ANNALES SCIENTIFIQUES DE L'É.N.S.

MICHEL LAZARD

Sur les groupes nilpotents et les anneaux de Lie

Annales scientifiques de l'É.N.S. 3^e série, tome 71, n° 2 (1954), p. 101-190

<http://www.numdam.org/item?id=ASENS_1954_3_71_2_101_0>

SUR LES GROUPES NILPOTENTS ET LES ANNEAUX DE LIE

PAR M. MICHEL LAZARD.

INTRODUCTION.

L'objet principal de ce travail est d'étudier certains aspects des relations entre les structures de groupes et d'anneaux de Lie. Malgré la généralité apparente de certains énoncés, les résultats obtenus ne concernent que des catégories particulières de groupes et d'anneaux de Lie : il s'agira toujours, en fait, de groupes nilpotents ou de N-groupes (groupes nilpotents généralisés).

Une N-suite dans un groupe G est, par définition, une suite décroissante de sous-groupes $H_1, H_2, \ldots$ telle que $H_1 = G$ et que le commutateur $xyx^{-1}y^{-1}$ de deux éléments choisis respectivement dans H_i et H_j appartienne toujours à H_{i+j}. Le groupe G est dit un N-groupe s'il possède une N-suite (H_i) telle que l'intersection des H_i se réduise à l'élément neutre.

Le chapitre I étudie un procédé qui associe un anneau de Lie gradué à toute N-suite d'un groupe donné. Il s'agit d'une extension naturelle d'une notion devenue courante en topologie algébrique et en algèbre : celle d'anneau gradué associé à un anneau filtré.

Au paragraphe 1 je présente des identités qui font immédiatement ressortir l'analogie entre d'une part, produit et commutateur dans un groupe, et d'autre part, somme et crochet dans un anneau de Lie. L'identité (1.1) est classique; la remarquable identité « jacobienne » (1.2) est due à M. P. Hall et m'a été communiquée par M. Kaloujnine. J'indique une première application de l'analogie entre groupes et anneaux de Lie en interprétant plus simplement certains calculs de Levi et van der Waerden [20].

Le paragraphe 2 donne la définition de l'anneau de Lie gradué associé à une N-suite; bien que cette notion soit extrêmement simple, elle ne paraît

avoir été reconnue (ou publiée) que dans deux cas particuliers, correspondant à deux N-suites particulières : la suite centrale descendante et la N-suite des groupes de dimension mod$p$ (premier) [23], [36]. Quelques propriétés qui résultent immédiatement de la définition générale sont rassemblées à la fin du paragraphe 2.

Le paragraphe 3 établit la possibilité d'obtenir une N-suite dans un groupe G au moyen d'un homomorphisme convenable de G dans le groupe multiplicatif des éléments inversibles d'un anneau filtré : les calculs correspondants peuvent être considérés comme connus (ils apparaissent en substance dans l'étude des groupes de ramification supérieurs d'une extension galoisienne d'un corps valué complet). J'ai signalé au passage (3.4) une importante généralisation de ces résultats obtenue par M. Kaloujnine. Le théorème (3.3), transposition aux N-suites du théorème de Jordan-Hölder, indique comment comparer les anneaux de Lie associés à deux N-suites d'un même groupe.

Le paragraphe 4 expose la méthode de M. Magnus [21] pour étudier un groupe libre : on le plonge dans le groupe multiplicatif des éléments inversibles d'une algèbre associative libre complétée (algèbre de Magnus). Je reprends ensuite la méthode de M. Witt [33] pour la détermination de la suite centrale descendante d'un groupe libre. Peut-être les considérations générales qui la précèdent ont-elles permis d'en faire ressortir plus nettement le principe.

La clé des développements ultérieurs du premier chapitre est constituée par le théorème (5.4) qui permet la détermination effective des N-suites d'un groupe libre associées à certaines filtrations d'une algèbre de Magnus. Son origine remonte à la détermination par M. Zassenhaus [36] des groupes de dimension mod$p$ (1). Mais, tandis que M. Zassenhaus s'appuyait sur les propriétés des algèbres de Lie restreintes (au sens de M. Jacobson [11]) (2), j'ai montré, au contraire (§ 6), que les propriétés des algèbres de Lie restreintes pouvaient se déduire des propriétés du groupe libre, ce qui rétablit l' « antériorité » du groupe par rapport à l'algèbre de Lie. De plus, le résultat indiqué permet de déterminer les groupes de dimension modp^h (h entier positif quelconque) d'un groupe libre, ainsi que d'autres N-suites, d'un caractère très différent, qui montrent combien sont variés les divers anneaux de Lie associés aux N-suites d'un même groupe libre. Il faut noter que les sous-groupes ainsi définis dans les groupes libres se trouvent caractérisés comme des sous-ensembles dont il n'est nullement évident, *a priori*, que ce sont des sous-groupes : cela permet d'obtenir diverses identités.

---

(1) J'ai conservé l'expression « groupes de dimension » consacrée par l'usage. Elle n'est pas très heureuse, puisqu'il s'agit en réalité, de certaines suites de sous-groupes caractéristiques définis d'abord dans les groupes libres (*cf.* § 4), puis, par passage aux quotients, dans des groupes quelconques.

(2) Il serait plus correct de dire « p-restreintes », puisqu'on introduit cette notion après s'être donné un nombre premier déterminé p.

Au paragraphe 6, j'introduis la notion de N-suite restreinte, plus simple par sa formulation que la notion d'algèbre de Lie restreinte, et j'étudie la correspondance entre ces deux notions : sur l'anneau de Lie associé à une N-suite restreinte, on peut définir canoniquement une structure d'algèbre de Lie restreinte à coefficients entiers mod$p$. D'autre part, toute N-suite restreinte, peut s'obtenir à partir d'une filtration convenable de l'anneau du groupe à coefficients entiers mod$p$. Ce résultat (6.7), dont la démonstration est assez pénible, permet de démontrer certaines propriétés de structure des algèbres de Magnus (6.11), (6.12).

Le paragraphe 7, consacré à l'étude des groupes de dimension mod$n$ (entier quelconque) fait apparaître l'analogie entre l'étude « locale » d'un groupe libre (§ 5) et l'étude « locale » de l'anneau des entiers rationnels (c'est-à-dire la théorie des entiers p-adiques).

Le paragraphe 8 apporte quelques commentaires et signale quelques-uns des très nombreux problèmes ouverts. J'ai voulu surtout indiquer combien ces questions sont mal connues, et comment les « évidences » sont parfois trompeuses. Il se peut, bien entendu, que mon information ait été insuffisante.

Le chapitre II (dont la lecture ne suppose connus que les paragraphes 1 à 4 du chapitre I) étudie une correspondance beaucoup plus fine entre groupes et anneaux de Lie, correspondance fondée sur l'application de la formule de Hausdorff [9]. Les paragraphes 1 et 3 ont été développés un peu plus qu'il n'était strictement nécessaire en raison de leur intérêt propre. Au paragraphe 1, je considère une algèbre de Lie libre complétée L à coefficients rationnels, qui devient un groupe si l'on y définit une multiplication au moyen de la formule de Hausdorff. Les générateurs de L engendrent (au sens de la multiplication) un groupe libre. J'étudie dans L certaines suites d'éléments qui peuvent être représentées en quelque sorte par des séries de Taylor par rapport à une variable entière. Si l'on exige seulement que la série converge, on est conduit à la notion de suite analytique (1.14a); mais il est préférable d'imposer une condition plus forte, qui donne la définition des suites typiques (1.1) : au lieu d'imposer seulement que l'ordre du $i^{\text{ième}}$ coefficient a_i de la série considérée tende vers l'infini avec i, on exige qu'il soit toujours au moins égal à i. Les suites typiques constituent un sous-groupe et une sous-algèbre de Lie dans l'ensemble de toutes les suites à valeurs dans L (1.4). Un théorème général (1.5) montre la possibilité de représenter une suite typique comme un produit infini; la représentation dépend du choix d'une suite de polynomes à coefficients rationnels.

Un premier choix conduit au théorème (1.10) qui ne concerne plus qu'un groupe libre; la structure d'algèbre de Lie n'a joué qu'un rôle auxiliaire dans la démonstration. Ce théorème constitue une généralisation et en même temps une réciproque d'un théorème de M. P. Hall ([8], § 3); c'est de là que je suis parti pour aboutir à la notion de suite typique, car une suite typique dans un

groupe libre est précisément une suite d'éléments qui vérifie le théorème de M. P. Hall. La méthode des suites typiques est moins directe que le procédé original de M. P. Hall (le « collecting process »), mais elle me paraît plus aisée et plus puissante.

Un second choix de la suite de polynomes (1.5) conduit, au paragraphe 2, à la description complète de la structure d'algèbre de Lie topologique de L à partir de sa structure de groupe topologique (2.4). C'est ce que j'appelle réaliser l'inversion générique de la formule de Hausdorff. Des formules d'inversion « explicites » (c'est-à-dire théoriquement calculables) montrent que la somme et le crochet de deux éléments de L sont égaux à des produits infinis de « mots » en ces deux éléments, affectés d'exposants rationnels dont on connaît certaines propriétés arithmétiques.

Le paragraphe 3 établit quelques résultats auxiliaires; la notion d'algèbre de Lie n'y intervient pas, et la structure fondamentale étudiée est celle d'un groupe dans lequel on s'est donné une suite centrale possédant certaines propriétés. Le théorème (3.2) établit l'existence de certaines suites centrales. Le théorème (3.6) donne une condition pour qu'un homomorphisme d'un sous-groupe puisse s'étendre univoquement à un homomorphisme du groupe tout entier. Le théorème (3.10), dont la démonstration est la plus longue, établit l'existence de certaines extensions de groupes.

Le paragraphe 4 aborde la question des groupes discrets (ou de leurs limites projectives) qu'on peut définir à partir d'anneaux de Lie par la formule de Hausdorff. Le théorème (4.2) indique une catégorie d'anneaux de Lie où l'on peut appliquer la formule de Hausdorff, et le théorème (4.3) montre que, dans la catégorie de groupes ainsi obtenue, l'inversion de la formule de Hausdorff (au sens du paragraphe 2) est possible, et qu'on retrouve bien l'anneau de Lie initial. Ces théorèmes conduisent à des résultats satisfaisants dans le cas des groupes de torsion (4.6) et des groupes sans torsion (4.15). Par contre, dans le cas général, il est impossible de faire correspondre l'anneau de Lie au groupe (ou le groupe à l'anneau de Lie) sans faire un choix particulier de la suite de sous-groupes (ou d'idéaux) qui intervient dans les énoncés (4.2), (4.3). Les résultats concernant les groupes de torsion avaient été partiellement énoncés par M. Magnus [23]; ceux concernant les groupes sans torsion ont été démontrés par M. Malcev [26], [27]. Mais la méthode de M. Malcev fait appel à la théorie des groupes de Lie [25], alors que la méthode proposée ici est purement algébrique. J'ai développé à nouveau la théorie de M. Malcev concernant certaines extensions canoniques des groupes nilpotents sans torsion (4.8) que j'ai appelées complétions de Malcev. Outre son avantage méthodologique, le procédé que j'ai suivi permet certaines généralisations (4.17) auxquelles la méthode analytique ne semble pas conduire. On voit, en particulier, que la complétion de Malcev ne fait pas appel aux structures d'algèbres de Lie.

Le paragraphe 5 expose la construction d'un groupe particulier. Je l'ai pré-

senté pour légitimer la généralité du théorème (4.6), et aussi pour montrer que la possibilité de remplacer certaines structures de p-groupes par des structures d'algèbres de Lie peut effectivement simplifier des constructions.

Il aurait été possible d'obtenir certains résultats par des procédés plus rapides [*cf.*, par exemple, (4.18)]. J'ai choisi un mode d'exposition général qui ne va pas sans une certaine lourdeur.

Il me semble qu'on pourrait tirer de ce travail une confirmation des points de vue suivants : d'abord l'intérêt que présente l'étude de groupes définis à partir d'autres structures possédant plusieurs opérations (par exemple des algèbres de Lie). En effet, la simplicité apparente des axiomes des groupes ne fait souvent que masquer une extrême complexité, et d'autres structures, plus riches par le nombre de leurs axiomes, se laissent plus facilement étudier. D'autre part, si l'étude des relations entre groupes et algèbres de Lie est encore très incomplète, on peut estimer néanmoins que les algèbres de Lie se révèleront insuffisantes, même pour l'étude des p-groupes finis. Il conviendrait donc de rechercher si d'autres structures algébriques pourraient permettre la construction de nouvelles catégories de groupes. Mais il est possible qu'on n'aboutisse pas à des formules génériques (comme l'est la formule de Hausdorff) en raison de l'existence d'invariants de structure des groupes, dont la théorie de l'homologie pourrait peut-être rendre compte. Il ne s'agit là que de conjectures imprécises, et de nombreuses recherches seront nécessaires pour élucider ces questions encore très obscures.

Je tiens à remercier M. L. Kaloujnine pour toute l'aide qu'il m'a apportée, tant au cours de nombreuses conversations personnelles qu'à l'occasion du Séminaire de théorie des groupes qu'il a dirigé à Paris en 1950. Qu'il trouve ici l'expression de mon amicale reconnaissance.

J'exprime ma profonde reconnaissance à M. A. Châtelet dont les conseils et les encouragements m'ont été très précieux. Je remercie MM. J. Favard, L. Schwartz, P. Samuel qui ont bien voulu se joindre à M. Châtelet pour constituer le jury auquel je soumets cette Thèse, ainsi que M. A. Denjoy qui a bien voulu présenter mes Notes à l'Académie des Sciences, et M. P. Montel qui a bien voulu accepter ce travail dans les *Annales de l'École Normale Supérieure*.

CHAPITRE I.

Une extension aux groupes de la méthode des filtrations.

1. Le calcul des commutateurs. — Nous conviendrons de représenter par (x, y) le commutateur $xyx^{-1}y^{-1}$ de deux éléments x et y d'un groupe G noté multiplicativement. Si H et K sont deux sous-groupes de G, (H, K) désignera le

sous-groupe de G engendré par tous les commutateurs (x, y) où $x \in H$ et $y \in K$ (3).

Nous aurons très souvent à considérer des suites de sous-groupes (H_i) dans un groupe $G (i = 1, 2, \ldots)$. Il s'agira de *suites décroissantes, commençant au groupe* G, c'est-à-dire qu'on aura :

$$G = H_1 \supset H_2 \supset \ldots \supset H_i \supset H_{i+1} \supset \ldots.$$

La notion usuelle de suite de composition d'un groupe s'obtient en exigeant que chaque sous-groupe H_{i+1} soit invariant dans le précédent [ce qui peut s'écrire $(H_i, H_{i+1}) \subset H_{i+1}$], et que les sous-groupes H_i se réduisent à l'élément neutre à partir d'une certaine valeur de l'indice i.

Nous dirons généralement qu'une suite de sous-groupes (H_i) est *finie* si $H_i = (e)$, élément neutre du groupe, à partir d'une certaine valeur de l'indice i; nous dirons qu'elle est *séparante* si l'intersection des sous-groupes H_i se réduit à l'élément neutre :

$$\bigcap_i H_i = (e).$$

Nous appellerons *suite centrale* dans un groupe G une suite de sous-groupes (H_i) telle que $(G, H_i) \subset H_{i+1}$ pour tout i, c'est-à-dire telle que H_i/H_{i+1} s'identifie à un sous-groupe du centre de G/H_{i+1} (pour tout $i \geqq 1$). Les sous-groupes H_i sont alors tous invariants dans G [puisque $(G, H_i) \subset H_{i+1} \subset H_i$]. Un groupe qui possède une suite de composition centrale est dit *nilpotent*.

Dans un groupe G quelconque, on définit par induction les sous-groupes de la suite centrale descendante au moyen des relations :

$$G_1 = G, \qquad G_{i+1} = (G, G_i).$$

Un groupe nilpotent est caractérisé par le fait qu'à partir d'un certain rang tous les sous-groupes de la suite centrale descendante sont réduits à l'élément neutre e. En effet, pour toute suite centrale (H_i) dans G, on a les relations $G_i \subset H_i$ qui s'établissent par induction : $G_1 \subset H_1 = G$ et $G_i \subset H_i$ implique

$$(G, G_i) = G_{i+1} \subset (G, H_i) \subset H_{i+1}.$$

Ainsi la suite centrale descendante « décroît plus vite » que toute autre suite centrale. La *classe* d'un groupe nilpotent G, égale par définition au nombre minimum de quotients distincts d'une suite de composition centrale, peut donc être définie comme l'entier c vérifiant

$$G_c \neq (e), \qquad G_{c+1} = (e).$$

Dans un groupe non nilpotent, la suite centrale peut se terminer à un sous-groupe non réduit à l'élément neutre, ou (si G est infini) avoir tous ses termes

(3) Pour les notions générales rappelées dans ce paragraphe, on pourra consulter Zassenhaus [34].

distincts. Nous appellerons N-*groupes* les groupes G tels que l'intersection des sous-groupes G_i de leur suite centrale descendante, se réduise à l'élément neutre $\left(\bigcap G_i = (e)\right)$; l'exemple le plus important de N-groupes non nilpotents est celui des groupes libres (4).

Le système de deux opérations constitué par le produit xy et la commutation (x, y) dans un groupe possède des propriétés formelles qui l'apparente au système constitué par l'addition $x+y$ et le crochet de Lie $[x, y]$ dans une algèbre de Lie (5). A la distributivité du crochet de Lie correspondent les relations suivantes, où l'on convient de noter x^y le transformé yxy^{-1} de x par l'automorphisme intérieur associé à y :

$$(1.1)\qquad \begin{cases} (x, yz) = (x, y)\,(x, z)^y = (x, y)\,(x, z)\big((z, x), y\big), \\ (xy, z) = (y, z)^x (x, z) = \big(x, (y, z)\big)\,(y, z)\,(x, z). \end{cases}$$

A l'identité de Jacobi correspond la relation suivante, due à P. Hall :

$$(1.2)\qquad \big((x, y), z^y\big)\big((y, z), x^z\big)\big((z, x), y^x\big) = e.$$

Cette analogie des groupes et des algèbres de Lie peut conduire à des conséquences intéressantes dans le cas des N-groupes et en particulier des groupes nilpotents. Montrons, par exemple, comment elle conduit à retrouver les résultats de Levi et van der Waerden [20] concernant les groupes d'exposant 3 (groupes où $x^3 = e$ pour tout élément x). Ces groupes possèdent la propriété plus générale que chaque élément permute avec chacun de ses conjugués. En effet, dans un tel groupe,

$$xyxy^{-1} = (xy)^{-2}xy^{-1} = y^{-1}x^{-1}y^{-2} = y^{-1}x^{-1}y = y^{-1}(x^{-1}y)^{-2} = y^{-2}xy^{-1}x = yxy^{-1}x,$$

donc x et yxy^{-1} commutent.

Étudions généralement les groupes G où chaque élément permute avec tous ses conjugués, propriété que nous pouvons exprimer par l'identité :

$$\big((x, y), y\big) = e,$$

---

(4) *Cf.* § 4.

(5) Étant donné un anneau commutatif Ω possédant une unité, nous appelons Ω-*algèbre de Lie* un Ω-module unitaire L muni d'une opération bilinéaire $[x, y]$ appelée *crochet* (de Lie) vérifiant les axiomes suivants :

$$[x, x] = 0 \qquad \text{et} \qquad [[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$

pour tous $x, y, z \in L$. Le résultat de l'opération « crochet » appliquée à deux éléments x et y de L s'appellera encore le crochet de x et de y. Étant donné une famille $(x_\iota)_{\iota\in I}$ d'éléments de L, nous appellerons *alternants* par rapport aux (x_ι) les éléments de L définis ainsi : Chaque x_ι est un alternant, et le crochet de deux alternants par rapport aux (x_ι) est encore un alternant par rapport aux (x_ι). Lorsque l'anneau d'opérateurs Ω se réduit à l'anneau Z des entiers rationnels, nous parlerons simplement d'*anneaux de Lie* (au lieu de Z-algèbres de Lie).

pour tous $x, y \in G$. L'identité correspondante dans une algèbre de Lie serait :

$$[[x, y], y] = 0.$$

Nous en déduisons dans ce cas :

$$[[x, y], z] + [[x, z], y] = [[x, y + z], y + z] - [[x, y], y] - [[x, z], z] = 0.$$

La fonction $[[x, y], z]$ de x, y, z est une fonction alternée, puisqu'elle est transformée en son opposée lorsqu'on transpose x et y ou y et z. L'identité de Jacobi donne alors :

$$3[[x, y], z] = 0.$$

De plus,

$$[[x, y], z] = [[y, z], x] = -[x, [y, z]].$$

On voit de même que la fonction $[[[x, y], z], t]$ de x, y, z, t est alternée, puisqu'une transposition de deux variables consécutives la transforme en son opposée. En particulier :

$$[[[x, y], z], t] = [[[z, t], x], y].$$

Mais

$$\begin{aligned}[[[x, y], z], t] &= -[[x, y], [z, t]] = [[z, t], [x, y]] \\ &= -[[[z, t], x], y] = -[[[x, y], z], t].\end{aligned}$$

Ainsi $2[[[x, y], z], t] = 0$ et comme $3[[[x, y], z], t] = 0$, il en résulte que

$$[[[x, y], z], t] = 0.$$

Le même raisonnement s'étend au cas des groupes où $\big((x, y), y\big) = e$. Tout d'abord

$$e = (x, yy^{-1}) = (x, y)\,(x, y^{-1})^{y} = (x, y)\,(x, y^{-1}) \quad \text{et} \quad \big((x, y)^{z}, y\big) = (y^{zxy^{-z}}, y) = e,$$

puisque y permute avec ses conjugués.

Développons maintenant $e = \big((x, yz), yz\big)$ au moyen des formules (1.1). Nous obtenons :

$$\begin{aligned}e &= \big((x, y)\,(x, z)^{y}, yz\big) = \big((x, y)\,(x, z)^{y}, y\big)\big((x, y)\,(x, z)^{y}, z\big)^{y} \\ &= \big((x, z)^{y}, y\big)^{(x,y)}\big((x, y), y\big)\big((x, z)^{y}, z\big)^{y(x,y)}\big((x, y), z\big)^{y};\end{aligned}$$

les deuxième et troisième facteurs sont égaux à e, et il reste :

$$\big((x, z)^{y}, y\big)^{(x,y)}\big((x, y), z\big)^{y} = e.$$

Transformons par l'automorphisme intérieur associé à

$$(x, y)^{-1}y^{-1} = y^{-1}(x, y)^{-1};$$

il vient :

$$\big((x, z), y\big)\big((x, y), z\big) = e.$$

La démonstration s'achève alors comme dans le cas des algèbres de Lie; il suffit de remarquer que

$$\big((x, y), z^y\big) = \big((x, y), z\big)^y = \big((x, y), z\big),$$

car

$$\Big(\big((x, y), z\big), y\Big) = \Big(\big((x, y), y\big), z\Big) = e.$$

L'identité (1.2) peut donc remplacer l'identité de Jacobi pour démontrer que $\big((x, y), z\big)^3 = e$, et nous parvenons ainsi au

THÉORÈME (1.3). — *Si dans le groupe* G *tout élément commute avec chacun de ses conjugués,* G *est nilpotent de classe au plus égale à* 3 *et, si* $x \in G_3$ *(troisième groupe de la suite centrale descendante de* G), $x^3 = e$.

2. LES ANNEAUX DE LIE GRADUÉS ASSOCIÉS AUX N-SUITES D'UN GROUPE. — La comparaison des groupes aux algèbres de Lie, dont nous venons d'indiquer le principe, comprend deux étapes : on considère d'abord le groupe comme abélien, en associant à sa multiplication l'addition commutative d'une algèbre de Lie; puis on retrouve certaines propriétés résultant de la non-commutativité en leur faisant correspondre des propriétés du crochet de Lie. Nous allons montrer comment, par cette méthode, on peut associer des anneaux de Lie gradués à certaines suites de sous-groupes.

Définition. — Nous appellerons N-*suite* dans un groupe G une suite de sous-groupes (H_i) $(i = 1, 2, \ldots)$, tels que $H_1 = G$, $H_i \supset H_{i+1}$ et $(H_i, H_j) \subset H_{i+j}$ pour tous $i, j \geqq 1$.

D'après cette définition, toute N-suite est une suite centrale, un groupe qui possède une N-suite finie est nilpotent, et un groupe qui possède une N-suite séparante est un N-groupe.

Soit G un groupe, (H_i) une N-suite dans G. Les groupes quotients H_i/H_{i+1} sont abéliens, puisque $(H_i, H_i) \subset H_{2i} \subset H_{i+1}$. Nous les noterons additivement, et nous désignerons par $\tilde{x}_i$ l'élément de H_i/H_{i+1} constitué par la classe modulo H_{i+1} de $x_i \in H_i$; nous aurons donc

$$\widetilde{x_i x_i'} = \tilde{x}_i + \tilde{x}_i'.$$

Formons la somme directe $\Sigma_i H_i/H_{i+1}$. Nous obtenons un groupe abélien où nous introduisons une graduation en convenant que les éléments de H_i/H_{i+1} sont homogènes de degré i. Soient $x_i \in H_i$ et $x_j \in H_j$; alors $(x_i, x_j) \in H_{i+j}$, et, d'après les identités (1.1), la classe de (x_i, x_j) modulo H_{i+j+1} ne dépend que des classes de x_i et de x_j mod H_{i+1} (resp. H_{j+1}) : si, par exemple, $x_{j+1} \in H_{j+1}$,

$$(x_i, x_j x_{j+1}) = (x_i, x_j)\,(x_i, x_{j+1})^{x_j} \qquad \text{et} \qquad (x_i, x_{j+1})^{x_j} \in H_{i+j+1}.$$

Nous voyons donc que l'on peut définir une application de $(H_i/H_{i+1}) \times (H_j/H_{j+1})$

dans H_{i+j}/H_{i+j+1} en faisant correspondre au couple $\tilde{x}_i$, $\tilde{x}_j$ l'élément $\widetilde{(x_i, x_j)}$ que nous noterons $[\tilde{x}_i, \tilde{x}_j]$. Les identités (1.1) montrent de plus que cette application est bilinéaire, c'est-à-dire qu'on a identiquement :

$$[\tilde{x}_i + \tilde{x}'_i, \tilde{x}_j] = [\tilde{x}_i, \tilde{x}_j] + [\tilde{x}'_i, \tilde{x}_j] \qquad \text{et} \qquad [\tilde{x}_i, \tilde{x}_j + \tilde{x}'_j] = [\tilde{x}_i, \tilde{x}_j] + [\tilde{x}_i, \tilde{x}'_j].$$

Les identités $(x, x) = e$ et $(x, y) = (y, x)^{-1}$ conduisent immédiatement à

$$[\tilde{x}_i, \tilde{x}_i] = 0 \qquad \text{et à} \qquad [\tilde{x}_i, \tilde{x}_j] = -[\tilde{x}_j, \tilde{x}_i].$$

Nous étendons par linéarité la définition de $[\tilde{x}, \tilde{y}]$ à un couple d'éléments quelconques $\tilde{x}$ et $\tilde{y}$ de $\Sigma_i H_i/H_{i+1}$: si $\tilde{x} = \Sigma_i \tilde{x}_i$ et $y = \Sigma_j \tilde{y}_j$ sont les décompositions de $\tilde{x}$ et $\tilde{y}$ en leurs composantes homogènes, $[\tilde{x}, \tilde{y}]$ est égal par définition à $\Sigma_{i,j}[\tilde{x}_i, \tilde{y}_j]$. Alors $[\tilde{x}, \tilde{y}]$ est une opération bilinéaire vérifiant l'identité $[\tilde{x}, \tilde{x}] = 0$. L'identité de Jacobi;

$$[[\tilde{x}, \tilde{y}], \tilde{z}] + [[\tilde{y}, \tilde{z}], \tilde{x}] + [[\tilde{z}, \tilde{x}], \tilde{y}] = 0$$

est vérifiée pour $\tilde{x}$, $\tilde{y}$, $\tilde{z}$, homogènes [conséquence immédiate de l'identité (1.2)], donc pour $\tilde{x}$, $\tilde{y}$, $\tilde{z}$ quelconques (en les décomposant en leurs composantes homogènes). Nous avons donc associé canoniquement à la N-suite (H_i) un anneau de Lie gradué que nous noterons $\mathfrak{L}(H_i)$. D'où le

THÉORÈME (2.1). — *A toute* N*-suite* (H_i) *d'un groupe* G *se trouve associé canoniquement un anneau de Lie gradué* $\mathfrak{L}(H_i)$ *qui a pour support la somme directe* $\Sigma_i H_i/H_{i+1}$. *Le crochet de Lie de deux éléments homogènes s'obtient à partir du commutateur dans* G *par passage aux quotients.*

Les renseignements que permet d'obtenir sur le groupe G l'anneau de Lie $\mathfrak{L}(H_i)$ ne concernent en fait que le groupe quotient $G/\bigcap_i H_i$ de G par l'intersection des H_i, qui est un N-groupe. On pourrait donc se limiter à l'étude des N-suites séparantes, dont l'existence est une propriété caractéristique des N-groupes. On sait, en effet, que la suite centrale descendante est une N-suite. On a même le résultat plus fort : si (G_i) est la suite centrale descendante du groupe G et (H_i) une suite centrale quelconque dans G, alors $(G_i, H_j) \subset H_{i+j}$ pour tous i, $j \geq 1$; cette proposition se déduit aisément, par récurrence sur i, de l'identité (1.2) [8], [14].

Si l'on a un homomorphisme f d'un groupe G dans un groupe G′ et une N-suite (H'_i) dans G′, on en déduit une N-suite (H_i) dans G, dite image réciproque de (H'_i) par f en posant $H_i = f^{-1}(H'_i)$. De même, si (H_i) est une N-suite dans G et f un homomorphisme de G *sur* G′, on obtient une N-suite (H'_i) dans G′, dite image directe de (H_i) par f, en posant $H'_i = f(H_i)$. Ces propriétés résultent immédiatement de : $f\big((x, y)\big) = \big(f(x), f(y)\big)$. On obtient alors des homomorphismes des anneaux de Lie associés. Plus généralement :

THÉORÈME (2.2).—*Soient* G *et* G′ *deux groupes*, (H_i) *et* (H'_i) *deux* N-*suites dans* G *et* G′ *respectivement*, f *un homomorphisme de* G *dans* G′ *tel que, pour tout* i, $f(H_i) \subset H'_i$. *Alors, on peut définir un homomorphisme* $\tilde{f}$ *de* $\mathfrak{L}(H_i)$ *dans* $\mathfrak{L}(H'_i)$ *conservant les degrés des éléments homogènes et caractérisé par* $\tilde{f}(\tilde{x}_i) = \widetilde{f(x_i)}$. *De plus,* f *est un isomorphisme de* $\mathfrak{L}(H_i)$ *dans* $\mathfrak{L}(H'_i)$ *si et seulement si* (H_i) *est l'image réciproque de* (H'_i) *par* f.

Démonstration. — On a, par hypothèse,

$$f(H_i) \subset H'_i \qquad \text{et} \qquad f(H_{i+1}) \subset H'_{i+1}.$$

On en déduit donc, par passage aux quotients, l'homomorphisme associé de H_i/H_{i+1} dans H'_i/H'_{i+1} qu'on peut prolonger en un homomorphisme $\tilde{f}$ de $\Sigma_i H_i/H_{i+1}$ dans $\Sigma_i H'_i/H'_{i+1}$, et l'on voit immédiatement que $\tilde{f}$ est aussi un homomorphisme pour les structures d'anneaux de Lie. Si $H_i = f^{-1}(H'_i)$ pour tout i, la restriction de $\tilde{f}$ à H_i/H_{i+1} est, pour tout i, biunivoque; $\tilde{f}$ est donc un isomorphisme. Réciproquement, si pour un certain i, $f^{-1}(H'_i) \neq H_i$, il existe un $x \in G$ tel que $f(x) \in H'_i$, $x \notin H_i$; soit j l'entier tel que $x \in H_j$, $x \notin H_{j+1}$. On a $j < i$, et la restriction de $\tilde{f}$ à H_j/H_{j+1} n'est pas biunivoque.

Pour exprimer à quelle condition $\tilde{f}$ est un homomorphisme *sur* $\mathfrak{L}(H'_i)$, nous introduisons dans G′ la topologie obtenue en prenant les sous-groupes H'_i comme système fondamental de voisinage, de l'élément neutre. Nous l'appellerons brièvement la (H'_i)-*topologie*, et nous parlerons d'ensembles (H'_i)-fermés, etc., pour indiquer que nous nous référons à cette topologie. Remarquons que f est une représentation continue de G dans G′ munis respectivement de leurs (H_i)- et (H'_i)-topologies. Alors :

THÉORÈME (2.3). — *$\tilde{f}$ est un homomorphisme de* $\mathfrak{L}(H_i)$ SUR $\mathfrak{L}(H'_i)$ *si et seulement si* $f(H_j)$ *est, pour tout entier* j, (H'_i)-*dense dans* H'_j.

En effet, la restriction de $\tilde{f}$ à H_j/H_{j+1} est un homomorphisme sur H'_j/H'_{j+1} si et seulement si $H'_j = f(H_j)H'_{j+1}$. Cette relation devant être vérifiée pour tout j, on en déduit, par récurrence sur l'entier k : $H'_j = f(H_j)H'_{j+k}$, ce qui exprime précisément que $f(H_j)$ est (H'_i)-dense dans H'_j.

Si la N-suite (H_i) dans G est *séparante*, la (H_i)-topologie de G est *séparée* (vérifie l'axiome de Hausdorff), et réciproquement. On peut dans ce cas construire le complété $\overline{G}$ de G pour cette topologie, et l'on voit facilement que les adhérences $\overline{H}_i$ des sous-groupes H_i forment dans $\overline{G}$ une N-suite telle que $G \cap \overline{H}_i = H_i$. Il suffit alors d'appliquer les résultats précédents à l'isomorphisme canonique de G dans $\overline{G}$ pour montrer que $\mathfrak{L}(H_i)$ et $\mathfrak{L}(\overline{H}_i)$, construits respectivement à partir de G et de $\overline{G}$ sont canoniquement isomorphes.

Considérons maintenant un sous-groupe G′ dans le groupe G muni de la

N-suite (H_i). Alors, les sous-groupes $H'_i = H_i \cap G'$ constituent une N-suite dans G', qui n'est autre que l'image réciproque de (H_i) par l'isomorphisme canonique de G' dans G. D'après le théorème (2.2), nous en déduisons un isomorphisme de $\mathfrak{L}(H'_i)$ dans $\mathfrak{L}(H_i)$. Autrement dit, à tout sous-groupe G' de G se trouve associé canoniquement un sous-anneau homogène de $\mathfrak{L}(H_i)$ qu'on peut représenter par $\Sigma_i(G' \cap H_i)H_{i+1}/H_{i+1}$. Si G' est invariant dans G, le sous-anneau associé est un idéal homogène de $\mathfrak{L}(H_i)$; plus précisément :

THÉORÈME (2.4). — *Soit f un homomorphisme de* G SUR *le groupe* G', (H'_i) *l'image directe de* (H_i) *par f,* N *le noyau de f. Alors le noyau de l'homomorphisme f de* $\mathfrak{L}(H_i)$ *sur* $\mathfrak{L}(H'_i)$ *est l'idéal de* $\mathfrak{L}(H_i)$ *associé à* N (6).

D'après (2.3), $\tilde{f}$ est un homomorphisme *sur* $\mathfrak{L}(H'_i)$. Le sous-anneau associé à N est certainement contenu dans le noyau de f. Cela résulte de la proposition plus générale : si G, G', G'' sont trois groupes munis respectivement des N-suites (H_i), (H'_i), (H''_i), et f, g des homomorphismes de G dans G' (resp. de G' dans G'') tels que $f(H_i) \subset H'_i$ [resp. $g(H'_i) \subset H''_i$], enfin si h est l'homomorphisme composé gf de G dans G'', alors $\tilde{h} = \tilde{g}.\tilde{f}$. Par ailleurs, si $\tilde{f}(\tilde{x}_i) = 0$,

$$f(x_i) \in H'_{i+1} = f(H_{i+1}).$$

Il existe donc $x_{i+1} \in H_{i+1}$ et $x \in N$ tels que $x_i = x_{i+1}x$, autrement dit $x_i \in (N \cap H_i)H_{i+1}$, c'est-à-dire que $\tilde{x}_i$ est dans le sous-anneau associé à N, ce qui complète la démonstration.

Si (G_i) est la suite centrale descendante du groupe G et (H'_i) une N-suite quelconque dans le groupe G', on a $f(G_i) \subset H'_i$ pour tout homomorphisme f de G dans G'. De plus, si f est un homomorphisme de G *sur* G', $f(G_i)$ est le $i^{\text{ème}}$ sous-groupe G'_i de la suite centrale descendante de G'. Donc, $\mathfrak{L}(G'_i)$ est isomorphe au quotient de $\mathfrak{L}(G_i)$ par l'idéal associé au noyau de f. C'est ainsi que W. Magnus a défini $\mathfrak{L}(G'_i)$ en considérant G' comme le quotient d'un groupe libre G [23].

Il résulte de la définition de la suite centrale descendante (G_i) d'un groupe G que l'anneau de Lie $\mathfrak{L}(G_i)$ est engendré par ses éléments homogènes de degré 1. La réciproque de cette proposition est exacte en ce qui concerne les N-suites finies des groupes nilpotents :

THÉORÈME (2.5). — *Soit* (H_i) *une* N-*suite,* (G_i) *la suite centrale descendante du groupe* G. *Alors* $\mathfrak{L}(H_i)$ *est engendré par ses éléments homogènes de degré* 1 *si et seulement si, pour tout entier j,* G_j *est* (H_i)-*dense dans* H_j.

---

(6) Ce résultat peut encore s'énoncer ainsi : soit (K_i) la N-suite du noyau N de f définie par $K_i = H_i \cap N$. Alors à la suite exacte $N \to G \to G'$ correspond la suite exacte $\mathfrak{L}(K_i) \to \mathfrak{L}(H_i) \to \mathfrak{L}(H'_i)$ des anneaux de Lie gradués associés.

En effet, la condition pour que $\mathfrak{L}(H_i)$ soit engendré par ses éléments homogènes de degré 1 peut s'écrire $H_j = G_j H_{j+1}$ (pour tout j). On en déduit, par récurrence sur k, $H_j = G_j H_{j+k}$ pour tout k positif, ce qui exprime précisément que G_j est (H_i)-dense dans H_j. Si (H_i) est finie, $H_i = (e)$ à partir d'un certain indice i et $G_j = H_j$ pour tout j.

3. Modules filtrés et N-suites. — Rappelons qu'une filtration décroissante sur un module A est définie par une famille de sous-modules à indices entiers A_i vérifiant :

$$\bigcup_i A_i = A \qquad \text{et} \qquad A_i \supset A_{i+1} \quad \text{pour tout } i.$$

Nous nous bornerons aux filtrations positives, pour lesquelles $A_0 = A$. La filtration $\varphi(x)$ d'un élément x de A est le plus grand entier i tel que $x \in A_i$, ou bien le symbole ∞ si $x \in A_i$ pour tout i. Si A est une algèbre associative (resp. de Lie), on exige de plus que $A_i A_j \subset A_{i+j}$ (resp. $[A_i, A_j] \subset A_{i+j}$) pour tout couple i, j.

La donnée dans A d'une fonction $\varphi(x)$ à valeurs entières ≥ 0 et $+\infty$ définit une filtration si et seulement si :

$$\varphi(x-y) \geq \operatorname{Sup}\big(\varphi(x), \varphi(y)\big), \qquad \varphi(\alpha x) \geq \varphi(x),$$

α étant un élément de l'anneau d'opérateurs du module; enfin $\varphi(xy) \geq \varphi(x) + \varphi(y)$ dans le cas d'une algèbre associative, $\varphi([x, y]) \geq \varphi(x) + \varphi(y)$ dans le cas d'une algèbre de Lie.

On définit à partir d'un module filtré A le module gradué associé noté $\mathcal{G}(A)$: c'est la somme directe $\Sigma_i A_i/A_{i+1}$. Dans le cas d'une algèbre associative ou de Lie, on obtient par passage aux quotients une structure d'algèbre graduée, associative ou de Lie, sur $\mathcal{G}(A)$ (7).

Les N-suites permettent d'étendre aux groupes les constructions sur les modules filtrés, notamment celle du module gradué associé auquel correspond l'anneau de Lie gradué associé. Nous allons montrer comment définir des N-suites à partir d'applications de groupes dans des modules filtrés. Établissons d'abord le :

Théorème (3.1). — *Soit* G *un groupe et* g *une application de* G *dans une algèbre de Lie* L *munie de la filtration* φ, *telle que :*

1° $\varphi\big(g(x)\big) \geq 1$ *pour tout* $x \in G$;

2° $\varphi\big(g(xy^{-1}) - g(x) + g(y)\big) \geq \operatorname{Inf}\Big(\varphi\big(g(x)\big), \varphi\big(g(y)\big)\Big) + 1$ *pour tous* $x, y \in G$;

3° $\varphi\big(g(xyx^{-1}y^{-1}) - [g(x), g(y)]\big) \geq \varphi\big(g(x)\big) + \varphi\big(g(y)\big) + 1$ *pour tous* $x, y \in G$;

alors si l'on définit les parties H_i *de* G *en posant* $x \in H_i$ *si et seulement si* $\varphi\big(g(x)\big) \geq i$,

(7) Pour la notion de filtration, *cf.* J. Leray ou P. Samuel [19], [29].

(H_i) *est une* N-*suite dans* G *et* $\mathfrak{L}(H_i)$ *est canoniquement isomorphe à un sous-anneau de l'algèbre de Lie graduée* $\mathfrak{G}(L)$.

Démonstration. — Il résulte de la définition que $H_i \supset H_{i+1}$, et la condition 1° montre que $H_1 = G$. La condition 2° montre que H_i est un sous-groupe de G, et la condition 3° établit que $(H_i, H_j) \subset H_{i+j}$; (H_i) est donc une N-suite dans G.

Désignons par L_i l'ensemble des éléments de L de filtration $\geqq i$. Soit $x_i \in H_i$; alors $g(x_i) \in L_i$ et, d'après 2°, la classe de $g(x_i) \bmod L_{i+1}$ ne dépend que de la classe de $x_i \bmod H_{i+1}$. D'où, par passage aux quotients, une application $\tilde{g}$ de H_i/H_{i+1} dans L_i/L_{i+1}; la condition 2° appliquée encore une fois montre que $\tilde{g}$ est un isomorphisme de H_i/H_{i+1} dans L_i/L_{i+1}, que nous prolongeons en un isomorphisme $\tilde{g}$ de $\Sigma_i H_i/H_{i+1}$ dans $\Sigma_i L_i/L_{i+1}$; la condition 3° montre alors que $\tilde{g}$ est un isomorphisme pour les structures d'anneau de Lie de $\mathfrak{L}(H_i)$ et de $\mathfrak{G}(L)$.

On démontrerait sans peine que toutes les N-suites de G peuvent s'obtenir par le procédé précédent.

Nous allons appliquer (3.1) au cas où L est l'algèbre de Lie « portée » par une algèbre associative filtrée, c'est-à-dire est obtenue en conservant la structure du module filtré de l'algèbre associative et en y définissant le crochet de Lie par :

$$[x, y] = xy - yx.$$

L'algèbre de Lie graduée associée s'identifie alors à l'algèbre portée par l'algèbre associative graduée associée. Nous pouvons énoncer le

THÉORÈME (3.2). — *Soit* A *une algèbre associative de filtration* v *possédant une unité notée* 1. *Si* f *est un homomorphisme d'un groupe* G *dans le groupe multiplicatif des éléments inversibles de* A *tel que* $v\big(f(x) - 1\big) \geqq 1$ *pour tout* $x \in G$, *alors l'application* $g(x) = f(x) - 1$ *de* G *dans l'algèbre de Lie portée par* A *vérifie les conditions du théorème* (3.1). *On en déduit donc canoniquement une* N-*suite* (H_i) *dans* G *et un isomorphisme de* $\mathfrak{L}(H_i)$ *dans l'anneau de Lie porté par* $\mathfrak{G}(A)$.

Démonstration. — Soient $x, y \in G$; posons

$$f(x) = 1 + a, \qquad f(y) = 1 + b,$$
$$f(x^{-1}) = 1 + a', \qquad f(y^{-1}) = 1 + b', \qquad f(xy^{-1}) = 1 + c, \qquad f(xyx^{-1}y^{-1}) = 1 + d.$$

La condition 1° de (3.1) est satisfaite par hypothèse. Il nous reste à vérifier que :

$$v(c - a + b) \geqq \operatorname{Inf}\big(v(a), v(b)\big) + 1 \quad \text{(condition 2°)}$$

et

$$v(d - ab + ba) \geqq v(a) + v(b) + 1 \quad \text{(condition 3°)}.$$

Puisque f est un homomorphisme,

$$(1 + a)(1 + a') = (1 + b)(1 + b') = 1,$$

d'où

$$(\star) \qquad a + a' + aa' = b + b' + bb' = 0.$$

Nous allons transformer les expressions de

$$c = (1 + a)(1 + b') - 1 \qquad \text{et de} \qquad d = (1 + a)(1 + b)(1 + a')(1 + b') - 1$$

en tenant compte de $(\star)$. Nous obtenons :

$$c = a + b' + ab' = a - b + (a - b)b',$$

et nous sommes ramenés à démontrer

$$v\big((a - b)b'\big) \geqq \mathrm{Inf}\big(v(a), v(b)\big) + 1,$$

ce qui est immédiat puisque $v(b') \geqq 1$. De même

$$\begin{aligned} d &= a + a' + aa' + b + b' \\ &\quad + bb' + ab + ab' + abb' + ba' + a'b' + aba' + aa'b' + ba'b' + aba'b' \\ &= ba' + a'b' + aba' + aa'b' + ba'b' + aba'b' = ab - ba + aba' + abb' - baa' + ba'b' + aba'b'. \end{aligned}$$

Il s'agit donc de démontrer que

$$v(aba' + abb' - baa' + ba'b' + aba'b') \geqq v(a) + v(b) + 1.$$

Chaque terme de la somme considérée a au moins trois facteurs de filtration $\geqq 1$, parmi lesquels l'un est égal à a ou a', et un autre à b ou b' ; comme $v(a') = v(a)$ et $v(b') = v(b)$, la filtration de chaque terme est $\geqq v(a) + v(b) + 1$, ce qui achève la démonstration.

Exemple. — Soit A un module muni de la filtration v, E l'anneau des endomorphismes linéaires de A. Les sous-modules E_i de E, obtenus en posant $x \in \mathrm{E}_i$ si et seulement si $v\big(x(a)\big) \geqq v(a) + i$ pour tout $a \in \mathrm{A}$, définissant dans E une filtration w. Si G est un groupe d'automorphismes du module A tel que $w(g - 1) \geqq 1$ pour tout $g \in \mathrm{G}$, le théorème précédent montre qu'on obtient une N-suite (H_i) dans G en posant $\mathrm{H}_i = \mathrm{G} \cap (1 + \mathrm{E}_i)$. Plus particulièrement : si G est un groupe fini, et A l'anneau des entiers d'un corps valué complet à valuation discrète, alors G est un groupe de ramification, et (H_i) n'est autre que la suite des groupes de ramification supérieurs.

Comme dans le cas, entièrement analogue, d'un groupe muni d'une N-suite, nous définissons pour un module filtré les notions de topologie associée à la filtration, de filtration séparante, de module complété, etc. Si l'homomorphisme f du théorème (3.2) est un isomorphisme, nous pouvons identifier G à son image $f(\mathrm{G})$. Nous avons alors deux topologies sur G : celle induite par la topologie de l'algèbre A (associée à la filtration v), et la (H_i)-topologie, (H_i) désignant la N-suite du théorème (3.2). On vérifie sans peine que ces deux topologies coïncident; il en résulte que, dans le cas où v est une filtration

séparante, (H_i) est une N-suite séparante et le complété de G pour sa (H_i) topologie se trouve plongé canoniquement dans l'algèbre complétée de A.

Nous ne savons pas caractériser intrinsèquement les N-suites obtenues dans un groupe G par le procédé du théorème (3.2). Remarquons qu'on les obtient toutes en se bornant à considérer les filtrations de l'algèbre $Z(G)$ du groupe G à coefficients entiers rationnels. En effet, l'homomorphisme f de (3.2) se prolonge univoquement en un homomorphisme d'anneau $\bar{f}$ de $Z(G)$ dans A; et, si l'on pose $w(y) = v(\bar{f}(y))$ pour tout $y \in Z(G)$, w est une filtration sur $Z(G)$ qui permet d'obtenir la même N-suite (H_i) de G (8).

Terminons ces considérations générales en établissant une relation entre les anneaux de Lie $\mathfrak{L}(H_i)$ et $\mathfrak{L}(K_i)$ associés à deux N-suites (H_i) et (K_i) d'un même groupe G.

Pour cela considérons dans $\mathfrak{L}(H_i) = \Sigma_i H_i/H_{i+1}$ les sous-modules homogènes

$$\mathfrak{L}(H_i)_j = \Sigma_i (H_i \cap K_j) H_{i+1}/H_{i+1}.$$

Les éléments de $\mathfrak{L}(H_i)_j$ sont les éléments de $\mathfrak{L}(H_i)$ dont toutes les composantes homogènes peuvent s'obtenir, par passage aux quotients, à partir d'éléments de K_j. Cela montre que les sous-modules $\mathfrak{L}(H_i)_j$ définissent sur $\mathfrak{L}(H_i)$ une filtration compatible avec sa structure d'anneau de Lie. L'anneau de Lie gradué $\mathcal{G}\mathfrak{L}(H_i)$ associé à $\mathfrak{L}(H_i)$ ainsi filtré est naturellement bigradué, puisque la graduation primitive de $\mathfrak{L}(H_i)$ définit, par passage aux quotients, une graduation sur $\mathfrak{L}(H_i)_j/\mathfrak{L}(H_i)_{j+1}$. Nous dirons pour abréger que $\mathfrak{L}(H_i)$ est filtré à partir de la N-suite (K_j), et nous appellerons $\mathcal{G}\mathfrak{L}(H_i)$ l'anneau de Lie bigradué associé :

THÉORÈME (3.3). — *Soient* (H_i) *et* (K_i) *deux* N-*suites dans le groupe* G. *Considérons l'anneau de Lie* $\mathfrak{L}(H_i)$ *que nous filtrons à partir de la* N-*suite* (K_i), *ainsi que l'anneau de Lie* $\mathfrak{L}(K_i)$ *que nous filtrons à partir de la* N-*suite* (H_i). *Alors les anneaux de Lie bigradués associés :* $\mathcal{G}\mathfrak{L}(H_i)$ *et* $\mathcal{G}\mathfrak{L}(K_i)$ *sont canoniquement isomorphes.*

En effet, $\mathcal{G}\mathfrak{L}(H_i)$ s'identifie au groupe

$$\Sigma_{i,j} (H_i \cap K_j) H_{i+1}/(H_i \cap K_{j+1}) H_{i+1}$$

et de même $\mathcal{G}\mathfrak{L}(K_i)$ s'identifie à

$$\Sigma_{i,j} (K_i \cap H_j) K_{i+1}/(K_i \cap H_{j+1}) K_{i+1}.$$

Or le « lemme de Zassenhaus » classique établit l'isomorphisme des groupes quotients

$$(H_i \cap K_j) H_{i+1}/(H_i \cap K_{j+1}) H_{i+1} \quad \text{et} \quad (K_j \cap H_i) K_{j+1}/(K_j \cap H_{i+1}) K_{j+1}$$

(8) w est l'image réciproque de la filtration v de A par l'homomorphisme $\bar{f}$.

en montrant qu'ils admettent tous deux comme système de représentants un système de représentants quelconque du groupe

$$(H_i \cap K_j)/(H_i \cap K_{j+1})\,(H_{i+1} \cap K_j).$$

Nous voyons ainsi comment établir l'isomorphisme canonique des anneaux de Lie bigradués $\mathcal{GL}(H_i)$ et $\mathcal{GL}(K_i)$ en associant leurs composantes homogènes de degrés respectifs (i, j) et (j, i); l'existence d'un système de représentants communs montre qu'il s'agit bien d'un isomorphisme pour les structures d'anneaux de Lie, puisque les crochets de Lie s'obtiennent à partir des commutateurs dans G par passage aux quotients.

Remarque (3.4). — Nous avons démontré le théorème (3.2) par un calcul direct. Nous aurions pu le faire apparaître comme une conséquence d'un résultat plus profond dû à Kaloujnine ([13], [14]). Soient G un groupe (H_i) une suite de sous-groupes invariants dans G, K le groupe des automorphismes de G. Désignons par L_j la partie de K constituée par les automorphismes qui laissent invariants les groupes quotients H_i/H_{i+j} (c'est-à-dire que $\alpha \in L_j$ équivaut à $\alpha \in K$ et $x^{-1}\alpha(x) \in H_{i+j}$ pour tout entier positif i et tout $x \in H_i$). Alors (L_j) est une N-suite dans le sous-groupe L_1 de K. Pour retrouver le théorème (3.2), il faut identifier le groupe multiplicatif des éléments inversibles de l'anneau avec unité A à un sous-groupe du groupe des automorphismes du groupe additif de A (en considérant les multiplications à gauche).

4. La suite centrale descendante d'un groupe libre. — Soit Ω un anneau commutatif possédant une unité (notée 1), et $(x_\iota)_{\iota \in I}$ une famille d'éléments que nous prenons comme générateurs libres d'une Ω-algèbre associative avec unité, que nous noterons A. A est ainsi l'algèbre des polynomes à coefficients dans Ω par rapport aux « variables » non commutatives (x_ι), ou encore l'algèbre tensorielle du Ω-module libre de base (x_ι). A est porteur d'une graduation naturelle : les scalaires (éléments de Ω) sont de degré 0, les générateurs (x_ι) de degré 1. Nous appellerons *ordre* de $x \in A$, et nous noterons $\omega(x)$ le degré minimum des composantes homogènes non nulles de x; ω est alors une filtration séparante dans A, et, en complétant A pour la topologie associée, nous obtenons $\overline{A}$, algèbre des séries formelles non commutatives par rapport aux (x_ι) à coefficients dans Ω. Par définition, $\overline{A}$ sera appelé *algèbre de Magnus* à coefficients dans Ω et de générateurs $(x_\iota)_{\iota \in I}$. Dans $\overline{A}$, les éléments $1 + x_\iota$ deviennent inversibles $\left((1 + x_\iota)^{-1} = 1 - x_\iota + x_\iota^2 - x_\iota^3 \ldots\right)$ et engendrent donc un groupe multiplicatif G.

Théorème (4.1). — *Dans toute algèbre de Magnus de générateurs* $(x_\iota)_{\iota \in I}$, *les*

éléments $(1+x_\iota)_{\iota\in I}$ *engendrent, par rapport à la multiplication, un groupe libre* G (9).

Il s'agit de démontrer que

$$(1+x_{\iota_1})^{\alpha_1}\dots(1+x_{\iota_r})^{\alpha_r}\neq 1,$$

quand tous les exposants α_i sont des entiers rationnels $\neq 0$ et que deux indices consécutifs quelconques ι_i, ι_{i+1} sont distincts. Nous rapportons A à sa base naturelle constituée pár les produits de x_ι; alors tous les éléments de G ont pour coordonnées des multiples entiers de l'unité dans Ω. Nous pouvons donc nous borner au cas où G est l'anneau Z des entiers rationnels, ou l'anneau Z_n des entiers mod n. Le coefficient de $x_{\iota_1}^{\beta_1}\dots x_{\iota_r}^{\beta_r}$ dans le produit considéré est égal, si tous les exposants β_i sont $\neq 0$, au produit des coefficients binomiaux : $\binom{\alpha_1}{\beta_1}\dots\binom{\alpha_r}{\beta_r}$. Soit p un nombre premier qui sera supposé diviser n dans le cas où $\Omega = Z_n$. Alors, si nous définissons β_i comme la plus grande puissance de p divisant α_i, $\beta_i \geq 1$ et $\binom{\alpha_i}{\beta_i}\not\equiv 0 \pmod p$ (10). Ainsi le produit $\binom{\alpha_1}{\beta_1}\dots\binom{\alpha_r}{\beta_r}$ n'est pas divisible par p et ne peut donc être nul dans Ω, ce qui démontre le théorème.

Nous appliquerons le théorème (3.2) au groupe libre G plongé dans l'algèbre de Magnus $\overline{A}$ filtrée par son ordre. Lorsque $\Omega = Z$, les sous-groupes de la N-suite ainsi obtenue ont été appelés par Magnus « *groupes de dimension* » de G. Witt [33] et Magnus [22] ont établi ultérieurement que cette N-suite coïncidait avec la suite centrale descendante de G.

Lorsque $\Omega = Z_n$, on obtient les « *groupes de dimension* mod n » de G. Ils ont été caractérisés, pour n premier, par Zassenhaus [36]. Nous les étudierons dans le cas général. En tout cas, nous savons que les groupes de dimension constituent toujours des N-suites séparantes des groupes libres. D'où le résultat : tout groupe libre est un N-groupe.

Nous aurons à faire usage de certaines propriétés de l'*algèbre enveloppante universelle d'une algèbre de Lie*. Si L est une algèbre de Lie sur l'anneau commutatif d'opérateurs Ω, une algèbre enveloppante universelle A de L est une Ω-algèbre associative contenant L (comme sous-algèbre de l'algèbre de Lie portée par A), engendrée par L (en tant qu'algèbre associative), et telle que toute représentation linéaire f de L dans une Ω-algèbre associative B puisse

---

(9) Magnus [21].

(10) En effet, posons $\alpha = \beta\gamma$, β étant une puissance de p et γ un entier premier à p. Alors, si $\alpha > 0$,

$$(1+x)^\alpha = \big((1+x)^\beta\big)^\gamma \equiv (1+x^\beta)^\gamma \equiv (1+\gamma x^\beta+\dots) \pmod p.$$

Il en résulte, d'après le développement de $(1+x)^{-1}$, que

$$(1+x)^\alpha \equiv 1+\gamma x^\beta+\dots \pmod p,$$

quel que soit le signe de l'entier α.

être prolongée en un homomorphisme d'algèbres g de A dans B. Ces conditions déterminent A à un isomorphisme canonique près. Nous admettrons l'existence de A lorsque L possède une base sur Ω (Poincaré [28], Witt [33], Birkoff [2])(11); si $(e_\iota)_{\iota\in I}$ est une base de L sur Ω, on obtient une base de A sur Ω formée de monômes par rapport aux e_ι (produits de e_ι) en choisissant un représentant et un seul dans chacune des classes de monômes qui ne diffèrent que par l'ordre des facteurs. En particulier, les puissances e_ι^n ($\iota\in I$, n entier >0) dans A sont linéairement indépendantes sur Ω.

Montrons que dans l'algèbre de Magnus $\overline{A}$ de générateurs $(x_\iota)_{\iota\in I}$ à coefficients dans Ω, la sous-algèbre de Lie L engendré par les (x_ι) est une Ω-algèbre de Lie libre par rapport aux générateurs (x_ι). Soit, en effet, L' une Ω-algèbre de Lie libre par rapport aux générateurs $(y_\iota)_{\iota\in I}$ en correspondance biunivoque avec les (x_ι). L' admet une base sur Ω, donc une algèbre enveloppante A' qui admet les (y_ι) comme générateurs. Soit f l'homomorphisme de L' sur L qui applique chaque y_ι sur x_ι. f se prolonge en un homomorphisme g de A' sur la sous-algèbre A de $\overline{A}$ engendrée par les (x_ι); par définition, A est libre par rapport aux (x_ι), et g est donc biunivoque. Sa restriction f établit donc l'isomorphisme de L et L'.

Soient maintenant $\overline{A}$ l'algèbre de Magnus de générateurs $(x_\iota)_{\iota\in I}$ *à coefficients entiers rationnels*, G le groupe libre engendré par les $(1+x_\iota)$, et (H_i) la N-suite déterminée dans G par la filtration ω de $\overline{A}$ [th. (3.2)]. Si (G_i) désigne la suite centrale descendante de G, il existe d'après (2.2) un homomorphisme canonique de $\mathfrak{L}(G_i)$ dans $\mathfrak{L}(H_i)$ (12). $\mathfrak{L}(G_i)$ est engendré par ses éléments de degré 1, et par conséquent par les classes $\mathrm{mod}\,G_2$ des éléments $(1+x_\iota)$ qui engendrent évidemment G/G_2. L'image canonique $\mathfrak{M}$ de $\mathfrak{L}(G_i)$ dans $\mathfrak{L}(H_i)$ est donc engendrée par les images des classes $\mathrm{mod}\,G_2$ des $(1+x_\iota)$, c'est-à-dire (en traduisant la définition de l'homomorphisme utilisé) par les classes $\mathrm{mod}\,H_2$ des $(1+x_\iota)$, Or, $\mathfrak{L}(H_i)$ s'identifie canoniquement à un sous-anneau de l'anneau de Lie porté par $\mathfrak{G}(\overline{A})$, lequel à son tour s'identifie canoniquement à A. Si nous composons ces identifications, $\mathfrak{L}(H_i)$ devient un sous-anneau de l'anneau de Lie porté par A, et $\mathfrak{M}$ s'identifie au sous-anneau de Lie engendré par les (x_ι) dans A. Nous venons de démontrer que ce sous-anneau est un anneau de Lie libre par rapport aux générateurs (x_ι); cela entraîne que l'homomorphisme de $\mathfrak{L}(G_i)$ sur $\mathfrak{M}$ est biunivoque, ce qui n'est possible, d'après (2.2), que si $G_i = H_i$ pour tout entier i. Nous avons donc le :

THÉORÈME (4.2). — *L'anneau de Lie $\mathfrak{L}(G_i)$ associé à la suite centrale descen-*

(11) L'algèbre enveloppante n'existe pas toujours si L n'a pas de base (Chirchov [3]). Néanmoins, si Ω est un anneau principal (Z ou Z_n, par exemple), l'algèbre enveloppante existe (Lazard) [15].

(12) Associé à l'isomorphisme identique de G sur lui-même.

dante (G_i) *du groupe libre* G *est libre. Un système de générateurs indépendants de* $\mathfrak{L}(G_i)$ *est constitué par les classes* $\bmod G_2$ *d'un système de générateurs indépendants de* G. *Si* G *est identifié au groupe multiplicatif engendré par les* $(1+x_\iota)_{\iota\in I}$ *dans l'anneau de Magnus à coefficients entiers de générateurs* (x_ι), *chaque sous-groupe* G_i *est formé des éléments de* G *dont les composantes homogènes de degré strictement compris entre* 0 *et* i *sont nulles.*

Ce théorème admet une réciproque :

THÉORÈME (4.3). — *Soit* G *un groupe engendré par ses éléments* $(x_\iota)_{\iota\in I}$ *et* (H_i) *une* N-*suite dans* G. *Si les classes* $\bmod H_2$ *des* (x_ι) *constituent, dans l'anneau de Lie* $\mathfrak{L}(H_i)$, *un système de générateurs indépendants d'un sous-anneau de Lie libre, alors* G *est un groupe libre par rapport aux générateurs* (x_ι), *et* (H_i) *est sa suite centrale descendante.*

Considérons, en effet, un groupe libre G′ de générateurs $(y_\iota)_{\iota\in I}$ en correspondance biunivoque avec les (x_ι), et l'anneau de Lie $\mathfrak{L}(G'_i)$ associé à sa suite centrale descendante. A l'homomorphisme f de G′ sur G qui applique chaque y_ι sur x_ι est associé l'homomorphisme $\tilde{f}$ de $\mathfrak{L}(G'_i)$ dans $\mathfrak{L}(H_i)$ qui applique $y_\iota \bmod G'_2$ sur $x_\iota \bmod H_2$. Or, $\mathfrak{L}(G'_i)$ est engendré par les classes $y_\iota \bmod G'_2$ et $\tilde{f}$, qui applique $\mathfrak{L}(G'_i)$ sur un anneau de Lie libre par rapport aux $\tilde{f}(y_\iota \bmod G'_2)$, est donc biunivoque. Cela entraîne, d'après (2.2), $G'_i = f^{-1}(H_i)$ pour tout i. Le noyau de f est contenu dans l'intersection des G'_i, qui se réduit à l'élément neutre puisque G′ est un N-groupe. Ainsi f est un isomorphisme de G′ sur G tel que $H_i = f(G'_i)$ pour tout i, ce qui achève la démonstration.

5. LES p-FILTRATIONS DES ANNEAUX DE MAGNUS. — Soit p un nombre premier. Un module quelconque A est filtré par ses sous-modules $p^i A$ (i entier $\geqq 0$) constitués par les éléments de la forme $p^i x$, où $x \in A$. Nous désignons par $w_p(A; x)$ la filtration correspondante; ainsi $w_p(A; x) = i$ signifie $x \in p^i A$ et $x \notin p^{i+1} A$. Pour simplifier, nous écrirons $w_p(x)$ au lieu de $w_p(A; x)$ lorqu'il ne pourra pas y avoir d'équivoque sur le module A.

Prenons en particulier l'anneau de Magnus $\mathfrak{A}$ de générateurs $(x_\iota)_{\iota\in I}$, à coefficients entiers rationnels. w_p est une filtration séparante dans $\mathfrak{A}$, et le complété $\mathfrak{A}_p$ de $\mathfrak{A}$ pour la topologie associée à w_p s'identifie à l'algèbre de Magnus de générateurs (x_ι) à coefficients entiers p-adiques. Comme précédemment, nous considérerons le groupe libre engendré par les $(1+x_\iota)$ dans le groupe multiplicatif des éléments inversibles de $\mathfrak{A}_p$.

Nous connaissons deux filtrations sur $\mathfrak{A}_p$: w_p et l'ordre ω. Nous allons étudier certaines filtrations v sur $\mathfrak{A}_p$ construites à partir de w_p et de ω, qui devront vérifier les conditions suivantes :

(5.1) α. Si $\Sigma_{0\leq i<\infty} y_i$ est la décomposition de $y\in\mathfrak{A}_{\mathfrak{p}}$ en somme de ses composantes homogènes,

$$0\leq\varphi(y)=\operatorname*{Inf}_{0\leq i<\infty}\varphi(y_i).$$

De plus, si $\omega(y)\geq 1$, $\varphi(y)\geq 1$.

β. Si $y_i\in\mathfrak{A}_{\mathfrak{p}}$ est homogène de degré i, $\varphi(y_i)$ ne dépend que de i et de $w_p(\mathfrak{A}_{\mathfrak{p}}; y_i)$.

La condition α s'énonce encore ainsi : la filtration φ est compatible avec la graduation de $\mathfrak{A}_{\mathfrak{p}}$; $\varphi(x)\geq 0$ pour tout $x\in\mathfrak{A}_{\mathfrak{p}}$ et $\varphi(x_\iota)\geq 1$ pour un générateur quelconque x_ι de $\mathfrak{A}_{\mathfrak{p}}$.

D'après β, si $y\in\mathfrak{A}_{\mathfrak{p}}$ est homogène,

$$\varphi(y)=\mathrm{F}_\varphi\big(\deg y,\ w_p(y)\big),$$

$\mathrm{F}(i, j)$ désignant une fonction déterminée des variables entières ≥ 0, i et j, à valeurs entières ≥ 0 ou $+\infty$.

Réciproquement, pour que la fonction $\mathrm{F}_\varphi(i, j)$ définisse une filtration φ satisfaisant à (5.1), il faut et il suffit que les conditions suivantes soient vérifiées (pour tous entiers $i, j, i', j'\geq 0$) :

$$(5.2)\qquad \begin{cases} 0\leq\mathrm{F}_\varphi(i, j)\leq\infty, \qquad 1\leq\mathrm{F}_\varphi(1, 0),\\ \mathrm{F}_\varphi(i, j)+\mathrm{F}_\varphi(i', j')\leq\mathrm{F}_\varphi(i+i', j+j'). \end{cases}$$

Ces conditions s'obtiennent en explicitant les axiomes généraux des filtrations pour la fonction φ construite à partir de $\mathrm{F}_\varphi(i, j)$ conformément à (5.1).

Nous nous proposons d'étudier les N-suites de G associées (3.2) aux filtrations φ vérifiant (5.1). Nous aurons donc à calculer $\varphi(z-1)$ pour $z\in\mathrm{G}$. A cet effet, nous utiliserons une représentation de z comme produit infini, ce produit convergeant au sens de la topologie associée à la suite centrale descendante (G_i) de G. Rappelons (4.2) que (G_i) est associée à la filtration ω. Si nous convenons de poser $p^\infty=0$ et, par conséquent $z^{p^\infty}=1$ pour $z\in\mathrm{G}$, nous avons le

Lemme (5.3). — *Tout élément $z\in\mathrm{G}$ peut être représenté par un produit de puissances $z=z_1^{p^{k_1}}z_2^{p^{k_2}}\dots z_i^{p^{k_i}}\dots$; les k_i sont égaux à des entiers ≥ 0 ou bien au symbole ∞; pour tout i, $z_i\in\mathrm{G}_i$ et, si $k_i\neq\infty$,*

$$w_p(\mathrm{G}_i/\mathrm{G}_{i+1};\ z_i \bmod \mathrm{G}_{i+1})=0.$$

Supposons déjà définis, pour $1\leq i\leq j-1$, les éléments z_i et les exposants k_i vérifiant les conditions du lemme, et tels que

$$\big(z_1^{p^{k_1}}\dots z_{j-1}^{p^{k_{j-1}}}\big)^{-1}z=z_j'\in\mathrm{G}_j.$$

Si $z'_j \in G_{j+1}$, nous prendrons $k_j = \infty$, d'où $z_j^{\prime p^{k_j}} = 1$; sinon

$$w_p(G_j/G_{j+1}\,;\, z'_j \bmod G_{j+1}) = k_j$$

est fini (puisque G_j/G_{j+1} est un groupe abélien libre), et il existe $z_j \in G_j$ et $z'_{j+1} \in G_{j+1}$, tels que $z'_j = z_j^{p^{k_j}} z'_{j+1}$. Ainsi se poursuit la construction du produit ordonné $\prod_{i=1}^{\infty} z_i^{p^{k_i}}$ qui converge vers z pour la (G_i)-topologie puisque, pour tout entier j, $\prod_{i=1}^{j} z_i^{p^{k_i}} \in z G_{j+1}$.

Nous voyons qu'une grande indétermination subsiste quant aux choix des $z_i^{p^{k_i}}$: une fois choisis les $z_i^{p^{k_i}}$ pour $1 \leqq i \leqq j-1$, k_j est bien déterminé, mais z_j est seulement déterminé $\bmod G_{j+1}$. Néanmoins la donnée d'une suite (k_i) suffit pour calculer $\varphi(z-1)$, φ désignant une filtration satisfaisant à (5.1). Nous caractériserons la filtration φ au moyen de la fonction $F_\varphi(i, j)$ vérifiant (5.2).

Calculons d'abord $\varphi\left(z_i^{p^{k_i}} - 1\right)$, k_i étant fini. Posons

$$z_i = 1 + y_i + t_{i+1},$$

où y_i est la composante homogène de degré i de z_i, et, puisque $z_i \in G_i$, $\omega(t_{i+1}) \geqq i+1$. D'après (4.2), y_i appartient au sous-anneau de Lie L engendré dans $\mathfrak{A}_{\mathbf{p}}$ par ses générateurs (x_ι) et $w_p(G_i/G_{i+1}\,;\, z_i \bmod G_{i+1}) = 0$ équivaut à $w_p(L\,;\, y_i) = 0$. Mais, d'après les propriétés de l'algèbre enveloppante d'une algèbre de Lie, si $y_i \in L$, $w_p(\mathfrak{A}\,;\, y_i) = w_p(L\,;\, y_i)$ et, d'après les propriétés de la complétion p-adique, $w_p(\mathfrak{A}\,;\, y_i) = w_p(\mathfrak{A}_{\mathbf{p}}\,;\, y_i)$. Ainsi finalement $w_p(\mathfrak{A}_{\mathbf{p}}\,;\, y_i) = 0$, et, de même, $w_p(\mathfrak{A}_{\mathbf{p}}\,;\, y_i^r) = 0$ pour tout entier $r \geqq 1$.

D'après (5.1) :

$$\varphi\left((1+y_i)^{p^{k_i}} - 1\right) = \operatorname*{Inf}_{1 \leqq r \leqq p^{k_i}} \varphi\left(\binom{p^{k_i}}{r} y_i^r\right) = \operatorname*{Inf}_{1 \leqq r \leqq p^{k_i}} F_\varphi\left(ir,\, w_p\left(\binom{p^{k_i}}{r}\right)\right).$$

Montrons que

$$\varphi\left(z_i^{p^{k_i}} - (1+y_i)^{p^{k_i}}\right) \geqq \varphi\left((1+y_i)^{p^{k_i}} - 1\right) + 1.$$

En effet :

$$\varphi\left((1+y_i+t_{i+1})^{p^{k_i}} - (1+y_i)^{p^{k_i}}\right) \geqq \operatorname*{Inf}_{1 \leqq r \leqq p^{k_i}} \varphi\left(\binom{p^{k_i}}{r}\left((y_i+t_{i+1})^r - y_i^r\right)\right).$$

Or,

$$\omega\left((y_i+t_{i+1})^r - y_i^r\right) \geqq ir+1,$$

et, par conséquent,

$$\varphi\left(\binom{p^{k_i}}{r}\left((y_i+t_{i+1})^r - y_i^r\right)\right) \geqq F_\varphi\left(ir+1,\, w_p\left(\binom{p^{k_i}}{r}\right)\right) \geqq F_\varphi\left(ir,\, w_p\left(\binom{p^{k_i}}{r}\right)\right) + 1 \geqq \varphi\left((1+y_i)^{p^{k_i}} - 1\right) + 1.$$

Ainsi,

$$\varphi\left(z_i^{p^{k_i}} - 1\right) = \varphi\left((1+y_i)^{p^{k_i}} - 1\right) = \operatorname*{Inf}_{1 \leqq r \leqq p^{k_i}} F_\varphi\left(ir,\, w_p\left(\binom{p^{k_i}}{r}\right)\right).$$

Or, il est bien connu que $w_p\left(\binom{p^{k_i}}{r}\right)=k_i-w_p(r)$. Posons donc $r=p^h s$, avec $(s,p)=1$; ainsi $h=w_p(r)$. Alors $\mathrm{F}_v\left(ir,\ w_p\left(\binom{p^{k_i}}{r}\right)\right)=\mathrm{F}_v(ip^h s,\ k_i-h)$. Mais, si $s>1$;

$$\mathrm{F}_v(ip^h s,\ k_i-h)\geqq \mathrm{F}_v(ip^h,\ k_i-h)+ip^h(s-1)\geqq \mathrm{F}_v(ip^h,\ k_i-h)+1.$$

Cela montre qu'il suffit de donner à r les valeurs $p^h\ (0\leqq h\leqq k_i)$, et nous obtenons :

$$v\left(z_i^{p^{k_i}}-1\right)=\operatorname*{Inf}_{0\leqq h\leqq k_i}\mathrm{F}_v(ip^h,\ k_i-h),$$

$$v\left(z_i^{p^{k_i}}-1-\Sigma_{h=0}^{k_i}\binom{p^{k_i}}{p^h}y_i^{p^h}\right)\geqq v\left(z_i^{p^{k_i}}-1\right)+1.$$

Soit maintenant $z=\Pi_{i=1}^{\infty}z_i^{p^{k_i}}$ comme en (5.3). Nous savons (3.2) que

$$v(z-1)\geqq \operatorname*{Inf}_{1\leqq i<\infty}v\left(z_i^{p^{k_i}}-1\right)=\operatorname*{Inf}_{1\leqq i<\infty;\,0\leqq h\leqq k_i}\mathrm{F}_v(ip^h,\ k_i-h)=c.$$

Montrons que l'on a précisément $v(z-1)=c$. Pour simplifier, le signe $\equiv$ indiquera dans les lignes suivantes une congruence modulo l'idéal constitué par les éléments de $\mathfrak{A}_{\mathbf{p}}$ dont la filtration est au moins égale à $c+1$. Alors :

$$z_i^{p^{k_i}}\equiv 1+\Sigma_{0\leqq h\leqq k_i}\binom{p^{k_i}}{p^h}y_i^{p^h}\qquad\text{et}\qquad z\equiv 1+\Sigma_{\substack{1\leqq i\leqq\infty\\ 0\leqq h\leqq k_i}}\binom{p^{k_i}}{p^h}y_i^{p^h}.$$

Il existe, d'après la définition de c, un couple d'entiers m et n, tels que

$$\mathrm{F}_v(mp^n,\ k_m-n)=c,\quad y_m\neq 0\qquad\text{et}\qquad 0\leqq n\leqq k_m.$$

D'après (5.1), on ne peut avoir $v(z-1)>c$ que si la composante homogène de degré mp^n de z est de filtration $>c$. Cela se traduit par :

$$\Sigma_{\substack{ip^h=mp^n\\ 0\leqq h\leqq k_i}}\binom{p^{k_i}}{p^h}y_i^{p^h}\equiv 0,$$

et, pour montrer l'impossibilité de cette relation, il suffit d'établir que :

$$w_p\left(\Sigma_{ip^h=mp^n}\binom{p^{k_i}}{p^h}y_i^{p^h}\right)=\operatorname*{Inf}_{ip^h=mp^n}w_p\binom{p^{k_i}}{p^h}\leqq k_m-n.$$

Remarquons que les éléments y_i qui apparaissent dans le produit $\Pi_i(1+y_i+t_{i+1})^{p^{k_i}}$ peuvent, éventuellement, ne pas figurer parmi les éléments d'une même base du groupe abélien libre L. Par contre, la condition $w_p(\mathrm{L};y_i)=0$, pour tout i, montre que les y_i peuvent figurer parmi les éléments d'une même base, sur l'anneau des entiers p-adiques, de l'algèbre de Lie $\mathrm{L}_{\mathbf{p}}$ (complétée de L pour la filtration w_p) engendrée dans $\mathfrak{A}_{\mathbf{p}}$ par ses générateurs (x_ι). Mais nous avons vu que la sous-algèbre de $\mathfrak{A}_{\mathbf{p}}$ engendrée par les (x_ι) (dont $\mathfrak{A}_{\mathbf{p}}$ est la complétée pour la filtration ω) est une algèbre enveloppante universelle de $\mathrm{L}_{\mathbf{p}}$. Cela implique, comme nous l'avons rappelé au paragraphe 4, que toutes les puissances entières >0 des y_i peuvent figurer parmi les éléments d'une même base de cette sous-algèbre sur l'anneau des entiers p-adiques. La relation que

nous cherchons à établir en résulte immédiatement. Nous avons donc achevé la démonstration du :

THÉORÈME (5.4). — *Si v est une filtration de $\mathfrak{A}_\mathfrak{p}$ vérifiant* (5.1), *et si $\Pi_i z_i^{p^{k_i}}$ est une représentation comme produit de $z \in G$ vérifiant les conditions de* (5.3), *alors $v(z-1) = \operatorname{Inf} F_v(ip^h, k_i - h)$, la borne inférieure étant prise pour tous les couples d'entiers i, h tels que $1 \leq i$ et $0 \leq h \leq k_i$.*

Il est évident que n'importe quelle représentation de z comme produit doit conduire à la même valeur de $v(z-1)$. La borne inférieure figurant dans (5.4) est donc un invariant de toutes les suites (k_i) apparaissant dans les représentations d'un même $z \in G$.

Nous pouvons maintenant déterminer les sous-groupes de la N-suite $(H_{i,v})$ de G associée à la filtration v d'après (3.2). Par définition, $z \in H_{i,v}$ équivaut à $v(z-1) \geq i$, ou encore (5.4) :

$$F_v(jp^h, k_j - h) \geq i \qquad \text{pour} \quad 1 \leq j \quad \text{et} \quad 0 \leq h \leq k_j,$$

si $z = \Pi_{j=1}^{\infty} z_j^{p^{k_j}}$ est une représentation quelconque de z comme en (5.3). Pour i et j fixes, désignons par $\Phi_v(i, j)$ le plus petit entier k tel que $F_v(jp^h, k-h) \geq i$ pour tout h tel que $0 \leq h \leq k$, ou bien le symbole ∞ si de tels entiers n'existent pas. Nous pouvons alors énoncer le :

THÉORÈME (5.5). — *Le $i^{ième}$ sous-groupe $H_{i,v}$ de la* N*-suite de* G *associée à la filtration v vérifiant* (5.1) *est de la forme :*

$$H_{i,v} = \Pi_{j=1}^{\infty} G_j^{p^{\Phi_v(i,j)}}.$$

Autrement dit si le produit $z = \Pi_{j=1}^{\infty} z_j^{p^{\Phi_v(i,j)}}$ appartient à G *et si chaque $z_j \in G_j$ alors $z \in H_{i,v}$; réciproquement, si $\Pi_{j=1}^{\infty} z_j^{p^{k_i}}$ est une représentation de $z \in H_{i,v}$ vérifiant les conditions de* (5.3), *$k_j \geq \Phi_v(i, j)$ pour tout j.*

Nous sommes maintenant en mesure de déterminer les « groupes de dimension modulo p^h » d'un groupe libre, définis à partir de l'algèbre de Magnus $\mathfrak{A}_{p^h}$ à coefficients dans l'anneau Z_{p^h} des entiers mod p^h. Il revient au même d'introduire dans $\mathfrak{A}_\mathfrak{p}$ la filtration définie par $F_h(i, j) = \infty$ si $j \geq h$ et $F_h(i, j) = i$ si $0 \leq j \leq h-1$, car le quotient de $\mathfrak{A}_\mathfrak{p}$ par l'ensemble de ses éléments de filtration ∞ s'identifie alors à $\mathfrak{A}_{p^h}$. Un calcul très simple nous montre que

$$\operatorname*{Inf}_{0 \leq r \leq k} F_h(ip^r, k-r) = i \qquad \text{si} \quad k < h$$

ou bien

$$\operatorname*{Inf}_{\leq r \leq k} F_h(ip^r, k-r) = ip^{(k-h+1)} \qquad \text{si} \quad k \geq h.$$

Nous pouvons écrire dans les deux cas :

$$\operatorname*{Inf}_{0\leq r\leq k} \mathrm{F}_h(ip^r,\ k-r) = ip^{(k-h+1)^+},$$

en posant selon l'usage $n^+ = \mathrm{Sup}\,(n,\ 0)$. D'où :

THÉORÈME (5.6). — *Le $i^{ième}$ sous-groupe de dimension de* $\mathrm{G} \bmod p^h$, *noté* G_{i,p^h} *est constitué par les éléments* $z \in \mathrm{G}$ *dont les représentations* (5.3) $\Pi_{j=1}^{\infty} z_j^{p^{k_j}}$ *vérifient* $jp^{(k_j-h+1)^+} \geqq i$ *pour tout* j.

Dans le cas où $h = 1$, on obtient les groupes de dimension $\bmod p$, déterminés par Zassenhaus [36].

Ces N-suites correspondant aux différentes valeurs de l'exposant h se déduisent facilement les unes des autres. Ainsi, si $h < h'$:

$$\mathrm{G}_{j,p^{h'}} = \mathrm{G}_{jp^{h'-h},p^h}\mathrm{G}_j \tag{5,7}$$

et, en particulier,

$$\mathrm{G}_{j,p^h} = \mathrm{G}_{jp^{h-1},p}\mathrm{G}_j.$$

En effet, si $z = \Pi_i z_i^{p^{k_i}} \in \mathrm{G}_{j,p^{h'}}$, nous avons, pour tout i tel que $1 \leq i \leq j-1$:

$$ip^{(k_i-h'+1)^+} \geqq j, \qquad \text{donc} \quad ip^{(k_i-h'+1)} \geqq j,$$

ce qui équivaut à : $ip^{(k_i-h+1)} \geqq jp^{h'-h}$. Ainsi

$$\Pi_{i=1}^{j-1} z_i^{p^{k_i}} \in \mathrm{G}_{jp^{h'-h},p^h}, \qquad \text{d'où} \qquad \mathrm{G}_{j,p^{h'}} \subset \mathrm{G}_{jp^{h'-h},p^h}\mathrm{G}_j$$

et l'on montre de même que

$$\mathrm{G}_{j,p^{h'}} \supset \mathrm{G}_{jp^{h'-h},p^h}\mathrm{G}_j.$$

Le théorème (5.4) nous permet de déterminer une N-suite dans G chaque fois que nous avons une fonction $\mathrm{F}(i,j)$ vérifiant les conditions (5.2). Prenons, en particulier, $\mathrm{F}(i,j) = ri + sj$ (r et s entiers $\geqq 1$). Nous aurons d'abord à calculer

$$\operatorname*{Inf}_{0\leq h\leq k} \mathrm{F}(ip^h,\ k-h) = \operatorname*{Inf}_{0\leq h\leq k} rip^h + s(k-h).$$

Si p, r et s sont fixes, la borne inférieure est atteinte pour $h = 0$ si i est suffisamment grand $\left(\text{en tout cas si } i \geqq \frac{s}{r\log p}\right)$; des irrégularités apparaissent pour les petites valeurs de i.

Prenons d'abord $r = s = 1$. Alors la borne inférieure est $i+k$, quels que soient i et p. Par conséquent $v(z-1) = \operatorname*{Inf}_{1\leq i}(k_i+i)$ et :

(5.8) La N-suite de G associée à la filtration définie par $\mathrm{F}(i,j) = i+j$ est composée des sous-groupes $\mathrm{H}_i = \mathrm{G}_1^{p^{i-1}}\mathrm{G}_2^{p^{i-2}}\ldots\mathrm{G}_i$.

Soit maintenant $\mathrm{F}(i,j) = i+2j$. Alors nous avons

$$\operatorname*{Inf}_{0\leq h\leq k}\left(ip^h + 2(k-h)\right) = i+2k,$$

sauf pour $p=2$, $i=1$, où $\operatorname{Inf}_{0\leq h\leq k} 2^h+2(k-h)=2k$. Désignons par $\{x\}$ le plus petit entier $\geq x$, de sorte que $\{x\}-1<x\leq\{x\}$. Alors :

(5.9) La N-suite de G associée à la filtration définie par $F(i,j)=i+2j$ est composée des sous-groupes $K_i=G_1^{p^{\left\{\frac{i-1}{2}\right\}}}G_2^{p^{\left\{\frac{i-2}{2}\right\}}}\dots G_j^{p^{\left\{\frac{i-j}{2}\right\}}}\dots G_i$ si p est impair, et $K_i=G_1^{2^{\left\{\frac{i}{2}\right\}}}G_2^{2^{\left\{\frac{i-2}{2}\right\}}}\dots G_j^{2^{\left\{\frac{i-j}{2}\right\}}}\dots G_i$ pour $p=2$.

Les filtrations que nous venons d'étudier vérifient, outre (5.1), la condition :

$$(5.10)\qquad F(i,0)<\infty \quad\text{et}\quad \lim_{j\to\infty}F(i,j)=\infty \qquad\text{pour tout}\quad i\geq 1.$$

$F(i,0)<\infty$ pour tout i est la condition nécessaire et suffisante pour que la N-suite (H_i) associée à la filtration considérée soit séparante ; $\lim_{j\to\infty}F(i,j)=\infty$ est la condition pour que z^{p^h} tende vers 1 [au sens de la (H_i)-topologie] quand h tend vers ∞, quel que soit $z\in G$. Nous appellerons désormais *p-filtrations* les filtrations de $\mathfrak{A}_p$ vérifiant (5.1) et (5.10).

Théorème (5.11).— *Toutes les* N*-suites de* G *associées aux p-filtrations définissent sur G la même topologie, que nous appellerons la* p-topologie de G.

Soient, en effet, φ et φ' deux p-filtrations de $\mathfrak{A}_p$, (H_i) et (H'_i) les N-suites qui leur sont respectivement associées. Nous devons montrer que pour tout $i\geq 1$ on peut trouver un j tel que $H'_j\subset H_i$. Soit $z=\Pi_r z_r^{p^{k_r}}$ comme en (5.3). $z\in H_i$ équivaut à $k_r\geq\Phi_\varphi(i,r)$ pour $1\leq r\leq i-1$, puisque $\Phi_\varphi(i,r)=0$ pour $r\geq i$ (5.5). Or la condition (5.10), vérifiée par φ et φ', montre que $\Phi_\varphi(i,r)<\infty$ pour tous $i.r$ et que $\lim_{j\to\infty}\Phi_{\varphi'}(j,r)=\infty$ pour tout r fixe. On peut donc choisir j assez grand pour que $\Phi_{\varphi'}(j,r)\geq\Phi_\varphi(i,r)$ pour tout r, c'est-à-dire pour que $H'_j\subset H_i$.

Remarquons que les p-filtrations ne définissent pas toutes sur $\mathfrak{A}_p$ la même topologie, puisque certaines des topologies associées ne sont pas séparées [*cf.* (5.6)]. Par contre, toutes les p-filtrations *séparantes* de $\mathfrak{A}_p$ [caractérisées par $F(i,j)\leq\infty$ pour tous $i,j<\infty$] définissent sur $\mathfrak{A}_p$ une même topologie qu'on peut caractériser ainsi : on considère $\mathfrak{A}_p$ comme le produit direct de ses composantes homogènes ; on prend sur chaque composante la topologie p-adique et sur $\mathfrak{A}_p$ la topologie produit (rappelons que si l'on prenait sur chaque composante la topologie discrète on obtiendrait sur $\mathfrak{A}_p$ la topologie associée à l'ordre). Il résulte de cette interprétation que $\mathfrak{A}_p$ est complet (comme produit de groupes complets) pour la topologie associée à une p-filtration séparante [par exemple $w_p+\omega$, comme en (5.8)]. Ainsi le complété $\overline{G}_p$ de G pour sa p-topologie se trouve plongé canoniquement dans $\mathfrak{A}_p$, et c'est pour cette raison que nous avons pris comme anneau de base l'anneau des entiers p-adiques et non l'anneau des entiers rationnels.

Ce résultat s'établit plus simplement en considérant toutes les algèbres de

Magnus $\mathfrak{A}_{p^h}$ à coefficients dans Z_{p^h} (anneau des entiers mod p^h) obtenues comme quotients de $\mathfrak{A}_{\mathbf{p}}$: $\mathfrak{A}_{p^h} = \mathfrak{A}_{\mathbf{p}}/p^h\mathfrak{A}_{\mathbf{p}}$. Nous avons alors le diagramme d'homomorphismes suivant :

$$\mathfrak{A}_p \leftarrow \mathfrak{A}_{p^2} \leftarrow \ldots \leftarrow \mathfrak{A}_{p^h} \leftarrow \ldots \leftarrow \mathfrak{A}_{\mathbf{p}},$$

qui fait apparaître $\mathfrak{A}_{\mathbf{p}}$ comme la limite projective des $\mathfrak{A}_{p^h}$. Plus précisément, si l'on prend sur chaque $\mathfrak{A}_{p^h}$ la topologie associée à l'ordre, la topologie ainsi définie sur leur limite projective $\mathfrak{A}_{\mathbf{p}}$ coïncide avec la topologie définie par une p-filtration séparante. Chacune des algèbres de Magnus contient une image isomorphe du groupe libre $G \subset \mathfrak{A}_{\mathbf{p}}$, ainsi que de son complété $\overline{G}_p$ pour la p-topologie. Les isomorphismes de ces différents groupes les uns sur les autres sont induits par les homomorphismes des algèbres $\mathfrak{A}_{p^h}$ les unes sur les autres, et il en résulte à nouveau que la limite projective $\mathfrak{A}_{\mathbf{p}}$ contient $\overline{G}_p$. L'anneau des entiers p-adiques apparaît ainsi plus naturellement comme limite projective des anneaux Z_{p^h}.

Si G a un nombre fini de générateurs, les groupes G_i/G_{i+1} sont des groupes abéliens libres de dimensions finies d_i (*cf.* Witt [33]). Alors si (H_i) est la N-suite associée à une p-filtration v, G/H_i est, pour tout i, un p-groupe fini. En effet, $G_i \subset H_i$ et une formule connue de la théorie des groupes donne, pour le calcul des indices :

$$(G:H_i) = (G_1:H_iG_2)\,(G_2:H_iG_3 \cap G_2)\ldots(G_j:H_iG_{j+1} \cap G_j)\ldots(G_{i-1}:H_i \cap G_{i-1});$$

or, d'après (5.5),

$$(G_j:H_iG_{j+1} \cap G_j) = p^{d_j\Phi_v(i,j)}.$$

Par conséquent :

$$(G:H_i) = p^{\sum_j d_j\Phi_v(i,j)}. \tag{5.12}$$

Le complété $\overline{G}_p$ de G peut s'identifier à la limite projective des groupes finis G/H_i (munis de la topologie discrète). Il est donc compact. Soit, d'autre part, N un sous-groupe invariant de G tel que G/N soit un p-groupe fini. Alors G/N est nilpotent ; si c est sa classe, $G_{c+1} \subset N$. Si p^h est l'ordre maximum d'un élément de G/N, $z^{p^h} \in N$ pour tout $z \in G$; donc (5.6) $G_{c+1,\,p^{h+1}} \subset N$, ce qui montre que N est un sous-groupe invariant ouvert de G. Réciproquement, tout sous-groupe invariant ouvert N de G est tel que G/N soit un p-groupe fini. Si n est le nombre des générateurs de G, on peut considérer que les p-groupes finis ayant n générateurs déterminés forment une catégorie partiellement ordonnée : si les générateurs de G_1 et G_2 sont respectivement $e_1, \ldots, e_n$ et $f_1, \ldots, f_n$, on pose $G_1 \leqq G_2$ s'il existe un homomorphisme, nécessairement unique, de G_2 sur G_1 appliquant f_i sur e_i. Nous pouvons alors prendre la limite projective de ces p-groupes finis, qui s'identifie à $\overline{G}_p$. Le groupe compact $\overline{G}_p$ apparaît dans la théorie de Shafarevitch [32] comme le groupe de Galois de la p-extension maximale d'un corps $\mathfrak{p}$-adique ne contenant pas les racines $p^{\text{ièmes}}$ de l'unité.

Les sous-groupes H_i d'une N-suite obtenue à partir d'une p-filtration dans un groupe libre sont entièrement définis à partir des sous-groupes G_i et de la fonction $F_p(i, j)$. Si f est un homomorphisme de G sur un groupe G', l'image directe $(f(H_i))$ de la N-suite (H_i) de G est une N-suite dans G', construite par le même procédé à partir des sous-groupes de la suite centrale descendante de G' et, par conséquent, ne dépend que de $F_p(i, j)$, et non pas de G ni de f. C'est ainsi, par exemple, que nous pouvons parler des groupes de dimension $\bmod p^h$ dans un groupe G' quelconque. Remarquons que dans le cas où G' est un p-groupe fini, les groupes de dimension $\bmod p^h$ se confondent avec les sous-groupes de la suite centrale descendante dès que h est suffisamment grand.

6. Algèbres de Lie restreintes et N-suites restreintes. — Nous nous proposons d'abord d'étudier l'anneau de Lie $\mathfrak{L}(G_{i,p})$ associé à la N-suite $(G_{i,p})$ des groupes de dimension $\bmod p$ d'un groupe libre G (p désigne comme précédemment un nombre premier fixe). La N-suite $(G_{i,p})$ est obtenue par le procédé du théorème (3.2) en plongeant G dans l'algèbre de Magnus $\mathfrak{A}_p$ (à coefficients dans le corps Z_p des entiers $\bmod p$) filtrée par l'ordre ω. L'algèbre graduée $\mathfrak{G}(\mathfrak{A}_p)$, associée à l'algèbre filtrée $\mathfrak{A}_p$, s'identifie canoniquement à l'algèbre associative libre de générateurs $(x_\iota)_{\iota\in I}$ contenue dans $\mathfrak{A}_p$ (et obtenue en prenant les éléments qui n'ont qu'un nombre fini de composantes homogènes non nulles). $\mathfrak{L}(G_{i,p})$ s'identifie, d'après (3.2), à une sous-algèbre de Lie homogène de $\mathfrak{A}_p$, que nous désignerons par R. R contient déjà la sous-algèbre de Lie libre L, engendrée dans $\mathfrak{A}_p$ par les générateurs (x_ι) qui correspondent aux classes $\bmod G_{2,p}$ des générateurs $(1+x_\iota)$ de G. Plus précisément, ce sont les classes $\bmod G_{i+1,p}$ des éléments z_i de G_i tels que $w_p(G_i/G_{i+1}\,;\, z_i \bmod G_{i+1}) = 0$ qui ont pour images canoniques les éléments homogènes de degré i de L ; autrement dit, ces éléments z_i s'écrivent dans $\mathfrak{A}_p$ sous la forme $z_i = 1 + y_i + t_{i+1}$, avec $y_i \in L$, $y_i \neq 0$ et $\omega(t_{i+1}) \geqq i+1$. Alors

$$z_i^{p^k} = 1 + y_i^{p^k} + t_{ip^k+1}, \qquad \text{avec} \quad \omega(t_{ip^k+1}) \geqq ip^k + 1.$$

Il nous suffit d'appliquer (5.6) pour obtenir le :

Théorème (6.1) — *Soit $i = jp^h$, j étant premier à p. Alors les éléments homogènes de degré i de la sous-algèbre de Lie* R *de $\mathfrak{A}_p$, à laquelle nous avons identifié $\mathfrak{L}(G_{i,p})$, sont les éléments de la forme :*

$$y_{jp^h} + y'_{jp^{h-1}} + \ldots + y'^{p^{h-1}}_{jp} + y'^{p^h}_{j},$$

où y_{jp^r} désigne un élément homogène de degré jp^r appartenant à L, *sous-algèbre de Lie engendrée par les générateurs $(x_\iota)_{\iota\in I}$ dans $\mathfrak{A}_p$.*

Le fait que R soit une sous-algèbre de Lie dans un algèbre associative libre sur Z_p nous conduit à retrouver les propriétés fondamentales des algèbres de

Lie *retreintes* sur un corps de caractéristiques p, dont la théorie est due à N. Jacobson [11]. Supposons pour simplifier que les générateurs (x_ι) soient au nombre de deux, notés x et y. Alors, puisque $p+1$ n'est pas divisible par p et que $[x, y^p] \in R$, nous devons avoir $[x, y^p] \in L$. $[x, y^p]$ est homogène de degré 1 par rapport à x et de degré p par rapport à y; il ne peut donc être égal qu'à $[\ldots[[x, y], y], \ldots y]$ (p fois), multiplié par un scalaire dont on vérifie immédiatement qu'il est égal à 1. Si $ad\,y$ désigne l'endomorphisme défini par $x \to [x, y]$, nous avons :

$$(6.2) \qquad ad\,(y^p) = (ad\,y)^p,$$

résultat valable dans toute algèbre associative sur un corps de caractéristique p, et d'ailleurs aisé à vérifier directement.

Considérons maintenant $x^p + y^p \in R$. D'après (6.1), il existe α et $\beta \in Z_p$, tels que $x^p + y^p - (\alpha x + \beta y)^p \in L$. En égalant les coefficients de x^p et de y^p, on obtient immédiatement $\alpha = \beta = 1$. Ainsi :

(6.3) *Identité de Jacobson* [10] :

$$(x+y)^p = x^p + y^p + \Lambda_p(x, y), \qquad \text{où} \quad \Lambda_p(x, y) \in L.$$

$\Lambda_p(x, y)$ est un élément de l'algèbre de Lie de générateurs x et y à coefficients dans Z_p. On peut donc calculer $\Lambda_p(x, y)$ dans toute algèbre de Lie sur un corps de caractéristique p. L'identité (6.3) est ainsi valable dans toute algèbre associative sur un corps de caractéristique p. (Pour un calcul plus explicite de $\Lambda_p(x, y)$, d'après un procédé de E. Artin, *cf.* Zassenhaus [35]).

A cette identité de Jacobson correspond dans un groupe une identité de P. Hall: soit G le groupe libre engendré par x et y. Alors d'après (5.6) $x^p y^p \in G_{p,p}$, ce qui implique :

$$(6.4) \qquad x^p y^p = (xy)^p z_2^p \ldots z_{p-1}^p z_p, \qquad \text{où} \quad z_i \in G_i \qquad (2 \leq i \leq p).$$

Une algèbre de Lie *restreinte* $\mathfrak{L}$ sur un corps k de caractéristique p est, par définition, une algèbre de Lie telle qu'à tout élément $x \in \mathfrak{L}$ se trouve associé un élément $x^{[p]} \in \mathfrak{L}$, pour lequel $ad(x^{[p]}) = (ad\,x)^p$. Cette conditition détermine univoquement $x^{[p]}$ si le centre de $\mathfrak{L}$ est réduit à (0); sinon $x^{[p]}$ est seulement déterminé modulo le centre. Nous exigerons donc de plus que $(\lambda x)^{[p]} = \lambda^p x^{[p]}$ pour $\lambda \in k$, et que

$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + \Lambda_p(x, y);$$

$x^{[p]}$ est alors déterminé pour tout $x \in \mathfrak{L}$ dès qu'il est connu pour les éléments d'une base de $\mathfrak{L}$ sur k. Réciproquement, la donnée d'éléments $e_\nu^{[p]}$ tels que

$$ad(e_\nu^{[p]}) = (ad\,e_\nu)^p,$$

où e_ν parcourt les éléments d'une base de $\mathfrak{L}$ sur k détermine bien une structure d'algèbre de Lie restreinte sur k.

Une représentation linéaire *restreinte* f d'une algèbre de Lie restreinte dans une algèbre associative A devra vérifier, en plus des conditions générales d'une représentation linéaire, $f(x^{[p]})=(f(x))^p$. On en déduit la notion d'algèbre enveloppante restreinte universelle d'une algèbre de Lie restreinte, et la construction d'une base de cette algèbre [11]. Comme dans le cas des algèbres de Lie ordinaires, on démontre que la sous-algèbre de Lie restreinte engendrée par les générateurs d'une algèbre associative libre est libre (*cf.* § 4). Nous pouvons donc énoncer le :

THÉORÈME (6.5). — *L'algèbre de Lie* $\mathfrak{L}(G_{i,p})$ *associée à la* N*-suite des groupes de dimension* mod$p$ *d'un groupe libre* G *de générateur* $(x_\iota)_{\iota\in I}$ *est l'algèbre de Lie restreinte libre à coefficients entiers* mod$p$ *ayant pour générateurs les classes des* (x_ι) mod $G_{2,p}$.

Définition. — Nous appellerons N-suite restreinte dans un groupe G une N-suite (H_i) telle que, pour tout $x\in H_i$, $x^p\in H_{ip}$ (p désignant toujours le même nombre premier fixe).

Nous montrerons que si (H_i) est une N-suite restreinte, $\mathfrak{L}(H_i)$ est, canoniquement, une algèbre de Lie restreinte sur Z_p [il est évident que $\mathfrak{L}(H_i)$ est une algèbre sur Z_p, puisque tout élément non nul de H_i/H_{i+1} est d'ordre p]. Démontrons d'abord un résultat qui précise (3.2).

THÉORÈME (6.6). — *Soient* A *une algèbre associative sur le corps* Z_p *des entiers* mod$p$ *possédant une unité notée* 1 *et munie d'une filtration* v; G *un groupe,* f *un homomorphisme de* G *dans le groupe multiplicatif des éléments inversibles de* A, *tel que* $v(f(x)-1)\geqq 1$ *pour tout* $x\in G$. *Alors la* N*-suite* (H_i), *définie en posant* $x\in H_i$ *si et seulement si* $v(f(x)-1)\geqq i$, *est une* N*-suite restreinte. Si* $\tilde{x}_i$ *désigne généralement la classe* mod H_{i+1} *de* $x_i\in H_i$, *la correspondance* $\tilde{x}_i\to\tilde{x}_i^p=\widetilde{x_i^p}$ *est bien déterminée, et définit sur* $\mathfrak{L}(H_i)$ *une structure d'algèbre de Lie restreinte sur* Z_p. *L'isomorphisme canonique de* $\mathfrak{L}(H_i)$ *dans* $\mathfrak{G}(A)$ *est en même temps une représentation restreinte.*

Démonstration. — Soit $x_i\in H_i$; alors $v(f(x_i)-1)\geqq i$. Mais

$$v(f(x_i^p)-1)=v(f(x_i)^p-1)=v\big((f(x_i)-1)^p\big)\geqq ip.$$

Donc $x_i^p\in H_{ip}$ et (H_i) est une N-suite restreinte. Soit de plus $x_i'\in H_{ip}$; $x_i=\tilde{x}_i'$ équivaut à $v(f(x_i)-f(x_i'))\geqq i+1$. Dans ce cas,

$$f(x_i^p)-f(x_i'^p)=(f(x_i))^p-(f(x_i'))^p=\big(f(x_i')+(f(x_i)-f(x_i'))\big)^p-(f(x_i'))^p$$

et, par conséquent,

$$v(f(x_i^p)-f(x_i'^p))\geqq ip+1,$$

ce qui signifie que $\widetilde{x_i^p} = \widetilde{x_i'^p}$, en considérant x_i^p et $x_i'^p$ comme des éléments de H_{ip}. L'application $\tilde{x}_i \to \widetilde{x_i^p} = \tilde{x}_i^p$ est donc bien déterminée, et, en appelant φ l'isomorphisme canonique de $\mathfrak{L}(H_i)$ dans $\mathfrak{G}(A)$, le calcul précédent montre que $\varphi(\tilde{x}_i^p) = (\varphi(\tilde{x}_i))^p$. Ainsi $\tilde{x}_i^p$ définit sur $\mathfrak{L}(H_i)$ une structure d'algèbre de Lie restreinte sur Z_p; on doit étendre la définition de x^p aux éléments non homogènes au moyen de

$$(x+y)^p = x^p + y^p + \Lambda_p(x, y),$$

et φ est une représentation restreinte.

Toute N-suite restreinte ainsi obtenue à partir d'un homomorphisme de G dans une Z_p-algèbre associative A peut aussi s'obtenir en prenant sur l'algèbre $Z_p(G)$ du groupe G à coefficient dans Z_p l'image réciproque de la filtration de A par l'homomorphisme associé de $Z_p(G)$ dans A. Nous allons établir la réciproque de (6.6), c'est-à-dire :

THÉORÈME (6.7). — *Toute* N*-suite restreinte de* G *peut être obtenue par le procédé du théorème* (6.6) *à partir d'une filtration convenable de* $Z_p(G)$.

D'où en appliquant (6.6), le :

COROLLAIRE (6.8). — *Si* (H_i) *est une* N*-suite restreinte dans le groupe* G, $\mathfrak{L}(H_i)$ *est, canoniquement, une algèbre de Lie restreinte sur* Z_p *avec* $\tilde{x}_i^p = \widetilde{x_i^p}$.

Démonstration. — Soit G un groupe, (H_i) une N-suite restreinte dans G. Nous avons seulement à démontrer (6.7) dans le cas où (H_i) est séparante : il nous suffira ensuite de prendre l'image réciproque dans $Z_p(G)$ d'une filtration convenable de $Z_p(G/H)$, où $H = \bigcap_i H_i$, par l'homomorphisme canonique de $Z_p(G)$ sur $Z_p(G/H)$. Supposons donc $\bigcap_i H_i = (1)$. Pour tout $x \in G$, nous définirons $w(x)$ par $x \in H_{w(x)}$ et $x \notin H_{w(x)+1}$. Ainsi $1 \leqq w(x) < \infty$, sauf si $x = 1$. Nous cherchons une filtration sur $Z_p(G)$ telle que $v(x-1) = w(x)$ pour tout $x \in G$. Or, dans l'algèbre $A = Z_p(G)$, les sous-modules A_i constitués par les sommes d'élément de la forme $(z_1 - 1)(z_2 - 1)\dots(z_r - 1)$, où $z_j \in G$ et $\Sigma_{j=1}^{r} w(z_j) \geqq i$ définissent une filtration v (il est évident que $A_i A_j \subset A_{i+j}$), et $v(x-1) \geqq w(x)$ pour $x \in G$. Si v' est une filtration de A vérifiant $v'(x-1) \geqq w(x)$ pour tout $x \in G$, on a $v'(y) \geqq v(y)$ pour tout $y \in A$. Nous sommes donc ramené à démontrer que $v(x-1) = w(x)$ pour tout $x \in G$.

Choisissons une famille (x_ι) d'éléments de G, où ι parcourt l'ensemble bien ordonné I, possédant les propriétés suivantes : si $w(x_\iota) < w(x_\lambda)$, on a $\iota < \lambda$; les classes $\bmod H_{i+1}$ des x_ι tels que $w(x_\iota) = i$ forment une base du Z_p-module H_i/H_{i+1} pour tout entier $i \geqq 1$. Pour construire une telle famille, il suffit de prendre, pour chaque i, une famille de représentants d'une base bien ordonnée de H_i/H_{i+1}, et d'ordonner leur réunion en accord avec la première condition.

Nous supposons désormais que la N-suite restreinte (H_i) est finie, c'est-à-dire que $H_n=(1)$ pour un certain entier n. Alors tout élément z de G s'écrit, d'une manière et d'une seule, sous la forme

$$z=x_{\iota_1}^{\alpha_1}x_{\iota_2}^{\alpha_2}\dots x_{\iota_r}^{\alpha_r}, \qquad \text{avec} \quad \iota_1<\iota_2<\dots<\iota_r \quad \text{et} \quad 0\leqq\alpha_s\leqq p-1 \quad (\text{pour } 1\leqq s\leqq r).$$

La démonstration procède par récurrence modG_i [*cf.* (5.3)]. Nous écrivons $z=\Pi_\iota x_\iota^{h_\iota}$, où tous les h_ι sont nuls, sauf pour $\iota=\iota_1, \dots, \iota_r$ et où $0\leqq h_\iota\leqq p-1$. Les facteurs sont ordonnés dans l'ordre croissant, de gauche à droite. Montrons qu'une base de A sur Z_p est constituée par les éléments $\Pi_\iota(x_\iota-1)^{h_\iota}$, où les familles d'exposants $(h_\iota)_{\iota\in I}$ sont caractérisées par $0\leqq h_\iota\leqq p-1$ pour tout ι et $h_\iota=0$ sauf pour un nombre fini d'indices ι. En écrivant

$$x_\iota^{h_\iota}=\big(1+(x_\iota-1)\big)^{h_\iota}=\Sigma_{r=0}^{h_\iota}\binom{h_\iota}{r}(x_\iota-1)^r,$$

et en remplaçant chaque $x_\iota^{h_\iota}$ par son développement dans le produit $z=\Pi_\iota x_\iota^{h_\iota}$, nous voyons que tout $z\in G$ est une combinaison linéaire des $\Pi_\iota(x_\iota-1)^{h_\iota}$ qui engendrent donc A. D'autre part, $\Sigma_{(h_\iota)}a_{(h_\iota)}\Pi_\iota(x_\iota-1)^{h_\iota}$ (où tous les $a_{(h_\iota)}$ sont nuls sauf un nombre fini) ne peut être nul que si les coefficients $a_{(h_\iota)}\in Z_p$ sont nuls. En effet, ordonnons lexicographiquement les familles (h_ι), c'est-à-dire, posons $(h_\iota)<(k_\iota)$ s'il existe $\lambda\in I$ tel que $h_\iota=k_\iota$ pour $\iota<\lambda$, et $h_\lambda<k_\lambda$. Alors, parmi les familles (h_ι) telles que $a_{(h_\iota)}\neq 0$, il existe un maximum, soit (k_ι), et l'on voit que, rapportée à la base de A constituée par les éléments de G, la composante de $\Sigma_{(h_\iota)}a_{(h_\iota)}\Pi_\iota(x_\iota-1)^{h_\iota}$ suivant $\Pi_\iota x_\iota^{k_\iota}$ est $a_{(k)}\neq 0$.

Convenons d'appeler « représentation » de $y\in A$ une égalité de la forme

$$y=\Sigma(z_1-1)\dots(z_r-1),$$

où Σ est le symbole d'une sommation finie, et où tous les z_s appartiennent à G; la « filtration apparente » de cette représentation sera, par définition, le nombre $\mathrm{Inf}\big(\Sigma_{s=1}^r w(z_s)\big)$, la borne inférieure étant prise pour tous les termes de la somme. Alors, si nous supposons $\varphi(y)\geqq 1$, $\varphi(y)$ est égal à la borne supérieure des filtrations apparentes de toutes les représentations de y. Si nous exprimons y comme une combinaison linéaire des éléments basiques $\Pi(x_\iota-1)^{h_\iota}$, nous obtenons une représentation de y que nous appellerons représentation réduite. Nous allons montrer que $\varphi(y)$ coïncide avec la filtration apparente de la représentation réduite de y. Il en résultera bien $w(z)=\varphi(z-1)$ pour tout $z\in G$; si, en effet, $z=\Pi_\iota x_\iota^{h_\iota}$, il existe au moins un ι, soit λ tel que $h_\lambda\neq 0$ et que $w(x_\lambda)=w(z)$. Or la représentation réduite de z contient le terme $h_\lambda(x_\lambda-1)$ et, par conséquent

$$\varphi(z-1)\leqq w(z), \qquad \text{donc} \quad \varphi(z-1)=w(z).$$

Nous voulons montrer qu'on peut passer d'une représentation quelconque à la représentation réduite sans diminuer la filtration apparente. Supposons ce résultat vrai pour toutes les représentations $\Sigma\big(\Pi(z-1)\big)$ où tous les $z\in G$ qui

apparaissent explicitement, sont contenus dans H_{i+1}. Nous allons le démontrer en remplaçant H_{i+1} par H_i [notre hypothèse de récurrence est vérifiée pour $i+1=n$, puisque $H_n=(1)$]. Si la proposition était fausse, il existerait un produit $(z_1-1)\dots(z_r-1)$, où $w(z_s)\geqq i\,(1\leqq s\leqq r)$, dont la filtration apparente diminuerait quand on passe à sa représentation réduite. Si nous remplaçons chaque facteur $(z-1)$ pour lequel $w(z)=i$ par sa représentation réduite, nous voyons qu'on pourrait trouver un produit de la forme

$$P_1(x_{\iota_1}-1)\,P_2(x_{\iota_2}-1)\dots(x_{\iota_k}-1)\,P_{k+1},$$

où les P_s représentent des produits (éventuellement vides) de facteurs $(z-1)$, avec $z\in H_{i+1}$, $w(x_{\iota_s})=i$ pour $1\leqq s\leqq k$, la filtration apparente du produit étant strictement supérieure à celle de sa représentation réduite. Raisonnons maintenant par récurrence sur k (pour $k=0$ la proposition est vraie par l'hypothèse de récurrence précédente). Montrons d'abord qu'il est possible de se ramener à un produit de la forme $(x_{\iota_1}-1)\dots(x_{\iota_k}-1)\,P$, où P désigne un produit de $(z-1)$, avec $z\in H_{i+1}$. Il suffira pour cela d'appliquer un certain nombre de fois l'identité :

$$(z-1)(x-1)=(x-1)(x^{-1}zx-1)+(x^{-1}zxz^{-1}-1)(z-1)+(x^{-1}zxz^{-1}-1),$$

en tenant compte des relations

$$w(x^{-1}zx)=w(z),\qquad w(x^{-1}zxz^{-1}-1)\geqq w(z)+w(x),$$

et de l'hypothèse de récurrence sur k. Ensuite, nous passerons à un produit de la forme $(x_{\iota'_1}-1)\dots(x_{\iota'_k}-1)\,P'$, où les facteurs $(x_{\iota'}-1)$ sont les facteurs $(x_\iota-1)$ précédents, rangés dans l'ordre croissant de leurs indices, et où P' est un produit de $(z-1)$ avec $z\in H_{i+1}$. Il suffira pour cela d'appliquer un certain nombre de fois l'identité

$$\begin{aligned}(x_2-1)(x_1-1)&=(x_1-1)(x_2-1)\\&\quad+\big((x_1-1)(x_2-1)+(x_1-1)+(x_2-1)+1\big)(x_2^{-1}x_1^{-1}x_2x_1-1).\end{aligned}$$

Nous parvenons donc à un produit de la forme $(x_{\iota'_1}-1)^{\alpha_1}\dots(x_{\iota'_r}-1)^{\alpha_r}P''$, où $\Sigma\alpha_s=k$, et où P'' désigne un produit de facteurs $(z-1)$, avec $z\in H_{i+1}$. Si tous les $\alpha_s\,(1\leqq s\leqq r)$ sont inférieurs à p, il suffit de réduire P'' pour parvenir à la représentation réduite du produit sans abaisser la filtration apparente. Sinon, il existe un indice s tel que $\alpha_s\geqq p$. Nous pouvons alors remplacer $(x_{\iota'_s}-1)^{\alpha_s}$ par $(x_{\iota_s}-1)^{\alpha_s-p}(x_{\iota'_s}^{p}-1)$, ce qui diminue de p le nombre de facteurs $(x_\iota-1)$ sans abaisser la filtration apparente, puisque $w(x_\iota^{p})\geqq p_i$ [c'est ici qu'apparaît essentiellement la condition que (H_i) est une N-suite restreinte]. Nous avons donc achevé la démonstration de la récurrence sur k; il en résulte la démonstration de la récurrence sur i, et la proposition est démontrée pour les N-suites finies. Remarquons que v est une filtration séparante sur $A=Z_p(G)$, mais que A ne peut être complet pour la topologie associée que si G est fini : en effet,

les éléments du complété $\overline{A}$ de A s'identifient canoniquement aux séries $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$ qui convergent formellement (c'est-à-dire qui n'ont qu'un nombre fini de termes de filtration $\leq k$ pour tout entier k).

Soit maintenant G un groupe, (H_i) une N-suite restreinte séparante dans G. Nous introduisons dans $A = Z_p(G)$ la filtration φ précédemment définie et la topologie associée. Montrons d'abord que φ est séparante. Pour cela, considérons les groupes G/H_n munis des N-suites restreintes finies $(H_i/H_n)_{(1 \leq i \leq n)}$, leurs algèbres $A_n = Z_p(G/H_n)$ munies des filtrations φ_n définies à partir de ces N-suites, et enfin les homomorphismes canoniques φ_n de A sur A_n. On établit sans peine que $\varphi_n\big(\varphi_n(y)\big) \geq \varphi(y)$ pour tout $y \in A$ [considérer une représentation de y dont la filtration apparente est $\varphi(y)$]. Si $y \neq 0$, il existe un entier n pour lequel $\varphi_n(y) \neq 0$; en effet, si $y = \Sigma_{i=1}^{r} a_i z_i$, $z_i \in G$, il existe un indice n pour lequel tous les z_i sont distincts modulo H_n, ce qui entraîne $\varphi_n(y) \neq 0$. Alors $\varphi_n\big(\varphi_n(y)\big) < \infty$ et, *a fortiori*, $\varphi(y)$ est fini. Considérons dans A les éléments $\Pi_\iota (x_\iota - 1)^{h_\iota}$ où les familles $(h_\iota)_{\iota \in I}$ vérifient les conditions précédentes : tous les h_ι sont compris entre 0 et $(p-1)$ inclus, et sont nuls sauf un nombre fini d'entre eux. Ces éléments sont encore linéairement indépendants (même démonstration). Soit $z \in G$; on peut écrire, d'une seule manière, $z = \Pi_\iota x_\iota^{u_\iota}$, où $0 \leq u_\iota \leq (p-1)$ pour tout $\iota \in I$, et où les u_ι non nuls tels que $w(x_\iota) \leq k$ sont en nombre fini pour tout entier k. Le produit $\Pi_\iota x_\iota^{u_\iota}$ converge dans G pour la (H_i)-topologie, ainsi que dans l'algèbre A pour la topologie associée à φ. Il en résulte que tout élément de G, donc de A, peut être représenté, par une série convergente $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$, où $a_{(h_\iota)} \in Z_p$: il suffit de remplacer, dans $\Pi_\iota x_\iota^{u_\iota}$, chaque $x_\iota^{u_\iota}$ par son développement $\big(1 + (x_\iota - 1)\big)^{u_\iota}$. Si $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$ converge dans A vers y, $\varphi(y) = \operatorname{Inf}\big(\Sigma_\iota w(h_\iota) h_\iota\big)$, la borne inférieure étant prise pour toutes les suites (h_ι) telles que $a_{(h_\iota)} \neq 0$. Posons, en effet,

$$c = \operatorname{Inf}\big(\Sigma_\iota w(h_\iota) h_\iota\big); \qquad \text{alors} \quad \varphi(y) \geq c.$$

Mais, d'après l'étude faite dans le cas des N-suites finies, nous pouvons choisir n assez grand pour que $\varphi_n\big(\varphi_n(y)\big) = c$. Alors

$$c = \varphi_n\big(\varphi_n(y)\big) \geq \varphi(y), \qquad \text{d'où} \qquad \varphi(y) = c.$$

Comme précédemment, nous en déduisons que $\varphi(z-1) = w(z)$ pour $z \in G$, ce qui achève la démonstration de (6.7).

La topologie induite sur G par la topologie de A est sa (H_i)-topologie. Il en résulte que le complété $\overline{A}$ de A contient canoniquement le complété $\overline{G}$ de G. Montrons que $\overline{A}$ contient l'algèbre $Z_p(\overline{G})$, c'est-à-dire que les éléments de $\overline{G}$ sont linéairement indépendants dans $\overline{A}$. En effet, l'homomorphisme canonique φ_n de $Z_p(G) = A$ sur $Z_p(G/H_n)$ se prolonge en un homomorphisme $\overline{\varphi}_n$ de $\overline{Z_p(G)} = \overline{A}$ sur $\overline{Z_p(G/H_n)}$. Alors, si $z \in \overline{G}$, $z' \in G$, $zz'^{-1} \in \overline{H}_n$, on a $\overline{\varphi}_n(z) = \varphi_n(z')$. Si $\Sigma_{s=1}^{r} \alpha_s z_s$

est combinaison linéaire finie d'éléments de $\overline{G}$ à coefficients non nuls dans Z_p, on peut trouver un entier n et des éléments z'_s de G tels que

$$z_s^{-1} z'_s \in \overline{H}_n, \qquad z'_s (z'_{s'})^{-1} \notin H_n \qquad (\text{pour } 1 \leq s, s' \leq r, s \neq s').$$

Alors

$$\overline{\varphi}_n(\Sigma \alpha_s z_s) = \Sigma \alpha_s \overline{\varphi}_n(z_n) = \Sigma \alpha_s \varphi_n(z'_s) \neq 0;$$

ainsi $\Sigma \alpha_s z_s \neq 0$, ce qui montre que les éléments de $\overline{G}$ sont linéairement indépendants dans $\overline{A}$. Nous pouvons donc préciser le théorème (6.7) :

THÉORÈME (6.9). — *Soit, dans le groupe G, une* N*-suite restreinte séparante* (H_i). *Définissons la fonction* $v(y)$ *dans* $Z_p(G)$ *comme la borne inférieure des* $v'(y)$, *où* v' *parcourt toutes les filtrations de* $Z_p(G)$ *telles que* $v'(z-1) \geq i$ *si* $z \in H_i$. *Alors* v *est une filtration séparante dans* $Z_p(G)$, $z \in H_i$ *si et seulement si* $v(z-1) \geq i$ (*en supposant* $z \in G$), *et le complété* $\overline{Z_p(G)}$ *de* $Z_p(G)$ *pour la topologie associée à* v *contient canoniquement* $Z_p(\overline{G})$, $\overline{G}$ *désignant le complété de* G *pour la* (H_i)*-topologie.*

Parmi les N-suites restreintes d'un groupe quelconque G, celle constituée par les groupes de dimension modulo p, $(G_{i,p})$, est celle qui « décroît le plus vite » : si (H_i) est une N-suite restreinte, $H_i \supset G_{i,p}$ pour tout i [d'après (5.6) et la définition des N-suites restreintes]. L'algèbre $\mathfrak{L}(G_{i,p})$ est, en tant qu'algèbre de Lie restreinte, engendrée par ses éléments de degré 1 et l'on peut sans difficulté démontrer une réciproque analogue au théorème (2.5). La N-suite $(G_{i,p})$ peut être obtenue au moyen de la filtration v du théorème (6.8) sur l'algèbre $Z_p(G)$; v est dans ce cas la borne inférieure des filtrations v' telles que $v'(z-1) \geq 1$ pour tout $z \in G$ [ce résultat est exact même si $(G_{i,p})$ n'est pas séparante]. Nous pouvons donc énoncer :

THÉORÈME (6.10). — *On obtient les groupes de dimension modulo p d'un groupe quelconque* G *en filtrant l'algèbre* $Z_p(G)$ *par les puissances de l'idéal engendré dans* $Z_p(G)$ *par les éléments* $z-1$, *où* $z \in G$.

Dans le cas où G est un p-groupe fini, ce théorème est dû à S. A. Jennings [12]. Nous allons en faire usage pour étudier la structure des algèbres de Magnus.

Considérons le groupe libre G de générateurs $(e_\nu)_{\nu \in N}$. Nous introduisons sur $Z_p(G)$ la filtration v associée, comme en (6.9) aux groupes de dimension mod$p$, $(G_{i,p})$. Nous allons montrer que l'algèbre complétée $\overline{Z_p(G)}$ s'identifie canoniquement à l'algèbre de Magnus de générateurs $(e_\nu - 1)_{\nu \in N}$ et à coefficients dans Z_p. Considérons, en effet, l'algèbre de Magnus $\mathfrak{A}_p$ à coefficients dans Z_p, de générateurs $(x_\nu)_{\nu \in N}$ (en correspondance biunivoque avec les générateurs e_ν de G). L'isomorphisme canonique de G dans $\mathfrak{A}_p$ se prolonge en un homomorphisme ψ de $Z_p(G)$ dans $\mathfrak{A}_p$, avec $\psi(e_\nu) = 1 + x_\nu$ pour tout $\nu \in N$. D'autre part, ω désignant comme précédemment l'ordre dans $\mathfrak{A}_p$, $\omega(\psi(y)) \geq v(y)$ pour

tout $y \in Z_p(G)$, puisque $\omega(\psi(y))$ définit sur $z_p(G)$ une filtration à laquelle est associée, par définition, la N-suite $(G_{i,p})$ [th. (6.9)]. Désignons par G_0 le semi-groupe multiplicatif engendré par les (e_ν) et l'unité dans G. Nous pouvons identifier l'algèbre $Z_p(G_0)$ à une sous-algèbre de $Z_p(G)$: $Z_p(G_0) \subset Z_p(G)$. La restriction de ψ à $Z_p(G_0)$ est un isomorphisme, puisque $\psi(Z_p(G_0))$ est la sous-algèbre avec unité engendrée par les (x_ν) dans $\mathfrak{A}_p$, qui est libre par définition. Mais ω est évidemment la plus petite filtration de $\psi(Z_p(G_0))$ pour laquelle $\omega(x_\nu) \geqq 1$ pour tout $\nu \in N$. Donc, pour tout $y \in Z_p(G_0)$,

$$\omega(\psi(y)) \leqq v(y) \qquad \text{et ainsi} \qquad \omega(\psi(y)) = v(y).$$

Remarquons que $Z_p(G_0)$ est dense dans $Z_p(G)$, ce qui résulte, par exemple, des relations $\lim_{r \to \infty} e_\nu^{p^r - 1} = e_\nu^{-1}$ dans $Z_p(G)$. La complétée $\overline{Z_p(G_0)}$ s'identifie donc à $\overline{Z_p(G)}$. Alors l'isomorphisme de $Z_p(G_0)$, qui transforme la filtration v en la filtration ω, se prolonge canoniquement en un isomorphisme $\bar{\psi}$ des algèbres complétées $(\bar{\psi} : \overline{Z_p(G)} = \overline{Z_p(G_0)} \to \mathfrak{A}_p)$; $\bar{\psi}$ coïncide évidemment avec ψ sur $Z_p(G)$. Nous avons donc identifié $Z_p(G)$ et $\mathfrak{A}_p$, avec correspondance des filtrations v et ω. Nous allons en déduire le :

THÉORÈME (6.11). — *Si l'on considère le groupe libre* G *et son complété* $\overline{G}_p$ *pour sa p-topologie plongés canoniquement dans les anneaux de Magnus* $\mathfrak{A}_{p^h}$ *et* $\mathfrak{A}_{\mathfrak{p}}$ *à coefficients entiers* modp^h (*resp. entiers p-adiques*), *l'algèbre du groupe* $\overline{G}_p$ *à coefficients entiers* modp^h (*resp. entiers p-adiques*) *est représentée fidèlement dans* $\mathfrak{A}_{p^h}$ (*resp.* $\mathfrak{A}_{\mathfrak{p}}$).

COROLLAIRE (6.12). — *L'algèbre* $Z(\overline{G})$ *du groupe* $\overline{G}$ *complété de* G *pour la topologie associée à sa suite centrale descendante est représentée fidèlement dans l'anneau de Magnus correspondant* $\mathfrak{A}$, *à coefficients entiers rationnels.*

Démonstration. — Nous venons d'établir (6.11) pour le cas où $h = 1$. Soit

$$z = \Sigma_{s=1}^{r} \alpha_s z_s, \qquad \text{où} \quad z \in \mathfrak{A}_{p^h}, \quad \alpha_s \in Z_{p^h}, \quad \alpha_s \neq 0, \quad z_s \in \overline{G}_p,$$

les z_s étant tous distincts $(1 \leqq s \leqq r)$. Si $k = \operatorname{Inf}_{1 \leqq s \leqq r} w_p(\alpha_s)$, on a

$$0 \leqq k \leqq h - 1 \qquad \text{et} \qquad \alpha_s = p^k \alpha'_s,$$

les α'_s n'étant pas tous nuls mod$p$. L'image de $z' = \Sigma_{s=1}^{r} \alpha'_s z_s$ par l'homomorphisme canonique de $\mathfrak{A}_{p^h}$ sur $\mathfrak{A}_p$ n'est pas nulle, ce qui peut s'énoncer : $w_p(z') = 0$, et par conséquent $w_p(z) = k < \infty$, donc $z \neq 0$, c'est-à-dire (6.11). La même démonstration reste valable pour l'algèbre de Magnus $\mathfrak{A}_{\mathfrak{p}}$

Les sous-groupes G_i de la suite centrale descendante de G sont *fermés* pour la *p*-topologie de G [*cf.* (5.6)], ce qui permet d'identifier $\overline{G}$ à un sous-groupe

de $\overline{G}_p$. Des identifications canoniques évidentes montrent qu'une relation de dépendance linéaire entre éléments de $\overline{G}$ dans $\mathfrak{A}$ aurait pour conséquence une relation de dépendance linéaire entre éléments de $\overline{G}_p$ dans $\mathfrak{A}_{\mathbf{p}}$, contrairement à (6.11), d'où (6.12). Si l'on se restreint aux éléments de G, on voit que Z(G) est plongé canoniquement dans $\mathfrak{A}$, ce qui constitue le « théorème d'unicité pour les développements en séries de puissances » de R. H. Fox [5].

Le théorème (6.11) peut être précisé en considérant certaines bases dans $\mathfrak{A}_{p^h}$ et dans $\mathfrak{A}_{\mathbf{p}}$. Reprenons les notations introduites dans la démonstration de (6.7) : G désigne maintenant un groupe libre, $(H_i) = (G_{i,p})$ ses groupes de dimension mod$p$; $\overline{Z_p(G)}$ s'identifie, comme nous l'avons vu, à $\mathfrak{A}_p$. Les éléments basiques $\Pi_\iota(x_\iota - 1)^{h_\iota}$ peuvent être considérés dans toutes les algèbres de Magnus $\mathfrak{A}_{p^h}$ et dans $\mathfrak{A}_{\mathbf{p}}$. Démontrons que les séries $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$ convergent dans $\mathfrak{A}_{p^h}$ et en représentent univoquement tous les éléments si les conditions suivantes sont bien remplies : $a_{(h_\iota)} \in Z_{p^h}$ pour toute suite (h_ι) et les $a_{(h_\iota)}$ non nuls tels que $\Sigma_\iota h_\iota w(x_\iota) \leqq k$ sont en nombre fini pour tout entier k. Établissons d'abord la convergence; nous désignons par ω_{p^h} l'ordre dans $\mathfrak{A}_{p^h}$. Montrons que les coefficients $a_{(h_\iota)}$ non nuls pour lesquels $\omega_{p^h}\left(\Pi_\iota (x_\iota - 1)^{h_\iota}\right) \leqq k$ sont en nombre fini pour tout entier k. Nous n'avons à considérer que les familles (h_ι) pour lesquelles $\Sigma_\iota h_\iota \leqq k$ [puisque $\omega_{p^h}(z-1) \geqq 1$ pour tout $z \in G$], et nous avons, par hypothèse,

$$\Sigma_\iota h_\iota w(x_\iota) \geqq k(k+1)p^{h-1}$$

pour tous les $a_{(h_\iota)} \neq 0$, à l'exception d'un nombre fini entre eux. Mais $\Sigma_\iota h_\iota \leqq k$ et $\Sigma_\iota h_\iota w(x_\iota) \geqq k(k+1)p^{h-1}$ impliquent qu'il existe au moins un x_ι avec $h_\iota \neq 0$ et $w(x_\iota) \geqq (k+1)p^{h-1}$. Alors $x_\iota \in G_{(k+1)p^{h-1},p} \subset G_{k+1,p^h}$ [d'après (5.7)], et $\omega_{p^h}(x_\iota - 1) \geqq (k+1)$. *A fortiori* $\omega_{p^h}\left(\Pi_\iota (x_\iota - 1)^{h_\iota}\right) \geqq k+1$. La convergence des séries étudiées est donc établie. Le fait qu'une série $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$ ne peut être nulle que si tous les $a_{(h_\iota)}$ sont nuls s'établit en posant

$$k = \mathrm{Inf}_{(h_\iota)} w_p(a_{(h_\iota)}), \qquad a_{(h_\iota)} = p^k a'_{(h_\iota)},$$

et en utilisant l'homomorphisme canonique de $\mathfrak{A}_{p^h}$ sur $\mathfrak{A}_p$, comme dans la démonstration de (6.11). Enfin, tout $y \in \mathfrak{A}_{p^h}$ peut être mis sous la forme $\Sigma_{(h_\iota)} a_{(h_\iota)} \Pi_\iota (x_\iota - 1)^{h_\iota}$: en appliquant toujours l'homomorphisme de $\mathfrak{A}_{p^h}$ sur $\mathfrak{A}_p$, nous construisons une série y_1 du type considéré, qui approche y mod$p$, puis nous commençons la construction pour $y' \in \mathfrak{A}_{p^h}$ tel que $y = y_1 + py'$, ... Finalement, nous obtenons y sous la forme $y_1 + py_2 + \ldots + p^{h-1}y_p$, les y_s étant des séries du type considéré.

Si nous considérons $\mathfrak{A}_{\mathbf{p}}$ comme la limite projective des algèbres de Magnus $\mathfrak{A}_{p^h}$ avec, bien entendu, la topologie correspondante, les résultats précédents restent valables, à ceci près qu'il est nécessaire, pour obtenir tous les éléments de $\mathfrak{A}_{\mathbf{p}}$ de remplacer la condition « les $a_{(h_\iota)}$ non nuls tels que $\Sigma_\iota h_\iota w(x_\iota) \leqq k$ sont en nombre fini pour tout entier k » par la condition moins forte « les $a_{(h_\iota)}$ non nuls tels que $\Sigma_\iota h_\iota w(x_\iota) \leqq k$ et $w_p(a_{(h_\iota)}) \leqq k$ sont en nombre fini pour tout entier k ». Nous pouvons unifier ces énoncés en exigeant seulement que les séries convergent dans l'algèbre considérée.

Si nous étions partis d'une N-suite restreinte séparante de G distincte de $(G_{i,p})$, ces derniers résultats resteraient valables. Mais l'isomorphisme entre $\overline{Z_p(G)}$ filtré à partir de la N-suite considérée (6.8) et $\mathfrak{A}_p$ n'identifierait plus les filtrations.

Déterminons maintenant les anneaux de Lie $\mathfrak{L}(G_{i,p^h})$ associés aux groupes de

dimension modp^h d'un groupe libre G($h > 1$). Ce sont des algèbres de Lie graduées sur Z_{p^h}, qui peuvent être plongées canoniquement dans l'algèbre associative libre contenue dans l'algèbre de Magnus $\mathfrak{A}_{p^h}$ (dont les générateurs sont en correspondance biunivoque avec ceux de G). Comme au début de ce paragraphe, nous désignons par L la sous-algèbre de Lie libre contenue dans $\mathfrak{A}_{p^h}$, et par R la sous-algèbre de Lie de $\mathfrak{A}_{p^h}$ identifiée à $\mathfrak{L}(G_{i,p^h})$. Alors $L \subset R$ et la forme générale d'un élément de degré jp^k [où $(j, p) = 1$] de R est :

$$y_{jp^k} + p^{h-1} y_{jp^{k-1}}^{p} + \ldots + p^{h-1} y_j^{p^k}, \tag{6.13}$$

où y_i désigne généralement un élément homogène de degré i de L. Il suffit, en effet, de reprendre le raisonnement qui nous a conduit à (6.1), en remplaçant l'identité

$$(1+x)^{p^k} \equiv 1 + x^{p^k} \qquad (\mathrm{mod}\, p)$$

par l'identité

$$(1+x)^{p^{k+h-1}} \equiv (1+x^{p^k})^{p^{h-1}} \qquad (\mathrm{mod}\, p^h).$$

Nous sommes conduits à considérer R comme une algèbre de Lie « restreinte » sur l'anneau Z_{p^h}, où l'opération $x \to x^{\underline{p}}$ vérifiant $(ad\, x)^p = \left(ad(x^{\underline{p}})\right)$ n'est définie que pour les éléments x tels que $px = 0$; ces éléments constituent évidemment un idéal, dans lequel l'identité de Jacobson (6.3) s'applique. Avec la définition des Z_{p^h}-algèbres de Lie restreintes qui se présente ainsi naturellement, $\mathfrak{L}(G_{i,p^h})$ est caractérisé comme une Z_{p^h}-algèbre de Lie restreinte libre.

Indiquons enfin la structure de l'anneau de Lie $\mathfrak{L}(H_i)$, où (H_i) est la N-suite déterminée dans le groupe libre plongé dans $\mathfrak{A}_{\mathbf{p}}$ par la filtration $v = \omega + w_p$ (5.8). $\mathfrak{L}(H_i)$ s'identifie à une sous-algèbre de Lie $\mathfrak{G}(\mathfrak{A}_{\mathbf{p}})$, algèbre associative graduée associée à l'algèbre de Magnus $\mathfrak{A}_{\mathbf{p}}$ filtrée par v. Pour tout entier $k \geq 0$, la composante homogène de degré k de $\mathfrak{G}(\mathfrak{A}_{\mathbf{p}})$ s'identifie canoniquement à la somme directe des composantes homogènes de degré $\leq k$ de $\mathfrak{A}_p$ (ou de $\mathfrak{A}_{\mathbf{p}}$ réduit mod$p$) : un élément $y \in \mathfrak{A}_{\mathbf{p}}$ tel que $v(y) \geq k$ possède une décomposition homogène de la forme

$$y = p^k y_0 + p^{k-1} y_1 + \ldots + y_k + \ldots,$$

et nous lui faisons correspondre $y'_0 + y'_1 + \ldots + y'_k$ les composantes y'_i étant les images des y_i par l'homomorphisme canonique de $\mathfrak{A}_{\mathbf{p}}$ sur $\mathfrak{A}_p$. $\mathfrak{G}(\mathfrak{A}_{\mathbf{p}})$ se trouve ainsi naturellement bigradué. Cette identification de $\mathfrak{G}(\mathfrak{A}_{\mathbf{p}})$ permet, en utilisant (5.8), de déterminer la structure de $\mathfrak{L}(H_i)$: la composante homogène de degré j de $\mathfrak{L}(H_i)$ est canoniquement isomorphe à la somme des composantes homogènes de degré $\leq j$ d'une algèbre de Lie libre sur Z_p dont les générateurs sont en correspondance biunivoque avec ceux de G. Plus précisément, si p est un nombre premier impair, G le groupe libre de générateurs $(x_\iota)_{\iota \in I}$, L l'algèbre de Lie libre (non restreinte) de générateurs $(y_\iota)_{\iota \in I}$ sur Z_p. (H_i) la N-suite de G définie par (5.8), et pour tout entier $i \geq 1$,, L_i le sous-module de L constitué

par les éléments dont les composantes homogènes de degré $>i$ sont nulles, nous pouvons, d'une seule manière, définir des applications φ_i de H_i dans L ($i=1, 2, \ldots$) vérifiant les conditions suivantes : si $x_i \in H_i$, $\varphi_i(x_i)$ ne dépend que de la classe de $x_i \bmod H_{i+1}$, et définit ainsi une application déterminée $\tilde{\varphi}_i$ de H_i/H_{i+1} dans L; $\tilde{\varphi}_i$ est un isomorphisme de H_i/H_{i+1} sur L_i; si $x_i \in H_i$, $x_j \in H_j$,

$$\varphi_{i+j}\big((x_i, x_j)\big) = [\varphi_i(x_i), \varphi_j(x_j)];$$

si $x_i \in H_i$, $x_i^p \in H_{i+1}$ et

$$\varphi_i(x_i) = \varphi_{i+1}(x_i^p);$$

enfin $\varphi_1(x_\iota) = y_\iota$ pour tout $\iota \in I$. Ce résultat doit être légèrement modifié pour $p=2$.

7. Les groupes de dimension modulo n. — Si n est un entier ≥ 2 quelconque, on obtient la N-suite $(G_{i,n})$ des groupes de dimension modulo n du groupe libre G en considérant l'algèbre de Magnus correspondante $\mathfrak{A}_n$ à coefficients dans l'anneau Z_n des entiers modulo n. Nous pouvons aussi considérer l'algèbre de Magnus $\mathfrak{A}$ à coefficients entiers rationnels, et définir $(G_{i,n})$ à partir de la filtration ν_n, image réciproque de l'ordre ω_n par l'homomorphisme canonique de $\mathfrak{A}$ sur $\mathfrak{A}_n$. Si $n = p_1^{h_1} \ldots p_r^{h_r}$ est la décomposition de n en facteurs premiers distincts, $\nu_n(y) = \operatorname*{Inf}_{1 \leq s \leq r} \nu_{p_s^{h_s}}(y)$, pour tout $y \in \mathfrak{A}$ (cela résulte du fait qu'un entier est divisible par n si et seulement s'il est divisible par tous les $p_s^{h_s}$). Nous en déduisons immédiatement :

$$G_{i,n} = \bigcap_{1 \leq s \leq r} G_i, p_s^{h_s}, \tag{7.1}$$

ce qui ramène l'étude de la N-suite $(G_{i,n})$ aux suites (G_{i,p^h}) déjà étudiées.

Nous pouvons indiquer la forme générale des éléments de $G_{i,n}$ en modifiant légèrement la représentation des éléments de G donnée par le lemme (5.3) :

Lemme (7.2). — *Tout élément* Z *de* G *peut être réprésenté par un produit* [*convergeant au sens de la topologie associée à la suite centrale descendante* (G_i)] $z = z_1^{k_1} z_2^{k_2} \ldots z_i^{k_i} \ldots$, *tel que, pour tout* i, $z_i \in G_i$ *et que : ou bien* $z_i = 1$, *ou bien la classe* $\tilde{z}_i$ *de* $z_i \bmod G_{i+1}$ *puisse figurer parmi les éléments d'une base du groupe abélien libre* G_i/G_{i+1}.

Cette dernière condition est équivalente à $w_p(z_i) = 0$ dans G_i/G_{i+1} pour tout nombre premier p. Les éléments z_i et leurs exposant k_i sont choisis successivement comme dans la démonstration de (5.3). Alors :

Théorème (7.3). — *Si* $z = \Pi_i z_i^{k_i}$ *comme en* (7.2), $z \in G_{j,n}$ *si et seulement si* $ip_s^{(w_{p_s}(k_i) - h_s + 1)^+} \geq j$, *pour tout* $i \geq 1$ *et tout* s $(1 \leq s \leq r)$.

Il suffit, en effet, d'appliquer (7.1) et (5.7) en remarquant que, si l'on

pose $z_i' = z_i^{k_i/p^{w_p(k_i)}}$, $z = \Pi_i z_i'^{p^{w_p(k_i)}}$ est une représentation de z vérifiant les conditions de (5.3).

Nous pourrions de même généraliser les p-filtrations (§ 5) en considérant les filtrations de $\mathfrak{A}$ qui ne dépendent que des propriétés de divisibilité des composantes homogènes.

La topologie de G définie par la N-suite $(G_{i,n})$ est la moins fine parmi les topologies de G plus fines que toutes les p_s-topologies $(1 \leqq s \leqq r)$. Remarquons que les diverses p-topologies du groupe G sont indépendantes, comme le sont les diverses valuations d'un corps. Plus précisément :

THÉORÈME (7.4). — *Soient $p_s (1 \leqq s \leqq r)$ des nombres premiers distincts, H_s des voisinages de l'unité dans* G, *pour les p_s-topologies respectives, z_s des éléments quelconques de* G. *Il existe alors $z \in G$ tel que $z_s z^{-1} \in H_s$ pour $1 \leqq s \leqq r$.*

Nous pouvons, en effet, supposer que les parties H_s sont des sous-groupes invariants contenant toutes les puissances $z_s^{p^{n_s}}$ où $z \in G$, n_s désignant des entiers convenablement choisis. Il suffit alors de déterminer des entiers α_s tels que $\alpha_s \equiv 1 \pmod{p_s^{n_s}}$ et $\alpha_s \equiv 0 \pmod{p_{s'}^{n_{s'}}}$, pour $1 \leqq s$, $s' \leqq r$, $s \neq s'$ et de prendre $z = z_1^{\alpha_1} z_2^{\alpha_2} \dots z_s^{\alpha_s}$.

Enfin, l'anneau de Lie $\mathfrak{L}(G_{i,n})$ est le produit direct des $\mathfrak{L}(G_{i,p_s^{h_s}})$ pour $1 \leqq s \leqq r$. En effet, $\mathfrak{A}_n$ est le produit direct des anneaux de Magnus $\mathfrak{A}_{p_s^{h_s}}$, ce qui montre que $\mathfrak{L}(G_{i,n})$ est isomorphe à un sous-anneau de Lie du produit direct $\Pi_{1 \leqq s \leqq r} \mathfrak{L}(G_{i,p_s^{h_s}})$, et (7.4) montre que cet isomorphisme applique $\mathfrak{L}(G_{i,n})$ sur $\Pi_{1 \leqq s \leqq r} \mathfrak{L}(G_{i,p_s^{h_s}})$.

8. REMARQUES ET PROBLÈMES. — La correspondance indiquée au paragraphe 2 qui associe aux sous-groupes d'un groupe G muni d'une N-suite (H_i) des sous-anneaux de $\mathfrak{L}(H_i)$ n'est ni biunivoque ni *sur*. Ainsi, par exemple, on peut construire un groupe G d'ordre 16, une N-suite (H_i) dans G, et deux idéaux I_1 et I_2 de $\mathfrak{L}(H_i)$ tels que I_1 soit associé à deux sous-groupes distincts de G, que I_2 ne soit associé à aucun sous-groupe de G, et que, néanmoins, I_1 et I_2 soient transformés l'un en l'autre par un automorphisme de $\mathfrak{L}(H_i)$.

Un problème qui se pose naturellement est celui de caractériser les anneaux de Lie qui peuvent s'obtenir sous la forme $\mathfrak{L}(H_i)$. On sait, par exemple, qu'une algèbre de Lie libre sur le corps Z_p des entiers mod$p$ (premier) ne peut jamais être ainsi obtenue (Magnus [24]). Comme cas particulier, se pose le problème de caractériser les quotients successifs de la suite centrale descendante d'un p-groupe.

Toutes les N-suites que nous avons étudiées dans un groupe libre ont été obtenues par le procédé du théorème (3.2), qui revient à filtrer l'algèbre du groupe à coefficients entiers rationnels. On peut se poser le problème de caractériser les N-suites d'un groupe donné G qui peuvent être obtenues par

le procédé (3.2). Plus particulièrement, peut-on obtenir ainsi la suite centrale descendante de G? Il suffirait alors de filtrer l'algèbre Z(G) par les puissances successives de l'idéal engendré par les éléments $(z-1)$, où $z \in G$. Une réponse affirmative à ce problème semble admise dans les articles de O. Grün [6] et R.H. Fox [5]; un essai incomplet de démonstration a été donné par P.M. Cohn [4]; j'ignore si une démonstration complète ou un (contre-exemple) ont été trouvés.

Nous avons démontré (6.10) que les groupes de dimension mod$p$ d'un groupe quelconque G s'obtiennent en filtrant l'algèbre $Z_p(G)$ à coefficients entiers mod$p$. On peut se demander si ce résultat demeure exact en remplaçant les groupes de dimension mod$p$ par les groupes de dimension modp^h $(h > 1)$, et l'anneau des coefficients par Z_{p^h}.

L'une des principales difficultés rencontrées dans l'étude de l'anneau $\mathfrak{L}(H_i)$ associé à à une N-suite (H_i) d'un groupe G provient de ce que seule l'addition d'éléments homogènes du même degré dans $\mathfrak{L}(H_i)$ s'obtient à partir de la multiplication dans G par passage aux quotients. On ne peut pourtant pas se dispenser de considérer les éléments non homogènes de $\mathfrak{L}(H_i)$. L'intérêt du théorème (3.3) vient principalement de ce qu'il fait correspondre, dans une certaine mesure, des sommes d'éléments homogènes de $\mathfrak{L}(H_i)$ à des sommes d'éléments non homogènes de $\mathfrak{L}(K_i)$. On remarquera que toute l'étude des N-suites associées aux p-filtrations des groupes libres (§5) est fondée sur leur comparaison à la suite centrale descendante par une méthode analogue à celle de (3.3), mais plus précise. D'ailleurs l'anneau $\mathfrak{L}(H_i)$ associé à la N-suite (5.8) est canoniquement isomorphe à l'anneau bigradué obtenu en le filtrant au moyen de la suite centrale descendante, ainsi que nous l'avons indiqué à la fin du paragraphe 6.

Une des principales applications de la théorie des anneaux de Lie associés aux N-suites est l'étude du problème de Burnside : il s'agit d'étudier les groupes ayant un nombre donné (fini) de générateurs qui ne sont liés que par les relations résultant de l'identité générique $x^n = 1$ (n étant un entier fixe) et, en particulier, de déterminer s'ils sont finis. Un cas particulier de ce problème, dont la solution générale paraît encore lointaine, est le suivant : n est un nombre premier p et l'on se borne à rechercher si les sous-groupes de la suite centrale descendante du groupe G considéré coïncident à partir d'un certain rang. C'est l'« hypothèse faible » de Burnside (Baer [1]). Elle est équivalente à la nilpotence de l'anneau $\mathfrak{L}(G_i)$ associé à la suite centrale descendante de G. La suite centrale descendante coïncide avec les groupes de dimension mod$p$ en raison de l'identité générique $x^p = 1$. $\mathfrak{L}(G_i)$ est donc une algèbre de Lie graduée restreinte sur Z_p; de plus, avec les notations du paragraphe 6, $x^{[p]} = 0$ pour tout $x \in \mathfrak{L}(G_i)$. Cela est évident lorsque x est homogène (6.8), et pour x non homogène, cela résulte de considérations assez délicates de Sanov [30], qui a établi, pour les composantes homogènes de degré $\leq 2p-2$, l'isomorphisme de $\mathfrak{L}(G_i)$ avec l'algèbre de Lie restreinte engendrée par des générateurs

en même nombre que ceux de G, et liés par les seules relations découlant de l'identité générique $x^p = 0$. On ne sait pas si ce résultat reste valable pour les degrés $\geqq 2p-1$. Si l'on considère G comme le quotient d'un groupe libre K par le sous-groupe $K(p)$ engendré par toutes les $p^{\text{ièmes}}$ puissances dans K, $\mathfrak{L}(G_i)$ s'identifie au quotient de l'anneau de Lie libre $\mathfrak{L}(K_i)$ par l'idéal associé à $K(p)$ (2.4). Une réponse affirmative à la dernière question mentionnée entraînerait que cet idéal est complètement caractéristique dans $\mathfrak{L}(K_i)$, c'est-à-dire stable pour tous les endomorphismes de $\mathfrak{L}(K_i)$. A ma connaissance, même cette hypothèse n'a pas été démontrée.

Les N-suites associées aux p-filtrations des groupes libres permettent d'obtenir, comme conséquence du théorème (5.5), toute une série de relations entre $p^{\text{ièmes}}$ puissances et commutateurs, utilisables dans l'étude du problème de Burnside pour un exposant premier ou puissance d'un nombre premier. On en connaît d'autres, obtenues par une voie différente (*cf.* Sanov [31] et O. Grün [6]). La suite des exposants $\Phi_v(i, j)$, pour i fixé, qui apparaît dans l'énoncé de (5.5), n'est évidemment pas arbitraire. Il serait intéréressant de préciser ce point en déterminant à quelles conditions doit satisfaire une suite (k_j) d'entiers $\geqq 0$ pour que $\Pi_{j=1}^{\infty} G_j^{p^{k_j}}$ définisse un sous-groupe du groupe libre G, au sens indiqué en (5.5).

CHAPITRE II.

Groupes nilpotents et N-groupes définis par la formule de Hausdorff.

1. Suites typiques. — Rappelons d'abord quelques résultats concernant la formule de Hausdorff ([13]). Considérons l'algèbre de Magnus A à coefficients rationnels engendrée par les générateurs indépendants x et y (chap. I, § 4). Comme précédemment, ω désignera l'ordre dans A. Pour tout $z \in A$ tel que $\omega(z) \geqq 1$, nous définissons $\exp z \in A$ et $\operatorname{Log}(1+z) \in A$ au moyen des séries classiques

$$\exp z = \Sigma_{i=0}^{\infty} \frac{z^i}{i!} \qquad \text{et} \qquad \operatorname{Log}(1+z) = \Sigma_{i=1}^{\infty} (-1)^{i+1} \frac{z^i}{i}.$$

Nous avons bien

$$\operatorname{Log}(\exp z) = z \qquad \text{et} \qquad \exp\big(\operatorname{Log}(1+z)\big) = 1+z.$$

Mais, si $z, z' \in A$ avec $[\omega(z), \omega(z') \geqq 1]$, on n'a pas

$$(\exp z)(\exp z') = \exp(z+z')$$

([13]) La formule de Hausdorff s'est dégagée assez lentement de la théorie des groupes de Lie. Son histoire est marquée par les noms de Poincaré, Schur, Campbell, Baker, Pascal, Hausdorff (sans que la liste soit probablement épuisée). Le mérite de Hausdorff est, semble-t-il, d'en avoir donné une démonstration [9] algébrique (ou « symbolique ») assez brève et compréhensible.

parce que z et z' ne commutent pas (en général). Nous poserons

$$(\exp x)(\exp y) = \exp\big(\Phi(x, y)\big);$$

$\Phi(x, y) \in A$ est définie par

$$\Phi(x, y) = \mathrm{Log}\big((\exp x)(\exp y)\big) = x + y + \tfrac{1}{2}[xy - yx] + \ldots.$$

Nous admettrons que toutes les composantes homogènes de $\Phi(x, y)$ appartiennent à la sous-algèbre de Lie engendrée par x et y dans l'algèbre de Lie portée par A (où l'on prend comme crochet $[z, z'] = zz' - z'z$); cette sous-algèbre est une algèbre de Lie libre de générateurs x et y (chap. I, § 4). On peut donc écrire $\Phi(x, y)$ comme une somme infinie d'alternants en x et y multipliés par des coefficients rationnels ; c'est ainsi qu'on obtient la *formule de Hausdorff* :

$$\Phi(x, y) = x + y + \tfrac{1}{2}[x, y] + \tfrac{1}{12}[[x, y], y] + \tfrac{1}{12}[[y, x], x] + \ldots.$$

Nous n'aurons pas besoin de connaître une loi explicite de formation des termes de cette formule, qui peut être écrite de diverses manières puisqu'on n'a pas de base canonique pour les alternants d'un degré donné. Par contre, dans l'algèbre associative A, $\Phi(x, y)$ s'écrit comme une suite infinie de monomes en x et y dont les coefficients (nombres rationnels) sont bien déterminés. Une remarque simple jouera un grand rôle dans la suite : désignons par Q_n l'anneau des nombres rationnels qui, écrits comme fractions irréductibles, n'admettent au dénominateur que des facteurs premiers $\leq n$ (nombres rationnels p-entiers pour $p > n$); alors le coefficient d'un monome de degré total n en x et y du développement de $\Phi(x, y)$ dans A appartient à Q_n [conséquence immédiate de la propriété arithmétique correspondante des développements de $\exp x$ et de $\mathrm{Log}(1 + x)$]. Or, le *sous-anneau* associatif engendré dans A par x et y contient comme facteur direct (en tant que groupe abélien libre) le *sous-anneau* de Lie libre engendré par x et y (chap. I, § 4); il en résulte qu'on peut écrire la formule de Hausdorff de telle manière que les alternants de degré total n en x et y se trouvent multipliés par des coefficients appartenant à Q_n.

Soit maintenant L l'*algèbre de Lie libre complétée à coefficients rationnels* engendrée par les générateurs indépendants $(x_\iota)_{\iota \in I}$, où l'ensembls d'indices I contient plus d'un élément : nous l'obtenons en construisant d'abord l'algèbre de Lie libre à coefficients rationnels de générateurs $(x_\iota)_{\iota \in I}$ qui est munie d'une graduation naturelle (où chaque x_ι a le degré 1), puis en complétant, c'est-à-dire en formant l'algèbre des « séries » dont les termes ont des degrés qui croissent indéfiniment. Nous désignerons par ω l'ordre dans L [$\omega(y)$ est le degré minimum des composantes homogènes non nulles de $y \in L$], et nous noterons L_i l'idéal de L constitué par les éléments d'ordre $\geq i$ ($i = 1, 2, \ldots$). La défini-

tion de L est entièrement analogue à la définition des algèbres de Magnus. De plus, les résultats du chapitre I (§ 4) montrent que L peut être plongée canoniquement dans l'algèbre de Magnus B de générateurs $(x_i)_{i\in I}$ à coefficients rationnels.

A tous $x, y \in L$ nous pouvons faire correspondre au moyen de la formule de Hausdorff un élément déterminé de L que nous noterons simplement xy et que nous appellerons le produit de x et de y :

$$xy = x + y + \frac{1}{2}[x, y] + \dots.$$

La propriété fondamentale de la formule de Hausdorff est la suivante : L devient, par rapport au produit xy, un *groupe non abélien*. Pour le démontrer, il suffit de plonger L dans l'algèbre de Magnus B et de remarquer que

$$(xy)z = \mathrm{Log}\big((\exp x)(\exp y)(\exp z)\big) = x(yz);$$

l'existence de l'élément neutre (le zéro de L) et de l'inverse de $x \in L$ (qui coïncide avec $-x$) s'établit immédiatement.

Lorsque nous parlerons désormais sans préciser de sous-groupes de L, etc., il sera sous-entendu que nous nous référerons à l'opération xy, c'est-à-dire à la structure de groupe non abélien de L.

Pour tous $r, s \in Q$ (corps des nombres rationnels) et $x \in L$, nous avons :

$$(rx)(sx) = (r + s)x.$$

Ainsi, les puissances entières de $x \in L$ coïncident avec ses multiples entiers. De plus,

$$(x, y) = xyx^{-1}y^{-1} = [x, y] + \dots$$

pour tous $x, y \in L$, les points de suspension indiquant des termes de degré $\geqq 3$ en x et y. On en déduit que les idéaux L_i de l'algèbre de Lie L constituent une N-suite dans le groupe L et que le groupe quotient L_i/L_{i+1} coïncide, en tant que groupe de classes suivant L_{i+1}, avec le quotient des groupes *abéliens* L_i et L_{i+1} (pour tout i).

Nous nous proposons d'étudier certaines suites d'éléments de L :

Définition (1.1). — Une suite $g(t)$ d'éléments de L dépendant du paramètre entier positif ou nul t sera dite *suite typique* (dans L) si l'on peut trouver des éléments $a_i \in L$ (i entier $\geqq 1$) tels que $a_i \in L_i$ (pour tout i) et que, pour tout t :

$$g(t) = \Sigma_{i=1}^{\infty} t^i a_i.$$

H désignant une partie de L, $g(t)$ sera dite *suite typique dans* H si elle est assujettie à la condition supplémentaire $g(t) \in H$ pour tout t.

Nous désignerons par la même lettre Δ l'opérateur qui fait correspondre à une suite d'éléments $g(t)$ la suite $\Delta g(t) = g(t+1) - g(t)$ et l'opérateur qui

fait correspondre à un polynome $P(t)$ le polynome $\Delta P(t) = P(t+1) - P(t)$. Les puissances successives de l'opérateur Δ seront notées Δ^k.

THÉORÈME (1.2). — *Une suite d'éléments $g(t) \in L$ est une suite typique si et seulement si $g(0) = 0$ et $\Delta^k g(0) \in L_k$ pour tout entier $k \geqq 1$.*

Démonstration. — Soit d'abord $g(t) = \Sigma_{i=1}^{\infty} t^i a_i$ une suite typique. Alors

$$\Delta g(t) = \Sigma_{i=1}^{\infty} (t+1)^i a_i - \Sigma_{i=1}^{\infty} t^i a_i = \Sigma_{i=1}^{\infty} \left((t+1)^i - t^i\right) a_i = \Sigma_{i=1}^{\infty} \Delta t^i a_i.$$

Plus généralement :

$$\Delta^k g(t) = \Sigma_{i=1}^{\infty} \Delta^k t^i a_i$$

pour tout entier $k \geqq 1$. Or, $\Delta^k t^i = 0$ si $k > i$, donc

$$\Delta^k g(t) = \Sigma_{i=k}^{\infty} \Delta^k t^i a_i \in L_k$$

et, en particulier, $\Delta^k g(0) \in L_k$.

Réciproquement, soit $g(t)$ une suite d'éléments de L, avec $g(0) = 0$. Nous pouvons calculer les termes de la suite $g(t)$ à partir des $\Delta^k g(0)$ $(k \geqq 1)$, par la formule connue :

$$g(t) = \Sigma_{k=1}^{\infty} \binom{t}{k} \Delta^k g(0),$$

où $\binom{t}{k}$ désigne le coefficient binomial que nous pouvons considérer comme un polynome en t à coefficients rationnels et de degré k. Aucune difficulté de convergence ne se présente, puisque la série considérée n'a qu'un nombre fini de termes non nuls pour toute valeur entière $\geqq 0$ de t. Pour démontrer que les relations $\Delta^k g(0) \in L_k$ entraînent que $g(t)$ est une suite typique, nous établissons plus généralement le :

LEMME (1.3). — *Soit a_k une suite d'éléments de* L *tendant vers zéro et $P_k(t)$ une suite de polynomes à coefficients rationnels sans termes constants, telles que $\deg P_k(t) \leqq \omega(a_k)$ pour tout $k \geqq 1$. Alors $g(t) = \Sigma_{k=1}^{\infty} P_k(t) a_k$ est une suite typique.*

Posons, en effet,

$$P_k(t) = \Sigma_{i=1}^{\infty} c_{i,k} t^i; \qquad c_{i,k} \in Q.$$

Alors

$$g(t) = \Sigma_{k=1}^{\infty} (\Sigma_{i=1}^{\infty} c_{i,k} t^i) a_k = \Sigma_{i=1}^{\infty} t^i (\Sigma_{k=1}^{\infty} c_{i,k} a_k).$$

La condition $\deg P_k(t) \leqq \omega(a_k)$ peut s'énoncer ainsi :

$$\omega(a_k) \geqq i \qquad \text{si} \quad c_{i,k} \neq 0;$$

l'interversion des sommations est donc licite, et

$$b_i = \Sigma_{k=1}^{\infty} c_{i,k} a_k \in L_i,$$

ce qui montre que $g(t) = \Sigma_{i=1}^{\infty} t^i b_i$ est une suite typique.

Nous pouvons définir sur l'ensemble des suites $g(t)$ à valeur dans L une structure d'algèbre de Lie en posant

$$(\lambda g)(t) = \lambda g(t), \qquad (g+h)(t) = g(t) + h(t), \qquad [g, h](t)] = [g(t), h(t)]$$

et une structure de groupe, en posant $(gh)(t) = g(t)h(t)$. Nous introduisons sur cet ensemble la topologie de la convergence simple : une famille $g_\nu(t)$ de suites converge vers $g(t)$ si $g_\nu(t)$ converge vers $g(t)$ pour tout t fixé. Avec ces conventions :

THÉORÈME (1.4). — *Les suites typiques constituent, dans l'ensemble de toutes les suite d'éléments de* L *une sous-algèbre de Lie fermée, et, par conséquent, un sous-groupe.*

Démonstration. — Soient

$$g(t) = \Sigma_{i=1}^{\infty} t^i a_i \qquad \text{et} \qquad h(t) = \Sigma_{i=1}^{\infty} t^i b_i$$

deux suites typiques. Alors

$$(\lambda g)(t) = \Sigma_{i=1}^{\infty} t^i \lambda a_i \qquad (\lambda \in \mathrm{Q}), \qquad (g+h)(t) = \Sigma_{i=1}^{\infty} t^i (a_i + b_i)$$

et

$$[g, h](t) = [\Sigma_{i=1}^{\infty} t^i a_i, \Sigma_{i=1}^{\infty} t^i b_i] = \Sigma_{i=1}^{\infty} t^i (\Sigma_{r=1}^{i-1} [a_r, b_{i-r}]).$$

Les relations $a_i \in \mathrm{L}_i$, $b_i \in \mathrm{L}_i$ impliquent évidemment

$$\lambda a_i \in \mathrm{L}_i, \qquad a_i + b_i \in \mathrm{L}_i \qquad \text{et} \qquad \Sigma_{r=1}^{i-1} [a_r, b_{i-r}] \in \mathrm{L}_i.$$

Les suites typiques constituent donc une sous-algèbre de Lie.

Soit $g_\nu(t)$ une famille de suites typiques tendant vers la suite $g(t)$. Alors, pour tout entier $k \geqq 1$, $\Delta^k g_\nu(0)$ tend vers $\Delta^k g(0)$; comme, pour tous ν, k,

$$\Delta^k g_\nu(0) \in \mathrm{L}_k, \qquad \Delta^k g(0) \in \mathrm{L}_k,$$

ce qui montre (1.2) que l'ensemble des suites typiques est fermé.

Enfin, si nous considérons

$$gh(t) = g(t) + h(t) + \frac{1}{2}[g(t), h(t)] + \ldots,$$

nous voyons que la somme des termes de degré $\leqq n$ de ce développement de Hausdorff est, pour tout entier n, une suite typique. Nous pouvons donc passer à la limite, puisque l'ensemble des suites typiques est fermé, ce qui établit que $gh(t)$ est une suite typique.

Nous allons maintenant chercher à caractériser les suites typiques en faisant abstraction de la structure d'algèbre de Lie de L, et en ne retenant que sa structure de groupe.

Nous avons déjà remarqué que si $x \in \mathrm{L}$, $r \in \mathrm{Z}$ (anneau des entiers), $rx = x^r$. Nous pouvons caractériser complètement en termes de théorie des groupes la

multiplication des éléments de L par les scalaires rationnels : si $r, s \in \mathbf{Z}$, $x \in \mathrm{L}$, nous définissons $x^{r/s} = y$ par les conditions $y \in \mathrm{L}$ et $x^r = y^s$: alors

$$y = x^{r/s} = (r/s)x.$$

Nous voyons donc que les *puissances fractionnaires* (rationnelles) des éléments de L sont bien déterminées. Elles vérifient évidemment les identités

$$(x^\lambda)^\mu = x^{\lambda\mu} \qquad \text{et} \qquad x^\lambda x^\mu = x^{\lambda+\mu} \qquad (\lambda, \mu \in \mathrm{Q}).$$

THÉORÈME (1.5). — *Si* $\big(\mathrm{P}_i(t)\big)$ *désigne une suite de polynomes en t à coefficients rationnels et sans termes constants, chaque polynome* $\mathrm{P}_i(t)$ *étant précisément de degré i, la relation :*

$$g(t) = a_1^{\mathrm{P}_1(t)} a_2^{\mathrm{P}_2(t)} \ldots a_i^{\mathrm{P}_i(t)} \ldots$$

établit une correspondance biunivoque entre l'ensemble des suites typiques et l'ensemble des suites (a_i) *d'éléments de* L *telles que* $a_i \in \mathrm{L}_i$ *pour tout entier positif i.*

Démonstration. — Si (a_i) est une suite d'éléments de L tels que $a_i \in \mathrm{L}_i$, $a_i^{\mathrm{P}_i(t)} = \mathrm{P}_i(t) a_i$ est une suite typique pour tout i, d'après (1.3). Il en est donc de même du produit $a_1^{\mathrm{P}_1(t)} \ldots a_i^{\mathrm{P}_i(t)} \ldots = g(t)$, d'après (1.4).

Pour démontrer que la suite (a_i) est uniquement déterminée, nous nous appuierons sur le :

LEMME (1.6). — *Soit* H *un groupe,* (K_i) *une suite centrale dans* H, *c'est-à-dire une suite de sous-groupes tels que* $\mathrm{K}_1 = \mathrm{H}$, $\mathrm{K}_i \supset \mathrm{K}_{i+1}$ et $(\mathrm{H}, \mathrm{K}_i) \subset \mathrm{K}_{i+1}$ *pour tout* $i \geqq 1$. *On suppose que* $\bigcap_i \mathrm{K}_i = (e)$ (*l'élément neutre de* H), *que* H *est complet pour la topologie obtenue en prenant les* (K_i) *comme système fondamental de voisinages de e, et que tous les quotients* $\mathrm{K}_i/\mathrm{K}_{i+1}$ *sont sans torsion. Soit* $\big(\mathrm{P}_i(t)\big)$ *une suite de polynomes à valeurs entières pour t entier* (14), *chaque* $\mathrm{P}_i(t)$ *étant précisément de degré i. Alors, si* (a_i) *et* (b_i) *désignent deux suites d'éléments de* H *tendant vers e, on ne peut avoir :*

$$(\bigstar) \qquad a_1^{\mathrm{P}_1(t)} a_2^{\mathrm{P}_2(t)} \ldots a_i^{\mathrm{P}_i(t)} \ldots = b_1^{\mathrm{P}_1(t)} b_2^{\mathrm{P}_2(t)} \ldots b_i^{\mathrm{P}_i(t)} \ldots,$$

pour toute valeur entière $\geqq 0$ *de t que si* $a_i = b_i$ *pour tout* $i \geqq 1$.

Supposons que, pour un entier k donné, nous ayons démontré les relations $b_i \in a_i \mathrm{H}_k$ pour tout $i \geqq 1$ (cela est évident pour $k = 1$).

Posons donc

$$b_i = a_i c_i, \qquad c_i \in \mathrm{H}_k.$$

(14) Rappelons que ces polynomes ne sont autres que les combinaisons linéaires à coefficients entiers des polynomes $\binom{t}{i}$ $(1 \leqq i < \infty)$.

Notre relation (★) s'écrit :

$$a_1^{P_1(t)}\dots a_i^{P_i(t)}\dots = (a_1c_1)^{P_1(t)}\dots(a_ic_i)^{P_i(t)}\dots.$$

Prenons le quotient de H par K_{k+1}, et désignons par $\hat{x}$ l'image canonique dans H/K_{k+1} de $x \in H$. La relation (★) nous donne :

$$\hat{a}_1^{P_1(t)}\dots\hat{a}_i^{P_i(t)}\dots = (\hat{a}_1\hat{c}_1)^{P_1(t)}\dots(\hat{a}_i\hat{c}_i)^{P_i(t)}\dots.$$

Mais par hypothèse, $\hat{c}_i$ appartient au centre de H/K_{k+1}. Donc

$$(\hat{a}_i\hat{c}_i)^{P_i(t)} = \hat{a}_i^{P_i(t)}\hat{c}_i^{P_i(t)}$$

et nous pouvons regrouper les facteurs du produit

$$\hat{a}_1^{P_1(t)}\hat{c}_1^{P_1(t)}\dots\hat{a}_i^{P_i(t)}\hat{c}_i^{P_i(t)}\dots = (\hat{a}_1^{P_1(t)}\dots\ \hat{a}_i^{P_i(t)}\dots)\,(\hat{c}_1^{P_1(t)}\dots\hat{c}_i^{P_i(t)}\dots).$$

Nous parvenons ainsi à la relation :

$$\hat{c}_1^{P_1(t)}\dots\hat{c}_i^{P_i(t)}\dots = \hat{e}$$

dans le groupe abélien K_k/K_{k+1}. Remarquons que tous les (a_i), (b_i) appartiennent à K_{k+1}, sauf un nombre fini d'entre eux. Par conséquent, $\hat{c}_i = \hat{e}$, sauf pour un nombre fini d'indices. Adoptons la notation additive; supposons, dans un groupe abélien sans torsion, une suite d'éléments d_i, tous nuls sauf un nombre fini d'entre eux, et tels que $\Sigma_{i=1}^{\infty} P_i(t)\,d_i = 0$, pour toute valeur entière ≥ 0 de t. Si tous les d_i ne sont pas nuls, soit l le plus grand indice tel que $d_l \neq 0$. Alors

$$\Sigma_{i=1}^{l}\,\Delta^l P_i(t)\,d_i = 0;$$

mais $\Delta^l P_i(t) = 0$ pour $i < l$, et $\Delta^l P_l(t) = l!\,\lambda_l$ [λ_l désignant le coefficient de t^l dans $P_l(t)$]. Ainsi $(l!\lambda_l)\,d_l = 0$, ce qui implique que $d_l = 0$. Tous les d_i sont donc nuls. Il en résulte que $\hat{c}_i = \hat{e}$ pour tout i, autrement dit : $b_i \in a_i K_{k+1}$ pour tout i. Cela étant vrai pour tout indice k, nous avons bien démontré les relations $a_i = b_i$, comme conséquence de la relation (★).

Remarques (1.7). — L'énoncé (1.6) admet un certain nombre de variantes, qui n'entraînent que des modifications insignifiantes dans la démonstration. Tout d'abord nous aurions pu supposer que la relation (★) n'est vérifiée que pour une infinité de valeurs de t (au lieu de toutes les valeurs entières ≥ 0 de t). En effet, tout se ramène à démontrer que, dans un groupe abélien sans torsion, une famille d'éléments $d_i\ (1 \leq i \leq n)$ ne peut satisfaire à $\Sigma_{i=1}^{n} P_i(t)\,d_i = 0$ pour une infinité de valeurs de t que si tous les d_i sont nuls. Si $P_i(t) = \Sigma_{j=1}^{i}\lambda_{i,j}t^j$, nous pouvons supposer, en multipliant éventuellement tous les $P_i(t)$ par un entier convenable, que les coefficients $\lambda_{i,j}$ sont entiers; alors

$$\lambda_{i,i} = \lambda_i \neq 0 \qquad \text{et} \qquad \Sigma_{i=1}^{n} P_i(t)\,d_i = \Sigma_{i=1}^{n} t^i e_i;$$

avec

$$e_i = \Sigma_{j=1}^{n}\lambda_{j,i}\,d_j.$$

Un calcul de déterminant de Vandermonde montre que tous les e_i sont nuls [il suffit que la relation $\Sigma_{i=1}^{n} t^i e_i$ soit vérifiée pour $(n+1)$ valeurs de t]; les conditions $\lambda_{i,i} \neq 0$ (pour $1 \leq i \leq n$) montrent que tous les d_i sont alors nuls. Contentons-nous d'indiquer les énoncés suivants, qui se démontrent comme (1.6) :

a. On remplace dans (1.6) la condition « tous les K_i/K_{i+1} sans torsion » par la condition « le coefficient de t^i dans chaque polynome $P_i(t)$ est $1/i!$ ». Par exemple :

$$P_i(t) = \binom{t}{i}.$$

b. On remplace la condition « les (a_i) et (b_i) tendent vers e » par $a_i = b_i = e$ pour $i > n$, on suppose que le coefficient de t^i dans chaque $P_i(t)$ est égal à 1, et l'on remplace la condition « K_i/K_{i+1} sans torsion » par « l'ordre d'aucun élément (excepté l'élément neutre) des quotients K_i/K_{i+1} ne divise $n!$ ».

c. On remplace la condition « les (a_i) et (b_i) tendent vers e » par « $a_i \in K_i$ et $b_i \in K_i$ pour tout i », on suppose que le coefficient de t^i dans chaque $P_i(t)$ est égal à 1, et l'on remplace la condition « K_i/K_{i+1} sans torsion » par « l'ordre d'aucun élément (excepté l'élément neutre) de K_i/K_{i+1} ne divise $i!$, quel que soit $i \geq 1$ ».

d. On remplace la condition « K/K_{i+1} sans torsion » par la condition « l'ordre d'aucun élément de K_i/K_{i+1} (excepté l'élément neutre) ne divise n », et l'on suppose que le coefficient de t^i dans chaque $P_i(t)$ est de la forme $\frac{r}{i!}$, où r divise une puissance de l'entier n donné.

L'unicité de la représentation (1.5),

$$g(t) = a_1^{P_1(t)} \ldots a_i^{P_i(t)} \ldots$$

des suites typiques résulte immédiatement de (1.6), en prenant $H = L$, $K_i = L_i$, et en remplaçant, si nécessaire $P_i(t)$ par $n_i P_i(t)$ et a_i par $a_i^{\frac{1}{n_i}}$, (n_i) désignant une suite d'entiers convenables.

Nous voyons, de plus, que la suite (a_i) d'éléments de L intervenant dans la définition (1.1) des suites typiques est bien déterminée par la suite $g(t)$: il suffit d'appliquer (1.6) à L considéré comme un groupe abélien. Enfin, $g(t) \in L_k$ pour tout t si et seulement si $a_i \in L_k$ pour tout i [appliquer (1.6) au groupe abélien L/L_k].

Achevons la démonstration de (1.5). Soit $g(t)$ une suite typique. Supposons que nous ayons déjà construit, pour certain entier i, des éléments $a_{1,i}$, $a_{2,i}$, ..., $a_{i,i}$, tels que $a_{r,i} \in L_r$ pour $1 \leq r \leq i$ et que

$$\big(g(t)\big)^{-1} a_{1,i}^{P_1(t)} a_{2,i}^{P_2(t)} \ldots a_{i,i}^{P_i(t)} \in L_{i+1}$$

pour tout t entier ≥ 0. Alors

$$h(t) = \big(g(t)\big)^{-1} a_{1,i}^{\mathrm{P}_1(t)} \dots a_{i,i}^{\mathrm{P}_i(t)}$$

est une suite typique dans L_{i+1}.

Nous avons donc, d'après la dernière proposition énoncée,

$$h(t) = \Sigma_{j=1}^{\infty} t^j b_j, \qquad \text{avec} \qquad b_j \in \mathrm{L}_j \cap \mathrm{L}_{i+1}.$$

Puisque chaque polynome $\mathrm{P}_i(t)$ est de degré i et sans terme constant, nous pouvons calculer sans ambiguïté les nombres rationnels $\lambda_{j,k}$ tels que $\Sigma_{k=1}^{j} \lambda_{j,k} \mathrm{P}_k(t) = t^j$. Alors :

$$\Sigma_{j=1}^{i+1} t^j b_j = \Sigma_{j=1}^{i+1} \big(\Sigma_{k=1}^{j} \lambda_{j,k} \mathrm{P}_k(t)\big) b_j = \Sigma_{k=1}^{i+1} \mathrm{P}_k(t) \, (\Sigma_{j=k}^{i+1} \lambda_{j,k} b_j).$$

Posons $c_k = -\Sigma_{j=k}^{i+1} \lambda_{j,k} b_j$. Alors la formule de Hausdorff montre immédiatement que :

$$h(t) \Pi_{k=1}^{i+1} c_k^{\mathrm{P}_k(t)} \in \mathrm{L}_{i+2} \quad \text{pour tout } t.$$

Or les éléments c_k appartiennent tous à L_{i+1}, ce qui implique que les éléments $c_k^{\mathrm{P}_k(t)}$ permutent, modulo L_{i+2}, avec tous les éléments de L. Ainsi :

$$a_{1,i}^{\mathrm{P}_1(t)} \dots a_{i,i}^{\mathrm{P}_i(t)} c_1^{\mathrm{P}_1(t)} \dots c_i^{\mathrm{P}_i(t)} c_{i+1}^{\mathrm{P}_{i+1}(t)} \equiv (a_{1,i} c_1)^{\mathrm{P}_1(t)} \dots (a_{i,i} c_i)^{\mathrm{P}_i(t)} c_{i+1}^{\mathrm{P}_{i+1}(t)} \pmod{\mathrm{L}_{i+2}}.$$

Posons

$$a_{r,i+1} = a_{r,i} c_r \qquad \text{pour} \quad 1 \leq r \leq i \quad \text{et} \quad a_{i+1,i+1} = c_{i+1}.$$

La famille $a_{r,i+1}$ possède, pour l'indice $i+1$, les mêmes propriétés que la famille $a_{r,i}$ pour l'indice i, et $a_{r,i+1} \equiv a_{r,i} \pmod{\mathrm{L}_{i+1}}$. Nous pouvons donc poser

$$a_i = \lim_{r \geq i, r \to \infty} a_{i,r},$$

et nous voyons que

$$g(t)^{-1} a_1^{\mathrm{P}_1(t)} \dots a_j^{\mathrm{P}_j(t)} \dots \in \mathrm{L}_i,$$

quel que soit i, c'est-à-dire que

$$g(t) = a_1^{\mathrm{P}_1(t)} \dots a_j^{\mathrm{P}_j(t)} \dots, \qquad \text{avec} \quad a_j \in \mathrm{L}_j \quad \text{pour tout } j.$$

La construction indiquée ne fait pas intervenir de choix arbitraire.

Nous allons d'abord appliquer le théorème (1.5) en prenant $\mathrm{P}_i(t) = \binom{t}{i}$.

Définition (1.8). — Soit une suite d'éléments $g(t)$ (t entier ≥ 0) dans un groupe quelconque H, $g(0)$ étant égal à l'élément neutre. Il existe alors dans H une suite (a_i) d'éléments déterminés, telle que :

$$g(t) = a_1^{\binom{t}{1}} a_2^{\binom{t}{2}} \dots a_i^{\binom{t}{i}} \dots \quad \text{pour tout } t.$$

L'élément a_i sera dit $i^{\text{ième}}$ *différence non abélienne* de la suite $g(t)$, et noté $\delta_i g(t)$; il ne dépend que des valeurs de $g(t)$ pour $1 \leq t \leq i$.

En effet, $\binom{t}{i} = 0$ pour tout $t < i$, et il s'agit donc toujours de produits finis dans H. Supposons déjà calculé a_i pour $1 \leq i \leq j-1$: nous devrons avoir

$$g(j) = a_i^{\binom{j}{1}} \dots a_{j-1}^{\binom{j}{j-1}} a_j,$$

ce qui détermine univoquement a_j.

Nous pouvons alors, d'après (1.5), énoncer :

THÉORÈME (1.9). — *Soit* H *un sous-groupe quelconque de* L. *La condition nécessaire et suffisante pour qu'une suite d'éléments* $g(t)$ *de* H *soit une suite typique dans* H *est que* $g(0) = 0$ *et que* $\delta_i g(t) \in L_i \cap H$ *pour tout* $i \geq 1$.

Prenons, en particulier, pour H le sous-groupe G de L engendré par ses générateurs $(x_\iota)_{\iota \in I}$. Alors G est un groupe libre par rapport aux générateurs (x_ι), et les sous-groupes $G_i = G \cap L_i$ constituent la suite centrale descendante de G. Il suffit, en effet, pour le démontrer d'appliquer les théorèmes (3.1) et (4.3) du chapitre I, en remarquant que le sous-anneau de Lie engendré par les (x_ι) dans L est libre.

Le théorème (1.9) nous donne donc une caractérisation des suites typiques dans le groupe libre G, sans plus faire aucunement intervenir l'algèbre de Lie L. Ainsi :

THÉORÈME (1.10). — *Une suite typique dans le groupe libre* G, *dont la suite centrale descendante est notée* (G_i), *est une suite* $g(t)$ *d'éléments de* G *telle que* $g(0)$ *soit l'élément neutre et que* $\delta_i g(t) \in G_i$ *pour tout entier* $i \geq 1$. *Dans l'ensemble des suites d'éléments de* G, *les suites typiques constituent un sous-groupe fermé. Si* $P_i(t)$ *est un polynome à valeurs entières pour* t *entier et de degré* i, $x^{P_i(t)}$ *est une suite typique dans* G *si et seulement si* $x \in G_i$.

Le théorème (1.10) nous permet d'établir immédiatement des identités du type de l'identité fondamentale de P. Hall ([8], § 3]). Prenons, par exemple, deux éléments x et y dans le groupe libre G ; $x^t y^t = g(t)$ est une suite typique et :

$$x^t y^t = a_1^{\binom{t}{1}} a_2^{\binom{t}{2}} \dots a_i^{\binom{t}{i}} \dots . \tag{1.11}$$

avec

$$a_1 = xy, \qquad a_2 = y^{-1}(x^{-1}, y^{-1})y, \qquad \dots, \qquad a_i = \delta_i g(t) \in G_i.$$

Pour trouver une identité de la forme $(xy)^t = x^t y^t \dots$, il suffit de considérer la suite typique : $y^{-t}x^{-t}(xy)^t = h(t)$. Ainsi :

$$(xy)^t = x^t y^t b_2^{\binom{t}{2}} \dots b_i^{\binom{t}{i}} \dots, \tag{1.12}$$

avec

$$b_2 = y^{-1}(y^{-1}, x^{-1})y, \qquad b_i = \delta_i h(t) \in G_i.$$

Rappelons que (1.11), où l'on fait $t=p$, donne l'identité (6.4) du chapitre I.

Des identités analogues s'établissent pour des suites typiques telles que (x^t, y), des suites typiques impliquant plus de deux éléments, etc. L'avantage des formes canoniques que nous trouvons est qu'elles découlent sans calculs de (1.10), et qu'elles ne font intervenir que des produits finis. Par contre, la vérification que les $i^{\text{èmes}}$ différences non abéliennes sont des produits de commutateurs de poids $\geq i$ entraîne des calculs pénibles, même pour les suites typiques les plus simples et les petites valeurs de i. Aussi allons-nous donner une forme non canonique des suites typiques qui met en évidence les sous-groupes G_i.

G désigne comme précédemment le groupe libre engendré par les $(x_\iota)_{\iota\in I}$ dans L. Nous choisissons une famille d'éléments $(y_\nu)_{\nu\in N}$ d'élément de G, ν parcourant un ensemble N bien ordonné, de façon que $\omega(y_\nu)<\omega(y_{\nu'})$ implique $\nu<\nu'$, et que les y_ν pour lesquels $\omega(y_\nu)=i$ constituent, $\mathrm{mod}\,G_{i+1}$, une base du groupe abélien libre G_i/G_{i+1} (*cf.* § 6, chap. I). Alors, tout élément du complété $\overline{G}$ de G dans L s'écrit, d'une manière et d'une seule, comme un produit infini ordonné (convergeant au sens de la topologie dans L) : $\Pi_{\nu\in N}y_\nu^{h_\nu}$, où les h_ν sont des entiers qui doivent vérifier la condition suivante : pour tout i, les h_ν correspondant aux indices ν tels que $\omega(y_\nu)=i$ sont nuls, sauf un nombre fini d'entre eux. Nous énoncerons désormais plus simplement cette condition en disant que le produit doit converger. Les composantes homogènes de degré $\omega(y_\nu)$ des y_ν (c'est-à-dire leurs « parties principales ») constituent une base, sur l'anneau Z des entiers rationnels, du sous-anneau de Lie libre engendré par les (x_ι) dans L (chap. I, § 4). Elles constituent donc aussi une base, sur le corps Q des nombres rationnels, de l'algèbre de Lie libre dont L est le complété. Nous en déduisons sans peine que les éléments de L sont représentés univoquement par les produits convergents $\Pi_{\nu\in N}y_\nu^{h_\nu}$, où les h_ν sont des nombres rationnels. Une suite d'éléments $g(t)$ dans $\overline{G}$ (resp. dans L) peut donc être mise sous la forme $\Pi_\nu y_\nu^{h_\nu(t)}$, où les $h_\nu(t)$ sont des fonctions de t déterminées à valeurs entières (resp. rationnelles).

Théorème (1.13). — *Une suite d'éléments $g(t)=\Pi_{\nu\in N}y_\nu^{h_\nu(t)}$ est une suite typique dans $\overline{G}$ (resp. dans* L*) si et seulement si le produit converge pour tout $t\geq 0$, $h_\nu(0)=0$, pour tout $\nu\in N$, et enfin si pour tout $\nu\in N$, la fonction $h_\nu(t)$ peut être représentée par un polynome à valeurs entières (resp. un polynome à coefficients rationnels) de degré $\leq\omega(y_\nu)$.*

Démonstration. — Un produit du type considéré représente bien une suite typique, d'après (1.4). Réciproquement, soit $g(t)=\Pi_{\nu\in N}y_\nu^{h_\nu(t)}$ une suite typique dans $\overline{G}$ (resp. dans L). Désignons généralement par ν_i le plus petit indice ν tel

que $\omega(y_\nu)=i$. Supposons démontré que, pour $\nu<\nu_i$, les fonctions $h(t)$ vérifient les conditions du théorème. Alors $(\Pi_{\nu<\nu_i} y_\nu^{h_\nu(t)})^{-1} g(t)$ est une suite typique dans $\overline{G}_i$ (resp. L_i), donc de la forme $\Sigma_{j=1}^{\infty} t^j a_j$, avec $a_j \in L_i \cap L_j$ pour tout j. D'après les propriétés des y_ν, nous pouvons trouver des coefficients rationnels $\lambda_{j,\nu}$ ($1 \leq j < \infty$; $\nu \in N$) tels que

$$a_j \equiv \Sigma_{\nu_i \leq \nu < \nu_{i+1}} \lambda_{j,\nu} y_\nu \pmod{L_{i+1}} \qquad \text{pour} \quad 1 \leq j \leq i.$$

Il en résulte que

$$h_\nu(t) = \Sigma_{1 \leq j \leq i} \lambda_{j,\nu} t^j,$$

ce qui démontre (1.13).

(1.14) *Remarques.* — *a.* Si, dans la définition (1.1) des suites typiques, nous remplaçons la condition $a_i \in L_i$ pour tout i par la condition plus faible $\lim_{i\to\infty} \omega(a_i) = \infty$, nous parvenons à la notion de *suite analytique* dans L. Les suites typiques ne sont donc qu'un cas particulier des suites analytiques, mais ce sont les seules dont nous ayons ici à faire usage. Tous les résultats que nous avons démontrés pour les suites typiques s'établissent, en modifiant convenablement les énoncés, pour les suites analytiques. Ainsi, dans (1.2). on doit remplacer la condition « $\Delta^k g(0) \in L_i$ pour tout i » par la condition « $\lim_{k\to\infty} \omega\big(\Delta^k g(0)\big) = \infty$ » ; la même modification doit intervenir dans le théorème (1.9), les différences $\Delta^k g(0)$ étant remplacés par les différences non abéliennes $\delta_i g(t)$. L'énoncé du lemme (1.6) s'applique directement aux suites analytiques, et permet de démontrer, pour les suites analytiques, le théorème (1.5) où il faut seulement remplacer la condition « $a_i \in L_i$ pour tout i » par la condition plus faible « $\lim_{i\to\infty} \omega(a_i) = \infty$ ».

b. Si deux suites typiques (resp. analytiques) $g(t)$ et $h(t)$ coïncident pour une infinité de valeurs de t, elles coïncident pour toutes les valeurs (entières ≥ 0) de t. Il suffit, en effet, d'appliquer aux deux suites le théorème (1.5) en prenant, par exemple, $P_i(t) = \binom{t}{i}$ [*cf.* (1.9)], puis d'appliquer la remarque (1.7).

c. Nous avons supposé, dans la définition d'une suite typique (resp. analytique) $g(t)$ que $g(0) = 0$. Cette condition n'est pas essentielle, mais elle simplifie certains énoncés, et correspond aux besoins des applications.

d. Nous aurions pu, dans la définition (1.1) des suites typiques faire intervenir toutes les valeurs entières de t. Alors les théorèmes (1.2) et (1.9) ne seraient plus exacts [puisqu'ils ne font intervenir que les valeurs de $g(t)$ pour $t \geq 0$]. Par contre, les théorèmes (1.4) et (1.5) restent valables (une seule modification doit être apportée, pour démontrer que l'ensemble des suites typiques, considéré comme partie de l'ensemble des applications de Z

dans L, est fermé). De même, nous aurions pu faire intervenir toutes les valeurs rationnelles de t. Mais, avec ces définitions, la remarque b précédente resterait valable : deux suites typiques coïncidant pour une infinité de valeurs de t coïncideraient pour toutes les valeurs (entières ou rationnelles, suivant la définition adoptée) de t. Il en résulte que nous n'avons essentiellement qu'une seule définition des suites typiques, car l'extension d'une suite typique, définie comme en (1.1). à toutes les valeurs entières ou rationnelles de t est évidemment possible, et n'est possible que d'une seule manière.

Application. — Les identités telles que (1.11) et (1.12) que nous avons établies pour t entier ≥ 0 restent vraies pour t négatif, les produits envisagés étant alors effectivement infinis. (Si l'on veut considérer les valeurs non entières de t, on doit évidemment se placer dans le groupe L.) Toutes ces considérations s'appliquent au cas des suites analytiques.

e. Tous les résultats concernant les suites typiques (resp. analytiques) peuvent se généraliser à des familles d'éléments dépendant de plusieurs paramètres. On pourrait ainsi donner des identités du type de P. Hall pour $x^t y^{t'} z^{t''}$, ... Les énoncés seraient sensiblement plus compliqués, et, pour avoir des représentations en produit [*cf.* (1.8), (1.9)], on serait obligé d'ordonner totalement les couples (ou n-uples) d'entiers positifs, ce qui laisserait subsister beaucoup d'arbitraire. Aussi, semble-t-il raisonnable d'attendre les applications éventuelles avant de développer la théorie dans cette direction.

2. Inversion de la formule de Hausdorff (*Formules génériques*). — Nous commençons par appliquer le théorème (1.5) en prenant $P_i(t) = t^i$. Il en résulte la correspondance biunivoque entre les suites typiques

$$g(t) = \Sigma_{i=1}^{\infty} t^i a_i$$

et les développements en produit :

$$g(t) = \Pi_{i=1}^{\infty} b_i^{t^i}, \qquad \text{avec} \quad b_i \in \mathrm{L}_i \text{ pour tout } i.$$

Nous appellerons b_i le $i^{\text{ième}}$ *résidu* de la suite typique $g(t)$. Contrairement à ce qui se passe pour les différences non abéliennes, les résidus ne se calculent pas simplement à partir des valeurs $g(t)$ de la suite typique dans le groupe L; par contre, nous allons voir comment ils se calculent au moyen des coefficients a_i et des opérations de l'algèbre de Lie L.

Nous désignons par Q_i l'ensemble des nombres rationnels qui, écrits comme fractions irréductibles, n'admettent au dénominateur que des facteurs premiers au plus égaux à i. Rappelons alors que, dans la formule de Hausdorff,

$$xy = x + y + \frac{1}{2}[x, y] + \dots$$

la composante homogène de degré i peut s'écrire sous la forme d'une somme

d'alternants de degré total i par rapport à x et y, multipliés par des coefficients de Q_i. Nous remarquons d'abord que, dans le développement

$$\Pi_{i=1}^{n} b_i^{t^i} = \Sigma_{i=1}^{\infty} t^i a_{i,n},$$

le coefficient $a_{i,n}$ ne dépend que des b_j pour lesquels $1 \leq j \leq i$. En passant à la limite, nous voyons qu'il en est de même du coefficient a_i dans le développement de $\Pi_{i=1}^{\infty} b_i^{t^i}$. Les premiers coefficients a_i sont donnés par les formules :

$$(2.1) \qquad \begin{cases} a_1 = b_1, \\ a_2 = b_2, \\ a_3 = b_3 + \frac{1}{2}[b_1, b_2], \\ a_4 = b_4 + \frac{1}{2}[b_1, b_3] + \frac{1}{12}[[b_2, b_1], b_1], \end{cases}$$

On voit facilement que, pour calculer a_i, il suffit de connaître $b_1, b_2, \ldots b_i$ et les termes de la formule de Hausdorff jusqu'au degré $(i-1)$ inclus. Nous en déduisons que $a_i - b_i$ est une somme d'alternants par rapport à $b_1, \ldots, b_{i-1}$, multipliés par des coefficients appartenant à Q_{i-1} ; nous pouvons préciser que ces alternants ont le poids i, si l'on attribue à chaque b_j le poids j, et si l'on attribue au crochet $[u, v]$ un poids égal à la somme des poids de u et de v.

Nous savons déjà (1.5), qu'on peut calculer les b_i en fonction des a_i. Les formules (2.1) conduisent à ;

$$(2.2) \qquad \begin{cases} b_1 = a_1, \\ b_2 = a_2, \\ b_3 = a_3 - \frac{1}{2}[a_1, a_2], \\ b_4 = a_4 - \frac{1}{2}[a_1, a_3] + \frac{1}{6}[[a_2, a_1], a_1]. \end{cases}$$

Nous pouvons énoncer généralement le :

THÉORÈME (2.3). — *Toute suite typique $g(t) = \Sigma_{i=1}^{\infty} t^i a_i$ peut être représentée, d'une manière et d'une seule, par un produit ordonné $g(t) = \Pi_{i=1}^{\infty} b_i^{t^i}$. Le $i^{ième}$ résidu b_i de la suite $g(t)$ se calcule au moyen des opérations de l'algèbre de Lie à partir des coefficients $a_j (1 \leq j \leq i)$; plus précisément, pour tout i, $b_i - a_i$ est égal à une somme d'alternants par rapport aux $a_j (1 \leq j \leq i-1)$ multipliés des coefficients de Q_{i-1}.*

L'intérêt principal de ce théorème est qu'il nous permet de décrire complètement, à partir de la structure de groupe de L, sa structure d'algèbre de Lie :

THÉORÈME (2.4). — *Soient x et y deux éléments de* L. *Alors il existe une suite d'éléments b_i de* L *tendant vers zéro, et une seule, telle que pour tout entier t :*

$$x^t y^t = b_1^t b_2^{t^2} \ldots b_i^{t^i} \ldots,$$

et l'on a

$$b_1 = x + y, \qquad b_2^2 = [x, y].$$

Démonstration. — Il suffit de considérer la suite typique

$$x^t y^t = t(x+y) + \frac{t^2}{2}[x, y] + \dots$$

et d'appliquer (2.3). Nous aurions pu, pour calculer $[x, y]$, utiliser la suite typique

$$(x, y^t) = c_1^t c_2^{t^2} \dots, \qquad \text{où} \quad c_1 = [x, y], \qquad \dots.$$

Ce théorème nous permet de caractériser la structure d'algèbre de Lie de L à partir de sa structure de groupe topologique. Il réalise, en quelque sorte, l'inversion « descriptive » de la formule de Hausdorff, c'est-à-dire qu'il définit les opérations $x+y$ et $[x, y]$ à partir de propriétés du groupe L. Il nous faut encore rechercher comment calculer ces opérations à partir des opérations connues du groupe : produit, exponentiation, passage à la limite. Remarquons qu'il est impossible de calculer la somme $x+y$ et le crochet $[x, y]$ de deux éléments de L au moyen de produits et de passages à la limite (sans considérer les puissances fractionnaires). En effet, le groupe libre G engendré par les générateurs indépendants (x_ι) de L n'est pas un sous-anneau de Lie, non plus que son adhérence $\overline{\mathrm{G}}$.

Il serait sans doute intéressant (pour le problème de Burnside en particulier) de pouvoir caractériser, de façon « constructive », le plus petit sous-groupe de L qui contienne G et soit en même temps un sous-anneau de Lie. Faute de pouvoir résoudre ce problème, nous allons considérer un sous-groupe M de L qui contiendra G, sera un sous-anneau de Lie, et ne sera « pas trop grand » pour les applications que nous en voulons donner.

Définition (2.5). — Dans l'algèbre de Lie libre complétée à coefficients rationnels L, nous désignerons par M l'ensemble des éléments dont les composantes homogènes de degré i sont des sommes d'alternants de degré i par rapport aux générateurs indépendants (x_ι) de L, multipliés par des coefficients appartenant à Q_i (pour tout entier $i \geqq 1$). M est en même temps une sous-algèbre de Lie fermée et un sous-groupe de L.

Le fait que M soit une sous-algèbre fermée de L résulte immédiatement de la définition ; la propriété arithmétique des coefficients de la formule de Hausdorff, rappelée plus haut, montre que M est un sous-groupe.

Théorème (2.6). — *Soit*

$$g(t) = \Sigma_{i=1}^{\infty} t^i a_i = \Pi_{i=1}^{\infty} b_i^{t^i}$$

une suite typique à valeurs dans M. *Alors, pour tout* $i \geqq 1$,

$$a_i \in \mathrm{M} \qquad \text{et} \qquad b_i \in \mathrm{M}.$$

Démonstration. — Considérons le *groupe abélien* $L/M = N$. Le groupe abélien N est gradué, comme L et son sous-groupe homogène M. Sa composante homogène de degré i est le quotient des composantes homogènes de degré i de L et de M : c'est donc un groupe de torsion, mais (d'après la définition de M), l'ordre d'aucun de ses éléments ne divise i! Considérons alors la relation $g(t) = \Sigma_{i=1}^{\infty} t^i a_i$, où $g(t) \in M$ pour tout entier $t \geq 0$. Si nous désignons par $\hat{a}$ la classe mod M de $a \in L$, nous avons donc $\Sigma_{i=1}^{\infty} t^i \hat{a}_i = 0$ dans N. De plus, puisque $g(t)$ est une suite typique, $a_i \in L_i$ pour tout i, et $\hat{a}_i \in N_i = L_i + M/M = L_i/M \cap L_i$. Le quotient N_i/N_{i+1} s'identifie à la composante homogène de degré i de N, et nous pouvons appliquer (1.7c), qui nous donne le résultat cherché : $\hat{a}_i = 0$ pour tout i.

Pour démontrer que $b_i \in M$ pour tout i, nous ne pouvons pas appliquer la même méthode au groupe *non abélien* L, car M n'en est pas un sous-groupe invariant. Par contre, il nous suffit d'appliquer le résultat précédent, joint au théorème (2.3) (nous pourrions aussi établir la proposition directement, en démontrant par récurrence sur j, que $b_i \in M + L_j$ pour tous i, j).

Considérons maintenant dans le groupe libre G engendré par les générateurs $(x_\iota)_{\iota \in I}$ de L une famille d'éléments $(y_\nu)_{\nu \in N}$ possédant les mêmes propriétés qu'en (1.13). Nous avons vu que tout élément de L s'écrit univoquement comme un produit bien ordonné convergent : $\Pi_\nu y_\nu^{h_\nu}$, où $h_\nu \in Q$.

LEMME (2.7). — *Soit* $z \in L$, $z = \Pi_\nu y_\nu^{h_\nu}$. *Alors* $z \in M$ *si et seulement si* $h_\nu \in Q_{\omega(y_\nu)}$ *pour tout* $\nu \in N$.

La démonstration procède, comme d'habitude, par récurrence sur $\omega(y_\nu)$. Désignons généralement par ν_i le plus petit indice ν pour lequel $\omega(y_\nu) = i$. Supposons déjà démontré $h_\nu \in Q_{\omega(y_\nu)}$ pour $\nu < \nu_i$. Considérons $z_i = (\Pi_{\nu < \nu_i} y_\nu^{h_\nu})^{-1} z$. Pour tout $\nu < \nu_i$, nous avons $y_\nu \in M$ (puisque $y_\nu \in G$) et $y_\nu^{h_\nu} = h_\nu y_\nu \in M$; puisque $h_\nu \in Q_{\omega(y_\nu)}$. Ainsi $z_i \in M \cap L_i$, et les exposants $h_\nu (\nu_i \leq \nu < \nu_{i+1})$ sont uniquement déterminés par la relation :

$$z_i - \Sigma_{\nu_i \leq \nu < \nu_i} h_\nu y_\nu \in L_{i+1}.$$

Cette relation entraîne $h_\nu \in Q_i$ pour $\nu_i \leq \nu < \nu_{i+1}$, puisque $z_i \in M \cap L_i$ et que les $(y_\nu)_{\nu_i \leq \nu < \nu_{i+1}}$ constituent, modulo L_{i+1}, une base de la composante homogène de degré i du sous-anneau de Lie libre engendré par les $(x_\iota)_{\iota \in I}$.

Nous pouvons maintenant définir des formules « constructives » d'inversion de la formule de Hausdorff. Supposons que L possède deux générateurs indépendants, notés x et y, et qu'on ait fait choix d'une suite d'éléments z_i possédant les propriétés de la famille $(y_\nu)_{\nu \in N}$ précédente. Cela peut se faire, par exemple, en utilisant le procédé de Marshall Hall [7]. Alors il existe deux suites d'exposants rationnels, h_i et k_i, tels que l'on ait :

$$x + y = \Pi_{i=1}^{\infty} z_i^{h_i}, \qquad [x, y] = \Pi_{i=1}^{\infty} z_i^{k_i}, \tag{2.8}$$

où

$$h_i \in Q_{\omega(z_i)}, \qquad k_i \in Q_{\omega(z_i)}.$$

On aura, par exemple,

$$x+y=xy(x,y)^{-\frac{1}{2}}\dots, \qquad [x,y]=(x,y)\left((x,y),y\right)^{\frac{1}{2}}\dots.$$

Connaissant les premiers termes de la formule de Hausdorff, on pourra calculer les premiers termes des formules d'inversion, par l'algorithme exposé dans la démonstration de (2.7).

Nous étudierons plus loin (§ 4) dans quels groupes il est possible d'appliquer les formules d'inversion de façon qu'elle définissent une structure d'anneau de Lie, et qu'on puisse, au moyen de la formule de Hausdorff, retrouver la structure de groupe dont on était parti. Nous aurons besoin, pour cela, de résultats auxiliaires, exposés au paragraphe 3. Par contre, on démontre immédiatement que les formules d'inversion s'appliquent dans M.

(2.9) *Remarque.* — Les formules d'inversion (2.8) dépendent formellement du choix de la suite z_i, mais les valeurs des produits correspondants n'en dépendent manifestement pas. Nous pouvons plus généralement chercher à résoudre le problème suivant : soit k un nombre rationnel ; existe-t-il une suite u_i de produits de commutateurs en x et y de poids $\geqq 3$ et une suite d'exposants k_i, telles que le produit infini ordonné $xy(x,y)^k u_1^{k_1}u_2^{k_2}\dots u_i^{k_i}\dots$ converge lorsque l'on substitue à x et y deux éléments quelconques de L et définisse ainsi dans L une opération associative? La réponse est affirmative, quel que soit k. Si $k\neq -\frac{1}{2}$; on obtient la loi de groupe non abélien $\left(x^{\frac{2k+1}{2}}y^{\frac{2k+1}{2}}\right)^{\frac{2}{2k+1}}$, et en particulier la loi du groupe opposé yx pour $k=-\frac{3}{2}$; si $k=-\frac{1}{2}$, on obtient la loi de groupe abélien $x+y$ que nous avons déjà trouvée ([15]).

3. Quelques problèmes d'extension et de prolongement. — *Définitions et notations.* P désignant un ensemble de nombres premiers, n un entier positif, on exprimera par la notation n/P le fait que tous les facteurs premiers de n appartiennent à P.

Un groupe multiplicatif G (dont l'unité est notée 1) sera dit *sans* P-*torsion* si $x\in\mathrm{G}$, n/P et $x^n=1$ impliquent $x=1$. G sera dit P-*divisible* si $x\in\mathrm{G}$, n/P impliquent qu'il existe $y\in\mathrm{G}$ avec $y^n=x$ (il suffirait, dans ces deux définitions, de prendre pour n un nombre premier appartenant à P). Un élément $x\in\mathrm{G}$ sera dit élément de P-torsion s'il existe n, avec n/P et $x^n=1$; si tous les éléments de G sont de P-torsion, G sera dit un *groupe de* P-*torsion*.

Dans tout ce paragraphe nous désignerons (P_i) une suite d'ensemble de nombres premier $\mathrm{P}_1\subset\mathrm{P}_2\subset\dots\subset\mathrm{P}_i\subset\mathrm{P}_{i+1}\subset\dots$. Il sera commode [dans la

([15]) Ce genre de questions sera étudié dans un article à paraître sous le titre : *Éléments d'une théorie algébrique des groupes analytiques.*

démonstration de (3.2)] de désigner par P_0 l'ensemble vide : ainsi n/P_0 signifiera $n=1$.

Nous aurons à considérer dans un groupe G des suites de sous-groupes invariants (H_i), où $i=1, 2, \ldots$. Il s'agira toujours, sauf mention expresse du contraire, de suites décroissantes commençant à G :

$$H_1=G\supset H_2\supset\ldots\supset H_i\supset H_{i+1}\supset\ldots.$$

Rappelons qu'une telle suite est dite *finie* si $H_i=(1)$ à partir d'une certaine valeur de i; resp. *séparante* si $\bigcap_i H_i=(1)$; (H_i) est une *suite centrale* si $(G, H_i)\subset H_{i+1}$ pour tout i; resp. une N-*suite* si $(H_i, H_j)\subset H_{i+j}$ pour tout i, j.

Lemme (3.1). — *Soit* G *un groupe nilpotent de classe au plus égale à* c, x *et* y *deux éléments de* G. *Alors :*

a. Si $(x^r, y^s)=1$, $(x, y)^{(rs)^{c-1}}=1$;

b. Si $x^r=y^s=1$ *et si* t *désigne le plus grand commun diviseur des entiers* r *et* s, $(xy)^{rst^{c-2}}=1$.

Démonstration. — Considérons le sous-groupe H de G engendré par x et y, et sa suite centrale descendante (H_i). La classe de H ne dépasse pas celle de G, et ainsi $H_{c+1}=(1)$. Considérons (*cf.* chap. I, § 2) l'anneau de Lie $\mathfrak{L}(H_i)=\Sigma_i H_i/H_{i+1}$. Il est engendré par les classes $\tilde{x}$ et $\tilde{y}$ de x et y mod H_2; $\tilde{x}$ et $\tilde{y}$ sont de degré 1 dans $\mathfrak{L}(H_i)$, et les éléments de degré 2 sont des multiples entiers de $[\tilde{x}, \tilde{y}]$. Nous en déduisons que si, pour un entier n, $n[\tilde{x}, \tilde{y}]=0$, $n\tilde{z}=0$ pour tout $\tilde{z}\in\mathfrak{L}(H_i)$, $\tilde{z}$ étant homogène de degré ≥ 2. Il suffit de raisonner par récurrence sur le degré de $\tilde{z}$: si $\tilde{z}$ est homogène de degré $i\geq 3$, $\tilde{z}$ est une somme de crochets $[\tilde{u}, \tilde{v}]$, où $\deg\tilde{u}+\deg\tilde{v}=i$; alors une au moins des relations $2\leq\deg\tilde{u}<i$ et $2\leq\deg\tilde{v}<i$ est vérifiée; si, par exemple, $2\leq\deg\tilde{u}<i$, $n\tilde{u}=0$ par l'hypothèse de récurrence, donc $n\tilde{z}=0$. Revenant à la définition de $\mathfrak{L}(H_i)$, nous voyons que $z\in H_i$ implique $z^n\in H_{i+1}$ et, par une récurrence évidente $z^{n^j}\in H_{i+j}$. En particulier, $z\in H_2$ implique $z^{n^{c-1}}=1$.

Alors, dans le cas *a*, $rs[\tilde{x}, \tilde{y}]=0$, puisque $rs[\tilde{x}, \tilde{y}[=[r\tilde{x}, s\tilde{y}]$ s'identifie à la classe de (x^r, y^s) mod H_3. Ainsi $(x, y)^{(rs)^{c-1}}=1$.

Dans le cas *b*,

$$r[\tilde{x}, \tilde{y}]=[r\tilde{x}, \tilde{y}]=0 \qquad \text{et} \qquad s[\tilde{x}, \tilde{y}]=[\tilde{x}, s\tilde{y}]=0,$$

puisque ces éléments s'identifient respectivement aux classes mod H_3 de (x^r, y) et (x, y^s). Il existe des entiers r' et s' tels que

$$r'r+s's=t, \qquad \text{d'où} \qquad t[\tilde{x}, \tilde{y}]=0.$$

Enfin x et y commutent modulo H_2, si bien que $(xy)^{\frac{rs}{t}}\in H_2$, et ainsi $(xy)^{rst^{c-2}}=1$.

A partir de ce lemme, on démontre immédiatement des théorèmes classiques de la théorie des groupes nilpotents, tels que : l'ensemble des éléments de P-torsion d'un groupe nilpotent est un sous-groupe ; un groupe nilpotent de torsion est le produit direct de ses sous-groupes de Sylow, etc.

THÉORÈME (3.2). — *Soit, dans un groupe* G, (H_i) *une suite centrale finie (resp. une* N*-suite finie). La condition nécessaire et suffisante pour qu'il existe une suite centrale finie [respectivement* N*-suite finie]* (K_i), *telle que, pour tout* i, $H_i \subset K_i$ *et que* K_i/K_{i+1} *soit sans* P_i*-torsion, est que* H_i *soit sans* P_i*-torsion (pour tout* i*).*

Démonstration. — La condition est nécessaire. En effet, supposons l'existence d'une suite (K_i) de sous-groupes de G ayant les propriétés voulues. Soit $x \in H_i$, n/P_i, $x^n = 1$. Alors, si $x \neq 1$, il existe j tel que $x \in K_j$ et $x \notin K_{j+1}$ [puisque (K_i) est finie]. De plus $j \geq i$, puisque $K_i \supset H_i$. Alors n/P_j (puisque $P_j \supset P_i$), et $x^n = 1 \in K_{j+1}$ implique $x \in K_{j+1}$, contrairement à l'hypothèse (puisque K_j/K_{j+1} est sans P_j-torsion).

La condition est suffisante. Supposons chaque H_i sans P_i-torsion. Définissons F_j par la relation : $x \in F_j$ si et seulement s'il existe n/P_{j-1} tel que $x^n \in H_j$ $(j \geq 1)$. Si nous considérons l'homomorphisme canonique f_j de G sur G/H_j, nous voyons que $x \in F_j$ si et seulement si $f_j(x)$ est un élément de P_{j-1}-torsion dans G/H_j. F_j est donc un sous-groupe invariant de G, contenant H_j (c'est l'image réciproque, par f_j, du sous-groupe de (P_{j-1}-torsion de G/H_j).

Posons maintenant $L_i = \bigcap_{j=1}^{i} F_j$. Alors L_i est un sous-groupe invariant de G,

$$L_1 = G \supset L_2 \supset \ldots \supset L_i \supset L_{i+1} \supset \ldots,$$

et $L_i \supset H_i$ pour tout i. Montrons que $H_{c+1} = (1)$ entraîne $L_{c+1} = (1)$. Soit $x \in L_{c+1}$. Il existe alors des entiers $n_1, \ldots, n_c$ tels que n_i/P_i et $x^{n_i} \in H_{i+1}$. Supposons démontré que $x^{n_i} = 1$ $(i \geq 2)$. Alors $x^{n_{i-1}} \in H_i$ et $(x^{n_{i-1}})^{n_i} = 1$, ce qui implique $x^{n_{i-1}} = 1$. Comme $x^{n_i} \in H_{i+1} = (1)$, on parvient à $x^{n_1} = 1$ qui implique $x = 1$. Montrons que L_i/L_{i+1} est sans P_i-torsion. Soit $x \in L_i$, n/P_i, $x^n \in L_{i+1}$. Puisque $L_{i+1} = L_i \cap F_{i+1}$, il suffit d'établir que $x \in F_{i+1}$. Or, puisque $x^n \in F_{i+1}$, il existe n'/P_i tel que $(x^n)^{n'} \in H_{i+1}$. Mais nn'/P_i et ainsi $x^{nn'} \in H_{i+1}$, ce qui implique $x \in F_{i+1}$. Nous avons donc établi le théorème dans le cas d'une suite finie de sous-groupes invariants. Montrons de plus que si (K_i) est une suite finie de sous-groupes invariants telle que, pour tout i, $H_i \subset K_i$ et que K_i/K_{i+1} soit sans P_i-torsion, $L_i \subset K_i$ pour tout $L_i \subset K_i$. Sinon nous pourrions trouver $x \in L_i$ et $j < i$ avec $x \in K_j$, $x \notin K_{j+1}$. Mais alors $x \in F_{j+1}$; donc il existe n/P_j tel que $x^n \in H_{j+1} \subset K_{j+1}$. Puisque K_j/K_{j+1} est sans P_j-torsion, $x \in K_{j+1}$, contrairement à l'hypothèse. La suite (L_i) est donc celle qui décroît le plus vite parmi les suites répondant à la question.

Utilisons maintenant le fait que (H_i) est une suite centrale. Soit $x \in G$,

$y \in L_i$. Pour tout j tel que $1 \leq j \leq i$, il existe n_j/P_{j-1} tel que $y^{n_j} \in H_j$. Donc $(x, y^{n_j}) \in H_{j+1}$ et ainsi $(x, y)^{n_j^{c-1}} \in H_{j+1}$ [appliquer (3.1 a) à G/H_{j+1}]. Comme n_j^{c-1}/P_j, $(x, y) \in F_{j+1}$ pour $1 \leq j \leq i$, et $(x, y) \in L_{j+1}$, ce qui montre que (L_i) est une suite centrale.

Enfin, supposons que (H_i) soit une N-suite. Soit $x \in L_i$ et $y \in L_j$. Nous voulons montrer que $(x, y) \in L_{i+j}$. Pour tout k tel que $2 \leq k \leq i+j$, nous pouvons trouver i' et j' tels que $1 \leq i' \leq i$, $1 \leq j' \leq j$ et $i'+j' = k$. Alors, puisque $x \in F_{i'}$ et $y \in F_{j'}$, il existe $m/P_{i'-1}$ et $n/P_{j'-1}$ tels que $x^m \in H_{i'}$, $y^n \in H_{j'}$, et ainsi $(x^m, y^n) \in H_k$. Appliquant (3.1 a) à G/H_k, nous voyons que $(x, y)^{(mn)^{c-1}} \in H_k$, donc $(x, y) \in F_k$, puisque mn/P_{k-1}. Ainsi $(x, y) \in L_{i+j}$.

Lemme (3.3). — *Soit* (H_i) *une suite centrale séparante dans* G *supposé* (H_i)*-complet* [16] *:*

a. Si H_i/H_{i+1} *est* P_i*-divisible pour tout* i*, chaque* H_i *est* P_i*-divisible.*

b. Si H_i/H_{i+1} *est sans* P_i*-torsion pour tout* i*,* $x \in H_i$*,* $y \in H_i$*,* n/P_i *et* $x^n = y^n$ *impliquent* $x = y$*. En particulier,* H_i *est sans* P_i*-torsion.*

c. Si H_i *est* P_i*-divisible et sans* P_i*-torsion pour tout* i*, alors* H_i/H_{i+1} *est* P_i*-divisible et sans* P_i*-torsion pour tout* i*.*

d. Si tous les P_i *sont égaux à un même ensemble de nombres premiers* P*, et si, pour tout* i*,* H_i/H_{i+1} *est sans* P*-torsion, alors* $x \in H_i$*,* n/P et $y^n = x$ *impliquent* $y \in H_i$*. En particulier, si* G *est* P*-divisible, il en est de même de tous les* H_i*.*

Démonstration. — *a.* Soit $x \in H_i$, n/P_i. Supposons établie l'existence d'un $y \in H_i$ tel que $y^n \equiv x \pmod{H_{i+j}}$, $j \geq 0$. Alors $xy^{-n} \in H_{i+j}$ et H_{i+j}/H_{i+j+1} est P_i-divisible. Il existe donc $z \in H_{i+j}$ tel que $z^n \in xy^{-n} \pmod{H_{i+j+1}}$ et, puisque (H_i) est une suite centrale,

$$x \equiv (yz)^n \pmod{H_{i+j+1}}, \qquad \text{avec} \quad yz \equiv y \pmod{H_{i+j}}.$$

b. Si l'on avait $x \neq y$, soit $x = yz$, $z \in H_j$, $z \notin H_{j+1}$ (avec $j \geq i$). Alors $y^n \equiv y^n z^n \pmod{H_{j+1}}$, et puisque H_j/H_{j+1} est sans P_i-torsion, $z \in H_{j+1}$ contrairement à l'hypothèse.

c. Il est évident que H_i/H_{i+1} est P_i-divisible (comme groupe quotient d'un groupe P_i-divisible). Montrons que si H_i/H_{i+1} n'était pas sans P_i-torsion, H_i aurait un élément de P_i-torsion. Nous pourrions trouver en effet n/P_i, $x \in H_i$, $x \notin H_{i+1}$, avec $x^n \in H_{i+1}$. Supposons déjà construit $y \in xH_{i+1}$ tel que $y^n \in H_{i+j}$. Alors il existe $z \in H_{i+j}$, avec $z^n = y^n$ et, par conséquent, $(yz^{-1})^n \in H_{i+j+1}$, $yz^{-1} \equiv y \pmod{H_{i+j}}$. Il en résulte donc l'existence dans H_i d'un élément $u \notin H_{i+1}$ avec $u^n = 1$, contrairement à l'hypothèse.

d. Soit $y \in H_j$, $y \notin H_{j+1}$. Alors $x = y^n \notin H_{j+1}$ et ainsi $j \geq i$, $y \in H_i$.

---

(16) C'est-à-dire que G est complet pour la topologie où les sous-groupes (H_i) forment un système fondamental de voisinages de l'élément neutre.

LEMME (3.4) (Unicité des prolongements d'homomorphismes). — *Soient* G *un groupe*, G' *un sous-groupe de* G, (K_i) *une suite finie de sous-groupes invariants de* G *telle que, pour tout* i, $K_i/(G' \cap K_i)K_{i+1}$ *soit un groupe de* P_i*-torsion. Soit, d'autre part,* H *un groupe,* (L_i) *une suite centrale finie dans* H *telle que, pour tout* i, L_i/L_{i+1} *soit sans* P_i*-torsion. Soient enfin* f *et* g *deux homomorphismes de* G *dans* H *tels que* $f(K_i) \subset L_i$ *et* $g(K_i) \subset L_i$ *pour tout* i. *Alors* f *et* g *sont identiques si leurs restrictions à* G' *coïncident.*

Démonstration. — Supposons démontré que f et g coïncident sur K_{i+1}, et montrons que f et g coïncident sur K_i [l'hypothèse de récurrence sera évidemment satisfaite pour i assez grand, puisque (K_i) est finie]. Soit $x \in K_i$. Par hypothèse il existe n/P_i, $y \in G'$, $z \in K_{i+1}$ tels que $x^n = yz$. Alors

$$f(x^n) = f(yz) = f(y)f(z) = g(y)g(z) = g(yz) = g(x^n).$$

Ainsi

$$f(x)^n = g(x)^n, \qquad f(x) \in L_i, \quad g(x) \in L_i, \quad \text{ce qui implique } f(x) = g(x), \text{ d'après } (3.3b).$$

LEMME (3.5) (Existence du prolongement simple). — *Soient* G *un groupe*, G' *un sous-groupe invariant de* G, (K_i) *une suite centrale finie dans* G. *On suppose que* $G' \supset K_{j+1}$ *et que* G/G' *est un groupe cyclique d'ordre* n, *avec* n/P_j, *engendré par la classe* $\bmod G'$ *d'un élément* x *de* K_j. *Soient, d'autre part,* H *un groupe,* (L_i) *une suite centrale finie dans* H *telle que chaque* L_i/L_{i+1} *soit sans* P_i*-torsion. Soit enfin* f *un homomorphisme de* G' *dans* H *tel que* $f(G' \cap K_i) \subset L_i$ *pour tout* i. *Alors, il existe un prolongement* g *de* f *à* G *tel que, pour tout* i, $g(K_i) \subset L_i$ *si et seulement s'il existe* $u \in L_j$ *tel que* $u^n = f(x^n)$.

Démonstration. — La condition est évidemment nécessaire. Supposons-la satisfaite. Tout élément de G s'écrit sous la forme $x^r y$, $y \in G'$. Posons $g(x^r y) = u^r f(y)$; g est alors une application univoque de G dans H. Si, en effet,

$$x^r y = x^{r'} y', \qquad x^{r-r'} = y' y^{-1} \in G'.$$

Donc

$$r - r' = ns, \qquad y' y^{-1} = (x^n)^s \qquad \text{et} \qquad f(y')f(y)^{-1} = u^{ns},$$

d'où

$$u^r f(y) = u^{r'} f(y'),$$

ce qui montre que g est univoque.

Soit maintenant $y \in G'$; alors $xyx^{-1} \in G'$ et, si g est un homomorphisme, on doit avoir

$$f(xyx^{-1}) = uf(y)u^{-1}.$$

Nous allons démontrer la relation équivalente

$$f\big((x, y)\big) = \big(u, f(y)\big).$$

Considérons la suite typique (x^t, y) à valeurs dans K_{j+1}. D'après (1.10), il existe une suite finie d'éléments de K_{j+1} : $a_1, \ldots, a_l$ telle que

$$(x^t, y) = a_1^t a_2^{\binom{t}{2}} \ldots a_l^{\binom{t}{l}}.$$

De plus $a_1 = (x, y)$. Alors, appliquant l'homorphisme f :

$$f\big((x^t, y)\big) = f(a_1)^t \ldots f(a_l)^{\binom{t}{l}}.$$

Considérons, d'autre part, la suite typique $\big(u^t, f(y)\big)$ dans L_{j+1}. D'après (1.10), il existe une suite finie d'éléments de L_{j+1} : $b_1, \ldots, b_m$ telle que

$$\big(u^t, f(y)\big) = b_1^t \ldots b_m^{\binom{t}{m}}.$$

De plus, $b_1 = \big(u, f(y)\big)$. Posons maintenant $t = nt'$; pour toutes les valeurs entières de t', $f\big((x^{nt'}, y)\big) = \big(u^{nt'}, f(y)\big)$. Ainsi

$$f(a_1)^{nt'} \ldots f(a_l)^{\binom{nt'}{l}} = b_1^{nt'} \ldots b_m^{\binom{nt'}{m}}$$

pour toutes les valeurs entières de t'. D'après (1.7d) que nous appliquons au groupe L_{j+1} avec sa suite centrale $L_{j+i}(i \geqq 1)$, en prenant $P_i(t) = \binom{nt}{i}$, cela implique $f(a_i) = b_i$ pour tout i, et, en particulier

$$f(a_1) = f\big((x, y)\big) = b_1 = \big(u, f(y)\big).$$

Nous avons donc $f(xyx^{-1}) = uf(y)u^{-1}$ et, par une récurrence évidente,

$$f(x^r y x^{-r}) = u^r f(y) u^{-r}$$

pour tout entier r. Il en résulte que g est un homomorphisme. Soient, en effet, $x^r y$ et $x^{r'} y'$ deux éléments de $G(y, y' \in G')$. Ainsi

$$x^r y x^{r'} y' = x^{r+r'} x^{-r'} y x^{r'} y'.$$

Alors

$$g(x^r y x^{r'} y') = u^{r+r'} f(x^{-r'} y x^{r'} y') = u^{r+r'} f(x^{-r'} y x^{r'}) f(y') = u^r f(y) u^{r'} f(y') = g(x^r y) g(x^{r'} y').$$

Il reste seulement à démontrer que $g(K_i) \subset L_i$ pour i. Soit d'abord $i \leqq j$; alors $x^r y \in K_i$, $y \in G'$ impliquent $y \in G' \cap K_i$. Dans ce cas

$$g(x^r y) = u^r f(y) \in L_i, \qquad \text{puisque} \quad u \in L_j \quad \text{et} \quad f(G' \cap K_i) \subset L_i.$$

Si maintenant $i > j$,

$$x^r y \in K_i \subset G' \qquad \text{et} \qquad g(x^r y) = f(x^r y) \in L_i.$$

Théorème (3.6). — *Soient* G *un groupe,* G′ *un sous-groupe de* G, (K_i) *une suite centrale finie dans* G, *telle que, pour tout* i, $K_i/(K_i \cap G')K_{i+1}$ *soit un groupe de* P_i*-torsion. Soient* H *un groupe,* (L_i) *une suite centrale finie dant* H *telle que, pour*

tout i, L_i/L_{i+1} soit P_i-divisible et sans P_i-torsion. Soit enfin f un homomorphisme de G' dans H tel que, pour tout i, $f(G' \cap K_i) \subset L_i$. Alors il existe un homomorphisme g et un seul de G dans H, prolongeant f, et tel que $g(K_i) \subset L_i$ pour tout i.

Démonstration. — Nous considérons les couples (Γ, h) constitués par un sous-groupe Γ de G contenant G', et un homomorphisme h de Γ dans H, prolongeant f, et tel que $h(\Gamma \cap K_i) \subset L_i$ (pour tout i). Nous introduisons naturellement une relation d'ordre dans l'ensemble de ces couples, en posant $(\Gamma_1, h_1) \leqq (\Gamma_2, h_2)$ si $\Gamma_1 \subset \Gamma_2$ et si h_2 est un prolongement de h_1. Alors l'ensemble ainsi ordonné est inductif, et d'après le lemme classique de Zorn, il existe un couple (Γ', h') maximal. Montrons que $\Gamma' = G$. Sinon soit $j+1$ le plus petit entier tel que $K_{j+1} \subset \Gamma'$. Soit $x \in K_j$, $x \notin \Gamma'$. Alors $x\Gamma' x^{-1} = \Gamma'$. Soit Γ le sous-groupe de G engendré par Γ' et x. Γ/Γ' est un groupe cyclique engendré par la classe de x modulo Γ', et d'ordre n avec n/P_j. Puisque chaque L_i/L_{i+1} est P_i-divisible, L_j est P_j-divisible (3.3a). Donc il existe $u \in L_j$ tel que $u^n = h'(x^n)$. Nous pouvons donc appliquer (3.5), en faisant jouer à Γ, Γ', $(\Gamma \cap K_i)$, x, h' les rôles respectifs de G, G', (K_i), x, f dans l'énoncé de ce lemme. Nous en déduisons l'existence d'un prolongement h de h' à Γ tel que $h(\Gamma \cap K_i) \subset L_i$ pour tout i, contrairement à l'hypothèse que (Γ', h') est maximal. Ainsi $\Gamma' = G$, le prolongement g de f à G existe et est unique d'après (3.4).

Définition (3.7). — Soit G un groupe, (K_i) une suite centrale finie telle que, pour tout i, K_i/K_{i+1} soit sans P_i-torsion. Nous dirons qu'un groupe $\overline{G}$ contenant G comme sous groupe et muni d'une suite centrale finie $(\overline{K}_i)$ est une (P_i, K_i)-complétion de G si $K_i = \overline{K}_i \cap G$, $\overline{K}_i/\overline{K}_{i+1}$ est sans P_i-torsion et P_i-divisible et enfin $\overline{K}_i/K_i\overline{K}_{i+1}$ est un groupe de P_i-torsion, pour tout $i \geqq 1$ ([16]).

Nous démontrerons que, sous les hypothèses de (3.7), un groupe G admet une (P_i, K_i)-complétion qui est bien déterminée à un isomorphisme canonique près. Nous pouvons considérer cette proposition comme classique dans le cas des groupes abéliens :

Soit A un groupe abélien sans P-torsion ; alors il existe un groupe abélien $\overline{A}$, dit P-complétion de A, tel que $\overline{A}$ contienne A, soit sans P-torsion, P-divisible et que $\overline{A}/A$ soit un groupe de P-torsion. Ces propriétés déterminent $\overline{A}$ à un isomorphisme canonique près conservant les éléments de A ; si de plus B est un groupe sans P-torsion, contenant A et tel que B/A soit un groupe de P-torsion, B s'identifie canoniquement à un sous-groupe de $\overline{A}$ ([17]).

([16]) Pour simplifier les énoncés, nous nous sommes permis un abus de langage en considérant une extension de G comme un groupe contenant G. Il serait plus correct de parler d'un groupe contenant une image isomorphe déterminée de G.

([17]) Rappelons que $\overline{A}$ peut être obtenu comme un produit tensoriel $Q_P \otimes A_P$, où Q_P désigne l'anneau des nombres rationnels de la forme $\frac{r}{s}$, où $r \in Z$, s/P.

Considérons d'abord un groupe G et une suite centrale (resp. N-suite) finie (K_i) dans G telle que K_i/K_{i+1} soit sans P_i-torsion pour tout i et que K_i/K_{i+1} soit P_i-divisible pour $i \geqq j+1$, j désignant un entier positif fixé. Soient G^1 une extension de G, (K_i^1) une suite centrale (resp. N-suite) finie dans G^1. On suppose que :

$$G^1 = G K_j^1, \qquad G \cap K_i^1 = K_i;$$

K_i^1/K_{i+1}^1 est sans P_i-torsion ; $K_i^1/K_iK_{i+1}^1$ est un groupe de P_i-torsion (pour tout i). On démontre facilement que ces conditions impliquent que

$$K_i^1 = K_i \quad \text{pour } i \geqq j+1 \qquad \text{et que} \qquad K_i^1 = K_iK_{i+1}^1 \quad \text{pour } 1 \leqq i \leqq j-1.$$

Par conséquent,

$$K_i^1/K_iK_{i+1}^1 = (1) \qquad \text{pour} \quad i \neq j.$$

Désignons par A le groupe abélien sans P_j-torsion K_j/K_{j+1}, et par $\overline{A}$ une P_j-complétion de A déterminée. Nous pouvons considérer $K_j^1/K_{j+1}^1 = K_j^1/K_{j+1}$ comme une extension de K_j/K_{j+1}. Le quotient $(K_j^1/K_{j+1})/(K^j/K_{j+1})$ s'identifie à K_j^1/K_j et est donc un groupe de P_j-torsion. Par conséquent, K_j^1/K_{j+1} s'identifie canoniquement à un sous-groupe de A^1 de $\overline{A}$ (avec $A \subset A_1 \subset \overline{A}$).

Soit G^2 une extension de G munie d'une suite centrale (resp. N-suite) (K_i^2) possédant, par rapport à $G(K_i)$ les mêmes propriétés que G^1, (K_i^1). Il lui correspond un sous-groupe A^2 de $\overline{A}$. Interprétons la relation d'inclusion $A^1 \subset A^2$. Soit $x^{(1)} \in K_j^1$; alors il existe n/P_j tel que $(x^{(1)})^n = x \in K_j$; la relation $A^1 \subset A^2$ signifie qu'il existe dans K_j^2 un élément $x^{(2)}$ tel que

$$(x^{(2)})^n = x \qquad (\mathrm{mod}\, K_{j+1}).$$

Mais, puisque K_i/K_{i+1} est P_i-divisible pour $i \geqq j+1$, la démonstration du lemme $(3.3a)$ montre qu'on peut choisir $x^{(2)}$ de telle sorte que

$$(x^{(2)})^n = x = (x^{(1)})^n.$$

Alors, en appliquant comme dans la démonstration du théorème (3.6), le lemme de Zorn et le lemme (3.5), on démontre que la relation $A^1 \subset A^2$ équivaut à l'existence d'un homomorphisme f de G^1 dans G^2, induisant l'identité sur G et tel que $f(K_i^1) \subset K_i^2$ pour tout i; f est nécessairement unique d'après (3.4); et l'on démontre immédiatement que c'est un isomorphisme.

Nous voyons donc que la donnée de A^1 détermine l'extension G^1, (K_i^1) à un isomorphisme canonique près conservant les éléments de G. A quels sous-groupes de $\overline{A}$ contenant A correspondent effectivement des extensions de G? On démontre sans peine que, si A^1 correspond à une extension, il en est de même de tout sous-groupe de A^1 contenant A. Nous voulons démontrer qu'il correspond une extension à $\overline{A}$ lui-même; pour cela nous appliquons encore le lemme de Zorn : l'ensemble, ordonné par inclusion, des sous-groupes de $\overline{A}$

contenant A et auxquels correspondent des extensions est inductif. Soit, en effet, $(A^\iota)_{\iota\in I}$ une famille de tels sous-groupes, ι parcourant un ensemble I totalement ordonné ([18]). Nous choisissons des modèles G^ι, (K_i^ι) des extensions correspondantes, qui sont déterminés à des isomorphismes canoniques près. Pour $\iota<\lambda$, nous avons, un isomorphisme déterminé $f_{\lambda\iota}$ de G^ι, (K_i^ι) dans G^λ, (K_i^λ), la propriété de transitivité permettant de considérer la limite inductive $\hat{G}$, $(\hat{K}_i)$ des G^ι, (K_i^ι) est satisfaite, et l'on démontre immédiatement que $\hat{G}$, $(\hat{K}_i)$ possède les propriétés voulues et correspond à la réunion des sous-groupes A^ι. D'après le lemme de Zorn, l'existence d'une extension G correspondant à $\overline{A}$ est donc ramenée au problème suivant : si K_j/K_{j+1} n'est pas P_j-divisible, existe-t-il une extension propre G^1, (K_i^1) de G ayant les propriétés indiquées? Établissons d'abord le :

LEMME (3.8). — *Soit* G *un groupe,* (K_i) *une suite centrale finie dans* G *telle que* K_i/K_{i+1} *soit* P_i*-divisible et sans* P_i*-torsion pour* $i\geq j+1$ (j *désignant un entier positif fixe*). *Soit* α *un automorphisme de* G *tel que :*

(A) : *pour tout* i *et tout* $x\in K_i$, $\alpha x.x^{-1}\in K_{i+j}$ [*ou resp.* (B) *pour tout* $x\in G$, $\alpha x.x^{-1}\in K_{j+1}$ *et, pour tout* i *et tout* $x\in K_i$, $\alpha x.x^{-1}\in K_{i+1}$].

Alors si n/P_{j+1}, *il existe un automorphisme* β *de* G *et un seul vérifiant* (A) [*resp.* (B)] *et tel que* $\beta^n=\alpha$.

Démonstration. — Soit c la longueur de la suite centrale (K_i), c'est-à-dire l'entier c tel que $K_c\neq(1)$ et $K_{c+1}=(1)$. Notre démonstration va procéder par récurrence sur c. Remarquons d'abord que si $c\leq j$, la condition (A) [resp. (B)] implique que α et β sont l'automorphisme identique, et la proposition est triviale. Nous allons donc supposer $c\geq j+1$, et la proposition démontrée pour les suites de longueur strictement inférieure à c.

1° Considérons le groupe $G^\star=G/K_c$ avec sa suite centrale $(K_i^\star)$ définie par $K_i^\star=K_i/K_c$ pour $1\leq i\leq c-1$, et $K_i^\star=(1)$ pour $i\geq c$. La longueur de $(K_i^\star)$ est au plus $c-1$; l'automorphisme α conserve K_c et définit donc un automorphisme $\alpha^\star$ de $G^\star$. Nous voyons immédiatement que les conditions imposées à (K_i) et α sont satisfaites dans le groupe $G^\star$ pour $(K_i^\star)$ et $\alpha^\star$. Il existe un automorphisme $\beta^\star$ de $G^\star$ et un seul, vérifiant (A) [resp. (B)] par rapport à $(K_i^\star)$ et tel que $(\beta^\star)^n=\alpha^\star$.

Considérons le groupe K_2 avec sa suite centrale (K_i'), où $K_i'=K_{i+1}$. (K_i') est de longueur $c-1$. La restriction de α à K_2 vérifie la condition (A) [resp. vérifie la condition (B) en remplaçant j par $\mathrm{Sup}(j-1, 1)$]. Dans tous les cas, les hypothèses faites sur G, (K_i) et α sont vérifiées pour K_2, (K_i') et la restriction de α. Il existe donc un automorphisme γ de K_2 et un seul, vérifiant (A) [resp. (B) modifiée] et tel que γ^n coïncide avec la restriction de α.

([18]) Les A^ι sont eux-mêmes ordonnés par inclusion.

Considérons enfin le groupe $K_2/K_c = K_2^*$, avec sa suite centrale $(K_i'^*)$ ([19]), de longueur $\leqq c-2$. Les hypothèses du lemme sont vérifiées pour K_2^*, $(K_i'^*)$ et la restriction de α^* à K_2^*. Nous déduisons donc de notre hypothèse de récurrence (concernant l'unicité) que la restriction de β^* à K_2^* coïncide avec γ^* (obtenu à partir de γ par passage aux quotients).

2° Nous allons chercher à établir l'existence d'un automorphisme β_1 de G conservant K_c et tel que l'automorphisme β_1^* de G^* obtenu par passage aux quotients coïncide avec β^*. Nous commençons par choisir une application β_1 de G dans lui-même telle que la classe $\bmod K_c$ de $\beta_1(x)$ ne dépende que de la classe $\bmod K_c$ de x, et que l'application β_1^* de G^* dans lui-même associé à β_1 coïncide avec β^* : cela peut se faire, par exemple, en choisissant un système de représentants pour les classes de G $\bmod K_c$. Le fait que β^* soit un automorphisme implique :

$$\beta_1(xy) = \beta_1(x)\beta_1(y)g(x, y), \qquad \text{où} \quad x \in G,\ y \in G,\quad g(x, y) \in K_c.$$

Si l'on modifie généralement le choix de β_1, on devra remplacer $\beta_1(x)$ par

$$\beta_1'(x) = \beta_1(x)f(x),$$

où f désigne une application quelconque de G dans K_c. Alors,

$$\begin{aligned}\beta_1'(xy) &= \beta_1(xy)f(xy) = \beta_1(x)\beta_1(y)g(x, y)f(x, y)\\ &= \beta_1'(x)\beta_1'(y)g(x, y)f(x, y)f(x)^{-1}f(y)^{-1}.\end{aligned}$$

Nous avons utilisé le fait que K_c est contenu dans le centre de G. Ainsi $g(x, y)$ se trouve remplacé par $g(x, y)f(xy)f(x)^{-1}f(y)^{-1}$. Or, nous voulons remplacer $g(x, y)$ par 1. $\beta_1(x)$ peut donc être choisi parmi les automorphismes de G si et seulement s'il existe $f: G \to K_c$ telle que

$$g(x, y) = f(x)f(y)f(x, y)^{-1}.$$

Remarque. — En calculant de deux manières différentes $\beta_1(xyz)$, nous verrions que, quel que soit l'automorphisme β^* de G/K_c que nous cherchons à « remonter » dans G,

$$g(y, z)g(xy, z)^{-1}g(x, yz)g(x, y)^{-1} = 1.$$

β^* définit donc un élément du second groupe de cohomologie $H^2(G/K_c, K_c)$ qui doit être nul. Le résultat s'interprète facilement dans le langage de la cohomologie : le groupe des automorphismes de G/K_c opère (à droite) sur $H^2(G/K_c, K_c)$ et l'élément de $H^2(G/K_c, K_c)$ correspondant à l'extension G doit être invariant par β^*.

3° Supposons que nous ayons pu choisir β_1 de telle sorte que β_1 coïncide

---

([19]) $K_i'^* = K_{i+1}^*$.

avec γ sur K_2 et que $g(x, y)$ ne dépende que des classes de x et de $y \bmod K_2$. Alors

$$g(1, x) = g(x, 1) = 1 \qquad \text{et} \qquad \beta_1(xy) = \beta_1(x)\beta_1(y)$$

si x ou y appartient à K_2. Étudions les puissances de β_1,

$$\begin{aligned}\beta_1^2(xy) &= \beta_1\big(\beta_1(x)\beta_1(y)g(x, y)\big) = \beta_1\big(\beta_1(x)\beta_1(y)\big)g(x, y)\\ &= \beta_1^2(x)\beta_1^2(y)g\big(\beta_1(x), \beta_1(y)\big)g(x, y).\end{aligned}$$

Mais $\beta_1(x).x^{-1} \in K_2$ et $\beta_1(y)y^{-1} \in K_2$. Donc

$$g\big(\beta_1(x), \beta_1(y)\big) = g(x, y) \qquad \text{et} \qquad \beta_1^2(xy) = \beta_1^2(x)\beta_1^2(y)g(x, y)^2.$$

Par une récurrence évidente, on démontre que

$$\beta_1^r(xy) = \beta_1^r(x)\beta_1^r(y)g(x, y)^r,$$

pour tout entier positif r. Mais l'automorphisme α vérifie $\alpha(x) = \beta_1^n(x)f(x)$, où f est une application de G dans K_c. Nous en déduisons, d'après ce qui précède :

$$g(x, y)^n = f(x)f(y)f(xy)^{-1}.$$

K_c est abélien, sans P_{j+1}-torsion et P_{j+1}-divisible. Il existe donc une application déterminée f' de G dans K_c telle que

$$f'(x)^n = f(x) \qquad \text{et} \qquad g(x, y)f'(xy)f'(x)^{-1}f'(y)^{-1} = 1,$$

ce qui nous permet de choisir pour β_1 un automorphisme de G.

4° Si β_1 coïncide avec γ sur K_2, et si $g(x, y)$ ne dépend que des classes mod K_2 de x et de y, nous avons pour $x \in G$, $y \in K_2$:

$$\beta_1(xy) = \beta_1(x)\beta_1(y)g(x, y) = \beta_1(x)\gamma(y)g(x, 1) = \beta_1(x)\gamma(y).$$

De même :

$$\beta_1(yx) = \gamma(y)\beta_1(x).$$

Nous allons d'abord chercher à vérifier la première relation. Soit $x \in G$, $x \notin K_2$; choisissons arbitrairement $\beta_1(x)$. Alors tout élément de xK_2 s'écrit univoquement sous la forme xy, avec $y \in K_2$, et nous devrons prendre $\beta_1(xy) = \beta_1(x)\gamma(y)$. Nous aurons alors

$$\beta_1(xyy') = \beta_1(x)\gamma(yy') = \beta_1(x)\gamma(y)\gamma(y') = \beta_1(xy)\gamma(y'),$$

c'est-à-dire que la première relation sera vérifiée sur la classe xK_2. Cherchons si, de plus, la deuxième relation peut être vérifiée : nous avons certainement

$$\beta_1(yx) = \gamma(y)\beta_1(x)\theta(y),$$

où θ désigne une application de K_2 dans K_c. On voit immédiatement que θ ne dépend pas du choix de $\beta_1(x)$ [une modification de ce choix conduit à multi-

plier tous les $\beta_1(x)$ par un même élément de K_c quand x parcourt la classe modK_2 considérée]. De même, $\theta(y)$ est indépendant du choix de x comme représentant de la classe xK_2, car

$$\beta_1(yxy') = \beta_1(yx)\gamma(y') = \gamma(y)\beta_1(x)\theta(y)\gamma(y') = \gamma(y)\beta_1(xy')\theta(y) \quad \text{pour} \quad y, y' \in K_2.$$

Ainsi θ ne dépend que de β^* et de γ, et nous devons montrer que $\theta(y) = 1$. Nous savons que θ est un homomorphisme; en effet :

$$\beta_1(yy'x) = \gamma(yy')\beta_1(x)\theta(yy') = \gamma(y)\beta_1(y'x)\theta(y) = \gamma(y)\gamma(y')\beta_1(x)\theta(y')\theta(y),$$

d'où

$$\theta(yy') = \theta(y)\theta(y').$$

Cherchons à calculer les homomorphismes θ correspondant aux puissances β_1^r. Nous avons

$$\beta_1^2(yx) = \beta_1\big(\gamma(y)\beta_1(x)\theta(y)\big) = \beta_1\big(\gamma(y)\beta_1(x)\big)\theta(y) = \gamma^2(y)\beta_1^2(x)\theta\big(\gamma(y)\big)\theta(y).$$

Par une récurrence évidente, nous parvenons à

$$\beta_1^r(yx) = \gamma^r(y)\beta_1^r(x)\theta\big(\gamma^{r-1}(y)\big)\theta\big(\gamma^{r-2}(y)\big)\dots\theta(y).$$

Mais l'homomorphisme θ associé à β_1^n et γ^n doit être égal à 1, puisque le problème qui nous occupe admet comme solution l'automorphisme α. Ainsi

$$\theta(\gamma^{n-1}y)\dots\theta(y) = 1.$$

Supposons démontré $\theta(y) = 1$ pour $y \in K_{i+1}$, ce qui est évident pour $i = c$, et montrons que $\theta(y) = 1$ pour $y \in K_i$. Nous avons pour tout entier r

$$\theta\big(\gamma^r(y)\big) = \theta(y)\theta\big(y^{-1}\gamma^r(y)\big) = \theta(y),$$

puisque, pour $y \in K_i$, $y^{-1}\gamma^{r-1}(y) \in K_{i+1}$. Ainsi, pour $y \in K_i$, $\theta(y)^n = 1$, ce qui implique $\theta(y) = 1$. Finalement nous parvenons à $\theta(y) = 1$ pour tout $y \in K_2$, et nous pouvons construire un automorphisme β_1 de G, coïncidant avec γ sur K_2, et tel que $\beta_1^* = \beta^*$.

5° Formons maintenant l'automorphisme $\alpha\beta_1^{-n}$ de G. Si nous posons

$$\alpha\beta_1^{-n}(x) = x\,\delta(x),$$

nous voyons que $\delta(x) \in K_c$ pour tout $x \in G$, et que $\delta(x) = 1$ pour tout $x \in K_2$. Alors

$$xy\,\delta(xy) = x\,\delta(x)\,y\,\delta(y) = xy\,\delta(x)\,\delta(y).$$

Ainsi δ est un homomorphisme de G dans K_c. Nous déterminons univoquement $\delta'(x)$ par la condition

$$\big(\delta'(x)\big)^n = \delta(x), \qquad \delta'(x) \in K_c.$$

Alors $\beta_2(x) = x\,\delta'(x)$ représente un automorphisme de G qui permute avec l'automorphisme β_1, car $\delta'(x) = 1$ pour $x \in K_2$; nous avons

$$\beta_2''(x) = x\big(\delta'(x)\big)^n = x\,\delta(x) = \alpha\beta_1^{-n}(x).$$

Posons donc $\beta = \beta_1\beta_2$; β est un automorphisme de G répondant à toutes les conditions du lemme. Si β' est un autre automorphisme vérifiant ces conditions, nous avons

$$\beta'\beta^{-1}(x) = x\,\delta''(x),$$

où δ'' représente un homomorphisme de G dans K_r, tel que $\delta''(x) = 1$ pour $x \in K_2$. Ainsi β et β' permutent et

$$(\beta')^n\beta^{-n}(x) = x\big(\delta''(x)\big)^n = x \qquad \text{pour tout } x \in G,$$

ce qui implique

$$\delta''(x) = 1 \qquad \text{et} \qquad \beta = \beta'.$$

Remarque. — Si l'on suppose que α vérifie (A) et que β vérifie la condition plus faible (B), on en déduit facilement que β vérifie la condition (A). De même, si y est un élément de G invariant par α, y est invariant par β.

LEMME (3.9). — *Soit* G *un groupe,* (K_i) *une suite centrale (resp.* N*-suite) finie dans* G *telle que* K_i/K_{i+1} *soit sans* P_i*-torsion pour tout* i*, et* P_i*-divisible pour* $i \geq j+1$. *Soient* $y \in K_j$, $p \in P_j$ *tels qu'il n'existe pas d'élément* x *dans* K_j *avec* $x^p = y$. *Alors il existe une extension* G′ *de* G *et une suite centrale (resp.* N*-suite) finie* (K'_i) *dans* G′, *les conditions suivantes étant vérifiées :*

1° $K'_i \cap G = K_i$ *pour tout* i ;
2° $K'_i = K_i$ *pour* $i \geq j+1$;
3° $K'_i = K_iK'_{i+1}$ *pour* $1 \leq i \leq j-1$;
4° *Enfin,* K'_j *est engendré par* K_j *et un élément* x *tel que* $x^p = y$.

Démonstration. — Soit α l'automorphisme $z \to y^{-1}zy$ de G ; α vérifie la condition (B) de (3.8) dans le cas de la suite centrale, la condition (A) dans le cas de la N-suite. Nous construisons, conformément à (3.8), l'automorphisme β de G vérifiant la même condition que α, et tel que $\beta^p = \alpha$. La relation $\alpha(y) = y$ implique $\beta(y) = y$. Cela nous permet de construire un groupe G′ contenant G comme sous-groupe invariant, le quotient G′/G étant cyclique d'ordre p et engendré par la classe mod G de $x \in G'$, avec $x^p = y$; de plus, pour $z \in G$, $x^{-1}zx = \beta(z)$. Il nous suffira pour cela de prendre sur l'ensemble des couples (n, z), où n parcourt l'ensemble des entiers et z parcourt G, la loi de groupe $(n, z)(n', z') = \big(n+n', \beta^{n'}(z)z'\big)$. Puis nous prendrons le quotient de ce groupe par le sous-groupe central engendré par (p, y^{-1}). Nous identifierons $z \in G$ à la classe de $(0, z)$, et nous définirons x comme la classe de $(1, 1)$. Nous définirons dans G′ une suite de sous-groupes (K'_i) en posant $K'_i = K_i$

pour $i \geqq j+1$ et $K'_i = \{K_i, x\}$ pour $1 \leqq i \leqq j$, $\{K_i, x\}$ désignant le sous-groupe engendré par K_i et x. Les conditions (1° à 4°) de l'énoncé se vérifient immédiatement. Il reste à montrer que (K'_i) est une suite centrale (resp. N-suite) dans G'. Pour cela on remarquera que (K'_i) est en tout cas une suite de sous-groupes invariants de G', et l'on calculera le commutateur $(x^n z, x^{n'} z')$ en s'appuyant, par exemple, sur la formule

$$(ab, cd) = (b, c)^a (a, c)(b, d)^{ca} (a, d)^c \quad [cf. (1.1), \text{chap. I}]$$

et en tenant compte de ce que l'automorphisme intérieur $z \to xzx^{-1}$ vérifie la condition (B) (resp. A).

Remarquons que, pour $i \neq j$, K'_i/K'_{i+1} s'identifie à K_i/K_{i+1}, $K'_i/K'_{i+1}K_i$ étant réduit à l'élément neutre. Le quotient $K'_j/K_j K'_{j+1}$ est cyclique, d'ordre p, avec $p \in P_j$, et l'on démontre immédiatement que K'_j/K'_{j+1} est une extension cyclique, sans P_j-torsion, de K_j/K_{j+1}.

Le lemme (3.9) établit précisément le résultat qui nous manquait pour affirmer l'existence d'une (P_i, K_i)-complétion :

THÉORÈME (3.10). — *Soit* G *un groupe,* (K_i) *une suite centrale* (*resp.* N-*suite*) *finie dans* G *telle que, pour tout* i, K_i/K_{i+1} *soit sans* P_i-*torsion. Alors,* G *admet une* (P_i, K_i)-*complétion, c'est-à-dire une extension* $\overline{G}$ *munie d'une suite centrale* (*resp.* N-*suite*) *finie* $\overline{K}_i$ *de telle sorte que, pour tout* i, $K_i = \overline{K}_i \cap G$, $\overline{K}_i/\overline{K}_{i+1}$ *soit sans* P_i-*torsion et* P_i-*divisible et que* $\overline{K}_i/K_i\overline{K}_{i+1}$ *soit un groupe de* P_i-*torsion. Cette* (P_i, K_i)-*complétion est unique à un isomorphisme près conservant les éléments de* G ([20]).

Démonstration. — Supposons que l'existence de la (P_i, K_i)-complétion ait été démontrée lorsqu'on impose à G, (K_i) la condition supplémentaire que K_i/K_{i+1} est P_i-divisible pour $i \geqq j$ (ce qui est évident pour $j = 1$, le groupe G coïncidant avec sa complétion). Prenons un groupe G et une suite centrale (resp. N-suite) finie (K_i) dans G telle que K_i/K_{i+1} soit sans P_i-torsion pour tout i, et P_i-divisible pour $i \geqq j+1$. Alors le lemme (3.9) et les développements qui suivent la définition (3.7) montrent l'existence d'une extension G' de G munie d'une suite centrale (resp. N-suite) finie (K'_i) telle que, pour tout i, $K_i = G \cap K'_i$, K'_i/K'_{i+1} soit sans P_i-torsion, $K'_i/K_i K'_{i+1}$ soit un groupe de P_i-torsion et qu'enfin, pour tout $i \geqq j$, K'_i/K'_{i+1} soit P_i-divisible. La (P_i, K'_i)-complétion de G', qui existe d'après notre hypothèse de récurrence, fournit la (P_i, K_i)-complétion de G

([20]) M. Serre m'a communiqué une nouvelle démonstration de ce théorème, après avoir pris connaissance de ma rédaction. La méthode de M. Serre revient à remplacer le lemme (3.8) par l'utilisation de la suite spectrale d'une extension de groupe (*cf.* G. HOCHSCHILD et J. P. SERRE, *Trans. Amer. Math. Soc.*, t. 74, 1953, p. 110-134). Bien que M. Serre soit parvenu ainsi à un résultat plus fort, j'ai préféré laisser à mon exposé son caractère élémentaire en conservant ma démonstration originale.

cherchée. L'unicité de cette complétion, à un isomorphisme canonique près conservant les éléments de G, résulte du théorème (3.6).

Remarque. — Dans la (P_i, K_i)-complétion $\overline{G}$ de G, chaque sous-groupe $G\overline{K}_{i+1}$ est invariant dans $G\overline{K}_i$. Par contre, G n'est pas, en général, un sous-groupe invariant de $\overline{G}$.

Extension des théorèmes précédents aux N-*groupes.* — Nous allons indiquer quelles modifications dans les énoncés introduit la substitution de suites séparantes de sous-groupes aux suites finies qui interviennent dans les théorèmes de ce paragraphe.

(3.11) Si, dans la démonstration du théorème (3.2), on remplace (H_i) par une suite séparante, en conservant la définition des sous-groupes L_i, la même démonstration montre que (L_i) est une suite centrale (resp. une N-suite), que L_i/L_{i+1} est sans P_i-torsion que $L_i \supset H_i$ (pour tout i) et enfin que (L_i) décroît le plus vite parmi toutes les suites possédant cette propriété. Par contre :

$$\bigcap_i L_i = \bigcap_i F_i$$

est, en général, différent de (1). Si, par exemple, nous prenons pour chaque P_i l'ensemble de tous les nombres premiers et pour (H_i) les groupes de dimension $\mathrm{mod}\, p(G_{i,p})$ d'un groupe libre G, $L_i = G$ pour tout i, bien que $(G_{i,p})$ soit séparante et chaque $G_{i,p}$ sans torsion. Il faut donc poser comme condition supplémentaire $\bigcap_i F_i = (1)$ pour obtenir une suite séparante (L_i).

Théorème (3.12). — *Soit* G *un groupe,* G′ *un sous-groupe de* G, (K_i) *une suite centrale séparante dans* G *telle que, pour tout* i, $K_i/(K_i \cap G')K_{i+1}$ *soit un groupe de* P_i*-torsion. Soient* H *un groupe,* (L_i) *une suite centrale séparante dans* H, *telle que* H *soit* (L_i)*-complet et que, pour tout* i, L_i/L_{i+1} *soit* P_i*-divisible et sans* P_i*-torsion. Soit enfin,* f *un homomorphisme de* G′ *dans* H *tel que, pour tout* i, $f(G' \cap K_i) \subset L_i$. *Alors, il existe un homomorphisme* g *et un seul de* G *dans* H, *prolongeant* f *et tel que* $g(K_i) \subset L_i$ *pour tout* i.

Démonstration. — Par hypothèse, H s'identifie à la limite projective de ses quotients H/L_i, munis de leurs homomorphismes naturels [puisque (L_i) est séparante et $H(L_i)$-complet]; d'autre part, G s'identifie à un sous-groupe de la limite projective de ses quotients G/K_i munis de leurs homomorphismes naturels [puisque (K_i) est séparante]. Alors, le théorème (3.6) montre qu'on peut, pour tout i prolonger d'une seule manière l'homomorphisme de G dans H/L_i obtenu en composant avec f l'homomorphisme canonique de H sur H/L_i.

Plus précisément, on écrira le diagramme commutatif suivant ([21]) :

$$\begin{array}{ccccccccccc}
G/K_1 & \leftarrow & G/K_2 & \leftarrow\ldots\leftarrow & G/K_i & \leftarrow & G/K_{i+1} & \leftarrow\ldots\leftarrow & G \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
G'/G'\cap K_1 & \leftarrow & G'/G'\cap K_2 & \leftarrow\ldots\leftarrow & G'/G'\cap K_i & \leftarrow & G'/G'\cap K_{i+1} & \leftarrow\ldots\leftarrow & G' \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow f \\
H/L_1 & \leftarrow & H/L_2 & \leftarrow\ldots\leftarrow & H/L_i & \leftarrow & H/L_{i+1} & \leftarrow\ldots\leftarrow & H
\end{array}$$

D'après le théorème (3.6), il est possible, d'une manière et d'une seule d'introduire dans ce diagramme, sans détruire sa commutativité, des homomorphismes $g_i : G/K_i \to H/L_i$. L'existence et l'unicité des homomorphismes g_i entraînent immédiatement l'existence et l'unicité d'un homomorphisme g de G, dans H répondant aux conditions de (3.12).

THÉORÈME (3.13). — *Soit* G *un groupe,* (K_i) *une suite centrale* (*resp.* N-*suite*) *séparante dans* G *telle que, pour tout i,* K_i/K_{i+1} *soit sans* P_i-*torsion. Alors,* G *admet une* (P_i, K_i)-*complétion, c'est-à-dire une extension* $\overline{G}$ *munie d'une suite centrale* (*resp.* N-*suite*) *séparante* $(\overline{K}_i)$ *de telle sorte que* $\overline{G}$ *soit* $(\overline{K}_i)$-*complet et que les conditions suivantes soient vérifiées pour tout i;* $K_i = \overline{K}_i \cap G$, $\overline{K}_i/\overline{K}_{i+1}$ *est* P_i-*divisible sans* P_i-*torsion, et* $\overline{K}_i/K_i\overline{K}_{i+1}$ *est un groupe de* P_i-*torsion. Cette* (P_i, K_i)-*complétion est déterminée à un isomorphisme canonique près conservant les éléments de* G.

Démonstration. — G s'identifie à un sous-groupe de la limite projective de ses quotients G/K_j, munis de leurs homomorphismes naturels. Nous pouvons, d'après (3.10) construire les $(P_i, K_i/K_j)$-complétion des groupes G/K_j. D'après (3.6), il existe des homomorphismes de ces groupes les uns sur les autres qui prolongent les homomorphismes naturels des groupes G/K_j. Nous pouvons donc construire la limite projective $\overline{G}$ des $(P_i, K_i/K_j)$-complétion des groupes G/K_j, et introduire dans $\overline{G}$ la suite centrale (resp. N-suite) $\overline{K}_j$ de telle sorte que la $(P_i, K_i/K_j)$-complétion de G/K_j s'identifie à $\overline{G}/\overline{K}_j$. On vérifie alors immédiatement que $\overline{G}$ muni de sa suite centrale (resp. N-suite) séparante $(\overline{K}_i)$ est une (P_i, K_i)-complétion de G. L'unicité de $\overline{G}$ à un isomorphisme canonique près résulte de l'unicité dans le cas d'une suite finie (3.10) ou encore du théorème (3.12).

4. GROUPES NILPOTENTS ET N-GROUPES DÉFINIS PAR LA FORMULE DE HAUSDORFF. — Nous conservons les notations antérieures; (V_i) désignera, dans ce paragraphe, la suite d'ensembles de nombres premiers obtenue en prenant pour V_i l'ensemble de tous les nombres premiers $\leqq i$. Comme précédemment, Q_i désigne l'anneau

([21]) Pour la définition et l'usage de tels diagrammes, *cf.* EILENBERG-STEENROD, *Fundations of algebraic Topology* (Princeton).

des nombres rationnels de la forme $\frac{r}{n}$ (r entier, n/V_i). V_∞ désignera l'ensemble de tous les nombres premiers; selon l'usage, nous parlerons de groupes sans torsion, de torsion, divisibles, au lieu de groupes sans V_∞-torsion, de V_∞-torsion, V_∞-divisibles. Par contre, pour éviter une équivoque, nous serons obligés de parler de la $(\mathrm{V}_\infty, \mathrm{K}_i)$-complétion lorsque, dans la définition (3.7), $\mathrm{P}_i = \mathrm{V}_\infty$ pour tout i.

(4.1). *Caractérisation des anneaux de Lie* L *et* M *à partir du groupe libre* G. — Considérons, comme au paragraphe 1, l'algèbre de Lie libre complétée à coefficients rationnels L, engendrée par les générateurs indépendants $(x_\iota)_{\iota \in \mathrm{I}}$. Nous avons vu qu'en définissant sur L une structure de groupe par la formule de Hausdorff, les (x_ι) engendrent un groupe libre G. En posant $\mathrm{G}_i = \mathrm{G} \cap \mathrm{L}_i$ où L_i désigne l'ensemble des éléments de L d'ordre $\geqq i$, on obtient la suite centrale descendante de G. Nous savons de plus que, pour tout i, $\mathrm{L}_i/\mathrm{G}_i\mathrm{L}_{i+1}$ est un groupe de torsion, que $\mathrm{L}_i/\mathrm{L}_{i+1}$ est divisible et sans torsion (c'est un espace vectoriel sur le corps Q) et que $\mathrm{G}_i/\mathrm{G}_{i+1}$ est sans torsion (c'est un groupe abélien libre). Si nous appliquons le théorème (3.13), nous voyons que L peut être défini, à un isomorphisme canonique près conservant les éléments de G, comme sa $(\mathrm{V}_\infty, \mathrm{G}_i)$-complétion.

Considérons maintenant, comme au paragraphe 2, l'anneau de Lie $\mathrm{M} \subset \mathrm{L}$. En posant $\mathrm{M}_i = \mathrm{M} \cap \mathrm{L}_i$ ([22]), (M_i) est une N-suite dans M, M est (M_i)-complet, $\mathrm{M}_i/\mathrm{M}_{i+1}$ est V_i-divisible et sans V_i-torsion pour tout i. Enfin, pour tout i, $\mathrm{M}_i/\mathrm{G}_i\mathrm{M}_{i+1}$ est un groupe de V_i-torsion. Toutes ces propriétés résultent immédiatement de la définition de M. Alors, d'après (3.13), M peut être défini à un isomorphisme canonique près conservant les éléments de G comme la $(\mathrm{V}_i, \mathrm{G}_i)$-complétion de G.

Ces définitions de L et de M à partir d'un groupe libre G justifient les notations L(G) et M(G) que nous utiliserons pour les désigner.

Soit, maintenant $\mathfrak{L}$ un anneau de Lie. Désignons par $(\mathfrak{L}_i)$ la suite centrale descendante de $\mathfrak{L}$, c'est-à-dire la suite d'idéaux définie par

$$\mathfrak{L}_1 = \mathfrak{L} \qquad \text{et} \qquad \mathfrak{L}_{i+1} = [\mathfrak{L}, \mathfrak{L}_i] \quad \text{pour tout } i.$$

Tout comme dans le cas des groupes, on a

$$[\mathfrak{L}_i, \mathfrak{L}_j] \subset \mathfrak{L}_{i+j} \quad \text{pour tous } i, j.$$

Nous pouvons, plus généralement, définir dans $\mathfrak{L}$ la notion de suite centrale (resp. N-suite) d'idéaux, ainsi que la notion de suite finie ou séparante. Cherchons à déterminer à quelles conditions doit satisfaire $\mathfrak{L}$ pour qu'il soit possible

([22]) Signalons que (M_i) n'est pas la suite centrale descendante de M, ni son adhérence.

d'y définir, au moyen de la formule de Hausdorff, une loi de groupe. La difficulté est double : d'une part, la formule de Hausdorff

$$xy = x + y + \frac{1}{2}[x, y] + \dots$$

apparaît comme une série infinie, qui devra donc converger dans L au sens d'une certaine topologie; d'autre part, la formule de Hausdorff ne fait pas seulement intervenir les opérations de l'anneau de Lie, mais aussi des multiplications $x \to \lambda x$, où $\lambda \in Q$, $x \in \mathfrak{L}$, qui n'ont aucun sens dans un anneau de Lie quelconque. Nous allons seulement indiquer une catégorie d'anneaux de Lie où l'on peut appliquer la formule de Hausdorff, sans chercher à discuter ici un problème dont l'énoncé même est trop imprécis.

THÉORÈME (4.2). — *Soit $\mathfrak{L}$ un anneau de Lie, (H_i) une suite centrale séparante d'idéaux dans $\mathfrak{L}$, telle que $\mathfrak{L}$ soit (H_i)-complet et que, pour tout i, H_i/H_{i+1} soit V_i-divisible et sans V_i-torsion. Alors, il est possible de définir univoquement sur $\mathfrak{L}$ une structure de groupe au moyen de la formule de Hausdorff, en convenant de choisir dans H_i les termes de degré total i en x et y (pour tout $i \geqq 1$). Avec cette nouvelle structure de groupe, (H_i) reste une suite centrale et les deux groupes H_i/H_{i+1} définis à partir de la structure de groupe abélien de $\mathfrak{L}$ et de sa nouvelle structure de groupe coïncident (en tant que groupes de classes).*

Démonstration. — D'après (3.3), H_i est V_i-divisible et sans V_i-torsion pour tout i. Autrement dit, nous pouvons considérer H_i comme un Q_i-module, en posant

$$y = \frac{r}{s}x \qquad \text{si} \quad sy = rx \; (x, y \in H_i;\ s/V_i,\ r \in Z).$$

Le produit d'un élément x de $\mathfrak{L}$ et d'un nombre rationnel λ se trouve ainsi bien défini, à condition qu'il existe un indice i tel que $\lambda \in Q_i$, $x \in H_i$. Or, puisque (H_i) est une suite centrale d'idéaux dans $\mathfrak{L}$, tout alternant de degré total i appartient à H_i. Si nous prenons soin de représenter la composante homogène de degré i dans la formule de Hausdorff, comme une somme d'alternants de degré i multipliés par des éléments de Q_i, nous voyons qu'on peut calculer univoquement cette composante dans $\mathfrak{L}$. La série $xy = x + y + \frac{1}{2}[x, y] + \dots$ converge quels que soient x et $y \in \mathfrak{L}$, puique $\mathfrak{L}$ est supposé (H_i)-complet. Il reste à montrer que nous obtenons bien une structure de groupe. Nous pourrions, pour cela, construire un homomorphisme de l'anneau de Lie M(G) sur $\mathfrak{L}$, G désignant un groupe libre convenable [*cf.* la démonstration de (4.3)]. Mais nous pouvons raisonner directement. Si x, y, z sont trois éléments quelconques de $\mathfrak{L}$, nous calculons $(xy)z - x(yz)$, en remarquant que chaque H_i est non seulement un Q_i-module, mais une Q_i-algèbre de Lie : $(xy)z - x(yz)$ se ramène ainsi à une somme d'alternants en x, y, z multipliés par des scalaires rationnels. Or,

nous pouvons choisir ces alternants parmi une certaine famille qui, au cas où le sous-anneau de Lie engendré par x, y et z serait libre, en constituerait une base (*cf.*, par exemple, l'algorithme de M. Hall [7]). Mais, la propriété fondamentale de la formule de Hausdorff nous montre que les coefficients des alternants considérés sont alors tous nuls, puisque une Q-algèbre de Lie libre contient l'anneau de Lie libre engendré par ses générateurs indépendants (autrement dit : un anneau de Lie libre est sans torsion). Nous avons donc défini univoquement sur $\mathfrak{L}$ une structure de groupe, que nous notons multiplicativement. Les relations

$$(x, y) \in [x, y] + H_{i+1} \qquad \text{si} \quad x \text{ ou } y \in H_i,$$
$$xy \in x + y + H_{i+1} \qquad \text{si} \quad x \text{ ou } y \in H_i$$

s'établissent immédiatement, ainsi que la relation

$$xH_i = x + H_i \quad \text{pour tout } x \in \mathfrak{L} \qquad \text{et} \qquad \text{tout } i \geqq 1,$$

ce qui achève la démonstration.

L'intérêt principal du théorème (4.2) provient de l'existence de sa réciproque :

THÉORÈME (4.3). — *Soit* G *un groupe,* (H_i) *une suite centrale séparante dans* G. *On suppose que* G *est* (H_i)*-complet et que, pour tout* i, H_i/H_{i+1} *est* V_i*-divisible et sans* V_i*-torsion. Alors, étant donné deux éléments quelconques* x *et* y *de* G, *il existe une suite* (a_i) *d'éléments de* G *et une seule telle que* $a_i \in H_i$ *pour tout* i *et que*

$$x^t y^t = a_1^t a_2^{t^2} \dots a_i^{t^i} \dots$$

pour tout entier t, *le produit convergeant au sens de la* (H_i)*-topologie. Si l'on pose*

$$x + y = a_1, \qquad [x, y] = a_2^2,$$

on définit sur G *une structure d'anneau de Lie. On retrouve la structure de groupe de* G *en appliquant, dans l'anneau de Lie défini sur* G, *le procédé du théorème* (4.2) *avec la suite centrale* (H_i).

Démonstration. — Soit G′ un groupe libre, f un homomorphisme de G′ *sur* G, (G'_i) la suite centrale descendante de G′. Désignons par M une (V_i, G'_i)-complétion de G′ que nous considérons, d'après (4.1) à la fois comme un groupe et comme un anneau de Lie. Puisque (H_i) est une suite centrale, $f(G'_i) \subset H_i$ pour tout i. D'après le théorème (3.12), il existe un homomorphisme g et un seul de M sur G, qui prolonge f et qui vérifie $g(M_i) \subset H_i$.

Soient x, y deux éléments quelconques de G, ξ, η des éléments de M tels que $g(\xi) = x$, $g(\eta) = y$. Alors, d'après (1.5), (2.4) et (2.6), il existe dans M une suite d'éléments (α_i) telle que $\alpha_i \in M_i$ pour tout i et que, pour tout entier t :

$$\xi^t \eta^t = \alpha_1^t \alpha_2^{t^2} \dots \alpha_i^{t^i} \dots .$$

De plus,

$$\alpha_1 = \xi + \eta \qquad \text{et} \qquad \alpha_2^2 = [\xi, \eta].$$

Puisque $g(\mathrm{M}_i) \subset \mathrm{H}_i$, $g(\alpha_i) = a_i \in \mathrm{H}_i$ pour tout i. Appliquons l'homomorphisme g : pour tout entier t, et pour tout $i \geqq 1$,

$$x^t y^t \equiv a_1^t a_2^{t^2} \dots a_i^{t^i} \qquad (\mathrm{mod}\, \mathrm{H}_{i+1}),$$

c'est-à-dire que

$$x^t y^t = a_1^t a_2^{t^2} \dots a_i^{t^i} \dots .$$

D'après (1.6) et (1.7c), la suite (a_i) est univoquement déterminée dans G par la donnée de x et y. Par conséquent, a_1 et a_2^2 sont des fonctions déterminées de x et y, et nous pouvons poser

$$x + y = a_1 \qquad \text{et} \qquad [x, y] = a_2^2.$$

Alors,

$$g(\xi + \eta) = g(\xi) + g(\eta) \qquad \text{et} \qquad g([\xi, \eta]) = [g(\xi), g(\eta)],$$

pour tous ξ, $\eta \in \mathrm{M}$. Il est bien connu que toute structure algébrique quotient d'une structure d'anneau de Lie par une relation d'équivalence compatible avec les opérations, est une structure d'anneau de Lie. G devient ainsi un anneau de Lie, et g est un homomorphisme de M sur G à la fois pour les structures de groupe et d'anneau de Lie.

Dans l'anneau de Lie M les formules d'inversion (2.8) permettent de calculer la somme et le crochet de deux éléments; aucune difficulté ne provient des puissances fractionnaires qui sont univoquement déterminées dans M. Si l'on utilise l'homomorphisme g de M sur G, on voit que les mêmes formules d'inversion permettent de calculer la somme et le crochet de deux éléments de G. Mais, il est nécessaire de faire une convention, analogue à celle du théorème (4.2) : pour tout i, le sous-groupe H_i de G est V_i-divisible (3.3). Il faut alors convenir que toute puissance z^k intervenant dans les formules (2.8) [ou dans des formules plus générales, cf. (2.9)] doit être choisie dans H_i si $z \in \mathrm{H}_i$ (pour tout i).

Au moyen des formules (2.8), on démontre immédiatement que (H_i) est une suite centrale d'idéaux dans l'anneau de Lie L. L'homomorphisme g montre alors que la structure de groupe de G se reconstitue à partir de sa structure d'anneau de Lie par le procédé (4.2), en utilisant la suite (H_i).

La structure d'anneau de Lie définie sur G ne dépend évidemment que de la structure de groupe de G et du choix de la suite centrale (H_i).

Corollaire (4.4). — *Soient* G *et* G′ *deux groupes,* (H_i) *et* (H'_i) *deux suites centrales dans* G *et* G′ *respectivement, vérifiant les conditions de* (4.3). *Alors, si* f *est un homomorphisme de* G *dans* G′ *tel que* $f(\mathrm{H}_i) \subset \mathrm{H}'_i$ *pour tout* i, f *est en même temps un homomorphisme pour les structures d'anneaux de Lie de* G *et* G′.

La démonstration résulte immédiatement de l'énoncé de (4.3).

Remarque. — Si nous appliquons le corollaire au cas où $G = G'$ et où f est l'identité, nous voyons que deux suites (H_i) et (H'_i) satisfaisant aux conditions de (4.3) définissent sur G la même structure d'anneau de Lie, si, pour tout i, $H_i \subset H'_i$.

Nous allons appliquer cette remarque au cas des groupes de torsion et des groupes sans torsion.

LEMME (4.5). — *Pour qu'un groupe de torsion* G *possède une suite* (H_i) *vérifiant les conditions* (4.3), *il faut et il suffit que* G *soit un produit direct de p-groupes, chacun des p-groupes étant de classe strictement inférieure à p. Dans ce cas, la suite centrale descendante de* G *répond à la question.*

Démonstration. — Puisque (H_i) est une suite centrale séparante, G doit être un N-groupe de torsion; G est donc le produit direct de ses p-sous-groupes de Sylow. Si (G_i) est la suite centrale descendante de G, G_i doit être sans V_i-torsion, puisque $G_i \subset H_i$ (pour tout i), d'après (3.2) et (3.11). Or, il est évident, que si G est un p-groupe, G_i ne peut être sans V_i-torsion pour un entier $i \geqq p$ que si $G_i = (1)$. La condition de (4.5) est donc nécessaire.

Si, réciproquement, elle est satisfaite, G_i/G_{i+1} est un groupe abélien de torsion sans p-composantes, pour tout p premier $\leqq i$. On sait alors que G_i/G_{i+1} est V_i-divisible et sans V_i-torsion.

Comme la suite centrale descendante de G décroît plus vite que toute autre suite centrale, le corollaire (4.4) montre que la structure d'anneau de Lie définie sur G par une suite (H_i) vérifiant les conditions de (4.3) coïncide avec la structure d'anneau de Lie définie par (G_i). Par conséquent, cette structure d'anneau de Lie est caractéristique, c'est-à-dire ne dépend que de la structure de groupe. L'anneau de Lie G se décompose en un produit direct de p-anneaux de Lie, c'est-à-dire d'anneaux de Lie, qui sont des p-groupes si on les considère comme des groupes abéliens. Ces p-sous-anneaux de Lie de G coïncident avec les p-sous-groupes de Sylow de G. Aussi allons-nous nous borner désormais à la considération des p-groupes; les théorèmes généraux sur les groupes de torsion considérés s'en déduisent en formant des produits directs.

La somme et le crochet de deux éléments x et y d'un p-groupe G de classe inférieure à p peuvent se calculer au moyen des formules d'inversion (2.8). Les exposants fractionnaires qui interviennent appartiennent tous à Q_{p-1}.

Soient $x \in G$, $x^{p^h} = 1$, n/V_{p-1}, $r \in Z$; pour calculer $x^{\frac{r}{n}}$, nous déterminons deux entiers λ et μ tels que $\lambda n + \mu p^h = r$, et nous posons $x^{\frac{r}{n}} = x^{\lambda}$. Il en résulte que $x^{\frac{r}{n}}$ est une puissance entière de x. Pour avoir une formule indépendante de h, il nous suffit d'écrire $\frac{r}{n} \in Q_{p-1}$ comme un entier p-adique :

$$\frac{r}{n} = \Sigma_{i=0}^{\infty} a_i p^i,$$

où tous les coefficients a_i sont des entiers. Alors, pour h donné, on peut prendre $\lambda = \Sigma_{i=0}^{h-1} a_i p^i$, d'où la notation $x^{\frac{r}{h}} = x^{\sum_{i=0}^{\infty} a_i p^i}$. Ces remarques montrent que, dans le cas d'un p-groupe de classe inférieure à p, tout sous-groupe est en même temps un sous-anneau (et réciproquement, comme le montrent les mêmes considérations appliquées à la formule de Hausdorff dans un p-anneau de Lie). De plus, pour définir la structure d'anneau de Lie sur un p-groupe G, il n'est pas nécessaire de supposer que G soit de classe inférieure à p : il suffit que tout sous-groupe engendré par trois éléments de G soit de classe inférieure à p. En effet, pour calculer la somme et le crochet de deux éléments x, y de G, il nous suffit d'appliquer les formules d'inversion en supposant que x et y engendrent un sous-groupe de classe inférieure à p. Pour vérifier que nous obtenons bien un anneau de Lie, il nous suffit de montrer que les identités génériques (distributivité, identité de Jacobi, etc.) sont satisfaites : or, elles ne font intervenir que trois éléments génériques de G. Elles sont donc satisfaites si tout sous-groupe à trois générateurs est de classe inférieure à p. Le même raisonnement montre la possibilité d'appliquer la formule de Hausdorff dans tout p-anneau de Lie dont chaque sous-anneau à trois générateurs est de classe inférieure à p.

La condition imposée aux sous-groupes à trois générateurs ne résulte pas de la même condition imposée aux sous-groupes à deux générateurs, qui suffit pourtant pour calculer $x+y$ et $[x, y]$ ainsi que pour démontrer

$$x+y=y+x, \qquad [x, y][y, x]^{-1}=1, \qquad [x, x]=1$$

(c'est-à-dire les identités génériques à un ou deux éléments). Comme contre exemple, on peut prendre le groupe générique à trois générateurs où tout élément x vérifie $x^3=1$ (*cf.* chap. I, § 1 et [20]). De même, un p-groupe dont tous les sous-groupes à trois générateurs sont de classe $<p$, n'est pas nécessairement de classe $<p$. Il suffit, d'après ce qui précède, de donner un exemple pour les p-anneaux. Or, on peut construire une algèbre de Lie, de dimension 91 sur le corps Z_5 des entiers modulo 5, qui est engendré par quatre générateurs, qui est de classe 5, et dont toutes les sous-algèbres à trois générateurs sont de classe au plus égale à 4 ([23]).

Nous pouvons donc énoncer valablement le :

THÉORÈME (4.6). — *Chaque p-anneau de Lie, tel que tout sous-anneau à trois générateurs soit de classe inférieure à p, est porteur d'une structure de p-groupe, définie par la formule de Hausdorff. Réciproquement, chaque p-groupe tel que tout sous-groupe à trois générateurs soit de classe inférieure à p, est porteur d'une structure de p-anneau de Lie, définie au moyen des formules d'inversion* (2.8) *de la formule de Hausdorff. Pour les structures considérées, les notions*

([23]) La construction, un peu longue, est exposée au paragraphe 5.

de sous-groupe (resp. sous-groupe invariant) et de sous-anneau (resp. idéal) coïncident, ainsi que les notions d'homomorphisme de groupes et d'homomorphisme d'anneaux de Lie ([24]).

Ce résultat constitue apparemment l'exemple le plus simple d'une correspondance entre certaines structures de groupes et d'anneaux de Lie.

Nous allons maintenant étudier les groupes nilpotents sans torsion, et retrouver les résultats de Malcev [26], [27].

Soit G un groupe nilpotent sans torsion, (G_i) sa suite centrale descendante. Alors, d'après le théorème (3.2), il existe dans G une N-suite finie (H_i) dont les quotients H_i/H_{i+1} sont sans torsion, et qui décroît le plus vite parmi toutes les suites centrales de G possédant cette propriété. La démonstration de (3.2) se simplifie considérablement, et les sous-groupes H_i peuvent être ainsi définis : Soit $x \in G$; alors, $x \in H_i$, si et seulement s'il existe un entier $n \neq 0$, tel que $x^n \in G_i$. Nous appellerons (H_i) *la suite rectifiante* de G. La suite rectifiante (H_i) possède donc les propriétés suivantes : c'est une N-suite; si c est la classe de G, $H_{c+1} = (1)$; H_i/H_{i+1} est sans torsion pour tout i, et si (K_i) est une suite centrale dans G dont les quotients sont sans torsion, $K_i \supset H_i$ pour tout i. Si G et G' sont deux groupes nilpotents sans torsion, (G_i) et (G'_i) leurs suites centrales descendantes, (H_i) et (H'_i), leurs suites rectifiantes, et enfin, f un homomorphisme de G dans G', alors, $f(H_i) \subset H'_i$ pour tout i. Nous savons, en effet, que $f(G_i) \subset G'_i$; alors si $x \in H_i$, $n \neq 0$, $x^n \in G_i$,

$$f(x)^n = f(x^n) \in f(G_i) \subset G'_i, \qquad \text{d'où} \qquad f(x) \in H'_i.$$

Si G est un groupe nilpotent sans torsion et divisible, tous les sous-groupes de sa suite rectifiante sont divisibles (3.3d).

Définition (4.7). — Soit G un groupe nilpotent sans torsion. Nous appellerons « *complétion de Malcev* » de G une extension G' de G qui devra être un groupe nilpotent sans torsion et divisible, et vérifier la condition suivante : si $x \in G'$, il existe un entier $n \neq 0$ tel que $x^n \in G$.

On remarquera que cette définition ne fait pas intervenir de suites de sous-groupes dans les groupes considérés. Sa légitimité va résulter du :

THÉORÈME (4.8). — *Un groupe nilpotent sans torsion* G, *possède une complétion de Malcev* G', *qui est déterminée à un isomorphisme canonique près, conservant les éléments de* G.

Démonstration. — Soit (H_i) la suite rectifiante de G. Construisons, confor-

([24]) L'existence d'une correspondance biunivoque entre p-groupes finis de classe inférieure à p et p-anneaux finis de classe inférieure à p avait été indiquée par Magnus [23] avec une esquisse de démonstration plutôt sommaire. J'ai abouti indépendamment au même résultat que je n'ai pas vu mentionné dans la littérature ultérieure.

mément à (3.10), une (V_∞, H_i)-complétion de G, soit $\overline{G}$, $(\overline{H}_i)$. Alors $\overline{G}$ est un groupe nilpotent (plus précisément un groupe de même classe que G); il est sans torsion (3.3*b*) et divisible (3.3*a*). Soit $x \in \overline{G}$; supposons déjà trouvé un entier $n \neq 0$ tel que $x^n = gy$, où $g \in G$, $y \in \overline{H}_i$. Alors, puisque $\overline{H}_i/H_i\overline{H}_{i+1}$ est un groupe de torsion, il existe $n' \neq 0$ tel que $y^{n'} \in H_i\overline{H}_{i+1}$. Mais y est central modulo $\overline{H}_{i+1}$, ce qui montre que $(gy)^{n'} \in g^{n'}y^{n'}\overline{H}_{i+1}$. Ainsi $x^{nn'} \in G\overline{H}_{i+1}$, et l'on voit que $\overline{G}$ est une complétion de Malcev de G.

Soit maintenant G′ une complétion de Malcev de G, H'_i la suite rectifiante de G′. Alors, $H_i = G \cap \overline{H}_i \subset G \cap H'_i$, puisque $(G \cap H'_i)$ est une suite centrale à quotients sans torsion.

Les groupes H'_i/H'_{i+1} sont divisibles et sans torsion. Nous pouvons donc appliquer (3.6), qui nous montre l'existence d'un homomorphisme f de $\overline{G}$ dans G′ conservant les éléments de G [et tel que $f(\overline{H}_i) \subset H'_i$ pour tout i]. Montrons que f est un isomorphisme de $\overline{G}$ sur G′, et que si g est un homomorphisme de $\overline{G}$ dans G′, conservant les éléments de G, il coïncide nécessairement avec f. Soit $x \in \overline{G}$, $x \neq 1$; alors il existe $n \neq 0$ tel que $x^n \in G$. Puisque $\overline{G}$ est sans torsion, $x^n \neq 1$. Alors,

$$f(x^n) = x^n = f(x)^n \neq 1,$$

ce qui montre que $f(x) \neq 1$; de plus, $f(x)^n = g(x)^n$, ce qui implique

$$f(x) = g(x),$$

d'après (3.3*b*). Enfin, si $y \in G'$, il existe $n \neq 0$ tel que $y^n \in G$; puisque $\overline{G}$ est divisible, il existe $x \in \overline{G}$ tel que $x^n = y^n$. Alors,

$$f(x)^n = f(x^n) = x^n = y^n,$$

ce qui montre que $f(x) = y$. Remarquons que si nous prenons $G' = \overline{G}$, f est l'identité, ce qui montre que $\overline{H}_i$ est la suite rectifiante de $\overline{G}$.

THÉORÈME (4.9). — *Soit* G *un groupe nilpotent sans torsion. Alors, toute extension* G′ *de* G *qui est un groupe nilpotent sans torsion et vérifie la condition suivante : « si* $x \in G'$, *il existe un entier* $n \neq 0$ *tel que* $x^n \in G$ », *s'identifie (canoniquement) à un sous-groupe d'une complétion de Malcev de* G.

Démonstration. — Soit $\overline{G}'$ une complétion de Malcev de G′. Alors $\overline{G}'$ est une complétion de Malcev de G : il suffit de remarquer que, si $x \in \overline{G}'$, il existe $n \neq 0$ tel que $x^n \in G'$, puis $n' \neq 0$ tel que $x^{nn'} \in G$.

THÉORÈME (4.10). — *Soient* G, G′ *deux groupes nilpotents sans torsion,* $\overline{G}$, $\overline{G}'$ *leurs complétions de Malcev, f un homomorphisme de* G *dans* G′. *Alors il*

existe un homomorphisme g et un seul de $\overline{G}$ dans $\overline{G}'$ qui prolonge f. Si f est un isomorphisme de G dans G' (resp. homomorphisme de G sur G'), il en est de même de g.

Démonstration. — Soient $(\overline{H}_i)$, $(\overline{H}'_i)$ les suites rectifiantes de $\overline{G}$ et $\overline{G}'$. Les suites $(G \cap \overline{H}_i)$ et $(G' \cap \overline{H}'_i)$ sont respectivement les suites rectifiantes de G et G'. Par conséquent, $f(G \cap \overline{H}_i) \subset G' \cap \overline{H}'_i$ pour tout i, et le prolongement g de f à $\overline{G}$ existe d'après (3.6). Son unicité, et la dernière partie du théorème se démontrent comme en (4.8).

Remarque (4.11). — Nous pouvons considérer les éléments de la complétion de Malcev $\overline{G}$ d'un groupe nilpotent sans torsion, comme des puissances fractionnaires des éléments de G (*cf.* § 1) en posant

$$y = x^{\frac{r}{s}} \quad \text{si} \quad x^r = y^s \qquad (r, s \in Z).$$

Cela nous permet d'obtenir directement l'ensemble $\overline{G}$ comme quotient du produit cartésien $Z \times G$ par la relation d'équivalence

$$(n, x) \equiv (n', x') \qquad \text{si et seulement si} \quad x'^n = x^{n'},$$

en associant à la classe de (n, x) l'élément $x^{\frac{1}{n}}$ de $\overline{G}$. Des difficultés notables apparaissent si l'on veut expliciter la loi de groupe sur G. On se ramène, étant donné $x, y \in G$, $n \in Z$, à calculer $z \in G$ et $n' \in Z$ tels que $x^{\frac{1}{n}} y^{\frac{1}{n}} = z^{\frac{1}{n'}}$. Dans le cas abélien, il suffit de prendre $z = xy$ et $n' = n$ (alors, $\overline{G} = G \otimes Q$). Dans le cas général, il est impossible de prendre pour z un mot en x et y ([25]) indépendant de n. On peut établir le résultat suivant : si le groupe G est de classe $\leqslant c$, on peut prendre $n' = n^{\frac{c(c+1)}{2}}$; z est alors représenté par un mot en x et y (qui dépend de l'entier n). Par exemple, pour

$$c = 2, \qquad n' = n^3 \qquad \text{et} \qquad z = x^{n^2} y^{n^2} (y, x)^{\frac{n(n^2-1)}{2}}.$$

L'existence de ces formules se démontre de la manière suivante : on considère le groupe H engendré par deux générateurs indépendants x et y, (H_i) sa suite centrale descendante, et enfin H' le sous-groupe de H engendré par x^n et y^n, n désignant un entier positif donné. Alors, on démontre, par récurrence sur i, que

$$(xy)^{n^{\frac{i(i+1)}{2}}} \in H' H_{i+1} \quad (cf. \text{ chap. I, § 2-4}).$$

L'existence de ces formules nous permet de définir la complétion de Malcev et de démontrer les théorèmes (4.8) à (4.10) pour une catégorie de groupes sans

([25]) C'est-à-dire un élément du groupe libre engendré par les symboles x et y.

torsion plus étendue que les groupes nilpotents : la catégorie des *groupes sans torsion dont chaque sous-groupe à trois générateurs est nilpotent* [*cf.* (4.6)].

(4.12) *Extension des résultats précédents aux* N-*groupes topologiques sans torsion.* — Soit G un N-groupe sans torsion. Nous pouvons définir, comme précédemment, la suite rectifiante (H_i) de G : c'est, parmi les suites centrales de G dont les quotients sont sans torsion, celle qui décroît le plus vite. Mais nous ne pouvons pas affirmer en général que la suite rectifiante soit séparante [*cf.* (3.11)]. Pour généraliser convenablement les résultats précédents, nous introduirons une catégorie de groupes topologiques, que nous appellerons N-*groupes topologiques sans torsion*. Par définition, un N-groupe topologique sans torsion, sera un groupe dont la topologie est définie en prenant comme système fondamental de voisinage de l'unité les sous-groupes d'une suite centrale séparante dont les quotients sont sans torsion. Tous les homomorphismes de groupes de cette catégorie seront supposés continus ; de même, une extension G′ d'un N-groupe topologique sans torsion G sera un groupe topologique contenant G comme sous-groupe topologique.

Définition (4.13). — Nous appellerons, suivant Malcev, R-groupe un N-groupe topologique sans torsion qui sera supposé, de plus, divisible et complet (par rapport à sa topologie).

THÉORÈME (4.14). — *Soit* G *un* N-*groupe topologique sans torsion. Nous appellerons complétion de Malcev de* G *une extension* $\overline{G}$ *qui devra être un* R-*groupe et vérifier de plus la condition suivante : pour tout* $x \in \overline{G}$ *et tout voisinage* H *de l'unité dans* $\overline{G}$, *il existe un entier* $n \neq 0$ *tel que* $x^n \in GH$ [26]. *La complétion de Malcev d'un* N-*groupe topologique sans torsion existe, et est déterminée à un isomorphisme canonique près, conservant les éléments de* G.

Démonstration. — Soit (H_i) une suite centrale séparante dans G dont les quotients sont sans torsion et qui définit sa topologie. Construisons, conformément à (3.13) la (V_∞, H_i)-complétion de G, soit $\overline{G}$, $(\overline{H}_i)$. Alors, on démontre comme en (4.8) que $\overline{G}$, muni de sa $(\overline{H}_i)$-topologie, est une complétion de Malcev de G. Soit G′ une autre complétion de Malcev de G, (K'_i) une suite centrale de G′ à quotients sans torsion et définissant sa topologie. Posons, pour tout i, $K_i = G \cap K'_i$: alors G'/K'_i s'identifie à une complétion de Malcev du groupe nilpotent sans torsion G/K_i, et G′ est la limite projective de ses quotients G'/K'_i, puisqu'il est (K'_i)-complet. Or, (K_i) et (H_i) définissent la même topologie dans G; donc, pour tout entier i, il existe un entier j tel que $H_j \subset K_i$.

(26) Si l'on introduit une métrique convenable pour définir la topologie de $\overline{G}$, cela revient à exiger que la distance de G à l'ensemble des puissances positives d'un élément quelconque de $\overline{G}$ soit nulle.

Alors l'homomorphisme naturel de G/H_j sur G/K_i se prolonge en un homomorphisme de la complétion de Malcev $\overline{G}/\overline{H}_j$ sur G'/K'_i (4.10). D'où, par composition, un homomorphisme φ_i de $\overline{G}$ sur G'/K'_i, tel que $\varphi_i(H_j) \subset K'_i$. Les homomorphismes φ_i sont compatibles (c'est-à-dire forment un diagramme commutatif) avec les homomorphismes naturels des quotients G'/K'_i dont G' est la limite projective; par conséquent, φ_i peut être considéré comme le composé de l'homomorphisme naturel de G' sur G'/K'_i avec un homomorphisme φ déterminé de $\overline{G}$ dans G', dont on vérifie immédiatement qu'il laisse invariant les éléments de G. Jusqu'à présent, nous avons seulement utilisé le fait que la (H_i)-topologie de G est plus fine que sa (K_i)-topologie. Nous pourrons construire de même l'homomorphisme ψ de G' dans $\overline{G}$ conservant les éléments de G, en utilisant le fait que la (K_i)-topologie est plus fine que la (H_i)-topologie. On démontre alors immédiatement, que φ et ψ sont deux isomorphismes inverses l'un de l'autre, et que φ est entièrement déterminé par la condition de conserver les éléments de G et d'être un homomorphisme (continu) de $\overline{G}$ dans G'.

Les théorèmes (4.9) et (4.10) s'étendent sans difficulté à la catégorie des N-groupes topologiques sans torsion.

Remarquons que (4.14) nous permet de préciser la caractérisation (4.1) de l'algèbre de Lie libre complétée $L(G)$ à partir du groupe libre G : $L(G)$ est la complétion de Malcev de G topologisé par sa suite centrale descendante.

THÉORÈME (4.15). — *Tout* R-*groupe* G *est, canoniquement, porteur d'une structure d'algèbre de Lie sur le corps* Q *des nombres rationnels. La structure de groupe de* G *s'obtient à partir de sa structure d'algèbre de Lie par la formule de Hausdorff.*

Démonstration. — Soit G un R-groupe, (H_i) une suite centrale séparante dans G, dont les quotients sont sans torsion et qui définit sa topologie. Chaque sous-groupe H_i est divisible (3.3*c*), et nous pouvons donc appliquer le théorème (4.3). Il nous reste donc seulement à démontrer que les opérations de l'algèbre de Lie sont indépendantes du choix de (H_i). Soit donc (K_i) une autre suite possédant les mêmes propriétés. Alors, la suite $(H_i \cap K_i)$ définit encore la topologie de G; ses quotients sont sans torsion (si $x \in H_i \cap K_i$, $n \neq 0$, $x^n \in H_{i+1} \cap K_{i+1}$, on a $x \in H_{i+1}$ et $x \in L_{i+1}$) et, par conséquent, divisibles. La remarque qui suit le corollaire (4.4) nous montre que les suites (H_i) et (K_i) définissent toutes deux la même structure d'algèbre de Lie que la suite $(H_i \cap K_i)$.

Dans le cas des groupes nilpotents divisibles et sans torsion, on considère la topologie discrète, et l'on obtient canoniquement une structure d'algèbre de Lie nilpotente (et de même classe que le groupe).

Tout homomorphisme (continu) de R-groupes est en même temps un homomorphisme pour leurs structures d'algèbres de Lie (4.4). De même, la notion de sous-groupe (resp. sous-groupe invariant) fermé divisible et de sous-algèbre de Lie (resp. idéal) fermée divisible coïncident [*cf.* (4.6)].

Grâce à la complétion de Malcev, nous pouvons considérer tout N-groupe topologique sans torsion et en particulier, tout groupe nilpotent sans torsion, comme plongé canoniquement dans une algèbre de Lie sur le corps Q.

L'application du théorème (4.3) à des groupes nilpotents mixtes (c'est-à-dire possédant des éléments d'ordre fini et des éléments d'ordre infini), se heurte à une difficulté qui n'apparaît pas dans le cas des groupes de torsion ou des groupes sans torsion : on aboutit à différentes structures d'anneaux de Lie, suivant la suite centrale considérée.

Nous pouvons toutefois caractériser les sous-groupes des groupes possédant une suite centrale qui vérifie les propriétés établies en (4.3). Bornons-nous aux groupes nilpotents.

THÉORÈME (4.16). — *Pour qu'un groupe nilpotent* G *soit sous-groupe d'un groupe* G' *possédant une suite centrale finie* (H'_i) *telle que, pour tout* i, H'_i/H'_{i+1} *soit* V_i*-divisible et sans* V_i*-torsion, il faut et il suffit que, pour tout* i, *le* $i^{\text{ième}}$ *sous-groupe* G_i *de la suite centrale descendante de* G *soit sans* V_i*-torsion.*

Démonstration. — Soit $H_i = H'_i \cap G$. Alors, H_i est sans V_i-torsion ainsi que $G_i \subset H_i$. Réciproquement, si G_i est sans V_i-torsion, le théorème (3.2) nous permet de construire canoniquement une suite centrale finie (H_i) dans G, telle que H_i/H_{i+1} soit sans V_i-torsion. Il nous suffit alors de former (3.6) une (V_i, H_i)-complétion de G pour nous placer dans les conditions de l'énoncé (4.3).

La difficulté indiquée provient de ce qu'il n'est pas possible de définir canoniquement une suite centrale finie (K_i) dont les quotients sont non seulement sans V_i-torsion, mais aussi V_i-divisibles, même en postulant l'existence d'une telle suite.

Exemple. — Prenons le groupe G défini sur le produit cartésien $Z \times Z \times Q_2 \times T_2$ par la multiplication

$$(p, q, r, s)(p', q', r', s') = (p + p', q + q', r + r' - p'q, s + s');$$

Z désigne comme précédemment l'anneau des entiers rationnels, Q_2 l'anneau des nombres rationnels de la forme $\frac{m}{2^n}$ $(m, n \in Z)$, et enfin, T_2 le groupe additif quotient Q_2/Z. Nous désignons par $\bar{r}$ l'image de $r \in Q_2$ par l'homomorphisme canonique de Q_2 sur T_2.

G est un groupe nilpotent de classe 2. Posons $H_1 = G$, et prenons pour H_2 l'ensemble des éléments de la forme $(0, 0, r, 0)$. Alors, toutes les conditions du théorème (4.3) sont remplies pour la suite (H_i). La structure d'algèbre de Lie ainsi définie est la suivante :

$$\text{si} \quad x = (p, q, r, s), \qquad x' = (p', q', r', s'),$$

alors

$$[x, x'] = (x, x') = (0, 0, pq' - qp', 0)$$

et

$$x + x' = \left(p + p', q + q', r + r' - \frac{(pq' + qp')}{2}, s + s'\right).$$

Or, nous définissons un automorphisme φ de G en posant

$$\varphi(x) = (p, q, r, s + \bar{r}).$$

Si nous posons donc $K_1 = G$, $K_2 = \varphi(H_2)$, la suite (K_i) vérifie tout comme (H_i) les propriétés de (4.3). Mais cela nous conduit à une nouvelle addition sur G :

$$x \oplus x' = \varphi\left(\varphi^{-1}(x) + \varphi^{-1}(x')\right)$$
$$= \left(p + p', q + q', r + r' - \left(\frac{pq' + qp'}{2}\right), s + s' - \overline{\left(\frac{pq' + qp'}{2}\right)}\right).$$

On a bien $x \oplus x' \neq x + x'$ si $pq' + qp'$ est un entier impair.

Dans le cas général, j'ignore si deux structures d'anneaux de Lie définies sur un groupe nilpotent G par le procédé du théorème (4.3) sont toujours transformées l'une en l'autre par un automorphisme de G (comme dans l'exemple précédent).

(4.17) *Complétion de Malcev des groupes sans* P-*torsion.* — La théorie de la complétion de Malcev que nous avons exposée dans le cas le plus important, celui des groupes sans torsion, peut s'étendre à des catégories plus vastes de groupes nilpotents ou de N-groupes topologiques. Nos démonstrations reposent en effet, sur les résultats du paragraphe 3, et particulièrement sur le lemme (3.3*d*). Nous pouvons donc considérer la catégorie des groupes nilpotents sans P-torsion, P désignant un ensemble quelconque de nombres premiers. Nous définirons la *suite* P-*rectifiante* d'un groupe nilpotent sans P-torsion comme la suite centrale décroissant le plus vite parmi celles dont les quotients successifs sont sans P-torsion. Une P-*complétion de Malcev* d'un groupe nilpotent sans P-torsion G, sera une extension $\overline{G}$ de G possédant les propriétés suivantes : $\overline{G}$ est un groupe nilpotent sans P-torsion et P-divisible et, pour tout $x \in \overline{G}$, il existe un entier n/P tel que $x^n \in G$. On définira de même la P-complétion de Malcev d'un N-groupe topologique complet dont la topologie est définie par une suite centrale séparante dont les quotients successifs sont sans P-torsion. Les théorèmes (4.8) à (4.14) s'étendent alors sans modification notable des démonstrations. Les résultats nouveaux ainsi démontrés ne semblent pas présenter pour l'instant beaucoup d'intérêt, mais ils montrent tout au moins l'avantage que présente l'exposé de la complétion de Malcev sans faire appel à la théorie des groupes de Lie.

Remarque (4.18). — Il est possible d'exposer plus simplement que nous ne

l'avons fait la théorie de l'inversion de la formule de Hausdorff pour des catégories de groupes plus restreintes : les groupes nilpotents de classe $\leqslant n$, sans V_n-torsion et V_n-divisibles. La variante (1.7*b*) du lemme (1.6) correspond à ce cas. La simplification annoncée provient de ce qu'on peut alors éviter l'usage du théorème (3.6). Considérons, en effet, un groupe libre G, de générateurs indépendants $(x_\iota)_{\iota\in I}$, et sa complétion de Malcev L(G) lorsqu'on considère G comme un N-groupe sans torsion topologisé par sa suite centrale descendante (4.1). Considérons les sous-groupes $\Gamma_{(i)}$ de L(G) engendrés par les éléments $x_\iota^{(n!)^{-i}}$; alors, tous les $\Gamma_{(i)}$ sont des groupes libres engendrés par les générateurs indépendants $x_\iota^{(n!)^{-i}}$, et leur réunion Γ est une V_n-complétion de Malcev de G, considéré comme N-groupe sans V_n-torsion topologisé par sa suite centrale descendante (4.17). On voit ainsi comment tout homomorphisme f de G dans un groupe nilpotent H, V_n-divisible et sans V_n-torsion peut se prolonger en un homomorphisme unique g de Γ dans H : il suffira de prolonger successivement f aux groupes $\Gamma_{(i)}$. Si l'on suppose de plus que H est de classe n au plus, un homomorphisme g de Γ *sur* H permet d'établir la structure de Q_n-algèbre de Lie de H [*cf.* (4.5)].

5. Construction d'un groupe particulier. — Nous voulons construire une algèbre de Lie sur le corps Z_5 des entiers mod5, qui soit de classe 5 et dont toutes les sous-algèbres à trois générateurs soient de classe $\leqslant 4$.

Considérons d'abord l'algèbre de Lie libre L_0 engendrée sur le corps Z_5 par les cinq générateurs indépendants x_1, x_2, x_3, x_4, x_5. Nous noterons généralement $[y_1, y_2, \ldots, y_s]$ l'alternant par rapport à $y_1, \ldots, y_s \in L_0$ défini par la relation de récurrence :

$$[y_1, \ldots, y_{s-1}, y_s] = [[y_1, \ldots, y_{s-1}], y_s].$$

Nous savons que L_0 est une algèbre de Lie graduée, et même multigraduée, si l'on considère les degrés par rapport à chacun des générateurs.

Les éléments multilinéaires de degré total 5 (c'est-à-dire homogènes de degré 1 par rapport à chacun des générateurs) constituent, d'après les formules de Witt [33], un Z_5-module de dimension 24. Or, chacun d'eux est égal à une combinaison linéaire des éléments $[x_1, x_i, x_j, x_k, x_l]$, où (i, j, k, l) désigne l'une des 24 permutations des indices (2, 3, 4, 5). Ces éléments sont donc linéairement indépendants sur Z_5.

Nous allons maintenant prendre le quotient L de L_0 par l'idéal engendré par :

1° tous les éléments de degré total $\geqslant 6$;

2° tous les éléments de degré total 5 qui sont de degré au moins égal à 2 par rapport à l'un des générateurs x_i;

3° tous les éléments multilinéaires de degré total 5 qui sont de la forme

$$[x_1, x_2, x_3, x_4, x_5] - \varepsilon_\sigma [x_1, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}, x_{\sigma(5)}],$$

où σ désigne une permutation des indices 2, 3, 4, 5, et ε_σ sa signature.

Pour ne pas alourdir les notations, nous désignerons désormais par x_i l'image canonique dans L du générateur précédemment noté x_i de Γ_0 (qui n'interviendra plus).

On voit facilement que L est encore une algèbre multigraduée par rapport aux générateurs x_i. C'est une algèbre de classe 5, puisque

$$[x_1, x_2, x_3, x_4, x_5] = X \neq 0;$$

de plus, tout alternant de degré 5 est un multiple de X. Pour calculer $[y_1, y_2, y_3, y_4, y_5]$, où $y_i \in L$, nous pouvons remplacer chaque y_i par sa composante homogène de degré total 1. Posons donc

$$y_i = \Sigma_{j=1}^{5} a_{i,j} x_j \qquad (1 \leq i \leq 5;\ a_{i,j} \in \mathbf{Z}_5);$$

le calcul de $[y_1, y_2, y_3, y_4, y_5]$ se ramène alors au calcul des alternants $[x_i, x_j, x_k, x_l, x_m]$, où (i, j, k, l, m) représente une permutation des indices (1, 2, 3, 4, 5). D'après la construction de L, nous avons :

$$[x_1, x_i, x_j, x_k, x_l] = \varepsilon X, \tag{5.1}$$

où ε désigne la signature de la permutation (i, j, k, l) des indices (2, 3, 4, 5). Nous obtenons ensuite :

$$\begin{cases} [x_i, x_1, x_j, x_k, x_l] = -[x_1, x_i, x_j, x_k, x_l] = -\varepsilon X, \\ [x_i, x_j, x_1, x_k, x_l] = -[x_1, [x_i, x_j], x_k, x_l] = -2\varepsilon X, \\ [x_i, x_j, x_k, x_1, x_l] = -[x_1, [x_i, x_j, x_k], x_l] = 0, \end{cases} \tag{5.2}$$

et de même :

$$[x_i, x_j, x_k, x_l, x_1] = 0.$$

Les formules (5.1) et (5.2) nous permettent de calculer $[y_1, y_2, y_3, y_4, y_5] = \lambda X$, le coefficient $\lambda \in \mathbf{Z}_5$ étant égal au déterminant :

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ -2a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ 0 & a_{42} & a_{43} & a_{44} & a_{45} \\ 0 & a_{52} & a_{53} & a_{54} & a_{55} \end{vmatrix} = \lambda. \tag{5.3}$$

Pour montrer que toute sous-algèbre à trois générateurs z_1, z_2, z_3 est de classe ≤ 4, il suffit de montrer que tous les alternants de la forme $[z_i, z_j, z_k, z_l, z_m]$, où les indices i, j, k, l, m prennent indépendamment les valeurs 1, 2, 3, sont nuls. Or, dans ce cas, le déterminant (5.3) est nul, puisque, si on le développe suivant les éléments de la première colonne, chaque mineur a au moins deux lignes égales. Par contre, il existe des sous-algèbres de L à quatre générateurs qui sont de classe 5 : ainsi

$$[x_1 + x_2, x_3, x_1 + x_2, x_4, x_5] = -3X \neq 0.$$

Il est facile de calculer la dimension (sur Z_5) de la sous-algèbre engendrée par x_1+x_2, x_3, x_4, x_5. Le module de ses éléments de degré 5 a (comme pour L) la dimension 1. Quant aux éléments de degré ≤ 4, ils constituent des modules dont les dimensions sont les mêmes que pour une algèbre de Lie libre à quatre générateurs, c'est-à-dire (pour les degrés 1, 2, 3, 4 respectivement) : 4, 6, 20, 60.

Si nous définissons sur cette sous-algèbre de Lie une structure de groupe au moyen de la formule de Hausdorff, nous voyons que nous avons construit un groupe à quatre générateurs, d'ordre 5^{91}, de classe 5, et tel que chacun de ses sous-groupes à trois générateurs soit de classe 4 au plus (l'ordre de chaque élément du groupe, sauf l'élément neutre, est 5). L'énoncé du théorème (4.6) se trouve ainsi légitimé.

Bibliographie.

(Les titres d'articles en russe ont été traduits.)

[1] Baer (R.). — *The higher commutator subgroups of a group* (*Bull. Amer. Math. Soc.*, t. 50, 1944, p. 143-160).

[2] Birkhoff (G.). — *Representability of Lie algebras and Lie groups by matrices* (*Ann. Math.*, t. 38, 1937, p. 526-532).

[3] Chirchov (A. I.). — *Sur la représentation des anneaux de Lie dans les anneaux associatifs* (*Ousp. Mat. Naouk.*, t. 8, 1953, p. 173-175).

[4] Cohn (P. M.). — *Generalization of a theorem of Magnus* (*Proc. Lond. Math. Soc.*, 3e série, t. 2, 1952, p. 297-310).

[5] Fox (R. H.). — *Free differential calculus* (I) (*Ann. Math.*, t. 57, 1953, p. 547-560).

[6] Grün (O.). — *Zusammenhang zwischen Potenzbildung und Kommutatorbildung* (*J. R. An. Math.*, t. 182, 1940, p. 158-177).

[7] Hall (M.). — *A basis for free Lie rings and higher commutators in free groups* (*Proc. Amer. Math. Soc.*, t. 1, 1950, p. 575-581).

[8] Hall (P.). — *A contribution to the theory of groups of prime power order* (*Proc. Lond. Math. Soc.*, t. 36, 1934, p. 29-95).

[9] Hausdorff (F.). — *Die symbolische Exponentialformel in der Gruppentheorie* (*Ber. Sächs Ges.*, t. 58, 1906, p. 19-48).

[10] Jacobson (N.). — *Abstract derivations and Lie algebras* (*Trans. Amer. Math. Soc.*, t. 42, 1937, p. 206-224).

[11] Jacobson (N.). — *Restricted Lie algebras of characteristic p* (*Trans. Amer. Math. Soc.*, t. 50, 1941, p. 15-25).

[12] Jennings (S. A.). — *The structure of the group-ring of a p-group over a modular field* (*Trans. Amer. Math. Soc.*, t. 50, 1941, p. 175-185).

[13] Kaloujnine (L.). — *Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait* (*C. R. Acad. Sc.*, t. 230, p. 2067-2069).

[14] Kaloujnine (L.). — *Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait* (*généralisation d'un théorème de M. Ph. Hall*) (*C. R. Acad. Sc.*, t. 231, 1950, p. 400-402).

[15] Lazard (M.). — *Sur les algèbres enveloppantes universelles de certaines algèbres de Lie* (*C. R. Acad. Sc.*, t. 234, 1952, p. 788-791).

[16] LAZARD (M.). — *Sur certaines suites d'éléments dans les groupes libres et leurs extensions* (*C. R. Acad. Sc.*, t. **236**, 1953, p. 36-38).

[17] LAZARD (M.). — *Détermination et généralisation des groupes de dimension des groupes libres* (*C. R. Acad. Sc.*, t. **236**, 1953, p. 1222-1224).

[18] LAZARD (M.). — *Problèmes d'extension concernant les* N*-groupes; inversion de la formule de Hausdorff* (*C. R. Acad. Sc.*, t. **237**, 1953, p. 1377-1379).

[19] LERAY (J.). — *L'anneau spectral et l'anneau filtré d'homologie d'un espace localement compact et d'une application continue* (chap. I, § 1) (*J. Math. pures et appl.*, t. **29**, 1950, p. 10-14).

[20] LÉVI (F.) et VAN DER VAERDEN (B. L.). — *Ueber eine besondere Klasse von Gruppen* (*Abh. Mat. Sem. Hamb.*, t. **9**, 1952, p. 154-158).

[21] MAGNUS (W.). — *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring* (*Math. Ann.*, t. **111**, 1935, p. 159-280).

[22] MAGNUS (W.). — *Ueber Beziehungen zwischen höheren Kommutatoren* (*J. R. An. Math.*, t. **177**, 1937, p. 105-115).

[23] MAGNUS (W.). — *Ueber Gruppen und zugeordnete Liesche Ringe* (*J. R. An. Math.*, t. **182**, 1940, p. 142-149).

[24] MAGNUS (W.). — *A connection between the Baker-Hausdorff formula and a problem of Burnside* (*Ann. Math.*, t. **52**, 1950, p. 111-126).

[25] MALCEV (A. I.). — *Sur une classe d'espaces homogènes* (*Izvest. Akad. Nauk S. S. S. R.*, sér. Math., t. **13**, 1949, p. 9-32).

[26] MALCEV (A. I.). — *Groupes nilpotents sans torsion* (*Izvest. Akad. Nauk S. S. S. R.*, sér. Math., t. **13**, 1949, p. 201-212).

[27] MALCEV (A. I.). — *Sur les algèbres de Lie normées sur le corps des nombres rationnels* (*Dok. Akad. Nauk S. S. S. R.*, t. **62**, 1948, p. 745-748).

[28] POINCARÉ (H.). — *Sur les groupes continus* (*Œuvres*, t. III, p. 173-212, Paris, 1934).

[29] SAMUEL (P.). — *Algèbre locale* (*Mém. Soc. Math.*, t. **123**, 1953).

[30] SANOV (I. N.). — *Sur une liaison entre des groupes périodiques dont la période est un nombre premier et des anneaux de Lie* (*Izvest. Akad. Nauk S. S. S. R.*, sér. Mat., t. **16**, 1952, p. 23-58).

[31] SANOV (I. N.). — *Sur un système de relations dans les groupes périodiques dont la période est une puissonce d'un nombre premier* (*Izvest. Akad. Nauk S. S. S. R.*, sér. Mat., t. **15**, 1951, p. 477-502).

[32] SCHAFAREVITCH (I. R.). — *Sur les p-extensions* (*Mat. Sbor.*, t. **20**, 1947, p. 351-363).

[33] WITT (E.). — *Treue Darstellung Liescher Ringe* (*J. R. An. Math.*, t. **177**, 1937, p. 152-160).

[34] ZASSENHAUS (H.). — *The theory of groups* (New-York, Chelsea, 1949).

[35] ZASSENHAUS (H.). — *Ueber liesche Ringe mit Primzahlcharakteristik* (*Abh. Mat. Sem. Hamb.*, t. **13**, 1940, p. 1-100).

[36] ZASSENHAUS (H.). — *Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charakteristik p zuzuzuordnen* (*Abh. Mat. Sem. Hamb.*, t. **13**, 1940, p. 200-207).