1958), 245–318.

[5] A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique, I* : *Généralités, Descente par morphismes fidèlement plats*, Séminaire Bourbaki 1959/60, exposé n° 190.

[6] M. Nagata, *On the purity of branch loci in regular local rings*, Illinois J. of Math. **3** (1959), 328–333.

[7] O. Zariski et P. Samuel, *Commutative Algebra, Vol. 1*, Princeton, Van Nostrand (1958), (The University series in higher Mathematics).

[8] O. Zariski, *Algebraic Surfaces*, New York, Chelsea publishing Company (1948), (Ergebnisse der Mathematik, Band 3, 5); seconde édit. (1971).

[9] O. Zariski, *On the purity of the branch locus of algebraic functions*, Proc. Nat. Acad. Sc. U. S. A. **44** (1958), 791–796.

Séminaire Bourbaki décembre 1960
1960-61, exposé n° 209

GROUPES FINIS À COHOMOLOGIE PÉRIODIQUE

d'après R. Swan

1. Énoncé des résultats

Soit G un groupe fini d'ordre n, et soit k un entier $\geqslant 1$. On dit que la cohomologie de G est *périodique de période* k s'il existe un élément $u \in \mathrm{H}^k(\mathrm{G}, \mathbf{Z})$ d'ordre égal à n. On sait alors (cf. [2], Chap. XII) que, pour tout G-module A, et tout $q \in \mathbf{Z}$, l'application $x \mapsto u \cdot x$ est un isomorphisme de $\widehat{\mathrm{H}}^q(\mathrm{G}, \mathrm{A})$ sur $\widehat{\mathrm{H}}^{q+k}(\mathrm{G}, \mathrm{A})$, ce qui justifie la terminologie. 1

Si G opère librement sur la sphère $\mathbf{S}_{k-1}$ ($k \geqslant 2$), et si les éléments de G respectent l'orientation de $\mathbf{S}_{k-1}$, la cohomologie de G est périodique de période k (cf. [1], exposé 13, ou bien [2], p. 357). On savait peu de choses sur la réciproque (cf. Milnor [5], qui donne un certain nombre de contre-exemples). Les résultats de Swan montrent que, à condition de remplacer les sphères par des « sphères homotopiques », la question devient purement algébrique et peut se traiter à peu près complètement.

De façon précise, considérons une suite exacte de G-modules :

$$(1) \qquad 0 \longrightarrow \mathbf{Z} \longrightarrow \mathrm{P}_{k-1} \longrightarrow \mathrm{P}_{k-2} \longrightarrow \cdots \longrightarrow \mathrm{P}_1 \longrightarrow \mathrm{P}_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,,$$

où les P_i sont des *modules projectifs de type fini* sur l'algèbre $\mathbf{Z}[\mathrm{G}]$ du groupe G. Une telle suite exacte sera appelée une *résolution projective périodique de* $\mathbf{Z}$, de période k. Si tous les P_i sont des modules libres, on dira que c'est une *résolution libre.*

Théorème 1 (Swan [8], th. 4.1). — *Pour qu'il existe une résolution* projective *périodique de* $\mathbf{Z}$*, de période* k*, il faut et il suffit que la cohomologie de* G *soit périodique de période* k*.*

Soit d'autre part X un complexe cellulaire (au sens de J.H.C. WHITEHEAD [9]) sur lequel G opère. Nous dirons que G opère *cellulairement* si les éléments de G permutent les cellules de X.

THÉORÈME 2 (SWAN [8], prop. 3.1). — *Les deux conditions suivantes sont équivalentes* :

(1) *Il existe une résolution* libre *périodique de* $\mathbf{Z}$*, de période* k*.*

(2) *Il existe un complexe cellulaire fini* X*, de dimension* $k-1$*, ayant même type d'homotopie que* $\mathbf{S}_{k-1}$*, sur lequel* G *opère cellulairement, librement, et en conservant l'orientation.*

(Cette dernière hypothèse signifie que G opère trivialement sur $\mathrm{H}_{k-1}(\mathrm{X}, \mathbf{Z})$, qui est isomorphe à $\mathbf{Z}$.)

Le théorème suivant permet de passer des résolutions projectives aux résolutions libres :

THÉORÈME 3 (SWAN [8], corollaire 5.1). — *Supposons qu'il existe une résolution* projective *périodique de* $\mathbf{Z}$*, de période* k*. Il existe alors un entier* $d \geqslant 1$ *et une résolution* libre *périodique de* $\mathbf{Z}$*, de période* dk*.*

En combinant ces trois théorèmes, on obtient :

COROLLAIRE. — *Si la cohomologie de* G *est périodique de période* k*, il existe un complexe cellulaire fini* X*, de dimension* $dk-1$*, ayant même type d'homotopie que* $\mathbf{S}_{dk-1}$*, sur lequel* G *opère cellulairement, librement, et en conservant l'orientation.*

J'ignore s'il est possible de prendre $d = 1$ (c'est improbable). SWAN montre que l'on peut en tout cas prendre pour d le pgcd de $\varphi(n)$ et de n; on peut même remplacer $\varphi(n)$ par $\varphi(m)$, où m est le ppcm des ordres des éléments de G.

2. Résolutions libres, équivalences, etc.

Tous les G-modules considérés ci-après sont supposés *libres de type fini sur* $\mathbf{Z}$. Si P est un tel G-module, les propriétés suivantes sont équivalentes (cf. RIM [6]) :

a) P est faiblement injectif ([2], p. 197),

b) P est faiblement projectif (idem),

c) P est cohomologiquement trivial; i.e. on a $\widehat{\mathrm{H}}^q(\mathrm{G}', \mathrm{P}) = 0$ pour tout sous-groupe G' de G et tout $q \in \mathbf{Z}$,

d) P est $\mathbf{Z}[G]$-projectif.

Soient A et B deux G-modules et soit $f : A \to B$ une application G-linéaire. Nous dirons que f est *homotope à zéro*, s'il existe une application $\mathbf{Z}$-linéaire $g : A \to B$ telle que $f = Ng$, où N désigne la norme. Il revient au même de dire que, pour toute suite exacte $B' \to B \to 0$ de G-modules, il existe $f' : A \to B'$ relevant f (cf. ECKMANN [3]). Les *classes d'homotopie* d'applications de A dans B forment un groupe $\pi_0(A, B)$, qui s'identifie à $\hat{H}^0(G, \mathrm{Hom}_{\mathbf{Z}}(A, B))$. Une application f est appelée une *équivalence d'homotopie* si sa classe d'homotopie est inversible.

Lemme 1. — *Soit* $f : A \to B$ *une application* G*-linéaire* (A et B étant toujours supposés libres de type fini sur $\mathbf{Z}$). *Les trois propriétés suivantes sont équivalentes* :

(i) f *est une équivalence d'homotopie.*

(ii) *Il existe deux modules projectifs* P *et* Q *et un isomorphisme* $F : A \oplus P \to B \oplus Q$ *tels que le composé*

$$A \longrightarrow A \oplus P \xrightarrow{F} B \oplus Q \longrightarrow B$$

soit égal à f.

(iii) *Pour tout sous-groupe* G' *de* G *et tout* $q \in \mathbf{Z}$, *l'application de* $\hat{H}^q(G', A)$ *dans* $\hat{H}^q(G', B)$ *définie par* f *est un isomorphisme.*

Il est clair que (ii) entraîne (i). On voit facilement que (i) entraîne (iii). Montrons que (iii) entraîne (ii) :

Écrivons B comme quotient d'un module projectif P, et soit Q le noyau de l'homomorphisme surjectif $A \oplus P \to B$. En utilisant (iii), on voit que Q est cohomologiquement trivial, donc projectif. De plus, comme B est $\mathbf{Z}$-libre, Q est $\mathbf{Z}$-facteur direct dans $A \oplus P$; comme Q est faiblement injectif, il est « $(\mathbf{Z}[G], \mathbf{Z})$-injectif » au sens de HOCHSCHILD (cf. [4]), donc il est facteur direct dans $A \oplus P$ comme G-module, et $A \oplus P$ s'identifie à $B \oplus Q$, c.q.f.d.

Exemple. — On a $\pi_0(\mathbf{Z}, \mathbf{Z}) \simeq \mathbf{Z}/n\mathbf{Z}$; les classes d'homotopie $\mathbf{Z} \to \mathbf{Z}$ qui sont des équivalences forment un groupe isomorphe au groupe multiplicatif de $\mathbf{Z}/n\mathbf{Z}$.

On dit que deux G-modules A et B ont *même type d'homotopie* s'il existe une équivalence d'homotopie $A \to B$, et on écrit $A \sim B$. En particulier, $P \sim 0$ signifie que P est projectif. Comme l'ont remarqué ECKMANN et HILTON (cf. [3]), la situation est tout à fait analogue à celle que l'on rencontre en topologie; le « décalage » correspond à la formation de « l'espace des lacets », et est unique à homotopie près. De façon précise :

Lemme 2. — Soient

$$0 \longrightarrow A \longrightarrow P_{i-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow B \longrightarrow 0 \tag{2}$$

$$0 \longrightarrow A' \longrightarrow P'_{i-1} \longrightarrow \cdots \longrightarrow P'_0 \longrightarrow B' \longrightarrow 0 \tag{3}$$

deux suite exactes de G*-modules, où les* P_α *et les* P'_α *sont projectifs. Ces suites exactes définissent un isomorphisme de* $\pi_0(A, A')$ *sur* $\pi_0(B, B')$*. En particulier, toute équivalence d'homotopie* $f_B : B \to B'$ *définit une équivalence d'homotopie* $f_A : A \to A'$ *déterminée à homotopie près.*

La démonstration est immédiate.

[Deux homomorphismes f_A et f_B se correspondent si et seulement si l'on peut les prolonger en un homomorphisme de la suite exacte (2) dans la suite exacte (3).]

Le lemme 2 montre en particulier que, si $B = B'$, on a $A \sim A'$. Réciproquement :

Lemme 3. — Soit

$$0 \longrightarrow A \longrightarrow P_{i-1} \xrightarrow{\partial} P_{i-2} \xrightarrow{\partial} \cdots \longrightarrow P_0 \longrightarrow B \longrightarrow 0 \tag{2}$$

une suite exacte de G*-modules, avec* $i \geqslant 2$*. Soit* $A' \sim A$*, et soient* P *et* Q *des modules projectifs tels que* $A \oplus P = A' \oplus Q$*. Il existe alors une suite exacte de la forme* :

$$0 \longrightarrow A' \longrightarrow P_{i-1} \oplus P \xrightarrow{\partial + r} P_{i-2} \oplus Q \xrightarrow{(\partial, 0)} P_{i-3} \longrightarrow \cdots \longrightarrow B' \longrightarrow 0\,, \tag{3}$$

qui coïncide avec (2) *à partir de* P_{i-3}*.*

Puisque B et les P_i sont $\mathbf{Z}$-libres, A est facteur direct dans P_{i-1} comme $\mathbf{Z}$-module, et il en est de même de $A \oplus P = A' \oplus Q$ dans $P_{i-1} \oplus P$. Utilisant le fait que Q est faiblement injectif, on en conclut qu'il existe une rétraction $r : P_{i-1} \oplus P \to Q$, qui est un G-homomorphisme, et qui s'annule sur A'. Il est clair que l'application

$$\partial + r : P_{i-1} \oplus P \to P_{i-2} \oplus Q$$

a pour noyau A', et pour image le noyau de $(\partial, 0)$. D'où la suite exacte (3).

3. Démonstration du théorème 1

Si $\mathbf{Z}$ possède une résolution périodique, de période k, l'opérateur cobord itéré $\delta^k : \widehat{H}^q(G, \mathbf{Z}) \longrightarrow \widehat{H}^{q+k}(G, \mathbf{Z})$ est un isomorphisme. En particulier, prenant

$q = 0$, on voit que $\mathrm{H}^k(\mathrm{G}, \mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}$, ce qui montre que la cohomologie de G est périodique de période k.

Réciproquement, supposons cette propriété vérifiée, et considérons une suite exacte

$$0 \longrightarrow \mathrm{A} \longrightarrow \mathrm{P}_{k-1} \longrightarrow \cdots \longrightarrow \mathrm{P}_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,, \tag{4}$$

où les P_i sont projectifs (de type fini, comme toujours). Tenant compte de la périodicité de la cohomologie de G, on voit qu'il existe dans $\widehat{\mathrm{H}}^0(\mathrm{G}, \mathrm{A})$ une classe v telle que $x \mapsto v \cdot x$ soit un isomorphisme de $\widehat{\mathrm{H}}(\mathrm{G}, \mathbf{Z})$ sur $\widehat{\mathrm{H}}(\mathrm{G}, \mathrm{A})$; de plus, si G' est un sous-groupe de G et si $v' \in \widehat{\mathrm{H}}^0(\mathrm{G}', \mathrm{A})$, est la restriction de v, la classe v' jouit de la même propriété. On peut représenter v par une G-application

$$f : \mathbf{Z} \longrightarrow \mathrm{A}\,,$$

et le lemme 1 montre que c'est une équivalence d'homotopie. D'après le lemme 3 (applicable car $k \geqslant 2$ si G n'est pas réduit à $\{1\}$), il existe une suite exacte

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathrm{P}'_{k-1} \longrightarrow \cdots \longrightarrow \mathrm{P}'_0 \longrightarrow \mathbf{Z} \longrightarrow 0 \tag{5}$$

où les P'_i sont projectifs (et même égaux aux P_i pour $i < k-2$). On a donc bien construit une résolution projective périodique de $\mathbf{Z}$, de période k.

4. Classes de modules projectifs

Deux modules projectifs P et P′ sont dits *équivalents* s'il existe deux modules libres L et L′ tels que $\mathrm{P} \oplus \mathrm{L}$ soit isomorphe à $\mathrm{P}' \oplus \mathrm{L}'$. Les classes de modules projectifs (pour la relation d'équivalence précédente) forment un groupe abélien que l'on notera $\mathrm{K}_0(\mathrm{G})$; l'image dans $\mathrm{K}_0(\mathrm{G})$ d'un module projectif P sera noté $[\mathrm{P}]$. On a $[\mathrm{P}] = 0$ si et seulement s'il existe un module libre L tel que $\mathrm{P} \oplus \mathrm{L}$ soit libre (on ignore si cette condition entraîne que P soit libre — c'est vrai si G est commutatif). 2

Soient maintenant A et B deux G-modules (vérifiant les conditions du n° 2), et soit $f : \mathrm{A} \to \mathrm{B}$ une équivalence d'homotopie. D'après le lemme 1, il existe des modules projectifs P et Q, et un isomorphisme $\mathrm{F} : \mathrm{A} \oplus \mathrm{P} \to \mathrm{B} \oplus \mathrm{Q}$ tels que $\mathrm{pr}_1(\mathrm{F}(a, 0)) = f(a)$.

Lemme 4. — *L'élément* $[\mathrm{P}] - [\mathrm{Q}]$ *ne dépend que de* f.

Soient $(\mathrm{P}', \mathrm{Q}', \mathrm{F}')$ vérifiant les mêmes relations que ci-dessus. On va montrer que $\mathrm{P}' \oplus \mathrm{Q}$ est isomorphe à $\mathrm{P} \oplus \mathrm{Q}'$, ce qui établira le lemme. Soient $g : \mathrm{A} \to \mathrm{Q}$

et $g' : A \to Q'$ les applications définies par F et F′. On a la suite exacte :

$$0 \longrightarrow A \xrightarrow{(f,g)} B \oplus Q \longrightarrow P \longrightarrow 0\,, \tag{6}$$

ainsi qu'une suite exacte analogue avec Q' et P'. Définissons alors un module R au moyen de la suite exacte :

$$0 \longrightarrow A \xrightarrow{(f,g,g')} B \oplus Q \oplus Q' \longrightarrow R \longrightarrow 0\,. \tag{7}$$

La suite exacte (7) s'envoie de façon naturelle sur la suite exacte (6), d'où la suite exacte :

$$0 \longrightarrow Q' \longrightarrow R \longrightarrow P \longrightarrow 0\,. \tag{8}$$

Comme P est projectif, on en tire $R = P \oplus Q'$; de même, $R = P' \oplus Q$, c.q.f.d.

Nous noterons (f) l'élément $[P] - [Q]$. On vérifie tout de suite que $(fg) = (f) + (g)$, et que (f) ne dépend que de la classe d'homotopie de f.

Lemme 5. — *Soit* $f : A \to B$ *une équivalence d'homotopie. Pour que* $(f) = 0$, *il faut et il suffit qu'il existe des modules libres* L *et* M *et un isomorphisme* $F : A \oplus L \to B \oplus M$ *tels que le composé*

$$A \longrightarrow A \oplus L \longrightarrow B \oplus M \longrightarrow B$$

soit égal à f.

La condition est évidemment suffisante. Montrons qu'elle est nécessaire. On choisit un isomorphisme $A \oplus P \to B \oplus Q$, compatible avec f, et où P et Q sont projectifs. Par hypothèse, il existe des modules libres L_1 et L_2 tels que $P \oplus L_1 = Q \oplus L_2$; d'autre part, il existe un module projectif P' et un module libre L_3 tels que $P \oplus P' = L_3$. On en déduit un isomorphisme

$$F : A \oplus P \oplus P' \oplus L_2 \longrightarrow B \oplus Q \oplus P' \oplus L_2\,.$$

Comme $P \oplus P' \oplus L_2 = L_3 \oplus L_2$ est libre, de même que $Q \oplus P' \oplus L_2 = P \oplus L_1 \oplus P' = L_1 \oplus L_3$, le lemme est démontré.

Deux modules A et B tels qu'il existe une application f vérifiant les conditions du lemme 5 seront dits strictement équivalents, et on écrira $A \sim_L B$.

Lemme 6. — *Considérons un diagramme commutatif* :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0\,, \end{array} \tag{9}$$

où les lignes sont exactes, et où f, f', f'' *sont des équivalences d'homotopie. On a alors* $(f) = (f') + (f'')$.

Quitte à ajouter à A, A′ et A″ des modules libres [ce qui ne modifie pas (f), (f') et (f'')], on peut supposer que f, f', f'' sont surjectifs. Soient Q, Q′, Q″ leurs noyaux. Ils sont projectifs, et forment une suite exacte :

$$0 \longrightarrow \mathrm{Q}' \longrightarrow \mathrm{Q} \longrightarrow \mathrm{Q}'' \longrightarrow 0\,.$$

On a donc $[\mathrm{Q}] = [\mathrm{Q}'] + [\mathrm{Q}'']$. Comme $(f) = -[\mathrm{Q}]$, $(f') = -[\mathrm{Q}']$, $(f'') = -[\mathrm{Q}'']$, on a bien $(f) = (f') + (f'')$.

En itérant, on en déduit :

Lemme 7. — *Considérons un diagramme commutatif* :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{A}_n & \longrightarrow & \mathrm{A}_{n-1} & \longrightarrow \cdots \longrightarrow & \mathrm{A}_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_0} & & \\ 0 & \longrightarrow & \mathrm{B}_n & \longrightarrow & \mathrm{B}_{n-1} & \longrightarrow \cdots \longrightarrow & \mathrm{B}_0 & \longrightarrow & 0\ , \end{array} \tag{10}$$

où les lignes sont exactes, et où les f_i sont des équivalences d'homotopie. On a alors $\sum(-1)^i(f_i) = 0$.

Corollaire. — *Soient*

$$0 \longrightarrow \mathrm{A}_n \longrightarrow \mathrm{L}_{n-1} \longrightarrow \cdots \longrightarrow \mathrm{L}_0 \longrightarrow \mathrm{A}_0 \longrightarrow 0 \tag{11}$$

$$0 \longrightarrow \mathrm{B}_n \longrightarrow \mathrm{M}_{n-1} \longrightarrow \cdots \longrightarrow \mathrm{M}_0 \longrightarrow \mathrm{B}_0 \longrightarrow 0 \tag{12}$$

deux suites exactes, où les L_i et les M_i sont libres. Si A_0 est strictement équivalent à B_0, alors A_n est strictement équivalent à B_n (et réciproquement).

Soit $f_0 : \mathrm{A}_0 \to \mathrm{B}_0$ une équivalence d'homotopie telle que $(f_0) = 0$. On peut trouver des $g_i : \mathrm{L}_i \to \mathrm{M}_i$ et $f_n : \mathrm{A}_n \to \mathrm{B}_n$ définissant un homomorphisme de (11) dans (12). On a $(g_i) = 0$, et le lemme 7 donne $(f_n) = (-1)^{n+1}(f_0)$, d'où le corollaire.

Remarque. — Le corollaire ci-dessus peut aussi se démontrer, comme le fait Swan, à partir du « lemme de Schanuel », dont voici l'énoncé : Si $\mathrm{P}/\mathrm{R} = \mathrm{P}'/\mathrm{R}'$, avec P, P′ projectifs, on a $\mathrm{R} \oplus \mathrm{P}' = \mathrm{R}' \oplus \mathrm{P}$.

5. Démonstration du théorème 2

Supposons d'abord que G opère cellulairement, librement, et en conservant l'orientation, sur un complexe cellulaire fini S ayant même homologie que $\mathbf{S}_{k-1}$ (il n'est pas nécessaire de supposer X simplement connexe, ni même de dimension $k-1$). Supposons $\mathrm{G} \neq \{1\}$ (ce qui n'est guère une restriction!). La formule des points fixes montre alors que k est *pair*.

Soit $N = \dim X$; pour $0 \leqslant i \leqslant N$, soit C_i le groupe des chaînes de dimension i de X (au sens cellulaire), et soit $Z_i \subset C_i$ le sous-groupe des cycles. Ces groupes sont des G-modules, et, puisque G opère librement sur X, les C_i sont des G-modules *libres.* On a les deux suites exactes :

$$0 \longrightarrow C_N \longrightarrow C_{N-1} \longrightarrow \cdots \longrightarrow C_k \longrightarrow Z_{k-1} \longrightarrow \mathbf{Z} \longrightarrow 0 \tag{13}$$

$$0 \longrightarrow Z_{k-1} \longrightarrow C_{k-1} \longrightarrow \cdots \longrightarrow C_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,. \tag{14}$$

Si $B_{k-1} \subset Z_{k-1}$ désigne le groupe des bords de dimension $k-1$, la suite exacte (13) se décompose en les deux suites exactes :

$$0 \longrightarrow C_N \longrightarrow C_{N-1} \longrightarrow \cdots \longrightarrow C_k \longrightarrow B_{k-1} \longrightarrow 0 \tag{15}$$

$$0 \longrightarrow B_{k-1} \longrightarrow Z_{k-1} \xrightarrow{h} \mathbf{Z} \longrightarrow 0\,. \tag{16}$$

La suite (15) montre que B_{k-1} est projectif, et que $[B_{k-1}] = 0$ dans $K_0(G)$. En utilisant (16), on voit alors que h est une équivalence d'homotopie et que $(h) = 0$. Donc $Z_{k-1} \sim_L \mathbf{Z}$. En appliquant le lemme 3 à (14), on obtient une nouvelle suite exacte :

$$0 \longrightarrow \mathbf{Z} \longrightarrow C'_{k-1} \longrightarrow \cdots \longrightarrow C'_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,, \tag{17}$$

où les C'_i sont libres (et en fait égaux aux C_i si $i < k-2$). C'est la résolution libre périodique cherchée.

Réciproquement, supposons qu'il existe une telle résolution. Si G est cyclique, on sait qu'il peut opérer librement sur les sphères de dimension impaire. Supposons donc G non cyclique, ce qui entraîne que k est pair ([2], p. 261), et $\geqslant 4$ (si $k = 2$, le groupe $H^2(G, \mathbf{Z})$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, et comme ce groupe est dual de G/G', G est lui-même cyclique). On construit d'abord un complexe cellulaire fini, de dimension 2, qui soit connexe, et de groupe fondamental G; soit Y_2 un tel complexe, et soit X_2 son revêtement universel. On a la suite exacte de G-modules :

$$C_2(X_2) \xrightarrow{\partial} C_1(X_2) \xrightarrow{\partial} C_0(X_2) \longrightarrow \mathbf{Z} \longrightarrow 0\,. \tag{18}$$

Or, on a le lemme suivant :

Lemme 8. — Il existe une résolution libre périodique de $\mathbf{Z}$

$$0 \longrightarrow \mathbf{Z} \longrightarrow L_{k-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,. \tag{19}$$

qui coïncide avec (18) *en dimensions* $\leqslant 1$*, et qui est telle que* $L_2 = C_2(X_2) \oplus M$*, avec* M *libre, l'application* $C_2 \oplus M \to C_1$ *étant* $(\partial, 0)$.

On commence par prolonger (18) par des modules libres L'_i $(i \leqslant k-1)$. Soit A le noyau de $L'_{k-1} \to L'_{k-2}$. Puisque $\mathbf{Z}$ a une résolution libre de période k, le

corollaire au lemme 7 montre que A est strictement équivalent à $\mathbf{Z}$; on applique alors le procédé du lemme 3, pour « remplacer » A par $\mathbf{Z}$; on obtient ainsi (19).

(Noter qu'il n'est nécessaire d'introduire le module M que si $k = 4$.)

Quitte à adjoindre à X_2 des sphères (attachées chacune par un point), on peut supposer que $M = 0$. Le noyau de $C_2(X_2) \to C_1(X_2)$ s'identifie à $H_2(X_2) = \pi_2(X_2)$; soit (a_α) une $\mathbf{Z}[G]$-base de L_3 et soit (b_α) son image dans $\pi_2(X_2)$ par $L_3 \to L_2 = C_2(X_2)$; pour chaque α, soit $f_\alpha : \mathbf{S}_2 \to X_2$ une application continue de la classe b_α. Attachons à X_2 des cellules $e_{\alpha,\sigma}$ de dimension 3 au moyen des $\sigma \circ f_\alpha$; le groupe G opère de façon naturelle sur le complexe cellulaire X_3 ainsi obtenu, et l'on a $C_i(X_3) = L_i$ pour $0 \leqslant i \leqslant 3$. On définit de même $X_4, \ldots, X_{k-1}$ et il est clair que X_{k-1} répond à la question.

Remarque. — On peut s'arranger pour que les X_i soient des complexes simpliciaux sur lesquels G opère simplicialement ; cela se démontre par récurrence sur i, en choisissant des applications f_α simpliciales, et en utilisant un résultat de J.H.C. WHITEHEAD ([9], lemme 2, p. 239).

6. Démonstration du théorème 3

Soit r un entier premier à n. L'homomorphisme $r : \mathbf{Z} \to \mathbf{Z}$ est une équivalence d'homotopie, et définit donc un élément (r) de $K_0(G)$. On obtient ainsi un homomorphisme $(\mathbf{Z}/n\mathbf{Z})^* \to K_0(G)$ dont l'image sera notée D(G).

[Définition explicite de (r) : c'est la classe dans $K_0(G)$ de l'idéal de $\mathbf{Z}[G]$ engendré par r et N, cf. SWAN [8], § 6.]

Soit maintenant P une résolution projective périodique de $\mathbf{Z}$, de période k :

$$0 \longrightarrow \mathbf{Z} \longrightarrow P_{k-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,.$$

On posera :

$$\chi(P) = \sum_{i=0}^{i=k-1} (-1)^i [P_i] \quad \text{dans } K_0(G).$$

Soit P′ une autre résolution projective périodique de $\mathbf{Z}$, de période k. Il existe un homomorphisme de P dans P′ qui est l'identité sur le groupe $\mathbf{Z}$ « de droite »; sur le groupe de gauche, c'est la multiplication par un entier r, premier à n, et bien déterminé modulo n (cf. lemme 2, par exemple). On notera $d(P, P')$ la classe de r dans $(\mathbf{Z}/n\mathbf{Z})^*$. Ces notations étant introduites, on a :

Lemme 9. — $\chi(P) - \chi(P') = (-1)^k (d(P, P'))\,.$

On applique le lemme 7 à l'homomorphisme de P dans P′ construit ci-dessus; si l'on appelle f_i l'homomorphisme de P_i dans P'_i, le lemme 7 montre que l'on a :

$$\sum(-1)^i(f_i) + (-1)^k(r) = 0\,.$$

Mais on voit facilement que $(f_i) = [P'_i] - [P_i]$, d'où aussitôt le lemme.

COROLLAIRE. — *L'image de* $\chi(P)$ *dans* $K_0(G)/D(G)$ *est indépendante de la résolution* P.

On la notera c_k pour indiquer sa dépendance de l'entier k.

Lemme 10. — Pour tout entier $d \geqslant 1$, *on a* $c_{dk} = d\,c_k$.

Si l'on met bout à bout d résolutions de période k, on obtient une résolution de période dk, d'où le lemme.

Lemme 11. — Pour qu'il existe une résolution libre *périodique de* $\mathbf{Z}$, *de période* k, *il faut et il suffit que* $c_k = 0$.

C'est évidemment nécessaire. Réciproquement, supposons que c_k soit nul. On peut évidemment construire une suite exacte :

$$0 \longrightarrow A \longrightarrow L_{k-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow \mathbf{Z} \longrightarrow 0\,. \tag{20}$$

où les L_i sont libres.

Soit

$$0 \longrightarrow \mathbf{Z} \longrightarrow P_{k-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow \mathbf{Z} \longrightarrow 0 \tag{21}$$

une résolution projective périodique de $\mathbf{Z}$. Par hypothèse, $\chi(P) \in D(G)$. On peut construire un homomorphisme de (20) dans (21) qui soit égal à l'homothétie de rapport r donné (avec $(r, n) = 1$) sur les groupes $\mathbf{Z}$ de droite. Soit h l'homomorphisme de A dans $\mathbf{Z}$ induit par cet homomorphisme. En appliquant le lemme 7, on obtient la formule :

$$(-1)^k(h) + \chi(P) - (r) = 0\,.$$

On peut donc choisir r de telle sorte que $(h) = 0$, d'où $A \sim_L \mathbf{Z}$ et le lemme 3 permet de remplacer la suite exacte (20) par une résolution libre périodique de $\mathbf{Z}$, de période k.

Lemme 12 (SWAN [7], prop. 9.1). — *Le groupe* $K_0(G)$ *est un groupe fini.*

D'après un résultat de SWAN ([7], théorème A — voir aussi une note aux
3 Comptes Rendus de GIORGIUTTI, et un article à paraître de H. BASS), tout élément de $K_0(G)$ est de la forme [I], où I est un idéal de $\mathbf{Z}[G]$. Le lemme résulte alors de la « finitude du nombre de classes d'idéaux », c'est-à-dire du théorème de Jordan-Zassenhaus.

Nous pouvons maintenant démontrer le théorème 3 : puisque $K_0(G)$ est fini, il existe un entier $d \geqslant 1$, tel que $dc_k = 0$ En appliquant les lemmes 10 et 11, on en déduit qu'il existe une résolution libre périodique de $\mathbf{Z}$, de période dk,

c.q.f.d.

7. Compléments

a) *Évaluation de l'entier d.* — On montre facilement que, si H est un groupe cyclique, on a $D(H) = 0$, et $\chi(P)$ est indépendant de P, donc nul, vu le lemme 11. Il en résulte que, si G est maintenant un groupe quelconque, et si P est une résolution projective périodique de $\mathbf{Z}$ de période k, l'image de $\chi(P)$ dans les groupes $K_0(H)$ est nulle si H est cyclique. Un raisonnement à la ARTIN (cf. SWAN, [7], corollaire 9.3) montre alors que $n\chi(P) = 0$ et l'on peut donc prendre pour d l'entier n.

Pour obtenir $d = (\varphi(n), n)$, il faut utiliser, à la place des sous-groupes cycliques, les sous-groupes élémentaires (produits d'un p-groupe par un groupe cyclique d'ordre premier à p). C'est nettement plus délicat (cf. SWAN [8], §§ 8, 9, 10).

b) *$\mathscr{C}$-théorie.* — On se donne une famille $\mathscr{P}$ de nombres premiers, et l'on « néglige » les groupes finis dont l'ordre n'est divisible par aucun nombre premier $p \in \mathscr{P}$. L'anneau $\mathbf{Z}$ est remplacé par l'anneau des fraction a/b, avec $(b, p) = 1$ pour tout $p \in \mathscr{P}$. Il y a très peu de changements à faire dans les démonstrations.

Bibliographie

[1] H. CARTAN, *Homologie des groupes, théorie des faisceaux,* Séminaire Cartan 1950-51.

[2] H. CARTAN and S. EILENBERG, *Homological Algebra*, Princeton, Princeton University Press, 1956 (Princeton Mathematical Series **19**).

[3] B. ECKMANN, *Homotopie et dualité,* Colloque de Topologie algébrique [1956. Louvain], 41–53, Liège, Georges Thone ; Paris, Masson, 1957 (Centre belge de recherches mathématiques).

[4] G. HOCHSCHILD, *Relative homological algebra*, Trans. Amer. math. Soc. **82** (1956), 246–269.

[5] J. MILNOR, *Groups which act on* $\mathbf{S}_n$ *without fixed points*, Amer. J. of Math. **79** (1957), 623–630.

[6] D.S. RIM, *Modules over finite groups*, Ann. of Math. **69** (1959), 700–712.

[7] R.G. SWAN, *Induced representations and projective modules*, Ann. of Math. **71** (1960), 552–578.

[8] R.G. SWAN, *Periodic resolutions for finite groups*, Ann. of Math **72** (1960), 267–291.

[9] J.H.C. WHITEHEAD, *Combinatorial homotopy I*, Bull. A.M.S. **55** (1949), 213–245.

Séminaire Delange-Pisot-Poitou 28 mars 1966
1965-66, exposé n° 15

DÉPENDANCE D'EXPONENTIELLES p-ADIQUES

S. Lang (cf. [2], [3]) a récemment démontré que deux exponentielles 1
$e^{b_1 z}, e^{b_2 z}$ qui prennent des valeurs algébriques pour au moins trois valeurs indépendantes de z, sont multiplicativement dépendantes (i.e. le rapport b_1/b_2 est rationnel). Sa démonstration vaut aussi bien dans le cas réel ou complexe que dans le cas p-adique. Ce dernier cas est particulièrement intéressant : il a des applications à la théorie des représentations p-adiques des groupes de Galois des corps de nombres; j'espère revenir ailleurs sur ce point. 2

Le contenu de cet exposé est le suivant : le § 1 reproduit la démonstration du théorème de Lang, dans le cas p-adique; le § 2 en donne une généralisation à plusieurs variables, sous certaines hypothèses de répartition. Dans les deux cas, on a besoin de variantes p-adiques du lemme de Schwarz; elles sont démontrées en Appendice.

§ 1. Le théorème de Lang

1.1. Énoncé du théorème. — Soit k un corps complet pour une valuation réelle v; si c est tel que $0 < c < 1$, on pose

$$|x| = c^{v(x)}.$$

L'application $x \mapsto |x|$ est une valeur absolue ultramétrique sur k.

On suppose également que k est de caractéristique zéro, et que sa caractéristique résiduelle est p; on a $0 < v(p) < +\infty$.

On note E le « domaine de convergence » de la série exponentielle

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!},$$

autrement dit l'ensemble des $z \in k$ tels que $v(z) > v(p)/(p-1)$.

On se donne :

(i) Un sous-groupe A de k, libre de rang fini $a \geqslant 2$ sur $\mathbf{Z}$.
(ii) Des éléments b_i $(i = 1, \ldots, b)$ de k.

On pose :

$$e_i(z) = \exp(b_i z) \ .$$

On suppose que les e_i convergent sur A, i.e. que $b_i \mathrm{A} \subset \mathrm{E}$ pour tout i; les e_i définissent alors des *caractères* de A, autrement dit des homomorphismes de A dans k^*.

THÉORÈME 1. — *Supposons que tous les $e_i(x)$, $x \in \mathrm{A}$, $1 \leqslant i \leqslant b$, soient algébriques sur $\mathbf{Q}$. Alors, si $b > a/(a-1)$, les b_i sont linéairement dépendants sur $\mathbf{Q}$.*

Remarques. — 1^0) Si $a = 2$, le théorème s'applique pour $b \geqslant 3$; si $a \geqslant 3$, il s'applique pour $b \geqslant 2$. On ignore ce qui se passe pour $a = b = 2$.

2^0) Dire que les b_i sont linéairement dépendants sur $\mathbf{Q}$ équivaut à dire que les e_i sont *multiplicativement dépendants*, i.e. qu'il existe des entiers n_i non tous nuls tels que

$$\prod e_i^{n_i} = 1 \ .$$

1.2. Notations. — Soit K un corps de nombres. Si $x \in \mathrm{K}$, nous appellerons *dénominateur* de x le plus petit entier $\mathrm{D} \geqslant 1$ tel que $\mathrm{D}x$ soit entier. Nous appellerons *taille* de x, et nous noterons $t(x)$, le nombre

$$t(x) = \sup\,(\mathrm{D}, |\sigma(x)|_\infty),$$

où σ parcourt l'ensemble des plongements de K dans $\mathbf{C}$ et $|\ |_\infty$ désigne la valeur absolue usuelle sur $\mathbf{C}$. Lorsque x est entier, on a $\mathrm{D} = 1$, et $t(x) = \sup\,(|\sigma(x)|_\infty)$.

Nous appliquerons ceci au corps K engendré par les $e_i(a_j)$, où (a_j) $(1 \leqslant j \leqslant a)$ est une base de A; du fait que les e_i sont des homomorphismes, on a $e_i(x) \in \mathrm{K}$ pour tout $x \in \mathrm{A}$ et tout i.

D'autre part, si m est un entier $\geqslant 1$, nous noterons $\mathrm{A}(m)$ l'ensemble des éléments de A de la forme $\sum m_j a_j$, avec $0 \leqslant m_j < m$. On a $\mathrm{Card}(\mathrm{A}(m)) = m^a$.

1.3. Démonstration du théorème 1. — Quitte à multiplier les b_i par une puissance de p, on peut supposer que les séries $e_i(z)$ convergent sur le disque $|z| \leqslant \mathrm{R}$, avec $\mathrm{R} > 1$ (par abus de langage, nous dirons qu'une série $\sum a_n z^n$ *converge sur le disque* $|z| \leqslant \mathrm{R}$ si $\mathrm{R}^n |a_n|$ tend vers 0 – convention analogue pour plusieurs variables). Quitte à remplacer A par $p^n \mathrm{A}$, avec n assez grand, on peut aussi supposer que A est contenu dans le disque unité $|z| \leqslant 1$.

On aura à considérer des polynômes en les e_i :

$$\mathrm{P}(e)(z) = \sum c_{n_1 \cdots n_b} e_1(z)^{n_1} \cdots e_b(z)^{n_b} \ ;$$

on écrira un tel polynôme $\sum c_n e^n(z)$.

Soit maintenant N un entier $\geqslant 1$ (que l'on fera tendre vers $+\infty$), et considérons un polynôme du type précédent, avec $n_i < 2\mathrm{N}^a$ pour tout i. Cherchons à déterminer les coefficients c_n de telle sorte que $\mathrm{P}(e)$ s'annule en tous les éléments de $\mathrm{A}(\mathrm{N}^b)$. Les c_n répondant à la question sont les solutions d'un système linéaire homogène à $2^b\mathrm{N}^{ab}$ inconnues et N^{ab} équations. Les coefficients de ce système sont les

$$e^n(x) = \prod e_i(a_j)^{n_i m_j} \ , \quad \text{avec } n_i < 2\mathrm{N}^a, \ m_j < \mathrm{N}^b \ .$$

Ces coefficients appartiennent à K. De plus, si d est un entier $\geqslant 1$, tel que $d{\cdot}e_i(a_j)$ soit entier pour tout i, j, les produits

$$d^{2\mathrm{N}^{a+b}}{\cdot}e^n(x)$$

sont des entiers de K, et leur taille est majorée par $\mathrm{C}_1^{\mathrm{N}^{a+b}}$, où C_1 est une constante (i.e. ne dépend pas de N). D'après un lemme classique de SIEGEL (cf. [5], p. 37), on peut trouver une solution (c_n) non triviale du système en question, les c_n étant en outre des entiers de K de taille $\leqslant \mathrm{C}_2^{\mathrm{N}^{a+b}}$, où C_2 est une autre constante. Nous désignerons par P_N le polynôme en les e_i correspondant. C'est une série entière en z; elle converge sur le disque $|z| \leqslant \mathrm{R}$.

Supposons maintenant que les b_i soient *linéairement indépendants* sur $\mathbf{Q}$; les e_i sont alors multiplicativement indépendants, et les produits $e_1^{n_1} \cdots e_b^{n_b}$ sont deux à deux distincts. Comme ce sont des *homomorphismes*, un argument classique montre qu'ils sont *linéairement indépendants*. Il s'ensuit que 3
le polynôme P_N considéré ci-dessus n'est pas nul; il ne possède donc qu'un nombre fini de racines dans le disque $|x| \leqslant \mathrm{R}$. Il existe alors un plus grand entier M tel que P_N s'annule en tous les éléments de $\mathrm{A}(\mathrm{M}^b)$. On a $\mathrm{N} \leqslant \mathrm{M}$. Soit x un élément de $\mathrm{A}((\mathrm{M}+1)^b)$ en lequel P_N ne s'annule pas. Posons $y = \mathrm{P}_\mathrm{N}(x)$. Nous allons majorer la valeur absolue p-adique $|y|$ de y, ainsi que sa taille $t(y)$; la comparaison des résultats montrera que $b \leqslant a/(a-1)$.

Majoration de $t(y)$. — On a

$$y = \sum c_n e^n(x) \ ;$$

les c_n sont entiers, et leur taille est majorée par $\mathrm{C}_2^{\mathrm{N}^{a+b}}$. D'autre part, on a :

$$e^n(x) = \prod e_i(a_j)^{n_i m_j} \ , \text{ avec } n_i < 2\mathrm{N}^a \ , \ m_j \leqslant \mathrm{M}^b \ .$$

On en conclut que les $e^n(x)$ sont de taille $\leqslant C_3^{M^{a+b}}$, et ont un dénominateur commun $\leqslant C_4^{M^{a+b}}$. Comme le nombre de termes de la sommation est négligeable devant de tels facteurs, on en déduit

$$t(y) \leqslant C_5^{M^{a+b}} .$$

Majoration de $|y|$. — Soit $\sum p_n z^n$ le développement en série entière de la fonction P_N. Posons :

$$|P_N|_R = \sup (R^n |p_n|) \quad \text{et} \quad |P_N|_1 = \sup |p_n| .$$

Comme P_N converge sur le disque $|z| \leqslant R$, le produit $R^n|p_n|$ tend vers 0, et les nombres ci-dessus sont finis. Comme $|x| \leqslant 1$, on a $|y| = |P_N(x)| \leqslant |P_N|_1$. D'autre part, puisque P_N s'annule sur $A(M^b)$, il a au moins M^{ab} racines distinctes dans le disque unité, et le lemme de Schwarz (cf. Appendice, prop. 1) montre que

$$|P_N|_1 \leqslant R^{-M^{ab}} |P_N|_R .$$

Enfin, $|P_N|_R$ est majoré par $\sup (|e^n|_R)$, et ceux-ci sont eux-mêmes majorés par $C_6^{M^{a+b}}$, comme on le voit par un calcul analogue à celui fait pour $t(y)$. On en déduit :

$$|y| \leqslant |P_N|_1 \leqslant R^{-M^{ab}} C_6^{M^{a+b}} .$$

Supposons que $ab > a + b$, i.e. $b > a/(a-1)$. Le terme en M^{ab} l'emporte alors sur celui en M^{a+b} et l'on obtient une majoration :

$$|y| \leqslant C_7^{-M^{ab}} , \text{ avec } C_7 > 1 .$$

Mais il y a une relation entre $|y|$ et $t(y)$:

Lemme. — *Soit $d = [K : \mathbf{Q}]$, et supposons la valeur absolue de k normalisée de telle sorte que $|p| = 1/p$. On a alors*

$$|y| \geqslant t(y)^{-2d} \textit{ pour tout } y \in K^* .$$

Soit D le dénominateur de y, et soit $z = Dy$; l'élément z est entier. On a $|D| \leqslant 1$, d'où $|y| \geqslant |z|$. Soit Nz la norme de z dans $\mathbf{Q}$; c'est un entier, évidemment divisible par z; d'où $|z| \geqslant |Nz|$. Si p^a est la plus grande puissance de p qui divise Nz, on a $|Nz| = p^{-a}$, d'où $|Nz| \geqslant 1/|Nz|_\infty$, où $|Nz|_\infty$ désigne la valeur absolue *usuelle* de l'entier Nz. Comme Nz est le produit des conjugués de z, et que la valeur absolue usuelle de ceux-ci est $\leqslant D \cdot t(y)$, on a

$$|Nz| \geqslant D^{-d} t(y)^{-d} \geqslant t(y)^{-2d} ,$$

d'où le lemme.

Appliquons ce lemme à l'élément y considéré plus haut; on a vu que $t(y) \leqslant C_5^{M^{a+b}}$; on en tire $|y| \geqslant C_5^{-2dM^{a+b}}$, ce qui est en contradiction avec

$|y| \leqslant \mathrm{C}_7^{-\mathrm{M}^{ab}}$ pour $\mathrm{N} \to \infty$ puisque $ab > a+b$. On ne peut donc avoir à la fois l'indépendance des b_i et l'inégalité $b > a/(a-1)$, ce qui démontre le théorème.

§ 2. Le cas de plusieurs variables

2.1. La notion de parfaite densité. — Soit G un groupe topologique, isomorphe à $(\mathbf{Z}_p)^r$, où $\mathbf{Z}_p$ désigne le groupe des entiers p-adiques. Soit A un sous-groupe libre de type fini de G, et soit (a_j), $1 \leqslant j \leqslant a$, une base de A. Si m est un nombre réel > 0 (non nécessairement entier), nous désignerons par $\mathrm{A}(m)$ le sous-ensemble de A formé des $\sum m_j a_j$, avec $0 \leqslant m_j < m$.

Supposons que A soit *dense* dans G; cela équivaut à dire que, pour tout entier $n \geqslant 0$, l'application canonique $\mathrm{A} \to \mathrm{G}/p^n\mathrm{G}$ est surjective.

Définition. — *Soit λ un nombre réel positif $\leqslant 1$. On dit que* A *est λ-dense dans* G *s'il existe une constante* $\mathrm{C} > 0$ *telle que, pour tout entier $n \geqslant 0$, l'application*

$$\mathrm{A}(\mathrm{C}p^{\lambda n}) \longrightarrow \mathrm{G}/p^n\mathrm{G}$$

soit surjective.

Noter que, puisque A est dense, l'application $\mathrm{A}/p^n\mathrm{A} \to \mathrm{G}/p^n\mathrm{G}$ est surjective; comme $\mathrm{A}(p^n)$ est un système de représentants de $\mathrm{A}/p^n\mathrm{A}$, on en conclut que $\mathrm{A}(p^n) \to \mathrm{G}/p^n\mathrm{G}$ est surjectif. Il s'ensuit que A est *toujours* 1-*dense*; le seul cas intéressant est donc celui où $\lambda < 1$.

D'autre part, le nombre d'éléments de $\mathrm{G}/p^n\mathrm{G}$ est p^{nr}, et celui de $\mathrm{A}(\mathrm{C}p^{\lambda n})$ est équivalent à $\mathrm{C}^a p^{\lambda a n}$; le groupe A ne peut donc être λ-dense que si $\lambda a \geqslant r$, c'est-à-dire si $\lambda \geqslant r/a$.

Définition. — *On dit que* A *est parfaitement dense dans* G *s'il est λ-dense pour $\lambda = r/a$.*

Remarque. — On montre facilement que les définitions ci-dessus ne dépendent pas du choix de la base (a_j).

Exemple. — Si $\alpha \in \mathbf{Z}_p$ est quadratique sur $\mathbf{Q}$, le sous-groupe $\mathrm{A} = \mathbf{Z} + \alpha\mathbf{Z}$ de $\mathbf{Z}_p$ est parfaitement dense.

Question. — Prenons pour G le groupe multiplicatif des unités p-adiques congrues à 1 mod p (resp. congrues à 1 mod 4 si $p = 2$), et soit A le sous-groupe engendré par des nombres rationnels a_j multiplicativement indépendants. Supposons A dense dans G. Est-il vrai que A est parfaitement dense? J'ignore ce qu'il en est, même pour $p = 3$ et A engendré par 4 et 7.

2.2. Énoncé du théorème. — Conservons les notations précédentes, et donnons-nous une famille finie d'*homomorphismes continus* $e_i : \mathrm{G} \to k^*$, le corps k vérifiant les conditions de 1.1. Soit b le nombre des e_i.

THÉORÈME 2. — *Supposons que tous les* $e_i(x)$, $x \in \mathrm{A}$, $1 \leqslant i \leqslant b$, *soient*
4 *algébriques sur* $\mathbf{Q}$, *et que* A *soit* λ*-dense dans* G. *Alors, si* $b > r/(1-\lambda)$, *les* e_i *sont multiplicativement dépendants.*

Dans le cas où A est parfaitement dense, on a $\lambda = r/a$, et l'inégalité devient $b > ar/(a-r)$; pour $r = 1$, c'est l'inégalité $b > a/(a-1)$ du théorème 1 (mais ce dernier valait sans aucune hypothèse de λ-densité — le théorème 2 ne contient donc pas le théorème 1).

2.3. Démonstration du théorème 2. Préparatifs. — Soit C une constante telle que $\mathrm{A}(\mathrm{C}p^{\lambda n}) \to \mathrm{G}/p^n\mathrm{G}$ soit surjectif pour tout n. Nous choisirons dans $\mathrm{A}(\mathrm{C}p^{\lambda n})$ un système de représentants $\mathrm{B}(n)$ de $\mathrm{G}/p^n\mathrm{G}$; de plus, nous supposerons les $\mathrm{B}(n)$ choisis de telle sorte que $\mathrm{B}(n)$ soit contenu dans $\mathrm{B}(n+1)$; on voit tout de suite que c'est possible. On a

$$\mathrm{Card}(\mathrm{B}(n)) = p^{nr}\,.$$

On note K le sous-corps de k engendré par les $e_i(x)$, $x \in \mathrm{A}$; c'est un corps de nombres.

Enfin on *identifie* G à $(\mathbf{Z}_p)^r$ au moyen d'un isomorphisme. Les e_i sont alors transformées en des fonctions $e_i(z_1, \ldots, z_r)$ à r variables $z_i \in \mathbf{Z}_p$. Mais tout homomorphisme continu de $\mathbf{Z}_p$ dans k^* est donné localement par une exponentielle $z \mapsto \exp(bz)$, avec $b \in k$. Les e_i sont donc des produits d'exponentielles, et en particulier sont *analytiques* en $z_1, \ldots, z_r$. Sur un voisinage convenable $p^n\mathrm{G}$ de 0 dans G, on a

$$e_i(z) = \sum \alpha_{i,n} z^n \quad (\text{où } n \text{ désigne un multi-indice}),$$

la série étant convergente sur $p^n\mathrm{G}$. Quitte à remplacer e_i par sa puissance p^{n+1}-ième, on peut donc supposer que e_i est donné, *sur tout le polydisque unité* $(\mathbf{Z}_p)^r$, par une série $\sum \alpha_{i,n} z^n$ qui converge sur un polydisque $|z_i| \leqslant \mathrm{R}$, avec $\mathrm{R} > 1$. (Ici encore, ces précautions sont destinées à permettre l'application du lemme de Schwarz.)

2.4. Démonstration du théorème 2. — Elle est tout à fait analogue à celle du théorème 1. On commence par considérer des polynômes en les e_i de la forme

$$\mathrm{P}(e)(z) = \sum c_{n_1 \cdots n_b} e_1^{n_1}(z) \cdots e_b^{n_b}(z)\ ,$$

où tous les n_i sont $< 2p^{nr}$ (n étant un entier $\geqslant 0$ que l'on fait tendre vers $+\infty$). On cherche à déterminer les coefficients c de telle sorte que $\mathrm{P}(e)$ s'annule en tout point de l'ensemble $\mathrm{B}(bn)$ défini au n° 2.3. Cela donne un système linéaire homogène à $2^b p^{bnr}$ inconnues et p^{bnr} équations. Ses coefficients sont des produits

$$\prod e_i(a_j)^{n_i m_j}, \text{ avec } n_i < 2p^{nr},\ m_j < \mathrm{C}p^{\lambda bn} ;$$

on en déduit, comme précédemment, que l'on peut prendre pour coefficients c des entiers de K, non tous nuls, de taille $\leqslant \mathrm{C}_8^{p^{n(r+\lambda b)}}$. Soit P_n le polynôme correspondant.

Supposons que les e_i soient *multiplicativement indépendants*. Le même argument que dans le cas $r = 1$ montre que P_n est alors non nul. Comme la réunion des $\mathrm{B}(m)$ est dense dans G, il s'ensuit qu'il existe un plus grand entier m tel que P_n s'annule sur $\mathrm{B}(m)$; on a $m \geqslant bn$. Soit x un élément de $\mathrm{B}(m+1)$ tel que $y = \mathrm{P}_n(x)$ soit non nul. On va obtenir une contradiction en comparant des majorations de $|y|$ et de $t(y)$.

Majoration de $t(y)$. — On a

$$y = \sum c_{n_1 \cdots n_b} \prod e_i(a_j)^{n_i m_j} ,$$

avec $n_i < 2p^{nr} \leqslant 2p^{mr/b}$, $m_j < \mathrm{C}p^{\lambda(m+1)}$, $t(c) \leqslant \mathrm{C}_8^{p^{n(r+\lambda b)}}$. On en déduit :

$$t(y) \leqslant \mathrm{C}_9^{p^{m(\lambda + r/b)}} .$$

Majoration de $|y|$. — On définit comme dans le cas $r = 1$ les normes $|\mathrm{P}_n|_{\mathrm{R}}$ et $|\mathrm{P}_n|_1$ de P_n relativement aux polydisques $|z_i| \leqslant \mathrm{R}$ et $|z_i| \leqslant 1$. On a

$$|y| \leqslant |\mathrm{P}_n|_1 .$$

D'autre part, P_n s'annule en tous les points de $\mathrm{B}(m)$, et l'application $\mathrm{B}(m) \to \mathrm{G}/p^n\mathrm{G}$ est surjective. D'après une variante à r variables du lemme de Schwarz (cf. Appendice, prop. 2), on a donc :

$$|\mathrm{P}_n|_1 \leqslant \mathrm{R}^{-p^m} |\mathrm{P}_n|_{\mathrm{R}} .$$

Enfin, un calcul direct montre que $|\mathrm{P}_n|_{\mathrm{R}} \leqslant \mathrm{C}_{10}^{p^{m(\lambda + r/b)}}$.

Supposons alors que $1 > \lambda + r/b$, i.e. que $b > r/(1-\lambda)$. L'exposant p^m l'emporte sur l'exposant $p^{m(\lambda + r/b)}$, et l'on obtient la majoration :

$$|y| \leqslant \mathrm{C}_{11}^{-p^m}, \text{ avec } \mathrm{C}_{11} > 1 .$$

Mais les majorations obtenues pour $|y|$ et $t(y)$ sont incompatibles (pour n assez grand) avec le lemme du n° 1.3. Le théorème 2 est donc démontré.

Appendice
Analogues p-adiques du lemme de Schwarz

A.1. Notations. — Soit k un corps complet pour une valeur absolue ultramétrique non triviale. Soit

$$f = \sum a_{n_1 \cdots n_r} z_1^{n_1} \cdots z_r^{n_r} = \sum a_n z^n \ ,$$

une série formelle à coefficients dans k. Si R est un nombre réel > 0, on pose :

$$|f|_{\mathrm{R}} = \sup\left(\mathrm{R}^{|n|}|a_n|\right), \text{ où } |n| = \sum n_i \ .$$

On a $|f+g|_{\mathrm{R}} \leqslant \sup\left(|f|_{\mathrm{R}}, |g|_{\mathrm{R}}\right)$, $|\lambda f|_{\mathrm{R}} = |\lambda|.|f|_{\mathrm{R}}$, et $|fg|_{\mathrm{R}} = |f|_{\mathrm{R}}.|g|_{\mathrm{R}}$ si $|f|_{\mathrm{R}}$ et $|g|_{\mathrm{R}}$ sont finis.

Lorsque $|f|_{\mathrm{R}}$ est *fini*, la série converge dans le polydisque $|z_i| < \mathrm{R}$; elle converge même dans le polydisque $|z_i| \leqslant \mathrm{R}$ si $\mathrm{R}^{|n|}|a_n|$ tend vers 0. On a :

$$|f(z)| \leqslant |f|_{\mathrm{R}} \ .$$

Lorsque en outre le corps résiduel de k est infini, et que le groupe des valeurs de k^* est dense, on a

$$|f|_{\mathrm{R}} = \sup\left(|f(z)|\right) \ \text{ pour } |z_i| < \mathrm{R} \ .$$

Si $\mathrm{R}' \leqslant \mathrm{R}$, on a $|f|_{\mathrm{R}'} \leqslant |f|_{\mathrm{R}}$; le but du lemme de Schwarz est d'améliorer cette inégalité, sous l'hypothèse que f a « beaucoup » de racines dans le polydisque $|z_i| \leqslant \mathrm{R}'$.

A.2. Le cas des fonctions d'une variable. — Supposons que $r = 1$. Soient $\mathrm{R}' < \mathrm{R}$ deux nombres réels > 0, et soit $f(z) = \sum a_n z^n$ une série telle que $|f|_{\mathrm{R}}$ soit fini. Il en résulte que f converge sur le disque $|z| \leqslant \mathrm{R}'$; on peut donc parler de ses *racines* sur ce disque.

Proposition 1 (cf. Mahler [4]). — *Si f a au moins h racines dans le disque $|z| \leqslant \mathrm{R}'$, on a* :

$$|f|_{\mathrm{R}'} \leqslant \left(\frac{\mathrm{R}'}{\mathrm{R}}\right)^h |f|_{\mathrm{R}} \ .$$

Remarquons d'abord que, si f a une racine a telle que $|a| \leqslant \mathrm{R}'$, on peut écrire f sous la forme $f = (z-a)f_1$, avec $|f_1|_{\mathrm{R}} < +\infty$; en effet, c'est clair si $a = 0$, et le cas général se ramène à celui-là par translation. En appliquant ce résultat aux racines a_i $(1 \leqslant i \leqslant h)$ de f dans le disque $|z| \leqslant \mathrm{R}'$, on voit que l'on peut écrire f sous la forme

$$f = \mathrm{P} \cdot g, \text{ avec } \mathrm{P}(z) = \prod (z - a_i) \text{ et } |g|_{\mathrm{R}} < +\infty \ .$$

On a $|\mathrm{P}|_{\mathrm{R}} = \mathrm{R}^h$ et $|\mathrm{P}|_{\mathrm{R}'} = \mathrm{R}'^h$. On en déduit :

$$|f|_{\mathrm{R}'} = \mathrm{R}'^h \cdot |g|_{\mathrm{R}'} \leqslant \mathrm{R}'^h \cdot |g|_{\mathrm{R}} = \left(\frac{\mathrm{R}'}{\mathrm{R}}\right)^h \cdot \mathrm{R}^h \cdot |g|_{\mathrm{R}} = \left(\frac{\mathrm{R}'}{\mathrm{R}}\right)^h \cdot |f|_{\mathrm{R}} \ ,$$

c.q.f.d.

Remarque. — On aurait pu aussi appliquer la théorie du *polygone de Newton* à f.

A.3. Le cas général. Énoncé du résultat. — Lorsque $r > 1$, les racines de f dans le polydisque $|z_i| \leqslant \mathrm{R}'$ peuvent former des sous-espaces analytiques de dimension $r-1$, et sont en général en nombre infini. Le fait que f ait beaucoup de racines n'entraîne alors rien de plus que l'inégalité triviale :

$$|f|_{\mathrm{R}'} \leqslant \frac{\mathrm{R}'}{\mathrm{R}} |f|_{\mathrm{R}} \ .$$

Il est donc nécessaire de faire des hypothèses restrictives sur la *position* de ces racines. Je vais me borner à un cas très particulier, où l'on suppose que ces racines sont *très bien réparties*; il serait intéressant d'avoir des énoncés plus généraux.

Plus précisément, nous supposerons que k vérifie les hypothèses du n° 1.1, donc contient le corps p-adique $\mathbf{Q}_p$. On se donne un nombre entier $n \geqslant 0$, et un sous-ensemble B de $(\mathbf{Z}_p)^r$ tel que l'application $\mathrm{B} \to (\mathbf{Z}_p/p^n\mathbf{Z}_p)^r$ soit *bijective*. On se donne d'autre part une série $f(z_1, \cdots, z_r)$ telle que $|f|_{\mathrm{R}} < +\infty$, R étant un nombre réel > 1. Cette série converge sur le polydisque unité, lequel contient B.

Proposition 2. — *Si f s'annule sur* B*, on a*:

$$|f|_1 \leqslant \mathrm{R}^{-p^n} |f|_{\mathrm{R}} \ .$$

Noter que l'exposant de R^{-1} est bien p^n et non $\mathrm{Card}(\mathrm{B}) = p^{nr}$. L'exemple de la fonction $f = z_1(z_1-1)\cdots(z_1-p^n+1)$ montre d'ailleurs que cet exposant ne peut être amélioré.

Question. — Existe-t-il un résultat analogue dans le cas archimédien, autrement dit pour les fonctions de plusieurs variables complexes? Même question pour le théorème 2.

A.4. Démonstration de la proposition 2. — La méthode consiste à écrire f comme série de *polynômes d'interpolation* relatifs à la suite des entiers positifs (cf. Y. AMICE [1]). De façon précise, pour tout entier positif α, posons :

$$\mathrm{P}_\alpha(\mathrm{X}) = \mathrm{X}(\mathrm{X}-1)\cdots(\mathrm{X}-\alpha+1)\ ,$$

et si $\alpha = (\alpha_1, \ldots, \alpha_r)$ est un multi-indice, posons :

$$\mathrm{P}_\alpha(z) = \mathrm{P}_{\alpha_1}(z_1)\cdots\mathrm{P}_{\alpha_r}(z_r), \quad \text{où } z = (z_1, \ldots, z_r)\ .$$

On a

$$\mathrm{P}_\alpha(z) = z^\alpha + \sum_{|\beta|<|\alpha|} b_\beta^\alpha z^\beta, \quad \text{où les } b_\beta^\alpha \text{ sont des entiers.}$$

D'où :

$$z^\alpha = \mathrm{P}_\alpha + \sum_{|\beta|<|\alpha|} c_\alpha^\beta \mathrm{P}_\beta, \quad \text{où les } c_\alpha^\beta \text{ sont des entiers.}$$

Si $f = \sum a_\alpha z^\alpha$ est la série donnée, on a $a_\alpha \to 0$ (puisque $|f|_\mathrm{R}$ est fini). Remplaçant les z^α par leur expression en fonction des P_α, on obtient un développement en série pour f :

$$f = \sum b_\alpha \mathrm{P}_\alpha\ .$$

(En fait, les z^α et les P_α constituent deux bases normales de l'espace de Banach des séries convergentes sur le polydisque unité, la norme étant $f \mapsto |f|_1$. Cf. [1], Chap. III.)

On vérifie tout de suite que l'on a :

$$|f|_1 = \sup(|b_\alpha|) \quad \text{et} \quad |f|_\mathrm{R} = \sup(\mathrm{R}^{|\alpha|}\cdot|b_\alpha|)\ .$$

Tout revient donc à majorer les b_α.

Supposons que la valuation v soit normée de telle sorte que $v(p) = 1$, et posons :

$$\begin{aligned} b(\alpha) &= v(b_\alpha) \\ q(\alpha) &= v(\alpha!), \quad \text{où } \alpha! = \alpha_1!\cdots\alpha_r!\ . \end{aligned}$$

Lemme. — *Soit* X *l'ensemble des* $\alpha = (\alpha_1, \ldots, \alpha_r)$ *tels que* $\alpha_i \leqslant p^n - 1$ *pour tout* i. *Soit* m *le minimum de* $q(\alpha) + b(\alpha)$ *pour* $\alpha \in \mathrm{X}$. *Il existe* $\gamma \notin \mathrm{X}$ *tel que* $q(\gamma) + b(\gamma) \leqslant m$.

Soit X_m l'ensemble des $\alpha \in \mathrm{X}$ tels que $q(\alpha) + b(\alpha) = m$, et soit α un élément de X_m tel que $|\alpha|$ soit minimum. Soit x l'élément de B tel que $x \equiv \alpha \mod p^n$. Par hypothèse, on a $f(x) = 0$. Cela s'écrit :

$$\sum b_\gamma \mathrm{P}_\gamma(x) = 0\ .$$

La valuation de $b_\gamma \mathrm{P}_\gamma(x)$ est égale à $b(\gamma) + v(\mathrm{P}_\gamma(x))$. Or, on sait (cf. par exemple [1]) que le polynôme $\mathrm{Q}_\gamma = \mathrm{P}_\gamma/\gamma!$ applique $(\mathbf{Z}_p)^r$ dans $\mathbf{Z}_p$; on a donc $v(\mathrm{P}_\gamma(x)) \geqslant q(\gamma)$, d'où

$$v(b_\gamma \mathrm{P}_\gamma(x)) \geqslant q(\gamma) + b(\gamma) \ ,$$

l'égalité étant réalisée si et seulement si $\mathrm{Q}_\gamma(x) \not\equiv 0 \mod p$.

Supposons d'abord que l'on ait $\gamma \in \mathrm{X}$. La classe de $\mathrm{Q}_\gamma(x) \mod p$ ne dépend alors que de *la classe de* $x \mod p^n$ (c'est là une propriété générale des polynômes d'interpolation d'une suite très bien répartie, cf. [1], p. 135, lemme 4). On a donc

$$\mathrm{Q}_\gamma(x) \equiv \mathrm{Q}_\gamma(\alpha) \mod p \ .$$

Si $\gamma_i > \alpha_i$ pour un indice i, on a $\mathrm{Q}_\gamma(\alpha) = 0$, d'où

$$\mathrm{Q}_\gamma(x) \equiv 0 \mod p \ .$$

Pour $\gamma = \alpha$, on a $\mathrm{Q}_\alpha(\alpha) = 1$, d'où $\mathrm{Q}_\alpha(x) \equiv 1 \mod p$, et

$$v(b_\alpha \mathrm{P}_\alpha(x)) = q(\alpha) + b(\alpha) = m \ .$$

Si $\gamma \in \mathrm{X}$ *est distinct de* α, *on a* :

$$v(b_\gamma \mathrm{P}_\gamma(x)) \geqslant m + 1 \ .$$

En effet, c'est clair si $\gamma \notin \mathrm{X}_m$, car alors $q(\gamma) + b(\gamma) \geqslant m + 1$. Et si $\gamma \in \mathrm{X}_m$, on a $|\gamma| > |\alpha|$, et l'une des composantes γ_i de γ est $> \alpha_i$, d'où

$$v(\mathrm{P}_\gamma(x)) \geqslant q(\gamma) + 1 \ .$$

D'autre part, puisque la somme des $b_\gamma \mathrm{P}_\gamma(x)$ est nulle, il existe $\gamma \neq \alpha$ tel que

$$v(b_\gamma \mathrm{P}_\gamma(x)) \leqslant v(b_\alpha \mathrm{P}_\alpha(x)) = m \ .$$

Vu ce qui précède, on a $\gamma \notin \mathrm{X}$. D'autre part,

$$q(\gamma) + b(\gamma) \leqslant v(b_\gamma \mathrm{P}_\gamma(x)) \leqslant m \ ,$$

ce qui achève la démonstration du lemme.

Fin de la démonstration de la proposition 2. — Soit c le nombre réel < 1 tel que $x = c^{v(x)}$ pour tout $x \in k$. Ecrivons R et $|f|_\mathrm{R}$ comme puissance de c :

$$\mathrm{R} = c^{-k} \text{ (avec } k > 0) \text{ et } |f|_\mathrm{R} = c^h \ .$$

On a alors

$$b(\alpha) \geqslant k|\alpha| + h \ ,$$

et il nous faut prouver que $|f|_1 \leqslant c^{h+kp^n}$, i.e. que

$$b(\alpha) \geqslant k \cdot p^n + h \ .$$

C'est clair si $|\alpha| \geqslant p^n$. Dans le cas contraire, on a $\alpha \in \mathrm{X}$, et le lemme ci-dessus montre qu'il existe $\gamma \notin \mathrm{X}$ tel que

$$q(\gamma) + b(\gamma) \leqslant q(\alpha) + b(\alpha) \ .$$

On a alors :

$$b(\alpha) \geqslant b(\gamma) + q(\gamma) - q(\alpha) \ .$$

Puisque $\gamma \notin \mathrm{X}$, on a $|\gamma| \geqslant p^n$, d'où $b(\gamma) \leqslant kp^n + h$.

D'autre part, $q(\gamma) = \sum v(\gamma_i!)$; par hypothèse, l'un des γ_i est $\geqslant p^n$, d'où

$$q(\gamma) \geqslant v(\gamma_i!) \geqslant v(p^n!) = (p^n - 1)/(p - 1) \ .$$

Enfin, on a

$$q(\alpha) = \sum v(\alpha_i!) \leqslant \sum \alpha_i/(p-1) = |\alpha|/(p-1) \leqslant (p^n - 1)/(p-1)$$

puisqu'on a supposé $|\alpha| < p^n$.

En combinant ces inégalités, on trouve

$$b(\alpha) \geqslant kp^n + h \ ,$$

ce qui achève la démonstration.

Bibliographie

[1] Y. Amice, *Interpolation p-adique*, Bull. S.M.F. **92** (1964), 117–180.

[2] S. Lang, *Nombres transcendants*, Séminaire Bourbaki 1965/66, exposé n° 305.

[3] S. Lang, *Algebraic values of meromorphic functions II*, Topology **5** (1966), 363–370.

[4] K. Mahler, *Über transzendente p-adischen Zahlen*, Comp. Math. **2** (1935), 259–275.

[5] C.L. Siegel, *Transcendental Numbers*, Ann. of Math. Studies **16**, Princeton University Press, Princeton, 1949.

Séminaire Bourbaki novembre 1966
1966-67, exposé n° 318

GROUPES p-DIVISIBLES

On sait que de nombreuses propriétés des variétés abéliennes (par exemple celles liées à leur fonction zêta) peuvent se « lire » sur le *groupe des points d'ordre fini* de la variété, considéré comme module galoisien. Dans le cas local, l'étude de ce groupe s'est d'abord faite en utilisant le *groupe formel* (au sens de DIEUDONNÉ et LAZARD) attaché à la variété abélienne; c'est ainsi, par exemple, que l'on démontre le théorème de Lutz-Nagel [7], ou que l'on étudie les courbes elliptiques ayant une réduction de hauteur 2 (cf. [9]). Toutefois, on s'est aperçu récemment qu'il y a intérêt à remplacer les groupes formels par une nouvelle notion, plus souple, celle de *groupe p-divisible*. Le but de 1
cet exposé est d'indiquer les principaux résultats connus sur ces groupes. Ces résultats sont en très grande partie dus à TATE — parfois en collaboration. Ils ont été exposés dans plusieurs séminaires : Woods Hole [4], Collège de France [10], Driebergen [13].

§ 1. La notion de groupe p-divisible

Dans tout ce qui suit, p désigne un nombre premier.

Soit R un anneau commutatif (ou un schéma, si l'on préfère) et soit h un entier $\geqslant 0$. Un *groupe p-divisible de hauteur h* sur R est un système

$$\mathrm{G} = (\mathrm{G}_n, i_n)\,, \quad n \geqslant 1\,,$$

vérifiant les propriétés suivantes :

(a) G_n est un schéma en groupes commutatif [1] sur R, localement libre de rang p^{nh}.

(b) $i_n \colon \mathrm{G}_n \to \mathrm{G}_{n+1}$ est un homomorphisme de schémas en groupes.

(c) La suite

$$0 \longrightarrow \mathrm{G}_n \xrightarrow{i_n} \mathrm{G}_{n+1} \xrightarrow{p^n} \mathrm{G}_{n+1}$$

est exacte.

Si A_n désigne l'algèbre affine associée à G_n, la condition (a) signifie que A_n est munie d'une structure de bigèbre vérifiant certaines conditions (bicommutativité et biassociativité, notamment), et que A_n est un R-module projectif de rang p^{nh}. Lorsque R est local (ce qui est le cas essentiel dans les applications), cette dernière condition revient simplement à dire que A_n est un R-module *libre* de rang p^{nh}.

Quant à (c), elle signifie simplement que G_n s'identifie, au moyen de i_n, au noyau de $p^n : G_{n+1} \to G_{n+1}$; en particulier, i_n est une *immersion fermée*, et l'on peut considérer G comme la « réunion » des G_n (exactement comme le groupe $\mathbf{Q}_p/\mathbf{Z}_p$ est la réunion des groupes $\mathbf{Z}/p^n\mathbf{Z}$).

Remarque. — Si n, m sont des entiers $\geqslant 0$, la multiplication par p^n applique G_{n+m} dans G_m, et l'on démontre que l'on a une suite *exacte* (au sens de [1], exposé IV) :

$$0 \longrightarrow G_n \longrightarrow G_{m+n} \longrightarrow G_m \longrightarrow 0\,.$$

Exemples de groupes p-divisibles

1) *Groupes étales*

Supposons que Spec(R) soit connexe, et soit π son groupe fondamental. Soit T un $\mathbf{Z}_p$-module libre de rang h sur lequel π opère continûment ; les groupes $T_n = T/p^nT$ forment un système inductif de π-modules. On en déduit, par un procédé standard, un système (G_n, i_n), où les G_n sont *étales* sur R ; ce système est un groupe p-divisible de hauteur h. Inversement, tout groupe p-divisible étale de hauteur h s'obtient ainsi, de façon essentiellement unique.

Ceci s'applique notamment lorsque R est un *corps*, le groupe π étant simplement le groupe de Galois d'une clôture séparable de R, d'où une équivalence

« groupes p-divisibles étales » $\Longleftrightarrow$ « représentations p-adiques de π ».

De plus, lorsque R est de caractéristique différente de p, tout groupe p-divisible sur R est étale.

2) *Groupes définis par des schémas abéliens*

Soit A un *schéma abélien* sur R, de dimension relative r. Le noyau A_n de $p^n : A \to A$ est localement libre de rang p^{nh} avec $h = 2r$. Le système $A(p)$ formé des A_n est un groupe p-divisible de hauteur h.

Lorsque R est un corps de caractéristique différente de p, le groupe $A(p)$ est étale, et équivaut [d'après 1) ci-dessus] à la donnée du « module de Tate » $T_p(A)$, considéré comme module galoisien.

3) *Dual d'un groupe p-divisible*

Soit $G = (G_n, i_n)$ un groupe p-divisible de hauteur h. Le *dual* (au sens de Cartier) G'_n de G_n est défini par la bigèbre duale de celle de G_n; on peut aussi le définir comme représentant le foncteur $\mathscr{H}om_{\mathrm{gr}}(G_n, \mathbf{G}_m)$, cf. [1], exposé VIII. Les homomorphismes $G_{n+1} \to G_n$ induits par la multiplication par p définissent par transposition des homomorphismes $i'_n : G'_n \to G'_{n+1}$. Le système $G' = (G'_n, i'_n)$ est un groupe p-divisible de hauteur h, appelé le dual de G.

Le dual d'un groupe étale est un groupe *de type multiplicatif*, au sens de [1], *loc. cit.*

4) *Groupes p-divisibles et groupes formels*

Supposons, pour simplifier, que R soit un anneau local noethérien *complet, de caractéristique résiduelle p*. Soit Γ un *groupe formel commutatif* de dimension d sur R, au sens de DIEUDONNÉ-LAZARD ; l'algèbre Λ associée à Γ est isomorphe à $R[[T_1, \ldots, T_d]]$. Supposons en outre que la multiplication par p dans Γ soit une *isogénie* de degré p^h (i.e. fasse de Λ un Λ-module libre de rang p^h). On peut alors définir le *noyau* Γ_n de $p^n : \Gamma \to \Gamma$ comme un schéma en groupes sur R. Le système $\Gamma(p)$ des Γ_n est un groupe p-divisible de hauteur h sur R ; sa connaissance équivaut à celle de Γ (en effet, Γ est limite projective des algèbres des Γ_n). On obtient ainsi une *équivalence de catégories* entre :

– groupes p-divisibles connexes

– groupes formels commutatifs où p est une isogénie.

De plus, on montre que tout groupe p-divisible G sur R est extension d'un groupe *étale* par un groupe *connexe* G°, sa composante neutre. La dimension d de G° (considéré comme groupe formel) est appelée la dimension de G. Si G' est le dual de G, et si $d' = \dim(G')$, on a :

$$h = d + d' .$$

Cela résulte des propriétés des opérateurs V et F de la théorie de Dieudonné, cf. par exemple MANIN [8], ou [1], exposé VII.

Cas particulier. — Soit E une courbe elliptique définie sur R, et ayant « bonne réduction » (i.e. définissant un schéma abélien). Le groupe p-divisible $E(p)$ attaché à E a pour invariants $d = 1$, $d' = 1$ et $h = 2$. Si la *réduction* $\widetilde{E}$ de E est de hauteur 2 (cf. [9], § 2), $E(p)$ est connexe; c'est un groupe formel de hauteur 2. Si $\widetilde{E}$ est de hauteur 1, $E(p)$ est une extension d'un groupe étale de **2**
hauteur 1 (correspondant aux points d'ordre une puissance de p de $\widetilde{E}$) par un groupe formel de hauteur 1 (de type multiplicatif); lorsque cette extension est *triviale,* E est le « relèvement canonique » de $\widetilde{E}$, cf. § 5.

§ 2. Le premier théorème fondamental

On suppose R intègre, intégralement clos, noethérien, et de corps des fractions K de caractéristique zéro. On s'intéresse au foncteur qui associe à tout groupe p-divisible G sur R le groupe correspondant $G_K = G \times_R K$ sur K.

THÉORÈME 1. — *Sous les hypothèses ci-dessus, le foncteur* $G \to G \times_R K$ *est pleinement fidèle.*

Noter que, puisque K est de caractéristique zéro, le groupe G_K est *étale,* donc équivaut à la donnée d'un module galoisien T_pG, appelé le module de Tate de G. Le théorème 1 peut donc se reformuler ainsi :

THÉORÈME 1′. — *Si* G_1 *et* G_2 *sont deux groupes p-divisibles sur* R*, l'homomorphisme canonique*

$$\mathrm{Hom}_R(G_1, G_2) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}}(T_pG_1, T_pG_2)$$

est un isomorphisme.

COROLLAIRE 1. — *Si* $f : G_1 \to G_2$ *définit un isomorphisme de* T_pG_1 *sur* T_pG_2*, c'est un isomorphisme.*

COROLLAIRE 2. — *Si* G *est un groupe p-divisible, tout endomorphisme du module galoisien* T_pG *provient d'un endomorphisme de* G*.*

Pour la démonstration de ces résultats, voir TATE [13]. Indiquons simplement quelles sont les différentes étapes :

(i) On se ramène au cas où R est un *anneau de valuation discrète complet*, de caractéristique résiduelle p, et de corps résiduel algébriquement clos.

(ii) Si d et d' désignent les dimensions de G et G′ [cf. § 1, 4)], on montre que *le module galoisien* T_pG *détermine* (d, d'). On utilise pour cela les propriétés de T_pG données au § 4 ci-après (cor. au théorème 2)

(iii) On montre que le discriminant de l'algèbre A_n associée au groupe G_n est engendré par $p^{dnp^{hn}}$, cf. [13], prop. 2.

(iv) En combinant (ii) et (iii), on établit le corollaire 1.

(v) On déduit le théorème 1′ du corollaire 1 par une construction de « graphe » convenable.

3 *Remarques.* — 1) On ignore si le théorème 1 reste vrai lorsque K est un corps de caractéristique p.

2) On aimerait pouvoir compléter le théorème 1′ en disant quels sont les modules galoisiens qui sont de la forme T_pG, avec G p-divisible. Les résultats du § 4 donnent en tout cas des conditions *nécessaires* (cf. cor. au théorème 3).

§ 3. Quelques propriétés du complété de la clôture algébrique d'un corps local (TATE [13], SEN (non publié))

4

Soit R un anneau de valuation discrète complet, de corps résiduel k parfait de caractéristique p, et de corps des fractions K de caractéristique 0. Soit $\overline{\mathrm{K}}$ une clôture algébrique de K, et soit π le groupe de Galois de $\overline{\mathrm{K}}/\mathrm{K}$. On sait que la valuation de K se prolonge de manière unique en une valuation (à valeurs dans $\mathbf{Q}$) de $\overline{\mathrm{K}}$; soit C le *complété* de $\overline{\mathrm{K}}$ pour la topologie correspondante. Le groupe π *opère par continuité sur* C. TATE s'est aperçu que les propriétés du π-module C sont intimement liées à celles des groupes p-divisibles sur R (cf. § 4, ainsi que [13]). Il a été amené en particulier aux résultats suivants :

(i) *Le corps des invariants de* π *dans* C *est réduit à* K.

Cela résulte de :

(ii) *Il existe un entier* $n(\mathrm{K})$ *jouissant de la propriété suivante : Pour toute extension galoisienne finie* L/K, *d'anneau de valuation* $\mathrm{A_L}$, *le groupe* $\mathrm{H}^1(\mathrm{Gal}\,(\mathrm{L}/\mathrm{K}), \mathrm{A_L})$ *est annulé par* $p^{n(\mathrm{K})}$.

TATE démontre (ii) en « montant » de K à $\overline{\mathrm{K}}$ au moyen d'une extension intermédiaire K′ à groupe de Galois isomorphe à $\mathbf{Z}_p$ (cf. [13]).

Comme autres résultats, signalons :

(iii) *Le* K*-espace vectoriel* $\mathrm{H}^1(\pi, \mathrm{C})$ *est de dimension* 1 (noter la différence entre C et $\overline{\mathrm{K}}$!).

Soit H le module de Tate du groupe multiplicatif $\mathbf{G}_m$, et soit $\mathrm{C}(n)$ le produit tensoriel de C avec la puissance tensorielle n-ième de H. Alors :

(iv) *Si* $n \neq 0$, *on a* $\mathrm{H}^0(\pi, \mathrm{C}(n)) = \mathrm{H}^1(\pi, \mathrm{C}(n)) = 0$.

Remarque. — Shankar SEN a récemment amélioré (ii), en montrant qu'on peut prendre $n(\mathrm{K})$ égal à 1 si $p \neq 2$ et $n(\mathrm{K}) = 2$ si $p = 2$.

§ 4. La décomposition de $\mathrm{T}_p\mathrm{G} \otimes \mathrm{C}$ (TATE [13], § 4)

On conserve les notations et hypothèses du § 3, et l'on note $\mathfrak{m}$ l'idéal maximal de R. On considère un groupe p-divisible G de hauteur h sur R; on note G′ son dual.

a) Le groupe des points de G à valeurs dans R

Si N est un entier $\geqslant 1$, définissons le groupe des points de G à valeurs dans $\mathrm{R}/\mathfrak{m}^{\mathrm{N}}\mathrm{R}$ par la formule $\mathrm{G}(\mathrm{R}/\mathfrak{m}^{\mathrm{N}}\mathrm{R}) = \varinjlim \mathrm{G}_n(\mathrm{R}/\mathfrak{m}^n\mathrm{R})$ et définissons $\mathrm{G}(\mathrm{R})$ comme la limite projective des $\mathrm{G}(\mathrm{R}/\mathfrak{m}^{\mathrm{N}}\mathrm{R})$ pour $\mathrm{N} \to \infty$. Lorsque G est connexe, cette définition coïncide avec la définition habituelle des points

d'un groupe formel, au moyen de coordonnées. Dans le cas général, si t_G désigne l'espace tangent à la composante neutre G_0 de G, le *logarithme* donne un isomorphisme

$$L\colon G(R) \otimes \mathbf{Q}_p \longrightarrow t_G \otimes_R K\,.$$

b) **Le module** T_pG

Il a été défini au § 2 comme le π-module correspondant au groupe p-divisible $G \times_R K$. On peut également définir directement T_pG/p^nT_pG comme le noyau de p^n dans $G(R'_n)$, où R'_n est l'anneau de valuation d'une extension finie assez grande de K.

c) **Relations entre** G **et** G'

Soit R_C l'anneau de valuation de C. Utilisant la définition de la dualité de Cartier, on obtient un *isomorphisme*

$$T_pG' \simeq \mathrm{Hom}_{R_C}(G \times_R R_C, \mathbf{G}_m)\,.$$

Si $H = T_p(\mathbf{G}_m)$, on déduit d'abord de là un accouplement

$$T_pG' \times T_pG \longrightarrow H\,,$$

dont on montre facilement qu'il met ces deux modules en *dualité.*

Si U_C est le groupe des éléments inversibles de R_C congrus à 1, on en déduit aussi un homomorphisme

$$G(R_C) \longrightarrow \mathrm{Hom}(T_pG', U_C)\,,$$

d'où, par restriction à G(R), un homomorphisme

$$\alpha\colon G(R) \longrightarrow \mathrm{Hom}_\pi(T_pG', U_C)\,.$$

Par passage au logarithme, α définit une application K-linéaire

$$d\alpha\colon t_G \otimes K \longrightarrow \mathrm{Hom}_\pi(T_pG', C)\,.$$

THÉORÈME 2. — *Les applications* α *et* $d\alpha$ *sont des isomorphismes.*

La démonstration utilise l'égalité $h = d + d'$, ainsi que les propriétés de C énoncées au § 3 (cf. [13]).

COROLLAIRE. — *Le module galoisien* T_pG *détermine les invariants* d *et* d' *de* G.

En effet, T_pG détermine T_pG', et le th. 2 montre que $d = \mathrm{rang}\, t_G$ est égal à la dimension du K-espace vectoriel $\mathrm{Hom}_\pi(T_pG', C)$.

d) **La décomposition de Hodge de** $\mathrm{T}_p\mathrm{G} \otimes \mathrm{C}$

THÉORÈME 3. — *Le π-module* $\mathrm{T}_p\mathrm{G} \otimes \mathrm{C}$ *est canoniquement isomorphe à la somme directe*

$$t_{\mathrm{G}} \otimes \mathrm{C}(1) \ \oplus \ \mathrm{Hom}(t_{\mathrm{G}'}, \mathrm{C})\,.$$

(On note C(1) le produit tensoriel de C et de H, cf. § 3.)

Plus précisément, l'homomorphisme $d\alpha$, appliqué à G et G′, permet de définir des applications

$$0 \longrightarrow t_{\mathrm{G}} \otimes \mathrm{C}(1) \longrightarrow \mathrm{T}_p\mathrm{G} \otimes \mathrm{C} \longrightarrow \mathrm{Hom}(t_{\mathrm{G}'}, \mathrm{C}) \longrightarrow 0\,.$$

TATE démontre, par un calcul de dimensions, que cette suite est *exacte*, puis, en utilisant la propriété (iv) du § 3, il montre qu'elle se scinde de façon unique.

COROLLAIRE. — *Le π-module* $\mathrm{T}_p\mathrm{G} \otimes \mathrm{C}$ *est somme directe de d modules isomorphes à* C(1) *et de d' modules isomorphes à* C.

Remarque. — Soit X un schéma projectif et lisse sur R, et soit G le groupe p-divisible associé à la variété d'Albanese de X. On peut interpréter $\mathrm{T}_p\mathrm{G}$ comme le premier groupe de cohomologie p-adique (étale) de $\mathrm{X}_{\mathrm{C}} = \mathrm{X} \times_{\mathrm{R}} \mathrm{C}$ (à torsion près), et le théorème 3 apparaît comme un analogue p-adique de la décomposition de Hodge

$$\mathrm{H}^1(\mathrm{X}_{\mathbf{C}}) = \mathrm{H}^{1,0}(\mathrm{X}_{\mathbf{C}}) \oplus \mathrm{H}^{0,1}(\mathrm{X}_{\mathbf{C}})\,,$$

le corps C jouant le rôle du corps des nombres complexes.

On peut se demander s'il existe des décomposition analogues en dimension $\geqslant 2$ (elles ne peuvent en tout cas pas correspondre à des groupes p-divisibles — il faut trouver autre chose). Même en dimension 1, le cas d'une variété abélienne ayant mauvaise réduction n'est pas réglé. 5

§ 5. Relèvement des variétés abéliennes

Soit R un anneau artinien local de corps résiduel de caractéristique p. Soit A_0 une variété abélienne définie sur k, et soit $\mathrm{A}_0(p)$ le groupe p-divisible correspondant. Un *relèvement* de A_0 sur R est un schéma abélien A sur R muni d'un isomorphisme de la réduction $\widetilde{\mathrm{A}} = \mathrm{A} \times_{\mathrm{R}} k$ sur A_0; définition analogue pour $\mathrm{A}_0(p)$.

THÉORÈME 4. — *Les relèvements* (à isomorphisme près) *de* A_0 *et de* $\mathrm{A}_0(p)$ *se correspondent bijectivement*; *cette correspondance est fonctorielle.*

Plus correctement, soit $\mathscr{C}$ la catégorie des schémas abéliens sur R, et $\mathscr{C}(p)$ la catégorie des couples (A_0, G), où A_0 est une variété abélienne sur k et G un relèvement de $A_0(p)$ sur R. Le théorème 4 signifie que le foncteur $A \mapsto (A \times_R k, A(p))$ est une équivalence $\mathscr{C} \to \mathscr{C}(p)$.

La démonstration du théorème 4 est esquissée dans les notes de Woods Hole [4]. Elle repose essentiellement sur la technique de relèvement de GROTHENDIECK [2], combinée avec une cohomologie fabriquée par TATE.

COROLLAIRE. — *Soient* A *et* B *deux schémas abéliens sur un anneau local noethérien complet, de corps résiduel k de caractéristique p, et soient* A_0 *et* B_0 *leurs réductions. Pour qu'un homomorphisme $f_0 : A_0 \to B_0$ se relève en $f : A \to B$, il faut et il suffit que l'homomorphisme correspondant de $A_0(p)$ dans $B_0(p)$ se relève en un homomorphisme de $A(p)$ dans $B(p)$.*

Lorsque l'anneau est artinien, c'est un cas particulier du théorème 4. Le cas général en résulte, par passage à la limite, en utilisant [2].

Remarque. — Le théorème 4 équivaut à dire que la *variété formelle des modules* est la même pour une variété abélienne et pour le groupe p-divisible correspondant. Cela explique l'intérêt qui s'attache à la détermination des modules de groupes p-divisibles, et en particulier des modules de groupes formels (cf. [6], pour le cas de la dimension 1).

Un exemple : le relèvement canonique

Supposons k parfait, et prenons pour A_0 une variété abélienne de dimension r, telle que le groupe de ses points d'ordre divisant p soit de rang r (pour une courbe elliptique, c'est le cas « ordinaire », où l'invariant de Hasse est non nul.) On montre facilement que $A_0(p)$ est somme directe d'un groupe étale E_0 de hauteur r et d'un groupe M_0 de type multiplicatif. Chacun de ces groupes se relève de façon unique à R; soient E et M les groupes correspondants. Vu le théorème 4, il existe un relèvement A de A_0 tel que $A(p)$ soit isomorphe à la *somme directe* de E et de M (un relèvement pris au hasard donne simplement une *extension* de E par M). On appelle A le *relèvement canonique* de A_0; il est fonctoriel en A_0. Étant défini sur tout anneau local artinien R, de corps résiduel k, il peut aussi être défini (par passage à la limite) *sur l'anneau des vecteurs de Witt* sur k; comme l'a remarqué MUMFORD, le schéma formel ainsi obtenu est un schéma *abélien*, car toute polarisation $\lambda_0 : A_0 \to A_0'$ se relève en une polarisation λ de A.

Le foncteur « relèvement canonique » a de nombreuses propriétés agréables. Par exemple, lorsque le corps résiduel k est fini, il fournit des variétés abéliennes *de type* (CM) au sens de SHIMURA-TANIYAMA; cela résulte de la fonctorialité,

combinée avec un résultat récent de TATE [12]. Dans le cas elliptique, il n'est nullement facile d'expliciter les relations entre les invariants modulaires j_0 et j de la courbe et de son relèvement canonique. Pour $p = 5$, par exemple, et $j_0 = 1, 2, 3, 4$, on trouve que la courbe a pour anneau d'endomorphismes $\mathbf{Z} \oplus 2i\mathbf{Z}$, $\mathbf{Z} \oplus \frac{1+\sqrt{-11}}{2}\mathbf{Z}$, $\mathbf{Z} \oplus i\mathbf{Z}$ et $\mathbf{Z} \oplus \frac{1+\sqrt{-19}}{2}\mathbf{Z}$; on en déduit que j est égal à $2^3 3^3 11^3$, -2^{15}, $2^6 3^3$ et $-2^{15} 3^3$ respectivement.

§ 6. Applications et compléments

Signalons :

(1) Un théorème de prolongement des morphismes de schémas abéliens, utilisant essentiellement les théorèmes 1 et 4 (GROTHENDIECK [3]).

(2) Les hypothèses et notations étant celles du § 4, supposons que G soit *connexe* et de dimension 1. Soit L l'anneau des endomorphismes de G sur $\mathrm{R}_{\overline{\mathrm{K}}}$, et soit π_p l'image du groupe de Galois dans $\mathrm{Aut}(\mathrm{T}_p\mathrm{G})$. Le groupe π_p *contient un sous-groupe ouvert du groupe* $\mathrm{Aut}_{\mathrm{L}}(\mathrm{T}_p\mathrm{G})$*;* plus précisément les algèbres de Lie de ces deux groupes p-adiques *coïncident.* (La démonstration utilise la décomposition de Hodge de $\mathrm{T}_p\mathrm{G} \otimes \mathrm{C}$, cf. [11].)

Lorsque L est de rang h sur $\mathbf{Z}_p$, $\mathrm{Aut}_{\mathrm{L}}(\mathrm{T}_p\mathrm{G})$ s'identifie au groupe L^*, et l'on a des résultats beaucoup plus précis (ils se déduisent facilement de ceux de LUBIN-TATE [5]).

Terminons par une question (cf. [13], § 2.1) :

(3) Y a-t-il d'autres groupes p-divisibles sur $\mathbf{Z}$ que les groupes « triviaux » ? **6**

Bibliographie

[1] M. DEMAZURE et A. GROTHENDIECK, *Schémas en groupes,* SGA 3, I.H.E.S. 1963-64; L.N. **151-152-153**.

[2] A. GROTHENDIECK, *Géométrie formelle et géométrie algébrique,* Sém. Bourbaki 1958-59, exposé n° 182.

[3] A. GROTHENDIECK, *Un théorème sur les homomorphismes de schémas abéliens,* Invent. Math. **2** (1966), 59–78.

[4] J. LUBIN, J-P. SERRE et J. TATE, *Elliptic curves and formal groups,* Woods Hole Summer Institute, 1964, notes polycopiées[(1)].

[5] J. LUBIN et J. TATE, *One parameter formal Lie groups,* Ann. of Math. **80** (1964), 464–484.

[(1)] Ces notes sont accessibles via `http://www.ma.utexas.edu/users/voloch/lst.html`

[6] J. LUBIN et J. TATE, *Formal moduli for one-parameter formal Lie groups,* Bull. S.M.F. **94** (1966), 49–60.

[7] E. LUTZ, *Sur l'équation* $y^2 = x^3 - \mathrm{A}x - \mathrm{B}$ *dans les corps p-adiques,* J. reine ang. Math. **177** (1937), 237–247.

[8] Y. MANIN, *La théorie des groupes formels commutatifs sur les corps de caractéristique finie* (en russe), Usp. Mat. Nauk. **18**, (1963), 3–90. [Traduction anglaise : Russian Math. Surv. **18**, n° 6, 1–83.]

[9] J-P. SERRE, *Groupes de Lie ℓ-adiques attachés aux courbes elliptiques,* Coll. CNRS, n° 143, Clermont-Ferrand (1964), 239–256.

[10] J-P. SERRE, *Résumé des cours de 1965-1966,* Annuaire du Collège de France (1966), 49–58.

[11] J-P. SERRE, *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. conf. Local Fields (Driebergen, 1966), 118–131, Springer-Verlag, Berlin.

[12] J. TATE, *Endomorphisms of abelian varieties over finite fields,* Invent. Math. **2** (1966), 134–144.

[13] J. TATE, *p-divisible groups,* Proc. conf. Local Fields (Driebergen, 1966), 158–183, Springer-Verlag, Berlin.

Séminaire Bourbaki novembre 1977
1977-78, exposé n° 511

POINTS RATIONNELS DES COURBES MODULAIRES $X_0(N)$

d'après Barry MAZUR

Le présent exposé fait suite à ceux de 1970 et 1975 ([8], [6]). On conserve les notations de [6]. En particulier :

$\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$;

N est un nombre premier ;

$Y_0(N)$ est la courbe algébrique sur $\mathbf{Q}$ dont les points paramètrent les couples (E, A) formés d'une courbe elliptique E et d'un sous-groupe A d'ordre N de E ; on a

$$Y_0(N)(\mathbf{C}) = \{z \mid \mathrm{Im}(z) > 0\}/\Gamma_0(N);$$

$X_0(N)$ est la courbe projective obtenue en compactifiant $Y_0(N)$ par adjonction des « pointes » 0 et ∞ (qui correspondent à des couples (E, A) dégénérés, cf. [1]) ; son corps des fonctions est $\mathbf{Q}(j, j_N)$, où $j = j(z)$ est l'invariant modulaire usuel, et $j_N(z) = j(-1/Nz) = j(Nz)$;

w est l'involution canonique de $X_0(N)$; elle échange les pointes 0 et ∞, ainsi que les fonctions j et j_N.

§ 1. Résultats

Le plus important est le suivant ([5], th. 1) :

THÉORÈME 1. — *Si le nombre premier* N *n'appartient pas à l'ensemble*

$$\mathfrak{S} = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\},$$

la courbe modulaire $Y_0(N)$ *n'a aucun point rationnel sur* $\mathbf{Q}$.

Vu la propriété universelle de $Y_0(N)$, ceci équivaut à :

THÉORÈME 1′. — *Soient* E *une courbe elliptique sur* $\mathbf{Q}$ *et* A *un sous-groupe d'ordre* N *de* E *rationnel sur* $\mathbf{Q}$. *On a alors* $N \in \mathfrak{S}$.

Remarques. — 1) Dire que A est rationnel sur $\mathbf{Q}$ équivaut à dire que A, considéré comme sous-groupe de $E(\overline{\mathbf{Q}})$, est stable par $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.
2) Lorsque N appartient à $\mathfrak{S}$, la situation est la suivante :

a) pour $N = 2, 3, 5, 7, 13$, la courbe $Y_0(N)$ est unicursale, donc a une infinité de points rationnels ;

b) pour $N = 19, 43, 67, 163$, $Y_0(N)$ a un seul point rationnel, correspondant à une courbe elliptique à multiplications complexes par l'anneau des entiers de $\mathbf{Q}(\sqrt{-N})$;

c) pour $N = 17, 37$, $Y_0(N)$ a deux points rationnels, échangés par l'involution w ;

d) pour $N = 11$, $Y_0(N)$ a trois points rationnels ; l'un d'eux est du type b) ; les deux autres sont du type c).

Avant de donner la démonstration des théorèmes 1 et $1'$ (ce qui sera l'objet du § 2), en voici quelques applications, tirées de [5] :

THÉORÈME 2. — *Il existe une constante* C *telle que toute courbe elliptique sur* $\mathbf{Q}$ *soit* $\mathbf{Q}$*-isogène à au plus* C *courbes elliptiques* (à isomorphisme près).

Cela résulte du th. 1 et d'un théorème de MANIN (cf. [8]).

THÉORÈME 3 (([3], [4])). — *Si une courbe elliptique sur* $\mathbf{Q}$ *contient un point rationnel d'ordre premier* N*, on a* $N \leqslant 7$.

En effet,d'après le th. $1'$, il suffit de prouver que N est différent de 11, 13, 17, 19, 37, 43, 67, 163, ce qui est connu (voir par exemple [2]).

Compte tenu du th. IV.1.2 de [2], le th. 3 entraîne :

THÉORÈME 4. — *Soient* E *une courbe elliptique sur* $\mathbf{Q}$*, et* $E_{\mathrm{tors}}(\mathbf{Q})$ *le sous-groupe de torsion de* $E(\mathbf{Q})$. *Alors* $E_{\mathrm{tors}}(\mathbf{Q})$ *est isomorphe à l'un des groupes suivants* :

$\mathbf{Z}/m\mathbf{Z}$ $\quad (m \leqslant 10$ *et* $m = 12)$

$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}$ $\quad (m \leqslant 4)$.

Ces quinze groupes interviennent effectivement : les courbes modulaires correspondantes sont unicursales, cf. [2], p. 217.

Le th. 3, combiné à la prop. 21 de [9], entraîne :

THÉORÈME 5. — *Soit* E *une courbe elliptique sur* $\mathbf{Q}$. *Si* E *est semi-stable, et si* $N \geqslant 11$*, le groupe de Galois des points de* N*-division de* E *est isomorphe à* $\mathbf{GL}_2(\mathbf{F}_N)$.

L'hypothèse de semi-stabilité signifie que le conducteur de E est sans facteur carré, ou encore que l'on peut représenter E comme une cubique plane dont toutes les réductions modulo p sont non singulières ou ont un point double à tangentes distinctes.

Questions. — 1) Le th. 2 est-il vrai avec $C = 8$? 1

2) Le th. 5 reste-t-il valable si l'on remplace les hypothèses 2

$$\text{« E semi-stable »} \text{ et } \text{« } N \geqslant 11 \text{ »}$$

par

$$\text{« E n'a pas de multiplications complexes »} \text{ et } \text{« } N \geqslant 41 \text{ »?}$$

3) Si M n'est pas premier, est-il vrai que $Y_0(M)$ n'a pas de point rationnel en dehors des cas connus $M = 1, 4, 6, 8, 9, 10,12, 14, 15, 16, 18, 21, 27$? Compte tenu de [2], et du th.1, il suffirait de traiter les cinq cas suivants : 3

$$M = 3{\cdot}13,\ 5{\cdot}13,\ 7{\cdot}13,\ 13^2 \text{ et } 5^3.$$

4) Pour tout corps de nombres K, existe-t-il un ensemble fini S_K de nombres premiers tel que, si $N \notin S_K$, la courbe $Y_0(N)$ n'ait aucun point rationnel sur K, à part ceux provenant des courbes à multiplications complexes ? Lorsque K est quadratique imaginaire, on trouvera dans [5] un résultat partiel dans cette direction, basé sur un théorème de GOLDFELD. 4

§ 2. Démonstration des théorèmes 1 et 1′

Soit E une courbe elliptique sur $\mathbf{Q}$, munie d'un sous-groupe A rationnel sur $\mathbf{Q}$ d'ordre N. Il nous faut montrer que N appartient à l'ensemble $\mathfrak{S}$ du th. 1.

a) Propriétés de bonne réduction

PROPOSITION 1. — *Supposons* N *différent de* 2, 3, 5, 7, 13. *Alors* E *a potentiellement bonne réduction en tout nombre premier* $p \neq 2$, N.

Remarques. — 1) Dire que E a potentiellement bonne réduction en p signifie (cf. [10]) qu'il existe une extension finie du corps p-adique $\mathbf{Q}_p$ sur laquelle E acquiert bonne réduction, ou encore que l'invariant modulaire $j(E)$ de E est p-entier.

2) L'hypothèse $p \neq N$ n'est en fait pas nécessaire, cf. [5]. Il en est de même de $p \neq 2$, sauf lorsque $N = 17$.

Démonstration. — Notons x le point de $X_0(N)$ associé à (E, A) ; on a $x \neq 0, \infty$, puisque x n'est pas une « pointe ». Soit J la jacobienne de $X_0(N)$, et soit f l'application de $X_0(N)$ dans J définie par $f(P) = \mathrm{cl}((P) - (\infty))$. L'hypothèse faite sur N entraîne que $\dim J \geqslant 1$, et que f est un plongement. Notons $\pi : J \to \widetilde{J}$ la

projection de J sur son *quotient d'Eisenstein* $\widetilde{\mathrm{J}}$ (cf. [3], [6]) ; soit $\widetilde{f}$ l'application composée

$$\mathrm{X}_0(\mathrm{N}) \xrightarrow{f} \mathrm{J} \xrightarrow{\pi} \widetilde{\mathrm{J}}.$$

Posons $\mathrm{S} = \mathrm{Spec}(\mathbf{Z}) - \{2, \mathrm{N}\} = \mathrm{Spec}(\mathbf{Z}[1/2\mathrm{N}])$. On sait ([1]) que $\mathrm{X}_0(\mathrm{N})$ et J (et donc aussi $\widetilde{\mathrm{J}}$, cf. [10]) ont bonne réduction sur S (et même sur $\mathrm{Spec}(\mathbf{Z}) - \{\mathrm{N}\}$), i.e. se prolongent en des schémas projectifs et lisses sur S, que nous noterons $\mathrm{X}_0(\mathrm{N})_\mathrm{S}$, J_S et $\widetilde{\mathrm{J}}_\mathrm{S}$. Les points x, $f(x)$ et $\widetilde{f}(x)$ s'interprètent comme des S-*sections* de ces schémas, et l'on peut parler de leurs *valeurs* x_p, $f(x_p)$, $\widetilde{f}(x_p)$ en un nombre premier $p \neq 2$, N. Supposons alors que E n'ait *pas* potentiellement bonne réduction en p ; cela équivaut à dire que x_p est égal à l'une des deux pointes 0_p et ∞_p de la fibre de $\mathrm{X}_0(\mathrm{N})_\mathrm{S}$ en p. Quitte à remplacer x par $w(x)$, on peut supposer que $x_p = \infty_p$, d'où $\widetilde{f}(x_p) = 0$. Ainsi, $\widetilde{f}(x)$ s'annule en p. Or $\widetilde{f}(x)$ appartient au groupe $\widetilde{\mathrm{J}}(\mathbf{Q})$, qui est *fini* ([6], th. 2) ; on en tire, par un argument facile (où l'hypothèse $p \neq 2$ intervient), $\widetilde{f}(x) = 0$. On a donc

$$\widetilde{f}(x) = \widetilde{f}(\infty) \qquad \text{et} \qquad x_p = \infty_p ;$$

les deux sections x et ∞ de $\mathrm{X}_0(\mathrm{N})_\mathrm{S}$ ont même image par $\widetilde{f}$ et coïncident en p. Comme le morphisme $\widetilde{f} : \mathrm{X}_0(\mathrm{N})_\mathrm{S} \to \widetilde{\mathrm{J}}_\mathrm{S}$ est *non ramifié*, au sens de EGA IV.7.3.1, en tout point de la section ∞ ([5], prop. 3.1 — voir Appendice), cela entraîne $x = \infty$ d'après EGA IV.17.4.7. Cette contradiction établit la prop. 1.

b) **Action de** $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ **sur** A

Cette action est définie par un *caractère*

$$r : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_\mathrm{N}^* = \mathrm{Aut}(\mathrm{A}).$$

Du fait que $\mathbf{F}_\mathrm{N}^*$ est abélien, r se factorise à travers

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})^{\mathrm{ab}} = \mathrm{Gal}(\mathbf{Q}_{\mathrm{cycl}}/\mathbf{Q}),$$

où $\mathbf{Q}_{\mathrm{cycl}}$ désigne le corps obtenu par adjonction à $\mathbf{Q}$ de toutes les racines de l'unité. On a

$$\mathrm{Gal}(\mathbf{Q}_{\mathrm{cycl}}/\mathbf{Q}) = \prod_p \mathbf{Z}_p^* ;$$

si l'on note $r_p : \mathbf{Z}_p^* \to \mathbf{F}_\mathrm{N}^*$ la restriction de r à $\mathbf{Z}_p^*$, on a $r_p = 1$ pour presque tout p, et

$$r = \prod_p r_p .$$

PROPOSITION 2. — i) *Si $p \neq N$, le caractère r_p est d'ordre* 1, 2, 3, 4 *ou* 6.

ii) *Soit χ le caractère canonique $\mathbf{Z}_N^* \to \mathbf{F}_N^*$. Il existe un entier e, égal à* 1, 2, 3, 4 *ou* 6, *tel que*

$$(*) \qquad (r_N)^e = \chi^c, \quad \textit{avec} \quad 0 \leqslant c \leqslant e.$$

Le caractère χ est celui qui donne l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur le groupe μ_N des racines N-ièmes de l'unité.

Démonstration de i). — Du fait que r_p ne dépend que de l'action du groupe d'inertie en p, la question est *locale*. Si $j(E)$ n'est pas p-entier, E est une « courbe de Tate » sur $\mathbf{Q}_p$ (à torsion quadratique près), et la structure d'une telle courbe montre que r_p est d'ordre $\leqslant 2$. Si $j(E)$ est p-entier, il résulte de [10], § 2 (voir aussi [9], n° 5.6) que le groupe d'inertie en p opère sur les points de N-division de E à travers un groupe Φ_p d'automorphismes d'une courbe elliptique en caractéristique p ; un tel groupe Φ_p est cyclique d'ordre 1, 2, 3, 4 ou 6, ou non abélien d'ordre 12 ou 24 ; son image dans $\mathbf{F}_N^*$ est cyclique d'ordre 1, 2, 3, 4 ou 6.

Démonstration de ii). — L'argument est analogue. Si $j(E)$ n'est pas p-entier, la structure des courbes de Tate montre que $(r_N)^2 = 1$ ou χ^2. Si $j(E)$ est p-entier, il existe une extension finie de $\mathbf{Q}_p$, d'indice de ramification e égal à 1, 2, 3, 4 ou 6, sur laquelle E acquiert bonne réduction (du moins si $N \neq 2, 3$, ce que l'on peut supposer, la prop. 2 étant triviale si $N < 11$). En appliquant à cette extension la prop. 10 de [9] (ou le cor. 3.4.4 de [7]), on obtient le fait que $(r_N)^e$ est de la forme χ^c, avec $0 \leqslant c \leqslant e$.

Remarques. — 1) Le fait que $(r_p)^{12} = 1$ pour $p \neq N$ peut aussi se déduire des propriétés de ramification du revêtement $X_1(N) \to X_0(N)$, cf. [5], § 5.
2) Tout caractère $\mathbf{Z}_N^* \to \mathbf{F}_N^*$ est une puissance du caractère canonique χ, qui est d'ordre $N-1$. On a donc $r_N = \chi^k$, avec $k \in \mathbf{Z}/(N-1)\mathbf{Z}$, et la condition (*) de ii) peut s'écrire :

$$(*)' \qquad ek \equiv c \pmod{N-1}, \text{avec } 0 \leqslant c \leqslant e.$$

c) **Exploitation de** a) **et** b)

On suppose à partir de maintenant que $N \neq 2, 3, 5, 7, 13$. Soit p un nombre premier distinct de 2 et de N, et décomposons le caractère r en :

$$r = r_p \varphi_p, \quad \text{où} \quad \varphi_p = r_N \prod_{l \neq p, N} r_l.$$

Soit K_p l'extension cyclique de $\mathbf{Q}$ associée au noyau de r_p. C'est une sous-extension du corps cyclotomique $\mathbf{Q}(\mu_p)$ de degré égal à l'ordre de r_p. Elle est

totalement ramifiée en p. Notons $\mathfrak{p}$ son unique idéal premier de norme p.

PROPOSITION 3. — *Sur* K_p*, la courbe* E *a bonne réduction en* $\mathfrak{p}$.

En effet, la prop. 1 montre que E a potentiellement bonne réduction en $\mathfrak{p}$, et le groupe local $\varphi_{\mathfrak{p}}$ correspondant ([9], n° 5.6) fixe un point d'ordre N, donc est réduit à $\{1\}$, ce qui entraîne la propriété de bonne réduction cherchée, cf. [10], § 2.

On peut donc parler de la *réduction* mod. $\mathfrak{p}$ de E ; c'est une courbe elliptique sur $\mathbf{F}_p$. Notons a_p la trace de son endomorphisme de Frobenius. On a l'inégalité de Hasse :

$$(**) \qquad |a_p| \leqslant 2\sqrt{p}$$

et de plus :

PROPOSITION 4. — $a_p \equiv \varphi_p(p) + p\varphi_p(p)^{-1} \pmod{N}$.

[On identifie φ_p à un caractère de $\prod_{\ell \neq p} \mathbf{Z}_\ell^*$, ce qui donne un sens à $\varphi_p(p)$.]

Comme $\varphi_p(p) = r_N(p) \prod_{\ell \neq p, N} r_\ell(p)$, et $r_\ell(p)^{12} = 1$ pour $\ell \neq p$, N, on en déduit :

COROLLAIRE. — *Avec les notations de* $(*)'$*, on a*

$$(***) \qquad a_p \equiv \omega_p p^k + \omega_p^{-1} p^{1-k} \pmod{N},$$

où $\omega_p \in \mathbf{F}_N^*$ *est tel que* $\omega_p^{12} = 1$.

Démonstration de la prop. 4. — Soit $G \subset \mathbf{GL}_2(\mathbf{F}_N)$ le groupe de Galois obtenu par adjonction des points de N-division de E. Vu la prop. 3, cette extension est non ramifiée en $\mathfrak{p}$. Soit $\sigma_{\mathfrak{p}} \in G$ l'élément de Frobenius correspondant. On sait que

$$\mathrm{Tr}(\sigma_{\mathfrak{p}}) \equiv a_p \pmod{N}.$$

D'autre part, $\sigma_{\mathfrak{p}}$ agit sur A par homothétie de rapport $\varphi_p(p)$. L'une des valeurs propres de $\sigma_{\mathfrak{p}}$ est donc $\varphi_p(p)$ et l'autre est $p\varphi_p(p)^{-1}$ puisque $\det(\sigma_{\mathfrak{p}}) \equiv p \pmod{N}$. D'où

$$\mathrm{Tr}(\sigma_{\mathfrak{p}}) \equiv \varphi_p(p) + p\varphi_p(p)^{-1} \pmod{N},$$

ce qui démontre la proposition.

d) **Fin de la démonstration**

Revenons aux notations de $(*)'$: on a $ek \equiv c \pmod{N-1}$, avec $e = 1, 2, 3, 4, 6$ et $0 \leqslant c \leqslant e$; on en déduit que c est divisible par $\gcd(e, N-1)$, et le rapport c/e ne peut prendre que les valeurs suivantes :

$c/e = 0$ ou 1

$c/e = 1/3$ ou $2/3$ [si $e = 3$ ou 6, et $3 \nmid (N-1)$]

$c/e = 1/2$ [si $e = 4$ et $4 \nmid (N-1)$].

(Dans [5], § 5, MAZUR remarque que ces cinq valeurs correspondent aux cinq possibilités de [6], th. 6 ; nous n'utiliserons pas ce fait.)

Nous allons examiner successivement ces différents cas.

d_1) *Le cas* $c/e = 0$ *ou* 1

Soient $f_{i,p}(X)$, $1 \leqslant i \leqslant 4$, les polynômes suivants :

$f_{1,p}(X) = X + p + 1$;

$f_{2,p}(X) = X^2 + (p-1)^2$;

$f_{3,p}(X) = X^2 + (p+1)X + p^2 - p + 1$;

$f_{4,p}(X) = X^4 - (p^2 + 4p + 1)X^2 + (p^2 + p + 1)^2$.

LEMME 1. — *Supposons* E *de type* d_1). *Alors, pour tout* $p \neq 2$, N, *il existe* $i \in \{1, 2, 3, 4\}$ *et* $a \in \mathbf{Z}$ *tels que* $|a| \leqslant 2\sqrt{p}$ *et* $N | f_{i,p}(a)$.

Démonstration. — Puisque $c/e = 0$ ou 1, on a $ek \equiv 0$ ou $e \bmod (N-1)$, et d'après $(***)$, on en déduit

$$a_p \equiv \varepsilon_p + \varepsilon_p^{-1} p \pmod{N},$$

où $\varepsilon_p \in \mathbf{F}_N^*$ est d'ordre $1, 2, 3, 4, 6$ ou 12. Supposons par exemple que ε_p soit d'ordre 3 ou 6, i.e. que

$$\varepsilon_p + \varepsilon_p^{-1} \pm 1 \equiv 0 \pmod{N}.$$

En développant le produit $(a_p - \varepsilon_p - \varepsilon_p^{-1} p)(a_p - \varepsilon_p^{-1} - \varepsilon_p p)$, on voit que

$$a_p^2 \pm (p+1) a_p + p^2 - p + 1 \equiv 0 \pmod{N},$$

ce qui montre que N divise $f_{3,p}(\pm a_p)$, D'où le lemme dans ce cas. Lorsque ε_p est d'ordre 1 ou 2 (resp. 4, resp. 12), on utilise le polynôme $f_{1,p}$ (resp. $f_{2,p}$, resp. $f_{4,p}$).

Il est maintenant facile de conclure. Prenons en effet $p = 3$. La condition $|a| \leqslant 2\sqrt{p}$ signifie que $a = 0, \pm 1, \pm 2, \pm 3$; les valeurs des $f_{i,3}(X)$ en ces entiers sont les nombres

$$1, 2, 3, 4, 5, 6, 7;\ 4, 5, 8, 13;\ 3, 4, 7, 12, 19, 28;\ 52, 97, 148, 169.$$

Leurs diviseurs premiers sont $2, 3, 5, 7, 13, 19, 37, 97$ qui appartiennent tous à $\mathfrak{S}$, sauf 97. Pour montrer que N ne peut être égal à 97, on peut, soit invoquer des résultats connus (cf. [2]), soit recommencer le même calcul pour $p = 5$; on trouve alors pour valeurs des polynômes $f_{i,5}(\mathrm{X})$ les entiers

$$2, 3, 4, 5, 6, 7, 8, 9, 10;\quad 16, 17, 20, 25, 32;\quad 12, 13, 16, 21, 28, 37, 48, 61;$$
$$481, 628, 793, 916, 961,$$

et l'on constate que 97 ne divise aucun d'entre eux.

d_2) *Le cas* $c/e = 1/3$ *ou* $2/3$ $(3 \nmid (\mathrm{N}-1))$

Soient $f_{i,p}(\mathrm{X})$, $i = 5$, 6, les polynômes suivants :

$f_{5,p} = \mathrm{X}^3 - 3p\mathrm{X} + p^2 + p$;

$f_{6,p} = (\mathrm{X}^3 - 3p\mathrm{X})^2 + (p^2 - p)^2$.

Lemme 2. — *Supposons* E *de type* d_2). *Alors, pour tout* $p \neq 2$, N, *il existe* $i \in \{5, 6\}$ *et* $a \in \mathbf{Z}$ *tels que* $|a| \leqslant 2\sqrt{p}$ *et* $\mathrm{N} | f_{i,p}(a)$.

Démonstration. — On procède comme pour le lemme 1. On a d'après (iii),

$$a_p \equiv \varepsilon_p p^h + \varepsilon_p^{-1} p^{1-h} \pmod{\mathrm{N}},$$

avec $3h \equiv 1 \pmod{\mathrm{N}-1}$, et $\varepsilon_p^{12} = 1$. D'où ;

$$a_p^3 - 3pa_p \equiv \varepsilon_p^3 p + \varepsilon_p^{-3} p^2 \pmod{\mathrm{N}}.$$

Si ε_p^3 est d'ordre 1 (resp. 2, resp. 4), cette congruence montre que N divise $f_{5,p}(-a_p)$ (resp. $f_{5,p}(a_p)$, resp. $f_{6,p}(a_p)$). D'où le lemme.

Comme ci-dessus on applique le lemme avec $p = 3$. Les valeurs de $f_{5,3}(\mathrm{X})$ et $f_{6,3}(\mathrm{X})$ pour $\mathrm{X} = 0, \pm 1, \pm 2, \pm 3$ sont :

$$2, 4, 12, 20, 22;\ 36, 100, 136.$$

Leurs diviseurs premiers sont 2, 3, 5, 11, 17, qui appartiennent tous à $\mathfrak{S}$.

d_3) *Le cas* $c/e = 1/2$ $(4 \nmid (\mathrm{N}-1))$

Lemme 3. — *Supposons* E *de type* d_3). *Alors, pour tout* p *tel que* $2 < p < \mathrm{N}/4$, *on a* $\left(\frac{p}{\mathrm{N}}\right) = -1$.

Démonstration. — On a, d'après (iii),

$$a_p \equiv \varepsilon_p p^h + \varepsilon_p^{-1} p^{1-h} \pmod{\mathrm{N}},$$

avec $2h = 1 + (\mathrm{N}-1)/2$ et $\varepsilon_p^{12} = 1$. D'où :

$$a_p^2 - 2p \equiv (\varepsilon_p^2 + \varepsilon_p^{-2}) p^{1+(\mathrm{N}-1)/2} \pmod{\mathrm{N}}.$$

Du fait que 4 ne divise pas $N-1$, l'ordre de ε_p divise 6 et celui de ε_p^2 divise 3. On a donc

$$\varepsilon_p^2 + \varepsilon_p^{-2} \equiv \ 2 \ \text{ ou } \ -1 \pmod{N}.$$

Supposons alors que $\left(\frac{p}{N}\right) \equiv p^{(N-1)/2}$ soit égal à 1. Il vient :

$$a_p^2 - 2p \equiv \ 2p \ \text{ ou } \ -p \pmod{N},$$

d'où $a_p^2 \equiv 4p$ ou $p \pmod{N}$. Si en outre on a $N > 4p$, N est strictement plus grand que $|a_p^2 - 4p|$ et $|a_p^2 - p|$, et la congruence ci-dessus entraîne que a_p^2 est égal à $4p$ ou à p, ce qui est absurde. D'où le lemme.

LEMME 4. — *Si* $4 \nmid (N-1)$, *et si* $\left(\frac{p}{N}\right) = -1$ *pour tout* p *tel que* $2 < p < N/4$, *le nombre de classes du corps* $\mathbf{Q}(\sqrt{-N})$ *est égal à* 1.

Démonstration. — L'hypothèse faite sur N équivaut à dire que tout idéal du corps $\mathbf{Q}(\sqrt{-N})$ dont la norme est impaire et $< N/4$ est engendré par un élément de $\mathbf{Z}$. Distinguons alors deux cas :

α) $N \equiv 3 \pmod{8}$

On a $\left(\frac{2}{N}\right) = -1$, de sorte que tout idéal entier du corps $\mathbf{Q}(\sqrt{-N})$ de norme $< N/4$ est principal. D'après un théorème de MINKOWSKI, cela entraîne que le nombre de classes du corps est 1.

β) $N \equiv -1 \pmod{8}$

Nous allons voir que ce cas est impossible (N étant supposé > 7). Posons en effet $x = (1+\sqrt{-N})/2$ si $N \equiv 7 \pmod{16}$, et $x = (3+\sqrt{-N})/2$ si $N \equiv -1 \pmod{16}$. On vérifie que la norme de x est de la forme $2m$, avec m impair, $1 < m < N/4$. Il en résulte, d'après ce qui a été vu plus haut, que l'idéal (x) est produit d'un idéal de norme 2 par un idéal (a) engendré par un élément a de $\mathbf{Z}$, avec $a > 1$. L'élément x est donc divisible par a, ce qui est absurde puisque $\{1, x\}$ est une base de l'anneau des entiers de $\mathbf{Q}(\sqrt{-N})$.

Une fois les lemmes 3 et 4 démontrés, on n'a plus qu'à appliquer le théorème de Heegner-Stark-Baker (cf. [11]) pour conclure que N est égal à 11, 19, 43, 67 ou 163 ; cela achève la démonstration des théorèmes 1 et 1′.

Remarque. — La démonstration ci-dessus se simplifie considérablement si l'on n'a en vue que les théorèmes 3, 4 et 5 : les cas d_2) et d_3) n'interviennent pas. Par exemple, dans le cas du th. 3, on suppose que E a un point rationnel d'ordre N, i.e. que le caractère r est trivial. La prop. 3 montre alors que E a bonne réduction en tout $p \neq 2$, N, d'où le fait que N divise $p + 1 - a_p$ (cf. prop. 4) ; or c'est absurde si $p = 3$, car $p + 1 - a_p$ est compris entre 1 et 7. On a donc $N \in \{2, 3, 5, 7, 13\}$ et le cas $N = 13$ est exclu par un théorème de BLASS-MAZUR-TATE (voir [2]). D'où $N \leqslant 7$.

Appendice

Il s'agit de prouver le résultat suivant, utilisé dans la démonstration de la prop. 1 :

THÉORÈME. — *Le morphisme* $\widetilde{f} : \mathrm{X}_0(\mathrm{N})_{\mathrm{S}} \to \widetilde{\mathrm{J}}_{\mathrm{S}}$ *est non ramifié en tout point de la section* ∞.

Rappelons que $\mathrm{S} = \mathrm{Spec}(\mathbf{Z}) - \{2, \mathrm{N}\}$.

Soit B le noyau de $\pi : \mathrm{J} \to \widetilde{\mathrm{J}}$; c'est une sous-variété abélienne de J. Puisque J a bonne réduction sur S, il en est de même de B ; notons B_{S} son modèle de Néron. L'injection $\mathrm{B} \to \mathrm{J}$ se prolonge en un morphisme $\mathrm{B}_{\mathrm{S}} \to \mathrm{J}_{\mathrm{S}}$ dont l'image est l'adhérence $\overline{\mathrm{B}}$ de B dans J_{S}. RAYNAUD et MAZUR ont démontré que le morphisme $\mathrm{B}_{\mathrm{S}} \to \overline{\mathrm{B}}$ ainsi défini est un *isomorphisme*, de sorte que $\widetilde{\mathrm{J}}_{\mathrm{S}}$ s'identifie au quotient $\mathrm{J}_{\mathrm{S}}/\mathrm{B}_{\mathrm{S}}$, et que le morphisme $\pi : \mathrm{J}_{\mathrm{S}} \to \widetilde{\mathrm{J}}_{\mathrm{S}}$ est *lisse* ; la démonstration utilise le th. 3.3.3 de [7], appliqué à un sous-schéma en groupes fini convenable B_{S} (pour plus de détails, voir [5], § 1) ; le fait que Spec(S) ne contienne pas 2 est ici essentiel.

Supposons maintenant que $\widetilde{f}$ soit ramifié en un point de la section ∞, dont l'image dans S est le nombre premier p. Si l'on convient de noter par un indice p les fibres en p, cela signifie que l'application tangente en ∞_p à $\widetilde{f}_p : \mathrm{X}_0(\mathrm{N})_p \to \widetilde{\mathrm{J}}_p$ est nulle. Cette propriété peut se reformuler en termes de formes différentielles (i.e. de formes modulaires de poids 2) :

Notons Ω_p (resp. $\widetilde{\Omega}_p$) l'espace des formes invariantes sur J_p (resp. sur $\widetilde{\mathrm{J}}_p$) ; du fait que $\mathrm{J}_p \to \widetilde{\mathrm{J}}_p$ est lisse, on peut identifier $\widetilde{\Omega}_p$ à un sous-espace de Ω_p, qui lui-même s'identifie à l'espace des formes de première espèce sur $\mathrm{X}_0(\mathrm{N})_p$. Si $\omega \in \Omega_p$, on développe ω au voisinage de ∞_p à la manière habituelle (qui garde un sens en caractéristique p, on le sait) :

$$\omega = \big(a_1(\omega)q + \cdots + a_n(\omega)q^n + \cdots\big)\frac{dq}{q}.$$

Le fait que la différentielle de $\widetilde{f}_p$ soit nulle en ∞_p se traduit par la propriété :

$$a_1(\omega) = 0 \quad \text{pour tout } \omega \in \widetilde{\Omega}_p.$$

Mais $\widetilde{\Omega}_p$ est non nul (car $\dim \widetilde{\mathrm{J}} \geqslant 1$), et stable par les opérateurs de Hecke. Comme ces opérateurs commutent entre eux, ils ont un vecteur propre commun $\omega \neq 0$ dans $\widetilde{\Omega}_p$. Des formules standard permettent alors d'exprimer les $a_n(\omega)$ comme des multiples de $a_1(\omega)$; comme $a_1(\omega)$ est nul, il en est de même de tous les $a_n(\omega)$, et l'on a $\omega = 0$; contradiction !

Bibliographie

[1] P. Deligne et M. Rapoport, *Les schémas de modules de courbes elliptiques*, Lect. Notes in Math. **349**, 143–316, Springer-Verlag, 1973.

[2] D. Kubert, *Universal bounds on torsion of elliptic curves*, Proc. London Math. Soc. (3), **33** (1976), 193–237.

[3] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1978), 35–193.

[4] B. Mazur, *Rational points on modular curves*, Lect. Notes in Math. **601**, 107–148, Springer-Verlag, 1977.

[5] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[6] B. Mazur et J-P. Serre, *Points rationnels des courbes modulaires* $X_0(N)$, Séminaire Bourbaki 1974/75, exposé n° 469, Lect. Notes in Math. **514**, 238–255, Springer-Verlag, 1976.

[7] M. Raynaud, *Schémas en groupes de type* $(p, ..., p)$, Bull. S.M.F. **102** (1974), 241–280.

[8] J-P. Serre, *p-torsion des courbes elliptiques* (*d'après* Y. Manin), Séminaire Bourbaki 1969/70, exposé n° 380, Lect. Notes in Math. **180**, 281–294, Springer-Verlag, 1971.

[9] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[10] J-P. Serre et J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[11] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Mich. Math. J. **14** (1967), 1–27.

Séminaire Bourbaki juin 1999
1998-99, exposé n° 864

SOUS-GROUPES FINIS DES GROUPES DE LIE

Introduction

Les sous-groupes finis du groupe des rotations $\mathrm{SO}_3(\mathbf{R})$ sont bien connus. Ce sont :

les groupes cycliques C_n d'ordre $n = 1, 2, \ldots$;
les groupes diédraux D_n d'ordre $2n$, $n = 2, 3, \ldots$;
le groupe alterné Alt_4 d'ordre 12 ;
le groupe symétrique Sym_4 d'ordre 24 ;
le groupe alterné Alt_5 d'ordre 60.

On aimerait avoir une liste analogue pour d'autres groupes de Lie compacts, ou d'autres groupes algébriques (en caractéristique zéro, et même en caractéristique > 0). Ce serait utile pour beaucoup de questions (représentations ℓ-adiques, par exemple). Bien sûr, c'est trop demander, vu que tout groupe fini se plonge dans un groupe unitaire convenable ! On va voir que l'on peut tout de même dire pas mal de choses si l'on se borne à des groupes finis qui sont, soit abéliens, soit simples.

Hypothèses et notations

Plutôt que de travailler dans la catégorie des groupes de Lie compacts, on préfère se placer dans celle des groupes réductifs complexes. Cela ne change rien : on sait que, si K est un groupe de Lie compact, il possède un complexifié G qui est un groupe réductif sur $\mathbf{C}$; le groupe K est un sous-groupe compact maximal de $\mathrm{G}(\mathbf{C})$. Tout sous-groupe fini de $\mathrm{G}(\mathbf{C})$ est conjugué à un sous-groupe de K ; de plus, K « contrôle la fusion de K dans $\mathrm{G}(\mathbf{C})$ » au sens suivant : si A, B sont deux sous-groupes de K, et si $g \in \mathrm{G}(\mathbf{C})$ est tel que $g\mathrm{A}g^{-1} = \mathrm{B}$,

il existe un élément g_0 de K tel que $g_0 a g_0^{-1} = gag^{-1}$ pour tout $a \in A$ (cela se déduit de la décomposition de Cartan de $G(\mathbf{C})$). 1

(Dans le cas particulier $K = SO_3(\mathbf{R})$, on a $G = PGL_2$, de sorte que les groupes $C_n, D_n, \ldots$, Alt_5 s'interprètent comme des sous-groupes finis de $PGL_2(\mathbf{C})$, c'est-à-dire comme des groupes finis d'automorphismes de la droite projective.)

Dans ce qui suit, on adoptera le point de vue des groupes algébriques (qui a, entre autres avantages, celui de permettre des réductions modulo p). On fixe un corps k algébriquement clos de caractéristique zéro, ainsi qu'un groupe réductif connexe G défini sur k ; on se permet d'identifier G à $G(k)$. Le cas le plus intéressant est celui où G est « presque simple », i.e. semi-simple à système de racines irréductible ; le groupe adjoint G^{ad} est alors un groupe simple, au sens usuel du terme.

1. Le cas (presque) abélien

Lorsque $G = PGL_2$ les sous-groupes abéliens finis de G sont les groupes cycliques C_n et le groupe diédral D_2 qui est abélien élémentaire de type $(2, 2)$. Les C_n sont contenus dans un tore maximal, alors que D_2 ne l'est pas ; le nombre premier $p = 2$ joue donc un rôle particulier pour PGL_2. Nous allons trouver une situation analogue dans le cas général.

1.1. Sous-groupes toraux. — Un sous-groupe fini A de G est dit *toral* s'il est contenu dans un tore maximal T de G. La structure d'un tel sous-groupe est évidente : si $r = \dim T$ est le rang de G, A peut être engendré par r éléments ; inversement, tout groupe abélien ayant cette propriété est isomorphe à un sous-groupe toral de G.

Soit $N = N_G(T)$ le normalisateur de T dans G. Le quotient $W = N/T$ est le *groupe de Weyl* de G (plus correctement : du couple (G, T)). Ce groupe opère sur T par conjugaison, et il contrôle la fusion de T dans G :

1.1.1. *Si* A *et* B *sont des sous-groupes de* T*, et si* $g \in G$ *est tel que* $gAg^{-1} = B$*, il existe* $w \in W$ *tel que* $w(a) = gag^{-1}$ *pour tout* $a \in A$.

Cet énoncé est l'exact analogue d'un théorème de BURNSIDE sur les sous-groupes du centre d'un p-groupe de Sylow. Il se démontre de la même manière : on remarque que T et $g^{-1}Tg$ sont des tores maximaux du centralisateur $Z_G(A)$ de A, donc sont conjugués par $Z_G(A)$. Cela permet de remplacer g par un élément de N ; d'où le résultat cherché.

Les groupes abéliens ayant très peu de générateurs sont toraux :

1.1.2. *Soit* A *un sous-groupe abélien fini de* G. *Alors* A *est toral dans chacun des deux cas suivants* :

a) A *est cyclique*;

b) G *est simplement connexe, et* A *est engendré par deux éléments.*

Le cas a) est immédiat : tout élément d'ordre fini est semi-simple, donc contenu dans un tore maximal. Dans le cas b), supposons A engendré par x, y. Du fait que G est simplement connexe, le centralisateur $Z_G(x)$ est connexe. Le même argument que dans a) montre qu'il existe un tore maximal T de $Z_G(x)$ qui contient y. Ce tore est un tore maximal de G et il contient x, donc A.

1.2. Plongements dans N. — A défaut de pouvoir plonger un groupe abélien fini dans un tore maximal, on peut essayer de le plonger dans le normalisateur d'un tel tore. C'est toujours possible. Plus généralement (cf. Borel-Serre [6], Borel-Mostow [5] et Springer-Steinberg [33], II.5.6) :

1.2.1. *Soit* A *un sous-groupe fini hyper-résoluble de* G. *Il existe un tore maximal* T *de* G *dont le normalisateur* N *contient* A.

Rappelons qu'un groupe A est dit hyper-résoluble (« supersolvable ») s'il admet une suite de composition :

$$1 = A_0 \subset A_1 \subset \cdots \subset A_n = A,$$

où les A_i sont normaux dans A, et A_i/A_{i-1} est cyclique pour tout $i \geqslant 1$. On a les implications :

$$\text{abélien} \Longrightarrow \text{nilpotent} \Longrightarrow \text{hyper-résoluble} \Longrightarrow \text{résoluble}.$$

Voici une application simple de 1.2.1 :

1.2.2. *Soit p un nombre premier ne divisant pas l'ordre du groupe de Weyl* W. *Si* A *est un p-groupe contenu dans* G, A *est abélien et toral.*

En effet, on peut supposer, d'après 1.2.1, que A est contenu dans N. Vu l'hypothèse faite sur p, son image dans $W = N/T$ est triviale. Il est donc contenu dans T.

Remarque : Le groupe N est une extension, en général non triviale, de W par T. On trouvera dans Tits ([35], [36]) une description de cette extension, en termes d'un certain groupe fini $N_{\mathbf{Z}}$ défini explicitement par générateurs et relations ; voir aussi Bourbaki, LIE IX, p. 115, exerc. 12.

1.3. Nombres premiers de torsion

(Références : Borel [4], Steinberg [34] et Bourbaki, LIE IX, p. 120–121, exerc. 7 à 12.)

Un nombre premier p est dit *de torsion* (pour G) s'il vérifie les conditions équivalentes suivantes :

a) *Il existe un p-sous-groupe abélien de* G *qui n'est pas toral.*

a′) *Il existe un p-sous-groupe abélien élémentaire de* G*, de rang* $\leqslant 3$*, qui n'est pas toral.*

On note Tors(G) l'ensemble de ces nombres premiers ; d'après 1.2.2, c'est un sous-ensemble de l'ensemble des diviseurs premiers de l'ordre de W. Dans le cas particulier où $G = PGL_2$, on a $Tors(G) = \{2\}$.

Le terme de « torsion » provient du résultat suivant, dans lequel je suppose que $k = \mathbf{C}$ (sinon il faut faire intervenir la cohomologie étale) :

1.3.1. (cf. [4], [34]) *Pour que p appartienne à* Tors(G)*, il faut et il suffit que l'un des groupes d'homologie* $H_i(G, \mathbf{Z})$ *contienne un élément d'ordre p.*

(Noter qu'il revient au même de considérer l'homologie de $G = G(\mathbf{C})$ ou celle d'un compact maximal K, car $G(\mathbf{C})$ et K ont même type d'homotopie.)

On trouvera dans [4] et [34] une longue liste de propriétés caractérisant les éléments de Tors(G). En voici quelques-unes :

1.3.2. *On a* $Tors(G) = Tors(G')$*, où* G' *est le groupe dérivé de* G.

Comme G' est semi-simple, cela ramène l'étude de Tors(G) au cas où G est semi-simple. Dans ce cas, notons $\overline{G}$ le revêtement universel de G, notons $\pi_1(G)$ le noyau de $\overline{G} \to G$ et soit $Tors(\pi_1(G))$ l'ensemble des nombres premiers qui divisent l'ordre du groupe fini $\pi_1(G)$. Alors :

1.3.3. *On a* $Tors(G) = \cup_H Tors(\pi_1(H'))$*, où* H *parcourt les sous-groupes réductifs connexes de* G *ayant même rang que* G.

1.3.4. *On a* $Tors(G) = Tors(\overline{G}) \cup Tors(\pi_1(G))$.

Cet énoncé ramène la détermination de Tors(G) au cas où G est simplement connexe. En utilisant 1.3.3, on en déduit (cf. [4], [34]) :

1.3.5. *Supposons* G *simplement connexe et presque simple. Soit* (α_i) *une base de son système de racines, soit* β *la plus grande racine, et écrivons la racine duale* $\beta^\vee$ *de* β *sous la forme* :

$$\beta^\vee = \sum n_i \alpha_i^\vee,$$

où les n_i *sont des entiers* > 0*. Alors, pour que p soit de torsion pour* G*, il faut et il suffit qu'on ait* $p \leqslant \sup(n_i)$.

D'où :

1.3.6. *Supposons* G *simplement connexe et presque simple. Alors* :

$Tors(G) = \varnothing$ *si* G *est de type* A_n *ou* C_n ;

$Tors(G) = \{2\}$ *si* G *est de type* B_n $(n \geqslant 3)$, D_n $(n \geqslant 4)$ *ou* G_2 ;

$\mathrm{Tors}(\mathrm{G}) = \{2,3\}$ *si* G *est de type* F_4, E_6 *ou* E_7 ;
$\mathrm{Tors}(\mathrm{G}) = \{2,3,5\}$ *si* G *est de type* E_8.

1.4. Exemples de groupes abéliens élémentaires non toraux

(Références : Adams [1], Borel [4], Borel-Serre [6], Cohen-Seitz [10], Steinberg [34] et (surtout) Griess [17].)

Je me borne à deux exemples, l'un relatif à $p = 2$ et l'autre à $p = 5$.

1.4.1. Supposons que -1 appartienne au groupe de Weyl W ; c'est le cas pour les groupes de type A_1, B_n, C_n, D_n (n pair), G_2, F_4, E_7, E_8. Soit $g \in \mathrm{N}$ un représentant de l'élément -1 de W. On peut montrer que g^2 est d'ordre 1 ou 2, et appartient au centre de G. Supposons que $g^2 = 1$ (c'est le cas si G est de type adjoint). Soit A le groupe engendré par g et par les éléments d'ordre 2 de T ; c'est un groupe abélien élémentaire d'ordre 2^{n+1}, où n est le rang de G, i.e. la dimension de T. *Ce groupe n'est pas toral*; on peut même montrer que son centralisateur $\mathrm{Z}_\mathrm{G}(\mathrm{A})$ est fini.

Lorsque G est PGL_2, le groupe A est le groupe diédral D_2. Lorsque G est de type G_2, F_4 ou E_8, A est d'ordre 2^3, 2^5, 2^9 ; de tels sous-groupes jouent un grand rôle dans la cohomologie (usuelle — ou galoisienne) du groupe G. Noter que, dans ces trois cas, A est un sous-groupe élémentaire *maximal* de G : de façon générale, si G est simplement connexe, les p-sous-groupes abéliens de G sont de rang $\leqslant n+1$ si $p = 2$, et de rang $\leqslant n$ si $p > 2$, cf. Borel [4] et Cohen-Seitz [10].

1.4.2. Le groupe $\mathrm{G} = \mathrm{E}_8$ contient un élément z d'ordre 5 dont le centralisateur $\mathrm{Z}_\mathrm{G}(z)$ est de la forme $\mathrm{G}_1 \cdot \mathrm{G}_2$, où G_1 et G_2 sont isomorphes à SL_5, commutent, et ont pour intersection $\langle z \rangle$ (cela se déduit du diagramme de Dynkin complété de E_8 en remarquant que, si l'on en retranche la racine simple qui a le coefficient 5 dans la plus grande racine, on trouve deux diagrammes de type A_4). Dans $\mathrm{G}_1 = \mathrm{SL}_5$, il est facile de trouver des éléments x_1 , y_1 d'ordre 5 tels que $x_1 y_1 x_1^{-1} y_1^{-1} = z$; de même, il existe dans G_2 des éléments x_2 , y_2 d'ordre 5 tels que $x_2 y_2 x_2^{-1} y_2^{-1} = z^{-1}$. Si l'on pose $x = x_1 x_2$ et $y = y_1 y_2$, on constate que le groupe $\mathrm{A} = \langle x, y, z \rangle$ est abélien élémentaire d'ordre 5^3. *Ce groupe n'est pas toral*; on peut même montrer que $\mathrm{Z}_\mathrm{G}(\mathrm{A})$ est égal à A.

1.5. Relations entre cohomologie galoisienne et sous-groupes non toraux

Qu'il existe de telles relations est connu depuis longtemps. Voici deux exemples :

1.5.1 (Grothendieck [23]). *Les deux propriétés suivantes sont équivalentes* :

a) $\mathrm{Tors}(\mathrm{G}) = \varnothing$ (cela équivaut à dire que tout sous-groupe abélien de G est toral).

b) $\mathrm{H}^1(\mathrm{K}, \mathrm{G}) = 0$ *pour toute extension* K *de* k.

(Pour la définition de $\mathrm{H}^1(\mathrm{K}, \mathrm{G})$, voir par exemple [30].)

Lorsque G est semi-simple, ces propriétés sont satisfaites si et seulement si G est un produit de groupes simplement connexes de type A ou C, cf. § 1.3. Un tel groupe est parfois dit « spécial ».

1.5.2. *Supposons que* G *soit égal à* PGL_2, *ou soit de type* G_2. *Soit* A *le* 2*-sous-groupe élémentaire non toral de* G *défini dans* 1.4.1. *Alors, pour toute extension* K *de* k, *l'application* $\mathrm{H}^1(\mathrm{K}, \mathrm{A}) \to \mathrm{H}^1(\mathrm{K}, \mathrm{G})$ *est surjective.*

Noter que $\mathrm{H}^1(\mathrm{K}, \mathrm{A})$ n'est autre que $\mathrm{Hom}(\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K}), \mathrm{A})$. Dans le cas de PGL_2, les éléments de $\mathrm{H}^1(\mathrm{K}, \mathrm{A})$ peuvent donc s'interpréter comme des couples (λ, μ) d'éléments de $\mathrm{K}^*/\mathrm{K}^{*2}$ et l'élément correspondant de $\mathrm{H}^1(\mathrm{K}, \mathrm{PGL}_2)$ est l'algèbre de quaternions définie par deux générateurs i et j soumis aux relations

$$i^2 = \lambda\ , \quad j^2 = \mu\ , \quad ij = -ji.$$

Même chose pour G_2, les quaternions étant remplacés par les octonions.

L'énoncé 1.5.2, pour agréable qu'il soit, ne donne pas de moyen de prouver la non trivialité des éléments de $\mathrm{H}^1(\mathrm{K}, \mathrm{G})$ ainsi obtenus ; il faut le compléter par la construction d'*invariants cohomologiques*, cf. [30], §§ 6,7 et [25], § 31. Tout récemment, Reichstein et Youssin [29] ont obtenu un résultat bien plus satisfaisant. Pour le formuler, il faut d'abord définir la *dimension essentielle* $\mathrm{ed}(x)$ d'un élément x de $\mathrm{H}^1(\mathrm{K}, \mathrm{G})$: c'est la borne inférieure des degrés de transcendance sur k des sous-extensions K' de K telles que x appartienne à l'image de $\mathrm{H}^1(\mathrm{K}', \mathrm{G}) \to \mathrm{H}^1(\mathrm{K}, \mathrm{G})$. (En termes plus géométriques — et plus vagues — c'est le nombre minimum de paramètres dont on a besoin pour écrire le G-torseur x.) La borne supérieure des $\mathrm{ed}(x)$, quand K et x varient, est la *dimension essentielle* de G ; elle est notée $\mathrm{ed}(\mathrm{G})$. Nous pouvons maintenant énoncer le théorème principal de [29] :

1.5.3. *Si* G *contient un* p*-sous-groupe abélien élémentaire* A *dont le centralisateur est fini, on a* $\mathrm{ed}(\mathrm{G}) \geqslant \mathrm{rang}(\mathrm{A})$.

En combinant cet énoncé avec 1.4.1, on obtient :

1.5.4. *On a* $\mathrm{ed}(\mathrm{E}_7^{\mathrm{ad}}) \geqslant 8$ et $\mathrm{ed}(\mathrm{E}_8) \geqslant 9$.

Ainsi, il existe des E_8-torseurs dont la construction exige au moins 9 paramètres !

Remarques

1) L'hypothèse faite sur A dans 1.5.3 est équivalente à dire que A n'appartient à aucun sous-groupe parabolique propre de G. Elle entraîne que A n'est pas toral.

2) L'énoncé démontré dans [29] est plus précis que 1.5.3 ; c'est :

$$\mathrm{ed}(G;p) \geqslant \mathrm{rang}(A),$$

où $\mathrm{ed}(G;p)$ est la dimension essentielle de G « en p » (i.e. en considérant comme négligeables les extensions de corps de degré premier à p).

3) Les démonstrations de [29] utilisent la *résolution des singularités* (sous forme équivariante). Elles ne s'étendent pas, pour l'instant, aux corps de caractéristique $\neq 0$.

2. Le cas (presque) simple

On va maintenant s'intéresser aux plongements d'un groupe simple S (fini, non abélien) dans G.

Il est commode de considérer, plus généralement, les plongements des groupes $\overline{S}$ qui sont des extensions centrales de S (on peut imposer à $\overline{S}$ d'être égal à son groupe dérivé, cela ne change rien). Exemple typique :

$$S = L_2(q) = PSL_2(\mathbf{F}_q) \quad \text{et} \quad \overline{S} = 2 \cdot L_2(q) = SL_2(\mathbf{F}_q)\ , \qquad q \ \text{ impair.}$$

(Les notations $L_2(q)$ et $2 \cdot L_2(q)$ sont celles de l'ATLAS [15].)

Un plongement d'un tel groupe $\overline{S}$ dans G est appelé un *plongement projectif* de S. Le principal avantage de cette notion est la propriété d'invariance suivante : si $G' \to G$ est une isogénie, S a un plongement projectif dans G si et seulement si il a un plongement projectif dans G'.

Lorsque S et G sont donnés, et que G est un groupe classique, l'examen de la table des caractères de S (et de ses extensions centrales) permet de décider si S a un plongement (ou un plongement projectif) dans G ; c'est clair lorsque G est de type A_n, et c'est facile pour les types B_n, C_n, D_n. Une méthode analogue s'applique à G_2 (en utilisant sa représentation irréductible de degré 7 et la forme trilinéaire alternée correspondante), cf. Aschbacher [2] et Cohen-Wales [11]. Les types F_4, E_6, E_7, E_8 sont plus difficiles ; ce n'est que récemment (Griess-Ryba [22]) que la liste des S possibles a été complétée. Avant de donner cette liste (que l'on trouvera au § 2.4), je vais parler du cas $S = L_2(q)$, qui est le seul où l'on ait des énoncés généraux, i.e. valables aussi bien pour les groupes classiques que pour les groupes exceptionnels.

2.1. Plongements projectifs de $L_2(q)$ dans G ; énoncé du résultat. — On suppose $q > 2$. Le groupe $S = L_2(q) = PSL_2(\mathbf{F}_q)$ est alors un groupe simple (sauf si $q = 3$, où c'est le groupe Alt_4), et toute extension centrale $\overline{S}$ de S, égale à son groupe dérivé, est isomorphe, soit à $2 \cdot S = SL_2(\mathbf{F}_q)$, soit à S (sauf si $q = 4$ ou 9). On va donc s'intéresser aux homomorphismes

$$f : SL_2(\mathbf{F}_q) \longrightarrow G$$

de noyau égal à 1 ou à $\{\pm 1\}$. Un tel homomorphisme sera dit *non dégénéré*.

Écrivons q sous la forme p^e, avec p premier, $e \geqslant 1$. Le p-groupe de Sylow $U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ de $SL_2(\mathbf{F}_q)$ est isomorphe à $\mathbf{F}_q$. Le groupe $A = f(U)$ est un p-groupe abélien élémentaire de G de rang e. Nous dirons que f est *de type toral* si A est toral au sens du § 1.1. C'est le cas si $e = 1$, ou si $e = 2$ et G est simplement connexe (1.1.2), ou si p n'est pas un nombre premier de torsion pour G.

Nous allons donner un *critère pour l'existence d'un f non dégénéré de type toral*. Supposons G presque simple, de rang r ; soient k_i $(i = 1, \ldots, r)$ les exposants de son groupe de Weyl et soient $d_i = k_i + 1$ les degrés correspondants (BOURBAKI, LIE V, § 6, prop. 3). L'énoncé suivant résume une série de résultats dus à divers auteurs ([2], [8], [9], [11], [12], [14], [19], [20], [24], [28], [31]) :

2.1.1. *Pour qu'il existe un homomorphisme non dégénéré de type toral de $SL_2(\mathbf{F}_q)$ dans G, il faut et il suffit que $q-1$ divise l'un des entiers $2d_1, \ldots, 2d_r$.*

Remarque.— Lorsque $p = 2$ ou 3, il existe quelques plongements de $L_2(p^e)$ qui ne sont pas de type toral, par exemple :

$$L_2(4) \longrightarrow PGL_2\ ,\ L_2(8) \longrightarrow G_2\ ,\ L_2(16) \longrightarrow D_8\ , L_2(32) \longrightarrow E_8\ ;$$
$$L_2(9) \longrightarrow PGL_3\ ,\ L_2(27) \longrightarrow F_4.$$

Je ne sais pas en donner de description systématique.

Exemples

1) Si $G = SL_2$, on a $r = 1$ et $d_1 = 2$; la condition dit alors que $q-1$ divise 4, d'où $q = 3$ et $q = 5$, ce qui donne des plongements de $SL_2(\mathbf{F}_3)$ et $SL_2(\mathbf{F}_5)$ dans SL_2 ; d'où des plongements de $PSL_2(\mathbf{F}_3) = Alt_4$ et de $PSL_2(\mathbf{F}_5) = Alt_5$ dans PGL_2. On retrouve ainsi les groupes du tétraèdre et de l'icosaèdre (quant au groupe du cube, Sym_4, il s'interprète aussi comme $PGL_2(\mathbf{F}_3)$, et c'est le normalisateur du groupe Alt_4).

2) Si $G = G_2$, on a $r = 2$, $d_1 = 2$, $d_2 = 6$; la condition dit que $q-1$ divise 12, ce qui donne des plongements projectifs pour $q = 3, 5, 7, 13$. En fait, si $q = 7$

ou 13, ces plongements projectifs sont de vrais plongements de $\mathrm{L}_2(q)$, car sinon leurs images seraient contenues dans le centralisateur d'un élément d'ordre 2, qui est de type $\mathrm{A}_1 \cdot \mathrm{A}_1$, et cela contredirait l'exemple 1. (Ce genre d'argument s'applique à beaucoup d'autres cas : les plongements projectifs intéressants sont de vrais plongements.)

3) Si $\mathrm{G} = \mathrm{E}_8$, on a $(d_1, \ldots, d_8) = (2, 8, 12, 14, 18, 20, 24, 30)$ et l'on en déduit notamment des plongements de $\mathrm{L}_2(q)$ pour $q = 16, 31, 41, 49, 61$.

4) Le plus grand des entiers d_i est le *nombre de Coxeter* h, égal à

$$(\dim \mathrm{G})/r - 1.$$

L'énoncé 2.1.1 contient donc comme cas particulier la *conjecture de Kostant* : *si $q = 2h + 1$ est une puissance d'un nombre premier, le groupe G^{ad} contient un sous-groupe isomorphe à $\mathrm{L}_2(q)$.*

5) On a un énoncé analogue à celui de KOSTANT lorsque $h + 1$ est une puissance d'un nombre premier, d'où par exemple $\mathrm{L}_2(19) \to \mathrm{E}_7^{\mathrm{ad}}$ et $\mathrm{L}_2(31) \to \mathrm{E}_8$. Lorsque $h + 1$ est égal à un nombre premier p, on a un résultat plus précis (cf. [31]) : le groupe $\mathrm{PGL}_2(\mathbf{F}_p)$ (qui est « deux fois plus grand » que $\mathrm{PSL}_2(\mathbf{F}_p)$) est, lui aussi, plongeable dans G^{ad}. Lorsque $\mathrm{G} = \mathrm{PGL}_2$, on retrouve le groupe du cube $\mathrm{PGL}_2(\mathbf{F}_3)$, cf. exemple 1. De ce point de vue, on peut dire que « les analogues » pour E_8 des groupes Alt_4, Sym_4, et Alt_5 du début de l'exposé sont respectivement $\mathrm{PSL}_2(\mathbf{F}_{31})$, $\mathrm{PGL}_2(\mathbf{F}_{31})$ et $\mathrm{PSL}_2(\mathbf{F}_{61})$.

2.2. Le critère 2.1.1 : démonstration de la nécessité. — Il s'agit de prouver que, si $f : \mathrm{SL}_2(\mathbf{F}_q) \to \mathrm{G}$ est un homomorphisme non dégénéré de type toral, alors $q - 1$ divise l'un des entiers $2d_i$.

On utilise :

2.2.1. *Soit* A *un p-sous-groupe élémentaire toral de* G*, et soit $g \in \mathrm{N}_{\mathrm{G}}(\mathrm{A})$. Soit $\mathrm{I}_g \in \mathrm{GL}(\mathrm{A})$ l'automorphisme de* A (vu comme espace vectoriel sur $\mathbf{F}_p$) *défini par la conjugaison par g. Soit λ une valeur propre de I_g dans $\overline{\mathbf{F}}_p$ et soit m l'ordre de λ (dans $\overline{\mathbf{F}}_p^*$). Alors m divise l'un des d_i.*

(On peut supposer que A est contenu dans T ; d'après 1.1.1, il existe $w \in \mathrm{W}$ qui induit I_g sur A. L'une des valeurs propres de w en caractéristique 0 a pour réduction λ en caractéristique p. Son ordre est donc de la forme mp^a, avec $a \geqslant 0$. D'après un théorème de SPRINGER ([32], th. 3.4 (i)), mp^a divise l'un des d_i. Il en est donc de même de m.)

Revenons à f, et au p-Sylow $\mathrm{U} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Soit $\mathrm{A} = f(\mathrm{U})$, et soit $g = f(h)$, où $h = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$ est un générateur du sous-groupe diagonal de $\mathrm{SL}_2(\mathbf{F}_q)$. Si

l'on identifie U à $\mathbf{F}_q$, l'action de h sur ce groupe est l'homothétie de rapport c^2 ; ses valeurs propres (dans $\overline{\mathbf{F}}_p$) sont les conjugués de c^2, qui sont d'ordre $m = (q-1)/2$ si $p > 2$ et $m = q-1$ si $p = 2$. En appliquant 2.2.1 à A et g, on voit que m divise l'un des entiers d_i ; donc $q-1$ divise l'un des entiers $2d_i$.

Remarque.— Le même argument montre que, si f est un homomorphisme de $\mathrm{GL}_2(\mathbf{F}_q)$ dans G, qui est non dégénéré et de type toral (en un sens évident), alors $q-1$ divise l'un des d_i.

2.3. Le critère 2.1.1 : vérification de la suffisance. — On doit montrer que, si $q-1$ divise l'un des entiers $2d_i$, il existe $f : \mathrm{SL}_2(\mathbf{F}_q) \to \mathrm{G}$ qui est non dégénéré de type toral.

On ne connaît pas de démonstration générale de cet énoncé. On procède cas par cas :

1) Le cas où G est de type classique se traite facilement, grâce à la connaissance de la table des caractères de $\mathrm{SL}_2(\mathbf{F}_q)$; les caractères irréductibles de degré $(q \pm 1)/2$ sont particulièrement utiles. La condition de toralité est trivialement satisfaite si $p \neq 2$; dans le cas où $p = 2$, et où G est un groupe orthogonal, il faut faire un peu attention. La même méthode s'applique à G_2 (voir aussi [2], [11], [28]).

2) Pour les groupes exceptionnels, les inclusions des groupes classiques dans ceux-ci, et les plongements

$$\mathrm{G}_2 \longrightarrow \mathrm{F}_4 \longrightarrow \mathrm{E}_6 \longrightarrow \mathrm{E}_7 \longrightarrow \mathrm{E}_8,$$

montrent qu'il suffit de traiter les cas suivants :

$$\mathrm{F}_4\ (q = 25)\,; \quad \mathrm{E}_6\ (q = 19)\,; \quad \mathrm{E}_7\ (q = 29,\ 37)\,; \quad \mathrm{E}_8\ (q = 16,\ 31,\ 41,\ 49,\ 61).$$

Le cas (E_8 ; 16) se traite en remarquant que $\mathrm{L}_2(16)$ se plonge dans un groupe de type D_8, donc dans un groupe de type E_8 ; ce plongement n'est pas de type toral dans D_8, mais il le devient dans E_8 comme on le voit en appliquant [8], prop. 3.8.

Le cas (F_4 ; 25) se déduit de ce que $\mathrm{L}_2(25)$ se plonge dans le groupe de Tits ${}^2\mathrm{F}_4(2)'$, qui lui-même se plonge dans E_6, cf. 2.4.2, b) ci-après. On vérifie par un calcul de caractères que le sous-groupe de E_6 ainsi obtenu est contenu dans un conjugué de F_4, cf. Cohen-Wales [14].

Les cas (E_6 ; 19), (E_7 ; 37), (E_8 ; 31), (E_8 ; 41), (E_8 ; 49), (E_8 ; 61) ont été vérifiés par des calculs sur ordinateur, cf. Cohen-Wales [14], Kleidman-Ryba [24], Griess-Ryba [19] et [20], Cohen-Griess-Lisser [9].

Les cas (E_7 ; 37), (E_8 ; 31) et (E_8 ; 61) sont traités dans [31] par une méthode p-adique qui consiste à relever un plongement (bien choisi) de la caractéristique p à la caractéristique 0. Une variante non encore publiée de cette méthode 2
permet de traiter aussi (E_6 ; 19), (E_7 ; 29) et (E_8 ; 41). Ainsi, *tous les cas où q est premier peuvent être obtenus sans ordinateur.*

Remarque.— Les calculs sur ordinateur ont un inconvénient évident : ils ne sont pas vérifiables pas à pas, comme une démonstration doit l'être. Ils ont toutefois un avantage : dans certains cas, ils montrent *l'unicité* (à conjugaison près) du plongement considéré, cf. [19], [20]. C'est là un résultat que la méthode p-adique ne donne pas, au moins pour le moment.

2.4. Plongements projectifs des groupes finis simples dans les groupes de type exceptionnel. — La table suivante est extraite de Griess-Ryba [22] (avec une petite correction relative à F_4). Elle donne la liste des groupes simples ayant un plongement projectif dans $G_2, \ldots, E_8$. Je renvoie à [22] et [27] pour divers renseignements supplémentaires sur ces plongements, ainsi que pour des références.

Table

G_2 – Alt_n, $n = 5, 6$; $L_2(q)$, $q = 7, 8, 13$; $SU_3(3) = G_2(2)'$.

F_4 – *ceux de* G_2 *et* : Alt_n, $n = 7, 8, 9, 10$; $L_2(q)$, $q = 17, 25, 27$; $L_3(3)$; $SU_4(2)$; $Sp_6(2) = O_7(2)$; $O_8^+(2)$; ${}^3D_4(2)$.

E_6 – *ceux de* F_4 *et* : Alt_{11} ; $L_2(q)$, $q = 11, 19$; $L_3(4)$; $PSU_4(3)$; ${}^2F_4(2)'$; M_{11} ; $HJ = J_2$.

E_7 – *ceux de* E_6 *et* : Alt_n, $n = 12, 13$; $L_2(q)$, $q = 29, 37$; $PSU_3(8)$; M_{12}.

E_8 – *ceux de* E_7 *et* : Alt_n, $n = 14, 15, 16, 17$; $L_2(q)$, $q = 16, 31, 32, 41, 49, 61$; $L_3(5)$; $PSp_4(5)$; $G_2(3)$; ${}^2B_2(8) = Sz(8)$.

[Les notations sont celles de l'ATLAS [15]. En particulier $L_n(q)$ désigne le groupe $PSL_n(\mathbf{F}_q)$. Vu que $\mathrm{Alt}_5 = L_2(4) = L_2(5)$ et $\mathrm{Alt}_6 = L_2(9)$, la liste pour G_2 pourrait aussi être écrite :

G_2 – $L_2(q)$, $q = 4, 5, 7, 8, 9, 13$; $SU_3(3) = G_2(2)'$. De même, pour F_4, on peut remplacer Alt_8 par $L_4(2)$.]

La vérification de l'exactitude de cette table comporte deux parties. Tout d'abord :

2.4.1. *Un groupe simple qui ne figure pas dans la table n'a pas de plongement projectif dans* G.

Comme on peut s'y attendre, le point de départ est la *classification des groupes simples finis*, qui est admise (le lecteur curieux de savoir quelle partie de cette classification reste à démontrer pourra consulter ASCHBACHER [3]). Cela permet de passer en revue les différents cas possibles : groupes alternés, groupes de type algébrique, groupes sporadiques. Pour éliminer un groupe S, on utilise des arguments variés, par exemple 1.2.2 ou 2.2.1 (qui suffisent si le groupe est très gros), ou (dans les cas difficiles) la table des caractères du groupe. C'est un travail délicat. La moindre erreur peut conduire à éliminer à tort le groupe en question. C'est ce qui s'était passé dans une liste précédente [8] pour les groupes $L_2(41)$, $L_2(49)$ et $Sz(8)$ qui avaient été déclarés non plongeables dans E_8.

2.4.2. *Tout groupe figurant dans la table a au moins un plongement projectif dans* G.

On utilise différentes méthodes. Par exemple :

a) Le cas le plus facile est celui où l'on connaît un sous-groupe de G dans lequel S a un plongement projectif. Ainsi, pour traiter le cas de Alt_{10} et F_4, il suffit de remarquer que Alt_{10} a une représentation orthogonale évidente de degré 9, autrement dit se plonge dans un groupe de type B_4, et l'on utilise le plongement de B_4 dans F_4.

b) Certains cas peuvent se traiter à partir de la table des caractères de S (et de ses extensions centrales). Outre $G = G_2$, déjà signalé, il faut mentionner le cas où $G = E_6$ et où S est le groupe de Tits ${}^2F_4(2)'$ (COHEN-WALES [14]). On part du fait que le groupe $S \cdot 2 = {}^2F_4(2)$ a une représentation irréductible V de dimension 78 (cf. [15], p. 75). Un calcul de caractères montre que $\wedge^2 V$ contient V ; il existe donc un homomorphisme non nul $\wedge^2 V \to V$ compatible avec l'action de $S \cdot 2$, et un autre calcul de caractères montre que l'identité de Jacobi est satisfaite. D'où une structure d'algèbre de Lie sur V. Il est clair que cette algèbre de Lie est simple ; puisqu'elle est de dimension 78, elle est de type B_6, C_6 ou E_6. On élimine les types B_6 et C_6 qui conduiraient à des représentations de $S \cdot 2$ de degré trop petit. L'algèbre de Lie V est donc de type E_6, ce qui fournit un plongement de $S \cdot 2$ dans E_6^{ad}, donc *a fortiori* un plongement de S.

c) La plupart des autres plongements ont été construits au moyen de calculs sur ordinateur. Je renvoie à [22] pour une description des méthodes employées. Je signale seulement que les calculs ne se font pas sur le corps k, mais sur un corps fini $\mathbf{F}_\ell$, où ℓ est un nombre premier ne divisant pas l'ordre de S et tel que $\mathbf{F}_\ell$ contienne les racines de l'unité intervenant dans la construction : ainsi,

pour plonger $L_2(61)$ dans E_8, COHEN-GRIESS-LISSER [9] choisissent $\ell = 1831$. Le relèvement de $\mathbf{F}_\ell$ à $\mathbf{Z}_\ell$ (donc à la caractéristique 0) ne présente aucune difficulté vu que ℓ ne divise pas $|S|$. Il semble que, dans chaque cas, le calcul comporte suffisamment de vérifications internes pour qu'on puisse lui faire confiance.

2.5. Compléments

2.5.1. *Classification en caractéristique* > 0

L'analogue de 2.4 en caractéristique p a été fait par LIEBECK–SEITZ [27]. Tout groupe S intervenant en caractéristique 0 intervient aussi en caractéristique p (quel que soit p) ; c'est là une conséquence simple de la théorie de Bruhat–Tits, cf. [31], § 5. Outre ces groupes, et ceux qui sont « de caractéristique p », LIEBECK–SEITZ donnent la liste suivante :

G_2 – $p = 2 : J_2$; $p = 5 : \mathrm{Alt}_7$; $p = 11 : J_1$.

F_4 – *ceux de* G_2 *et* $p = 2 : L_4(3)$; $p = 3 : L_3(4)$; $p = 5 : Sz(8)$; $p = 11 : M_{11}$, Alt_{11}.

E_6 – *ceux de* F_4 *et* $p = 2 : M_{12}$, Alt_{12}, $G_2(3)$, $O_7(3)$, M_{22}, J_3, Fi_{22} ; $p = 3 : M_{12}$, Alt_{12} ; $p = 5 : M_{12}$; $p = 7 : M_{22}$.

E_7 – *ceux de* E_6 *et* $p = 5 : M_{22}$, Ru, HS ; $p = 7 : \mathrm{Alt}_{14}$.

E_8 – *ceux de* E_7 *et* $p = 2 : L_4(5)$; $p = 3 : \mathrm{Alt}_{18}$, Th ; $p = 5 : Sz(32)$.

Noter en particulier le groupe de Janko J_1 dans $G_2(\mathbf{F}_{11})$ et le groupe de Thompson Th dans $E_8(\mathbf{F}_3)$.

2.5.2. *Classes de conjugaison de plongements*

On aimerait pouvoir compléter la table 2.4 en décrivant les plongements à conjugaison près. Cela a été fait dans certains cas, mais pas dans tous, cf. [22]. Le cas des plongements de Alt_5 dans E_8 est particulièrement intéressant (cf. FREY [16]) ; on peut déterminer les triplets (x, y, z) de classes de conjugaison de E_8 d'ordres $(2, 3, 5)$ qui sont représentables dans un même sous-groupe Alt_5. Pour tous ces triplets, sauf un (celui appelé « 844 » dans [16]), FREY détermine le nombre de classes de conjugaison correspondantes (une ou deux). Par contre, pour le cas « 844 » (qui est le seul où le centralisateur du sous-groupe Alt_5 soit fini), on ne sait pas combien il y a de classes de conjugaison ; on dispose de plusieurs tels sous-groupes (par exemple un sous-groupe du groupe de Borovik [7], ou un sous-groupe de $L_2(41)$, ou de $L_2(61)$,...), mais il n'est pas facile de voir s'ils sont ou non conjugués. Comme Alt_5 admet la présentation : 3

$$(x, y, z \mid x^2 = y^3 = z^5 = 1 \ , \ xyz = 1),$$

c'est là un problème analogue à celui de la « rigidité » intervenant pour la classification des revêtements galoisiens de la droite projective ramifiés en 3 points.

2.5.3. *Rationalité*

On sait que G provient par extension des scalaires d'un groupe *déployé* G_{dep} défini sur $\mathbf{Q}$. Si S (ou $\overline{S}$) est plongeable dans $G(k)$, on peut se demander quels sont les sous-corps k' de k tels que S soit plongeable dans $G_{dep}(k')$. Cette question est étroitement liée à la précédente (celle des classes de conjugaison) : voir là-dessus [19], App. 2. Voici un exemple typique :

D'après ASCHBACHER [2], le groupe $S{\cdot}2 = G_2(2)$ admet un plongement dans $G_2(k)$, et un seul, à conjugaison près. Or, à la fois $S{\cdot}2$ et G_2 ont un centre trivial, et pas d'automorphisme externe. De plus, le centralisateur de $S{\cdot}2$ est trivial. Soit P l'ensemble de ces plongements ; c'est un G_2-torseur qui est défini de façon naturelle sur $\mathbf{Q}$. Il définit donc une $\mathbf{Q}$-forme G_2^0 de G_2, et l'on peut plonger $S{\cdot}2$ dans $G_2^0(\mathbf{Q})$ par définition même de G_2^0. Or, il n'y a que deux formes de G_2 sur $\mathbf{Q}$, que l'on distingue par leurs points réels ; la forme déployée ne peut pas contenir $S{\cdot}2$: son compact maximal est trop petit. Ainsi, G_2^0 est la forme non déployée de G_2, celle qui correspond aux octonions usuels. On conclut de là que le plongement cherché de $S{\cdot}2$ dans $G_{dep}(k')$ existe si et seulement si G_{dep} et G_2^0 sont k'-isomorphes, i.e. *si et seulement si* -1 *est somme de* 4 *carrés dans* k'. Un argument analogue montre que $L_2(13)$ est plongeable dans $G_{dep}(k')$ si et seulement si k' contient $\sqrt{13}$ et -1 est somme de 4 carrés dans k' ; même chose pour $L_2(8)$, avec $\sqrt{13}$ remplacé par $z_9 + \overline{z}_9$, où z_9 est une racine primitive 9-ième de l'unité. (Noter l'analogie de ces énoncés avec le suivant, connu depuis longtemps : Alt_4, Sym_4 et Alt_5 sont plongeables dans $PGL_2(k')$ si et seulement si -1 est somme de 2 carrés dans k' et (pour Alt_5) k' contient $\sqrt{5}$.)

Bibliographie

[1] J.F. ADAMS, 2-*tori in* E_8, Math. Ann. **287** (1987), 29–39 (= *Selected Works,* vol. II, 264–274).

[2] M. ASCHBACHER, *Chevalley groups of type* G_2 *as the group of a trilinear form*, J. Alg. **109** (1987), 193–259.

[3] M. ASCHBACHER, *Quasithin groups*, in *Algebraic Groups and their Representations* (R. Carter and J. Saxl edit.), NATO AS series, vol. **517**, 321–340, Kluwer, 1998.

[4] A. Borel, *Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tōhoku Math. J. **13** (1961), 216–240 (= *Œ.* II, n° 53 et *Commentaires*, 775–777).

[5] A. Borel and G.D. Mostow, *On semi-simple automorphisms of Lie algebras*, Ann. Math. **61** (1955), 389–405 (= A. Borel, *Œ.* I, n° 36).

[6] A. Borel et J-P. Serre, *Sur certains sous-groupes des groupes de Lie compacts*, Comm. Math. Helv. **27** (1953), 128–139 (= A. Borel, *Œ.* I, n° 24).

[7] A.V. Borovik, *A maximal subgroup in the simple finite group* $\mathrm{E}_8(q)$, Contemp. Math. A.M.S. **131** (1992), vol. I, 67–79.

[8] A.M. Cohen and R.L. Griess, Jr, *On finite simple subgroups of the complex Lie groups of type* E_8, A.M.S. Proc. Symp. Pure Math. **47** (1987), vol. II, 367–405.

[9] A.M. Cohen, R.L. Griess, Jr and B. Lisser, *The group* $\mathrm{L}(2,61)$ *embeds in the Lie group of type* E_8, Comm. Alg. **21** (1993), 1889–1907.

[10] A.M. Cohen and G.M. Seitz, *The r-rank of the groups of exceptional Lie type*, Indag. Math. **49** (1987), 251–259.

[11] A.M. Cohen and D.B. Wales, *Finite subgroups of* $\mathrm{G}_2(\mathbf{C})$, Comm. Alg. **11** (1983), 441–459.

[12] A.M. Cohen and D.B. Wales, *Embeddings of the group* $\mathrm{L}(2,13)$ *in groups of Lie type* E_6, Israel J. Math. **82** (1993), 45–86.

[13] A.M. Cohen and D.B. Wales, *Finite simple subgroups of semisimple complex Lie groups – a survey*, in *Groups of Lie type and their geometries*, LMS Lect. Notes **207** (1995), 77–96.

[14] A.M. Cohen and D.B. Wales, *Finite subgroups of* $\mathrm{F}_4(\mathbf{C})$ *and* $\mathrm{E}_6(\mathbf{C})$, Proc. London Math. Soc. **74** (1997), 105–150.

[15] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[16] D. Frey, *Conjugacy of alternating groups of degree* 5 *and* $\mathrm{SL}(2,5)$ *subgroups of the complex Lie groups of type* E_8, Memoirs A.M.S. **634** (1998).

[17] R.L. Griess, Jr, *Elementary abelian subgroups of algebraic groups*, Geom. Dedicata **39** (1991), 253–305.

[18] R.L. Griess, Jr and A.J.E. Ryba, *Embeddings of* $\mathrm{U}(3,8)$, $\mathrm{Sz}(8)$ *and the Rudvalis group in algebraic groups of type* E_7, Invent. math. **116** (1994), 215–241.

[19] R.L. Griess, Jr and A.J.E. Ryba, *Embeddings of* $\mathrm{PGL}(2,31)$ *and* $\mathrm{SL}(2,32)$ *in* $\mathrm{E}_8(\mathbf{C})$, Duke Math. J. **94** (1998), 181–211.

[20] R.L. Griess, Jr and A.J.E. Ryba, *Embeddings of* $\mathrm{PSL}(2,41)$ *and* $\mathrm{PSL}(2,49)$ *in* $\mathrm{E}_8(\mathbf{C})$, J. Symb. Comp. **11** (1999), 1–17.

[21] R.L. Griess, Jr and A.J.E. Ryba, *Embeddings of* $\mathrm{Sz}(8)$ *into exceptional Lie groups*, J. Crelle **523** (2000), 55–68.

[22] R.L. GRIESS, Jr and A.J.E. RYBA, *Finite simple groups which projectively embed in an exceptional Lie group are classified!*, Bull. A.M.S. **36** (1999), 75–93.

[23] A. GROTHENDIECK, *Torsion homologique et sections rationnelles*, Sém. Chevalley 1958, *Anneaux de Chow et Applications*, exposé n° 5.

[24] P.B. KLEIDMAN and A.J.E. RYBA, *Kostant's conjecture holds for* $\mathrm{E}_7 : \mathrm{L}_2(37) \subset \mathrm{E}_7(\mathbf{C})$, J. Alg. **161** (1993), 535–540.

[25] M.-A. KNUS, A. MERKURJEV, M. ROST and J.-P. TIGNOL, *The Book of Involutions*, A.M.S. Colloquium Publ. **44**, 1998.

[26] M.W. LIEBECK, *Subgroups of exceptional groups*, in *Algebraic Groups and their Representations* (R.W. Carter and J. Saxl edit.), NATO AS series, vol. **517**, 275–290, Kluwer, 1998.

[27] M.W. LIEBECK and G.M. SEITZ, *On finite subgroups of exceptional algebraic groups*, J. Crelle **515** (1999), 25–72.

[28] A. MEURMAN, *An embedding of* $\mathrm{PSL}(2,13)$ *in* $\mathrm{G}_2(\mathbf{C})$, Lect. Notes in Math. **933** (1982), 157–162.

[29] Z. REICHSTEIN and B. YOUSSIN, *Essential dimensions of algebraic groups and a resolution theorem for* G*-varieties, with an appendix by* J. KOLLÁR *and* E. SZABÓ, Canad. J. Math. **52** (2000), 1018–1056.

[30] J-P. SERRE, *Cohomologie galoisienne : progrès et problèmes*, Sém. Bourbaki 1993-94, exposé n° 783 (SMF, Astérisque **227** (1995), 229–257). (= *Œ.* 166)

[31] J-P. SERRE, *Exemples de plongements des groupes* $\mathbf{PSL}_2(\mathbf{F}_p)$ *dans des groupes de Lie simples*, Invent. math. **124** (1996), 525–562. (= *Œ.* 167)

[32] T.A. SPRINGER, *Regular elements of finite reflection groups*, Invent. math. **25** (1974), 159–198.

[33] T.A. SPRINGER and R. STEINBERG, *Conjugacy classes*, Lect. Notes in Math. **131** (1970), 281–312 (= R. Steinberg, *C.P.*, 293–323).

[34] R. STEINBERG, *Torsion in reductive groups*, Adv. in Math. **15** (1975), 63–92 (= *C.P.*, 415–444).

[35] J. TITS, *Normalisateurs de tores*, I. *Groupes de Coxeter étendus*, J. Alg. **4** (1966), 96–116.

[36] J. TITS, *Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples*, Publ. Math. IHES **31** (1966), 21–58.

Math. Medley
29 (2002), 3–18

Bull. A.M.S. **40** (2003), 429–440

ON A THEOREM OF JORDAN

The theorem of JORDAN which I want to discuss here dates from 1872. It is an elementary result on finite groups of permutations. I shall first present its translations in Number Theory and Topology.

1. Statements

1.1. Number Theory

Let $f = \sum_{m=0}^{n} a_m x^m$ be a polynomial of degree n, with coefficients in $\mathbf{Z}$. If p is a prime, let $\mathrm{N}_p(f)$ be the number of zeros of f in $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

THEOREM 1. — *Assume*

(i) $n \geqslant 2$,

(ii) f *is irreducible in* $\mathbf{Q}[x]$.

Then

(a) *There are infinitely many* p*'s with* $\mathrm{N}_p(f) = 0$.

(b) *The set* $\mathrm{P}_0(f)$ *of* p*'s with* $\mathrm{N}_p(f) = 0$ *has a density* $c_0 = c_0(f)$ *which is* > 0.

[Recall that a subset P of the set of primes has density c if

$$\lim_{\mathrm{X}\to\infty} \frac{\text{number of } p \in \mathrm{P} \text{ with } p \leqslant \mathrm{X}}{\pi(\mathrm{X})} = c,$$

where $\pi(\mathrm{X})$ is as usual the number of primes $\leqslant \mathrm{X}$.]

Moreover,

THEOREM 2. — *With the notation of Theorem 1, one has* $c_0(f) \geqslant \dfrac{1}{n}$, *with strict inequality if* n *is not a power of a prime.*

Example. — Let $f = x^2+1$. One has $p \in \mathrm{P}_0(f)$ if and only if $p \equiv -1 \pmod 4$; this set is well-known to have density $1/2$. We shall see more interesting examples in § 5.

1.2. Topology

Let $\mathbf{S}_1$ be a circle.
Let $f : \mathrm{T} \to \mathrm{S}$ be a finite covering of a topological space S. Assume :
(i) f has degree n (i.e. every fiber of f has n elements), with $n \geqslant 2$,
(ii) T is arcwise connected and not empty.

THEOREM 3. — *There exists a continuous map $\varphi : \mathbf{S}_1 \to \mathrm{S}$ which cannot be lifted to the covering* T (i.e. there does not exist any continuous map $\tilde{\varphi} : \mathbf{S}_1 \to \mathrm{T}$ such that $\varphi = f \circ \tilde{\varphi}$).

1.3. Finite Groups

Let G be a group acting on a finite set X. Put $n = |\mathrm{X}|$ [(1)].

THEOREM 4. — (JORDAN [9]) *Assume that*
(i) $n \geqslant 2$,
(ii) G *acts transitively on* X.
Then there exists $g \in \mathrm{G}$ which acts on X *without fixed point.*

Assume that G is finite (which is the case if G acts faithfully on X). Let G_0 be the set of $g \in \mathrm{G}$ with no fixed point. Call c_0 the ratio $\dfrac{|\mathrm{G}_0|}{|\mathrm{G}|}$.

THEOREM 5. — (CAMERON-COHEN [4]) *One has $c_0 \geqslant \dfrac{1}{n}$. Moreover, if n is not a power of a prime, then $c_0 > \dfrac{1}{n}$.*

2. Proofs of the group theoretical statements

2.1. Burnside's Lemma

Let G be a finite group acting on a finite set X. If $g \in \mathrm{G}$, let $\chi(g)$ be the number of fixed points of g on X, i.e. $\chi(g) = |\mathrm{X}^g|$.

BURNSIDE'S LEMMA. — (cf. [6, § 4.2], [3, § 145]) *The number of orbits of* G *in* X *is equal to*

$$\langle \chi, 1 \rangle = \tfrac{1}{|\mathrm{G}|} \textstyle\sum_{g \in \mathrm{G}} \chi(g) = \int \chi.$$

(1) If S is a finite set, we denote by $|\mathrm{S}|$ the number of elements of S.

(If φ is a function on G, and S is a subset of G, we denote by $\int_S \varphi$ the number $\frac{1}{|G|}\sum_{g\in S}\varphi(g)$. When $S = G$, we write $\int \varphi$ instead of $\int_G \varphi$.)

By decomposing X into orbits, it is enough to prove the lemma for $X \neq \varnothing$ and G transitive on X, i.e. $X \simeq G/H$ for some subgroup H of G.

We give three proofs, in different styles.

First Proof : *"Analytic Number Theory Style".*

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\sum_{\substack{x\in X\\ g\cdot x=x}} 1 = \sum_{x\in X}\sum_{\substack{g\in G\\ g\cdot x=x}} 1$$
$$= \sum_{x\in X}|H| = |H|\cdot|X| = |G|.$$

Second Proof : *"Combinatorics Style".* Let $\Omega \subset G\times X$ be the set of pairs (g,x) with $g\cdot x = x$. We compute $|\Omega|$ by projecting on each factor. In the projection $\Omega \to G$, the fiber of $g \in G$ has $\chi(g)$ elements and hence

$$|\Omega| = \sum_{g\in G}\chi(g).$$

On the other hand, in the projection $\Omega \to X$, the fiber of $x \in X$ is a conjugate of H and hence

$$|\Omega| = \sum_{x\in X}|H| = |H|\cdot|G/H| = |G|.$$

Third Proof : *"Algebra Style".* The function χ is the character of the permutation representation defined by X. Hence, $\langle\chi, 1\rangle$ is the dimension of the space of G-invariant elements of that representation, which is obviously 1.

2.2. Proof of Theorem 5

LEMMA. — $\int \chi^2 \geqslant 2$.

First Proof (by Burnside's Lemma). If $g \in G$, $\chi^2(g)$ is the number of points of $X\times X$ fixed by g and $\int\chi^2$ is the number of orbits of G on $X\times X$, which is $\geqslant 2$, as one sees by decomposing $X\times X$ into the diagonal and its complement.

This also shows that $\int\chi^2 = 2$ if and only if G is doubly transitive on X.

Second Proof (by Group Representations). We have $\chi = 1 + \chi'$, where χ' is a non-zero real character with $\int\chi' = 0$. Therefore,

$$\int\chi^2 = 1 + \int\chi'^2 \geqslant 2,$$

with equality if and only if χ' is irreducible.

We now prove Theorem 5. Recall that G_0 is the set of $g \in G$ with $\chi(g) = 0$. If $g \notin G_0$, then we have $1 \leqslant \chi(g) \leqslant n$ and therefore,

$$(\chi(g) - 1)(\chi(g) - n) \leqslant 0.$$

Hence,

$$\int_{G-G_0} (\chi(g) - 1)(\chi(g) - n) \leqslant 0,$$

i.e.,

$$\int_G (\chi(g) - 1)(\chi(g) - n) \leqslant \int_{G_0} (\chi(g) - 1)(\chi(g) - n) = n \int_{G_0} 1.$$

The right hand side is

$$n \int_{G_0} 1 = n\, c_0,$$

and the left hand side is

$$\int_G (\chi^2 - (n+1)\chi + n).$$

By the Lemma, and the fact that $\int \chi = 1$, we have

$$\int_G \left(\chi^2 - (n+1)\chi + n\right) \geqslant 2 - (n+1) + n = 1,$$

hence

$$1 \leqslant n\, c_0.$$

2.3. Equality in Theorem 5

The proof of Theorem 5 shows that equality holds if and only if $\int \chi^2 = 2$ and $(\chi(g) - 1)(\chi(g) - n) = 0$ for every $g \in G - G_0$, i.e. if and only if G is doubly transitive, and no element of $G - \{1\}$ fixes 2 points. By a theorem of FROBENIUS [8], the set $N = \{1\} \cup G_0$ is then a normal subgroup of G, and G is a semi-direct product : $G = H \cdot N$. Hence $|N| = n$, and $(n-1)/|G| = |G_0|/|G| = c_0 = 1/n$, i.e. $|G| = n(n-1)$, $|H| = n-1$. Moreover, the action of H on $N - \{1\}$ by conjugation is a free action. Since H and $N - \{1\}$ have the same number of elements, one sees that H acts freely and transitively on $N - \{1\}$. This implies that N is a p-group for some prime p [and even more : N is an elementary abelian p-group]. Hence, n is a power of a prime.

Remarks.

1. It is only for convenience that we have used Frobenius's Theorem [8]. It is possible to give a direct proof, as was already done in JORDAN's paper [9].

2. Conversely if n is a power of a prime, there exists a pair (G, X) with $|X| = n$ and $c_0 = 1/n$: take $X = k$, a finite field with n elements, and define G as the group of affine transformations $x \mapsto ax + b$ with $a \in k^*, b \in k$.

3. Proof of the covering space statement

With the same notation as in § 1.2, choose a point $s \in S$. Let $X = f^{-1}(s)$ be the fiber of s. Let $G = \pi_1(S, s)$ be the fundamental group of S at the point s. There is a natural action of G on X, and the hypothesis that T is arcwise connected implies that every two points in X can be connected by a path and hence G acts transitively on X. Since $n = |X| \geqslant 2$, Theorem 4 shows that there exists $g \in G$ which has no fixed point on X. If we represent g by a loop

$$\varphi : (\mathbf{S}_1, s_0) \longrightarrow (S, s),$$

where s_0 is a chosen point in $\mathbf{S}_1$, then φ cannot be lifted to T. Indeed, if $\tilde{\varphi} : \mathbf{S}_1 \to T$ were a lift of φ, the point $x = \tilde{\varphi}(s_0)$ would be a fixed point of G.

4. Proof of the number theoretic statement

We now prove Theorems 1 and 2 with the help of Theorems 4 and 5. Let $x_1, x_2, \cdots, x_n$ be the roots of f in an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. Let $E = \mathbf{Q}(x_1, x_2, \cdots, x_n)$ and let $G = \operatorname{Aut} E =$ the Galois group of $E/\mathbf{Q}$. The action of G on the set $X = \{x_1, x_2, \cdots, x_n\}$ is transitive since f is irreducible over $\mathbf{Q}$. Let G_0 be the subset of G having no fixed points. By Theorems 4 and 5, we have

$$\frac{|G_0|}{|G|} \geqslant \frac{1}{n}.$$

Let us define a finite set S of "bad" prime numbers, namely, those which divide the discriminant of f or divide the coefficient of x^n. Assume now that $p \notin S$. Then the reduction f_p of f modulo p is a polynomial of degree n, whose n roots (in an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$) are distinct. Let X_p be the set of such roots. We may identify X_p and X in the following way :

Let $R = \mathbf{Z}[x_1, x_2, \cdots, x_n]$ be the ring generated by the x_i's. Choose a homomorphism $\varphi : R \to \overline{\mathbf{F}}_p$ (such a homomorphism exists since $p \nmid a_0$) and any other such homomorphism is of the form $\varphi \circ s$, with $s \in G$. Such a φ defines a bijection $\varphi_p : X \to X_p$, which is well-defined up to an element of G. Let π_p be the Frobenius automorphism of $\overline{\mathbf{F}}_p$, i.e., $\lambda \mapsto \lambda^p$. The map π_p acts on X_p. If we identify X_p with X via φ_p, we get a permutation σ_p of X (depending on the choice of φ). One proves that this permutation belongs to G. It is called the *Frobenius substitution of* p (relative to the choice of φ); it is well-defined up to inner conjugation in G. We have

(∗) If $p \notin S$, N_p is the number of $x \in X$ fixed by σ_p.

This follows from the corresponding fact for X_p and π_p. [More generally, if σ_p is a product of disjoint cycles of lengths ℓ_α, then f_p decomposes into a product of $\mathbf{F}_p$-irreducible polynomials of degrees ℓ_α.] Hence, $N_p = 0$ if and only if $\sigma_p \in G_0$, where G_0 is the set of $s \in G$ which acts on X without fixed point. Note that G_0 is stable under conjugation so that "$\sigma_p \in G_0$" makes sense.

We now recall Chebotarev's Density Theorem (see Notes for § 4) :

CHEBOTAREV'S DENSITY THEOREM. — ([19], [1]). *Let* C *be a subset of* G*, stable under conjugation* (i.e. a union of conjugacy classes). *Then the set* $P_{C,S}$ *of primes* $p \notin S$ *with* $\sigma_p \in C$ *has a density, which is equal to* $\dfrac{|C|}{|G|}$.

Applying this Theorem to the case $C = G_0$ shows that the set $P_0(f)$ of Theorem 1 has density $c_0 = \dfrac{|G_0|}{|G|}$; by Theorems 4 and 5, this completes the proofs of Theorems 1 and 2.

5. Example : $N_p(f)$ for $f = x^n - x - 1$

5.1.

In this section, we consider the special case of $f = x^n - x - 1, n \geqslant 2$, and we relate the numbers $N_p(f)$ to the coefficients of suitable power series. We limit ourselves to stating the results; for the proofs, see the hints given in the Notes.

Here is a small table of $N_p(f)$ for $f = x^n - x - 1$, $n = 2, 3, 4, 5$:

p	$n=2$	$n=3$	$n=4$	$n=5$
2	0	0	0	0
3	0	0	0	0
5	1	1	0	0
7	0	1	1	0
11	2	1	1	0
13	0	0	1	0
17	0	1	2	2
19	2	1	0	1
23	0	2	1	1
...	...	...	...	...
59	2	3	1	0
...	...	...	...	...
83	0	1	4	0

5.2. The case $n = 2$

The discriminant of $f = x^2 - x - 1$ is 5; the polynomial f has a double root mod 5; hence $\mathrm{N}_5(f) = 1$. For $p \neq 5$, we have

$$\mathrm{N}_p(f) = \begin{cases} 2 & \text{if } p \equiv \pm 1 \pmod 5 \\ 0 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

If one defines a power series $\mathrm{F}(q) = \sum_{m=1}^{\infty} a_m q^m$ by

$$\mathrm{F} = \frac{q - q^2 - q^3 + q^4}{1 - q^5} = q - q^2 - q^3 + q^4 + q^6 - q^7 - q^8 + q^9 + \cdots,$$

the above formula can be restated as

$$\mathrm{N}_p(f) = a_p + 1 \quad \text{for all primes } p.$$

Note that the coefficients of F are *strongly multiplicative* : one has $a_{mm'} = a_m a_{m'}$ for every $m, m' \geqslant 1$. The corresponding Dirichlet series $\sum_{m=1}^{\infty} a_m m^{-s}$ is the L-series $\prod_p \left(1 - \left(\frac{p}{5}\right) p^{-s}\right)^{-1}$.

5.3. The case $n = 3$

The discriminant of $f = x^3 - x - 1$ is -23; the polynomial f has a double root and a simple root mod 23; hence $\mathrm{N}_{23}(f) = 2$. For $p \neq 23$, one has :

$$\mathrm{N}_p(f) = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\frac{p}{23}\right) = 1 \\ 1 & \text{if } \left(\frac{p}{23}\right) = -1. \end{cases}$$

Moreover, in the ambiguous case where $\left(\frac{p}{23}\right) = 1$, p can be written either as $x^2 + xy + 6y^2$ or as $2x^2 + xy + 3y^2$ with $x, y \in \mathbf{Z}$; in the first case, one has $\mathrm{N}_p(f) = 3$; in the second case, one has $\mathrm{N}_p(f) = 0$.
[The smallest p of the form $x^2 + xy + 6y^2$ is $59 = 5^2 + 5 \cdot 2 + 6 \cdot 2^2$, hence $\mathrm{N}_{59}(f) = 3$, cf. table above.]

Let us define a power series $\mathrm{F} = \sum_{m=0}^{\infty} a_m q^m$ by the formula

$$\begin{aligned}\mathrm{F} &= q\prod_{k=1}^{\infty}(1-q^k)(1-q^{23k}) \\ &= \frac{1}{2}\Big(\sum_{x,y\in\mathbf{Z}} q^{x^2+xy+6y^2} - \sum_{x,y\in\mathbf{Z}} q^{2x^2+xy+3y^2}\Big) \\ &= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + \cdots .\end{aligned}$$

The formula for $\mathrm{N}_p(f)$ given above can be reformulated as :

$$\mathrm{N}_p(f) = a_p + 1 \quad \text{for all primes } p.$$

Note that the coefficients of F are *multiplicative* : one has $a_{mm'} = a_m a_{m'}$ if m and m' are relatively prime. The q-series F is a newform of weight 1 and level 23. The associated Dirichlet series is

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = \prod_p \left(1 - \frac{a_p}{p^s} + \Big(\frac{p}{23}\Big)\frac{1}{p^{2s}}\right)^{-1}.$$

5.4. The case $n = 4$

The discriminant of $f = x^4 - x - 1$ is -283. The polynomial f has two simple roots and one double root mod 283, hence $\mathrm{N}_{283}(f) = 3$. If $p \neq 283$, one has

$$\mathrm{N}_p(f) = \begin{cases} 0 \text{ or } 4 & \text{if } p \text{ can be written as } x^2 + xy + 71y^2 \\ 1 & \text{if } p \text{ can be written as } 7x^2 + 5xy + 11y^2 \\ 0 \text{ or } 2 & \text{if } \left(\frac{p}{283}\right) = -1. \end{cases}$$

[These cases correspond to the Frobenius substitution of p being conjugate in S_4 to (12)(34) or 1; (123); (1234) or (12) respectively.]

A complete determination of $\mathrm{N}_p(f)$ can be obtained via a newform $\mathrm{F} = \sum_{m=1}^{\infty} a_m q^m$ of weight 1 and level 283 given in [5, p.80, example 2] :

$$\mathrm{F} = q + \sqrt{-2}q^2 - \sqrt{-2}q^3 - q^4 - \sqrt{-2}q^5 + 2q^6 - q^7 - q^9 + 2q^{10} + q^{11} + \sqrt{-2}q^{12} + \cdots .$$

One has :

$$\mathrm{N}_p(f) = 1 + (a_p)^2 - \left(\frac{p}{283}\right) \quad \text{for all primes } p \neq 283.$$

I do not know any closed formula for F, but one can give one for its reduction mod 283, see Notes. This is more than enough to determine the integers $N_p(f)$, since they are equal to $0, 1, 2$ or 4.

5.5. The case $n \geqslant 5$

Here the only known result seems to be that $f = x^n - x - 1$ is irreducible (SELMER [15]), and that its Galois group is the symmetric group S_n. No explicit connection with modular forms (or modular representations) is known, although some must exist because of the Langlands program.

Notes

1.1

Here is another interpretation of $c_0(f)$. Let $K = \mathbf{Q}[x]/(f)$ be the number field defined by f. We have $[K : \mathbf{Q}] = n \geqslant 2$. For every $d \geqslant 1$, let $a_d(K)$ be the number of the ideals $\mathfrak{a}$ of the ring of integers of K with $N(\mathfrak{a}) = d$. The zeta function of K is the Dirichlet series

$$\zeta_K(s) = \sum_{d \geqslant 1} \frac{a_d(K)}{d^s}.$$

Using standard recipes in analytic number theory, one can show that Theorem 1 is equivalent to saying that ζ_K is *lacunary* : most of its coefficients are zero. More precisely, if we denote by $N_K(X)$ the number of $d \leqslant X$ with $a_d(K) \neq 0$, one has

$$N_K(X) \sim c_K \frac{X}{(\log X)^{c_0(f)}} \quad \text{for } X \to \infty,$$

where c_K is a strictly positive constant (cf. ODONI [13] and SERRE [16, § 3.5]). As for Theorem 2, it can be reformulated as

$$N_K(X) = O\left(\frac{X}{(\log X)^{1/n}}\right) \quad \text{for } X \to \infty,$$

with "O" replaced by "o" if n is not a power of a prime.

1.2. Jordan's Theorem (Theorem 4)

The standard proof of Theorem 4 relies on the fact that the stabilizer H_x of a point x of X has $|G|/n$ elements, since $X \simeq G/H_x$. When x runs through the n points of X, the subgroups H_x have at least one point in common, namely the element 1. Hence, their union has at most $n \cdot |H_x| - (n-1)$ elements,

i.e. at most $|G| - (n-1)$ elements. This shows that there are at least $n-1$ elements of G which do not belong to any H_x, i.e. which have no fixed point. The interest of Theorem 5 is that it replaces the crude lower bound $n-1$ by $|G|/n$, which is close to being optimal.

Remark. Another way of stating Theorem 4 is :

THEOREM $4'$. — *If* H *is a proper subgroup of a finite group* G*, there is a conjugacy class of* G *which does not intersect* H*.*

In group-character language, this can be restated as :

THEOREM $4''$. — *There exist two characters of* G *which are distinct, but have the same restriction to* H*.*

In other words, the characters of G cannot be detected by their restriction to a proper subgroup of G. One needs at least two such subgroups (such as, for $\mathbf{GL}_2(\mathbf{F}_q)$, a Borel subgroup and a non-split Cartan subgroup). This is quite different from the case of compact connected Lie groups, where just one maximal torus is enough.

1.3. Theorem 5

Theorem 5 originated with a question of LENSTRA, in relation with Theorem 2. See BOSTON et al [2] for more on this story.

2. Burnside's Lemma

The first two proofs we offer are basically the same. Only their styles are different : analytic number theorists love to write $\sum 1$ and to permute summations, while combinatorists are fond of counting the elements of a set by mapping it into another one.

Note that Burnside's Lemma implies directly the weak form of Jordan's Theorem (Theorem 4 above). Indeed, since the mean value of $\chi(g)$ is 1, and the element $g = 1$ contributes $n > 1$, there has to be some $g \in G$ with $\chi(g) < 1$, hence $\chi(g) = 0$.

Note also that Burnside's Lemma, combined with Chebotarev's Density Theorem, gives the following result :

If f *is as in* § 1.1*, the mean value of* $N_p(f)$ *for* $p \to \infty$ *is equal to* 1*.*

In other words :

$$\sum_{p \leqslant X} N_p(f) \sim \pi(X) \quad \text{for } X \to \infty.$$

This is due to KRONECKER [10] and FROBENIUS [7], in the slightly weaker form where "natural density" is replaced by "analytic density".

3. Lifting circles to coverings

Theorem 3 does not extend to infinite coverings. Indeed, it is easy to construct an infinite free group G having a subgroup H of infinite index such that $\bigcup gHg^{-1} = G$. If one chooses a connected graph S with fundamental group isomorphic to G, the covering $T \to S$ associated with H has the property that every continuous map $\mathbf{S}_1 \to S$ can be lifted to T.

4. Chebotarev Density Theorem

The original proof can be found in [19]; it uses "analytic density" instead of "natural density". The more precise form we give was pointed out by ARTIN [1], even before Chebotarev's Theorem was proved.

For the history of this theorem, see [11], which also includes a sketch of proof. For applications, see for instance [16] or [18].

Note that, for the application we make to Theorems 1 and 2, a weaker version of the theorem would be enough, namely the one proved by FROBENIUS [7] (with, once again, the proviso that "analytic density" has to be replaced by the "natural density").

5.1. Computation of $N_p(f)$

For a given polynomial f, such as $x^3 - x - 1$, $x^4 - x - 1$, etc., the numerical computation of $N_p(f)$ is an interesting question, especially for large values of the prime p. There are essentially two methods :

— The naive one is to try successively all the values of x mod p, and count those which are zeros of f mod p. This is slow; it requires exponential time (with respect to the number of digits of p); it is reasonable for very small primes only (up to 5 digits, say).

— The second method is much faster (polynomial instead of exponential), and can handle primes of about 100 digits. It relies on the standard fact that computing x^p by successive squarings takes about $\log p$ operations. One applies this principle to the finite $\mathbf{F}_p$-algebra $A_p = \mathbf{F}_p[X]/(f)$, with x equal to the image of X in A_p. Once x^p is computed, one gets $N_p(f)$ by the formula :

$n - N_p(f) =$ rank of the linear endomorphism $u \mapsto (x^p - x)u$ of A_p.

Note that a variant of this method is incorporated in programs such as *PARI*, where one has only to ask `polrootsmod(f,p)?` to get the list of the roots of $f \bmod p$.

5.2. $\mathrm{N}_p(f)$ for $f = x^2 - x - 1$

For $p \neq 2, 5$, the roots of f_p in $\overline{\mathbf{F}}_p$ are $(1 \pm \sqrt{5})/2$; hence $\mathrm{N}_p(f) = 2$ if 5 is a square (mod p), and $\mathrm{N}_p(f) = 0$ if not. By quadratic reciprocity, the first case occurs if and only if $p \equiv \pm 1 \pmod 5$. A direct proof is as follows : call z a primitive 5^{th} root of unity in $\overline{\mathbf{F}}_p$ and put $x = -(z + z^4)$, $x' = -(z^2 + z^3)$. One has $x + x' = 1$ and $xx' = -1$ because $1 + z + z^2 + z^3 + z^4 = 0$. Hence, x, x' are the zeros of f_p. The action of the Frobenius σ_p on $\mathrm{X} = \{x, x'\}$ is clear : we have $\sigma_p(x) = -(z^p + z^{-p})$. If $p \equiv \pm 1 \pmod 5$, we have $z^p = z^{\pm 1}$, hence $\sigma_p(x) = x, \sigma_p(x') = x'$, and $\mathrm{N}_p(f) = 2$; if $p \equiv \pm 2 \pmod 5$, the same argument shows that σ_p permutes x and x', hence $\mathrm{N}_p(f) = 0$.

Remark. — Even though the two cases $\mathrm{N}_p(f) = 0$ and $\mathrm{N}_p(f) = 2$ arise "equally often" (in an asymptotic sense, when $p \to \infty$), yet there is a definite bias towards the first case. This is an example of what Rubinstein and Sarnak call "Chebyshev Bias", cf. [14].

5.3. $\mathrm{N}_p(f)$ for $f = x^3 - x - 1$

Let $\mathrm{E} = \mathbf{Q}[\mathrm{X}]/(f)$ be the cubic field defined by f, and let L be its Galois closure. We have $\mathrm{Gal}(\mathrm{L}/\mathbf{Q}) = \mathrm{S}_3$. The field L is a cubic cyclic extension of the quadratic field $\mathrm{K} = \mathbf{Q}(\sqrt{-23})$; it is unramified, and, since $h(-23) = 3$, it is the Hilbert class field of K, i.e. the maximal unramified abelian extension of K (as a matter of fact, it is also the maximal unramified extension – abelian or not – of K, as follows from the Odlyzko bounds, see e.g. Martinet [12].)

If $p \neq 23$, let σ_p be the Frobenius substitution of p in $\mathrm{S}_3 = \mathrm{Gal}(\mathrm{L}/\mathbf{Q})$; it is well-defined, up to conjugation. The image of σ_p by $\mathrm{sgn} : \mathrm{S}_3 \to \{\pm 1\}$ is $\varepsilon(p)$, where ε is the quadratic character associated with $\mathrm{K}/\mathbf{Q}$, i.e., $\varepsilon(p) = \left(\frac{p}{23}\right)$. This shows that σ_p is a transposition if $\left(\frac{p}{23}\right) = -1$, hence $\mathrm{N}_p(f) = 1$ in that case. When $\left(\frac{p}{23}\right) = 1$, σ_p is of order 1 or 3, hence $\mathrm{N}_p(f) = 3$ or $\mathrm{N}_p(f) = 0$. To distinguish between these two cases, one decomposes p in K as a product of two prime ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, and one has to decide whether $\mathfrak{p}$ is principal or not. The standard correspondence between ideal classes and binary quadratic forms shows that $\mathfrak{p}$ is principal is equivalent to p being representable by the form $x^2 + xy + 6y^2$, while $\mathfrak{p}$ is non principal is equivalent to p being representable by the form $2x^2 + xy + 3y^2$. This gives the recipe we wanted, namely,

$$\mathrm{N}_p(f) = \begin{cases} 3 & \text{if } p \text{ is representable by } x^2 + xy + 6y^2 \\ 0 & \text{if } p \text{ is representable by } 2x^2 + xy + 3y^2 \\ 1 & \text{if } \left(\frac{p}{23}\right) = -1. \end{cases}$$

The natural embedding ρ of $S_3 = \mathrm{Gal}(L/\mathbf{Q})$ in $\mathbf{GL}_2(\mathbf{C})$ gives rise to an Artin L-function

$$L(\rho, s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s},$$

with coefficients $a_m \in \mathbf{Z}$. One may characterize it by

$$L(\rho, s) = \zeta_E(s)/\zeta(s),$$

where $\zeta_E(s)$ is the zeta function of the cubic field E. This is equivalent to saying that the linear representation $\rho \oplus 1$ is isomorphic to the 3-dimensional permutation representation of S_3. By comparing the traces of σ_p in both representations, we get $N_p(f) = a_p + 1$ for every prime p (including $p = 23$). Since S_3 is a dihedral group, Hecke's theory applies and shows that the power series $F = \sum_{m=1}^{\infty} a_m q^m$ with the same coefficients as $L(\rho, s)$ is a cusp form of weight 1 and level 23, with respect to the character ε. The explicit expressions of F given in the text can be checked by standard modular methods.

5.4. $N_p(f)$ for $f = x^4 - x - 1$

Let E be the quartic field defined by f and L its Galois closure; the Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to S_4. Let H be the unique normal $(2,2)$-subgroup of G; the quotient G/H is isomorphic to S_3. The field L^H is the Hilbert class field of $\mathbf{Q}(\sqrt{-283})$; note that $h(-283) = 3$. The same argument as in Note 5.3 gives the image of the Frobenius σ_p in G/H in terms of $\left(\frac{p}{283}\right)$ and of the binary forms $x^2 + xy + 71y^2$ and $7x^2 + 5xy + 11y^2$ with discriminant -283.

To go further, one needs a result of TATE (reproduced in [17],[12],[5]) which says that the field L has a quadratic extension $\widetilde{L}$ having the following two properties :

- $\widetilde{L}$ is unramified over L (and hence also over $\mathbf{Q}(\sqrt{-283})$);
- $\widetilde{L}$ is a Galois extension of $\mathbf{Q}$.

(An explicit construction of $\widetilde{L}$, due to TATE, is : $\widetilde{L} = L(\sqrt{4 - 7x^2})$, where x is a root of f in L; the construction given in CRESPO [5] is more complicated.)

MARTINET [12] has shown that $\widetilde{L}$ is the maximal unramified extension of $\mathbf{Q}(\sqrt{-283})$; in other words, the fundamental group of $\mathrm{Spec}\,\mathbf{Z}[(1 + \sqrt{-283})/2]$ is isomorphic to the "binary tetrahedral group" $\widetilde{A_4} = \mathbf{SL}_2(\mathbf{F}_3)$.

The group $\widetilde{G} = \mathrm{Gal}(\widetilde{L}/\mathbf{Q})$ is isomorphic to $\mathbf{GL}_2(\mathbf{F}_3)$; it has a natural embedding ρ in $\mathbf{GL}_2(\mathbf{C})$; its character has values in $\mathbf{Z}[\sqrt{-2}]$. By a well-known

theorem of LANGLANDS and TUNNELL (see the references in [5]), the L-series attached to ρ corresponds to a modular form $\mathrm{F} = \sum_{m=0}^{\infty} a_m q^m$ of weight 1 and level 283 whose first hundred coefficients are computed in [5]. One checks (by a character computation) that one has

$$\rho \otimes \rho = \varepsilon \oplus (\theta - 1),$$

where θ is the 4-dimensional permutation representation of G and ε is the signature character of G. By taking traces, this gives

$$(a_p)^2 = \left(\frac{p}{283}\right) + \mathrm{N}_p(f) - 1, \text{for all primes } p \neq 283.$$

Remark. One may give an explicit formula for F (mod 283) as follows : by a known result [17, 9.3.1] F is congruent mod 283 to a modular form φ of weight $(283+1)/2 = 142$, and of level 1. Hence, φ can be written as a linear combination, with coefficients in $\mathbf{F}_{283}$, of the standard basis :

$$\mathrm{QR}^{23}\Delta,\ \ \mathrm{QR}^{21}\Delta^2,\ \ \ldots,\ \ \mathrm{QR}\Delta^{11}$$

(with Ramanujan's notation :

$$\mathrm{Q} = 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}, \quad \mathrm{R} = 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n},$$

and $\Delta = (\mathrm{Q}^3 - \mathrm{R}^2)/1728 = q\prod_{n=1}^{\infty}(1-q^n)^{24}$).

A computation, using only the first eleven coefficients of F, gives the coefficients of φ in that basis :

$$[1, 24, 52, 242, 40, 232, 164, 217, 262, 274, 128].$$

In other words, we have

$$\mathrm{F} \equiv \mathrm{QR}^{23}\Delta + 24\mathrm{QR}^{21}\Delta^2 + \cdots + 128\mathrm{QR}\Delta^{11} \pmod{283}.$$

(In these computations, I have selected 127 as "$\sqrt{-2}$" mod 283.)

References

[1] E. ARTIN, Über eine neue Art von L-Reihen, *Hamb.Abh.* **3** (1923), 89-108 (= Coll.Papers, 105-124).

[2] N. BOSTON, W. DABROWSKI, T. FOGUEL, P.J. GIES, D.A. JACKSON, J. LEAVITT and D.T. OSE, The proportion of fixed-point-free elements of a transitive permutation group, *Comm. Algebra* **21** (1993), 3259-3275.

[3] W. Burnside, Theory of Groups of Finite Order, 2nd edition, Cambridge Univ. Press 1911 (= Dover Publ., 1955).

[4] P.J. Cameron and A.M. Cohen, On the number of fixed point free elements in a permutation group, *Discrete Math.* **106/107** (1992), 135-138.

[5] T. Crespo, Galois representations, embedding problems and modular forms, *Collectanea Math.* **48** (1997), 63-83.

[6] F.G. Frobenius, Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, *J. Crelle* **101** (1887), 279-299 (= Ges.Abh., II, 304-330).

[7] F.G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitz.Akad.Wiss.Berlin* (1896), 689-703 (= Ges.Abh., II, 719-733).

[8] F.G. Frobenius, Über auflösbare Gruppen IV, *Sitz.Akad.Wiss.Berlin* (1901), 1216-1230 (= Ges.Abh., III, 189-203)

[9] C. Jordan, Recherches sur les substitutions, *J. Liouville* **17** (1872), 351-367 (= Oe.I.52).

[10] L. Kronecker, Über die Irreductibilität von Gleichungen, *Sitz.Akad.Wiss. Berlin* (1880), 155-162 (= Werke, II, 83-93).

[11] H.W. Lenstra, Jr. and P. Stevenhagen, Chebotarëv and his density theorem, *Math.Intelligencer* **18** (1996), 26-37.

[12] J. Martinet, Petits discriminants des corps de nombres, *Journées Arithmétiques 1980* (J.V.Armitage, edit.), Cambridge U.Press, Cambridge 1982, pp.151-193.

[13] R.W.K. Odoni, On the norms of algebraic integers, *Mathematika* **22** (1975), 71-80.

[14] M. Rubinstein and P. Sarnak, Chebyshev's Bias, *Experimental Math.* **3** (1994), 173-197.

[15] E.S. Selmer, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287-302.

[16] J-P. Serre, Divisibilité de certaines fonctions arithmétiques, *L'Ens. Math.* **22** (1976), 227-260 (= Oe.108).

[17] J-P. Serre, Modular forms of weight one and Galois representations, in *Algebraic Number Fields* (A.Fröhlich edit.), Acad.Press, London, 1977, pp.193-268 (= Oe.110).

[18] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ.Math.I.H.E.S.* **54** (1981), 123-201 (= Oe.125).

[19] N. Tschebotareff (Chebotarev), Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math.Ann.* **95** (1925), 191-228 (= Coll. Works, vol. 1, Moscow, 1949-1950).

[Texte rédigé avec l'aide de Heng Huat Chan.]

Séminaire Bourbaki mars 2004
2003-2004, exposé n° 932

COMPLÈTE RÉDUCTIBILITÉ

1. Introduction : le cas du groupe linéaire

1.1. Rappels

Soient k un corps commutatif et Γ un groupe. Un Γ-*module* (ou *une représentation linéaire* de Γ) est un k-espace vectoriel V de dimension finie, muni d'une action linéaire de Γ.

On dit que :

(1.1.1) V est *irréductible* (ou *simple*) si $V \neq 0$ et si V ne contient aucun sous-Γ-module distinct de 0 et de V.

(1.1.2) V est *complètement réductible* (ou *semi-simple*) si V est somme directe de Γ-modules irréductibles.

(1.1.3) V est *indécomposable* si $V \neq 0$, et si V n'est pas somme directe de deux sous-Γ-modules $\neq 0$.

[Dans la suite, nous abrégerons en écrivant ir, cr, ind respectivement.]

Les propriétés suivantes sont bien connues :

(1.1.4) V est cr si et seulement si, pour tout sous-module W de V, il existe un sous-module W' de V tel que $V = W \oplus W'$.

(1.1.5) Si V est somme directe de sous-modules V_i, alors V est cr $\Leftrightarrow$ tous les V_i sont cr.

On connaît moins bien les propriétés relatives au produit tensoriel $V \otimes V'$ de deux représentations V et V'. La plupart des cours d'Algèbre se bornent à définir le produit en question, et à en démontrer des propriétés évidentes. Aucun, à ma connaissance, ne signale le résultat très frappant suivant, dû à Chevalley :

Théorème 1.1 ([Ch 55, p. 88]). — *Supposons k de caractéristique 0. Si* V *et* V' *sont des* Γ*-modules complètement réductibles, leur produit tensoriel* $V \otimes V'$ *est complètement réductible.*

(Noter que l'on ne fait aucune hypothèse sur le groupe Γ.)

Lorsqu'on veut étendre ce théorème à la caractéristique p (avec des conditions restrictives sur dim V et dim V′, cf. prop. 5.8), il est utile de disposer d'une notion de *complète réductibilité* dans laquelle le groupe linéaire $\mathbf{GL}(\mathrm{V})$ est remplacé par un groupe réductif quelconque. Cette notion peut se définir, soit en termes de sous-groupes paraboliques, soit en termes d'*immeubles de Tits*, cf. [Se 97b], [Se 98]. C'est ce que nous allons voir. Les §§ 2,3 contiennent les énoncés généraux, et les §§ 4,5 donnent des critères plus précis, ainsi que diverses applications.

1.2. Exemple : l'immeuble de $\mathbf{GL}(\mathrm{V})$

Soit V un k-espace vectoriel de dimension finie n. On supposera $n \geqslant 2$ (sinon, l'immeuble correspondant est vide).

1.2.1. *Définition.* — L'immeuble de $\mathbf{GL}(\mathrm{V})$, appelé aussi immeuble de V, est un complexe simplicial $\mathrm{X} = \mathrm{X}(\mathrm{V})$, de dimension $n-2$, qui est défini de la manière suivante :

– les sommets de X correspondent bijectivement aux sous-espaces vectoriels de V distincts de 0 et de V. (Si W est un tel sous-espace, on note x_{W} le sommet correspondant.)

– un ensemble s de sommets de X est un simplexe de X si et seulement si les sous-espaces vectoriels correspondants forment un drapeau, i.e. une filtration strictement croissante de V. [Si l'on préfère la géométrie projective à la géométrie affine, on peut aussi voir les sommets de X comme les sous-variétés projectives de l'espace projectif $\mathbf{P}(\mathrm{V})$, distinctes de $\varnothing$ et de $\mathbf{P}(\mathrm{V})$.]

1.2.2. *Type.* — Si $x = x_{\mathrm{W}}$ est un sommet de X, on note $\mathrm{type}(x)$ la dimension de l'espace vectoriel W. L'ensemble des types de sommets est l'ensemble $\mathrm{I} = \{1, \ldots, n-1\}$.

1.2.3. *Opposition.* — Deux sommets $x = x_{\mathrm{W}}$ et $x' = x_{\mathrm{W}'}$ sont dits *opposés* si V est somme directe de W et W′ ; leurs types se correspondent par l'involution $t \mapsto n-t$ de I. Deux simplexes sont *opposés* si tout sommet de l'un est opposé à un sommet de l'autre. En termes de filtrations, cela correspond à la notion usuelle de *filtrations opposées*.

1.2.4. *Sous-groupes paraboliques.* — Les sous-groupes paraboliques de $\mathbf{GL}(\mathrm{V})$ sont les stabilisateurs des drapeaux de V. Les sous-groupes paraboliques *propres* (i.e. distincts de $\mathbf{GL}(\mathrm{V})$) correspondent donc aux simplexes non vides de l'immeuble X ; les paraboliques maximaux correspondent aux sommets de X et le groupe $\mathbf{GL}(\mathrm{V})$ au simplexe $\varnothing$. Deux simplexes s et s', correspondant aux paraboliques P et P′, sont opposés au sens du n° 1.2.3 si et seulement

si P et P′ sont opposés au sens usuel du terme, c'est-à-dire si $P \cap P'$ est un sous-groupe de Levi de chacun d'eux, cf. [BT 65, 4.8].

1.2.5. *Appartements.* — Soit T un tore déployé maximal de $\mathbf{GL}(V)$. L'action de T sur V décompose V en somme directe de droites D_i. Si, dans la définition de X, on se restreint aux W qui sont sommes directes de certaines des D_i, on obtient un sous-complexe C de X qui est isomorphe au *complexe de Coxeter* du groupe symétrique S_n. D'un point de vue combinatoire, c'est la subdivision barycentrique du bord d'un $(n-1)$-simplexe ; topologiquement, c'est une sphère de dimension $n-2$. Un sous-complexe de X obtenu de cette façon est appelé un *appartement* de X. Par construction, les appartements correspondent aux tores déployés maximaux de $\mathbf{GL}(V)$.

1.2.6. *Exemple.* — Prenons $n = 3$. L'immeuble correspondant est un *graphe*, qui a deux types de sommets : ceux qui correspondent aux points du plan projectif et ceux qui correspondent aux droites. Deux sommets sont voisins (i.e. sont les extrémités d'une arête) si et seulement si ils correspondent à un point situé sur une droite : la relation de voisinage est la relation d'incidence. Les appartements sont les hexagones *a-B-c-A-b-C-a* associés aux triangles *ABC*, de côtés $a = BC$, $b = CA$, $c = AB$: la théorie de Tits transforme triangles en hexagones !

1.3. Traductions immobilières : le cas de $\mathbf{GL}(V)$

Si V est un Γ-module, le groupe Γ opère de façon naturelle sur l'immeuble $X = X(V)$ du n° 1.2. Cette action respecte les types (au sens du n° 1.2.2). En particulier, si un simplexe s de X est stable par Γ, il est fixé par Γ. Si P est le sous-groupe parabolique correspondant à s, P est normalisé par Γ, i.e. contient Γ (puisqu'un parabolique est son propre normalisateur). Le sous-espace X^Γ des points fixes de Γ est un *sous-complexe simplicial* de X, et les définitions du n° 1.1 se traduisent de la façon suivante :

(1.3.1) V est *irréductible* $\Leftrightarrow X^\Gamma = \varnothing \Leftrightarrow$ Γ n'est contenu dans aucun sous-groupe parabolique propre de $\mathbf{GL}(V)$.

(1.3.2) V est *complètement réductible* $\Leftrightarrow$ pour tout sommet x de X^Γ il existe un sommet x' de X^Γ qui est opposé à x (cf. 1.2.3) $\Leftrightarrow$ pour tout parabolique maximal P contenant Γ, il existe un parabolique P′ opposé à P qui contient Γ.

(1.3.3) V est *indécomposable* $\Leftrightarrow X^\Gamma$ ne contient aucun couple de sommets opposés $\Leftrightarrow$ il n'existe pas de couple (P, P') de paraboliques propres de $\mathbf{GL}(V)$ qui soient opposés et contiennent tous deux Γ.

Il n'est pas difficile de montrer que (1.3.2) équivaut à :

(1.3.2′) pour tout simplexe s de X^Γ, il existe un simplexe s' de X^Γ qui est opposé à $s \Leftrightarrow$ pour tout parabolique P (maximal ou pas) contenant Γ, il existe un parabolique opposé à P qui contient Γ.

2. La complète réductibilité dans les immeubles sphériques

2.1. Immeubles sphériques

Un immeuble sphérique est un complexe simplicial X, muni d'une famille de sous-complexes appelés *appartements*. Je renvoie à [Ti 74] pour la liste des axiomes ; voir aussi [Br 89], [Ron 89] et [TW 02, § 40]. Voici quelques-unes des propriétés de ces immeubles :

2.1.1. *Dimension et rang.* — Le complexe X est de dimension finie. L'entier $r = \dim(X) + 1$ est appelé le *rang* de X. Lorsque $X = \varnothing$, on convient que $\dim(X) = -1$, de sorte que $r = 0$. Tout simplexe maximal est de dimension $\dim(X)$.

2.1.2. *Types des sommets.* — Soit $\mathrm{som}(X)$ l'ensemble des sommets de X. Il existe une unique relation d'équivalence R sur $\mathrm{som}(X)$ ayant les propriétés suivantes :

(a) L'ensemble quotient $\mathrm{som}(X)/R$ a r éléments.

(b) Deux sommets appartenant à un même simplexe ne sont R-équivalents que s'ils sont égaux.

Si $x \in \mathrm{som}(X)$, l'image de x dans $I = \mathrm{som}(X)/R$ est appelée le *type* de x, et notée $\mathrm{type}(x)$. On dit qu'un automorphisme f de X *préserve les types* si x et $f(x)$ ont même type quel que soit $x \in \mathrm{som}(X)$.

Exemple. Lorsque X est l'immeuble $X(V)$ du n° 1.2, on peut identifier I à $\{1, \ldots, n-1\}$, cf. 1.2.2.

2.1.3. *Appartements.* — Un appartement est isomorphe au complexe de Coxeter d'un groupe de Coxeter fini qui ne dépend que de X ; c'est une sphère de dimension $r - 1$. Deux simplexes quelconques sont contenus dans un appartement.

2.1.4. *Opposition et géodésiques.* — Soient x et y deux points de X (c'est-à-dire de sa réalisation géométrique), et soit A un appartement les contenant. On dit que x et y sont *opposés* dans X s'ils le sont dans A (ce qui a un sens puisque A est un complexe de Coxeter) ; cela ne dépend pas du choix de A. Deux simplexes sont dits opposés si chaque sommet de l'un est opposé à un sommet de l'autre. Si x et y ne sont pas opposés, il y a une unique géodésique xy

qui les joint dans A. Elle est indépendante (paramétrisation comprise) du choix de A.

2.1.5. *Convexité.* — Une partie Y de X est dite *convexe*, si l'on a $xy \subset Y$ pour tout couple de points x, y de Y, non opposés. On dit que Y est *strictement convexe* si Y est convexe et ne contient aucun couple de points opposés (c'est la notion de « convexité » de [Ti 74] et de [Mu 65, p. 63]).

2.1.6. *Sphères de Levi.* — Une sphère de Levi est un sous-complexe S de X qui est contenu dans un appartement A, et qui est l'intersection de A (vu comme sphère) avec un sous-espace vectoriel.

2.1.7. *Remarque.* — Ces définitions se présentent de façon un peu plus naturelle si l'on introduit l'immeuble vectoriel X^{vect} associé à X, dans lequel les points de X sont remplacés par des demi-droites, ayant en commun un point « 0 » (cf. [Rou 78]). Les appartements deviennent alors des espaces vectoriels de dimension r, et les sphères de Levi des sous-espaces vectoriels définis par l'annulation de certaines racines. Si x et y sont deux points de X^{vect}, leur somme $x + y$ a un sens, et l'on a

$$x + (y + z) = (x + y) + z$$

pourvu que x, y et z appartiennent à un même appartement. Deux points x et x' sont opposés si $x + x' = 0$. Une partie de X est convexe si le cône correspondant de X^{vect} est stable par $(x, y) \mapsto x + y$, autrement dit si son intersection avec tout appartement est un cône convexe au sens usuel du terme.

2.1.8. *Immeuble résiduel.* — Soit s un simplexe de X de dimension m. On note X_s, ou $St(s)$, l'immeuble résiduel (« link ») de X en s, cf. [Ti 74]). Rappelons que les simplexes de X_s de dimension d correspondent bijectivement aux simplexes de X contenant s de dimension $d + m + 1$ (de sorte que le simplexe vide de X_s correspond à s). Si Y est un sous-complexe de X, les simplexes de Y contenant s définissent un sous-complexe Y_s de X_s ; si Y est convexe, il en est de même de Y_s.

Soit S une sphère de Levi, et soient s et s' deux simplexes de S de dimension maximale. Il y a un isomorphisme canonique $proj : X_s \to X_{s'}$ (défini dans [Ti 74, § 3.19]). Ces isomorphismes satisfont à la condition de transitivité usuelle, ce qui permet d'écrire X_S à la place de X_s. L'immeuble X_S peut être appelé *l'immeuble* de S. Les sphères de Levi de X_S correspondent bijectivement aux sphères de Levi de X contenant S.

2.2. Complète réductibilité et contractibilité

2.2.1. *Définition.* — Une partie Y de X est dite *complètement réductible* (en abrégé : X-cr, ou simplement cr) si elle est convexe, et si, pour tout point $y \in Y$, il existe $y' \in Y$ qui est opposé à y.

Dans la suite, nous nous intéresserons surtout au cas où Y est un sous-complexe convexe de X (ou, parfois, de sa subdivision barycentrique) ; dans ce cas, la condition cr équivaut à dire que, pour tout simplexe s de Y, il existe un simplexe s' de Y qui est opposé à s (il suffit même que tout sommet de Y ait un opposé dans Y, cf. th. 2.2 ci-dessous).

Exemple de sous-complexe convexe. Prenons pour X l'immeuble X(V) du n° 1.2. Soit L un ensemble de sous-espaces vectoriels de V tel que :

$$W, W' \in L \implies W \cap W' \in L \text{ et } W + W' \in L.$$

Soit Y_L le sous-complexe plein de X(V) dont les sommets sont les x_W, pour $W \in L$ et $W \neq 0, V$ (cf. 1.2.1). Alors Y_L est *convexe*, et l'on obtient ainsi tous les sous-complexes convexes de X(V).

2.2.2. Nous allons donner un critère topologique permettant de reconnaître si un sous-complexe convexe est cr. Précisons que nous munissons X de la topologie limite inductive : une partie de X est ouverte si ses intersections avec les sous-complexes finis de X le sont. (Une autre topologie est souvent utile : celle définie par la distance angulaire ; elle n'interviendra pas ici.)

Rappelons d'autre part qu'un espace est *contractile* s'il a le type d'homotopie d'un point ; un espace discret est contractile si et seulement si son cardinal est égal à 1 (l'ensemble vide n'est pas contractile !).

THÉORÈME 2.1 ([Se 97b]). — *Soit* Y *un sous-complexe convexe de* X. *Les propriétés suivantes sont équivalentes* :

(a) Y *est* X-cr.

(b) Y *contient un couple* (s, s') *de simplexes opposés ayant même dimension que* Y.

(c) Y *contient une sphère de Levi* S *de dimension* $\dim(Y)$.

(d) Y *n'est pas contractile.*

Démonstration. — (a) $\Rightarrow$ (b) est clair.

(b) $\Rightarrow$ (c) : le plus petit sous-complexe convexe $C(s, s')$ contenant s et s' est une sphère de Levi.

(c) $\Rightarrow$ (d) : la sphère S définit un cycle dans Y qui n'est pas homologue à 0 puisqu'il est de même dimension que Y (ceci ne vaut que si $\dim(Y) \geqslant 1$, mais le cas $\dim(Y) \leqslant 0$ est immédiat).

(d) $\Rightarrow$ (a) : si Y n'est pas cr, il existe un point $y \in Y$ qui n'a pas d'opposé dans Y, et l'on contracte Y grâce aux géodésiques issues de y.

THÉORÈME 2.2. — *Les conditions* $(a), \ldots, (d)$ *du th.* 2.1 *sont équivalentes à* :

(e) *Pour tout sommet* x *de* Y*, il existe un sommet* x' *de* Y *qui est opposé à* x*.*

La démonstration sera donnée au n° 2.2.5 ci-dessous.

2.2.3. *Remarques.* — 1) Un résultat analogue au th. 2.1 vaut pour les sous-complexes convexes de la subdivision barycentrique de X, à condition d'utiliser d'autres sphères que les sphères de Levi.

2) Supposons que Y soit cr, et non vide. On peut préciser sa structure topologique de la façon suivante :

Choisissons un simplexe s de Y de dimension maximum, et soit $U(s)$ l'ensemble des simplexes de Y qui sont opposés à s. Si $t \in U(s)$, soit $S_t = C(s,t)$ la sphère de Levi définie par s et t. Soit $B = *\,S_t$ le bouquet des sphères S_t $(t \in U(s))$; le choix d'un point x de s permet d'envoyer B dans Y.

PROPOSITION 2.3. — *L'application* $B \to Y$ *ainsi définie est une équivalence d'homotopie.*

(Autrement dit, Y a le type d'homotopie d'un bouquet de n-sphères, où $n = \dim(Y)$.)

Démonstration. — Soit x un point intérieur à s, et soit Y' le complexe obtenu en retirant de Y les intérieurs des simplexes appartenant à $U(s)$. Si $y \in Y'$, il est clair que y n'est pas opposé à x ; de plus, on peut montrer que la géodésique xy est contenue dans Y'. Il en résulte que Y' est contractile. On peut donc contracter Y' en un point sans changer le type d'homotopie de Y. On obtient ainsi le bouquet de sphères B, et la prop.2.3 s'en déduit. (Noter que cet argument est le même que celui employé par SOLOMON-TITS [So 69] dans le cas particulier où $Y = X$.)

On peut aussi se placer à un point de vue homologique. Il est commode d'utiliser les groupes d'homologie réduits $\widetilde{H}_i(Y, \mathbf{Z})$; rappelons que ces groupes sont égaux aux groupes d'homologie usuels si $i > 0$ et que $\widetilde{H}_0(Y, \mathbf{Z})$ et $\widetilde{H}_{-1}(Y, \mathbf{Z})$ sont respectivement le noyau et le conoyau de l'homomorphisme $H_0(Y, \mathbf{Z}) \to \mathbf{Z}$. En particulier $\widetilde{H}_{-1}(Y, \mathbf{Z})$ est 0 si $Y \neq \varnothing$ et est $\mathbf{Z}$ si $Y = \varnothing$. Si Y est contractile, tous les $\widetilde{H}_i(Y, \mathbf{Z})$ sont nuls.

PROPOSITION 2.4. — *Si* Y *est un sous-complexe convexe de dimension* n*, on a* $\widetilde{H}_i(Y, \mathbf{Z}) = 0$ *pour* $i \neq n$*, et* $\widetilde{H}_n(Y, \mathbf{Z})$ *est un groupe abélien libre de rang égal à* $\mathrm{Card}(U(s))$ *; il est* $\neq 0$ *si et seulement si* Y *est* cr*.*

Cela résulte de la prop. 2.3.

2.2.4. *Réduction.* — L'énoncé suivant permet souvent de passer de X à l'un des immeubles résiduels X_s du n° 2.1.8.

PROPOSITION 2.5. — *Soit* Y *un sous-complexe convexe de* X*, et soit* S *une sphère de Levi contenue dans* Y*. Soit* X_S *l'immeuble associé à* S*, et soit* Y_S *le sous-complexe de* X_S *défini par* Y*. Pour que* Y *soit* X-cr*, il faut et il suffit que* Y_S *soit* X_S-cr*.*

(Précisons comment est défini Y_S : on choisit un simplexe s de S de dimension maximum, et l'on prend l'image de Y_s par l'isomorphisme naturel $X_s \to X_S$.)

La démonstration utilise le lemme suivant ([Ti 74, p. 54]) :

Lemme 2.6. — Soit $\{s, s'\}$ *un couple de simplexes opposés, et soient* t_1, t_2 *deux simplexes de* X_s *(identifiés à des simplexes de* X *contenant* s*). Soit* t_1' *le simplexe de* $X_{s'}$ *correspondant à* t_1 *par l'isomorphisme* $\mathrm{proj} : X_s \to X_{s'}$*. Alors :*

$$t_1 \text{ et } t_2 \text{ sont opposés dans } X_s \Leftrightarrow t_1' \text{ et } t_2 \text{ sont opposés dans } X.$$

Démonstration de la prop. 2.5. Soit s un simplexe de S de dimension maximum, et soit t_1 un simplexe de Y contenant s et de dimension égale à $\dim(Y)$. Supposons d'abord que Y_s soit X_s-cr. Soit s' l'unique simplexe de S opposé à s. Puisque Y_s est cr, il existe un simplexe t_2 de Y contenant s, qui est opposé à t_1 dans Y_s. Le simplexe t_1' du lemme 2.6 est opposé à t_2, et est contenu dans Y du fait que Y est convexe (utiliser la définition de l'isomorphisme $\mathrm{proj} : X_s \to X_{s'}$ donnée dans [Ti 74, § 3.19]). On en déduit que Y contient la sphère de Levi définie par $\{t_2, t_1'\}$, d'où le fait que Y est cr d'après le th. 2.1. Inversement, si Y est cr, il contient un simplexe opposé à t_1, d'où une sphère de Levi S' de même dimension que Y ; le sous-complexe S_s' de X_s est une sphère de Levi contenue dans Y_s et de même dimension ; il en résulte que Y_s est cr.

2.2.5. *Démonstration du théorème 2.2.* — Il s'agit de prouver que (e) $\Leftrightarrow$ (a). L'implication (a) $\Rightarrow$ (e) est évidente. On prouve (e) $\Rightarrow$ (a) par récurrence sur $\dim(X)$. Si $Y = \varnothing$, l'énoncé est clair. Sinon, choisissons un sommet y de Y, que nous identifions à un simplexe de dimension 0. Puisque Y satisfait à (e), il contient un sommet y' opposé à y. Le couple $\{y, y'\}$ est une sphère de Levi de dimension 0. Vu la prop. 2.5, pour prouver que Y est X-cr il suffit de montrer que le sous-complexe Y_y de l'immeuble résiduel X_y est X_y-cr. Comme $\dim(X_y) = \dim(X) - 1$, on peut appliquer l'hypothèse de récurrence au couple (X_y, Y_y) ; il suffit donc de prouver que Y_y a la propriété (e). Cela revient à montrer que, pour toute arête yz de Y d'extrémité y, il existe une autre

arête yz_1 qui est opposée à la précédente dans X_y. Choisissons un sommet z' de Y opposé à z, ce qui est possible d'après (e). Il existe une sphère de Levi D de dimension 1 (« cercle de Levi ») contenant z' et yz. De plus, z' et yz sont contenus dans le demi-cercle formé de la réunion de yz et de la géodésique yz'. Soit z_1 le sommet de la géodésique yz' qui est le plus proche de y, tout en étant distinct de y. L'image D_y de D dans X_y est égale à $\{yz, yz_1\}$, et c'est une sphère de Levi de dimension 0 de X_y ; il en résulte que yz et yz_1 sont opposés dans X_y, comme on le désirait.

2.3. Groupes agissant sur X

2.3.1. Soit Γ un groupe agissant sur X, i.e. muni d'un homomorphisme $\Gamma \to \mathrm{Aut}(X)$. Soit X^Γ le sous-espace de X fixé par Γ. Il est clair que X^Γ est convexe : si Γ fixe deux points x et y qui ne sont pas opposés, il fixe la géodésique xy. Par analogie avec le n° 1.3, nous dirons que l'action de Γ sur X est :

– *irréductible*, si $X^\Gamma = \varnothing$;
– *complètement réductible*, si X^Γ est cr ;
– *indécomposable*, si X^Γ est strictement convexe (cf. n° 2.1.5).

Comme précédemment, nous utiliserons les abréviations ir, cr et ind.

Remarque : L'espace X^Γ est un sous-complexe de la subdivision barycentrique de X. Si l'action de Γ préserve les types (ce qui sera le cas dans les § § 3,4,5), c'est même un sous-complexe de X. D'après le th. 2.1 (complété par la Remarque 2.2.3.1), X^Γ *est contractile si et seulement si l'action de* Γ *sur* X *n'est pas* cr.

2.3.2. Voici une propriété de réduction, au sens du n° 2.2.4 :

PROPOSITION 2.7. — *Supposons que* Γ *préserve les types, et qu'il fixe une sphère de Levi* S*, auquel cas il opère sur l'immeuble* X_S *correspondant. On a l'équivalence suivante* :

L'action de Γ *sur* X *est* cr $\Leftrightarrow$ *L'action de* Γ *sur* X_S *est* cr.

Cela résulte de la prop. 2.5, appliquée au sous-complexe $Y = X^\Gamma$ de X.

2.4. La conjecture du point fixe

CONJECTURE 2.8. — *Soit* Y *un sous-complexe de* X (ou de sa subdivision barycentrique)*, convexe et contractile. Il existe alors un point de* Y *qui est fixé par tout automorphisme de* X *qui stabilise* Y.

(Un tel point mérite d'être appelé un *centre* de Y.)

Cette conjecture a été faite par TITS dans les années 50, sous l'hypothèse supplémentaire que Y est strictement convexe ; son but était, semble-t-il, de prouver un résultat sur les groupes unipotents que BOREL et lui ont démontré ensuite par une méthode différente, cf. [BT 71]. Sous cette forme plus restrictive, la conjecture est signalée par MUMFORD [Mu 65, p. 64] à cause de ses relations avec la « Geometric Invariant Theory » (G.I.T.). En fait, le cas particulier utile pour G.I.T. a été démontré en 1978 par KEMPF [Ke 78] et ROUSSEAU [Rou 78]. Il y a d'ailleurs beaucoup d'autres cas où 2.8 a été démontrée, cf. [Rou 78], [Ti 97] et [Mü 97].

PROPOSITION 2.9. — *Admettons la conjecture* 2.8. *Soit* Y *un sous-complexe convexe contractile de* X *et soit* Γ *un groupe d'automorphismes de* X *préservant les types, et stabilisant* Y. *Alors* Y^Γ *est contractile.*

Il est clair que Y^Γ est un sous-complexe convexe de X. D'après 2.8, il est non vide. Il s'agit de montrer qu'il n'est pas cr. S'il l'était, il contiendrait une sphère de Levi S de même dimension, cf. th. 2.1. L'image Y_S de Y dans X_S est stable par Γ, et est contractile (prop. 2.5). En lui appliquant la conjecture 2.8, on en déduirait que $(Y^\Gamma)_S = (Y_S)^\Gamma$ est non vide, ce qui est impossible puisque S et Y^Γ ont la même dimension.

PROPOSITION 2.10. — *La prop.* 2.9 *est vraie* (*sans supposer que la conjecture* 2.8 *le soit*) *dans chacun des deux cas suivants* :

(a) $\dim(Y) \leqslant 1$.

(b) *L'image de* Γ *dans* $\mathrm{Aut}(Y)$ *est un groupe résoluble fini.*

Le cas (a) est clair si $\dim(Y) = 0$, car Y est réduit à un point ; il est facile si $\dim(Y) = 1$ car Y est un arbre de diamètre borné, et un tel arbre a un centre, à savoir le milieu des chemins sans aller-retour de longueur égale au diamètre.

Pour (b), on se ramène par dévissage au cas où Γ agit sur Y par un groupe cyclique d'ordre premier p. Comme les $\widetilde{H}_i(Y, \mathbf{Z}/p\mathbf{Z})$ sont tous nuls, il en est de même des $\widetilde{H}_i(Y^\Gamma, \mathbf{Z}/p\mathbf{Z})$ d'après la théorie de Smith; en effet, cette théorie dit que, si $\Gamma \simeq \mathbf{Z}/p\mathbf{Z}$ opère sur un complexe Y de dimension finie, et si les $\widetilde{H}_i(Y, \mathbf{Z}/p\mathbf{Z})$ sont nuls pour $i > N$ (où N est un entier fixé), il en est de même des $\widetilde{H}_i(Y^\Gamma, \mathbf{Z}/p\mathbf{Z})$ pour $i > N$. Or, si Y n'était pas contractile, il serait cr, et le groupe $\widetilde{H}_i(Y^\Gamma, \mathbf{Z}/p\mathbf{Z})$ correspondant à $i = \dim(Y^\Gamma)$ serait non nul d'après la prop. 2.4.

Action de sous-groupes normaux

PROPOSITION 2.11. — *Admettons la conjecture* 2.8. *Soit* Γ *un groupe d'automorphismes de X respectant les types, et soit* Γ' *un sous-groupe normal de* Γ.

Si l'action de Γ *est* cr, *il en est de même de celle de* Γ'.

(Comparer avec le résultat bien connu suivant : si une représentation linéaire d'un groupe Γ est complètement réductible, il en est de même de ses restrictions aux sous-groupes normaux de Γ, cf. e.g. [Se 94, lemme 5].)

Posons $Y' = X^{\Gamma'}$ et $Y = X^{\Gamma} = Y'^{\Gamma/\Gamma'}$. Il s'agit de montrer que Y' n'est pas contractile. S'il l'était, la prop. 2.9, appliquée à (X, Y', Γ), montrerait que $Y = X^{\Gamma}$ est contractile, contrairement à l'hypothèse faite.

Un argument analogue, utilisant la prop. 2.10, démontre :

PROPOSITION 2.12. — *Si* Γ/Γ' *est un groupe résoluble fini, la prop.* 2.11 *est vraie sans supposer que la conjecture* 2.8 *le soit.*

Nous verrons au § 3.3 un autre cas du même genre (th. 3.6).

3. Complète réductibilité des sous-groupes d'un groupe réductif

Dans ce qui suit, G désigne un groupe algébrique réductif sur un corps k (cf. [BT 65]). Rappelons qu'un tel groupe est lisse et connexe.

Par un « sous-groupe algébrique » de G, on entend un k-sous-groupe algébrique (« défini sur k »).

3.1. L'immeuble de G

3.1.1. *Sous-groupes paraboliques.* — Un sous-groupe parabolique de G est un sous-groupe algébrique P tel que G/P soit une variété projective (définition équivalente : après extension des scalaires, P contient un sous-groupe de Borel). Un tel groupe est lisse, connexe, et coïncide avec son normalisateur dans G. Les propriétés de ces groupes dont nous aurons besoin se trouvent dans [BT 65] ; voir aussi [DG 70, XXVI].

3.1.2. *L'immeuble de* G. — Sa définition est donnée dans [Ti 74, § 5]. On le notera X(G) ou simplement X. Ses simplexes correspondent aux sous-groupes paraboliques de G ; si s est un simplexe, on note P_s le sous-groupe parabolique correspondant. Les sommets de X correspondent aux paraboliques propres maximaux ; le simplexe vide correspond à G. Le rang r de X est égal au k-rang semi-simple de G, c'est-à-dire au k-rang (ou *rang relatif*) de $G^{ad} = G/C_G$, où C_G est le centre de G. On a $r = 0$ (et $X = \varnothing$) si G^{ad} est anisotrope.

3.1.3. *Appartements.* — Ils correspondent aux tores déployés maximaux (de G, ou de G^{ad}, c'est la même chose).

3.1.4. *Types de sommets.* — L'ensemble I des types de sommets peut être identifié à l'ensemble des sommets du k-diagramme de Dynkin de G.

3.1.5. *Opposition.* — Deux simplexes s et s' de X sont opposés si et seulement si les paraboliques P_s et $\mathrm{P}_{s'}$ sont opposés au sens de [BT 65, § 4], i.e. si $\mathrm{P}_s \cap \mathrm{P}_{s'}$ est réductif, auquel cas c'est un sous-groupe de Levi de chacun d'eux.

3.1.6. *Action de* $\mathrm{G}(k)$. — Le groupe $\mathrm{G}(k)$ des k-points de G opère sur X (par conjugaison des paraboliques). Cette action respecte les types. Si s est un simplexe de X, le sous-groupe de $\mathrm{G}(k)$ fixant (ou stabilisant) s est $\mathrm{P}_s(k)$.

3.1.7. *Sphères de Levi.* — Soit L un sous-groupe de Levi d'un parabolique. Les sous-groupes paraboliques contenant L correspondent aux simplexes d'une *sphère de Levi* S_L, et l'on obtient ainsi une bijection entre les L et les sphères de Levi (ce qui explique la terminologie utilisée au § 2). Les paraboliques ayant L pour sous-groupe de Levi correspondent aux simplexes de dimension maximale de la sphère S_L. Si s est l'un de ces simplexes, l'immeuble résiduel X_s (cf. 2.1.8) peut être identifié à l'immeuble de L.

3.1.8. *Critère de convexité.* — Soit Y un sous-complexe de X, et soit H l'ensemble des paraboliques correspondant aux simplexes de Y.

PROPOSITION 3.1. — *Pour que* Y *soit convexe, il faut et il suffit que* H *satisfasse à la propriété suivante* :

(C) *Si trois paraboliques* P, P', Q *sont tels que* $\mathrm{P} \in \mathrm{H}$, $\mathrm{P}' \in \mathrm{H}$, *et* $\mathrm{Q} \supset \mathrm{P} \cap \mathrm{P}'$, *alors* $\mathrm{Q} \in \mathrm{H}$.

(Attention : l'inclusion $\mathrm{Q} \supset \mathrm{P} \cap \mathrm{P}'$ est une inclusion de groupes algébriques. Il ne suffit pas que $\mathrm{Q}(k)$ contienne $\mathrm{P}(k) \cap \mathrm{P}'(k)$.)

L'énoncé revient à déterminer l'enveloppe convexe de la réunion de deux simplexes (ceux correspondant à P et P′), ce qui se fait au moyen d'un appartement les contenant tous deux.

3.1.9. *Relations avec les sous-groupes multiplicatifs à 1 paramètre (G.I.T.).*

Soit $\lambda : \mathbf{G}_m \to \mathrm{G}$ un homomorphisme. On peut lui associer de façon naturelle deux points opposés $h_+(\lambda)$ et $h_-(\lambda)$ de l'immeuble vectoriel $\mathrm{X}^{\mathrm{vect}}$, cf. 2.1.7. Si λ est à valeurs dans le centre de G, on a $h_+(\lambda) = h_-(\lambda) = 0$. Sinon, les demi-droites engendrées par $h_+(\lambda)$ et $h_-(\lambda)$ définissent deux points $x_+(\lambda)$ et $x_-(\lambda)$ de l'immeuble X ; ces points sont opposés. Soient $s_+(\lambda)$ et $s_-(\lambda)$ les plus petits simplexes de X contenant respectivement $x_+(\lambda)$ et $x_-(\lambda)$, et soient $\mathrm{P}_+(\lambda)$ et $\mathrm{P}_-(\lambda)$ les sous-groupes paraboliques correspondants. Le groupe $\mathrm{P}_+(\lambda)$ est formé des points g de G qui sont *contractés* par λ, i.e. tels que $\lambda(t).g.\lambda(t^{-1})$ ait une limite pour $t \to 0$ (cf. [Mu 65, p. 55] ou [Ri 88,

§ 2]). De même, $P_-(\lambda)$ est l'ensemble des g tels que $\lambda(t).g.\lambda(t^{-1})$ ait une limite pour $t \to \infty$, et le groupe de Levi $P_+(\lambda) \cap P_-(\lambda)$ est le *centralisateur* de l'image de λ.

Remarque. — Les $h_+(\lambda)$ jouent le rôle de *points entiers* pour l'immeuble vectoriel, et les $x_+(\lambda)$ sont les *points rationnels* de l'immeuble sphérique. L'interprétation des sous-groupes paraboliques en termes de contractions est à la base de la "Geometric Invariant Theory"; elle joue un rôle essentiel dans les résultats de RICHARDSON et de BATE-MARTIN-RÖHRLE cités plus loin.

3.2. Les propriétés G-ir, G-cr et G-ind

3.2.1. À partir de maintenant, Γ désigne un sous-groupe de $G(k)$. Son action sur X permet de lui appliquer les définitions du n° 2.3.1 : irréductibilité, complète réductibilité et indécomposabilité. Pour mettre G en évidence, nous écrirons G-ir, G-cr et G-ind. Autrement dit :

Γ *est* G-ir $\Leftrightarrow$ Γ *n'est contenu dans aucun sous-groupe parabolique propre de* G.

Γ *est* G-cr $\Leftrightarrow$ *Pour tout parabolique* P *de* G *contenant* Γ, *il existe un sous-groupe de Levi de* P *contenant* Γ (ou, ce qui revient au même, il existe un parabolique P' opposé à P tel que $\Gamma \subset P(k) \cap P'(k)$).

Γ *est* G-ind $\Leftrightarrow$ Γ *n'est contenu dans aucun sous-groupe de Levi d'un sous-groupe parabolique propre de* G.

3.2.2. *Exemples.* — Lorsque G est un groupe classique (ou un groupe de type G_2) la notion de « G-cr » peut se traduire très concrètement :

(a) Lorsque $G = \mathbf{GL}(V)$, elle signifie que le Γ-module V est semi-simple, cf. n° 1.3.

(b) Supposons k de caractéristique $\neq 2$, et prenons pour G un groupe $\mathbf{SO}(V)$ (ou $\mathbf{Sp}(V)$), relatif à une forme bilinéaire symétrique (ou alternée) B sur V, non dégénérée. La définition de « G-cr » donnée ci-dessus dit que Γ est G-cr si et seulement si, pour tout sous-Γ-module totalement isotrope W de V, il existe un autre sous-Γ-module totalement isotrope W', de même dimension, tel que la restriction de B à $W + W'$ soit non dégénérée. Un argument élémentaire permet de montrer que *cela se produit si et seulement si le* Γ*-module* V *est semi-simple* (c'est aussi une conséquence de la théorie de Richardson, du moins quand k est algébriquement clos, cf. [Ri 88, cor. 16.10]).

(c) Supposons G de type G_2, et k de caractéristique $\neq 2$. Soit V l'unique représentation irréductible de G de dimension 7. Ici encore, on peut montrer que Γ *est* G-cr *si et seulement si le* Γ*-module* V *est semi-simple.* Cela se voit en utilisant la description des paraboliques donnée dans [As 86].

On verra au § 5 des résultats analogues pour d'autres représentations – mais on devra alors éviter d'autres caractéristiques que la caractéristique 2.

3.2.3. La proposition suivante est une conséquence immédiate de la prop. 2.5 :

PROPOSITION 3.2. — *Supposons que* Γ *soit contenu dans un sous-groupe de Levi* L *d'un sous-groupe parabolique de* G. *On a alors*

$$\Gamma \text{ est G-cr} \iff \Gamma \text{ est L-cr.}$$

(Lorsque $G = \mathbf{GL}_n$, cela redonne (1.1.5).)

3.2.4. On peut définir un « G-analogue » de la *semi-simplification* d'une représentation :

Choisissons un parabolique P contenant Γ et minimal pour cette propriété (cela revient à choisir un simplexe de dimension maximum de X^Γ). Soit L un sous-groupe de Levi de P et soit $\pi : P \to L$ la projection de P sur L de noyau le radical unipotent $R_u(P)$ de P.

PROPOSITION 3.3. — (a) *Le groupe* $\pi(\Gamma) \subset L(k)$ *est* L-ir *et* G-cr.

(b) *Différents choix de* (P, L) *donnent des homomorphismes* $\Gamma \to L(k) \to G(k)$ *qui sont conjugués par* $G(k)$.

(Lorsque $G = \mathbf{GL}(V)$, l'homomorphisme $\Gamma \to L(k) \to G(k)$ est le semi-simplifié de $\Gamma \to G(k)$, et l'assertion d'unicité de (b) est le *théorème de Jordan-Hölder.*)

Dans (a), le fait que $\pi(\Gamma)$ soit L-ir provient de ce que P est minimal ; on en déduit que Γ est G-cr en appliquant la prop. 3.2. On prouve (b) en remarquant que, pour P fixé, le choix de L n'a pas d'importance puisque deux L différents sont conjugués par $R_u(P)(k)$; et, pour un autre choix P' de P, on utilise le fait que P et P' ont un sous-groupe de Levi commun (c'est une propriété générale des simplexes maximaux d'un sous-complexe convexe).

3.2.5. Voici un autre résultat, inspiré par des arguments de [Ri 88] et de [BMR 05] :

PROPOSITION 3.4. — *Soit* C_Γ *le centralisateur de* Γ *dans* G. *Soit* T *un tore déployé maximal de* C_Γ, *et soit* L *le centralisateur de* T *dans* G. *On a* $\Gamma \subset L(k)$. *De plus* :

(a) L *est un sous-groupe de Levi d'un parabolique de* G ; *il est minimal parmi tous les Levi de paraboliques contenant* Γ.

(b) Γ *est* L-ind.

(c) *Pour que* Γ *soit* G-cr, *il faut et il suffit qu'il soit* L-ir.

(d) *Si k est parfait, les différents choix de* L *sont conjugués par* $C_\Gamma(k)$.

(Lorsque $G = \mathbf{GL}(V)$, le choix de L correspond à une décomposition du Γ-module V en somme directe de modules indécomposables, et (d) est le *théorème de Krull-Remak-Schmidt.*)

L'assertion (a) se déduit du fait que les sous-groupes de Levi de paraboliques sont les centralisateurs des tores déployés de G, cf. [BT 65, 4.16]. L'assertion (b) provient de la minimalité de L, et (c) se déduit de (b) et de la prop. 3.2. Quant à (d), il résulte de la conjugaison des tores déployés maximaux de C_Γ, qui est valable quand k est parfait, d'après [BT 65, 11.6].

3.3. La propriété de « forte réductivité » de Richardson

On suppose maintenant que k est *algébriquement clos*, ce qui assure que tous les tores sont déployés. La prop. 3.4 (c) s'énonce alors de la façon suivante :

THÉORÈME 3.5 ([BMR 05]). — *Soit* T *un tore maximal du centralisateur de* Γ*, et soit* L *le centralisateur de* T*. Les deux propriétés suivantes sont équivalentes* :

(i) Γ *est* G-cr.

(ii) Γ *n'est contenu dans aucun sous-groupe parabolique propre de* L.

La propriété (ii) a été introduite en 1988 par RICHARDSON [Ri 88, § 16] sous le nom de « strong reductivity ». Ce n'est que tout récemment que BATE, MARTIN et RÖHRLE ont démontré qu'elle équivaut à la propriété (i). Ils en ont tiré de nombreuses conséquences, que l'on trouvera dans [BMR 05]. En voici quelques unes :

THÉORÈME 3.6 ([Ma 03b] et [BMR 05]). — *Soit* Γ' *un sous-groupe normal de* Γ*. Si* Γ *est* G-cr*, il en est de même de* Γ'*.*

(Comparer avec la prop. 2.11 du § 2.)

THÉORÈME 3.7 ([Ri 88] et [BMR 05]). — *Supposons que* Γ *soit engendré topologiquement par des éléments* $x_1, \ldots, x_m$*. Soit* $f : G \to G \times \cdots \times G$ (m *copies*) *l'application*

$$g \longmapsto (gx_1g^{-1}, ..., gx_mg^{-1}).$$

Pour que Γ *soit* G-cr*, il faut et il suffit que* $f(G)$ *soit une partie fermée de* $G \times \cdots \times G$*.*

Dans le cas particulier $m = 1$, on retrouve le fait qu'une classe de conjugaison est fermée si et seulement si ses éléments sont semi-simples.

THÉORÈME 3.8 ([BMR 05]). — *Soit* G' *un groupe réductif contenant* G*, et tel que* :

(a) *Le centralisateur* (schématique) *de* Γ *dans* G' *est lisse.*

(b) *Il existe un sous-espace vectoriel* m *de* Lie G'*, stable par conjugaison par* G *et tel que* Lie $G' = m \oplus$ Lie G.

Alors, si Γ *est* G'-cr*, il est* G-cr.

(Dans [BMR 05], la condition (a) est appelée « séparabilité » ; quant à (b), elle exprime que (G', G) est un « couple réductif » au sens de RICHARDSON.)

COROLLAIRE 3.9. — *Soit* V *un* G*-module fidèle. Supposons que la forme bilinéaire* $(x, y) \mapsto Tr(x_V.y_V)$ *sur* Lie G *soit non dégénérée. Alors, si* V *est* Γ*-semi-simple, le groupe* Γ *est* G-cr.

Cela résulte du th. 3.8, appliqué à $G' = \mathbf{GL}(V)$. La condition (a) est satisfaite. La condition (b) l'est aussi : on prend pour m l'orthogonal de Lie G dans Lie $\mathbf{GL}(V)$ pour la forme trace.

4. Critères de complète réductibilité

Dans ce qui suit, G est un groupe réductif sur un corps algébriquement clos k, et Γ est un sous-groupe de $G(k)$. À partir du n° 4.2, on suppose que la caractéristique p de k est > 0.

On se propose de donner des critères, aussi explicites que possible, permettant de reconnaître si Γ possède la propriété G-cr. Si $\bar{\Gamma}$ est l'adhérence de Γ pour la topologie de Zariski, il est clair que Γ est G-cr $\iff$ $\bar{\Gamma}$ est G-cr. Cela nous permettra souvent de supposer que Γ est fermé, i.e. que c'est un sous-groupe algébrique (lisse) de G.

[Il serait intéressant de considérer aussi le cas d'un sous-groupe algébrique *non nécessairement lisse*. Il n'y a pas de difficulté à étendre à de tels groupes la définition de « G-cr », non plus que celle du sous-complexe convexe « X^Γ ». Ce qui est moins clair, c'est ce qui doit remplacer la *saturation* du § 5. Une fois cet obstacle surmonté, on peut espérer que les résultats des n^{os} 5.2 et 5.3 s'étendent sans changement.]

4.1. Une première condition

Notons $R_u(\Gamma)$ le radical unipotent de Γ, i.e. son plus grand sous-groupe unipotent normal (connexe ou non). (Lorsque k est de caractéristique $p > 0$, et que Γ est fini, on a $R_u(\Gamma) = O_p(\Gamma)$, avec les notations usuelles de la théorie des groupes finis.)

PROPOSITION 4.1. — *Si* Γ *est* G-cr*, on a* $R_u(\Gamma) = 1$.

Quitte à remplacer G par un Levi de l'un de ses sous-groupes paraboliques, on peut supposer que Γ est G-ir (cf. prop. 3.3). Soit alors U l'adhérence de $R_u(\Gamma)$. D'après [BT 71, prop. 3.1], il existe un sous-groupe parabolique P de G, avec $U \subset R_u(P)$, qui est stable par tout automorphisme du couple (G, U). Comme Γ normalise U, il normalise P, donc est contenu dans P. Puisque Γ est G-ir, cela entraîne $P = G$, d'où $U = 1$ puisque $R_u(G) = 1$.

PROPOSITION 4.2. — *Supposons k de caractéristique* 0*, et supposons que* Γ *soit fermé. Les propriétés suivantes sont équivalentes* :

(i) Γ *est* G-cr.
(ii) $R_u(\Gamma) = 1$.
(iii) *La composante neutre* Γ^0 *de* Γ *est un groupe réductif.*

L'équivalence de (ii) et (iii) provient de ce que tout sous-groupe unipotent de Γ est contenu dans Γ^0. L'implication (i) $\Rightarrow$ (ii) est la prop. 4.1. L'implication (iii) $\Rightarrow$ (i) provient du fait bien connu suivant (spécial à la caractéristique 0) : toute extension de Γ par un groupe unipotent est scindée, et deux scindages quelconques sont conjugués (on se ramène, par dévissage à une annulation de groupes de cohomologie, cf. [Mo 56] et [DG 70, p. 393]).

COROLLAIRE 4.3. — *Supposons k de caractéristique* 0*. Soit* $f : G \to G'$ *un homomorphisme de* G *dans un groupe réductif* G'*. Si* Γ *est* G-cr*, alors* $f(\Gamma)$ *est* G'-cr ; *la réciproque est vraie si f est presque fidèle.*

(Un homomorphisme f est dit *presque fidèle* si $\mathrm{Ker}(f)$ est un groupe de type multiplicatif.)

C'est clair, grâce à (iii).

Remarques. — 1) Le cor. 4.3 redonne le théorème de Chevalley cité au n° 1.1 : il suffit de l'appliquer à l'homomorphisme naturel $f : \mathbf{GL}(V) \times \mathbf{GL}(V') \to \mathbf{GL}(V \otimes V')$.

2) La prop. 4.2 montre que la propriété « G-cr » n'a pas grand intérêt en caractéristique 0. C'est pour cela que, à partir de maintenant, *on supposera que le corps k est de caractéristique* $p > 0$. On donnera alors des conditions sur p (du genre « p est assez grand ») permettant d'avoir des résultats analogues à ceux de la caractéristique 0, cf. th. 4.4, th. 4.5 et th. 5.3.

4.2. Le cas où Γ est connexe

Définissons un entier $a(G)$ par la recette suivante :

(1) Si G est simple :
$$a(G) = 1 + \mathrm{rang}(G).$$

(2) Si $\{G_1, \dots, G_r\}$ sont les quotients simples de G, on pose :
$a(G) = \sup(1, a(G_1), \dots, a(G_r))$.

THÉORÈME 4.4. — (JANTZEN, MCNINCH, LIEBECK-SEITZ). — *Supposons que* $p \geqslant a(G)$, *que* Γ *soit un sous-groupe fermé de* G, *et que* $(\Gamma : \Gamma^0)$ *soit premier à* p. *Il y a alors équivalence entre* :

(i) Γ *est* G-cr.
(ii) Γ^0 *est réductif.*

L'implication (i) $\Rightarrow$ (ii) a été démontrée plus haut. Supposons que la condition (ii) soit satisfaite. En utilisant le fait que $(\Gamma : \Gamma^0)$ est premier à p, on démontre facilement que Γ^0 est G-cr $\Rightarrow$ Γ est G-cr. On peut donc supposer que Γ est connexe, autrement dit que c'est un sous-groupe réductif de G ; on peut aussi supposer que G est quasi-simple. Le cas où G est de type exceptionnel est traité dans [LS 96] (sauf pour $p = 3$ et G de type G_2, mais ce cas n'offre pas de difficultés). Lorsque G est de type A_n, le théorème signifie que toute représentation linéaire de degré $\leqslant p$ d'un groupe réductif est semi-simple, ce qui a été démontré par JANTZEN [Ja 97]. De même, si G est de type B_n, C_n ou D_n, on est ramené à montrer que toute représentation self-duale d'un groupe réductif est semi-simple si sa dimension est $< 2p$; cela a été démontré récemment par MCNINCH (non publié : le cas crucial est celui où le groupe réductif est de type A_1 – les autres cas se déduisent de [Mc 98]).

Remarque. — La borne $p \geqslant a(G)$ du th. 4.4 est essentiellement optimale lorsque le groupe Γ^0 est de rang 1. Elle peut par contre être améliorée lorsque les facteurs simples de Γ^0 sont de rang > 1, cf. [LS 96] et [Mc 98].

4.3. Le cas non connexe

On se borne au cas où $G^{ad} = G/C_G$ est un groupe simple. On remplace l'entier $a(G)$ du n° 4.2 par un entier $b(G)$ un peu plus grand :

$b(G) = 2, 3, 5$ si G^{ad} est de type A_1, A_2, B_2 ;
$b(G) = n + 3$ si G^{ad} est de type A_n $(n \geqslant 3)$;
$b(G) = 2n + 3$ si G^{ad} est de type B_n, C_n $(n \geqslant 3)$ ou D_n $(n \geqslant 4)$;
$b(G) = 11, 29, 29, 59, 251$ si G^{ad} est de type G_2, F_4, E_6, E_7, E_8.

THÉORÈME 4.5. — *Supposons que* Γ *soit un sous-groupe fermé de* $G(k)$, *avec* G^{ad} *simple, et* $p \geqslant b(G)$. *Il y a équivalence entre* :

(i) Γ *est* G-cr.
(ii) $R_u(\Gamma) = 1$.

(Autrement dit, on a le même énoncé que 4.2, pourvu que $p \geqslant b(G)$.)

Ici encore, il suffit de montrer que (ii) $\Rightarrow$ (i). Le cas essentiel est celui où $G = \mathbf{GL}_n$; il est dû à GURALNICK, cf. [Gu 99, th. C]. (La démonstration est loin d'être élémentaire : elle utilise non seulement la classification des groupes finis simples, mais aussi la liste des caractères modulaires irréductibles des groupes sporadiques donnée dans [JLPW 95].) Les autres cas s'en déduisent en appliquant le th. 5.4 ci-dessous à des représentations linéaires de G de basse dimension.

Remarques. 1) Voici quelques exemples de couples (Γ, G) montrant que, *pour les groupes classiques*, la condition $p \geqslant b(G)$ du th. 4.5 ne peut guère être améliorée :

Type A : $\Gamma = S_p$; $G = \mathbf{SL}_{p-1}$

Types B, C, D : $\Gamma = \mathbf{SL}_2(\mathbf{F}_p)$ ou $\mathbf{PSL}_2(\mathbf{F}_p)$; $G = \mathbf{SO}_{p+2}, \mathbf{Sp}_{p-1}, \mathbf{SO}_{p+1}$.

Supposons $p > 3$. Dans chaque cas, on a $R_u(\Gamma) = 1$, et l'on peut construire un plongement de Γ dans $G(k)$ qui donne une représentation linéaire non semi-simple, ce qui signifie que Γ n'est pas G-cr, d'après 3.2.2. On a $p = b(G) - 2, b(G) - 4, b(G) - 4, b(G) - 2$ respectivement.

2) La situation est différente *pour les groupes exceptionnels*; la borne $p \geqslant b(G)$ peut être grandement améliorée, par exemple en utilisant les méthodes de [LS 96]. Ainsi, pour le type G_2, on peut remplacer « $p \geqslant 11$ » par « $p \geqslant 5$ », qui est optimal. J'ignore quelles sont les bornes optimales pour les types F_4, E_6, E_7 et E_8.

5. Saturation et représentations linéaires

5.1. Exponentielle et saturation

On note $h(G)$ la borne supérieure des nombres de Coxeter des quotients simples de G. (S'il n'y en a aucun, i.e. si G est un tore, on convient que $h(G) = 1$.) Rappelons que, si G est simple, on a $h(G) = \dim(G)/\mathrm{rang}(G) - 1$; les valeurs de h pour les différents types sont :

$A_n : h = n + 1$; $B_n, C_n : h = 2n$; $D_n : h = 2n - 2$; $G_2 : h = 6$; $F_4, E_6 : h = 12$; $E_7 : h = 18$; $E_8 : h = 30$.

Supposons maintenant que $p \geqslant h(G)$. Soit u un élément unipotent de G. D'après [Te 95], on a $u^p = 1$. De plus, si t est un élément de k, on peut définir *de façon canonique* (c'est là un point essentiel) la « t-ième puissance » u^t de u, cf. [Se 98] (voir aussi [S 00] qui traite un cas plus général). L'application $t \mapsto u^t$ est un homomorphisme du groupe additif $\mathbf{G}_a$ dans le groupe G. Lorsque $G = \mathbf{GL}_n$, l'hypothèse $p \geqslant h(G)$ signifie que $p \geqslant n$, de sorte que $u = 1 + v$ avec $v^p = 0$, et u^t est donné par le développement binomial : $(1+v)^t = 1 + t \cdot v + \cdots$.

[L'hypothèse « k algébriquement clos » faite au début du § 4 n'intervient pas dans la définition de l'exponentielle u^t. En fait, le cas crucial est celui d'un schéma en groupes semi-simples, déployé et simplement connexe, sur le localisé $\mathbf{Z}_{(p)}$ de $\mathbf{Z}$ en p. Les autres cas s'en déduisent par descente, en utilisant les méthodes de [DG 70], cf. [S 00, § 5].]

DÉFINITION 5.1. — *Un sous-groupe* Γ *de* $\mathrm{G}(k)$ *est dit saturé s'il est fermé et si l'on a* $u^t \in \Gamma$ *pour tout élément unipotent* u *de* Γ*, et tout* $t \in k$*.*

[Par exemple, tout sous-groupe parabolique est saturé ; tout centralisateur d'un sous-groupe est saturé.]

On démontre facilement :

PROPOSITION 5.2. — *Si* Γ *est saturé, l'indice de* Γ^0 *dans* Γ *est premier à* p*.*

Pour tout sous-groupe Γ de $\mathrm{G}(k)$, il existe un plus petit sous-groupe saturé le contenant ; on l'appelle le *saturé* de Γ et on le note Γ^{sat}. (Lorsque $\mathrm{G} = \mathbf{GL}_n$, on retrouve la notion utilisée dans [No 87] et [Se 94].)

THÉORÈME 5.3 ([Se 98, th. 8]). — *Il y a équivalence entre* :
(i) Γ *est* G-cr.
(ii) Γ^{sat} *est* G-cr.
(iii) *La composante neutre de* Γ^{sat} *est un groupe réductif.*
(Rappelons que l'on suppose $p \geqslant h(\mathrm{G})$.)

L'équivalence (i) $\Leftrightarrow$ (ii) est claire : les sous-groupes paraboliques et leurs sous-groupes de Levi sont saturés. L'équivalence de (ii) et (iii) résulte du th. 4.4 et de la prop. 5.2 ; noter que le th. 4.4 est applicable car $a(\mathrm{G}) \leqslant h(\mathrm{G})$.

5.2. Représentations linéaires : l'invariant $n(\mathrm{V})$

Choisissons un tore maximal T de G, ainsi qu'un sous-groupe de Borel B de G contenant T. Soit $\mathrm{X}(\mathrm{T}) = \mathrm{Hom}(\mathrm{T}, \mathbf{G}_m)$ le groupe des caractères de G, et soit $\mathrm{Y}(\mathrm{T}) = \mathrm{Hom}(\mathbf{G}_m, \mathrm{T})$ son dual. Notons $\mathrm{R} \subset \mathrm{X}(\mathrm{T})$ le système de racines de (G, T). Si $a \in \mathrm{R}$, notons a^* la racine duale ; c'est un élément de $\mathrm{Y}(\mathrm{T})$.

Pour tout $\chi \in \mathrm{X}(\mathrm{T})$, on pose

$$n(\chi) = \sum \langle \chi, a^* \rangle ,$$

où a parcourt les éléments > 0 de R (pour la relation d'ordre associée à B).

Si V est un G-module, on définit un *invariant* $n(\mathrm{V})$ de V par la formule :

$n(\mathrm{V}) = \sup n(\chi)$, où χ parcourt l'ensemble des poids de T dans V,

cf. [Dy 52, n° 12]. C'est un entier $\geqslant 0$. Voici quelques unes de ses propriétés (on en trouvera d'autres dans [Dy 52], [Se 98] et [IMP 03]) :

(5.2.1) Si V a une suite de composition dont les facteurs successifs sont $V_1, \ldots, V_r$, on a $n(V) = \sup n(V_i)$.

(5.2.2) Si V est irréductible de plus grand poids λ, on a $n(V) = n(\lambda)$.

(5.2.3) On a $n(V) = 0$ si et seulement si le groupe dérivé de G opère trivialement sur V, i.e. si l'image de $G \to \mathbf{GL}(V)$ est un tore.

(5.2.4) Si V est presque fidèle (au sens du cor. 4.3), on a $n(V) \geqslant h(G) - 1$.

(5.2.5) Si $V = V_1 \otimes V_2$, on a $n(V) = n(V_1) + n(V_2)$.

(5.2.6) On a $n(\text{Lie } G) = 2h(G) - 2$.

Remarque. — L'invariant $n(V)$ « se calcule sur $\mathbf{SL}_2$ » au sens suivant :

Soit $f : \mathbf{SL}_2 \to G$ un homomorphisme tel que le composé $\mathbf{G}_m \to \mathbf{SL}_2 \to G$ soit à valeurs dans T, et soit égal dans Y(T) à la somme $\sum a^*$, où a parcourt les racines > 0. Un tel f existe : cela se démontre par réduction à partir de la caractéristique 0. Grâce à f, le G-module V peut être vu comme un $\mathbf{SL}_2$-module, et son invariant $n(V)$ comme G-module est le même que son invariant $n(V)$ comme $\mathbf{SL}_2$-module. [Autre interprétation de $n(V)$: à un facteur 2 près, c'est le degré en la variable « q » de la *dimension quantique* de V.]

L'intérêt de l'invariant $n(V)$ provient du théorème suivant, qui relie la semi-simplicité du Γ-module V à la propriété « G-cr » :

THÉORÈME 5.4. — *Supposons $p > n(V)$. Soit Γ un sous-groupe de $G(k)$.*

(i) *Si Γ est* G-cr*, alors* V *est Γ-semi-simple* (i.e. semi-simple comme Γ-module)*.*

(ii) *Inversement, si* V *est Γ-semi-simple, et si* V *est presque fidèle, alors Γ est* G-cr*.*

(Si l'on regarde V comme un $\mathbf{SL}_2$-module – cf. *Remarque* ci-dessus – l'hypothèse $p > n(V)$ signifie que V est un $\mathbf{SL}_2$-module *restreint* (« restricted ») : ses poids sont $< p$.)

On peut supposer que V est presque fidèle. D'après (5.2.4), on a alors $p \geqslant h(G)$, ce qui permet d'utiliser le th. 5.3. Les détails de la démonstration se trouvent dans [Se 98] (voir aussi [IMP 03]).

COROLLAIRE 5.5. — *Supposons $p > 2h(G) - 2$. Les deux propriétés suivantes sont équivalentes* :

(cr) Γ *est* G-cr*.*

(ad) *L'algèbre de Lie* Lie G *de* G *est un Γ-module semi-simple.*

Cela résulte du th. 5.4 et de la formule (5.2.6).

Remarque 5.6. —La condition $p > 2h(G) - 2$ est presque optimale pour l'implication (cr) $\Rightarrow$ (ad). En effet, supposons que cette condition ne soit pas

satisfaite, et que G soit simple ; on peut alors construire (à deux exceptions près, cf. ci-après) un sous-groupe Γ de G, isomorphe à $\mathbf{SL}_2$ ou $\mathbf{PGL}_2$, qui satisfait à (cr) mais pas à (ad). (Les deux exceptions sont : $p = 3$, G de type B_2, et $p = 5$, G de type G_2.)

Par contre, l'implication (ad) $\Rightarrow$ (cr) est en général valable sous des conditions bien moins restrictives que $p > 2h(G) - 2$. Par exemple, si G est de type E_8, le cor. 3.9 montre que la condition $p > 2h(G) - 2 = 58$ peut être remplacée par $p > 5$.

5.3. Applications

Le th. 5.4 peut être utilisé pour prouver des énoncés où la notion de « G-cr » n'intervient pas explicitement. Par exemple :

PROPOSITION 5.7. — *Soit* $\Gamma \subset G(k)$, *où* G *est de type* E_8. *Soient* $V_1, \ldots, V_8$ *les huit représentations irréductibles fondamentales de* G. *Supposons que l'un des* Γ*-modules* V_i *soit semi-simple. Alors tous les autres le sont pourvu que* $p > 270$.

(J'ignore si la minoration $p > 270$ est optimale.)

Soit (α_i) une base du système de racines et soit $\sum c_i \alpha_i^*$ la somme des duales des racines positives. Il résulte de (5.2.2) que l'on a $n(V_i) = c_i$ pour tout i. Dans le cas de E_8, cela donne :

$n(V_i) = 92, 136, 182, 270, 220, 168, 114, 58$ pour $i = 1, \ldots, 8$.

D'où le résultat, d'après le th. 5.4.

Voici deux autres applications. La première est l'analogue en caractéristique p du théorème de Chevalley cité au n° 1.1 :

PROPOSITION 5.8 ([Se 94]). — *Soient* V_i *des représentations linéaires semi-simples d'un groupe* Γ. *Si* $p > \sum(\dim(V_i) - 1)$, *la représentation* $\bigotimes V_i$ *est* Γ*-semi-simple.*

On applique le th. 5.4 à $G = \prod \mathbf{GL}(V_i)$. L'hypothèse que les V_i sont semi-simples signifie que l'image de Γ dans G est G-cr. D'autre part, il résulte de (5.2.5) que l'invariant $n(V)$ de la G-représentation $\bigotimes V_i$ est égal à $\sum(\dim(V_i) - 1)$. D'où le résultat.

Autre énoncé du même goût :

PROPOSITION 5.9 ([Se 98] et [Mc 00]). — *Si* V *est une représentation linéaire semi-simple d'un groupe* Γ, *il en est de même de* $\wedge^i V$, *si* $p > i(\dim(V) - i)$.

On applique le th. 5.4 à $G = \mathbf{GL}(V)$. On peut supposer que $0 \leqslant i \leqslant \dim(V)$. On a alors $n(\wedge^i V) = i(\dim(V) - i)$. D'où le résultat.

Remarque. — Dans les deux cas ci-dessus, on peut se proposer de prouver des réciproques. Par exemple, si $\wedge^i V$ est semi-simple, est-il vrai (si $0 < i < \dim(V)$ et si p est assez grand) que V est semi-simple ? Le th. 5.4 dit que « oui » si $p > i(n-i)$ où $n = \dim(V)$. En fait, un argument tannakien élémentaire ([Se 97a]) donne un résultat nettement meilleur : il suffit que p ne divise aucun des entiers $n-2, n-3, \ldots, n-i$.

Références

[AS 86] M. Aschbacher – *Chevalley groups of type* G_2 *as the group of a trilinear form*, J. Algebra **109** (1986), 193-259.

[BMR 05] M. Bate, B.M.S. Martin et G. Röhrle – *A geometric approach to complete reducibility*, Invent. math. **161** (2005), 177-218.

[BT 65] A. Borel et J. Tits – *Groupes réductifs*, Publ. Math. IHES **27** (1965), 55-150.

[BT 71] A. Borel et J. Tits – *Éléments unipotents et sous-groupes paraboliques de groupes réductifs* I, Invent. math. **12** (1971), 95-104.

[Br 89] K. Brown – *Buildings*, Springer-Verlag, 1989.

[Ch 55] C. Chevalley – *Théorie des Groupes de Lie*, vol. III, Hermann, Paris, 1955.

[DG 70] M. Demazure et A. Grothendieck – *Structure des schémas en groupes réductifs* (SGA 3 III), Lect. Notes **153**, Springer-Verlag, 1970.

[Dy 52] E.B. Dynkin – *Sous-groupes maximaux des groupes classiques* (en russe), Trudy Mosc. Mat. Obsh. **1** (1952), 39-116 ; trad. anglaise : *Selected Papers*, A.M.S., 2000, 37-170.

[Gu 99] R.M. Guralnick – *Small representations are completely reducible*, J. Algebra **220** (1999), 531-541.

[IMP 03] S. Ilangovan, V.B. Metha et A.J. Parameswaran – *Semistability and semisimplicity in representations of low height in positive characteristic*, in *A Tribute to C.S. Seshadri*, edited by V. Lakshmibai et al, Hindustani Book Ag., New Delhi, 2003.

[JLPW 95] C. Jansen, K. Lux, R. Parker et R. Wilson – *An atlas of Brauer characters*, LMS Monographs, Clarendon Press, Oxford, 1995.

[Ja 97] J.C. Jantzen – *Low dimensional representations of reductive groups are semisimple*, in *Algebraic Groups and Lie Groups*, Cambridge U. Press, Cambridge, 1997, 255-266.

[Ke 78] G.R. KEMPF – *Instability in invariant theory*, Ann. Math. **108** (1978), 299-316.

[LS 96] M.W. LIEBECK et G.M. SEITZ – *Reductive Subgroups of Exceptional Algebraic Groups*, Memoirs A.M.S. **580**, 1996.

[Ma 03a] B.M.S. MARTIN – *Reductive subgroups of reductive groups in nonzero characteristic*, J. Algebra **262** (2003), 265-286.

[Ma 03b] B.M.S. MARTIN – *A normal subgroup of a strongly reductive subgroup is strongly reductive*, J. Algebra **265** (2003), 669-674.

[Mc 98] G.J. MCNINCH – *Dimensional criteria for semisimplicity of representations*, Proc. London Math. Soc. **76** (1998), 95-149.

[Mc 00] G.J. MCNINCH – *Semisimplicity of exterior powers of semisimple representations of groups*, J. Algebra **225** (2000), 646-666.

[Mo 56] G.D. MOSTOW – *Fully reducible subgroups of algebraic groups*, Amer. J. Math. **78** (1956), 200-221.

[Mu 65] D.MUMFORD – *Geometric Invariant Theory*, Springer-Verlag, 1965 ; third enlarged edit. (D. Mumford, J. Fogarty, F. Kirwan), 1994.

[Mü 97] B. MÜHLHERR – *Complete reducibility in projective spaces and polar spaces*, preprint, Dortmund, 1997.

[No 87] M.V. NORI – *On subgroups of* $\mathbf{GL}(n, \mathbf{F}_p)$, Invent. math. **88** (1987), 257-275.

[Ri 88] R.W. RICHARDSON – *Conjugacy classes of n-tuples in Lie algebras and algebraic groups*, Duke Math. J. **57** (1988), 1-35.

[Ron 89] M. RONAN – *Lectures on Buildings*, Acad. Press, San Diego, 1989.

[Rou 78] G. ROUSSEAU – *Immeubles sphériques et théorie des invariants*, C.R.A.S. **286** (1978), 247-250.

[S 00] G.M. SEITZ – *Unipotent elements, tilting modules, and saturation*, Invent. math. **141** (2000), 467-502.

[Se 94] J-P. SERRE – *Sur la semi-simplicité des produits tensoriels de représentations de groupes*, Invent. math. **116** (1994), volume dédié à Armand Borel, 513-530.

[Se 97a] J-P. SERRE – *Semisimplicity and tensor products of group representations*: *converse theorems* (with an Appendix by Walter Feit), J. Algebra **194** (1997), 496-520.

[Se 97b] J-P. SERRE – *La notion de complète réductibilité dans les immeubles sphériques et les groupes réductifs*, Séminaire au Collège de France, résumé dans [Ti 97, pp. 93-98].

[Se 98] J-P. SERRE – *The notion of complete reducibility in group theory*, Moursund Lectures Part II, Eugene 1998 (Notes by W.E. Duckworth), `http://darkwing.uoregon.edu/~math/serre/index.html`

[So 69] L. SOLOMON – *The Steinberg character of a finite group with BN-pair*, Theory of Finite Groups, Benjamin, 1969, 213-221.

[Te 95] D.M. TESTERMAN – A_1*-type overgroups of elements of order p in semi-simple algebraic groups and the associated finite groups*, J. Algebra **177** (1995), 34-76.

[Ti 74] J. TITS – *Buildings of spherical type and finite BN-pairs*, LN **386**, Springer-Verlag, 1974.

[Ti 97] J. TITS – *Résumé des cours de 1996-1997*, Annuaire du Collège de France **97** (1997), 89-102.

[TW 02] J. TITS et R.M. WEISS – *Moufang Polygons*, Springer-Verlag, 2002.

NOTES

Séminaire Bourbaki 1949-50, exposé 27

1. Cet « exposé ultérieur » a été fait par A. BOREL (Sém. Bourbaki 1949-50, exposé n° 29).

2. Dans le présent exposé « extension du groupe F par le groupe B » signifie (comme chez IWASAWA [**2**]) que F est un sous-groupe normal, et que B est le quotient. Ce n'est pas la convention choisie par BOURBAKI, et utilisée dans les exposés suivants; lorsqu'il s'agit (par exemple) de modules, on préfère qu'une « extension de A par B » corresponde à un élément de $\mathrm{Ext}(A, B)$ et non à un élément de $\mathrm{Ext}(B, A)$.

3. « représentation » = homomorphisme.

4. « noyau de groupe » = group chunk (en anglais) = morceau de groupe (en géométrie algébrique) = groupuscule (Bourbaki LIE III.1.10).

5. Il vaut mieux supposer aussi que le graphe de la relation d'équivalence définie par F est fermé dans $E \times E$, cf. Sém. Cartan 1949-1950, exposé 6, n° 4. Dire que E est un F-espace fibré principal revient alors à dire que F opère *librement* et *proprement* sur E (Bourbaki, TG III, § 4, prop. 6).

6. « ... du F-fibré G ». Ceci n'est correct que si F se plonge comme sous-groupe fermé dans le groupe linéaire G. Cette condition est satisfaite si F est *compact*, ce qui est le cas considéré par Gleason (Proc. A.M.S. **1** (1950), 35–43). Dans le cas général, il faut raisonner de façon purement locale, comme indiqué dans la Remarque.

Pour une autre démonstration (et une généralisation) du théorème de Gleason, voir : R.S. PALAIS, *On the existence of slices for actions of non-compact Lie groups*, Ann. of Math. **73** (1961), 295–323, § 4.1.

7. Le « calcul immédiat » est le suivant. On écrit le membre de gauche comme

$$\int \big[u(x,y) - x{\cdot}u(y,t) + u(xy,t) - u(x,t)\big]k(t)\,dt\ ;$$

en utilisant le fait que u est un cocycle, ceci se récrit :

$$\int \big[u(x,yt) - u(x,t)\big]k(t)\,dt\ .$$

8. On peut aussi procéder de la façon suivante : si les s_i sont des sections continues au-dessus d'ouverts U_i recouvrant la base, on choisit une partition de l'unité (f_i) subordonnée aux (U_i) et l'on définit une section globale s par la formule $s = \sum f_i s_i$.

9. Il s'agit, bien sûr, des groupes de cohomologie H^q, avec $q > 0$.

10. Référence : C. Chevalley, *On the topological structure of solvable groups*, Ann. of Math. **42** (1941), 668–675.

Séminaire Cartan 1950-51, exposé 5

1. Il n'est pas indispensable d'utiliser des cochaînes normalisées, mais c'est parfois commode [par exemple pour que l'élément neutre de l'extension soit représenté par le couple (0,1)].

Séminaire Cartan 1950-51, exposés 6 et 7

1. Les références sont relatives à la première édition du livre d'Algèbre de Bourbaki.

2. Soit V un espace vectoriel de base $(e_i)_{i\in \mathrm{I}}$; si $x = \sum \lambda_i e_i$ est un élément de V, notons $\mathrm{S}(x)$ l'ensemble des indices i tels que $\lambda_i \neq 0$. Soit W un sous-espace vectoriel de V. Un élément $x \neq 0$ de W est dit *primordial* si $\mathrm{S}(x)$ est un élément *minimal* de l'ensemble des $\mathrm{S}(y)$, avec $y \in \mathrm{W} - \{0\}$. Les éléments primordiaux de W engendrent W.

(Cette notion figurait dans la première édition de Bourbaki, Alg. II; elle a disparu des éditions suivantes.)

3. Le groupe $\mathrm{Br}_{\mathbf{Q}}$ est le sous-groupe de $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Q}/\mathbf{Z} \oplus \mathbf{Q}/\mathbf{Z} \oplus \cdots$ formé des éléments dont la somme dans $\mathbf{Q}/\mathbf{Z}$ est nulle (ce qui a un sens si l'on identifie $\mathbf{Z}/2\mathbf{Z}$ à un sous-groupe de $\mathbf{Q}/\mathbf{Z}$).

4. Il me paraît plus simple de définir l'algèbre A par le procédé suggéré à la page suivante :

Pour tout $g \in \mathrm{G}$, l'image réciproque I_g de g dans l'extension E est un L^*-torseur à gauche. En lui adjoignant un élément 0 on en déduit un L-espace vectoriel N_g de dimension 1. On définit alors A comme la somme directe des N_g, pour $g \in \mathrm{G}$. Le produit $\mathrm{I}_g \times \mathrm{I}_{g'} \to \mathrm{I}_{gg'}$ se prolonge en $\mathrm{N}_g \times \mathrm{N}_{g'} \to \mathrm{N}_{gg'}$. D'où la structure d'algèbre de A.

5. On utilise le fait élémentaire suivant : avec les notations de la note **2** ci-dessus, si x est un élément primordial de W, et si y est un élément de W tel que $\mathrm{S}(y) \subset \mathrm{S}(x)$, alors y est un multiple scalaire de x.

Séminaire Cartan 1953-54, exposés IV et V

1. Pour un exposé « faisceautique » du théorème de Riemann-Roch (dans le cas des courbes algébriques), voir *Un théorème de dualité*, Comm. Math. Helv. **29** (1955), 1-26.

2. La définition de $\mathrm{F}(x)$ donnée dans le texte a un sens si x n'appartient pas au support de D, car alors les $f_i(x)$ sont $\neq \infty$, et ne sont pas tous nuls. Lorsque x appartient au support de D, il convient de remplacer les $f_i(x)$ par $t^n f_i(x)$, où t est une uniformisante locale en x et $n = \mathrm{o}_x(\mathrm{D})$.

3. Le « poids » dont il s'agit ici est l'exposant du jacobien; c'est la moitié du poids modulaire usuel.

4. D'après un théorème de Siegel (Ann. of Math. **46** (1945), 708–718), les deux propriétés suivantes sont équivalentes :

(i) $\widehat{\mathrm{X}}$ est compact;

(ii) l'aire de $\mathrm{X} = \mathrm{Y}/\mathrm{G}$ est finie.

5. Si l'on fait une représentation conforme $z \mapsto \zeta = i\frac{\mathrm{Q}+z}{\mathrm{Q}-z}$, le disque Y devient le demi-plan supérieur $\mathrm{Im}(\zeta) > 0$ et son bord $|z| = 1$ devient la droite projective $\overline{\mathbf{R}} = \mathbf{R} \cup \{\infty\}$, avec $\mathrm{Q} \mapsto \infty$. Le groupe G_{Q} est engendré par une transformation

de la forme $\zeta \mapsto \zeta + \lambda$, avec λ réel > 0. Cela se traduit par $z \mapsto z'$, avec

$$1/(z' - \mathrm{Q}) = 1/(z - \mathrm{Q}) + h, \quad \text{où} \quad h = i\lambda\overline{\mathrm{Q}}/2\,,$$

d'où le fait que $h/i\overline{\mathrm{Q}}$ est un nombre réel > 0, ce qui précise le « choix convenable » du texte.

6. Ici encore, $2\pi\mathrm{A}$ est l'aire de $\mathrm{X} = \mathrm{Y}/\mathrm{G}$.

7. On peut ajouter à la Bibliographie les deux ouvrages suivants :
G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Princeton Univ. Press, 1971.
C.L. Siegel. *Topics in Complex Function Theory*, vol. II : *Automorphic functions and abelian integrals*, Intersc. Tracts, Wiley-Interscience, 1971.

Séminaire Cartan 1953-54, exposé XVI

1. Les références sont relatives à la première édition du livre des EVT.

2. Au lieu de « homomorphisme », on dit maintenant « morphisme strict ».

3. Cela peut se voir en appliquant le th. 1 de Bourbaki, TG I.75, qui montre que l'application w est *propre*.

4. Pour un énoncé général, voir Bourbaki, TG IX.22, prop. 18.

Séminaire Cartan 1953-54, exposés XVIII et XIX

1. Voir là-dessus *Un théorème de dualité*, § 2.

2. « est isomorphe » : il serait plus correct de dire « est anti-isomorphe ».

3. Oui, ce résultat s'étend à toute variété analytique complexe. Cela peut se déduire d'un théorème de Lojasiewicz et Malgrange (cf. Sém. Bourbaki 1959-60, exposé n°203, cor. au th. 4).

4. Dans cet exposé, ainsi que dans les suivants, un homomorphisme de faisceaux analytiques est dit *analytique* s'il est $\mathscr{O}$-linéaire.

5. Le lemme en question est le célèbre « lemme de Nakayama ».

6. « ... on obtient ainsi toutes les sections de $\mathscr{O}(n)$ ». C'est vrai si $n \geqslant 0$ ou si $r > 0$; c'est faux si $n < 0$ et $r = 0$ (i.e. X réduit à un point).

Séminaire Cartan 1953-54, exposé XX

1. Les hypothèses (i) et (ii) signifient que le groupe G opère *proprement* sur l'espace X, au sens de BOURBAKI, TG III.32.

2. « forme automorphe de poids n, au sens usuel » : il s'agit plutôt du poids $2n$.

3. Voir FAC, Chap. III, § 2, pour cette correspondance entre faisceaux cohérents et modules gradués.

4. HIRZEBRUCH venait d'annoncer sa démonstration du théorème de Riemann-Roch pour les variétés projectives non singulières (Proc. Nat. Acad. Sci. USA **40** (1954), 110-114).

Séminaire Bourbaki 1953-54, exposé 100

1. Je m'étais basé sur deux textes que BOREL m'avait envoyés. L'un d'eux a été incorporé à ses *Œuvres* (vol. I, n° 30); l'autre (celui relatif au § 2) est resté inédit.

2. Le terme de « variété symplectique » a maintenant un sens différent.

3. Pour les relations entre groupes complexes et groupes compacts, voir C. CHEVALLEY, *Theory of Lie Groups*, Princeton Univ. Press (1946), Chap. VI, ainsi que le § 5 de *Gèbres*, L'Ens. Math. **39** (1993), 33–85.

4. Pour la classification de ces structures complexes, voir BOREL-HIRZEBRUCH, Amer. J. of Math. **80** (1958), 458–538, prop. 13.4.

5. Parler du « poids dominant » d'une représentation peut prêter à confusion. Il vaut mieux dire « plus grand poids », cf. BOURBAKI LIE VII, § 7.

6. « ample » → « très ample ».

Séminaire Cartan 1954-55, exposé 20

1. Les « produits basiques » correspondent aux éléments d'un *ensemble de Hall*, au sens de BOURBAKI, LIE II, § 2, n° 10.

2. Voir E. WITT, *Treue Darstellung Liescher Ringe*, J. Crelle **177** (1937), 152–160 (=*Ges. Abh.* n° 25).

Séminaire Chevalley 1958, exposé 1

1. Pour la théorie des revêtements dans le cadre des schémas, voir GROTHENDIECK, SGA 1 (Lect. Notes in Math. **224**). La terminologie de GROTHENDIECK est quelque peu différente de celle utilisée ici : « non ramifié » est remplacé par « étale ».

2. Oui, on peut définir un schéma quotient ayant des propriétés raisonnables, cf. SGA 3 (Lect. Notes in Math. **151**), exposés V et VI_{A}.

3. « dépourvu d'éléments nilpotents » signifie « réduit », i.e. sans élément nilpotent $\neq 0$.

4. Voir SGA 1, exposé 1.

5. Voir SGA 1, *loc. cit.*, prop. 9.2.

6. Ce « résultat bien connu » est parfois appelé « lemme de Shapiro ».

7. « revêtement galoisien » : il vaudrait mieux dire « $\mathfrak{g}$-revêtement », car l'adjectif « galoisien » laisse penser que $\mathfrak{g}$ est le groupe des automorphismes du revêtement, ce qui n'est pas vrai en général (sauf si Y est connexe).

8. La définition des espaces fibrés principaux (ou *torseurs*) donnée ici a été réinterprétée l'année suivante par GROTHENDIECK (Sém. Bourbaki 1959-60, exposé n°190, § 6) comme la locale trivialité par rapport à une « topologie » qu'il a appelée plus tard la topologie « étale finie », cf. SGA 3, exposé IV, § 6.3. En fait GROTHENDIECK a montré que les topologies les plus commodes sont la topologie *étale* et la topologie *fidèlement plate de présentation finie* (f.p.p.f.); ce sont elles qui sont maintenant les plus utilisées, cf. par exemple, J.S. MILNE, *Étale Cohomology*, Princeton Univ. Press, 1980, Chap. IV, § 4.

Lorsque le groupe structural est un groupe linéaire lisse, les différentes topologies mentionnées ci-dessus conduisent à la même notion de torseur (GROTHENDIECK, *loc. cit.*, p. 190–27); il n'en est pas de même lorsque le groupe structural est une variété abélienne : il peut exister des torseurs pour la topologie étale qui ne sont pas localement isotriviaux, cf. note **13** ci-après.

9. Voir là-dessus le texte de GROTHENDIECK cité dans la note précédente.

10. Il faut être un peu plus soigneux. On choisit d'abord U assez petit pour que $\mathrm{U}' \to \mathrm{U}$ soit entier, puis on le rétrécit grâce à 1.2 pour que $\mathrm{U}' \to \mathrm{U}$ soit non ramifié.

11. Ici encore, on aura intérêt à se reporter à GROTHENDIECK, *loc. cit.*

12. « la vraie cohomologie ». Dès la fin de l'exposé oral, GROTHENDIECK m'a dit : cela va donner la cohomologie de Weil en toute dimension! J'avais trouvé cela très optimiste. Bien sûr, la topologie de Zariski donne un π_1 et un H^1 trop petits, et j'avais remédié à ce défaut. Mais était-ce suffisant? Mes réflexes de topologue me disaient qu'il fallait aussi s'occuper des groupes d'homotopie supérieurs : π_2, π_3, etc. La suite a montré que GROTHENDIECK avait raison (à un détail technique près : le remplacement de « isotrivial » par « étale », cf. note **8** ci-dessus).

13. « ... deux droites ayant un point en commun » : non, il faut utiliser deux droites ayant 2 points en commun.

Une autre possibilité (RAYNAUD, Lect. Notes in Math. **119**, p. 199, exemple III.3.1 — je dois cette référence à J-L. COLLIOT-THÉLÈNE) consiste à prendre pour base une cubique ayant un point double ordinaire (i.e. une droite projective dont on a identifié deux points distincts). Si l'on choisit pour groupe structural une courbe elliptique E, on constate que les E-torseurs de X (au sens de la topologie f.p.p.f.) forment un groupe isomorphe à $E(k)$. Si a est un point de $E(k)$ et si Y_a est le E-torseur correspondant, les trois propriétés suivantes sont équivalentes :

(i) la fibration $Y_a \to X$ est localement isotriviale;
(ii) a est d'ordre fini dans $E(k)$;
(iii) Y_a est une surface projective.

En prenant a d'ordre infini, cela donne un exemple de fibré principal pour la topologie étale qui n'est pas localement isotrivial (et cela donne en même temps un exemple de surface complète qui n'est pas projective).

14. Il existe une théorie des revêtements où les groupes finis sont remplacés par des schémas en groupes finis. Cela conduit à un groupe fondamental qui est proalgébrique, cf. V. NORI, Proc. Indian Math. Soc. **91** (1982), 73–122.

15. La réponse à cette question est « oui ». En effet, grâce au lemme 4, il suffit de le démontrer lorsque G est linéaire, et ce cas a été traité par J-L. COLLIOT-THÉLÈNE et M. OJANGUREN, Publ. Math. I.H.E.S. **75** (1992), 97–122.

16. Ici encore, la réponse est « oui »; cela résulte du fait que le corps des fonctions d'une courbe est de dimension cohomologique 1.

17. Cela a été démontré par GROTHENDIECK, cf. SGA 1, exposé XII, p. 332, th. 5.1.

18. « un calcul explicite » : je n'ai pas conservé les détails de ce calcul, et je ne peux pas garantir qu'il soit correct; il se peut que $\theta_Y(\beta)$ soit égal à $-\alpha$ et non à α.

19. Pour un résumé de la théorie des fibrés algébriques de Weil, voir Sém. Bourbaki 1952-53, exposé n° 82.

Séminaire Chevalley 1958-59, exposé 10

1. Les notations et conventions sont les mêmes que dans l'exposé précédent : le corps de base k est algébriquement clos, et les « variétés » sont supposées irréductibles. Si V est une variété, R(V) désigne le corps des fonctions rationnelles de V.

2. Ce lemme est standard, cf. e.g. BOURBAKI, A V.113.

3. « fonction » = application rationnelle.

4. « théorème principal » : il s'agit du « Main Theorem » de Zariski, cf. EGA III.4.4.3 et EGA IV.8.12.6.

5. Il devrait être possible de prouver les propriétés (i), ..., (iv), mais je ne crois pas que cela figure explicitement dans la littérature.

6. Oui, cf. note **17** à l'exposé précédent.

7. Oui, ce n'est pas difficile à démontrer.

Séminaire Chevalley 1958-59, exposé 11

1. Le corollaire 3 ne s'étend pas à la caractéristique $p > 0$. MUMFORD (Amer. J. Math. **83** (1961), 339–342) a même montré qu'il existe des exemples de *formes de première espèce* qui ne sont pas fermées (de façon plus précise, il a montré que toute forme de degré 1 sur une surface devient de première espèce sur un revêtement ramifié convenable).

Séminaire Bourbaki 1959-60, exposé 198

1. Pour la factorisation des fonctions entières p-adiques, voir par exemple M. LAZARD, Publ. Math. I.H.E.S. **14** (1962), 47–75.

Séminaire Bourbaki 1959-60, exposé 204

1. « j'ignore quel travail... ». Il a fallu une vingtaine d'années pour y parvenir. Voir là-dessus l'exposé de DELIGNE au Séminaire Bourbaki 1979-80, n° 543, sur les travaux de FULTON et HANSEN. Voir aussi M.V. NORI, Ann. Sci. E.N.S. **16** (1983), 305–344.

2. Les « variétés » considérées ici sont supposées irréductibles. On ne s'occupe que de revêtement connexes.

3. Voir les travaux cités dans la note **1** ci-dessus.

4. Pour des démonstrations générales du théorème de pureté, voir GROTHENDIECK, SGA 2, exposé X, th. 3.4, ainsi que M. AUSLANDER, Amer. J. of Math. **84** (1962), 116–125.

5. On doit supposer que W est non singulière; sinon, on peut simplement affirmer que $W' \to W$ est non ramifié en dehors d'un sous-espace de codimension > 1.

Pour une version locale de ce lemme, voir SGA 1, exposé XIII, § 5.

Séminaire Bourbaki 1960-61, exposé 209

1. La notation $\widehat{H}^q(G, A)$, avec $q \in \mathbf{Z}$, désigne le q-ième groupe de cohomologie de G, à coefficients dans A, modifié à la Tate si $q \leqslant 0$, cf. CARTAN-EILENBERG, [**2**], Chap. XII, § 2.

2. Non, $[P] = 0$ n'entraîne pas que P soit libre; SWAN en a fabriqué un exemple, où le groupe G est le groupe quaternionien d'ordre 32 (Ann. of Math. **76** (1962), 55–61).

3. Les références des articles de GIORGIUTTI et de BASS sont :
I. GIORGIUTTI, C.R.A.S. **250** (1960), 1419–1420;
H. BASS, Ann. of Math. **73** (1961), 532–542.

Séminaire Delange-Pisot-Poitou 1965-66, exposé 15

1. Il s'agit du théorème dit « des six exponentielles ».

2. Ce théorème a des applications à la théorie des représentations ℓ-adiques abéliennes, cf. *Abelian ℓ-adic Representations and Elliptic Curves* (Benjamin, New York, 1968 — 2nd edit. AK Peters, Wellesley, 1998, p. III–24). Dans cette direction, un énoncé nettement plus fort a été obtenu par M. WALDSCHMIDT (Invent. Math. **63** (1981), 97–127); voir aussi G. HENNIART, Séminaire de Théorie des Nombres 1980-81, Birkhäuser-Verlag 1982, 107–126.

3. Pour cet « argument classique » (dû, je crois, à DEDEKIND), voir BOURBAKI, A V.26, cor. 1 au th. 1.

4. J'avais eu l'espoir d'appliquer cet énoncé aux représentations ℓ-adiques abéliennes, cf. note **2** ci-dessus. Je n'y suis pas parvenu, faute de pouvoir vérifier la condition de « λ-densité » dans le cas qui m'intéressait.

Séminaire Bourbaki 1966-67, exposé 318

1. Pour un exposé des principales propriétés des groupes p-divisibles (également appelés « groupes de Barsotti-Tate »), voir :

L. SZPIRO, *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell*, Astérisque **127**, exposé VI (par L. ILLUSIE), 151–198.

2. Précisons que c'est le groupe étale qui est le quotient.

3. Le th. 1 a été étendu par A.J. DE JONG au cas d'égale caractéristique : Invent. Math. **134** (1998), 301–333; Erratum, *ibid.* **138** (1999), 225.

4. Référence : S. SEN, Ann. of Math. **90** (1969), 33–46 et Invent. Math. **62** (1980), 89–116.

5. Ce problème (existence d'une décomposition de Hodge-Tate pour la cohomologie p-adique en toute dimension) a été essentiellement résolu par FONTAINE-MESSING et FALTINGS. Voir par exemple :

J-M. FONTAINE et W. MESSING, Contemp. Math. **67**, A.M.S. (1987), 179–207,

G. FALTINGS, J. A.M.S. **1** (1988), 255–299,

ainsi que :

T. TSUJI, Invent. Math. **137** (1999), 233–411.

6. Pour $p = 2$, il existe un groupe p-divisible de hauteur 2 sur $\mathbf{Z}$ qui n'est pas « trivial », i.e. pas produit de deux groupes de hauteur 1 (mais il est 2-isogène à un tel produit).

Pour $p = 3, 5, \ldots, 17$, tout groupe p-divisible sur $\mathbf{Z}$ est trivial; cela a été démontré par V.A. ABRASHKIN (Izv. Mat. S.S.S.R. **31** (1988), 1–46) et par J-M. FONTAINE (Invent. Math. **81** (1985), 515–538), en utilisant des minorations de discriminants à la Odlyzko.

Le cas $p > 17$ reste ouvert.

Séminaire Bourbaki 1977-78, exposé 511

1. Oui, la valeur optimale de C est 8, cf. M.A. KENKU, J. Number Theory **15** (1982), 199-202.

2. Cette question est encore ouverte.

3. La réponse à la question 3) est « oui », cf. M.A. KENKU, J. London Math. Soc. **23** (1981), 415–427.

4. Cette question est encore ouverte; par contre la question analogue pour $Y_1(N)$ a été résolue par L. MEREL (Invent. Math. **124** (1996), 437–449).

Séminaire Bourbaki 1998-99, exposé 864

1. Cf. A. BOREL, *Linear Algebraic Groups* (2nd enlarged edition), Springer-Verlag 1991, § 24.7.

2. Pour cette « variante non encore publiée », voir les notes d'un cours donné à Eugene (Oregon) en 1998 :
`http://darkwing.uoregon.edu/~math/serre/index.html`

3. Ce problème a été résolu (positivement) par G. LUSZTIG (J. Algebra **260** (2003), 298–322).

INDEX

Ce volume regroupe des exposés donnés par J.-P. Serre entre 1950 et 1999 dans les séminaires Bourbaki, Cartan, Chevalley et Delange-Pisot-Poitou. Les thèmes abordés vont de la topologie algébrique à la théorie des nombres en passant par les groupes de Lie, la géométrie algébrique et les formes modulaires. On y trouve à la fois des présentations de travaux d'autres mathématiciens (Borel, Dwork, ...) et de travaux plus personnels comme l'exposé du séminaire Chevalley sur les espaces fibrés algébriques qui devait inspirer à Grothendieck la définition de la cohomologie étale. Aucun de ces textes ne figurait déjà dans les quatre volumes des « Collected Papers » de J.-P. Serre.

La deuxième édition de ce volume a été augmentée de deux textes récents : « On a theorem of Jordan » (Math. Medley 2002) et « Complète réductibilité » (Sém. Bourbaki 2003-2004).