PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

MICHEL LAZARD

Groupes analytiques *p*-adiques

Publications mathématiques de l'I.H.É.S., tome 26 (1965), p. 5-219.

<http://www.numdam.org/item?id=PMIHES_1965__26__5_0>

INTRODUCTION

1. Groupes analytiques et application exponentielle.

Cet article traite des *groupes analytiques p-adiques*, ou groupes analytiques sur $\mathbf{Q}_p$, et de leur *cohomologie*.

Il existe une théorie générale des groupes analytiques sur un corps de caractéristique zéro, complet pour une valeur absolue : voir l'article de Dynkin [6] et sa bibliographie. Dynkin met en évidence les propriétés communes aux groupes analytiques sur $\mathbf{R}$ et sur $\mathbf{Q}_p$ (complétions du corps premier $\mathbf{Q}$); sa théorie est locale : elle n'étudie que certains voisinages des éléments neutres des groupes; par contre les espaces ne sont pas supposés de dimension finie.

Nous nous intéressons seulement ici aux propriétés des groupes p-adiques. *Ces groupes admettent leurs sous-groupes ouverts comme système fondamental de voisinages de l'unité.* La théorie « locale » est ainsi « globale » en ce sens qu'elle permet d'étudier des groupes proprement dits. Cela nous conduit à introduire diverses catégories de groupes; disons, en première approximation, qu'il s'agit des groupes qu'on peut construire à partir d'algèbres de Lie par l'*application exponentielle*, ainsi que de leurs *sous-groupes fermés*.

Rappelons que, pour un groupe analytique *réel* G, l'application exponentielle est définie sur toute l'algèbre de Lie L de G, et prend ses valeurs dans G (voir, par ex. [5], chap. IV, n° 8). Elle n'est pas nécessairement injective ni surjective, et son image n'est pas nécessairement un sous-groupe de G. Au contraire, si G est un groupe analytique *p-adique*, et L son algèbre de Lie, l'application exponentielle *n'est définie que sur une partie de* L; elle est *injective* et son image est un *sous-groupe ouvert* de G. En fait, si G est une limite projective de p-groupes discrets, c'est l'application « logarithme » qui est définie sur G tout entier et prend ses valeurs dans L; l'exponentielle n'est alors qu'une application réciproque partielle du logarithme.

Ces phénomènes apparaissent clairement dans l'étude du groupe multiplicatif $\mathrm{G}=\mathbf{Q}_p^*$ dont l'algèbre de Lie est le groupe additif $\mathrm{L}=\mathbf{Q}_p$. L'application exponentielle est définie par la série classique

$$\exp x = \sum_{n \in \mathbf{N}} (n!)^{-1} x^n. \tag{1}$$

Celle-ci converge pour les $x \in \mathbf{Q}_p$ de valuation $\geqslant 1$ si $p>2$ (resp. $\geqslant 2$ si $p=2$). Il vaut beaucoup mieux dire que la série (1) *converge pour les x vérifiant*

$$v(x) > (p-1)^{-1}, \tag{2}$$

où v désigne la valuation p-adique normalisée par la condition

$$v(p)=1. \tag{3}$$

En effet ce dernier énoncé vaut encore si x est pris dans une extension valuée complète de $\mathbf{Q}_p$, et nous parviendrons à le généraliser sous cette forme. Avant d'exposer ces généralisations, résumons quelques notions d'analyse p-adique qui font l'objet du chapitre I^er^.

2. Espaces de Banach p-adiques et notions dérivées.

Tous les *espaces vectoriels normés* rencontrés jusqu'à présent (cf. [26]) sur un *corps valué* k vérifient la relation *ultramétrique* (ou inégalité du triangle renforcée)

$$|x+y| \leqslant \max(|x|, |y|). \tag{4}$$

Les *boules* centrées à l'origine d'un tel espace sont alors des *modules* sur l'*anneau* Ω *des entiers* du corps k. Il nous sera plus commode de formuler nos résultats pour des Ω-modules que pour des k-espaces vectoriels.

Tout d'abord nous remplacerons la notation multiplicative des valeurs absolues et des normes par la *notation additive* des valuations, en conservant les conventions usuelles (les « majorations » sont des minorations, etc.).

Ensuite nous nous contenterons des *boules unités*, c'est-à-dire des éléments de valuation $\geqslant 0$. Exception faite des corps valués (qui n'interviendront que rarement) « valué » signifiera « *positivement* valué ».

Enfin nous utiliserons une notion de *filtration (positive)* plus générale que celle de valuation. Notre définition d'*anneau filtré* est donnée en (I, 2.1.1), celle de *module filtré sur un anneau filtré* en (I, 2.1.3). Les *anneaux et modules valués* sont définis en (I, 2.2.1) et (I, 2.2.2). La principale différence entre filtrations et valuations telles que nous les rencontrerons est que les premières servent aux définitions et les secondes aux théorèmes (voir, par exemple, la définition du produit tensoriel filtré en (I, 2.1.9) ainsi que le théorème (I, 3.2.1)).

Les anneaux (resp. modules) filtrés possèdent des anneaux (resp. modules) *gradués associés*. Les degrés sont des nombres réels $\geqslant 0$, non nécessairement entiers (définitions en (I, 1.1)). Lorsque l'anneau gradué Γ est un *anneau de polynômes en une lettre sur un corps* (muni de sa graduation naturelle), les Γ-modules gradués ont une structure particulièrement simple : il est plus important de supposer les degrés positifs que de les supposer entiers (I, 1.2).

Les *morphismes de modules filtrés* sont définis de telle sorte que le passage au gradué associé soit un foncteur, que nous notons « gr ». Nous utilisons le langage des catégories, mais seulement d'un point de vue naïf : nous n'avons pas besoin d'Univers. Les modules gradués (sur un même anneau gradué) constituent une catégorie *abélienne*, tandis que les modules filtrés (sur un même anneau filtré) forment seulement une catégorie *additive*. Cela explique peut-être l'importance du foncteur gr, qui ne sait pourtant pas distinguer un module de son séparé-complété.

L'introduction de filtrations à valeurs réelles positives entraîne quelques complications par rapport aux filtrations à valeurs entières : cf., par ex. (I, 2.3.8) et [3], prop. 2, p. 25. Le point important n'est pas que les valeurs des filtrations soient entières, mais qu'elles constituent une *partie discrète* de $\mathbf{R}$: cette propriété définit les *filtrations discrètes* (I, 2.1.12). Il est commode, pour travailler avec des filtrations discrètes, d'avoir supposé les filtrations positives (car toute partie discrète de $\mathbf{R}_+$ engendre un sous-monoïde additif discret).

Nous avons introduit les modules valués comme sous-modules d'une « boule unité ». Réciproquement, à partir d'un *module valué* M sur un *anneau valué commutatif* Ω, nous pouvons reconstruire la boule unité du plus petit espace vectoriel (sur le corps k des fractions de Ω) contenant M. Nous appelons *divisé de* M et notons div M le module valué ainsi obtenu. En complétant div M nous obtenons la boule unité du plus petit espace de Banach contenant M; nous appelons ce module *saturé de* M et nous le notons Sat M. Les foncteurs « div » et « Sat » sont définis en (I, 2.2).

Nous aurons surtout à utiliser des *modules valués* sur $\mathbf{Z}_p$. La plupart des propriétés de ces modules restent valables si $\mathbf{Z}_p$ est remplacé par un *anneau de valuation discrète complet* Ω (I, 3). Le gradué associé est un anneau de polynômes en une lettre sur le corps résiduel de Ω. Les Ω-modules *valués complets* pour une filtration *discrète* ont une structure simple (I, 3.1.3); les Ω-modules *valués de type fini* sont complets et de valuation discrète (I, 3.1.4). Il est possible de définir dans la catégorie des Ω-modules valués un *produit tensoriel* dont les propriétés sont presque aussi simples que celles du produit tensoriel d'espaces vectoriels (I, 3.2). Cela permet d'étudier les produits tensoriels *complétés* ou *saturés*, ainsi que les algèbres tensorielles, symétriques et extérieures dans la catégorie des Ω-modules valués (I, 3.3).

3. Construction de groupes; algèbres diagonales.

La formule de Hausdorff (IV, 3.2.2)

$$\Phi(x,y)=x+y+\frac{1}{2}[x,y]+\ldots+u_n(x,y)+\ldots \tag{5}$$

est « symbolique » en ce sens qu'elle est seulement une égalité de séries formelles : le corps de base $\mathbf{Q}$ y est pris avec sa topologie discrète.

Nous nous intéressons ici à la topologie p-adique de $\mathbf{Q}$ et aux algèbres de Lie topologiques correspondantes. L'écriture explicite de $\Phi(x,y)$ par Dynkin et la majoration p-adique qui s'ensuit [6] ne sont pas « les meilleures possibles ». En fait *la série de Hausdorff* (5) *a même rayon de convergence p-adique que la série exponentielle* (1).

Pour préciser cet énoncé, supposons que L soit une $\mathbf{Z}_p$-algèbre de Lie valuée, la valuation w satisfaisant à l'axiome

$$w([x,y])\geqslant w(x)+w(y). \tag{6}$$

La structure de $\mathbf{Z}_p$-algèbre de Lie se prolonge naturellement au module saturé Sat L. Disons, avec Serre [28], que L est *$*$-saturée* si L s'identifie à l'ensemble des éléments de valuation $>(p-1)^{-1}$ de Sat L. Si L est une telle algèbre de Lie, les « polynômes de Lie » u_n de (5) définissent des *fonctions* non seulement dans $\mathbf{Q}_p\otimes_{\mathbf{Z}_p}\mathrm{L}$, mais aussi *dans l'algèbre de Lie* L, et la série (5) *converge* lorsqu'on remplace x et y par deux éléments de L. Ces assertions, prouvées directement dans [18], nous permettent d'*associer un groupe à chaque* $\mathbf{Z}_p$*-algèbre* $*$*-saturée*, par l'introduction d'une nouvelle opération sur le même ensemble.

Nous adopterons ici une méthode indirecte, mais plus puissante. Au lieu de prendre la série (5) comme donnée, *nous justifierons toujours la formule*

$$\exp\Phi(x,y)=(\exp x)(\exp y). \tag{7}$$

Pour cela nous nous ramènerons à l'étude d'une $\mathbf{Z}_p$*-algèbre associative saturée* A, dont la valuation vérifie

$$w(xy)\geqslant w(x)+w(y). \tag{6'}$$

Nous calculerons dans A les exponentielles (resp. logarithmes) des éléments x vérifiant $w(x)>(p-1)^{-1}$ (resp. $w(x-1)>(p-1)^{-1}$); cf. (III, 1.1). Par « sous-algèbre de Lie de A » nous entendrons un sous-$\mathbf{Z}_p$-module stable pour le crochet $[u,v]=uv-vu$.

L'assertion suivante équivaut à la formule de Hausdorff avec sa majoration p-adique : *si* L *est une sous-algèbre de Lie* $*$*-saturée de* A, *l'ensemble des éléments* $\exp x$, x *parcourant* L, *est un sous-groupe multiplicatif de* A.

Nous définissons (IV, 1.2) une $\mathbf{Z}_p$-algèbre diagonale saturée comme une $\mathbf{Z}_p$*-algèbre supplémentée saturée*, munie d'un *homomorphisme*

$$\Delta:\ \mathrm{A}\to\mathrm{Sat}(\mathrm{A}\otimes_{\mathbf{Z}_p}\mathrm{A}). \tag{8}$$

Dans une telle algèbre, l'ensemble $\mathscr{L}$A des éléments vérifiant

$$\Delta x=x\otimes 1+1\otimes x \tag{9}$$

est une *sous-algèbre de Lie saturée*; l'ensemble $\mathscr{L}^*$A des $x\in\mathscr{L}$A vérifiant $w(x)>(p-1)$ est une *sous-algèbre de Lie* $*$*-saturée*.

D'autre part, nous notons $\mathscr{G}$A l'ensemble des $x\in\mathrm{A}$ d'augmentation unité, vérifiant

$$\Delta x=x\otimes x. \tag{10}$$

La partie $\mathscr{G}^*$A de $\mathscr{G}$A, définie par la condition $w(x-1)>(p-1)^{-1}$, est un *groupe multiplicatif* dans A.

Un théorème presque évident, mais fondamental, établit un isomorphisme « foncториel » entre $\mathscr{L}^*$A et $\mathscr{G}^*$A, au moyen des fonctions exp et Log (IV, 1.3.5).

Partons d'une $\mathbf{Z}_p$-algèbre de Lie valuée L; construisons les algèbres UL (algèbre enveloppante de L) et Sat UL, puis prenons sur Sat UL la structure naturelle d'algèbre diagonale, définie par la condition : $\mathrm{L}\subset\mathscr{L}\,\mathrm{Sat\,UL}$.

Nous avons alors le *théorème de saturation* (IV, 3.1.3), qui consiste principalement en la formule

$$\mathscr{L}\ \mathrm{Sat\,UL}=\mathrm{Sat\,L}. \tag{11}$$

La formule de Hausdorff et sa majoration p-adique s'en déduisent aisément. L'essentiel dans la preuve du théorème de saturation est l'analogue « infinitésimal » du théorème de Dedekind sur l'indépendance linéaire des automorphismes de corps.

4. Filtrations de groupes.

Une filtration d'un groupe G est une fonction à valeurs *strictement positives* (et $+\infty$) qui vérifie les deux axiomes (II, 1.1.1)

$$\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y)); \tag{12}$$

$$\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y). \tag{13}$$

Une *algèbre de Lie graduée* gr G peut être associée au groupe filtré G (II, 1.1.7); les morphismes sont définis afin d'avoir un *foncteur* « gr ».

Soient A un *anneau filtré*, G un groupe multiplicatif dans A, tels que $w(x-1) > 0$ pour tout $x \in \mathrm{G}$. Nous définissons la *filtration induite* ω de G en posant

$$\omega(x) = w(x-1) \qquad \text{pour} \qquad x \in \mathrm{G}, \tag{14}$$

et nous obtenons une injection canonique de gr G dans gr A (II, 1.1.9).

Lorsque la condition de normalisation (3) est vérifiée dans A, c'est-à-dire si $w(p) = 1$, la filtration induite ω satisfait à l'axiome supplémentaire (II, 1.2.1)

$$\omega(x^p) \geqslant \min(\omega(x) + 1, p\omega(x)). \tag{15}$$

Nous prenons cet axiome comme *définition des p-filtrations* (II, 1.2.10). Dans un groupe p-filtré G, l'élévation à la p-ième puissance donne, par passage au quotient, un opérateur P défini sur l'ensemble des éléments homogènes de gr G. Nous obtenons ainsi sur gr G une structure que nous appelons *algèbre de Lie mixte* (II, 1.2.5) et (II, 1.2.11). Cette dénomination vient de ce que gr G « commence » comme une algèbre de Lie restreinte (au sens de Jacobson), et « finit » comme une Γ-algèbre de Lie graduée, Γ désignant l'anneau de polynômes $\mathbf{F}_p[\pi]$ avec sa graduation naturelle ($\deg \pi = 1$).

Les groupes *p-valués*, définis en (III, 2.1.2), sont, parmi les groupes p-filtrés, l'analogue des $\mathbf{Z}_p$-modules valués parmi les $\mathbf{Z}_p$-modules filtrés. Si G est p-valué, gr G est une Γ-algèbre de Lie, libre en tant que Γ-module, dont le rang sur Γ est dit *rang* de G.

L'algèbre $\mathbf{Z}_p[\mathrm{G}]$ d'un groupe p-valué G peut être munie canoniquement (III, 2.3.1) d'une structure de *$\mathbf{Z}_p$-algèbre associative valuée*, dont la filtration induit celle de G, de telle sorte que gr $\mathbf{Z}_p[\mathrm{G}]$ s'identifie à U gr G (l'algèbre enveloppante de la Γ-algèbre gr G). Ce résultat (III, 2.3.3) est important, car il nous permet de construire la $\mathbf{Z}_p$-algèbre *saturée* Sat $\mathbf{Z}_p[\mathrm{G}]$, et cette dernière possède une application diagonale naturelle, définie par la condition $\mathrm{G} \subset \mathscr{G}^* \operatorname{Sat} \mathbf{Z}_p[\mathrm{G}]$.

Définissons l'extension Sat G d'un groupe p-valué G par la formule (IV, 3.3.1)

$$\operatorname{Sat} \mathrm{G} = \mathscr{G}^* \operatorname{Sat} \mathbf{Z}_p[\mathrm{G}]. \tag{16}$$

Appelons *p-saturé* un groupe p-valué G tel que $G = \mathrm{Sat}\, G$. Cette relation est vérifiée si et seulement si G est *complet* (pour la topologie définie par sa filtration) et si *tout élément de filtration* $> p(p-1)^{-1}$ *est une p-ième puissance dans* G. L'assertion précédente est contenue dans le « théorème de saturation des groupes » (IV, 3.2.5), qui nous apprend aussi que la catégorie des $\mathbf{Z}_p$-algèbres diagonales de la forme Sat $\mathbf{Z}_p[G]$, où G est un groupe p-valué, coïncide avec celle des Sat UL, où L est une $\mathbf{Z}_p$-algèbre de Lie valuée. Cette *égalité* de deux catégories de $\mathbf{Z}_p$-algèbres diagonales saturées conduit à l'*isomorphisme* de deux catégories : celle des $\mathbf{Z}_p$-*algèbres de Lie* $*$-saturées et celle des *groupes* p-saturés (IV, 3.2.6).

5. Groupes analytiques.

Faisons maintenant des hypothèses de finitude. Nous réserverons le nom de variétés analytiques p-adiques aux variétés analytiques de *dimension finie* sur $\mathbf{Q}_p$: cf. [28], [30].

Un *groupe analytique de dimension r sur* $\mathbf{Q}_p$ (III, 3.1.1) est localement compact et totalement discontinu. Sa topologie est donc définie par ses *sous-groupes ouverts compacts* (ou *profinis* [23]). Parmi ces sous-groupes ouverts compacts, il en est qui peuvent être munis d'une *filtration à valeurs entières* pour laquelle ils sont *p-saturés de rang r* (III, 3.1.3).

Soit G un groupe *p-valué complet de rang fini r*. Nous pouvons choisir dans G une *base ordonnée* (III, 2.2.4) qui définit un système de « *coordonnées de seconde espèce* » identifiant le groupe à $\mathbf{Z}_p^r$. Cette identification met en évidence l'*analyticité* de G; plus précisément (III, 3.1.5) le produit et l'inverse sont donnés dans G par des fonctions *analytiques strictes* au sens de (III, 1.3.5). Si G est *p-saturé*, ces fonctions sont même *analytiques tayloriennes* (III, 3.3.1) au sens de (III, 1.3.4).

Nous définissons (III, 3.1.6) les groupes *p-valuables* (resp. *p-saturables*) comme les groupes admettant une *p-valuation* pour laquelle ils sont *complets* (resp. *saturés*) *de rang fini* (un groupe p-valué n'est donc pas toujours p-valuable...). Des propriétés de la *catégorie* des groupes p-valuables (resp. p-saturables) sont énoncées en (III, 3.1.7) (resp. (III, 3.2.2)).

Si un *pro-p-groupe* (II, 2.1.2), ou plus généralement un groupe profini G, admet une structure analytique sur $\mathbf{Q}_p$, celle-ci est unique (III, 3.2.2) et (comme l'a remarqué Chevalley) ne dépend que du groupe « abstrait » G (et non de sa topologie, contrairement aux groupes de Lie réels). La question « *le pro-p-groupe* G *est-il analytique ?* » possède donc un sens.

Nos *critères d'analyticité* concernent les pro-p-groupes de *type fini* (II, 2.1.4). Ils expriment sous différentes formes l'idée suivante : les pro-p-groupes analytiques sont ceux où l'on rencontre beaucoup plus de p-ièmes puissances que de commutateurs; cf. (A, 1.2) et (A, 1.9).

Nous utilisons essentiellement certaines p-filtrations, appelées (t, p)-filtrations ou (x, τ, p)-filtrations (II, 3.2). Ces dernières font intervenir explicitement une famille de générateurs, et sont, de ce fait, assez compliquées; cependant elles fournissent toutes les p-valuations des groupes p-valuables (III, 3.1.10), et nous les rencontrons « naturellement » dans certains exemples (III, 3.2.7), (IV, 3.4.10).

Un critère simple (III, 3.4.4) permet d'établir un théorème de Serre (III, 3.4.5) concernant les extensions de groupes analytiques sur $\mathbf{Q}_p$.

Les séries de Golod-Chafarévitch [19] fournissent un critère d'analyticité pour lequel il faut recourir à l'analyse classique : c'est « l'alternative des gocha » (A, 3.11).

6. Cohomologie.

La cohomologie de Tate des groupes profinis ([29], chap. Ier) fait opérer ceux-ci *continûment* sur des modules *discrets*. Le complexe des *cochaînes continues* permet de définir plus généralement la *cohomologie continue* $\mathrm{H}_c^*(\mathrm{G}, \mathrm{M})$ d'un groupe topologique G opérant continûment sur un module topologique M.

Nos résultats (V) concernent le cas où G est un *pro-p-groupe analytique*, ou un *groupe compact analytique sur* $\mathbf{Q}_p$. Quant au G-module topologique M, nous devons supposer que c'est une *limite projective de p-groupes additifs discrets* (non nécessairement finis).

Les complexes standard complétés (V, 1.2) traduisent la définition par cochaînes continues. Le rôle de l'algèbre $\mathbf{Z}[\mathrm{G}]$ en cohomologie discrète est joué, en cohomologie continue, par la *$\mathbf{Z}_p$-algèbre complétée du groupe* G, notée Al G, définie comme limite projective :

$$\mathrm{Al}\,\mathrm{G} = \varprojlim \mathbf{Z}_p[\mathrm{G}/\mathrm{U}], \tag{17}$$

U parcourant les sous-groupes ouverts distingués de G.

Lorsque G est un groupe p-valué complet de rang r, l'algèbre Al G est valuée (III, 2.3.3) et gr Al G s'identifie à U gr G (rappelons que gr G est une Γ-algèbre de Lie et un Γ-module libre de rang r). Il existe alors un complexe standard de gr G (V, 1.3.4), homotopiquement équivalent au complexe standard de U gr G (V, 1.2.1), mais beaucoup plus maniable. Un lemme de Serre (V, 2.1) permet de « remonter » le complexe standard de gr G : nous obtenons ainsi un *complexe quasi-minimal* (V, 2.2) qui est une *résolution* Al G-*libre et acyclique de* $\mathbf{Z}_p$, *nulle en dimensions* $>r$.

Utilisant la « dualité de Poincaré », développée par Serre-Tate-Verdier [29], ainsi qu'un théorème récent de Serre [31], nous parvenons à l'énoncé suivant, qui précise (V, 2.5.8) : *un pro-p-groupe analytique sans torsion est un groupe de Poincaré ; sa dimension cohomologique est égale à sa dimension de variété analytique sur* $\mathbf{Q}_p$ *; le caractère qui définit son module dualisant est le déterminant de sa représentation adjointe sur son algèbre de Lie.*

Même si le groupe G a de la torsion, nous avons (V, 3.2.7)

$$\mathrm{H}_c^n(\mathrm{G}, \mathrm{M}) = \mathrm{Ext}_{\mathrm{Al}\,\mathrm{G}}^n(\mathbf{Z}_p, \mathrm{M}). \tag{18}$$

J'ignore si ce résultat vaut encore quand G n'est plus analytique sur $\mathbf{Q}_p$.

Lorsque le module M est de la forme $\mathbf{Z}_p^r \times \mathbf{Q}_p^s$, nous pouvons définir le complexe des *cochaînes analytiques*. Nous obtenons ainsi des groupes de *cohomologie analytique* $\mathrm{H}_a^*(\mathrm{G}, \mathrm{M})$ et des homomorphismes naturels

$$\mathrm{H}_a^*(\mathrm{G}, \mathrm{M}) \to \mathrm{H}_c^*(\mathrm{G}, \mathrm{M}). \tag{19}$$

Ces derniers sont bijectifs (V, 2.3.10). Pour prouver ce théorème, nous traduisons l'hypothèse d'analyticité des cochaînes au moyen d'un critère de J. Hily et Y. Amice (III, 1.3.9).

Lorsque le module M est un $\mathbf{Q}_p$-espace vectoriel de dimension finie, l'*algèbre de Lie* L du groupe G (V, 2.4.2) opère sur M, ce qui permet de calculer ses groupes de cohomologie $H^*(L, M)$. Ces derniers s'identifient à la *cohomologie stable* $H^*_{st}(G, M)$, définie comme limite inductive pour la restriction :

$$H^*_{st}(G, M) = \varinjlim H^*_c(U, M), \tag{20}$$

U parcourant les sous-groupes ouverts de G. Le groupe G opère sur $H^*(L, M)$, et $H^*_c(G, M)$ s'identifie aux *points fixes* de $H^*(L, M)$: cf. (III, 2.4.10).

7. Divers.

L'Appendice qui termine ce travail devrait se trouver à la suite du chapitre III, qu'il prolonge directement.

Si le lecteur ne s'intéresse pas aux critères d'analyticité, il peut négliger la notion générale d'algèbre de Lie mixte (II, 1.2), pour ne considérer que des algèbres de Lie ordinaires : cf. (III, 2.1.1).

Le chapitre IV (formule de Hausdorff, etc.) se trouve assez isolé. Exception faite de (V, 2.4), nous utilisons rarement ses résultats, et la théorie des groupes analytiques p-adiques pourrait sans doute être développée sans parler de l'application exponentielle.

Parmi les nombreuses questions ouvertes, en voici quatre qui me paraissent assez vastes.

A) Le foncteur « Ala », défini en (III, 3.3), n'est pas utilisé plus loin. La *cohomologie taylorienne* d'un groupe *p-saturé* de rang fini G est définie comme la cohomologie continue de l'algèbre Ala G (V, 1.1.7). Si $G = \mathbf{Z}_p$, on retrouve des calculs de [16] par une voie différente. J'ai décrit dans [20] un complexe de H. Cartan qui joue, pour la cohomologie taylorienne, le même rôle que le complexe de Koszul pour la cohomologie continue. Par produits tensoriels on atteint facilement les groupes commutatifs de la forme $\mathbf{Z}_p^r$, mais l'extension du lemme de Serre (V, 2.1), qui permettrait de prouver quelques résultats généraux sur la cohomologie taylorienne, n'est pas encore au point. Lorsqu'on étudie la cohomologie taylorienne d'un groupe G à coefficients dans des $\mathbf{F}_p$-*espaces vectoriels*, on trouve la *cohomologie rationnelle* (au sens de Hochschild [11]) de G/G^p, considéré comme groupe algébrique sur $\mathbf{F}_p$.

B) Nous avons utilisé la « majoration p-adique » de la formule de Hausdorff, mais l'étude des *propriétés arithmétiques fines* de cette formule (notamment des valuations p-adiques de ses termes) reste à faire. On peut encore en espérer des applications intéressantes à la théorie des p-groupes.

C) L'étude comparée des cohomologies des groupes et des algèbres de Lie a été menée brutalement (V, 2.4) : nous avons tué toute la torsion. Pour un groupe

p-saturable G, la comparaison *arithmétique* des cohomologies de G et de la $\mathbf{Z}_p$-algèbre de Lie associée reste à faire.

D) De même qu'on étudie des groupes de Lie complexes, il y aurait lieu d'examiner les groupes analytiques sur une extension finie K de $\mathbf{Q}_p$. Pour ne pas allonger l'exposé, je n'ai pas signalé les énoncés obtenus (au chap. IV) en supposant donnés les « sous-groupes à un paramètre analytique sur K »; cf. aussi [6]. Il conviendrait de généraliser les résultats de (V, 2.3) en définissant la *cohomologie holomorphe* d'un pro-p-groupe analytique sur K. Il est vraisemblable que, si la « dimension cohomologique holomorphe » est finie, elle est égale à la dimension du groupe comme variété analytique sur K.

Je n'aurais pas pu entreprendre ni achever ce travail sans le concours de Jean-Pierre Serre qui, dans les rôles multiples d'inspirateur, de référendaire, voire même de lecteur, a constitué en fait un jury, à qui je présente ces thèses avec une reconnaissance sincère et amicale.

Conventions générales

Anneaux et algèbres. — Le mot « anneau » signifiera toujours dans cet article « anneau associatif possédant une unité distincte du zéro ».

Les *modules* seront unitaires et, sauf mention du contraire, à gauche sur l'anneau de base.

Les *algèbres* seront *associatives* ou *de Lie*. Les algèbres associatives seront unitaires.

Une *algèbre supplémentée* A sur l'anneau commutatif Ω est une Ω-algèbre associative, donnée avec un homomorphisme $\varepsilon : A \rightarrow \Omega$, appelé *augmentation*; cf. [4], chap. X.

Multidegrés. — Pour tout ensemble I, $\mathbf{N}^I$ désigne l'ensemble des applications de I dans $\mathbf{N}$, c'est-à-dire des familles $\alpha = (\alpha_i)_{i \in I}$ d'entiers $\geqslant 0$. La partie $\mathbf{N}^{(I)}$ de $\mathbf{N}^I$ est formée des α tels que $\alpha_i = 0$, sauf pour un nombre fini d'indices $i \in I$. Nous posons alors $|\alpha| = \sum_{i \in I} \alpha_i$.

Nous munissons $\mathbf{N}^I$ et $\mathbf{N}^{(I)}$ de leurs structures de monoïdes additifs ordonnés : $(\alpha + \beta)_i = \alpha_i + \beta_i$ pour tout i, et $\alpha \leqslant \beta$ équivaut à $\alpha_i \leqslant \beta_i$ pour tout i.

Constantes. — Les lettres grasses sont, en principe, réservées aux *constantes* : $\mathbf{Z}$ désigne les entiers rationnels, etc.

Voici les exceptions à l'usage que le lecteur rencontrera.

Des lettres grecques grasses sont utilisées au chapitre V pour désigner des multidegrés.

La lettre p représente un *nombre premier* fixe. La lettre π est utilisée dans différents contextes, mais, à partir du théorème (3.11) de l'Appendice, elle désigne la constante connue 3,14...

Renvois. — Les numéros entre crochets renvoient à la bibliographie, ceux entre parenthèses au présent article. Les chiffres romains (ou la lettre A) indiquent le numéro du chapitre (ou l'Appendice); leur absence signifie qu'il s'agit du même chapitre (ou de l'Appendice).

CHAPITRE PREMIER

GRADUATIONS, FILTRATIONS, VALUATIONS

1. GRADUATIONS

(1.1) Anneaux et modules gradués.

(1.1.1) *Définition.* — Nous réserverons le nom d'anneau gradué aux anneaux gradués *de type* $\mathbf{R}_+$. Un tel anneau Γ est donc la *somme directe* de ses *composantes homogènes* Γ_ν (sous-groupes additifs), l'indice ν *(degré)* parcourant l'ensemble $\mathbf{R}_+$ des nombres réels $\geqslant 0$. Les éléments homogènes de Γ sont ceux qui appartiennent à l'un des Γ_ν; le produit de deux éléments homogènes de degrés ν et ν' est homogène de degré $\nu+\nu'$.

(1.1.2) Nous appellerons de même module sur l'anneau gradué Γ un Γ-*module gradué de type* $\mathbf{R}_+$. Un tel module M est donc la somme directe de ses composantes homogènes M_ν ($\nu\in\mathbf{R}_+$), et la relation

$$\Gamma_\nu . M_{\nu'} \subset M_{\nu+\nu'}$$

est supposée vérifiée pour tous $\nu, \nu'\in\mathbf{R}_+$.

(1.1.3) Les anneaux et modules gradués usuels, c'est-à-dire gradués de type $\mathbf{N}$, entrent dans notre définition si nous convenons que leurs composantes homogènes de degrés non entiers sont nulles.

Nous dirons que la graduation d'un anneau ou d'un module est *discrète* si l'ensemble des degrés des composantes homogènes non nulles est une partie discrète de $\mathbf{R}_+$.

Rappelons qu'une partie discrète de $\mathbf{R}_+$ est soit une partie finie, soit une suite indéfiniment croissante. Le sous-monoïde (additif) de $\mathbf{R}_+$ engendré par une partie discrète est encore une partie discrète.

(1.1.4) Si M et M′ sont deux modules sur l'anneau gradué Γ, nous appellerons *morphisme* $f : M \to M'$ une application Γ-linéaire de M dans M′, homogène de degré zéro, c'est-à-dire vérifiant $f(M_\nu)\subset M'_\nu$ pour tout ν.

Cette convention achève de définir la *catégorie* $\mathrm{Gr}(\Gamma)$ des modules gradués sur l'anneau gradué Γ. Définitions analogues pour les modules à droite.

(1.1.5) La catégorie $\mathrm{Gr}(\Gamma)$ est une catégorie abélienne. Autrement dit nous ne considérons que des sous-modules *gradués* (c'est-à-dire engendrés par leurs éléments homogènes), et les modules quotients sont toujours munis de leur graduation quotient (qui est définie puisque les noyaux sont gradués). Les sommes directes et les limites inductives existent dans $\mathrm{Gr}(\Gamma)$.

(1.1.6) Nous appellerons *famille de générateurs* d'un Γ-module gradué une famille de générateurs *homogènes*. Un Γ-module *libre* sera un Γ-module (gradué), libre pour une certaine famille de générateurs (homogènes).

(1.1.7) *Produit tensoriel gradué.* — Soient M un module à droite (mentionnons-le expressément!) et M′ un module à gauche, tous deux gradués sur l'anneau gradué Γ.

Le produit tensoriel $M''=M\otimes_\Gamma M'$ est un groupe additif (et un Γ-module si Γ est commutatif, auquel cas il est inutile d'introduire des modules à droite). Le groupe additif (resp. le module) M'' peut être muni d'une graduation définie univoquement par la condition suivante : *si* $x\in M$ *et* $x'\in M'$ *sont tous deux homogènes, de degrés* ν *et* ν', *alors* $x\otimes x'\in M''$ *est homogène de degré* $\nu+\nu'$.

L'unicité de cette graduation résulte de la représentation des éléments de M et de M′ comme sommes de leurs composantes homogènes. Son existence peut s'établir comme suit.

Restreignons les scalaires à la composante homogène Γ_0 de Γ. Comme les sous-groupes M_ν et $M'_{\nu'}$ sont des sous-Γ_0-modules, le produit tensoriel $M^*=M\otimes_{\Gamma_0}M'$ est la somme directe des sous-groupes $M_\nu\otimes_{\Gamma_0}M'_{\nu'}$ (pour $\nu,\nu'\in\mathbf{R}_+$), d'où l'existence de la graduation du groupe additif M^*. Or M'' s'obtient comme le quotient de M^* par le sous-groupe qu'engendrent les relations

$$x\lambda\otimes x'-x\otimes\lambda x' \qquad (x\in M,\ x'\in M',\ \lambda\in\Gamma).$$

Comme ces relations sont trilinéaires en (x, x', λ) nous pouvons supposer ces éléments homogènes, et le groupe gradué M'' (resp. le module gradué si Γ est commutatif) s'obtient comme quotient du groupe gradué M^*.

Le produit tensoriel $M''=M\otimes_\Gamma M'$, muni de la graduation précisée, sera dit le *produit tensoriel gradué* de M et M′ (sur Γ).

(1.1.8) *Propriétés du produit tensoriel gradué ; exemple.* — Le produit tensoriel gradué est « associatif » et il permute aux limites inductives. Cela veut dire que les mêmes assertions concernant le produit tensoriel usuel s'étendent sans modification au produit tensoriel gradué.

Supposons que M soit un module (à droite) libre engendré par les générateurs e_i de degrés τ_i $(i\in I)$ et que M′ soit libre pour les générateurs f_j de degrés θ_j $(j\in J)$. Alors le produit tensoriel gradué $M''=M\otimes_\Gamma M'$ est la somme directe des sous-groupes $e_i\Gamma\otimes f_j$; ses éléments homogènes de degré ν s'écrivent univoquement

$$\sum_{i,j} e_i\lambda_{i,j}\otimes f_j,$$

où les $\lambda_{i,j}$ sont des éléments de Γ, homogènes de degrés respectifs $\nu-(\tau_i+\theta_j)$ et presque tous nuls. Si Γ est commutatif, M'' est un Γ-module libre.

(1.1.9) *Algèbres graduées.* — Une algèbre sur l'anneau gradué Γ est un Γ-module gradué (1.1.2) muni d'une multiplication bilinéaire pour laquelle le produit de deux éléments homogènes est encore homogène, son degré étant la somme des degrés des facteurs. En d'autres termes la multiplication de l'algèbre A est définie par une application Γ-linéaire : $A \otimes_\Gamma A \to A$, et nous exigeons que cette application soit un *morphisme dans* $\mathrm{Gr}(\Gamma)$ (1.1.4). Cela suffit pour les *algèbres de Lie*. Les *algèbres associatives* sont supposées unitaires, et nous exigeons que l'homomorphisme d'algèbres $\Gamma \to A$ soit un morphisme dans $\mathrm{Gr}(\Gamma)$. Enfin pour définir une *algèbre supplémentée* nous devons nous donner un homomorphisme d'algèbres $A \to \Gamma$; nous supposons encore que c'est un morphisme dans $\mathrm{Gr}(\Gamma)$.

Le produit tensoriel gradué de deux Γ-algèbres associatives (resp. supplémentées) est encore une Γ-algèbre associative (resp. supplémentée).

(1.1.10) *Modification des degrés : homothétie et translation.* — Quand nous étudions un anneau gradué Γ et la catégorie $\mathrm{Gr}(\Gamma)$, nous pouvons multiplier par un même nombre strictement positif les degrés des éléments de Γ et des Γ-modules. Quand nous étudions un certain module M sur l'anneau gradué Γ, nous pouvons additionner une constante aux degrés des éléments homogènes non nuls de M (sans modifier les degrés dans Γ); cette constante peut être négative, pourvu que les nouveaux degrés dans M restent positifs.

(1.2) La catégorie $\mathrm{Gr}(\Gamma)$, où Γ est un anneau de polynômes en une indéterminée à coefficients dans un corps.

(1.2.1) *Définition de l'anneau gradué* Γ. — Soient k un *corps* commutatif et π une *indéterminée*. Nous formons l'anneau de polynômes $\Gamma = k[\pi]$ et nous munissons Γ de sa graduation naturelle. Précisons que la composante de degré zéro, Γ_0, est égale à k, et que π est homogène de degré strictement positif. Il est préférable de ne pas supposer que $\deg \pi = 1$: nous pourrons toujours appliquer la remarque (1.1.10).

(1.2.2) Γ-*modules sans torsion.* — Un Γ-module sans torsion M est un Γ-module gradué (1.1.2), sans torsion en tant que module : si λ et x sont deux éléments non nuls dans Γ et M respectivement, leur produit $\lambda x \in M$ est encore différent de zéro. Pour vérifier que M est sans torsion, il nous suffit de prendre x et λ homogènes (considérer les composantes homogènes de x et de λ). Puis il suffit de prendre $\lambda \in \Gamma$ de la forme π^n ($n \in \mathbf{N}$), car k est un corps. Enfin nous voyons que M *est un* Γ-*module sans torsion si et seulement si la multiplication par* π *est une injection de* M *dans lui-même*. Dans ce cas, la division par π des éléments de M est univoque lorsqu'elle est possible, et elle diminue les degrés de la constante $\deg \pi$ (>0). *Si* M *est sans torsion, à tout* $x \in M$ *correspond un plus grand entier* $n \in \mathbf{N}$ *tel qu'il existe* $y \in M$ *vérifiant* $\pi^n y = x$; *l'élément* y *est univoquement déterminé par* x.

Les démonstrations des deux théorèmes qui suivent seront données en (1.3).

(1.2.3) *Théorème : liberté des* Γ-*modules sans torsion.* — *Tout* Γ-*module sans torsion* M *est libre. Si* X ($\subset M$) *est une base de* M *et* X_ν *l'ensemble des éléments de* X *de degré* ν, *alors les cardinaux des ensembles* X_ν ($\nu \in \mathbf{R}_+$) *sont déterminés par* M. *Ces cardinaux définissent* M *à un isomorphisme près.*

(1.2.4) *Théorème des bases adaptées. — Soient* M *un* Γ*-module sans torsion et* N *un sous-module de* M. *Il existe une base* X *de* M (1.2.3) *possédant la propriété suivante. A tout* $x \in \mathrm{X}$ *associons le plus petit entier* $n_x \in \mathbf{N}$ *tel que* $\pi^{n_x} x \in \mathrm{N}$, *ou bien posons* $n_x = \infty$ *si* $\pi^n x \notin \mathrm{N}$ *pour tout* n ; *alors les éléments* $\pi^{n_x} x$ *constituent une base du module* N, x *parcourant la partie* X′ *de* X *sur laquelle* $n_x < \infty$. *Pour* $\nu \in \mathbf{R}_+$ *et* $n \in \mathbf{N} \cup \{\infty\}$, *définissons* $\mathrm{X}_{\nu,n}$ *comme l'ensemble des* $x \in \mathrm{X}$ *pour lesquels* $\deg x = \nu$ *et* $n_x = n$. *Le couple* (M, N) *détermine les cardinaux des* $\mathrm{X}_{\nu,n}$, *qui définissent le couple à un isomorphisme près.*

(1.2.5) *Corollaire. — Tout* Γ*-module* (1.1.2) *est somme directe de* Γ*-modules monogènes, isomorphes à* Γ *ou à* $\Gamma/\pi^n\Gamma$, *après translation des degrés* (1.1.10).

Preuve. — Chaque module est quotient d'un module libre (1.1.6), dans lequel nous prenons une base adaptée au noyau (1.2.4).

(1.2.6) *Corollaire. — Soient* $f : \mathrm{N} \to \mathrm{M}$ *et* $f' : \mathrm{N}' \to \mathrm{M}'$ *deux morphismes injectifs de* Γ*-modules sans torsion. Alors le morphisme* $f \otimes f' : \mathrm{N} \otimes_\Gamma \mathrm{N}' \to \mathrm{M} \otimes_\Gamma \mathrm{M}'$ *est injectif.*

Preuve. — Nous prenons des bases adaptées à M et $f(\mathrm{N})$ ainsi qu'à M′ et $f(\mathrm{N}')$, puis nous appliquons (1.1.8) : nous obtenons une base de $\mathrm{M} \otimes \mathrm{M}'$ adaptée à $(f \otimes f')(\mathrm{N} \otimes \mathrm{N}')$.

(1.2.7) *Remarque.* — Les théorèmes (1.2.3) et (1.2.4) ne font pas intervenir la commutativité de k. Ils restent vrais lorsque Γ est un anneau de polynômes « tordus » ainsi défini : k est un corps (non nécessairement commutatif), σ est un automorphisme de k, les éléments de Γ s'écrivent univoquement sous la forme $\sum_{i \in \mathbf{N}} \lambda_i \pi^i$ ($\lambda_i \in k$, presque tous nuls) et enfin $\pi\lambda = \lambda^\sigma \pi$, pour $\lambda \in k$. La composante Γ_0 de Γ est toujours supposée égale à k.

(1.3) Preuves des théorèmes (1.2.3) et (1.2.4).

(1.3.1) *Décomposition de la catégorie* Gr(Γ). — Quitte à diviser tous les degrés par $\deg \pi$, nous pouvons supposer que $\deg \pi = 1$ (1.1.10). Pour tout Γ-module M et tout nombre réel e, avec $0 \leqslant e < 1$, nous posons

(1.3.1.1) $$\mathrm{M}(e) = \coprod_{\nu - e \in \mathbf{N}} \mathrm{M}_\nu$$

Autrement dit, M(e) est la somme directe des composantes homogènes de M de degrés $e, e+1, e+2, \ldots$ Alors M(e), n'est pas seulement un sous-groupe additif, mais aussi un sous-Γ-module de M, et nous avons une décomposition de M en somme directe de Γ-modules :

(1.3.1.2) $$\mathrm{M} = \coprod_{0 \leqslant e < 1} \mathrm{M}(e).$$

Si $f : \mathrm{M} \to \mathrm{M}'$ est un morphisme de Γ-modules (1.1.4), f applique M(e) dans M′(e) pour tout e. Il nous suffira donc de démontrer les théorèmes (1.2.3) et (1.2.4) pour un Γ-module M tel que $\mathrm{M} = \mathrm{M}(e)$. D'après (1.1.10) nous pourrons diminuer de e les degrés des éléments homogènes de M, et *nous ramener ainsi à un module gradué de type* **N** (tel que $\mathrm{M} = \mathrm{M}(0)$), ce que nous supposerons désormais.

(1.3.2) *Cas particulier.* — Soit M un Γ-module sans torsion, gradué de type $\mathbf{N}$ et engendré (en tant que Γ-module) par sa composante M_α pour un certain entier $\alpha\in\mathbf{N}$. Les éléments homogènes non nuls de M sont de degré $\alpha+i$, $i\in\mathbf{N}$, et s'écrivent univoquement (1.2.2) sous la forme $\pi^i x$, $x\in M_\alpha$. Nous vérifions qu'une base $X\subset M_\alpha$ du k-espace vectoriel M_α est une base de M sur Γ, et que toute base de M sur Γ est une base de M_α sur k.

(1.3.3) *Preuve de* (1.2.3) *pour un* Γ*-module sans torsion* M, *gradué de type* $\mathbf{N}$. — Pour tout $\alpha\in\mathbf{N}$, notons ${}_\alpha M$ le sous-module de M engendré par les composantes M_i, où $0\leqslant i\leqslant\alpha$, et f_α le morphisme canonique de ${}_\alpha M$ sur le quotient ${}_\alpha M/{}_{\alpha-1}M$. Les ${}_\alpha M$ croissent avec α et leur réunion est M. Le module ${}_\alpha M/{}_{\alpha-1}M$ est engendré par ses éléments de degré α, et ses éléments homogènes non nuls sont ceux qui s'écrivent sous la forme $f_\alpha(\pi^i x)$, où $i\in\mathbf{N}$ et $x\in M_\alpha$ n'est pas divisible par π (1.2.2). Les modules ${}_\alpha M/{}_{\alpha-1}M$ sont donc sans torsion. Nous appliquons (1.3.2) et nous choisissons, pour chaque $\alpha\in\mathbf{N}$, une partie $X_\alpha\subset M_\alpha$ telle que la famille $f_\alpha(X_\alpha)$ soit une base de ${}_\alpha M/{}_{\alpha-1}M$. Par récurrence sur α nous voyons que $\bigcup_{0\leqslant i\leqslant\alpha} X_i$ est une base de ${}_\alpha M$, donc que $X=\bigcup_{i\in\mathbf{N}} X_i$ est une base de M. Réciproquement toute base de M s'obtient de cette manière, ce qui achève de prouver (1.2.3).

(1.3.4) *Preuve de* (1.2.4) *dans un cas particulier.* — Supposons comme en (1.3.2), que le module M soit engendré par sa composante M_α et prenons un sous-module quelconque N de M. Le module N est sans torsion, et possède donc (1.2.3) une base Y. A chaque élément $y\in Y$ associons l'élément $x\in M_\alpha$ et l'entier $n_x\in\mathbf{N}$, déterminés par la relation $y=\pi^{n_x}x$. Notons X′ la partie de M_α formée des x ainsi obtenus; la partie X′ est libre sur k, donc se complète en une base $X=X'\cup X''$ de M_α sur k, c'est-à-dire (1.3.2) de M sur Γ. Si N′ désigne le sous-module de M engendré par les $x\in X'$, le cardinal de X″ est déterminé par le quotient M/N′. Or N′ peut être défini comme l'ensemble des $z\in M$ tels qu'existe $n\in\mathbf{N}$ avec $\pi^n z\in N$. Nous avons donc prouvé (1.2.4) dans le cas particulier étudié.

(1.3.5) *Preuve de* (1.2.4) *lorsque* M *est un* Γ*-module sans torsion gradué de type* $\mathbf{N}$. — Reprenons les notations de (1.3.3), et soit N un sous-module de M. Posons, pour chaque $\alpha\in\mathbf{N}$, ${}^\alpha N={}_\alpha M\cap N$. Les ${}^\alpha N$ croissent avec α, et leur réunion est N. Soit Y_α une partie de ${}^\alpha N$ formée d'éléments homogènes, et telle que la famille $f_\alpha(Y_\alpha)$ soit une base du module sans torsion $f_\alpha({}^\alpha N)$. A chaque $y\in Y_\alpha$ associons $x\in M_\alpha$ et l'entier n_x défini par $y=\pi^{n_x}x$; notons X'_α l'ensemble des $x\in M_\alpha$ ainsi obtenu. Appliquant (1.3.4) au module ${}_\alpha M/{}_{\alpha-1}M$, nous voyons qu'il existe une partie X''_α de M_α telle que la famille $f_\alpha(X'_\alpha\cup X''_\alpha)$ soit une base de ${}_\alpha M/{}_{\alpha-1}M$. Posons

$$X_\alpha=X'_\alpha\cup X''_\alpha,\quad X=\bigcup_{\alpha\in\mathbf{N}} X_\alpha \quad\text{et}\quad Y=\bigcup_{\alpha\in\mathbf{N}} Y_\alpha.$$

Nous savons (1.3.3) que X est une base de M sur Γ; et nous voyons de même que Y est une base de N. Nous avons ainsi obtenu des bases adaptées pour M et N, et nous vérifions que toutes les bases adaptées s'obtiennent par le procédé suivi, ce qui, grâce à (1.3.1), établit (1.2.4) dans le cas général.

2. FILTRATIONS ET VALUATIONS

(2.1) Anneaux et modules filtrés.

(2.1.1) *Définition.* — Nous appellerons *anneau filtré* un anneau Ω muni d'une application

$$v : \Omega \to \mathbf{R}_+ \cup \{+\infty\}$$

vérifiant les axiomes suivants. Pour tous $\lambda, \mu \in \Omega$,

(2.1.1.1) $$v(\lambda - \mu) \geqslant \min(v(\lambda), v(\mu));$$

(2.1.1.2) $$v(\lambda\mu) \geqslant v(\lambda) + v(\mu);$$

(2.1.1.3) $$v(1) = 0.$$

La fonction v sera dite la filtration de Ω; le nombre $v(\lambda)$ s'appellera la filtration de l'élément $\lambda \in \Omega$. S'il intervient plusieurs anneaux, nous écrirons parfois $v(\Omega; \lambda)$ la filtration de $\lambda \in \Omega$.

L'axiome (2.1.1.2) implique soit (2.1.1.3), soit $v(\lambda) = +\infty$ pour tout $\lambda \in \Omega$. Ce dernier cas est inintéressant.

(2.1.2) *Définition de l'anneau filtré Ω par les idéaux Ω_ν.* — Pour chaque $\nu \in \mathbf{R}_+$, notons Ω_ν l'ensemble des $\lambda \in \Omega$ tels que $v(\lambda) \geqslant \nu$. Les Ω_ν sont une famille *d'idéaux* bilatères de Ω, possédant les propriétés suivantes :

(2.1.2.1) $$\Omega_\nu = \bigcap_{\nu' < \nu} \Omega_{\nu'}, \qquad \text{pour tout } \nu \in \mathbf{R}_+;$$

(2.1.2.2) $$\Omega_\nu . \Omega_{\nu'} \subset \Omega_{\nu+\nu'}, \qquad \text{pour tous } \nu, \nu' \in \mathbf{R}_+.$$

Réciproquement, si nous avons une famille d'idéaux Ω_ν vérifiant les deux relations précédentes, elle provient d'une filtration v de Ω, que nous retrouvons en posant

(2.1.2.3) $v(\lambda) = \sup \nu$, la borne supérieure étant prise sur l'ensemble des $\nu \in \mathbf{R}_+$ tels que $\lambda \in \Omega_\nu$.

(2.1.3) *Un module filtré* sur l'anneau filtré Ω est un Ω-module M muni d'une application

$$w : \mathrm{M} \to \mathbf{R}_+ \cup \{+\infty\}$$

vérifiant les axiomes

(2.1.3.1) $$w(x-y) \geqslant \min(w(x), w(y)) \qquad \text{pour } x, y \in \mathrm{M};$$

(2.1.3.2) $$w(\lambda x) \geqslant v(\lambda) + w(x) \qquad \text{pour } \lambda \in \Omega \text{ et } x \in \mathrm{M}.$$

Éventuellement nous écrirons $w(\mathrm{M}; x)$ au lieu de $w(x)$.

Pour chaque $\nu \in \mathbf{R}_+$, nous définissons M_ν comme l'ensemble des $x \in \mathrm{M}$ vérifiant $w(x) \geqslant \nu$. Les M_ν sont des sous-modules de M, qui satisfont aux relations.

(2.1.3.3) $$\mathrm{M}_\nu = \bigcap_{\nu' < \nu} \mathrm{M}_{\nu'}, \qquad \text{pour tout } \nu \in \mathbf{R}_+;$$

(2.1.3.4) $$\Omega_\nu . \mathrm{M}_{\nu'} \subset \mathrm{M}_{\nu+\nu'}, \qquad \text{pour tous } \nu, \nu' \in \mathbf{R}_+.$$

Réciproquement une telle famille de sous-modules correspond à une valuation w.

(2.1.4) Soient M et M′ deux Ω-modules filtrés (2.1.3). Nous appellerons *morphisme* $f: M \rightarrow M'$ une application Ω-linéaire vérifiant

(2.1.4.1) $$w(M'; f(x)) \geqslant w(M; x) \qquad \text{pour } x \in M,$$

ou la relation équivalente

(2.1.4.2) $$f(M_\nu) \subset M'_\nu \qquad \text{pour } \nu \in \mathbf{R}_+.$$

Nous venons de définir la *catégorie* des modules filtrés sur l'anneau filtré Ω. Cette catégorie sera notée Fil(Ω). Ce n'est pas une catégorie abélienne.

(2.1.5) Nous appellerons *isométrie* un morphisme $f: M \rightarrow M'$ qui est *injectif* et qui conserve les filtrations, c'est-à-dire vérifie

(2.1.5.1) $$w(M'; f(x)) = w(M; x) \qquad \text{pour } x \in M.$$

Si M est un sous-module d'un module filtré M′, la *filtration induite* de M s'obtient par restriction de la fonction w :

(2.1.5.2) $$w(M; x) = w(M'; x) \qquad \text{pour } x \in M.$$

Une isométrie $f: M \rightarrow M'$ permet d'identifier M au sous-module $f(M)$ de M′, muni de sa filtration induite.

(2.1.6) *Borne inférieure d'une famille de filtrations.* — Soit (v_i) $(i \in I)$ une famille de filtrations d'un anneau Ω (2.1.1). Posons

(2.1.6.1) $$v(\lambda) = \inf_{i \in I} v_i(\lambda), \qquad \text{pour } \lambda \in \Omega.$$

La fonction v ainsi définie est encore une filtration de Ω, que nous appellerons *la borne inférieure des filtrations* v_i. Si nous notons $\Omega_\nu^{(i)}$ l'idéal Ω_ν (2.1.2) correspondant à la filtration v_i, la filtration v est définie par les idéaux

(2.1.6.2) $$\Omega_\nu = \bigcap_{i \in I} \Omega_\nu^{(i)}.$$

Donnons-nous maintenant un anneau filtré Ω, un Ω-module M et une famille w_i de filtrations de M (2.1.3). Nous définissons la *borne inférieure* w des filtrations w_i en posant

(2.1.6.3) $$w(x) = \inf_{i \in I} w_i(x), \qquad \text{pour } x \in M.$$

Nous pouvons, comme en (2.1.6.2) définir la filtration w par les sous-modules M_ν :

(2.1.6.4) $$M_\nu = \bigcap_{i \in I} M_\nu^{(i)}.$$

(2.1.7) *Filtration quotient.* — Soient M un Ω-module filtré, et $f: M \rightarrow M'$ un épimorphisme de Ω-modules. Nous définissons la *filtration quotient* de M′ (pour le morphisme f) comme la *borne inférieure des filtrations de* M′ *pour lesquelles* f *est un morphisme dans* Fil(Ω). Cette définition équivaut à poser, pour $x \in M'$,

(2.1.7.1) $$w(M'; x) = \sup_{f(y) = x} w(M; y).$$

(2.1.8) *Les sommes directes et les limites inductives existent dans la catégorie* Fil(Ω). — Ce sont les sommes directes (resp. limites inductives) dans la catégorie des Ω-modules, munies de filtrations qu'on peut définir comme bornes inférieures, cf. (2.1.7).

La filtration d'une somme directe M de la famille des Ω-modules filtrés $M^{(i)}$ est définie par la formule

(2.1.8.1) $w(M; x) = \inf_{i \in I} w(M^{(i)}; x_i)$, *où x_i désigne la composante dans* $M^{(i)}$ *de l'élément* $x \in M$.

Si $M = \varinjlim M^{(i)}$ est une limite inductive des $M^{(i)}$, définie par les applications Ω-linéaires $f_i : M^{(i)} \to M$, la filtration de M est la borne inférieure des filtrations pour lesquelles les f_i sont des morphismes (2.1.4). Autrement dit nous posons

(2.1.8.2) $$w(M; x) = \sup_{i,y} w(M^{(i)}; y),$$

la borne supérieure étant prise sur l'ensemble des $i \in I$ et $y \in M^{(i)}$ tels que $f_i(y) = x$.

(2.1.9) *Le produit tensoriel filtré.* — Lorsque l'anneau filtré Ω n'est pas commutatif, nous étendons les définitions précédentes aux Ω-modules à droite, ce qui nous permet d'introduire généralement le produit tensoriel $M'' = M \otimes_\Omega M'$ d'un Ω-module (à droite) filtré M par un Ω-module (à gauche) filtré M'. Pour obtenir le *produit tensoriel filtré* de M et M' nous munissons le groupe additif M'' (resp. le Ω-module M'', si Ω est commutatif) de la *borne inférieure des filtrations w pour lesquelles*

(2.1.9.1) $$w(M''; x \otimes y) \geqslant w(M; x) + w(M'; y),$$

pour tous $x \in M$ *et* $y \in M'$.

Cette borne inférieure peut encore être définie comme suit. Nous considérons toutes les écritures d'un même élément $z \in M''$ sous la forme

(2.1.9.2) $$z = \sum_i x_i \otimes y_i, \qquad x_i \in M, y_i \in M',$$

et nous définissons $w(M''; z)$ comme la borne supérieure des nombres

(2.1.9.3) $$\inf_i (w(M; x_i) + w(M'; y_i)).$$

(2.1.10) *Propriétés du produit tensoriel filtré.* — Le produit tensoriel filtré est « associatif » et permute aux limites inductives : les assertions concernant les modules s'étendent sans modification aux modules filtrés.

(2.1.11) *Algèbres filtrées.* — Une algèbre filtrée A sur un anneau commutatif filtré Ω est une Ω-algèbre et un Ω-module filtré. Nous lui imposons de vérifier

(2.1.11.1) $$w(A; xy) \geqslant w(A; x) + w(A; y),$$

pour $x, y \in A$.

Cette condition s'énonce encore en disant que l'application Ω-linéaire $A \otimes_\Omega A \to A$, qui définit la multiplication dans A, doit être un morphisme dans la catégorie Fil(Ω). De même les applications $\Omega \to A$ et $A \to \Omega$ des algèbres associatives et supplémentées doivent être des morphismes dans $\mathrm{Fil}(\Omega)$. Une algèbre supplémentée A s'identifie à la somme directe (2.1.8) de Ω et de son idéal d'augmentation.

Le produit tensoriel filtré de deux algèbres associatives (resp. supplémentées) est une algèbre associative (resp. supplémentée).

(2.1.12) *Filtrations discrètes.* — La filtration d'un anneau (ou d'un module) sera dite *discrète* si l'ensemble des filtrations finies des éléments de l'anneau (ou du module) est une partie discrète de $\mathbf{R}_+$. Citons, comme exemple de filtrations discrètes, les filtrations à valeurs dans $\mathbf{N}$ [3]. Les filtrations discrètes ne sont pas plus compliquées que celles à valeurs dans $\mathbf{N}$; elles permettent les mêmes raisonnements par récurrence. Par contre les filtrations générales (à valeurs dans $\mathbf{R}_+$) s'accompagnent de phénomènes désagréables. C'est ainsi que la borne supérieure dans la formule (2.1.7.1) peut ne pas être atteinte en un $y \in \mathrm{M}$; même remarque pour la formule (2.1.8.2).

(2.1.13) *Topologie associée à une filtration.* — Un anneau (resp. module) filtré est un anneau (resp. module) *topologique* lorsqu'on prend comme système fondamental de voisinages de zéro les idéaux Ω_ν de (2.1.2) (resp. les sous-modules M_ν de (2.1.3)). La filtration sera dite *séparée* si la topologie est séparée, c'est-à-dire si zéro est le seul element de filtration infinie.

Remarquons qu'une filtration discrète (2.1.12) ne correspond pas nécessairement à une topologie discrète. Un morphisme de modules filtrés (2.1.4) est une application linéaire continue, mais une application linéaire continue n'est pas nécessairement un morphisme.

(2.1.14) *Complétions.* — Nous utiliserons toujours le mot « complet » au sens de « séparé et complet ». Un anneau filtré Ω est complet si et seulement si l'application canonique $\Omega \to \varprojlim \Omega/\Omega_\nu$ est bijective; même énoncé pour les modules. Nous construisons le complété d'un anneau filtré séparé Ω (resp. d'un module filtré séparé M) sous la forme $\hat{\Omega} = \varprojlim \Omega/\Omega_\nu$ (resp. $\hat{\mathrm{M}} = \varprojlim \mathrm{M}/\mathrm{M}_\nu$).

Nous avons ainsi un foncteur « chapeau » qui possède d'aussi bonnes propriétés qu'en [3] parce que les topologies considérées sont *métrisables*, que les filtrations soient discrètes ou non (2.1.12). En toute rigueur il nous faudrait parler de $\hat{\mathrm{M}}$ comme d'un module complet, donné avec une *isométrie* $\mathrm{M} \to \hat{\mathrm{M}}$ (2.1.5); en fait nous considérons le plus souvent $\hat{\mathrm{M}}$ comme une extension de M. La définition usuelle de $\hat{\mathrm{M}}$ fait intervenir la topologie (plus précisément la structure uniforme) de M. Nous nous intéressons bien plus aux morphismes dans $\mathrm{Fil}(\Omega)$ qu'aux applications continues (2.1.13); c'est pourquoi le complété $\hat{\mathrm{M}}$ d'un module filtré séparé M interviendra par la propriété suivante : c'est une extension filtrée complète de M, et tout morphisme de M dans un module filtré complet N se prolonge univoquement en un morphisme de $\hat{\mathrm{M}}$ dans N.

La complétée d'une algèbre (filtrée séparée) est une algèbre de même espèce (de Lie, associative ou supplémentée).

(2.1.15) *Complété d'une somme directe.* — Soient $\mathrm{M}^{(i)}$ $(i \in \mathrm{I})$ une famille de Ω-modules filtrés séparés, $\mathrm{M} = \coprod_{i \in \mathrm{I}} \mathrm{M}^{(i)}$ leur somme directe dans $\mathrm{Fil}(\Omega)$ (2.1.8). Le complété de M, que nous appellerons *somme directe complétée* des $M^{(i)}$ et noterons $\widehat{\coprod_{i\in I}} M^{(i)}$ peut être identifié à un sous-module du produit direct $\prod_{i\in I} \hat{M}^{(i)}$ des complétés des $M^{(i)}$; ses éléments sont alors les familles (x_i) $(i\in I,\ x_i\in\hat{M}^{(i)})$, pour lesquelles $w(\hat{M}^{(i)};\ x_i)$ tend vers l'infini (suivant le filtre des complémentaires des parties finies de I).

(2.1.16) *Familles filtrées-libres et modules filtrés libres.* — Soit $(x_i)_{i\in I}$ une famille d'éléments dans un Ω-module filtré M. Cette famille sera dite *filtrée-libre* si les conditions suivantes sont vérifiées.

(2.1.16.1) *Pour toute famille* $(\lambda_i)_{i\in I}$ *d'éléments de* Ω, *presque tous nuls,*

$$w(\sum_{i\in I}\lambda_i x_i)=\inf_{i\in I}(w(x_i)+v(\lambda_i)).$$

(2.1.16.2) *Les* $(x_i)_{i\in I}$ *sont linéairement indépendants sur* Ω.

Si nous supposons Ω et M séparés (2.1.13), la relation (2.1.16.1) implique (2.1.16.2), pourvu que les x_i soient tous différents de zéro.

Nous dirons qu'un Ω-module filtré M est *filtré-libre* (pour la *base filtrée* $(x_i)_{i\in I}$) s'il est engendré par la famille filtrée-libre $(x_i)_{i\in I}$. Un tel module est déterminé (à un isomorphisme près) par la donnée de l'ensemble I et de la famille des filtrations $w(x_i)$; celles-ci peuvent être choisies arbitrairement, et (2.1.16.1) définit la filtration du module de base filtrée $(x_i)_{i\in I}$.

Le module filtré-libre M est caractérisé (à un isomorphisme près) par la propriété suivante : quel que soit le Ω-module filtré N et la famille $(y_i)_{i\in I}$ d'éléments de N vérifiant

$$w(N;y_i)\geqslant w(M;x_i) \qquad \text{pour} \qquad i\in I,$$

il existe un morphisme $f: M\to N$, et un seul, vérifiant $f(x_i)=y_i$ pour $i\in I$.

(2.1.17) *Bases topologiques et modules complets libres.* — Nous supposons que l'anneau filtré Ω est *complet*. Nous dirons que la famille $(x_i)_{i\in I}$ d'éléments du Ω-module filtré M est une base *topologique* de M si elle est filtrée-libre (2.1.16) et si M est le *complété* du sous-module (filtré-libre) qu'engendrent les $(x_i)_{i\in I}$. Un module M qui possède une base topologique sera dit *complet-libre* (pour la base topologique en question).

Le module filtré-libre engendré par les éléments $(x_i)_{i\in I}$ d'une base topologique du module complet libre M est somme directe (2.1.8) des sous-modules monogènes Ωx_i $(i\in I)$. Ceux-ci sont complets (puisque Ω est supposé complet), et (2.1.15) nous permet de décrire M en tant que somme directe complétée. *Les éléments de* M *s'écrivent univoquement comme sommes des séries*

(2.1.17.1) $$\sum_{i\in I}\lambda_i x_i,$$

où les $(\lambda_i)_{i\in I}$ *sont des éléments de* Ω *tels que*

(2.1.17.2) $$v(\lambda_i)+w(x_i)$$

tende vers l'infini (suivant le filtre des complémentaires des parties finies de I). La filtration de M est définie par la formule

$$w\left(\sum_{i\in I}\lambda_i x_i\right)=\inf_{i\in I}(v(\lambda_i)+w(x_i)). \tag{2.1.17.3}$$

Si N est un Ω-*module filtré complet*, et $(y_i)_{i\in I}$ une famille d'éléments de N vérifiant $w(N;y_i)\geqslant w(M;x_i)$ pour $i\in I$, il existe un morphisme $f:M\to N$, et un seul, tel que $f(x_i)=y_i$ pour $i\in I$. Cette propriété justifie l'expression *complet-libre* (ou, sans abréviation, « libre dans la catégorie des Ω-modules filtrés complets par rapport à la famille d'éléments $(x_i)_{i\in I}$ dont les filtrations $w(x_i)_{i\in I}$ sont données »).

(2.2) Anneaux et modules valués, les foncteurs div et Sat.

(2.2.1) *Définition. — Un anneau valué* Ω est un anneau filtré (2.1.1) qui est *séparé* (2.1.13) et qui vérifie l'axiome suivant :

$$v(\lambda\mu)=v(\lambda)+v(\mu) \qquad \textit{pour tous } \lambda,\mu\in\Omega. \tag{2.2.1.1}$$

Un anneau valué commutatif est *intègre*.

La notion d'anneau valué, que nous venons de définir, ne comporte pas celle de corps valué comme cas particulier. Nous convenons d'appeler *corps valué* un corps muni d'une valuation à valeurs réelles; à cette seule exception près nos valuations seront à valeurs dans $\mathbf{R}_+$.

De même un anneau valué n'est pas un anneau de valuation tel qu'on le définit en Algèbre Commutative. Nous donnons plus loin (2.2.6) la définition des anneaux de valuation que nous utilisons.

(2.2.2) Un Ω-*module valué* sur un anneau valué Ω est un Ω-module filtré M (2.1.3) qui est *séparé* (2.1.13) et qui vérifie l'axiome suivant :

$$w(\lambda x)=v(\lambda)+w(x), \qquad \textit{pour } \lambda\in\Omega \textit{ et } x\in M. \tag{2.2.2.1}$$

Exemple. — Un Ω-module filtré-libre (2.1.16) est valué.

Un *morphisme* $f:M\to M'$ de Ω-modules valués est un morphisme de modules filtrés. Autrement dit, nous définissons la *catégorie* Val(Ω) des Ω-modules valués comme une sous-catégorie pleine de Fil(Ω) (2.1.4).

(2.2.3) Si nous avons, sur un Ω-module M, une famille de valuations w_i, leur *borne inférieure* (2.1.6) est encore une valuation. Un *sous-module* (2.1.5) d'un module valué est valué; une *somme directe* (2.1.8) de modules valués est valuée. Une limite inductive (2.1.8) de modules valués est valuée si et seulement si elle est séparée. Un *complété* d'un module valué est valué.

Par exemple, un Ω-module complet-libre (2.1.17) est valué.

(2.2.4) Si Ω est un anneau valué (2.2.1) commutatif, nous appellerons Ω-*algèbre valuée* une Ω-*algèbre filtrée* (2.1.11), *valuée* en tant que Ω-*module* : il pourrait y avoir équivoque pour les Ω-algèbres associatives qui sont des anneaux. Nous signalerons éventuellement qu'une Ω-algèbre associative valuée est valuée en tant qu'anneau.

Exemple. — Soient M un Ω-module valué et A l'ensemble des *endomorphismes* de M, c'est-à-dire des morphismes de M dans M *au sens de* (2.1.4). L'ensemble A possède une structure naturelle de Ω-algèbre associative. Posons, pour tout $f \in \mathrm{A}$,

(2.2.4.1) $$w(\mathrm{A}; f) = \inf_{x \in \mathrm{M}-\{0\}} (w(\mathrm{M}; f(x)) - w(\mathrm{M}; x)).$$

Nous définissons ainsi une *valuation* de A, qui devient une Ω-algèbre associative valuée (mais non pas valuée en tant qu'anneau, en général).

(2.2.5) *Valuation d'un corps de fractions.* — Soit Ω un anneau valué (2.2.1) commutatif. La valuation de Ω s'étend d'une manière, et d'une seule, au *corps des fractions* K de Ω : pour $\lambda, \mu \in \Omega, \lambda \neq 0$, nous posons $v(\lambda^{-1}\mu) = v(\mu) - v(\lambda)$. Le corps K devient ainsi un *corps valué* (2.2.1). Lorsque Ω n'est pas commutatif, mais possède un corps des fractions à gauche (resp. à droite), une valuation de Ω se prolonge de même à son corps des fractions.

(2.2.6) Nous appellerons ici *anneau de valuation* un anneau valué Ω (2.2.1) qui est *commutatif* et vérifie l'axiome suivant :

(2.2.6.1) *Si λ et λ' sont deux éléments de Ω, tels que $v(\lambda) \geqslant v(\lambda')$, il existe un élément $\mu \in \Omega$ vérifiant* $\lambda = \lambda' \mu$.

Dans un anneau de valuation Ω, les éléments de valuation strictement positive constituent un idéal maximal I dit *idéal de valuation.* Le corps quotient Ω/I est dit *corps résiduel* de Ω.

L'ensemble des éléments de valuation positive dans un corps commutatif valué est un anneau de valuation, dit *anneau des entiers* du corps valué.

(2.2.7) Soit Ω *un anneau valué* (2.2.1) *commutatif.* Nous appellerons *Ω-module divisible* un *Ω-module valué* M (2.2.2) qui possède la propriété suivante.

(2.2.7.1) *Si $\lambda \in \Omega$ et $x \in \mathrm{M}$ avec $v(\lambda) \leqslant w(x)$, il existe $y \in \mathrm{M}$ tel que $\lambda y = x$.*

En particulier, un anneau de valuation (2.2.6) est un anneau commutatif valué Ω qui est divisible en tant que Ω-module. Pratiquement, les anneaux Ω sur lesquels nous considérons des modules divisibles seront des anneaux de valuation.

(2.2.8) *Le foncteur* div. — Soient Ω un anneau *valué commutatif* et M un Ω-module *valué.* Montrons qu'il existe un *Ω-module divisible* M′ (2.2.7) et un *morphisme* $i_{\mathrm{M}} : \mathrm{M} \to \mathrm{M}'$ (2.2.2) possédant la propriété suivante : si $f : \mathrm{M} \to \mathrm{N}$ est un morphisme de M dans un Ω-module *divisible* N, il existe *un morphisme* $g : \mathrm{M}' \to \mathrm{N}$, *et un seul*, tel que $f = g \circ i_{\mathrm{M}}$.

Pour cela construisons le corps des fractions K de Ω (2.2.5), et le produit tensoriel $\mathrm{K} \otimes_{\Omega} \mathrm{M}$. D'après la définition des éléments de K, nous voyons que tout élément de $\mathrm{K} \otimes_{\Omega} \mathrm{M}$ peut s'écrire sous la forme

(2.2.8.1) $$\lambda^{-1} \otimes x, \text{ où } \lambda \in \Omega - \{0\},\ x \in \mathrm{M}.$$

Le nombre $w(M; x)-v(\lambda)$ ne dépend que de $\lambda^{-1}\otimes x$ (et non du choix de λ et x); nous pouvons poser

(2.2.8.2) $$w(\lambda^{-1}\otimes x) = w(M; x) - v(\lambda),$$

puis définir M′ comme *l'ensemble des éléments* $y \in K\otimes_\Omega M$ *pour lesquels* $w(y) \geqslant 0$.

Nous munissons M′ de sa structure naturelle de Ω-module, et nous posons $i_M(x) = 1\otimes x$ pour $x \in M$. Les assertions concernant M′ et i_M sont vérifiées.

Nous noterons désormais div M le module M′ dont nous venons de donner une construction explicite et nous l'appellerons le *divisé* de M. Nous avons d'abord défini div M (à un isomorphisme canonique près) par une propriété universelle : il représente les morphismes de M dans les Ω-modules divisibles, ce qui montre que div est un foncteur covariant appliquant la catégorie des Ω-modules *valués* (2.2.2) dans la sous-catégorie (pleine) des Ω-modules *divisibles*.

Exemples. — Si nous prenons pour M l'anneau Ω lui-même, div Ω s'identifie à *l'anneau des entiers* du corps valué K (2.2.6). Plus généralement, le module div M possède une *structure naturelle de* div Ω*-module*.

Si Ω est un *anneau de valuation* (2.2.6) *complet*, et si M est une Ω-algèbre commutative, valuée en tant qu'anneau, telle que le corps des fractions L de M soit algébrique sur le corps des fractions K de Ω, alors div M est la *clôture intégrale* de M.

(2.2.9) *Propriétés du foncteur* div. — Le morphisme canonique d'un Ω-module valué M dans div M est une *isométrie* (2.1.5), ce qui nous permet de considérer div M comme une *extension valuée de* M.

Si M′ est un Ω-module valué contenant M comme sous-module (pour la filtration induite), les deux propriétés suivantes sont nécessaires et suffisantes pour que M′ s'identifie à div M :

(2.2.9.1) M′ est divisible;

(2.2.9.2) M′/M est un Ω-module de torsion.

Si $f : M \to N$ est une isométrie de Ω-modules valués, le morphisme

$$\operatorname{div} f : \operatorname{div} M \to \operatorname{div} N$$

est encore une isométrie.

Si A est une Ω-algèbre valuée (2.2.4), div A est encore une Ω-algèbre valuée, de même espèce. Si A est une Ω-algèbre associative valuée, et M un A-module filtré et (par restriction des scalaires à Ω) un Ω-module valué, alors div M a une structure de div A-module.

(2.2.10) *Modules saturés.* — Nous disons qu'un module M sur un anneau valué commutatif Ω est *saturé* s'il est *divisible* et *complet*.

L'étude des modules saturés s'appuie sur la proposition suivante :

Le complété $\hat{M}$ *d'un* Ω*-module divisible* M *est saturé.*

Preuve. — Par définition, il s'agit de montrer que le module complet $\hat{M}$ est divisible, c'est-à-dire qu'à tout $\lambda \in \Omega$ et $x \in \hat{M}$ vérifiant $v(\lambda) \leqslant w(x)$ correspond un $y \in \hat{M}$ tel que $\lambda y = x$.

Nous pouvons supposer $\lambda \neq 0$. L'élément x est la limite d'une suite $(x_n)_{n \in \mathbf{N}}$ d'éléments de M et, pour n assez grand, $w(x_n) = w(x)$. Puisque M est divisible il existe, pour ces $n \in \mathbf{N}$, des éléments $y_n \in M$ tels que $x_n = \lambda y_n$, et la suite (y_n) converge vers un élément y de $\hat{M}$, car $w(y_n - y_{n'}) = w(x_n - x_{n'}) - v(\lambda)$ tend vers l'infini avec n et n'. La relation $\lambda y = x$ résulte de $\lambda y_n = x_n$ par passage à la limite.

Remarque. — Le divisé d'un module valué complet peut n'être pas complet.

(2.2.11) *Le foncteur* Sat. — Si M est un module valué sur l'anneau valué commutatif Ω, nous appelons *saturé* de M et notons Sat M le complété (2.1.14) du module div M (2.2.8). Cela définit le foncteur Sat comme composé de « chapeau » et div. Nous pouvons aussi le définir directement :

Le module Sat M est une *extension saturée* du Ω-module valué M, et tout morphisme $f : M \to N$ de M dans un Ω-module *saturé* N *se prolonge* en un *morphisme* g : Sat $M \to N$, *et un seul.*

Si $f : M \to N$ est une isométrie de modules valués, Sat f : Sat M $\to$ Sat N est une isométrie.

Les propriétés concernant les divisées des algèbres, énoncées à la fin de (2.2.9), valent pour les saturées des algèbres.

(2.3) Gradués associés (le foncteur gr).

(2.3.1) *Notations* $\Omega_{\nu+}$, $M_{\nu+}$. — Soit Ω un anneau filtré (2.1.2) (resp. M un Ω-module filtré (2.1.3)). Pour tout $\nu \in \mathbf{R}_+$ nous noterons $\Omega_{\nu+}$ (resp. $M_{\nu+}$) l'ensemble des éléments de Ω (resp. de M) qui vérifient

$$v(\lambda) > \nu \qquad (\text{resp. } w(x) > \nu).$$

(2.3.2) *Définition de* gr Ω. — Partons de l'anneau filtré Ω; pour chaque $\nu \in \mathbf{R}_+$ nous avons deux sous-groupes additifs emboîtés $\Omega_{\nu+} \subset \Omega_\nu$; formons leur quotient $\Omega_\nu / \Omega_{\nu+}$ que nous noterons $\mathrm{gr}_\nu \Omega$, puis la somme directe des $\mathrm{gr}_\nu \Omega$ (pour $\nu \in \mathbf{R}_+$) que nous noterons gr Ω :

(2.3.2.1)
$$\mathrm{gr}\,\Omega = \coprod_{\nu \in \mathbf{R}_+} \mathrm{gr}_\nu \Omega.$$

Si $\lambda \in \Omega_\nu$, $\mu \in \Omega_{\nu'}$, alors $\lambda\mu \in \Omega_{\nu+\nu'}$, et l'image de $\lambda\mu$ dans $\mathrm{gr}_{\nu+\nu'}\Omega$ ne dépend que des images respectives de λ et μ dans $\mathrm{gr}_\nu \Omega$ et $\mathrm{gr}_{\nu'}\Omega$.

Cela définit sur le groupe additif gradué gr Ω une multiplication des éléments homogènes. Nous prolongeons cette multiplication par linéarité pour obtenir enfin l'*anneau gradué* gr Ω *associé* à l'anneau filtré Ω : cf. [3], chap. III, § 2, n° 3.

(2.3.3) *Définition de* gr M. — Soit M un module filtré sur l'anneau filtré Ω. Formons, pour chaque $\nu \in \mathbf{R}_+$, le groupe additif quotient $M_\nu / M_{\nu+}$ que nous notons $\mathrm{gr}_\nu M$, puis la somme directe gr M :

(2.3.3.1)
$$\mathrm{gr}\,M = \coprod_{\nu \in \mathbf{R}_+} M_\nu / M_{\nu+}.$$

Nous définissons la structure de gr Ω-module (gradué) sur gr M, par restriction, passage au quotient, et prolongement par linéarité (cf. [3], *loc. cit.*).

(2.3.4) *Termes dominants et représentants.* — Si ξ est un élément *homogène* de gr M, c'est-à-dire un élément d'un $\mathrm{gr}_\nu \mathrm{M} = \mathrm{M}_\nu/\mathrm{M}_{\nu^+}$, nous appelons *représentant* de ξ (dans M) un élément de M_ν dont la classe mod M_{ν^+} est ξ.

Si x est un élément de M dont la *filtration* $w(x) = \nu$ est *finie*, nous appelons *terme dominant* de x son image canonique dans $\mathrm{gr}_\nu \mathrm{M}$. Ainsi un terme dominant n'est jamais nul.

Les mêmes définitions vaudront pour un anneau filtré Ω et son gradué associé gr Ω.

Un élément de *filtration finie* d'un module (ou anneau) filtré est un représentant de son terme dominant. Un élément *homogène non nul* d'un gradué associé est le terme dominant d'un quelconque de ses représentants.

(2.3.5) *Le foncteur* gr. — Si Ω est un anneau filtré, et $f : \mathrm{M} \to \mathrm{N}$ un morphisme de Ω-modules filtrés (2.1.4), la restriction de f applique M_ν dans N_ν pour chaque $\nu \in \mathbf{R}_+$ et définit, par passage au quotient, une application additive de $\mathrm{gr}_\nu \mathrm{M}$ dans $\mathrm{gr}_\nu \mathrm{N}$. La somme directe de ces applications est une application

$$\mathrm{gr} f : \mathrm{gr}\,\mathrm{M} \to \mathrm{gr}\,\mathrm{N} \tag{2.3.5.1}$$

dont nous vérifions qu'elle est un morphisme de gr Ω-modules gradués (1.1.2).

Cela achève la définition du *foncteur covariant* gr, qui envoie la catégorie $\mathrm{Fil}(\Omega)$ des Ω-modules filtrés (2.1.4) dans la catégorie $\mathrm{Gr}(\mathrm{gr}\,\Omega)$ des gr Ω-modules (gradués).

(2.3.6) *Traductions.* — L'utilisation du foncteur gr permet de traduire certaines définitions antérieures. La *filtration* de Ω (resp. de M) est *discrète* (2.1.12) si et seulement si la *graduation* de gr Ω (resp. de gr M) est discrète (1.1.3). Une *isométrie* f de Ω-modules filtrés est un morphisme dans $\mathrm{Fil}(\Omega)$ tel que gr f *et* f soient *injectifs*; il suffit de supposer gr f injectif si le module de départ est séparé. Pour qu'un anneau filtré Ω soit *valué*, il faut et il suffit qu'il soit *séparé* et que gr Ω soit *sans diviseurs de zéro.* Pour qu'un module filtré M sur un anneau valué Ω soit *valué*, il faut et il suffit que M soit *séparé* et que gr M soit un gr Ω-module *sans torsion.*

(2.3.7) *Sommes directes et complétés.* — Si $\mathrm{M} = \coprod_{i \in \mathrm{I}} \mathrm{M}^{(i)}$ est une somme directe de Ω-modules filtrés (2.1.8), le morphisme canonique

$$\coprod_{i \in \mathrm{I}} \mathrm{gr}\,\mathrm{M}^{(i)} \to \mathrm{gr}\,\mathrm{M} \tag{2.3.7.1}$$

est un isomorphisme. Autrement dit le *foncteur* gr *permute aux sommes directes.*

Si M est un Ω-module filtré séparé, et $\hat{\mathrm{M}}$ son complété, le morphisme canonique

$$\mathrm{gr}\,\mathrm{M} \to \mathrm{gr}\,\hat{\mathrm{M}} \tag{2.3.7.2}$$

est bijectif. *La complétion d'un module (ou d'un anneau) laisse invariant son gradué associé.*

(2.3.8) *Suites exactes, limites inductives.* — Soient Ω un anneau filtré et

$$0 \to \mathrm{M}' \to \mathrm{M} \to \mathrm{M}'' \to 0 \tag{2.3.8.1}$$

une suite exacte de Ω-modules. Nous supposons M *filtré*, et nous munissons M' de la *filtration induite* (2.1.5) et M'' de la *filtration quotient* (2.1.7). Si nous appliquons le foncteur gr, nous obtenons une *suite exacte* dans $\mathrm{Gr}(\mathrm{gr}\,\Omega)$:

(2.3.8.2) $$0 \to \mathrm{gr}\,M' \to \mathrm{gr}\,M \to \mathrm{gr}\,M''.$$

Si la filtration de M est discrète, le morphisme $\mathrm{gr}\,M \to \mathrm{gr}\,M''$ est surjectif : [3], chap. III, § 2, n° 4, prop. 2. Si la filtration de M n'est pas discrète, il se peut que $\mathrm{gr}\,M \to \mathrm{gr}\,M''$ ne soit pas surjectif : cf. (2.1.12).

Soient maintenant $(M^{(i)})_{i\in I}$ une famille de Ω-modules filtrés, indexée par un ensemble ordonné filtrant I, et $f_{ji} : M^{(i)} \to M^{(j)}$ $(i, j \in I, i \leqslant j)$ les morphismes permettant de construire la *limite inductive* $M = \varinjlim M^{(i)}$.

Les morphismes $f_i : M^{(i)} \to M$ définissent (en appliquant les foncteurs « ν en indice », « ν^+ en indice » et gr) des morphismes

(2.3.8.3) $$\varinjlim M^{(i)}_\nu \to M_\nu;$$

(2.3.8.4) $$\varinjlim M^{(i)}_{\nu^+} \to M_{\nu^+};$$

(2.3.8.5) $$\varinjlim \mathrm{gr}\,M^{(i)} \to \mathrm{gr}\,M.$$

Si nous appliquons la construction explicite d'une limite inductive filtrée (2.1.8), nous voyons que le morphisme (2.3.8.3) est *injectif*, et (2.3.8.4) *bijectif*. Appliquons maintenant le foncteur *exact* $\varinjlim$ aux suites exactes

$$0 \to M^{(i)}_{\nu^+} \to M^{(i)}_\nu \to \mathrm{gr}_\nu M^{(i)} \to 0.$$

Nous obtenons les suites exactes

$$0 \to \varinjlim M^{(i)}_{\nu^+} \to \varinjlim M^{(i)}_\nu \to \varinjlim \mathrm{gr}_\nu M^{(i)} \to 0.$$

Compte tenu des propriétés de (2.3.8.3) et (2.3.8.4), nous en déduisons que (2.3.8.5) est un morphisme *injectif*.

(2.3.9) Lorsque les filtrations sont à valeurs entières, ou, plus généralement, lorsque la filtration de $\coprod_{i\in I} M^{(i)}$ est *discrète*, les morphismes (2.3.8.3) et (2.3.8.5) sont *bijectifs*, et, dans ce cas, nous pouvons dire que le foncteur gr permute aux limites inductives.

Nous rencontrerons un autre cas particulier important. N'imposons aucune condition supplémentaire aux filtrations, mais supposons que les morphismes f_{ji} soient tous des *isométries* (2.1.5). Aux abus de langage près, cela veut dire que la limite inductive est une réunion. Dans ce cas les morphismes (2.3.8.3) et (2.3.8.5) sont bijectifs, et gr M est la limite inductive (ou réunion) des $\mathrm{gr}\,M^{(i)}$. Plus particulièrement, si Ω est *valué* (2.2.1) et si les f_{ji} sont des *isométries* de Ω-modules *valués* (2.2.2), alors $M = \varinjlim M^{(i)}$ est un Ω-module *valué* qui peut être considéré comme la réunion des $M^{(i)}$.

(2.3.10) *Produits tensoriels : un morphisme fonctoriel.* — Soient Ω un anneau filtré, M et M' deux Ω-modules filtrés dont nous puissions construire le produit tensoriel filtré $M'' = M \otimes_\Omega M'$ (2.1.9).

Prenons deux éléments $\xi \in \mathrm{gr}\,M$ et $\eta \in \mathrm{gr}\,M'$, homogènes de degrés respectifs ν et ν'. Choisissons des représentants (2.3.4) x et y de ξ et η dans M et M'. L'image de $x \otimes y \in M''$ dans $\mathrm{gr}_{\nu+\nu'}M''$ ne dépend que de ξ et η. Nous venons de définir une application du produit $\mathrm{gr}_\nu M \times \mathrm{gr}_{\nu'} M'$ dans $\mathrm{gr}_{\nu+\nu'}M''$. Nous vérifions que cette application définit un *morphisme* :

(2.3.10.1) $$\mathrm{gr}\,M \otimes_{\mathrm{gr}\,\Omega} \mathrm{gr}\,M' \to \mathrm{gr}(M \otimes_\Omega M').$$

Précisons que (2.3.10.1) est un *morphisme* de gr Ω-*modules* gradués (1.1.4), (1.1.7) si Ω est commutatif, ou un morphisme de *groupes additifs gradués* si Ω n'est pas commutatif (nous supposons alors que M est un module à droite). Le morphisme (2.3.10.1) est un *morphisme fonctoriel* (les modules $\mathrm{gr}\,M \otimes_{\mathrm{gr}\,\Omega} \mathrm{gr}\,M'$ et $\mathrm{gr}(M \otimes_\Omega M')$ sont des bifoncteurs covariants en M et M').

Lorsque les filtrations de M et M' sont *discrètes*, le morphisme (2.3.10.1) est *surjectif* : cela résulte de la construction explicite du produit tensoriel filtré (2.1.9).

(2.3.11) *Gradué associé d'une algèbre.* — Soient Ω un anneau filtré commutatif et A une Ω-algèbre filtrée (2.1.11). Alors le gr Ω-module gr A possède une structure naturelle de gr Ω-*algèbre* (de même espèce que A). Cette structure peut se définir directement comme en (2.3.2), ou à partir du morphisme fonctoriel (2.3.10). En effet la multiplication dans A est définie par un morphisme dans $\mathrm{Fil}(\Omega)$:

(2.3.11.1) $$A \otimes_\Omega A \to A;$$

si nous lui appliquons le foncteur gr, nous obtenons un morphisme dans $\mathrm{Gr}(\mathrm{gr}\,\Omega)$:

(2.3.11.2) $$\mathrm{gr}(A \otimes_\Omega A) \to \mathrm{gr}\,A,$$

et si nous composons ce dernier avec le morphisme fonctoriel

(2.3.11.3) $$\mathrm{gr}\,A \otimes_{\mathrm{gr}\,\Omega} \mathrm{gr}\,A \to \mathrm{gr}(A \otimes_\Omega A),$$

nous obtenons la multiplication dans gr A.

(2.3.12) *Traduction.* — Soient Ω un anneau filtré séparé, $(x_i)_{i \in I}$ une famille d'éléments de filtrations finies dans un Ω-module filtré M, et $(\xi_i)_{i \in I}$ les termes dominants (2.3.4) des (x_i). Les deux assertions suivantes sont équivalentes.

La famille $(x_i)_{i \in I}$ *est filtrée-libre dans* M (2.1.16).

La famille $(\xi_i)_{i \in I}$ *est libre dans* gr M, *sur* gr Ω.

(2.3.13) *Proposition.* — *Soit* $f : M \to M'$ *un morphisme de* Ω-*modules filtrés* (2.1.4). *Si la filtration de* M' *est séparée et discrète, et si* $\mathrm{gr} f : \mathrm{gr}\,M \to \mathrm{gr}\,M'$ *est surjectif, alors* $f(M)$ *est dense dans* M'. *Si, de plus,* M *est complet, alors* f *est surjectif et* M' *est complet.*

Preuve (cf. [3], chap. III, § 2, nº 8). — Soient $\nu_0 < \nu_1 < \dots$ les différentes valeurs des filtrations des éléments de M'. Pour tout $x \in M'$, avec $w(M'; x) = \nu_i$, la surjectivité de $\mathrm{gr} f$ implique l'existence d'un $y \in M$ avec $w(M; y) = \nu_i$ et $w(M'; x - f(y)) > \nu_i$, c'est-à-dire $w(M'; x - f(y)) \geqslant \nu_{i+1}$. Par récurrence sur $j \geqslant 1$, nous voyons l'existence d'éléments $y_j \in M$ vérifiant $w(M'; x - f(y_j)) \geqslant \nu_{i+j}$, ce qui prouve que $f(M)$ est dense dans M'.

De plus, nous pouvons vérifier les conditions $w(\mathrm{M}; y_j) = \nu_i$ et $w(\mathrm{M}; y_j - y_{j+1}) \geqslant \nu_{i+j}$. La suite (y_j) est alors une suite de Cauchy dans M; si M est complet, elle converge vers $y \in \mathrm{M}, f(y) = x$ et f est surjectif. Nous voyons ensuite qu'une suite de Cauchy dans M′ est l'image d'une suite de Cauchy dans M, ce qui prouve que M′ est complet.

(2.3.14) *Corollaire. — Si* M *est filtré complet, si la filtration de* M′ *est séparée et discrète, alors tout morphisme* $f : \mathrm{M} \to \mathrm{M}'$, *dont le gradué associé* $\mathrm{gr} f$ *est bijectif, est un isomorphisme.*

(2.3.15) *Corollaire. — Si* N *et* N′ *sont deux sous-modules fermés d'un module filtré séparé* M, *de filtration discrète, si* $\mathrm{N} \subset \mathrm{N}'$ *et enfin si* $\mathrm{gr}\, \mathrm{N} = \mathrm{gr}\, \mathrm{N}'$ (en identifiant gr N et gr N′ à des sous-modules de gr M, d'après (2.3.8)), *alors* $\mathrm{N} = \mathrm{N}'$.

(2.3.16) *Corollaire. — Soit* M *un module filtré séparé de filtration discrète. Si les éléments d'une partie* X *de* M *ont pour termes dominants une famille de générateurs de* gr M, *alors* X *engendre dans* M *un sous-module dense.*

(2.3.17) *Théorème. — Soient* Ω *un anneau filtré complet et* N *un* Ω*-module filtré complet. Si la filtration de* M *est discrète, et si* gr M *est un* gr Ω*-module libre* (1.1.6), *alors* M *est complet-libre* (2.1.17) *et toute famille de représentants* (2.3.4) *d'une base de* gr M *est une base topologique* (2.1.17) *de* M.

Preuve. — Soit $(x_i)_{i \in \mathrm{I}}$ une famille d'éléments de M dont les termes dominants $(\xi_i)_{i \in \mathrm{I}}$ constituent une base de gr M. La famille (x_i) est donc filtrée-libre dans M (2.3.12) et engendre un sous-module dense du module complet M (2.3.16), ce qui prouve notre assertion.

3. MODULES VALUÉS SUR UN ANNEAU DE VALUATION DISCRÈTE COMPLET Ω

(3.1) Modules valués de type fini; modules complets-libres.

(3.1.1) *Notation.* — Jusqu'à la fin de ce chapitre (à l'exception des n^os (3.3.1) à (3.3.6)), nous désignerons par Ω *un anneau de valuation discrète complet* (cf. [25], première partie). L'anneau Ω est donc un anneau de valuation (2.2.6), sa filtration est discrète (2.1.13) et il est complet (2.1.15). Si ϖ est une *uniformisante* de Ω, c'est-à-dire un élément de valuation strictement positive minima, tout élément $x \in \Omega$ s'écrit univoquement sous la forme $\varpi^n . u$, où $n = v(x)/v(\varpi) \in \mathbf{N}$ et $u \in \Omega$ est une unité. Les idéaux de Ω sont engendrés par les puissances de ϖ.

Nous nous intéresserons surtout, par la suite, au cas d'inégale caractéristique. Le corps résiduel k de Ω est alors de caractéristique $p > 0$, tandis que le corps des fractions de Ω est de caractéristique 0. La valuation v est déterminée à un facteur multiplicatif près par la donnée de Ω (en tant qu'anneau). Nous la déterminons complètement par la condition :

(3.1.1.1) $$v(p) = 1.$$

Si e désigne l'indice de ramification absolue de Ω, la valuation d'une uniformisante de Ω est alors e^{-1}.

(3.1.2) *Structure de* $\Gamma = \mathrm{gr}\,\Omega$. — Nous notons Γ le gradué associé de Ω. La composante homogène Γ_0 est le *corps résiduel* k de Ω. Choisissons une fois pour toutes une uniformisante ϖ de Ω, et notons π *le terme dominant* de ϖ (2.3.4). Le degré de π est égal à $v(\varpi)$, qui n'est pas nécessairement égal à 1. L'anneau gradué Γ s'identifie à l'*anneau de polynômes* $k[\pi]$: cf. [3], chap. III, § 2, n° 3, exemple 1. Les considérations de (1.2) vont donc s'appliquer aux gradués associés des Ω-modules filtrés, et surtout aux Ω-*modules valués* (2.2.2) pour lesquels le gradué associé est un Γ-module sans torsion (2.3.6).

(3.1.3) *Proposition. — Un Ω-module valué complet* M, *de valuation discrète, est complet-libre, et les bases topologiques de* M *sont les familles de représentants des bases de* gr M *sur* Γ.

Preuve. — C'est une conséquence des théorèmes (1.2.3) et (2.3.17).

(3.1.4) *Théorème. — Un Ω-module valué de type fini (c'est-à-dire engendré, en tant que module, par une partie finie) est filtré-libre* (2.1.16).

Preuve. — Soit M un Ω-module valué de type fini. Alors gr M est un Γ-module libre. Prenons des représentants $(x_i)_{i\in \mathrm{I}}$ d'une base de gr M. Nous obtenons une famille filtrée-libre dans M (2.3.12), et *a fortiori* une famille libre sur Ω. Or le cardinal d'une famille libre dans M ne peut dépasser celui d'une famille de générateurs de M (d'après l'algèbre linéaire élémentaire). Le module gr M est donc de rang fini; sa graduation est donc discrète (1.1.3), ainsi que la filtration de M (2.3.6). Le Ω-module filtré-libre engendré par les $(x_i)_{i\in \mathrm{I}}$ (auxquels nous donnons les filtrations $w(\mathrm{M}; x_i)$) est complet, puisque Ω est complet et I fini. Le corollaire (2.3.14) permet d'achever la démonstration.

(3.1.5) *Critère de compacité. — Soit* M *un Ω-module valué, complet, non nul. Pour que* M *soit compact, il faut et il suffit que les trois conditions suivantes soient vérifiées :*

(3.1.5.1) Ω *est compact.*

(3.1.5.2) *La filtration de* M *est discrète.*

(3.1.5.3) *Si* $(x_i)_{i\in \mathrm{I}}$ *est une base topologique de* M, $w(x_i)$ *tend vers* $+\infty$ *(suivant le filtre des complémentaires des parties finies de* I).

Preuve. — Supposons d'abord les trois conditions vérifiées. Alors M est complet-libre (3.1.3), et la condition (3.1.5.3) montre que M s'identifie, en tant que module topologique, au module *produit* Ω^{I} (2.1.17), qui est compact puisque Ω est compact.

Supposons maintenant M compact. Prenons $x\in \mathrm{M}$, $x \neq 0$ (nous avons supposé M non nul). L'application $\lambda \to \lambda x$ est, à une translation près, une isométrie de Ω dans M, donc un homéomorphisme. L'image Ωx de Ω est complète (car Ω est complet), donc fermée, donc compacte, ce qui prouve (3.1.5.1). Le module M s'identifie à $\varprojlim \mathrm{M}/\mathrm{M}_\nu$ (2.1.14) et les quotients $\mathrm{M}/\mathrm{M}_\nu$ sont discrets et compacts, c'est-à-dire *finis*, ce qui entraîne (3.1.5.2) et (3.1.5.3).

(3.1.6) *Divisé d'un Ω-module filtré-libre. — Soit* M *un Ω-module filtré-libre pour la base* $(x_i)_{i\in \mathrm{I}}$ (2.1.16). *Posons*

$$w(\mathrm{M}; x_i) = \tau_i \qquad \textit{et} \qquad v(\varpi) = e^{-1} \qquad (\varpi \textit{ uniformisante de } \Omega).$$

Le module div M *(considéré comme extension de* M) *est filtré-libre pour la base* $(y_i)_{i\in \mathrm{I}}$, *avec*

(3.1.6.1) $$w(\operatorname{div} \mathrm{M}; y_i) = \tau_i - n_i e^{-1},$$

(3.1.6.2) $$n_i = [\tau_i e] \qquad ([\nu] \text{ désignant la partie entière de } \nu \in \mathbf{R})$$

(3.1.6.3) $$x_i = \varpi^{n_i} y_i.$$

Preuve. — D'après la définition (2.2.7), les éléments $x_i \in \operatorname{div} \mathrm{M}$ sont divisibles respectivement par ϖ^{n_i} dans div M, car $v(\varpi^{n_i}) \leqslant w(x_i)$, ce qui établit l'existence des y_i. De plus les y_i vérifient

(3.1.6.4) $$0 \leqslant w(\operatorname{div} \mathrm{M}; y_i) < e^{-1} = v(\varpi).$$

L'hypothèse que $(x_i)_{i\in \mathrm{I}}$ est une famille filtrée-libre et les relations (3.1.6.3) impliquent que $(y_i)_{i\in \mathrm{I}}$ est filtrée-libre dans le Ω-module valué div M. La relation (3.1.6.4) montre que le module engendré par les y_i est divisible, c'est-à-dire coïncide avec div M.

Cette démonstration vaut pour un anneau de valuation discrète, non nécessairement complet.

(3.1.7) *Saturé d'un module filtré-libre ou complet-libre.*

Soit M *un* Ω*-module filtré-libre (resp. complet-libre) pour la base filtrée (resp. base topologique)* $(x_i)_{i\in \mathrm{I}}$. *Avec les notations de* (3.1.6), *le module* Sat M *est complet-libre, et possède comme base topologique la famille* $(y_i)_{i\in \mathrm{I}}$ *caractérisée par les relations* (3.1.6.1), (3.1.6.2) et (3.1.6.3).

Preuve. — C'est une conséquence de (3.1.6) et de la définition du saturé (2.2.11).

(3.1.8) *Lemme.* — *Soit* M *un* Ω*-module valué, engendré (en tant que module) par une famille d'éléments* $(x_i)_{i\in \mathrm{I}}$ *dont les valuations tendent vers l'infini. Alors la filtration de* M *est discrète.*

Preuve. — Soit $\nu \in \mathbf{R}_+$. Nous devons montrer que les éléments de M ne peuvent avoir qu'un nombre fini de valuations $\leqslant \nu$. Soit $\mathrm{J} \subset \mathrm{I}$ l'ensemble des i pour lesquels $w(x_i) \leqslant \nu$.

Tout élément de M est donc congru, mod M_{ν^+}, à un élément du sous-module engendré par les x_i, $i \in \mathrm{J}$. Par hypothèse J est fini, et ce sous-module est donc de filtration discrète, d'après le théorème (3.1.4), ce qui prouve le lemme.

(3.1.9) *Proposition.* — *Soit* M *un* Ω*-module saturé* (2.2.10) *engendré (en tant que module saturé) par une famille dénombrable* $(x_n)_{n\in \mathbf{N}}$. *Alors* M *possède une base topologique.*

Preuve. — Posons $y_n = \varpi^n x_n$. Les valuations des y_n tendent vers l'infini, et le sous-module engendré par les y_n est donc de filtration discrète (3.1.8). L'adhérence M′ de ce sous-module dans M est complète, donc complète-libre d'après (3.1.3). Comme M est le module saturé de M′, nous appliquons (3.1.7) pour obtenir une base topologique de M.

Bien entendu la filtration de M n'est pas nécessairement discrète.

(3.1.10) *Corollaire.* — *Soit* A *une* Ω*-algèbre saturée, engendrée (en tant que* Ω*-algèbre saturée) par une famille dénombrable. Alors* A *possède une base topologique.*

Preuve. — *L'algèbre* A *est engendrée, en tant que* Ω*-module saturé,* par les *monômes* en les générateurs. Ces monômes forment encore une famille dénombrable, ce qui nous ramène à (3.1.9).

(3.2) Le produit tensoriel dans la catégorie $\mathrm{Val}(\Omega)$.

(3.2.1) *Théorème.* — *Soient* M *et* M' *deux* Ω*-modules valués, et* $M''=M\otimes_\Omega M'$ *leur produit tensoriel filtré* (2.1.9). *Alors :*

(3.2.1.1) *Le* Ω*-module* M'' *est valué.*

(3.2.1.2) *Pour tout* $\nu\in\mathbf{R}_+$, *le sous-module* M''_ν (2.1.3) *est engendré par les éléments* $x\otimes y$, *où* $x\in M$, $y\in M'$, $w(M;x)+w(M';y)\geqslant\nu$.

(3.2.1.3) *Le morphisme fonctoriel* $\mathrm{gr}\,M\otimes_\Gamma \mathrm{gr}\,M'\to \mathrm{gr}\,M''$ (2.3.10) *est bijectif.*

(3.2.1.4) *Soient* N, N' *deux* Ω*-modules valués, et* $f:N\to M, f':N'\to M'$ *deux isométries. Alors le morphisme* $f\otimes f':N\otimes_\Omega N'\to M\otimes_\Omega M'$ *est encore une isométrie.*

(3.2.1.5) *Pour tous* $x\in M$, $y\in M'$, *nous avons* $w(M'';x\otimes y)=w(M;x)+w(M';y)$.

(3.2.1.6) *Si* $(x_i)_{i\in I}$ *et* $(y_j)_{j\in J}$ *sont des familles filtrées-libres dans* M *et* M' *respectivement, alors*

$$(x_i\otimes y_j)_{(i,j)\in I\times J}$$

est filtrée-libre dans M''.

Preuve :

(3.2.2) Supposons d'abord M et M' de type fini. D'après le théorème (3.1.4), M et M' sont alors filtrés-libres, pour les bases respectives $(x_i)_{i\in I}$ et $(y_j)_{j\in J}$. Nous posons

$$w(M;x_i)=\tau_i \qquad \text{et} \qquad w(M';y_j)=\theta_j.$$

Le produit tensoriel M'' est libre pour la base $(x_i\otimes y_j)_{(i,j)\in I\times J}$. Si nous appliquons la définition (2.1.9) du produit tensoriel filtré, nous voyons que M'' est filtré-libre pour la base en question avec

$$w(M'';x_i\otimes y_j)=\tau_i+\theta_j. \tag{3.2.2.1}$$

Comme un module filtré-libre est valué, (3.2.1.1) est démontré. Nous vérifions de même (3.2.1.2).

Les Γ-modules gr M et gr M' sont libres, avec des bases $(\xi_i)_{i\in I}$ et $(\eta_j)_{j\in J}$ formées des termes dominants (2.3.4) des (x_i) et des (y_j) respectivement. Le produit tensoriel $\mathrm{gr}\,M\otimes \mathrm{gr}\,M'$ possède alors la base $(\xi_i\otimes\eta_j)_{(i,j)\in I\times J}$, avec $\deg(\xi_i\otimes\eta_j)=\tau_i+\theta_j$, d'après (1.1.8). Si nous appliquons la définition (2.3.10) du morphisme fonctoriel

$$\mathrm{gr}\,M\otimes \mathrm{gr}\,M'\to \mathrm{gr}\,M'', \tag{3.2.2.2}$$

nous voyons que $\xi_i\otimes\eta_j\in \mathrm{gr}\,M\otimes\mathrm{gr}\,M'$ a pour image le terme dominant de $x_i\otimes y_j\in M''$. Ce morphisme est donc bijectif, ce qui prouve (3.2.1.3).

(3.2.3) Démontrons maintenant (3.2.1.4), en supposant toujours M et M' de type fini. Alors N et N' sont aussi de type fini (puisque Ω est noethérien). Les morphismes $\mathrm{gr} f : \mathrm{gr}\, N \to \mathrm{gr}\, M$ et $\mathrm{gr} f' : \mathrm{gr}\, N' \to \mathrm{gr}\, M'$ sont *injectifs*, ainsi que leur produit tensoriel

(3.2.3.1) $$\mathrm{gr} f \otimes \mathrm{gr} f' : \mathrm{gr}\, N \otimes_\Gamma \mathrm{gr}\, N' \to \mathrm{gr}\, M \otimes_\Gamma \mathrm{gr}\, M',$$

d'après le corollaire (1.2.6).

Par définition d'un morphisme fonctoriel, nous avons le diagramme commutatif

(3.2.3.2)
$$\begin{array}{ccc} \mathrm{gr}\, N \otimes_\Gamma \mathrm{gr}\, N' & \xrightarrow[\mathrm{gr} f \otimes \mathrm{gr} f']{} & \mathrm{gr}\, M \otimes_\Gamma \mathrm{gr}\, M' \\ \downarrow & & \downarrow \\ \mathrm{gr}(N \otimes_\Omega N') & \xrightarrow[\mathrm{gr}(f \otimes f')]{} & \mathrm{gr}(M \otimes_\Omega M') \end{array}$$

Les flèches verticales sont des bijections d'après (3.2.1.3), et $\mathrm{gr} f \otimes \mathrm{gr} f'$ est injectif. Par conséquent $\mathrm{gr}(f \otimes f')$ est injectif, ce qui prouve (3.2.1.4) dans le cas particulier considéré.

(3.2.4) Passons maintenant au cas général. Nous considérons M et M′ comme les réunions, ou limites inductives de leurs sous-modules de type fini. Comme le produit tensoriel filtré permute aux limites inductives (2.1.10), le module filtré M″ est limite inductive des produits tensoriels filtrés des sous-modules de type fini de M et M′. Mais *les morphismes définissant cette limite inductive sont des isométries*, d'après le cas particulier de (3.2.1.4) déjà prouvé. Cette limite inductive est donc, par abus de langage, une simple réunion de modules valués (2.3.9), ce qui démontre généralement (3.2.1.1). Les propriétés (3.2.1.2) à (3.2.1.4) s'obtiennent de même, par passage aux limites inductives, à partir des modules de type fini. Quant à (3.2.1.5) et (3.2.1.6), ce sont des cas particuliers de (3.2.1.4), après qu'on a explicité la valuation d'un produit tensoriel de modules filtrés-libres (3.2.2).

(3.2.5) *Remarques.* — Le théorème (3.2.1) signifie que le produit tensoriel filtré est défini dans la catégorie $\mathrm{Val}(\Omega)$, et qu'il possède des propriétés très analogues à celles du produit tensoriel d'espaces vectoriels.

Signalons cependant que le théorème des bases adaptées n'est pas valable dans $\mathrm{Val}(\Omega)$, même si l'on se restreint aux modules de type fini. Soient, par exemple $\Omega = \mathbf{Z}_p$, M le module filtré-libre de base $\{x, y\}$ avec $w(x) = 0$ et $w(y) = 2$, et enfin N le sous-module de M engendré par $z = px + y$. Les modules M et N n'ont pas de bases filtrées adaptées.

(3.2.6) *Produit tensoriel complété.* — Soient M et M′ deux Ω-modules valués. Nous appellerons *produit tensoriel complété* de M et M′, et nous noterons

(3.2.6.1) $$M \hat{\otimes}_\Omega M'$$

le *complété du produit tensoriel valué* $M \otimes_\Omega M$.

A partir des isométries canoniques (ou inclusions) $M \to \hat{M}$ et $M' \to \hat{M}'$, nous obtenons (3.2.1.4) une isométrie de Ω-modules valués :

(3.2.6.2) $$M \otimes_\Omega M' \to \hat{M} \otimes_\Omega \hat{M}',$$

et l'image de $M \otimes M'$ est dense dans $\hat{M} \otimes \hat{M}'$, ce qui prouve que le morphisme

(3.2.6.3) $$M \hat{\otimes} M' \to \hat{M} \hat{\otimes} \hat{M}'$$

est un isomorphisme de modules valués complets.

Nous démontrons de même, à partir de l'associativité du produit tensoriel filtré (2.1.10), l'*associativité du produit tensoriel complété* : les modules $(M \hat{\otimes} M') \hat{\otimes} M''$ et $M \hat{\otimes} (M' \hat{\otimes} M'')$ s'identifient tous deux au *complété du module* $M \otimes M' \otimes M''$.

Si les modules M et M′ sont filtrés-libres (ou complets libres) pour les bases (ou bases topologiques) respectives $(x_i)_{i \in I}$ et $(y_j)_{j \in J}$, alors $M \hat{\otimes} M'$ est *complet-libre* pour la base topologique $(x_i \otimes y_j)_{(i,j) \in I \times J}$.

(3.2.7) *Produit tensoriel divisé.* — Le produit tensoriel divisé de deux Ω-modules valués M et M′ est le *divisé* (2.2.8) *de leur produit tensoriel*, c'est-à-dire $\operatorname{div}(M \otimes_\Omega M')$. Les isométries (ou inclusions) $M \to \operatorname{div} M$ et $M' \to \operatorname{div} M'$ donnent (3.2.1.4) une isométrie

(3.2.7.1) $$M \otimes M' \to \operatorname{div} M \otimes \operatorname{div} M',$$

le quotient de $\operatorname{div} M \otimes \operatorname{div} M'$ par l'image de $M \otimes M'$ est un Ω-module de torsion, ce qui prouve (2.2.9) que le morphisme

(3.2.7.2) $$\operatorname{div}(M \otimes M') \to \operatorname{div}(\operatorname{div} M \otimes \operatorname{div} M')$$

est un isomorphisme.

Un exemple où M et M′ sont filtrés-libres montre que $\operatorname{div} M \otimes \operatorname{div} M'$ n'est pas nécessairement divisible. Le produit tensoriel divisé est associatif.

(3.2.8) *Produit tensoriel saturé.* — *Le produit tensoriel saturé* de deux Ω-modules valués M et M′ est le saturé (2.2.11) de leur produit tensoriel, c'est-à-dire $\operatorname{Sat}(M \otimes_\Omega M')$. Comme précédemment (3.2.6) et (3.2.7), nous voyons que les isométries $M \to \operatorname{Sat} M$ et $M' \to \operatorname{Sat} M'$ déterminent un *isomorphisme*

$$\operatorname{Sat}(M \otimes M') \to \operatorname{Sat}(\operatorname{Sat} M \otimes \operatorname{Sat} M').$$

Le produit tensoriel saturé est associatif.

Si A et B sont deux Ω-algèbres valuées associatives (resp. supplémentées), leur produit tensoriel $A \otimes_\Omega B$ est encore une Ω-algèbre associative (resp. supplémentée), ainsi que $A \hat{\otimes} B$, $\operatorname{div}(A \otimes B)$ et $\operatorname{Sat}(A \otimes B)$.

(3.2.9) *Modules linéairement topologisés et produits tensoriels.* — Désignons de nouveau par Ω un anneau commutatif quelconque. Nous appelons Ω-*module linéairement topologisé* un Ω-module topologique M dont *les sous-modules ouverts constituent un système fondamental de voisinages de zéro.* Un tel module n'est pas nécessairement séparé; le module séparé associé à M est $M/(\bigcap_i A_i)$, A_i parcourant l'ensemble des sous-modules ouverts. Le module *séparé-complété* associé à M est la *limite projective* $\hat{M} = \varprojlim(M/A_i)$, les sous-modules ouverts A_i étant ordonnés par anti-inclusion. Si $f : M \to M'$ est une application Ω-linéaire continue, il lui correspond une application $\hat{f} : \hat{M} \to \hat{M}'$, ce qui définit le foncteur « séparé-complété ».

Soient M et N deux Ω-modules linéairement topologisés. Nous définissons une structure de module linéairement topologisé sur le produit tensoriel $M \otimes_\Omega N$ en prenant dans celui-ci un système fondamental de voisinages de zéro formé des sous-modules

(3.2.9.1) $$\mathrm{Im}(A_i \otimes N) + \mathrm{Im}(M \otimes B_j),$$

où A_i, B_j parcourent les ensembles des sous-modules ouverts de M et N (« Im » désigne l'image par l'application canonique). Le Ω-module linéairement topologisé $M \otimes N$ sera dit *produit tensoriel topologique* de M et de N.

Le produit tensoriel topologique est associatif et commutatif (au même sens que le produit tensoriel ordinaire sur un anneau commutatif).

Si $f : M \to M'$ et $g : N \to N'$ sont des applications linéaires continues de Ω-modules linéairement topologisés, alors $f \otimes g : M \otimes N \to M' \otimes N'$ est une application continue.

Nous notons $M \hat{\otimes} N$ *le module séparé-complété du produit tensoriel topologique de deux* Ω-*modules linéairement topologisés* M *et* N, et nous l'appelons *produit tensoriel séparé-complété*.

Comme le quotient de $M \otimes N$ par son sous-module ouvert (3.2.9.1) s'identifie à

(3.2.9.2) $$(M/A_i) \otimes (N/B_j),$$

nous obtenons $M \hat{\otimes} N$ sous la forme

(3.2.9.3) $$M \hat{\otimes} N = \varprojlim_{i,j} (M/A_i) \otimes (N/B_j),$$

où A_i (resp. B_j) parcourt l'ensemble des sous-modules ouverts de M (resp. N).

Le produit tensoriel séparé-complété est associatif et commutatif comme le produit tensoriel.

(3.2.10) *Proposition. — Produit tensoriel de modules valués. Soient* M *et* N *deux modules valués sur un anneau de valuation discrète complet* Ω. *Alors le produit tensoriel valué* (3.2.1) *coïncide, en tant que module topologique, avec le produit tensoriel topologique* (3.2.9).

Preuve. — Nous pouvons prendre les sous-modules M_ν (resp. N_ν) comme système fondamental de voisinages de zéro dans M (resp. N), ν parcourant $\mathbf{R}_+$.

La formule (3.2.9.1) nous montre que les sous-modules $M_\nu \otimes N + M \otimes N_\nu$ constituent un système fondamental de voisinages de zéro dans $M \otimes N$ (il est superflu d'indiquer qu'il s'agit d'images canoniques, d'après (3.2.1.4)).

Dans le produit tensoriel valué $M \otimes N$, nous avons la relation

(3.2.10.1) $$(M \otimes N)_{2\nu} \subset M_\nu \otimes N + M \otimes N_\nu \subset (M \otimes N)_\nu$$

pour tout $\nu \in \mathbf{R}_+$. La première inclusion résulte de (3.2.1.2). Les relations (3.2.10.1) prouvent notre proposition.

(3.2.11) *Proposition. — Produit tensoriel de modules compacts. Soient* Ω *un anneau commutatif,* I *et* J *deux ensembles ordonnés filtrants,* $(M_i)_{i\in I}$ *et* $(N_j)_{j\in J}$ *deux familles de* Ω*-modules linéairement topologisés et compacts. Supposons donnés des épimorphismes linéaires et continus* $f_{i',i}: M_i \to M_{i'}$ *et* $g_{j',j}: N_j \to N_{j'}$ *(pour* $i \geqslant i'$, $j \geqslant j'$*) permettant de construire les limites projectives*

$$M = \varprojlim M_i \quad et \quad N = \varprojlim N_j.$$

Les modules M *et* N *sont linéairement topologisés. Si, pour tous* $i \in I$ *et* $j \in J$, *le produit tensoriel topologique* (3.2.9) $M_i \otimes N_j$ *est complet, alors le produit tensoriel séparé-complété* $M \hat{\otimes} N$ *s'identifie à la limite projective* $\varprojlim M_i \otimes N_j$.

Preuve. — Les modules M et N sont *compacts*, et les applications canoniques $f_i: M \to M_i$, $g_j: N \to N_j$ sont *surjectives*.

Soit A un sous-module ouvert de M. Comme le complémentaire de A est compact et que l'intersection des noyaux des f_i se réduit à zéro, nous avons

(3.2.11.1) $$\operatorname{Ker} f_i \subset A \quad \textit{pour } i \in I \textit{ assez grand.}$$

Nous pouvons donc factoriser l'épimorphisme $M \to M/A$ en $M \to M_i \to M/A$.

Si B désigne un sous-module ouvert de N, nous avons de même une factorisation $N \to N_j \to N/B$ pour $j \in J$ assez grand. Nous en déduisons les applications

(3.2.11.2) $$M_i \otimes N_j \to (M/A) \otimes (N/B),$$

pour i et j assez grands, d'où, en passant à la limite projective sur i et j, l'application

(3.2.11.3) $$\varprojlim (M_i \otimes N_j) \to (M/A) \otimes (N/B).$$

Passons maintenant à la limite projective sur A et B; nous obtenons l'application

(3.2.11.4) $$\varprojlim M_i \otimes N_j \to M \hat{\otimes} N.$$

D'autre part, les morphismes $f_i: M \to M_i$ et $g_j: N \to N_j$ déterminent les morphismes

(3.2.11.5) $$f_i \hat{\otimes} g_j: M \hat{\otimes} N \to M_i \hat{\otimes} N_j,$$

d'où, par passage à la limite projective sur i et j, l'application

(3.2.11.6) $$M \hat{\otimes} N \to \varprojlim M_i \hat{\otimes} N_j.$$

Or nous avons supposé tous les produits tensoriels $M_i \otimes N_j$ complets, ce qui entraîne $M_i \otimes N_j = M_i \hat{\otimes} N_j$, et l'application (3.2.11.6) est réciproque de (3.2.11.4), ce qui prouve (et précise) notre proposition.

(3.3) Algèbres tensorielles, symétriques et extérieures.

(3.3.1) *Notations.* — Soient, de nouveau, Ω un *anneau commutatif (quelconque)* et M un Ω-module. Pour chaque $n \in \mathbf{N}$, nous notons $T^n M$ (resp. $S^n M$, $E^n M$) la *puissance* *tensorielle* (resp. *symétrique*, *extérieure*) n-ième du module M. En formant les sommes directes, nous obtenons *l'algèbre tensorielle* de M :

(3.3.1.1)
$$TM = \coprod_{n \in \mathbf{N}} T^n M,$$

l'algèbre symétrique de M :

(3.3.1.2)
$$SM = \coprod_{n \in \mathbf{N}} S^n M,$$

et *l'algèbre extérieure* de M :

(3.3.1.3)
$$EM = \coprod_{n \in \mathbf{N}} E^n M.$$

Ce sont des Ω-*algèbres supplémentées*; l'augmentation est donnée par la projection sur T^0M (resp. S^0M, E^0M), qui s'identifie à Ω. De même T^1M, S^1M et E^1M s'identifient tous trois à M, mais, quand on parle de produits d'éléments de M, il est indispensable de préciser dans quelle algèbre on les calcule. Les algèbres SM et EM sont définies comme des *quotients* de TM par les idéaux bilatères IM et KM engendrés respectivement par les éléments $x.y - y.x$ et $x.x$ (où $x, y \in M$). Nous avons donc les suites exactes

(3.3.1.4)
$$0 \to IM \to TM \to SM \to 0;$$

(3.3.1.5)
$$0 \to KM \to TM \to EM \to 0.$$

Pour chaque $n \in \mathbf{N}$, nous notons I^nM l'intersection de IM et de T^nM.

Nous venons de préciser les notations concernant des *foncteurs covariants* en M : TM, ..., I^nM, M parcourant la catégorie des Ω-modules. Tous ces foncteurs *permutent aux limites inductives*.

(3.3.2) *Le cas gradué.* — Supposons que Ω soit un anneau *gradué* (1.1.1) et M un Ω-module *gradué* (1.1.2).

Alors, pour chaque $n \in \mathbf{N}$, T^nM est un *module gradué*, d'après l'associativité du produit tensoriel gradué (1.1.8). Sur TM nous prenons la *graduation de somme directe* (1.1.5). Les idéaux IM et KM sont *gradués*, ce qui nous permet de définir SM et EM comme des *algèbres supplémentées graduées*.

(3.3.3) *Le cas filtré.* — Supposons désormais que Ω soit un *anneau filtré* (2.1.1) et M un Ω-*module* filtré (2.1.3). Nous définissons les *filtrations canoniques* de TM, SM et EM en prenant la *borne inférieure des filtrations de* Ω-*algèbres* (2.1.11) *pour lesquelles l'injection canonique de* M (dans l'algèbre considérée) *est un morphisme*. Cette injection est en fait une *isométrie*.

Nous vérifions que les algèbres TM, SM, EM sont respectivement les sommes directes filtrées (2.1.8) des modules T^nM, S^nM, E^nM.

La filtration de T^nM coïncide avec celle définie par récurrence, en construisant le *produit tensoriel filtré* (2.1.9) $T^{n-1}M \otimes_\Omega M$.

Nous définissons les *filtrations canoniques* de IM, I^nM et KM comme les *filtrations induites* (2.1.5) par celle de TM.

Les filtrations canoniques de SM et de EM peuvent encore s'obtenir comme *filtration quotient* (2.1.7), à partir des suites exactes (3.3.1.4) et (3.3.1.5).

(3.3.4) *Les morphismes fonctoriels* F gr$\to$gr F. — Conservons les notations de (3.3.3). Nous construisons l'anneau gradué gr Ω (2.3.2) et le gr Ω-module gr M (2.3.3). Désignons par F l'un des foncteurs T^n, E^n, S^n, T, E, S, I^n, I, K introduits en (3.3.1). Nous obtenons alors, à partir du foncteur F et du Ω-module M, deux gr Ω-modules gradués : F gr M et gr FM. Ces derniers sont reliés par un *morphisme fonctoriel*

(3.3.4.1) $$\mathrm{F\,gr\,M} \to \mathrm{gr\,FM},$$

que nous allons préciser (comme nous l'avons fait en (2.3.10)).

L'application

(3.3.4.2) $$\mathrm{T\,gr\,M} \to \mathrm{gr\,TM}$$

est déterminée par les deux conditions suivantes : c'est un *morphisme de* gr Ω-*algèbres supplémentées* ; *sa restriction à* T^1gr M *est l'identité* (rappelons que T^1gr M et gr T^1M sont tous deux identifiés à gr M). L'existence et l'unicité du morphisme (3.3.4.2) résultent de la définition du foncteur T comme solution d'un problème d'application universelle.

Lorsque F est l'un des foncteurs T^n, I^n, I, K, le morphisme (3.3.4.1) est défini par restriction à partir de (3.3.4.2).

Nous obtenons ensuite les morphismes S gr M$\to$gr SM et E gr M$\to$gr EM par passage aux quotients à partir de (3.3.4.2). Nous pourrions aussi les définir directement, comme le morphisme T gr M$\to$gr TM. Nous avons les diagrammes commutatifs :

(3.3.4.3) $$\begin{array}{ccccccccc} 0 & \to & \mathrm{I\,gr\,M} & \to & \mathrm{T\,gr\,M} & \to & \mathrm{S\,gr\,M} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{gr\,IM} & \to & \mathrm{gr\,TM} & \longrightarrow & \mathrm{gr\,SM} & \to & 0 \end{array}$$

(3.3.4.4) $$\begin{array}{ccccccccc} 0 & \to & \mathrm{K\,gr\,M} & \to & \mathrm{T\,gr\,M} & \to & \mathrm{E\,gr\,M} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{gr\,KM} & \to & \mathrm{gr\,TM} & \to & \mathrm{gr\,EM} & \to & 0 \end{array}$$

(3.3.5) *Cas d'un module filtré-libre.* — Supposons que le Ω-module M soit *filtré-libre* (2.1.16) *par rapport à la base* $(x_i)_{i\in \mathrm{I}}$.

Nous supposons l'ensemble d'indices I *totalement ordonné*, et nous posons $w(\mathrm{M}\,; x_i) = \tau_i$ pour $i \in \mathrm{I}$.

Pour chaque $n \in \mathbf{N}^*$, chacun des modules T^nM, S^nM, E^nM admet comme *base filtrée* (2.1.16) une partie des *monômes*

(3.3.5.1) $$x_{i_1} \ldots x_{i_n},$$

ayant les *filtrations*

(3.3.5.2) $$\tau_{i_1}+\ldots+\tau_{i_n},$$

et, bien entendu, calculés respectivement dans les algèbres TM, SM, EM. Les indices $i_1, \ldots, i_n$ doivent vérifier les conditions suivantes :

(3.3.5.3) $$i_1, \ldots, i_n \in \mathrm{I} \quad \textit{pour} \ \mathrm{T}^n\mathrm{M}.$$

(3.3.5.4) $$i_1, \ldots, i_n \in \mathrm{I} \quad \textit{et} \quad i_1 \leqslant i_2 \leqslant \ldots \leqslant i_n \quad \textit{pour} \ \mathrm{S}^n\mathrm{M}.$$

(3.3.5.5) $$i_1, \ldots, i_n \in \mathrm{I} \quad \textit{et} \quad i_1 < i_2 < \ldots < i_n \quad \textit{pour} \ \mathrm{E}^n\mathrm{M}.$$

Quant au module $\mathrm{I}^n\mathrm{M}$, il admet comme *générateurs* les éléments

(3.3.5.6) $$x_{i_1}\ldots x_{i_{\alpha-1}}(x_{i_\alpha}x_{i_{\alpha+1}}-x_{i_{\alpha+1}}x_{i_\alpha})x_{i_{\alpha+2}}\ldots x_{i_n}$$

calculés dans TM, qui ont la *filtration* $\tau_{i_1}+\ldots+\tau_{i_n}$ (*si* $i_\alpha \neq i_{\alpha+1}$). Les indices $i_1, \ldots, i_n$ varient dans I; l'indice entier α varie de 1 à $n-1$.

Les *morphismes fonctoriels* $\mathrm{T}^n\mathrm{gr}\ \mathrm{M} \to \mathrm{gr}\ \mathrm{T}^n\mathrm{M}$, $\mathrm{S}^n\mathrm{gr}\ \mathrm{M} \to \mathrm{gr}\ \mathrm{S}^n\mathrm{M}$, $\mathrm{E}^n\mathrm{gr}\ \mathrm{M} \to \mathrm{gr}\ \mathrm{E}^n\mathrm{M}$ et $\mathrm{I}^n\mathrm{gr}\ \mathrm{M} \to \mathrm{gr}\ \mathrm{I}^n\mathrm{M}$ sont alors tous *bijectifs*.

Les assertions précédentes résultent de la construction des algèbres tensorielle, symétrique et extérieure d'un module libre (non filtré), et du lemme suivant.

(3.3.6) *Lemme. — Soit* N *un* Ω*-module filtré-libre* (2.1.16) *pour la base* $(e_i)_{i\in \mathrm{I}}$, *avec* $w(e_i)=\tau_i$. *Définissons sur* N *une structure d'algèbre au moyen des « constantes de structure »* c_{ijk} *par les formules*

(3.3.6.1) $$e_ie_j=\sum_{k\in \mathrm{I}} c_{ijk}e_k,$$

pour tous $i, j \in \mathrm{I}$.

Alors, pour que N *soit une* Ω*-algèbre filtrée* (2.1.11), *il faut et il suffit que les filtrations* $v(c_{ijk})$ *des constantes de structure vérifient les relations*

(3.3.6.2) $$v(c_{ijk})+\tau_k \geqslant \tau_i+\tau_j \qquad (\textit{pour tous}\ i, j, k \in \mathrm{I}).$$

(3.3.7) *Théorème. — Désignons de nouveau par* Ω *un anneau de valuation discrète complet* (3.1.1) *et soit* M *un* Ω*-module valué. Alors :*

(3.3.7.1) *Les algèbres* TM, SM *et* EM *sont des* Ω*-algèbres supplémentées valuées; de plus,* TM *et* SM *sont valuées en tant qu'anneaux.*

(3.3.7.2) *Les morphismes fonctoriels*

$$\mathrm{T\ gr\ M} \to \mathrm{gr\ TM}, \quad \mathrm{S\ gr\ M} \to \mathrm{gr\ SM}, \quad \mathrm{E\ gr\ M} \to \mathrm{gr\ EM},$$
$$\mathrm{I\ gr\ M} \to \mathrm{gr\ IM}, \quad \mathrm{K\ gr\ M} \to \mathrm{gr\ KM}$$

sont tous bijectifs.

(3.3.7.3) *Si* $f: \mathrm{M} \to \mathrm{M}'$ *est une isométrie de* Ω*-modules valués, les morphismes* $\mathrm{T}f: \mathrm{TM} \to \mathrm{TM}'$, $\mathrm{S}f: \mathrm{SM} \to \mathrm{SM}'$, $\mathrm{E}f: \mathrm{EM} \to \mathrm{EM}'$ *sont tous des isométries.*

(3.3.7.4) *Pour chaque* $n \in \mathbf{N}$ *et chaque* $\nu \in \mathbf{R}_+$, *le sous-module* $(\mathrm{T}^n\mathrm{M})_\nu$ (*resp.* $(\mathrm{S}^n\mathrm{M})_\nu$, $(\mathrm{E}^n\mathrm{M})_\nu$) *est engendré par les produits* $x_1 \ldots x_n$, *calculés dans l'algèbre* TM (*resp.* SM, EM), *où* $x_1, \ldots, x_n$ *sont des éléments de* M *vérifiant*

$$w(x_1) + \ldots + w(x_n) \geqslant \nu.$$

Le module $(\mathrm{I}^n\mathrm{M})_\nu$ *est engendré par les éléments de la forme* $a(xy - yx)b$, *où* $x, y \in \mathrm{M}$, $a \in \mathrm{T}^i\mathrm{M}$, $b \in \mathrm{T}^j\mathrm{M}$, $i + j + 2 = n$, *et* $w(a) + w(b) + w(x) + w(y) \geqslant \nu$.

Preuve. — Nous procédons comme pour le théorème (3.2.1). Grâce au théorème (3.1.4), les vérifications faites en (3.3.5) prouvent nos assertions pour les *modules de type fini*; pour démontrer (3.3.7.3), nous utilisons le théorème (1.2.4). Nous passons ensuite à la *limite inductive*, pour une famille d'*isométries*.

CHAPITRE II

GROUPES FILTRÉS ET PRO-p-GROUPES

1. GROUPES FILTRÉS

(1.1) Filtrations de groupes.

(1.1.1) *Définition.* — Un groupe filtré est un groupe G muni d'une application $\omega : G \to \mathbf{R}_+^* \cup \{+\infty\}$ vérifiant les axiomes suivants. Pour tous $x, y \in G$,

(1.1.1.1) $$\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))\,;$$

(1.1.1.2) $$\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y).$$

La fonction ω sera dite *filtration*, et le nombre $\omega(x)$ *filtration de l'élément* x. Ces filtrations ont des valeurs *strictement positives*. Nous écrirons éventuellement $\omega(G; x)$ pour désigner la filtration de $x \in G$.

(1.1.2) *Les sous-groupes* G_ν *et* $G_{\nu+}$. — Pour chaque $\nu \in \mathbf{R}_+^*$, définissons G_ν (resp. $G_{\nu+}$) comme l'ensemble des $x \in G$ qui vérifient $\omega(x) \geqslant \nu$ (resp. $\omega(x) > \nu$). Les ensembles G_ν sont des *sous-groupes* distingués de G, et vérifient les trois propriétés suivantes :

(1.1.2.1) $$G = \bigcup_{\nu > 0} G_\nu.$$

(1.1.2.2) $$(G_\nu, G_{\nu'}) \subset G_{\nu+\nu'}, \qquad \text{pour tous } \nu, \nu' \in \mathbf{R}_+^*.$$

(1.1.2.3) $$G_\nu = \bigcap_{\nu' < \nu} G_{\nu'}, \qquad \text{pour tout } \nu \in \mathbf{R}_+^*.$$

Réciproquement, une famille de sous-groupes G_ν vérifiant ces trois propriétés provient d'une filtration ω, qu'on retrouve par la formule :

(1.1.2.4) $$\omega(x) = \sup \nu \qquad \textit{pour } x \in G_\nu.$$

Il n'est pas nécessaire de supposer les G_ν distingués (c'est une conséquence des trois propriétés).

Les $G_{\nu+}$ vérifient des axiomes analogues.

(1.1.3) *Morphismes, isométries.* — Soient G, H deux groupes filtrés. Nous appelons *morphisme* $f : G \to H$ un *homomorphisme* de groupes qui vérifie la relation

(1.1.3.1) $$\omega(H; f(x)) \geqslant \omega(G; x) \qquad \text{pour tout } x \in G,$$

ce que nous pouvons encore écrire

(1.1.3.2) $$f(G_\nu)\subset H_\nu \qquad \text{pour tout } \nu\in\mathbf{R}_+^*.$$

Nous venons de définir la *catégorie* des groupes filtrés. Une *isométrie* est un morphisme $f: G\rightarrow H$ qui est injectif et conserve les filtrations : $\omega(H; f(x))=\omega(G; x)$.

La filtration induite d'un sous-groupe d'un groupe filtré est définie par restriction, comme en (I, 2.1.5), et l'injection du sous-groupe devient une isométrie.

(1.1.4) *La borne inférieure* d'une famille de filtrations $(\omega_i)_{i\in I}$ sur un même groupe G est définie par la formule

(1.1.4.1) $$\omega(x)=\inf_{i\in I}\omega_i(x).$$

Si $\omega(x)>0$ *pour tout* $x\in G$, alors ω est une filtration, dite *borne inférieure* des $(\omega_i)_{i\in I}$. Comme en (I, 2.1.7) nous définissons la *filtration quotient* d'un groupe quotient d'un groupe filtré, ainsi que la filtration d'une *somme directe* et d'une *limite inductive* de groupes filtrés (I, 2.1.8).

(1.1.5) *Topologie et complétion.* — Une filtration ω définit une topologie sur un groupe G : les sous-groupes G_ν forment un système fondamental de voisinages de l'élément neutre. Le groupe G devient ainsi un groupe topologique éparpillé et métrisable. Les morphismes (1.1.3) sont des homomorphismes continus (réciproque inexacte). Une filtration ω est dite *séparée* quand la topologie est séparée, c'est-à-dire quand

(1.1.5.1) $$\omega(x)=+\infty \quad \text{implique} \quad x=1.$$

Par contre nous appelons, comme en (I, 2.1.12), *filtration discrète* une filtration dont *l'ensemble des valeurs finies* est une partie discrète de $\mathbf{R}_+$. La topologie associée n'est pas discrète, en général.

Le *complété* d'un groupe filtré séparé G peut s'obtenir sous la forme $\varprojlim G/G_\nu$. Le foncteur « chapeau » (complétion d'un groupe séparé) possède les mêmes propriétés que pour les groupes commutatifs : cf. (I, 2.1.14).

(1.1.6) *Identités dans les groupes.* — Les identités suivantes interviennent dans la démonstration d'existence du gradué associé d'un groupe filtré. Ce sont les identités (1.1) et (1.2) de [14], p. 7, à ceci près que nous écrivons maintenant $x^y=y^{-1}xy$ (au lieu de yxy^{-1}) et $(x,y)=x^{-1}y^{-1}xy$ (au lieu de $xyx^{-1}y^{-1}$).

(1.1.6.1) $$(xy, z)=(x, z)^y(y, z);$$

(1.1.6.2) $$(x, yz)=(x, z)(x, y)^z;$$

(1.1.6.3) $$(x^y, (y, z))(y^z, (z, x))(z^x, (x, y))=1.$$

(1.1.7) *Le gradué associé* gr G *d'un groupe filtré* G.

Pour chaque $\nu\in\mathbf{R}_+^*$, nous définissons le groupe quotient

(1.1.7.1) $$\mathrm{gr}_\nu G=G_\nu/G_{\nu^+}.$$

Ce groupe est *commutatif*, d'après (1.1.1.2), et nous le notons *additivement*. Nous définissons d'abord gr G comme un *groupe additif gradué* par la formule :

(1.1.7.2) $$\operatorname{gr} G = \coprod_{\nu \in \mathbf{R}_+^*} \operatorname{gr}_\nu G.$$

Pour les éléments homogènes de gr G, nous définissons le crochet $[\xi, \eta]$ à partir du commutateur, par passage aux quotients. L'axiome (1.1.1.2) et les identités (1.1.6.1), (1.1.6.2) montrent que cette définition est correcte. Le crochet est ensuite défini, par bilinéarité, pour des éléments quelconques de gr G. Il reste à vérifier l'*identité de Jacobi :* c'est une conséquence de l'identité de P. Hall (1.1.6.3). Ces vérifications sont exactement celles qui conduisent au théorème (2.1) de [14]; la seule différence est que gr G est une *algèbre de Lie graduée de type* $\mathbf{R}_+^*$ (et non plus $\mathbf{N}^*$). Le remplacement de $xyx^{-1}y^{-1}$ par $x^{-1}y^{-1}xy$ ne modifie pas la définition des crochets, car $[-\xi, -\eta] = [\xi, \eta]$.

Les notions de *termes dominants* et de *représentants* sont définies pour les groupes filtrés et leurs gradués associés comme en (I, 2.3.4).

(1.1.8) *Le foncteur* gr. — Si $f : G \to H$ est un morphisme de groupes filtrés, nous avons, pour tout $\nu \in \mathbf{R}_+^*$, une restriction $f : G_\nu \to H_\nu$, puis, par passage aux quotients, un homomorphisme $\operatorname{gr}_\nu G \to \operatorname{gr}_\nu H$ et enfin (par somme directe) une application

(1.1.8.1) $$\operatorname{gr} f : \operatorname{gr} G \to \operatorname{gr} H$$

qui est un *morphisme d'algèbres de Lie graduées.*

Nous avons donc un foncteur gr qui envoie la catégorie des *groupes filtrés* (1.1.3) dans celle des *algèbres de Lie graduées* (de type $\mathbf{R}_+^*$, c'est-à-dire en *degrés strictement positifs*).

Ce foncteur gr possède la plupart des propriétés des foncteurs du même nom, étudiés en (I, 2.3), qui envoyaient une catégorie Fil(Ω) dans la catégorie correspondante Gr(gr Ω).

Si nous avons une *isométrie* $f : G \to H$, alors $\operatorname{gr} f : \operatorname{gr} G \to \operatorname{gr} H$ est un *monomorphisme* (la réciproque est exacte si G est séparé).

Plus particulièrement, si G est un *sous-groupe* de H, muni de la *filtration induite,* alors gr G s'identifie à une *sous-algèbre de Lie de* gr H. Si G est *distingué* dans H, alors gr G est un *idéal* de gr H.

Si nous partons d'une *suite exacte* de groupes filtrés :

(1.1.8.2) $$1 \to G' \to G \to G'' \to 1,$$

où G′ a la filtration induite (1.1.3) et G″ la filtration quotient (1.1.4), nous obtenons une suite exacte *d'algèbres de Lie graduées*

(1.1.8.3) $$0 \to \operatorname{gr} G' \to \operatorname{gr} G \to \operatorname{gr} G''.$$

Lorsque la filtration de G est *discrète*, le morphisme $\operatorname{gr} G \to \operatorname{gr} G''$ est *surjectif.*

Si G est filtré séparé, son complété a même gradué associé : gr G et gr $\hat{G}$ s'identifient canoniquement.

La proposition (I, 2.3.13) et ses corollaires valent pour les groupes filtrés et leurs gradués associés.

(1.1.9) *Filtrations de groupes induites par des filtrations d'anneaux.* — La proposition suivante étend le théorème (3.2) de [14].

Soit A *un anneau filtré* (I, 2.1.1). *L'anneau gradué associé* gr A (I, 2.3.2) *est considéré comme une algèbre de Lie pour le crochet* $[\xi, \eta] = \xi\eta - \eta\xi$. *Notons* A^* *le groupe multiplicatif des éléments inversibles de* A, G *l'ensemble des* $x \in A^*$ *pour lesquels* $w(x-1) > 0$, *et posons* $\omega(x) = w(x-1)$ *pour* $x \in G$.

Alors G *est un sous-groupe de* A^* *et* ω *une filtration de* G. *Nous définissons comme suit un monomorphisme canonique* ι *de l'algèbre de Lie* gr G (*calculée pour la filtration* ω) *dans* gr A *(calculé pour la filtration* w) : *si* $\xi \in \mathrm{gr}_\nu G$, *nous prenons un représentant* x *de* ξ *dans* G, *puis le terme dominant de* $x-1$ *dans* $\mathrm{gr}_\nu A$, *que nous posons égal à* $\iota(\xi)$.

Preuve. — Les vérifications s'effectuent le plus simplement à partir des deux identités suivantes (où x et y sont deux éléments inversibles d'un anneau) :

(1.1.9.1) $$(xy^{-1}-1) = (x-1) - (y-1) - (xy^{-1}-1)(y-1).$$

(1.1.9.2) $$(x^{-1}y^{-1}xy-1) = (1 + (x^{-1}y^{-1}-1))((x-1)(y-1) - (y-1)(x-1)).$$

Dans la pratique, nous appliquerons la proposition précédente non pas au groupe G tout entier, mais à l'un de ses sous-groupes.

(1.1.10) *Exemple : algèbres de Magnus.* — Soient Ω un anneau commutatif et $(X_i)_{i \in I}$ un ensemble de « lettres ». Formons l'algèbre A des *séries formelles associatives* (mais *non commutatives* si I a plus d'un élément) *en les* $(X_i)_{i \in I}$ *à coefficients dans* A. Les éléments $1 + X_i$ sont inversibles dans A, car $(1+X_i)^{-1} = \sum_{n \in \mathbf{N}} (-X_i)^n$. Ces éléments engendrent dans A un *groupe libre* $\mathscr{F}$ (Magnus; cf. [14], théorème (4.1)). Toute filtration w de *l'algèbre de Magnus* A pour laquelle $w(X_i) > 0$ définit, par le procédé (1.1.9), une filtration du groupe libre $\mathscr{F}$.

(1.1.11) *Modifications d'une filtration de groupe.* — Soient G un groupe, ω une filtration de G (1.1.1) et f une application de $\mathbf{R}_+$ dans $\mathbf{R}$, prolongée par $f(+\infty) = +\infty$. Supposons vérifiées les conditions suivantes.

(1.1.11.1) *La fonction* f *est croissante.*

(1.1.11.2) $$f(\nu + \nu') \geqslant f(\nu) + f(\nu'), \qquad \textit{pour tous } \nu, \nu' \in \mathbf{R}_+.$$

(1.1.11.3) $$f(\omega(x)) > 0 \qquad \textit{pour tout } x \in G.$$

Alors la fonction $\omega' = f \circ \omega$ *est une filtration de* G.

Voici quelques exemples :

(1.1.11.4) $f(\nu) = a\nu$, où $a > 0$. Les valeurs de la filtration sont multipliées par a.

(1.1.11.5) $f(\nu) = \nu - c$, où $c \geqslant 0$. Nous supposons $\omega(x) > c$ pour tout $x \in G$.

Dans les deux exemples précédents, le nouveau gradué associé à G se déduit de l'ancien en modifiant seulement les degrés, comme en (I, 1.1.10).

(1.1.11.6) $f(\nu) = [\nu]$ (partie entière de ν), en supposant $\omega(x) \geqslant 1$ pour tout $x \in G$.

La nouvelle filtration ω' est à valeurs entières.

(1.2) Groupes p-filtrés et algèbres de Lie mixtes.

(1.2.1) Appliquons la construction de (1.1.9) au cas où $w(p)=1$ dans l'anneau filtré A (p désigne, comme toujours, un nombre premier). Cette condition signifie que A est une *algèbre associative filtrée* (I, 2.1.11) sur l'anneau $\mathbf{Z}$ *muni de sa filtration p-adique*. L'anneau gradué gr A est donc une algèbre sur gr $\mathbf{Z}$, et ce dernier anneau s'écrit encore $\Gamma=\mathbf{F}_p[\pi]$, π désignant le terme dominant de p ($\deg \pi=1$) : cf. [3], exemple 1, p. 23.

Soit $x=1+z\in A$, avec $w(z)>0$. Étudions $\omega(x^p)$, c'est-à-dire $w(x^p-1)$. Nous avons, par la formule du binôme :

(1.2.1.1)
$$x^p-1=pz+z^p+pz^2(\ldots),$$

où

(1.2.1.2)
$$(\ldots)=\sum_{1<i<p} p^{-1}\binom{p}{i} z^{i-2}$$

est un élément de A, et a donc une filtration $\geqslant 0$.

Posons $w(z)=\nu$. Nous voyons que, *à un terme de filtration* $\geqslant(2\nu+1)$ *près*, x^p-1 se réduit à $pz+z^p$. Nous avons, par les axiomes des filtrations

$$w(pz)\geqslant \nu+1 \quad \text{et} \quad w(z^p)\geqslant p\nu.$$

Il importe de savoir comparer les nombres $\nu+1$ et $p\nu$.

(1.2.2) *Définition de la fonction* φ. — *Pour tout nombre* $\nu\in\mathbf{R}_+$, *nous posons*

$$\varphi(\nu)=\min(\nu+1, p\nu).$$

Nous avons $\varphi(\nu)=p\nu$ pour $0\leqslant\nu\leqslant(p-1)^{-1}$ et $\varphi(\nu)=\nu^{-1}$ pour $(p-1)^{-1}\leqslant\nu$. Le nombre $(p-1)^{-1}$ est strictement compris entre 0 et 1, sauf si $p=2$, auquel cas il vaut 1.

(1.2.3) Revenons à l'algèbre A étudiée en (1.2.1). Nos calculs conduisent à l'énoncé suivant (G est défini comme en (1.1.9)) : si $x\in G_\nu$ alors $x^p\in G_{\varphi(\nu)}$.

De plus, l'image de x^p dans $\operatorname{gr}_{\varphi(\nu)}G$ ne dépend que de l'image de x dans $\operatorname{gr}_\nu G$, et l'élévation à la puissance p-ième définit ainsi, par passage aux quotients, des applications

(1.2.3.1)
$$P : \operatorname{gr}_\nu G \to \operatorname{gr}_{\varphi(\nu)} G.$$

Les propriétés de P s'obtiennent à partir de (1.2.1.1), et s'expriment par la structure *d'algèbre de Lie mixte* de gr G, telle que nous allons la définir en (1.2.5).

(1.2.4) *Définition du polynôme de Lie* Λ. — Dans l'algèbre associative (mais non commutative) libre engendrée par X et Y sur le corps premier $\mathbf{F}_p$, l'élément $(X+Y)^p-X^p-Y^p$ s'écrit au moyen de sommes et de crochets de Lie (le crochet $[u, v]$ est $uv-vu$) ; c'est l'identité de Jacobson (par exemple : [13], V, § 7). D'autre part, X et Y engendrent une $\mathbf{F}_p$-*algèbre de Lie libre*, si bien que nous pouvons écrire

(1.2.4.1)
$$(X+Y)^p-X^p-Y^p=\Lambda_p(X, Y),$$

où $\Lambda_p(X, Y)$ est un élément de la $\mathbf{F}_p$-algèbre de Lie libre engendrée par X et Y, ou encore un *polynôme de Lie en* X *et* Y *à coefficients dans* $\mathbf{F}_p$. L'élément $\Lambda_p(\xi, \eta)$ est donc calculable chaque fois que ξ et η appartiennent à une $\mathbf{F}_p$-algèbre de Lie. Nous écrirons Λ au lieu de Λ_p, le nombre p restant sous-entendu.

(1.2.5) *Définition des algèbres de Lie mixtes.* — Nous appellerons *algèbre de Lie mixte* une $\mathbf{F}_p$-*algèbre de Lie* L, *graduée de type* $\mathbf{R}_+^*$ $(\mathrm{L} = \coprod_{\nu \in \mathbf{R}_+^*} \mathrm{L}_\nu)$ dans laquelle à tout élément *homogène* x de degré ν est associé un élément *homogène* $\mathrm{P}x$, de degré $\varphi(\nu)$ (1.2.2), les axiomes suivants étant vérifiés.

(1.2.5.1) Pour $\nu \leqslant (p-1)^{-1}$ et $x, y \in \mathrm{L}_\nu$, $\mathrm{P}(x+y) = \mathrm{P}x + \mathrm{P}y + \Lambda(x, y)$.

(1.2.5.2) Pour $\nu > (p-1)^{-1}$ et $x, y \in \mathrm{L}_\nu$, $\mathrm{P}(x+y) = \mathrm{P}x + \mathrm{P}y$.

(1.2.5.3) Pour $\nu < (p-1)^{-1}$, $x \in \mathrm{L}_\nu, y \in \mathrm{L}$, $[\mathrm{P}x, y] = (\mathrm{ad}\, x)^p y$.

(1.2.5.4) Pour $\nu = (p-1)^{-1}$, $x \in \mathrm{L}_\nu, y \in \mathrm{L}$, $[\mathrm{P}x, y] = (\mathrm{ad}\, x)^p y + \mathrm{P}[x, y]$.

(1.2.5.5) Pour $\nu > (p-1)^{-1}$, $x \in \mathrm{L}_\nu, y \in \mathrm{L}$, $[\mathrm{P}x, y] = \mathrm{P}[x, y]$.

Ces axiomes justifient l'adjectif « mixte ». Pour les éléments de degrés $< (p-1)^{-1}$, l'opérateur P a les propriétés de la p-application d'une algèbre de Lie restreinte (au sens de Jacobson). Au contraire, pour les éléments de degrés $> (p-1)^{-1}$, l'opérateur P est la restriction d'un opérateur linéaire.

Si les composantes homogènes L_ν sont nulles pour $\nu \leqslant (p-1)^{-1}$, l'opérateur P se prolonge en un opérateur linéaire, et la notion d'algèbre de Lie mixte se réduit à celle de Γ-algèbre de Lie graduée (en posant $\pi x = \mathrm{P}x$). Nous rencontrerons ce cas particulier important à partir du chapitre III.

L'algèbre de Lie gr G, où G est défini comme en (1.2.3) et P en (1.2.3.1), est une algèbre de Lie mixte.

(1.2.6) *Morphismes d'algèbres de Lie mixtes.* — Soient L et L' deux algèbres de Lie mixtes (1.2.5). Un *morphisme* $f : \mathrm{L} \to \mathrm{L}'$ est un homomorphisme d'algèbres de Lie, qui vérifie, pour tout $\nu \in \mathbf{R}_+^*$ et tout $x \in \mathrm{L}_\nu$:

(1.2.6.1) $$f(x) \in \mathrm{L}'_\nu$$

et

(1.2.6.2) $$\mathrm{P}f(x) = f(\mathrm{P}x).$$

(1.2.7) *Représentations d'une algèbre de Lie mixte dans une* Γ-*algèbre associative ; l'algèbre enveloppante mixte.* — Les axiomes définissant les algèbres de Lie mixtes (1.2.5) paraissent assez compliqués et nous avons pris soin de montrer leur origine (1.2.1). Considérons une Γ-algèbre associative graduée A (I, 1.1.9) où $\Gamma = \mathbf{F}_p[\pi]$, $\deg \pi = 1$.

Prenons l'idéal A^+ engendré par les éléments de degrés strictement positifs, et posons, pour un élément x homogène de degré ν,

(1.2.7.1) $$\mathrm{P}x = x^p, \qquad \text{si } \nu < (p-1)^{-1},$$

(1.2.7.2) $$\mathrm{P}x = x^p + \pi x, \qquad \text{si } \nu = (p-1)^{-1},$$

(1.2.7.3) $$\mathrm{P}x = \pi x, \qquad \text{si } \nu > (p-1)^{-1}.$$

Nous définissons ainsi sur A^+ une structure d'algèbre de Lie mixte, que nous appellerons l'*algèbre de Lie mixte portée par* A (le crochet est défini par $xy-yx$).

Si L est une algèbre de Lie mixte, nous appellerons *représentation* (ou α-application) de L dans la Γ-algèbre associative A un *morphisme* (1.2.6) de L dans l'algèbre de Lie mixte portée par A.

Nous pouvons maintenant définir *l'algèbre enveloppante mixte* d'une algèbre de Lie mixte L : c'est une Γ-*algèbre associative* (graduée), que nous notons $U_{\text{mix}}L$, *donnée avec une représentation*

(1.2.7.4) $$\sigma : L \rightarrow U_{\text{mix}}L,$$

de telle sorte que *toute représentation* $f : L \rightarrow A$ *dans une* Γ-*algèbre associative admette une factorisation unique*

(1.2.7.5) $$f = g \circ \sigma, \quad \textit{où } g : U_{\text{mix}}L \rightarrow A$$

est un morphisme de Γ-*algèbres*.

L'existence de l'algèbre enveloppante mixte (ou « représentabilité » du foncteur) est élémentaire.

(1.2.8) *Théorème de Poincaré-Birkhoff-Witt pour les algèbres de Lie mixtes. — L'application* σ *qui intervient dans la définition de* $U_{\text{mix}}L$ (1.2.7.4) *est injective*, si bien que toute algèbre de Lie mixte peut être considérée comme une sous-algèbre d'une algèbre de Lie mixte portée par une Γ-algèbre associative.

La preuve de ce théorème est donnée plus loin (1.3). Elle apporte des précisions à l'énoncé du théorème.

(1.2.9) *Corollaire : algèbres de Lie mixtes libres.* — Les axiomes des algèbres de Lie mixtes (1.2.3) peuvent s'exprimer en n'utilisant que des opérations partout définies. Étant donné un ensemble de lettres $(X_i)_{i \in I}$ et une famille $(\tau_i)_{i \in I}$ de nombres réels strictement positifs, il en résulte l'existence d'une algèbre de Lie mixte *libre pour les générateurs* $(X_i)_{i \in I}$ *de degrés respectifs* τ_i. D'après le théorème de Poincaré-Birkhoff-Witt (1.2.8), celle-ci se plonge dans une Γ-algèbre associative. Les propriétés universelles de l'algèbre mixte libre et de son algèbre enveloppante montrent que cette dernière est *une* Γ-*algèbre associative libre engendrée par les* $(X_i)_{i \in I}$. Nous en avons une description très explicite : ses éléments sont les combinaisons linéaires (à coefficients dans Γ) des *monômes associatifs* $X_{i_1} X_{i_2} \ldots X_{i_n}$ (où $n \in \mathbf{N}, i_1, \ldots, i_n \in I$) *qui ont les degrés respectifs* $\tau_{i_1} + \ldots + \tau_{i_n}$.

(1.2.10) *Groupes p-filtrés.* — Une filtration ω d'un groupe G (1.1.1) sera dite une p-filtration si elle vérifie l'axiome suivant (1.2.2)

(1.2.10.1) $$\omega(x^p) \geqslant \varphi(\omega(x)), \qquad \textit{pour } x \in G.$$

Les filtrations induites étudiées en (1.2.1) sont des p-filtrations, mais j'ignore si toute p-filtration d'un groupe peut être ainsi définie. Par contre, la structure d'algèbre de Lie mixte sur gr G existe pour tout groupe p-filtré G.

(1.2.11) *Théorème.* — *Soit* G *un groupe* p*-filtré* (1.2.10). *Les éléments de* gr G *sont annulés par* p, *ce qui signifie que* gr G *est une* $\mathbf{F}_p$*-algèbre de Lie.*

Pour $\nu\in\mathbf{R}_+^*$ *et* $\xi\in\mathrm{gr}_\nu G$, *prenons un représentant* x *de* ξ, *puis l'élément* $x^p\in G_{\varphi(\nu)}$, *et enfin l'image de* x^p *dans* $\mathrm{gr}_{\varphi(\nu)}G$. *Ce dernier élément ne dépend que de* ξ. *Nous le notons* $P\xi$, *et nous achevons ainsi de définir une structure d'algèbre de Lie mixte* (1.2.5) *sur* gr G.

La preuve de ce théorème est exposée en (1.4).

Corollaire. — *Soit* $f: G\to H$ *un morphisme de groupes* p*-filtrés* (1.1.3), (1.2.10). *Alors le morphisme* $\mathrm{gr} f: \mathrm{gr}\, G\to\mathrm{gr}\, H$ *est un morphisme d'algèbres de Lie mixtes* (1.2.6).

(1.3) Preuve du théorème (1.2.8).

(1.3.1) Soit L une algèbre de Lie mixte. Construisons la Γ-algèbre de Lie graduée

(1.3.1.1) $$M=\Gamma\otimes_{\mathbf{F}_p}L,$$

déduite de L par extension des scalaires. Un élément homogène $y\in M_\nu$ s'écrit univoquement

(1.3.1.2) $$y=\sum_{0\leqslant i<\nu}\pi^i\otimes x_i \qquad \text{où } x_i\in L_{\nu-i}.$$

Pour simplifier, nous identifions $x\in L$ à $1\otimes x\in M$. L'algèbre L devient ainsi une partie de M (plus précisément une sous-$\mathbf{F}_p$-algèbre). La relation (1.3.1.2) implique

(1.3.1.3) $$M_\nu=L_\nu \qquad \text{pour tout } \nu\leqslant(p-1)^{-1}.$$

(1.3.2) Considérons dans l'algèbre de Lie M l'idéal J engendré par les éléments $Px-\pi x$, où $x\in L_\nu$ avec $\nu>(p-1)^{-1}$. L'axiome (1.2.5.5) nous montre que J coïncide avec le sous-Γ-module engendré par ces éléments. De plus, si nous appliquons l'axiome (1.2.5.2) et la relation (1.3.1.2), nous voyons que les éléments de J s'écrivent univoquement comme des sommes finies

(1.3.2.1) $$\sum_{i,\nu}\pi^i(Px_\nu-\pi x_\nu),$$

où $i\in\mathbf{N}$ et $\nu>(p-1)^{-1}$. Nous en déduisons la relation

(1.3.2.2) $$J\cap L=0,$$

ainsi que

(1.3.2.3) $$\pi^n x\notin J, \quad \text{pour } n\in\mathbf{N},\ \nu\leqslant(p-1)^{-1},\ x\in L_\nu \text{ et } x\neq 0.$$

Formons l'algèbre de Lie quotient

(1.3.2.4) $$N=M/J.$$

C'est une Γ-algèbre de Lie graduée. La restriction à L de l'épimorphisme canonique de M sur N est injective (1.3.2.2), ce qui nous permet encore d'*identifier* L *à une partie de* N. Nous avons maintenant

(1.3.2.5) $$Px=\pi x \qquad \text{pour } x\in L_\nu,\ \nu>(p-1)^{-1}.$$

Les éléments homogènes de degrés $\nu \leqslant (p-1)^{-1}$ dans N proviennent d'éléments du même degré dans M; nous avons donc (1.3.1.3)

(1.3.2.6) $$N_\nu = L_\nu \quad \text{pour } \nu \leqslant (p-1)^{-1}.$$

De plus, (1.3.2.3) nous montre que

(1.3.2.7) *Tout élément non nul de* N, *homogène de degré* $\nu \leqslant (p-1)^{-1}$, *est libre sur* Γ.

(1.3.3) Construisons l'algèbre enveloppante universelle $A = U\,N$ de N.

L'algèbre A est une Γ-algèbre associative graduée, et l'application canonique $N \to A$ est injective, ce qui nous permet d'identifier N (et par conséquent L) à une partie de A. Associons à chaque $x \in L_\nu$, $\nu \leqslant (p-1)^{-1}$, l'élément $u(x) \in A$ défini par

(1.3.3.1) $$u(x) = x^p - Px \qquad \text{si } \nu < (p-1)^{-1};$$

(1.3.3.2) $$u(x) = x^p + \pi x - Px \qquad \text{si } \nu = (p-1)^{-1}.$$

Soit K l'idéal engendré par ces éléments $u(x)$. Le théorème (1.2.8) sera démontré si nous prouvons la relation

(1.3.3.3) $$L \cap K = 0.$$

En effet, K est gradué, et nous aurons une représentation injective de L dans A/K. *La* Γ-*algèbre associative* A/K *est d'ailleurs l'algèbre enveloppante mixte* $U_{\text{mix}}L$.

(1.3.4) La Γ-algèbre de Lie N est somme directe de sous-modules monogènes :

(1.3.4.1) $$N = \coprod_{\nu > 0} \Gamma . x_i,$$

où (x_i), $i \in I$, est une famille d'éléments homogènes de N, dont nous supposons l'ensemble des indices I totalement ordonné (I, 1.2.5). D'après le théorème de Birkhoff-Witt, l'algèbre A est somme directe de sous-modules monogènes $\Gamma . x^\alpha$, où α parcourt $\mathbf{N}^{(I)}$, et $x^\alpha = \prod_{i \in I} x_i^{\alpha_i}$ (produit ordonné).

Associons maintenant à chaque monôme x^α un élément $x_\alpha \in A$ de la manière suivante. Considérons seulement les indices i pour lesquels $\deg x_i \leqslant (p-1)^{-1}$, ce qui implique $x_i \in L$. Posons alors $\alpha_i = \beta_i + p\gamma_i$, avec $\beta_i, \gamma_i \in \mathbf{N}$ et $0 \leqslant \beta_i < p$. Nous définissons x_α en remplaçant, dans le produit ordonné x^α, chaque facteur $x_i^{\alpha_i}$ par $x_i^{\beta_i} u(x_i)^{\gamma_i}$ (pour les i tels que $\deg x_i \leqslant (p-1)^{-1}$); cf. [13], p. 189.

Les éléments x^α et x_α ont toujours le même terme dominant pour la filtration croissante canonique de A. D'après (1.3.2.7), ils sont annulés par les mêmes éléments de Γ. Nous en déduisons que A est encore somme directe des sous-modules monogènes $\Gamma . x_\alpha$, pour $\alpha \in \mathbf{N}^{(I)}$.

(1.3.5) Les éléments $u(x)$ qui engendrent l'idéal K sont *centraux*, d'après la définition (1.3.3.1) et l'axiome (1.2.5.3) si $\deg x < (p-1)^{-1}$, et d'après la définition (1.3.3.2), l'axiome (1.2.5.4) et la relation (1.3.2.5) si $\deg x = (p-1)^{-1}$.

D'après l'axiome (1.2.5.1), nous avons

(1.3.5.1) $$u(x+y)=u(x)+u(y)$$

pour deux éléments $x, y \in L$, homogènes de même degré $\leqslant (p-1)^{-1}$.

Il en résulte que l'idéal K est engendré par certains des x_α, à savoir ceux pour lesquels il existe un indice $i \in I$ tel que $\deg x_i \leqslant (p-1)^{-1}$ et $\alpha_i \geqslant p$. Comme L est engendré par les x_α pour lesquels $|\alpha|=1$, la relation $K \cap L = 0$ est démontrée.

(1.4) Preuve du théorème (1.2.11).

(1.4.1) *Notations.* — Notons M le monoïde libre engendré par les deux lettres X et Y. Un élément $m \in M$ possède un degré en X, un degré en Y et un degré total, notés respectivement $\deg_X m$, $\deg_Y m$, $\deg m$. Ces degrés sont définis par les relations suivantes (où $m, m' \in M$) :

(1.4.1.1) $$\deg_X X = \deg_Y Y = 1.$$

(1.4.1.2) $$\deg_X Y = \deg_Y X = 0.$$

(1.4.1.3) $$\begin{cases} \deg_X mm' = \deg_X m + \deg_X m'. \\ \deg_Y mm' = \deg_Y m + \deg_Y m'. \end{cases}$$

(1.4.1.4) $$\deg m = \deg_X m + \deg_Y m.$$

L'algèbre de Magnus A (1.1.10) engendrée par X et Y sur $\mathbf{Z}$ est l'algèbre des *séries formelles associatives* en X et Y. Un élément $U \in A$ s'écrit univoquement comme une série

(1.4.1.5) $$U = \sum_{m \in M} c_m . m \qquad (c_m \in \mathbf{Z}).$$

L'ordre de cet élément, noté ord U, est le plus grand entier tel que $c_m = 0$ pour les $m \in M$ vérifiant $\deg m < \operatorname{ord} U$ (ou le signe $+\infty$ si $U=0$). L'ordre est une *valuation* de l'anneau A (I, 2.2.1).

Les éléments $X^* = 1 + X$ et $Y^* = 1 + Y$ engendrent dans A un groupe multiplicatif libre, que nous notons $\mathscr{F}$ (1.1.10). L'ordre définit sur $\mathscr{F}$ une filtration (1.1.9) à valeurs entières, ou encore une famille de sous-groupes $(\mathscr{F}_n)_{n \in \mathbf{N}^*}$. La relation $U \in \mathscr{F}_n$ équivaut à $U \in \mathscr{F}$ et $\operatorname{ord}(U-1) \geqslant n$. Les sous-groupes $\mathscr{F}_n$ constituent la *suite centrale descendante* de $\mathscr{F}$ (Magnus-Witt, cf. [14], théorème (4.2)). Ils sont définis par les relations de récurrence

(1.4.1.6) $$\mathscr{F}_1 = \mathscr{F} \qquad \text{et} \qquad (\mathscr{F}_n, \mathscr{F}) = \mathscr{F}_{n+1}.$$

L'algèbre de Lie $\operatorname{gr} \mathscr{F} = \coprod_{n \in \mathbf{N}^*} \mathscr{F}_n / \mathscr{F}_{n+1}$ (1.1.7) est une $\mathbf{Z}$-*algèbre de Lie libre* engendrée par les *termes dominants* de X^* et Y^*. L'image de $\operatorname{gr} \mathscr{F}$ par le monomorphisme ι de la proposition (1.1.9) est l'algèbre de Lie L engendrée dans A par X et Y.

(1.4.2) *Développements en produits des éléments de $\mathscr{F}$.* — Choisissons une base $(u_i)_{i\in\mathbf{N}}$ de l'algèbre de Lie libre L, engendrée par X et Y dans A, qui possède les propriétés suivantes (cf. par exemple [17], appendice).

(1.4.2.1) $$u_0 = \mathrm{X}, \qquad u_1 = \mathrm{Y}$$

(1.4.2.2) *Si* $i \in \mathbf{N}, i \geqslant 2,$ *il existe* $j, k \in \mathbf{N}$ *avec* $j < i, k < i$ *et* $u_i = [u_j, u_k]$.

(1.4.2.3) *Si* $i, j \in \mathbf{N}, i < j,$ *alors* $\deg u_i \leqslant \deg u_j$.

Les éléments u_i sont des *monômes de Lie*; ils sont *homogènes* en X et en Y. Leur degré croît avec leur indice (1.4.2.3), ce qui nous permet de définir les entiers d_n par les relations

(1.4.2.4) $$\deg u_i = n \quad \textit{équivaut à} \quad d_{n-1} \leqslant i < d_n.$$

En particulier $d_0 = 0, d_1 = 2, d_2 = 3$. Construisons maintenant une suite d'éléments $(\mathrm{U}_i)_{i\in\mathbf{N}}$ du groupe libre $\mathscr{F}$ qui vérifient les relations suivantes.

(1.4.2.5) $$\mathrm{U}_0 = \mathrm{X}^* = 1 + \mathrm{X}, \qquad \mathrm{U}_1 = \mathrm{Y}^* = 1 + \mathrm{Y}$$

(1.4.2.6) *Si* $i \in \mathbf{N}, i \geqslant 2,$ *alors* $\mathrm{U}_i = (\mathrm{U}_j, \mathrm{U}_k)$, *où j et k sont deux entiers reliés à i par la relation* (1.4.2.2).

Les éléments u_i sont donc les images par ι des termes dominants des U_i dans l'algèbre de Lie $\operatorname{gr}\mathscr{F}$ (1.1.9). Autrement dit

(1.4.2.7) $\operatorname{ord}(\mathrm{U}_i - 1 - u_i) > n$, *et les classes* mod $\mathscr{F}_{n+1}$ *des* U_i *forment une base du groupe abélien libre* $\mathscr{F}_n/\mathscr{F}_{n+1}$, *pour* $d_{n-1} \leqslant i < d_n$.

A chaque élément $\mathrm{U} \in \mathscr{F}$ nous associons une suite d'entiers $c_i(\mathrm{U}) \in \mathbf{Z}$ $(i \in \mathbf{N})$, univoquement déterminée par les conditions suivantes. Pour chaque $n \in \mathbf{N}^*$ nous définissons $r_n(\mathrm{U}) \in \mathscr{F}$ par la relation

(1.4.2.8) $$\mathrm{U} = \Bigl(\prod_{i < d_{n-1}} \mathrm{U}_i^{c_i(\mathrm{U})}\Bigr) . r_n(\mathrm{U}),$$

où $\prod$ indique un produit *ordonné*, et nous imposons les conditions

(1.4.2.9) $$r_n(\mathrm{U}) \in \mathscr{F}_n.$$

Si nous supposons calculés les exposants $c_i(\mathrm{U})$ pour $i < d_{n-1}$, nous savons déterminer univoquement les $c_i(\mathrm{U})$ pour $d_{n-1} \leqslant i < d_n$, en appliquant (1.4.2.7). Nous remplacerons (1.4.2.8) et (1.4.2.9) par la relation unique

(1.4.2.10) $$\mathrm{U} = \prod_i \mathrm{U}_i^{c_i(\mathrm{U})},$$

qui donne le développement en produit infini ordonné d'un élément de $\mathscr{F}$; ce produit converge au sens de la topologie définie sur $\mathscr{F}$ par sa suite centrale descendante $(\mathscr{F}_n)$.

(1.4.3) *Un lemme de théorie des groupes.* — Notons $\overline{\mathrm{A}}$ l'algèbre quotient $\mathrm{A}/p\mathrm{A}$, et $\overline{u}$ l'image canonique dans $\overline{\mathrm{A}}$ d'un élément $u \in \mathrm{A}$. L'algèbre $\overline{\mathrm{A}}$ est l'algèbre de Magnus *à coefficients dans* $\mathbf{F}_p$ engendrée par $\overline{X}$ et $\overline{Y}$. L'image $\overline{L}$ de L est la $\mathbf{F}_p$-algèbre de Lie libre engendrée par $\overline{X}$ et $\overline{Y}$. Voici notre lemme.

Définissons les deux éléments Z *et* T *du groupe* $\mathscr{F}$ *par les relations*

(1.4.3.1) $$(X^*Y^*)^p = X^{*p}Y^{*p}Z.$$

(1.4.3.2) $$(X^{*p}, Y^*) = (X^*, Y^*)^p T.$$

Alors les coefficients $c_i(Z)$ *et* $c_i(T)$ *des développements* (1.4.2.10) *de* Z *et de* T *vérifient les relations suivantes :*

(1.4.3.3) $$c_i(Z) = 0 \quad \textit{pour } i < 2$$

(1.4.3.4) $$c_i(T) = 0 \quad \textit{pour } i < 3.$$

(1.4.3.5) $$\sum_{i < d_p} c_i(Z)\overline{u}_i = \Lambda(\overline{X}, \overline{Y}).$$

(1.4.3.6) $$c_i(Z) \equiv 0 \ (\mathrm{mod}\ p), \qquad \textit{pour } i < d_{p-1}.$$

(1.4.3.7) $$\sum_{i < d_{p+1}} c_i(T)\overline{u}_i = (\mathrm{ad}\overline{X})^p\overline{Y}.$$

(1.4.3.8) $$c_i(T) \equiv 0 \ (\mathrm{mod}\ p), \qquad \textit{pour } i < d_p.$$

(1.4.3.9) $$\textit{Si } c_i(T) \not\equiv 0 \ (\mathrm{mod}\ p), \qquad \textit{alors } \deg_X u_i \geqslant p.$$

(1.4.4) *Preuve du lemme* (1.4.3). — Les relations (1.4.3.3) et (1.4.3.4) peuvent s'écrire respectivement $Z \in \mathscr{F}_2$ et $T \in \mathscr{F}_3$. Ces relations s'obtiennent à partir des propriétés de l'algèbre de Lie gr $\mathscr{F}$ (1.1.7).

Les relations suivantes s'établissent en étudiant les images $\overline{Z}$ et $\overline{T}$ dans $\overline{A}$. Rappelons que, dans l'anneau $\overline{A}$ de caractéristique p, nous avons l'identité $(1+U)^p = 1 + U^p$. La définition (1.4.3.1) de Z nous donne

(1.4.4.1) $$\overline{Z} = (1+\overline{Y}^p)^{-1}(1+\overline{X}^p)^{-1}(1+(\overline{X}+\overline{Y}+\overline{X}\overline{Y})^p).$$

Il en résulte que les termes de degré i en $\overline{X}$ et $\overline{Y}$ dans le développement de $\overline{Z}$ sont nuls pour $0 < i < p$ et que, pour $i = p$, ils valent $(\overline{X}+\overline{Y})^p - \overline{X}^p - \overline{Y}^p$, c'est-à-dire $\Lambda(\overline{X}, \overline{Y})$ d'après la définition (1.2.4).

Supposons démontrée la formule (1.4.3.6) pour $i < d_{n-1}$. La considération des termes de degré n dans le développement de $\overline{Z}$ conduit à (1.4.3.6) pour $i < d_n$ (si $n \leqslant p-1$). Lorsque (1.4.3.6) est démontré, la formule (1.4.3.5) s'établit par la considération des termes de degré p dans $\overline{Z}$.

De même, la définition (1.4.3.2) de T nous donne

(1.4.4.2) $$\overline{T} = (1+\overline{Y}, 1+\overline{X})^p(1+\overline{X}^p, 1+\overline{Y}).$$

Les termes de degré i dans le développement de $\overline{T}$ sont nuls pour $0 < i < p+1$. Pour $i = p+1$, ils valent $(\mathrm{ad}\overline{X})^p\overline{Y} = \overline{X}^p.\overline{Y} - \overline{Y}.\overline{X}^p$. Nous démontrons les relations (1.4.3.8) pour $i < d_n$, par récurrence sur n jusqu'à $n = p$, puis nous démontrons (1.4.3.7) par la considération des termes de degré $p+1$ dans $\overline{T}$.

Il ne nous reste plus à prouver que (1.4.3.9). Les relations (1.4.2.5) et (1.4.2.6) nous montrent (par récurrence sur i) que tous les monômes non nuls du développement de $U_i - 1$ (1.4.1.5) sont de degré en X au moins égal à $\deg_X u_i$. D'autre part, pour $i \geqslant 2$, les monômes du développement de $U_i - 1$ ont un degré en X au moins égal à 1, et, par conséquent, les monômes du développement de $\overline{U}_i^p - 1$ (dans $\overline{A}$) ont un degré en $\overline{X}$ au moins égal à p. Supposons démontrée la relation (1.4.3.9) pour $i < d_{n-1}$. Les remarques précédentes nous permettent d'établir que tous les monômes non nuls du développement de $\overline{r_n(T)}$ (1.4.2.8) ont un degré en $\overline{X}$ au moins égal à p, ce qui implique (1.4.3.9) pour $d_{n-1} \leqslant i < d_n$.

(1.4.5) *Application du lemme : le mot* $Z(x,y)$. — Soient G un groupe filtré (1.1.1) et x, y deux éléments de G. D'après la définition d'un groupe libre, il existe un unique homomorphisme de $\mathscr{F}$ dans G qui applique X^*, Y^* sur x, y respectivement. Nous notons $U(x,y)$ l'image de $U \in \mathscr{F}$ par cet homomorphisme. Les éléments U_i introduits en (1.4.2) possèdent la propriété suivante (pour tout $i \in \mathbf{N}$).

(1.4.5.1) $$\omega(U_i(x,y)) \geqslant \deg_X u_i . \omega(x) + \deg_Y u_i . \omega(y).$$

En effet (1.4.5.1) est évident d'après (1.4.2.5) pour $i = 0, 1$, et (1.4.2.6) l'établit par récurrence.

Si $U \in \mathscr{F}_n$, alors $\omega(U(x,y)) \geqslant n . \min(\omega(x), \omega(y))$. C'est une conséquence des relations de récurrence (1.4.1.6). Nous pouvons donc écrire, à partir d'un développement (1.4.2.10)

(1.4.5.2) $$U(x,y) = \prod_i U_i(x,y)^{c_i(U)}$$

et le produit ordonné converge dans le groupe topologique G (qu'il n'est pas nécessaire de supposer séparé).

Supposons désormais le groupe G *p-filtré* (1.2.10). Posons $\omega(x) = \nu$, $\omega(y) = \nu'$, avec $\nu \leqslant \nu'$. Pour démontrer que l'opérateur P du théorème (1.2.11) est bien défini, nous devons établir que

(1.4.5.3) $$Z(x,y) \in G_{\varphi(\nu)^+} \qquad \text{pour} \quad \nu < \nu'.$$

Or, d'après (1.4.3.3) et (1.4.5.2),

(1.4.5.4) $$Z(x,y) = \prod_{i \geqslant 2} U_i(x,y)^{c_i(Z)}.$$

Pour $2 \leqslant i < d_{p-1}$, nous avons $\omega(U_i(x,y)) \geqslant \nu + \nu'$, et $c_i(Z) \equiv 0 \pmod{p}$ (1.4.3.6), ce qui implique

(1.4.5.5) $$\omega(U_i(x,y)^{c_i(Z)}) \geqslant \varphi(\nu + \nu') > \varphi(\nu').$$

Pour $i \geqslant d_{p-1}$, nous avons (1.4.5.1)

(1.4.5.6) $$\omega(U_i(x,y)) \geqslant (p-1)\nu + \nu',$$

et, si $\nu < \nu'$, $(p-1)\nu + \nu' > p\nu \geqslant \varphi(\nu)$. L'existence de P est donc établie.

Démontrons maintenant l'axiome (1.2.5.1) pour l'opérateur P. Nous supposons donc $\nu=\nu'\leqslant(p-1)^{-1}$. Les facteurs $U_i(x,y)^{c_i(Z)}$ ont des filtrations $>\varphi(\nu)$, sauf éventuellement si $d_{p-1}\leqslant i<d_p$. Si nous multiplions par ν la filtration de $\mathcal{F}$, de telle sorte que l'homomorphisme de $\mathcal{F}$ dans G devienne un morphisme (1.1.3) et définisse le morphisme associé $\mathrm{gr}\,\mathcal{F}\to\mathrm{gr}\,G$, nous voyons que (1.4.3.5) achève de démontrer (1.2.5.1).

Si, par contre, nous avons $(p-1)^{-1}<\nu\leqslant\nu'$ alors $(p-1)\nu+\nu'>\nu'+1=\varphi(\nu')$, si bien que (1.4.5.5) et (1.4.5.6) entraînent l'énoncé suivant (dont l'axiome (1.2.5.2) est une conséquence).

(1.4.5.7) *Soient x et y deux éléments d'un groupe p-filtré* G, *avec* $(p-1)^{-1}<\omega(x)\leqslant\omega(y)$. *Alors* $y^{-p}x^{-p}(xy)^p\in G_{(\omega(y)+1)^+}$.

(1.4.6) *Fin de la preuve de* (1.2.11) : *le mot* T. — Soient x et y deux éléments du groupe p-filtré G, avec $\omega(x)=\nu$ et $\omega(y)=\nu'$.

Étudions le développement de $T(x,y)$; d'après (1.4.3.4)

(1.4.6.1) $$T(x,y)=\prod_{i\geqslant 3}U_i(x,y)^{c_i(T)}$$

Montrons que tous les facteurs de (1.4.6.1) ont une filtration $\geqslant\varphi(\nu)+\nu'$, l'égalité n'étant atteinte que si $d_p\leqslant i<d_{p+1}$, et $\nu\leqslant(p-1)^{-1}$. Ces propriétés, et la relation (1.4.3.7), nous permettront de vérifier les axiomes (1.2.5.3), (1.2.5.4) et (1.2.5.5), c'est-à-dire d'achever la démonstration du théorème (1.2.11).

Remarquons que nous avons toujours

(1.4.6.2) $$\varphi(\nu+\nu')\geqslant\varphi(\nu)+\nu',$$

et

(1.4.6.3) $$\varphi(\nu+\nu')>\varphi(\nu)+\nu' \quad \textit{si} \quad \nu<(p-1)^{-1} \quad \textit{et} \quad \nu'>0.$$

Pour tout $i\geqslant 3$, nous avons $\omega(U_i(x,y))>\nu+\nu'$. Si, par conséquent, $c_i(T)$ est divisible par p, nous avons

(1.4.6.4) $$\omega(U_i(x,y)^{c_i(T)})>\varphi(\nu+\nu')\geqslant\varphi(\nu)+\nu'.$$

Sinon nous avons (1.4.3.9) $\deg_X u_i\geqslant p$, ce qui implique, d'après (1.4.5.1),

(1.4.6.5) $$\omega(U_i(x,y))\geqslant p\nu+\nu',$$

l'égalité ne pouvant avoir lieu que si $\deg u_i=p+1$, c'est-à-dire $d_p\leqslant i<d_{p+1}$.

Or (1.2.2) nous avons $p\nu\geqslant\varphi(\nu)$, l'égalité n'étant atteinte que pour $\nu\leqslant(p-1)^{-1}$.

2. LES PRO-p-GROUPES ET LEURS Z_p-ALGÈBRES COMPLÉTÉES

(2.1) p-groupes et pro-p-groupes.

(2.1.1) *Définition.* — Nous appellerons *p-groupe* un groupe G où *l'ordre de chaque élément est une puissance de p* : pour tout $x\in G$, il existe $n\in\mathbf{N}$ tel que $x^{p^n}=1$.

Un *p-groupe fini* est un groupe fini dont l'ordre est une puissance de p.

(2.1.2) Nous appellerons *pro-p-groupe* un *groupe topologique* G qui est *limite projective* d'une famille de *p-groupes finis* munis de leur topologie discrète. Cette définition équivaut à la suivante : un pro-p-groupe est un groupe *pro-fini* (ou encore : *compact, totalement discontinu*) dont l'*ordre* est une puissance de p (finie, ou égale au « nombre surnaturel » p^{∞} ; cf. [29], chap. I, 1.4).

Un *morphisme* de pro-p-groupes est un homomorphisme continu.

(2.1.3) *Proposition.* — Pour qu'un groupe *p-filtré* G (1.2.10) soit un *pro-p-groupe*, il faut et il suffit que G soit *compact.*

Preuve. — Un pro-p-groupe est compact. Réciproquement un groupe p-filtré compact G est *complet*, et s'identifie à la limite projective des quotients G/G_{ν} (1.1.5). Ces derniers sont finis (car compacts et discrets), et sont des p-groupes (2.1.1) d'après la définition des p-filtrations (1.2.10).

(2.1.4) *Générateurs d'un groupe topologique, pro-p-groupes de type fini.* — Nous appellerons famille de *générateurs topologiques*, ou simplement famille de *générateurs*, une famille d'éléments $(x_i)_{i \in I}$ qui engendrent un *sous-groupe dense* dans un groupe topologique G.

Un groupe topologique, et en particulier un pro-p-groupe, sera dit de *type fini* s'il possède une *famille finie de générateurs.*

(2.1.5) *Remarque.* — Nous démontrerons plus loin (3.1.5) que tout pro-p-groupe de type fini peut être défini comme un groupe p-filtré. Il existe des groupes p-filtrés compacts qui ne sont pas de type fini : cf. par exemple (I, 3.1.5). Il existe aussi des pro-p-groupes dont la topologie ne peut pas être définie par une p-filtration (prendre un pro-p-groupe non métrisable).

(2.1.6) *Puissances p-adiques entières dans une limite projective de p-groupes.* — Soit G un groupe topologique, limite projective d'une famille de p-groupes topologiques séparés (2.1.1). Soient $x \in G$ et $\nu \in \mathbf{Z}_p$ un entier p-adique. Si $(n_i)_{i \in \mathbf{N}}$ est une suite d'entiers rationnels qui converge vers ν, la suite des puissances (x^{n_i}) converge dans G, car son image dans chaque p-groupe quotient de G est une suite stationnaire. La limite de la suite (x^{n_i}), pour $i \to \infty$, sera notée x^{ν} (« x puissance ν »). Les puissances p-adiques entières vérifient les mêmes identités que les puissances rationnelles entières.

(2.1.7) *Algèbres des p-groupes finis.*

Théorème. — *Soient* G *un p-groupe fini, et* $A = \mathbf{Z}_p[G]$ *son algèbre à coefficients entiers p-adiques. Notons* I *l'idéal d'augmentation de* A, *et* $R = I + (p)$ *l'idéal engendré par* I *et p. Alors* A *est un anneau local, dont le radical est* R. *La topologie* R*-adique de* A *et sa topologie de* $\mathbf{Z}_p$*-module libre de rang fini coïncident. L'anneau local* A *est compact.*

Preuve. — Réduisons A modulo p. L'algèbre A/pA s'identifie à l'algèbre de groupe $\mathbf{F}_p[G]$. Cette dernière est un anneau local artinien dont le radical I/pI est nilpotent ([25], chap. IX, § 1, corollaire, p. 147). Remontons dans A : il existe un entier $m \geqslant 1$ tel que $I^m \subset pI$. Pour tout $n \in \mathbf{N}$, nous avons donc $R^{mn} \subset p^n A$, ainsi que l'inclusion évidente $p^n A \subset R^n A$. La topologie R-adique de A est donc la topologie linéaire définie par les idéaux $p^n A$, c'est-à-dire la topologie de $\mathbf{Z}_p$-module libre de rang fini, pour laquelle A est compact. Le quotient A/R s'identifie au corps $\mathbf{F}_p$, et tout élément de la forme $1+x$, où $x \in \mathrm{R}$, est inversible dans A (puisque A est complet pour la topologie R-adique). Cela prouve que A est un anneau local de radical R.

(2.1.8) *Lemme. — Soient* G *un groupe discret,* $(x_j)_{j\in \mathrm{J}}$ *une famille de générateurs de* G, $\mathrm{A}=\Omega[\mathrm{G}]$ *l'algèbre de* G *à coefficients dans l'anneau commutatif* Ω, *et enfin* I *l'idéal d'augmentation de* A.

Alors I *est engendré, en tant qu'idéal à gauche, par les éléments* $(x_j - 1), j \in \mathrm{J}$.

Preuve. — L'idéal I est engendré, en tant que Ω-module, par les $y-1, y\in \mathrm{G}$. Nous écrivons y comme un produit de facteurs x_j ou x_j^{-1}; nous remplaçons x_j (resp. x_j^{-1}) par $(x_j-1)+1$ (resp. $1-x_j^{-1}(x_j-1)$), et nous développons.

(2.1.9) *Remarque.* — Le lemme (2.1.8) nous permettra de borner le nombre de générateurs du radical R dans l'énoncé du théorème (2.1.7). Ce théorème admet le complément suivant. Soit H le sous-groupe de Frattini de G, c'est-à-dire l'intersection de ses sous-groupes maximaux, ou encore le sous-groupe engendré par les commutateurs et les p-ièmes puissances. Alors G/H et I/RI sont *canoniquement isomorphes*. Leur dimension commune (en tant qu'espaces vectoriels sur $\mathbf{F}_p$) est le nombre minimum r de générateurs de G. Le nombre minimum de générateurs du radical R (en tant qu'idéal à gauche) est égal à la dimension de R/R^2, c'est-à-dire à $r+1$.

(2.2) Algèbres complétées des pro-p-groupes et $\mathbf{Z}_p$-modules complets.

(2.2.1) *Définition de la* $\mathbf{Z}_p$*-algèbre complétée d'un pro-p-groupe.* — Soit G un pro-p-groupe (2.1.2). A tout sous-groupe ouvert distingué U de G nous associons l'algèbre $\mathbf{Z}_p[\mathrm{G}/\mathrm{U}]$. Si $\mathrm{U}\subset\mathrm{U}'$, l'épimorphisme canonique $\mathrm{G}/\mathrm{U}\to\mathrm{G}/\mathrm{U}'$ se prolonge en un épimorphisme $f_{\mathrm{U}',\mathrm{U}}:\mathbf{Z}_p[\mathrm{G}/\mathrm{U}]\to\mathbf{Z}_p[\mathrm{G}/\mathrm{U}']$.

Nous appelons $\mathbf{Z}_p$*-algèbre complétée* de G, et nous notons $\mathbf{Z}_p[[\mathrm{G}]]$ ou Al G la limite projective $\varprojlim \mathbf{Z}_p[\mathrm{G}/\mathrm{U}]$, construite pour les morphismes $f_{\mathrm{U}',\mathrm{U}}$ sur l'ensemble des sous-groupes distingués ouverts de G ordonnés par anti-inclusion. L'algèbre Al G est munie de sa topologie de limite projective, les algèbres $\mathbf{Z}_p[\mathrm{G}/\mathrm{U}]$ ayant leur topologie de $\mathbf{Z}_p$-module libre de rang fini.

(2.2.2) *Théorème. — Soit* G *un pro-p-groupe. Son algèbre complétée* Al G *est un anneau local et une* $\mathbf{Z}_p$*-algèbre topologique compacte. Les idéaux ouverts de* Al G *constituent un système fondamental de voisinages de zéro. Si* R *désigne le radical de* Al G, *la topologie* R*-adique est plus fine que la topologie de* Al G, *ce qui signifie que tout voisinage de zéro contient* R^n *à partir d'une certaine valeur de* $n\in\mathbf{N}$. *Si* G *est de type fini* (2.1.4) *la topologie de* Al G *est sa topologie* R*-adique. Enfin il existe une injection canonique de* $\mathbf{Z}_p[\mathrm{G}]$ *sur une sous-algèbre dense de* Al G *(ce qui justifie le nom d'algèbre de groupe complétée), et la restriction de cette injection à* G *est un homéomorphisme de* G *sur son image.*

(2.2.3) *Preuve.* — Nous avons à prendre une limite projective d'*espaces compacts* pour une famille *d'épimorphismes*. Nous obtenons donc un *anneau compact* Al G, et les morphismes $\mathrm{Al\,G}\to\mathbf{Z}_p[\mathrm{G}/\mathrm{U}]$ sont surjectifs.

Les images réciproques dans Al G des idéaux ouverts de $\mathbf{Z}_p[G/U]$ constituent (lorsque U varie) un système fondamental de voisinages de zéro.

D'autre part une limite projective *d'anneaux locaux* pour une famille d'*épimorphismes* est encore un *anneau local*, et le radical de la limite projective est la limite projective des radicaux.

Chaque épimorphisme $G \to G/U$ se prolonge en un morphisme $\mathbf{Z}_p[G] \to \mathbf{Z}_p[G/U]$, d'où un homomorphisme

(2.2.3.1) $$\mathbf{Z}_p[G] \to \mathrm{Al}\, G.$$

Cet homomorphisme est *injectif*. En effet, si $\sum_{g \in G} \lambda_g . g \in \mathbf{Z}_p[G]$ est un élément de $\mathbf{Z}_p[G]$, nous pouvons choisir U assez petit pour que les éléments $g \in G$ dont les coefficients $\lambda_g \in \mathbf{Z}_p$ sont non nuls aient des images distinctes modulo U. L'élément considéré possède alors une image non nulle dans $\mathbf{Z}_p[G/U]$ et, par conséquent, dans Al G. La restriction de l'homomorphisme (2.2.3.1) à G est continue et injective : c'est donc un homéomorphisme sur l'image, car G est compact et Al G séparé.

L'image de $\mathbf{Z}_p[G]$ dans Al G est dense, parce que, pour chaque U, le morphisme composé $\mathbf{Z}_p[G] \to \mathbf{Z}_p[G/U]$ est surjectif.

Si R est le radical de Al G, l'image de R^n dans $\mathbf{Z}_p[G/U]$ est, pour chaque n et chaque U, la puissance n-ième du radical de $\mathbf{Z}_p[G/U]$. D'après (2.1.7), il en résulte que R^n tend vers zéro dans Al G.

Supposons enfin que G admette les générateurs x_i, $1 \leqslant i \leqslant r$. Cela signifie (2.1.4) que les images dans G/U des x_i engendrent ce groupe discret. Convenons de poser, dans Al G, $x_{r+1} = p+1$. Le radical de $\mathbf{Z}_p[G/U]$ est ainsi (2.1.8) l'idéal à gauche engendré par les images des $x_i - 1$, pour $1 \leqslant i \leqslant r+1$. L'idéal à gauche engendré par les $x_i - 1$ dans Al G est donc dense dans R. Cet idéal est d'autre part compact, comme image continue du compact $(\mathrm{Al}\, G)^{r+1}$ par l'application

$$(y_1, \ldots, y_{r+1}) \mapsto \sum_{1 \leqslant i \leqslant r+1} y_i(x_i - 1),$$

et il coïncide donc avec R.

Nous démontrons plus généralement que, pour tout $n \in \mathbf{N}$, l'idéal R^n est engendré, comme idéal à gauche, par les éléments $(x_{i_1} - 1) \ldots (x_{i_n} - 1)$. Les puissances de R sont donc *compactes*, et *d'indice fini* dans Al G (parce que Al G/R est fini). Les puissances de R sont donc *ouvertes* dans Al G, ce qui prouve que la topologie de Al G est sa topologie p-adique.

(2.2.3.2) *Nous identifierons désormais* G *et* $\mathbf{Z}_p[G]$ *à leurs images canoniques dans* Al G.

(2.2.4) *Définition de la catégorie* $\mathcal{C}$ *des* $\mathbf{Z}_p$*-modules complets.* — Nous appellerons $\mathbf{Z}_p$*-module complet une limite projective* M *de p-groupes discrets commutatifs, notée additivement* (rappelons (2.1.1) que ces p-groupes ne sont pas nécessairement finis). Nous avons défini en (2.1.6) les puissances p-adiques dans une limite projective de p-groupes, notée multiplicativement. En *notation additive*, nous obtenons une multiplication des éléments de M par les entiers p-adiques, et, plus précisément, *une structure de* $\mathbf{Z}_p$*-module sur* M. L'application $\mathbf{Z}_p \times M \to M$ est *continue*, M est *complet* et ses *sous-modules ouverts* forment un système fondamental de voisinages de zéro.

Réciproquement, si M est un $\mathbf{Z}_p$*-module topologique complet et linéairement topologisé* (c'est-à-dire dont les sous-modules ouverts forment un système fondamental de voisinages de zéro), le quotient M/M_i de M par un sous-module ouvert est un p-groupe additif discret, et M *s'identifie à la limite projective* $\varprojlim M/M_i$ *de ses quotients discrets.*

Nous achevons de définir la catégorie $\mathcal{C}$ en convenant que les *morphismes* sont les *homomorphismes continus*. Ils sont nécessairement $\mathbf{Z}_p$-linéaires.

Exemples :

(2.2.4.1) L'algèbre complétée Al G d'un pro-p-groupe G est un $\mathbf{Z}_p$-module complet (2.2.2).

(2.2.4.2) Les $\mathbf{Z}_p$-modules complets *discrets* sont les *p-groupes additifs discrets* (ou groupes abéliens de *p-torsion*).

(2.2.5) *Lemme.* — *Soient* G *un pro-p-groupe* (2.1.2) *et* M *un* $\mathbf{Z}_p$*-module complet* (2.2.4). *Alors toute application continue* $f: G \to M$ *se prolonge en un morphisme* (2.2.4) *et un seul* $g: \mathrm{Al}\, G \to M$.

Preuve. — L'application continue f de l'espace compact G dans l'espace uniforme M est *uniformément continue*. Autrement dit, à tout sous-module ouvert M_i de M nous pouvons associer un sous-groupe ouvert distingué U de G, de telle sorte que $x \in G, y \in G$ et $x^{-1}y \in U$ impliquent $f(x) - f(y) \in M_i$. Nous obtenons donc, par passage aux quotients, une application de G/U dans M/M_i.

Cette application s'étend en une application $\mathbf{Z}_p$-linéaire de $\mathbf{Z}_p[G/U]$ dans M/M_i, et, par composition, donne une application continue de Al G dans M/M_i. Cette dernière application ne dépend pas du choix de U.

La famille d'applications continues de Al G dans les M/M_i définit l'application continue cherchée $g: \mathrm{Al}\, G \to M$, le module M s'identifiant à $\varprojlim M/M_i$ (2.2.4).

Comme $\mathbf{Z}_p[G]$ est dense dans Al G, le prolongement linéaire continu de f est unique.

Enfin si f prend ses valeurs dans un sous-module fermé N de M, il en est de même de g.

(2.2.6) *Théorème.* — *Soient* G *un pro-p-groupe et* M *un* $\mathbf{Z}_p$*-module complet. Toute structure de* G*-module (à gauche) topologique sur* M *s'obtient par restriction à partir d'une structure de* Al G*-module topologique, linéairement topologisé, et d'une seule.*

Preuve. — Nous avons, par définition, une application continue $f: G \times M \to M$. Fixons $m \in M$; d'après le lemme (2.2.5), l'application continue $x \mapsto f(x, m)$ de G dans M se prolonge en un morphisme unique de Al G dans M, que nous notons $y \mapsto g(y, m)$, y parcourant Al G. L'unicité du prolongement (2.2.5) nous permet de démontrer que l'application de $(\mathrm{Al}\, G) \times M$ dans M, donnée par $(y, m) \mapsto g(y, m)$, définit sur M une structure de Al G-module.

Comme G est compact, nous pouvons associer à tout sous-module ouvert M_i de M un sous-module ouvert M_j, de telle sorte que $f(x, m) \in M_i$ pour tout $x \in G$ et tout $m \in M_j$. Nous en déduisons que $g(y, m) \in M_i$ pour tout $y \in \mathrm{Al}\, G$ et tout $m \in M_j$. Cette propriété, jointe à la continuité des applications partielles $y \mapsto g(y, m)$, entraîne la continuité de l'application bilinéaire g, et montre que la topologie de M est définie par ses sous-Al G-modules ouverts.

L'unicité de g résulte de l'unicité du prolongement de f à $(\mathbf{Z}_p[G]) \times M$, qui est dense dans $(\mathrm{Al}\, G) \times M$.

(2.2.7) *Propriétés fonctorielles de* Al. — Soit $f : G \to H$ un *morphisme de pro-p-groupes* (2.1.2). Alors f se prolonge en un homomorphisme d'algèbres $\mathbf{Z}_p[G] \to \mathbf{Z}_p[H]$, puis, par passage aux complétés, en un homomorphisme

(2.2.7.1) $$\mathrm{Al} f : \mathrm{Al}\, G \to \mathrm{Al}\, H.$$

Considérons, en particulier, un sous-groupe ouvert U de G, et notons i l'injection de U dans G. Alors *l'homomorphisme* $\mathrm{Al}\, i : \mathrm{Al}\, U \to \mathrm{Al}\, G$ *est injectif*, et Al G *est un* Al U-*module libre de rang* $(G : U)$.

En effet, pour construire Al G et Al U, nous pouvons utiliser les sous-groupes distingués ouverts U' de G qui sont contenus dans U. Nous obtenons Al G et Al U comme limites projectives de $\mathbf{Z}_p[G/U']$ et $\mathbf{Z}_p[U/U']$ respectivement. Un système de représentants des classes à droite de G suivant U constitue une base du Al U-module à gauche Al G.

(2.2.8) *Proposition. — Soient* G *et* H *deux pro-p-groupes. Alors la* $\mathbf{Z}_p$*-algèbre complétée de leur produit* $G \times H$ *s'identifie au produit tensoriel complété* (I, 3.2.9) *des algèbres* Al G *et* Al H :

$$\mathrm{Al}(G \times H) = \mathrm{Al}\, G \hat{\otimes} \mathrm{Al}\, H.$$

Preuve. — Lorsque G et H sont finis, l'identification s'obtient en écrivant $g \otimes h$ l'élément $(g, h) \in G \times H$. Nous passons au cas général en appliquant la proposition (I, 3.2.11).

3. FILTRATIONS DE PRO-p-GROUPES

(3.1) Pro-p-groupes libres de type fini.

(3.1.1) *Pro-p-groupes libres de type fini.* — Les pro-p-groupes libres sont définis généralement dans [29], Chap. Ier, 1.5. Nous n'utiliserons que des pro-p-groupes libres de type fini (2.1.4) dont voici une définition. *Le pro-p-groupe* G *est dit libre pour la famille d'éléments* x_i, $1 \leqslant i \leqslant r$, *si pour tout pro-p-groupe* H *et toute famille* $(y_i)_{1 \leqslant i \leqslant r}$ *d'éléments de* H *il existe un morphisme* $f : G \to H$, *et un seul, qui applique chaque* x_i *sur* y_i. La propriété universelle implique que les x_i *sont des générateurs* (2.1.4) de G.

Si les y_i sont des générateurs de H, alors le morphisme $f : G \to H$ est un *morphisme strict surjectif*, parce que G est compact.

Pour obtenir le pro-p-groupe libre engendré par les x_i, nous construisons d'abord le *groupe « abstrait »* libre engendré par les x_i, puis nous le *complétons* pour sa p-topologie (les sous-groupes d'indice égal à une puissance de p forment un système fondamental de voisinages de l'unité). Comme nous ne complétons que des groupes séparés, nous devons vérifier que la p-topologie d'un groupe libre de type fini est séparé : cf. (3.1.3).

(3.1.2) *Lemme. — Soit* G *un groupe p-filtré* (1.2.10) *admettant les générateurs* x_i, $1 \leqslant i \leqslant r$. *Alors les groupes quotients* G/G_ν (1.1.2) *sont finis. Si* G *est séparé (resp. complet) il est précompact (resp. compact).*

Preuve. — Soit t le minimum des $\omega(x_i)$. Donnons-nous $\nu \in \mathbf{R}_+^*$; définissons n comme la partie entière de ν/t et h comme le plus petit entier tel que $\varphi^h(t) \geqslant \nu$ (où φ^h désigne le h-ième itéré de la fonction φ (1.2.2)). Alors les puissances p^h-ièmes et les commutateurs de poids $n+1$ sont égaux à 1 dans le quotient G/G_ν, engendré par les images de $x_1, \ldots, x_r$. Si nous filtrons G/G_ν par sa suite centrale descendante, son gradué associé est une $(\mathbf{Z}/p^h\mathbf{Z})$-algèbre de Lie à r générateurs, nilpotente de classe $\leqslant n$; cette algèbre de Lie est donc finie, ainsi que G/G_ν; cf. [14], th. (2.5).

(3.1.3) *Valuations d'algèbres de Magnus.* — Donnons-nous r lettres $X_1, \ldots, X_r$ et r nombres réels strictement positifs $\tau_1, \ldots, \tau_r$. Construisons l'algèbre de Magnus A (1.1.10) engendrée par les X_i, à coefficients dans $\mathbf{Z}_p$. C'est l'algèbre des séries formelles associatives en les X_i (non commutatives si $r \geqslant 2$).

Munissons $\mathbf{Z}_p$ de sa filtration naturelle $(v(p)=1)$, et la $\mathbf{Z}_p$*-algèbre* A de la *borne inférieure* (I, 2.1.6) *des filtrations w pour lesquelles* $w(X_i) \geqslant \tau_i$ $(1 \leqslant i \leqslant r)$.

Cette filtration est une *valuation.* Pour tout monôme $m = X_{i_1} \ldots X_{i_n}$, nous avons $w(m) = \tau_{i_1} + \ldots + \tau_{i_n}$ et les monômes constituent une *base topologique* de A (I, 2.1.17). L'algèbre A est valuée en tant qu'anneau (I, 2.2.1).

La topologie de A *ne dépend pas du choix des* τ_i : c'est la topologie de la *convergence simple* des coefficients des séries formelles associatives en les X_i. L'algèbre A est *compacte.*

Le groupe $\mathscr{F}$ engendré dans A par les éléments $X_i^* = 1 + X_i$ est *libre pour ces générateurs* (1.1.10).

La filtration de A induit sur $\mathscr{F}$ une p-filtration (1.2.1) séparée (puisque A est séparé). D'après le lemme (3.1.2), *la p-topologie du groupe libre $\mathscr{F}$ est séparée.*

(3.1.4) *Proposition. — Conservons les notations de* (3.1.3). *L'adhérence $\overline{\mathscr{F}}$ du groupe libre $\mathscr{F}$ dans l'algèbre de Magnus* A *est un pro-p-groupe libre pour les générateurs* X_i^*, *et* A *s'identifie à la $\mathbf{Z}_p$-algèbre complétée* $\mathrm{Al}\,\overline{\mathscr{F}}$ *du pro-p-groupe* $\overline{\mathscr{F}}$ (2.2.1).

Preuve. — Construisons le pro-p-groupe G, libre pour les générateurs $x_1, \ldots, x_r$, et son algèbre complétée $\mathrm{Al}\,G = B$. Nous avons, par définition de G, un morphisme $f : G \to \overline{\mathscr{F}}$ vérifiant $f(x_i) = X_i^*$ pour tout i, qui, d'après le théorème (2.2.6), se prolonge en un morphisme $\alpha : B \to A$. La définition du *morphisme réciproque* $\beta : A \to B$ (vérifiant $\beta(X_i) = x_i - 1$ pour tout i) s'obtient à partir du théorème (2.2.2) : les images par β des monômes en les X_i tendent vers zéro. Nous retrouvons la proposition 7 de [29], chap. I^er^, 1.5.

(3.1.5) *Corollaire. — La topologie d'un pro-p-groupe de type fini peut être définie par une p-filtration.*

Preuve. — Soit H un pro-p-groupe de générateurs y_i, $1 \leqslant i \leqslant r$. D'après (3.1.1) et (3.1.4), nous pouvons considérer H comme le quotient (topologique) du pro-p-groupe libre $\bar{\bar{\mathscr{F}}}$ engendré par les $1+X_i$ dans l'algèbre de Magnus valué A (3.1.3). Le groupe $\bar{\bar{\mathscr{F}}}$ est p-filtré, et la topologie de H est définie par sa *filtration quotient* (1.4.1). Cette filtration quotient est une p-filtration, qui ne dépend que du choix des générateurs y_i et des nombres τ_i. Nous en donnerons une caractérisation directe.

(3.2) Les (t, p)-filtrations et les (x, τ, p)-filtrations.

(3.2.1) *Définition. — Soient* G *un groupe discret et t un nombre strictement positif. Nous appellerons (t, p)-filtration de* G *la borne inférieure des p-filtrations* ω *vérifiant* $\omega(x) \geqslant t$ *pour tout* $x \in G$.

La condition d'existence d'une borne inférieure (1.1.4) est vérifiée, car $t > 0$, et la (t, p)-filtration est une p-filtration (1.2.10).

Si $f: G \to H$ est un homomorphisme de groupes munis tous deux de leur (t, p)-filtration, alors f est un morphisme de groupes filtrés (1.1.3). En particulier les sous-groupes G_ν correspondant à la (t, p)-filtration de G sont *complètement invariants* dans G.

(3.2.2) *Définition. — Soient* G *un groupe discret,* (x_i) *une famille de générateurs de* G *et* (τ_i) *une famille de nombres strictement positifs* $(1 \leqslant i \leqslant r)$. *Nous appellerons* (x, τ, p)*-filtration de* G *la borne inférieure des p-filtrations* ω *qui vérifient*

(3.2.2.1) $$\omega(x_i) \geqslant \tau_i \quad \textit{pour} \quad 1 \leqslant i \leqslant r.$$

Nous pourrions donner la définition des (x, τ, p)-filtrations pour une famille de générateurs $(x_i)_{i \in I}$, non nécessairement finie, mais cette généralisation ne nous serait pas utile (et surtout la proposition (3.2.4) ne serait plus nécessairement vraie).

Si tous les τ_i sont égaux à un même nombre t, la (x, τ, p)-filtration coïncide avec la (t, p)-filtration.

(3.2.3) Considérons le groupe G de générateurs (x_i) comme le quotient du *groupe libre* $\mathscr{F}$ de générateurs (X_i^*) par l'épimorphisme f qui applique X_i^* sur x_i $(1 \leqslant i \leqslant r)$. Alors *la* (x, τ, p)*-filtration de* G *est la filtration quotient* (1.1.4) *de la* (X^*, τ, p)*-filtration* de $\mathscr{F}$. De même, la (t, p)-filtration de G est la filtration quotient de la (t, p)-filtration de $\mathscr{F}$.

(3.2.4) *Proposition. — Munissons le groupe* G *de sa* (x, τ, p)*-filtration* ω, *comme en* (3.2.2). *Alors* gr G *est une algèbre de Lie mixte* (1.2.11) *qui est engendrée par les images respectives des* x_i *dans* $\mathrm{gr}_{\tau_i} G$, *pour* $1 \leqslant i \leqslant r$.

La preuve de cette proposition sera donnée en (3.3.2).

(3.2.5) *Théorème. — Soient* G *un groupe engendré, en tant que groupe discret, par les générateurs* x_i, ω *une p-filtration de* G *et* (τ_i) *une famille de nombres réels strictement positifs tels que* $\omega(x_i) \geqslant \tau_i$ $(1 \leqslant i \leqslant r)$. *Notons* ξ_i *l'image de* x_i *dans* $\mathrm{gr}_{\tau_i} G$. *Alors les deux assertions suivantes sont équivalentes.*

(3.2.5.1) *Les* ξ_i *engendrent dans* gr G *une sous-algèbre de Lie mixte libre* $(1 \leqslant i \leqslant r)$.

(3.2.5.2) *Le groupe* G *est libre pour les générateurs* x_i *et* ω *est sa* (x, τ, p)*-filtration.*

De plus, la (x, τ, p)*-filtration d'un groupe libre de générateurs* x_i *est séparée.*

Preuve. — Soient $\mathscr{F}$ un groupe libre pour les générateurs X_i^*, et $f:\mathscr{F}\to G$ l'épimorphisme défini par $f(X_i^*)=x_i$. Munissons $\mathscr{F}$ de sa (X^*,τ,p)-filtration. Alors f est un morphisme (1.1.3), d'après les relations $\omega(x_i)\geqslant\tau_i$. Le gradué associé $\mathrm{gr} f$ est un morphisme d'algèbres de Lie mixtes (1.2.11). D'après la proposition (3.2.4), $\mathrm{gr}\,\mathscr{F}$ est engendrée par les images respectives des X_i^* dans $\mathrm{gr}_{\tau_i}\mathscr{F}$, que $\mathrm{gr} f$ applique sur les ξ_i.

Si (3.2.5.1) est vrai, le morphisme $\mathrm{gr} f$ est donc *injectif*, par définition d'une algèbre libre.

Prenons d'abord pour G le groupe $\mathscr{F}$ lui-même, ω étant la p-filtration de $\mathscr{F}$ définie en (3.1.3) (induite par une valuation de l'algèbre de Magnus). D'après (1.1.9), (1.2.9) et la définition de ω, la relation (3.2.5.1) est vérifiée.

Le morphisme f est l'identité. L'assertion « $\mathrm{gr} f$ est injectif » signifie que ω est la (X^*,τ,p)-filtration de $\mathscr{F}$; cette filtration est donc séparée.

Revenons au cas général. Puisque la (X^*,τ,p)-filtration est séparée, f est une isométrie dès que $\mathrm{gr} f$ est injectif, ce qui prouve que (3.2.5.1) implique (3.2.5.2). Nous avons démontré au passage l'implication réciproque.

(3.2.6) *Détermination de la (t,p)-filtration d'un groupe libre.* — Le théorème (3.2.5) nous permet d'obtenir la (t,p)-filtration d'un groupe libre à partir d'une valuation de l'algèbre de Magnus A (3.1.3).

Nous allons appliquer le théorème (5.4) du chap. Ier de [14]. L'expression « p-filtration » est employée dans [14], chap. Ier, § 5, pour désigner certaines filtrations d'une algèbre de Magnus, tandis que nous l'utilisons exclusivement dans le présent article au sens défini en (1.2.10). D'autre part les seules filtrations qui apparaissent dans [14] sont à valeurs entières, tandis que nous étudions maintenant des filtrations à valeurs réelles. Cependant, le théorème (5.4) de [14], chap. Ier, est applicable à la détermination de la (t,p)-filtration, en prenant la fonction F définie par $F(i,j)=ti+j$. Lorsque t est *rationnel*, nous sommes ramenés aux filtrations entières en multipliant toutes les filtrations par un entier n tel que $tn\in\mathbf{N}$. Si, par contre, t est irrationnel, il faut reprendre la preuve du théorème (5.4), ou utiliser un passage à la limite. Voici, en tout cas, l'énoncé qu'on obtient.

(3.2.6.1) *Soit $\mathscr{F}$ un groupe libre. Notons $\mathscr{F}_i$ le i-ième sous-groupe de la suite centrale descendante de $\mathscr{F}$, avec $\mathscr{F}_1=\mathscr{F}$. Disons qu'un élément $x\in\mathscr{F}_i$ est primitif si l'image de x dans $\mathscr{F}_i/\mathscr{F}_{i+1}$ n'est pas divisible par p dans ce dernier groupe. Notons enfin φ^k le k-ième itéré de la fonction φ (1.2.2) : $\varphi^0(\nu)=\nu$ et $\varphi^{k+1}(\nu)=\varphi(\varphi^k(\nu))$. Alors, si ω est la (t,p)-filtration de $\mathscr{F}$, si x est un élément primitif de $\mathscr{F}_i$, et $k\in\mathbf{N}$, nous avons*

$$\omega(x^{p^k})=\varphi^k(ti).$$

(3.2.6.2) *Si un élément $x\in\mathscr{F}$ est représenté par un produit ordonné $\Pi_i x_i^{p^{k_i}}$, où chaque x_i est un élément primitif de $\mathscr{F}_i$ (et $k_i\in\mathbf{N}$ ou $k_i=\infty$, auquel cas $x_i^{p^\infty}=1$), alors*

$$\omega(x)=\inf_i\omega(x_i^{p^{k_i}})=\inf_i\varphi^{k_i}(ti).$$

(3.2.6.3) En particulier, pour $t=1$, nous retrouvons un résultat de [14], chap. Ier, (5.8) : *si* ω *est la* $(1,p)$*-filtration du groupe libre* $\mathcal{F}$, *alors* $\omega(x)\geqslant i$ *équivaut à*

$$x\in\mathcal{F}_1^{p^{i-1}}\ldots\mathcal{F}_j^{p^{i-j}}\ldots\mathcal{F}_i.$$

(3.2.7) *Détermination de la* (x,τ,p)*-filtration d'un groupe libre : exercice.* — Le calcul « effectif » de la (x,τ,p)-filtration d'un groupe libre est plus compliqué que celui d'une (t,p)-filtration, parce que les générateurs interviennent individuellement. Nous nous contenterons de proposer comme exercice l'exemple suivant. Reprenons les notations de (1.4) et prenons la borne inférieure ω des p-filtrations du groupe libre $\mathcal{F}$ pour lesquelles $\omega(X^*)\geqslant\tau$ et $\omega(Y^*)\geqslant\theta$. Alors, si $U\in\mathcal{F}$ est donné par le développement (1.4.2.10), nous avons

(3.2.7.1) $$\omega(U)=\inf_i\omega(U_i^{c_i(U)})$$

(3.2.7.2) $$\omega(U_i^{c_i(U)})=\varphi^{k_i}(\omega(U_i)),\quad \text{où}$$

(3.2.7.3) $$k_i=v(c_i(U))\qquad\text{(valuation } p\text{-adique).}$$

(3.2.7.4) $$\omega(U_i)=\tau.\deg_X u_i+\theta.\deg_Y u_i.$$

(3.2.8) *Définition des* (t,p)*-filtrations et des* (x,τ,p)*-filtrations des pro-p-groupes de type fini.* — Les définitions données en (3.2.1) et (3.2.2) concernaient des groupes discrets, bien que les filtrations introduites correspondent, en général, à des topologies non discrètes. Pour un groupe libre de type fini $\mathcal{F}$, par exemple, toutes les filtrations définies en (3.2.1) et (3.2.2) correspondent à la p-topologie de $\mathcal{F}$.

Définissons maintenant les (t,p)-filtrations et les (X^*,τ,p)-filtrations d'un *pro-p-groupe libre* pour la famille de générateurs $(X_i^*)_{1\leqslant i\leqslant r}$ (3.1). Nous plongeons le pro-p-groupe libre $\overline{\overline{\mathcal{F}}}$ dans *l'algèbre de Magnus* A comme en (3.1.4), et nous valuons A comme en (3.1.3), par la borne inférieure w des filtrations qui vérifient $w(X_i)\geqslant\tau_i$ pour $1\leqslant i\leqslant r$ (resp. $w(X_i)\geqslant t$ s'il s'agit de la (t,p)-filtration).

La (X^*,τ,p)-filtration (resp. (t,p)-filtration) de $\overline{\overline{\mathcal{F}}}$ est, par définition, induite par la valuation w de A (1.1.10).

Soit maintenant G un *pro-p-groupe de générateurs (topologiques)* $(x_i)_{1\leqslant i\leqslant r}$. Nous considérons G comme le quotient de $\overline{\overline{\mathcal{F}}}$ par l'épimorphisme qui applique X_i^* sur x_i, et nous *définissons la* (x,τ,p)*-filtration de* G *comme le quotient de la* (X^*,τ,p)*-filtration de* $\overline{\overline{\mathcal{F}}}$ (1.1.4). D'après (3.1.5), cette filtration de G définit sa topologie. Nous pouvons aussi en donner la définition directe suivante.

(3.2.8.1) *La* (x,τ,p)*-filtration (resp. la* (t,p)*-filtration) du pro-p-groupe* G *de générateurs* $(x_i)_{1\leqslant i\leqslant r}$ *est la borne inférieure des p-filtrations qui définissent la topologie de* G *et qui vérifient* $\omega(x_i)\geqslant\tau_i$ *(resp.* $\omega(x_i)\geqslant t$*) pour* $1\leqslant i\leqslant r$.

Dans cette définition, la condition que ω définit la topologie de G peut être remplacée par la condition suivante : *les sous-groupes* G_ν *associés à la p-filtration* ω *doivent* *être fermés* (pour la topologie de G). Ces sous-groupes G_ν sont les *adhérences* de sous-groupes formés par certains mots en les générateurs x_i ; la description de ces mots n'est malheureusement pas très simple dans le cas général : cf. (3.2.7).

Rappelons que la (X^*, τ, p)-filtration du pro-p-groupe libre de type fini $\bar{\bar{\mathscr{F}}}$ est discrète (1.1.5). Il en est donc de même de la (x, τ, p)-filtration du pro-p-groupe G et le morphisme $\mathrm{gr}\,\bar{\bar{\mathscr{F}}} \to \mathrm{gr}\, G$ est surjectif. Nous avons donc, d'après (3.2.5) la propriété suivante.

(3.2.8.2) *Si le pro-p-groupe de type fini* G *est muni de sa* (x, τ, p)*-filtration, l'algèbre de Lie mixte* gr G *est engendrée par les images des générateurs* x_i *dans* $\mathrm{gr}_{\tau_i} G$.

(3.2.9) *Un exemple.* — Soient A l'algèbre de Magnus engendrée sur **Z** par les $(X_i)_{1 \leqslant i \leqslant r}$, et f un entier $\geqslant 1$. Considérons dans A l'idéal I engendré par les X_i et par p^f. Filtrons A par les puissances de I, c'est-à-dire posons, pour $x \in A$ et $n \in \mathbf{N}$,

(3.2.9.1) $$w(x) \geqslant n \Leftrightarrow x \in I^n.$$

Cette filtration w de A induit une filtration ω sur le groupe libre $\mathscr{F}$ de générateurs $X_i^* = 1 + X_i$ (1.1.10). La filtration ω est celle définie en [27], n° 6. Ce n'est pas une p-filtration (sauf si $f = 1$), mais nous pouvons l'obtenir comme suit.

Notons ω' la (f, p)-filtration de $\mathscr{F}$ (3.2.1), (3.2.5). La filtration ω se déduit de ω' par les procédés (1.1.11.4) et (1.1.11.6). Plus précisément :

(3.2.9.2) $$\omega(x) = [f^{-1}\omega'(x)] \qquad \text{pour tout } x \in G.$$

(3.3) Preuve de (3.2.4), et d'une propriété des algèbres de Lie mixtes.

(3.3.1) *Lemme.* — *Soient* G *un groupe discret muni de sa* (x, τ, p)*-filtration* ω, *comme en* (3.2.2), *et* ν *un nombre* >0. *Désignons par* H *le sous-groupe de* G *engendré par les éléments des trois types suivants : les générateurs* x_i *pour lesquels* $\tau_i > \nu$; *les puissances p-ièmes* y^p *pour lesquelles* $y \in G$, $\varphi(\omega(y)) > \nu$; *les commutateurs* (y, z), *où* $y \in G$, $z \in G$, $\omega(y) + \omega(z) > \nu$. *Alors* H *coïncide avec le sous-groupe* G_{ν^+}, *défini par* ω *comme en* (1.1.2).

Preuve. — Nous avons d'abord l'inclusion $H \subset G_{\nu^+}$. Définissons une famille de sous-groupes G'_λ, $\lambda \in \mathbf{R}_+^*$, en posant

(3.3.1.1) $$G'_\lambda = G_\lambda \qquad \text{si } \lambda \leqslant \nu ;$$

(3.3.1.2) $$G'_\lambda = G_\lambda \cap H \qquad \text{si } \lambda > \nu.$$

Les sous-groupes G'_λ vérifient les relations

(3.3.1.3) $$G'_\lambda = \bigcap_{\lambda' < \lambda} G'_{\lambda'} \qquad (\textit{pour } \lambda \in \mathbf{R}_+^*) ;$$

(3.3.1.4) $$(G'_\lambda, G'_\mu) \subset G'_{\lambda+\mu} \qquad (\textit{pour } \lambda, \mu \in \mathbf{R}_+^*) ;$$

(3.3.1.5) $$y^p \in G'_{\varphi(\lambda)} \qquad \textit{pour } \lambda \in \mathbf{R}_+^* \textit{ et } y \in G'_\lambda ;$$

(3.3.1.6) $$x_i \in G'_\tau \qquad \textit{pour } 1 \leqslant i \leqslant r.$$

Ces relations signifient que les G'_λ sont associés à une p-filtration ω' de G, pour laquelle $\omega'(x_i) \geqslant \tau_i$, $1 \leqslant i \leqslant r$. Comme $\omega'(y) \leqslant \omega(y)$ pour tout $y \in G$ nous avons $\omega(y) = \omega'(y)$, d'après la définition de ω comme borne inférieure d'une famille de filtrations. Nous en déduisons l'inclusion $G_{\nu^+} \subset H$, qui achève la preuve du lemme. Remarquons que nous n'avons pas utilisé la finitude de la famille de générateurs (x_i), $1 \leqslant i \leqslant r$.

(3.3.2) *Proposition. — Soient* G *un groupe discret et* ω *la* (x, τ, p)*-filtration de* G, *comme en* (3.2.2). *Désignons par* I *la plus petite partie de* $\mathbf{R}_+^*$ *qui contient les* τ_i *pour* $1 \leqslant i \leqslant r$, *et qui vérifie* $\lambda + \mu \in I$ *pour* $\lambda, \mu \in I$, *ainsi que* $\varphi(\lambda) \in I$ *pour* $\lambda \in I$. *Alors les degrés des composantes homogènes non nulles de* gr G *appartiennent à* I, *et l'algèbre de Lie mixte* gr G *est engendrée par les images respectives dans* $\mathrm{gr}_{\tau_i} G$ *des générateurs* x_i.

Preuve. — L'ensemble I est une *partie discrète* de $\mathbf{R}_+^*$, et nous pouvons écrire ses éléments comme une suite strictement croissante :

(3.3.2.1) $$\nu_0 < \nu_1 < \dots$$

Appelons L la sous-algèbre de Lie mixte de gr G engendrée par les images ξ_i des x_i dans $\mathrm{gr}_{\tau_i} G$, et notons L_λ la composante homogène de degré λ de L, pour tout $\lambda \in \mathbf{R}_+^*$. La définition des algèbres de Lie mixtes (1.2.5) nous montre que $L_\lambda = 0$ pour $\lambda \notin I$.

Considérons l'hypothèse de récurrence (en $i \in \mathbf{N}$)

(3.3.2.2) $$L_\lambda = \mathrm{gr}_\lambda G \quad \text{pour tout } \lambda \leqslant \nu_i.$$

Elle est vérifiée pour $i = 0$, car ν_0 est le plus petit des nombres τ_i $(1 \leqslant i \leqslant r)$, et $G_{\nu_0} = G$.

Supposons la relation (3.3.2.2) vérifiée pour un certain $i \in \mathbf{N}$. Appliquons le lemme (3.3.1) à la détermination des sous-groupes $G_{\nu_i^+}$. Nous voyons que

(3.3.2.3) $$G_{\nu_i^+} = G_{\nu_{i+1}},$$

ce qui implique $\mathrm{gr}_\lambda G = 0$ pour $\nu_i < \lambda < \nu_{i+1}$, et, de plus,

(3.3.2.4) $$\mathrm{gr}_{\nu_{i+1}} G = L_{\nu_{i+1}}.$$

Nous venons de démontrer la proposition (3.2.4). Nous avons utilisé essentiellement le fait que la famille de générateurs (x_i) est finie.

(3.3.3) *Lemme. — Soient* Ω *un anneau commutatif et* L *une* Ω*-algèbre de Lie engendrée par la famille* (x_i), $i \in I$. *Alors* L *est engendrée, en tant que* Ω*-module, par les éléments* x_i *et* $[y, x_i]$, *où* $i \in I$, $y \in L$.

Preuve. — L'algèbre L est engendrée, en tant que Ω-module, par les *monômes de Lie* en les x_i. Grâce à l'identité de Jacobi, que nous écrivons sous la forme

(3.3.3.1) $$[u, [v, w]] = [[u, v], w] - [[u, w], v],$$

nous voyons qu'il suffit de prendre comme générateurs du Ω-module L les monômes « normés à droite » ainsi définis : les x_i eux-mêmes sont normés à droite, et le monôme $[u, x_i]$ est normé à droite si le monôme u l'est aussi.

(3.3.4) *Lemme.* — *Soient* L *une algèbre de Lie restreinte (au sens de Jacobson) engendrée par une famille* (x_i), $i \in \mathrm{I}$, *sur un anneau commutatif* Ω *de caractéristique* p, *et* L^* *la sous-algèbre de Lie engendrée sur* Ω *par les* x_i *pour* $i \in \mathrm{I}$. *Alors nous avons l'inclusion*

$$(3.3.4.1) \qquad [\mathrm{L}, \mathrm{L}] \subset \mathrm{L}^*.$$

Preuve. — Considérons d'abord l'ensemble M des $y \in \mathrm{L}$ tels que

$$(3.3.4.2) \qquad [y, \mathrm{L}^*] \subset \mathrm{L}^*.$$

Cet ensemble est fermé pour le crochet, la p-application et les opérations de Ω-module; il contient les x_i pour $i \in \mathrm{I}$. C'est donc L tout entier.

Prenons maintenant l'ensemble N des y tels que

$$(3.3.4.2) \qquad [\mathrm{L}, y] \subset \mathrm{L}^*.$$

Nous venons de voir que N contient les x_i. Nous vérifions encore que c'est une sous-algèbre restreinte, autrement dit que $\mathrm{L} = \mathrm{N}$.

(3.3.5) *Lemme.* — *Soit* L *une algèbre de Lie mixte engendrée par la famille d'éléments (homogènes)* (x_i), $i \in \mathrm{I}$. *Notons* L^* *la sous-*$\mathbf{F}_p$*-algèbre de Lie engendrée par les* x_i *dans* L, *et* L_ν (*resp.* L^*_ν) *la composante homogène de degré* $\nu \in \mathbf{R}^*_+$ *de* L (*resp.* L^*). *Notons enfin* $\mathrm{P}\,\mathrm{L}_\nu$ *l'ensemble des éléments* $\mathrm{P}x$, *où* $x \in \mathrm{L}_\nu$. *Alors, pour tout* $\nu \in \mathbf{R}^*_+$, *nous avons*

$$(3.3.5.1) \qquad \mathrm{L}_{\varphi(\nu)} = \mathrm{P}\,\mathrm{L}_\nu + \mathrm{L}^*_{\varphi(\nu)}.$$

Preuve. — Considérons l'algèbre de Lie mixte L comme plongée dans son algèbre enveloppante mixte $\mathrm{U}_{\mathrm{mix}}\mathrm{L}$ (1.2.8). Notons L' la $\mathbf{F}_p$*-algèbre de Lie restreinte* engendrée dans $\mathrm{U}_{\mathrm{mix}}\mathrm{L}$ par les x_i (pour la p-application $x \mapsto x^p$). La définition de l'algèbre $\mathrm{U}_{\mathrm{mix}}\mathrm{L}$ nous donne

$$(3.3.5.2) \qquad \mathrm{L}_\nu \subset \mathrm{L}'_\nu + \sum_i \pi^i \mathrm{L}'_{\nu - i},$$

où l'entier i prend des valeurs vérifiant

$$(3.3.5.3) \qquad 1 \leqslant i \leqslant \nu - (p-1)^{-1}.$$

Notons $[\mathrm{L}, \mathrm{L}]_\nu$ la composante homogène de degré ν du module $[\mathrm{L}, \mathrm{L}]$; appliquons le lemme (3.3.4), ainsi que les relations (3.3.5.2) et (3.3.5.3). Nous obtenons

$$(3.3.5.4) \qquad [\mathrm{L}, \mathrm{L}]_\nu \subset \mathrm{L}^*_\nu + \sum_i \pi^i \mathrm{L}^*_{\nu - i},$$

où l'entier i prend des valeurs vérifiant

$$(3.3.5.5) \qquad 1 \leqslant i < \nu - (p-1)^{-1}.$$

Quel que soit $\nu \in \mathbf{R}^*_+$, le *module* $\mathrm{L}_{\varphi(\nu)}$ est toujours engendré par $\mathrm{P}\,\mathrm{L}_\nu$, $[\mathrm{L}, \mathrm{L}]_{\varphi(\nu)}$ et les x_i de degré $\varphi(\nu)$. Supposons d'abord $\nu \leqslant (p-1)^{-1}$.

Alors, d'après (3.3.5.4) et (3.3.5.5), nous avons $[\mathrm{L}, \mathrm{L}]_{\varphi(\nu)} \subset \mathrm{L}^*_{\varphi(\nu)}$. D'autre part, l'application $\mathrm{P} : \mathrm{L}_\nu \to \mathrm{L}_{\varphi(\nu)}$ est additive modulo $[\mathrm{L}, \mathrm{L}]_{\varphi(\nu)}$ et nous obtenons (3.3.5.1).

Supposons maintenant $\nu > (p-1)^{-1}$. Alors l'application $P : L_\nu \to L_{\varphi(\nu)}$ est additive, les relations (3.3.5.4) et (3.3.5.5) nous donnent

$$[L, L]_{\varphi(\nu)} \subset L^*_{\varphi(\nu)} + \pi L_\nu,$$

et nous vérifions encore (3.3.5.1).

(3.3.6) *Proposition. — Soit* L *une algèbre de Lie mixte engendrée par des éléments* x_i *de degrés respectifs* τ_i, *pour* $1 \leqslant i \leqslant r$. *Soient t le maximum des* τ_i $(1 \leqslant i \leqslant r)$ *et m un nombre* $> (p-1)^{-1}$.

Supposons que les applications

$$P : L_\nu \to L_{\nu+1} \tag{3.3.6.1}$$

soient surjectives pour tout ν *vérifiant* $m \leqslant \nu < m+t$. *Alors les applications* (3.3.6.1) *sont surjectives pour tout* $\nu \geqslant m$.

Preuve. — L'ensemble des ν pour lesquels $L_\nu \neq 0$ est *discret* (cf. (3.3.2)), et nous pouvons donc démontrer la surjectivité de P par récurrence sur ν, en la supposant vérifiée pour $m \leqslant \nu < \lambda$, avec $\lambda \geqslant m+t$. Le lemme (3.3.5) nous donne

$$L_{\lambda+1} = P\,L_\lambda + L^*_{\lambda+1}, \tag{3.3.6.2}$$

en désignant par L^* la sous-$\mathbf{F}_p$-algèbre de Lie engendrée par les x_i. Le lemme (3.3.3) nous donne

$$L^*_{\lambda+1} = \sum_{1 \leqslant i \leqslant r} [L^*_{\lambda+1-\tau_i}, x_i]. \tag{3.3.6.3}$$

Mais la relation $\lambda \geqslant m+t$ implique

$$m \leqslant \lambda - \tau_i < \lambda, \tag{3.3.6.4}$$

d'où, par l'hypothèse de récurrence,

$$L^*_{\lambda+1-\tau_i} \subset L_{\lambda+1-\tau_i} = P\,L_{\lambda-\tau_i}. \tag{3.3.6.5}$$

D'après les axiomes (1.2.5.2) et (1.2.5.5), ainsi que les relations (3.3.6.3) et (3.3.6.5), nous avons

$$L^*_{\lambda+1} \subset P\,L_\lambda, \tag{3.3.6.6}$$

d'où enfin la relation $L_{\lambda+1} = P\,L_\lambda$.

CHAPITRE III

GROUPES p-VALUÉS ET GROUPES ANALYTIQUES

1. FONCTIONS ANALYTIQUES

(1.1) Valuation des factorielles; fonctions exponentielle, logarithme et puissance.

(1.1.1) *Numération de base p.* — Tout entier $n \in \mathbf{N}$ admet un développement dans le système de numération de base p :

(1.1.1.1)
$$n = \sum_{i \in \mathbf{N}} a_i p^i.$$

Les entiers a_i vérifient

(1.1.1.2)
$$0 \leqslant a_i < p,$$

et sont dits les *chiffres* du développement de n. Le i-ième chiffre a_i, considéré comme fonction de n, s'exprime au moyen de parties entières. En effet, pour tout $j \in \mathbf{N}$,

(1.1.1.3)
$$[p^{-j}n] = \sum_{i \geqslant j} a_i p^{i-j},$$

d'où les relations

(1.1.1.4)
$$a_i = [p^{-i}n] - p[p^{-(i+1)}n].$$

(1.1.2) *Valuation des exponentielles; la fonction Schiff.* — Notons v la valuation p-adique, avec $v(p) = 1$. Nous avons

(1.1.2.1)
$$v(n!) = \sum_{1 \leqslant i \leqslant n} v(i),$$

et le nombre d'entiers i compris entre 1 et n pour lesquels $v(i) \geqslant j$ est égal à $[p^{-j}n]$. En regroupant les termes égaux dont le second membre de (1.1.2.1), nous obtenons

(1.1.2.2)
$$\begin{aligned} v(n!) &= \sum_{j \in \mathbf{N}} j([p^{-j}n] - [p^{-(j+1)}n]) \\ &= \sum_{j \in \mathbf{N}^*} [p^{-j}n]. \end{aligned}$$

Si nous appliquons (1.1.1.4), il vient

(1.1.2.3)
$$v(n!) = (p-1)^{-1}(n - \sum_{i \in \mathbf{N}} a_i).$$

Nous noterons Schiff n la somme des *chiffres* du développement de n (dans le système de base p; il serait plus correct d'écrire $\mathrm{Schiff}_p\, n$) :

(1.1.2.4) $$\mathrm{Schiff}\, n = \sum_{i\in\mathbf{N}} a_i, \qquad \text{pour } n = \sum_{i\in\mathbf{N}} a_i p^i,\ 0 \leqslant a_i < p.$$

Nous écrivons donc (1.1.2.3) sous la forme

(1.1.2.5) $$v(n!) = (p-1)^{-1}(n - \mathrm{Schiff}\, n).$$

(1.1.3) *Notations.* — Nous désignerons par Ω un *anneau de valuation discrète complet*, d'inégales caractéristiques, *vérifiant* $v(p) = 1$ (I, 3.1.1).

Nous noterons A une Ω-*algèbre associative saturée* (I, 2.2.4) et (I, 2.2.10).

(1.1.4) *La fonction exponentielle.* — Soit x un élément de A, vérifiant

(1.1.4.1) $$w(x) > (p-1)^{-1}.$$

Pour chaque $n \in \mathbf{N}$, *l'élément* $(n!)^{-1}x^n$ *appartient à* A, *et* $w((n!)^{-1}x^n)$ *tend vers l'infini avec* n. *Nous posons*

(1.1.4.2) $$\exp x = \sum_{n\in\mathbf{N}} (n!)^{-1}x^n.$$

Les éléments x *et* $\exp x - 1$ *ont mêmes termes dominants* (*si* $x \neq 0$) :

(1.1.4.3) $$w(\exp x - x - 1) > w(x).$$

Preuve. — D'après (1.1.2.5) et les axiomes des algèbres filtrées (I, 2.1.11) nous avons $v(n!) \leqslant w(x^n)$ pour tout n, d'où l'existence du terme $(n!)^{-1}x^n$ puisque A est divisible.

Nous avons

(1.1.4.4) $$w((n!)^{-1}x^n) \geqslant nw(x) - v(n!),$$

(1.1.4.5) $$(n-1)w(x) - v(n!) = (n-1)(w(x) - (p-1)^{-1}) + (p-1)^{-1}(\mathrm{Schiff}\ n - 1),$$

ce qui prouve la convergence de la série $\exp x$, puisque A est complet, ainsi que la relation (1.1.4.3).

(1.1.5) *La fonction logarithme.* — Soit $x \in$ A, avec

(1.1.5.1) $$w(x-1) > (p-1)^{-1}.$$

Pour chaque $n \in \mathbf{N}^*$, *l'élément* $n^{-1}x^n$ *appartient à* A *et* $w(n^{-1}x^n)$ *tend vers l'infini avec* n. *Nous posons*

(1.1.5.2) $$\mathrm{Log}\, x = \sum_{n\in\mathbf{N}^*} (-1)^{n+1} n^{-1}(x-1)^n.$$

Les éléments $\mathrm{Log}\, x$ *et* $x - 1$ *ont mêmes termes dominants* (*pour* $x \neq 1$) :

(1.1.5.3) $$w(x - 1 - \mathrm{Log}\, x) > w(x-1).$$

Preuve. — Nous avons

(1.1.5.4) $$n^{-1} = (n-1)!(n!)^{-1}, \qquad \text{pour tout } n \in \mathbf{N}^*,$$

ce qui nous ramène aux calculs de (1.1.4).

Si nous admettions des éléments de valuation négative (par exemple dans un corps valué), la série $\operatorname{Log} x$ pourrait converger sous la seule hypothèse $w(x-1)>0$.

Sans considérer d'éléments de valuation négative, la série (1.1.5.2) est définie et convergente dans A pour $w(x-1)\geqslant p^{-1}$, mais la relation (1.1.5.3) peut être en défaut si (1.1.5.1) n'est pas vérifié. Nous définissons seulement la fonction logarithme sur l'ensemble des x vérifiant $w(x-1)>(p-1)^{-1}$, car cette fonction ne nous intéresse ici que lorsqu'elle est réciproque de l'exponentielle.

(1.1.6) *La fonction puissance.* — Les puissances positives entières x^λ ($\lambda\in\mathbf{N}$) sont définies pour les éléments d'un monoïde multiplicatif, et en particulier d'un anneau. Dans ce dernier cas nous avons la formule du binôme

(1.1.6.1) $$x^\lambda=\sum_{n\in\mathbf{N}}\binom{\lambda}{n}(x-1)^n,$$

où

(1.1.6.2) $$\binom{\lambda}{n}\doteq(n!)^{-1}\lambda(\lambda-1)\ldots(\lambda-n+1).$$

Conservons les notations de (1.1.3). Nous voyons, comme pour la fonction exponentielle (1.1.4), que, *pour chaque* $x\in\mathrm{A}$ *vérifiant*

(1.1.6.3) $$w(x-1)>(p-1)^{-1}$$

et pour chaque $\lambda\in\Omega$, l'élément $\binom{\lambda}{n}(x-1)^n$ appartient à A, et qu'il tend vers zéro (quand n tend vers l'infini).

Sous ces hypothèses, la formule (1.1.6.1) définit donc la fonction puissance x^λ par une *série convergente*. De plus, $x^\lambda-1$ et $\lambda(x-1)$ ont *mêmes termes dominants* (*si* $x\neq 1$ *et* $\lambda\neq 0$) :

(1.1.6.3) $$w(x^\lambda-1-\lambda(x-1))>w(\lambda(x-1)).$$

Lorsque $\lambda\in\mathbf{Z}_p$, alors $\binom{\lambda}{n}\in\mathbf{Z}_p$ pour chaque $n\in\mathbf{Z}_p$; les termes de la série (1.1.6.1) sont définis dès que x appartient à une $\mathbf{Z}_p$-algèbre associative. Si nous voulons seulement nous assurer que cette série converge, nous pouvons, par exemple, supposer que la $\mathbf{Z}_p$-algèbre est un $\mathbf{Z}_p$-module complet (II, 2.2.4) dans lequel les puissances $(x-1)^n$ tendent vers zéro. En fait, nous rencontrerons surtout des puissances x^λ pour $\lambda\in\mathbf{Z}_p$, et la condition (1.1.6.3) se trouvera le plus souvent vérifiée.

(1.1.7) *Continuité et fonctorialité.* — Les fonctions que nous venons d'introduire sont définies par des séries de polynômes, donc de fonctions continues. La continuité de nos fonctions résulte de la convergence uniforme des séries.

Pour le logarithme, la convergence est uniforme sur l'ensemble des x tels que $w(x-1)>(p-1)^{-1}$. Pour l'exponentielle (resp. la puissance), la convergence est uniforme sur l'ensemble des x tels que $w(x)\geqslant\nu$ (resp. des couples x, λ tels que $w(x-1)\geqslant\nu$), ν désignant un nombre réel $>(p-1)^{-1}$.

Quant à la « fonctorialité » des fonctions, elle exprime le simple fait suivant. Si $f : A \to B$ est un *morphisme de Ω-algèbres associatives saturées*, et si $\exp x$ est défini pour un $x \in A$, alors $\exp f(x)$ est défini et

(1.1.7.1) $$f(\exp x) = \exp f(x).$$

Les mêmes relations de permutation aux morphismes valent pour les fonctions logarithme et puissance.

(1.1.8) *Les identités classiques.* — Soient $x, x', y, y' \in A$ et $\lambda, \mu \in \Omega$, avec

(1.1.8.1) $$w(x) > (p-1)^{-1}; \qquad w(x') > (p-1)^{-1}.$$

(1.1.8.2) $$w(y-1) > (p-1)^{-1}; \qquad w(y'-1) \geqslant (p-1)^{-1}.$$

(1.1.8.3) $$xx' = x'x; \qquad yy' = y'y.$$

Alors nous avons les relations :

(1.1.8.4) $$\operatorname{Log}(\exp x) = x \quad \text{et} \quad \exp(\operatorname{Log} y) = y.$$

(1.1.8.5) $$\begin{gathered} \exp(x + x') = (\exp x)(\exp x'); \\ \operatorname{Log}(yy') = \operatorname{Log} y + \log y'. \end{gathered}$$

(1.1.8.6) $$\begin{gathered} y^\lambda y^\mu = y^{\lambda+\mu}; \\ (y^\lambda)^\mu = y^{\lambda\mu}; \\ (yy')^\lambda = y^\lambda (y')^\lambda. \end{gathered}$$

(1.1.8.7) $$\begin{gathered} \operatorname{Log}(y^\lambda) = \lambda \operatorname{Log} y; \\ \exp(\lambda x) = (\exp x)^\lambda. \end{gathered}$$

Si $\lambda, \mu \in \mathbf{Z}_p$, les relations (1.1.8.6) sont valables sous des hypothèses plus générales, indiquées en (1.1.6).

(1.2) Fonctions continues de variables p-adiques entières.

(1.2.1) *Notations ; opérateurs de translation.* — Soient r un entier $\geqslant 1$ et M un groupe additif. Notons $F(\mathbf{N}^r, M)$ l'ensemble des applications de $\mathbf{N}^r$ dans M, muni de sa structure de groupe additif. Soit, pour chaque i compris entre 1 et r, δ_i l'élément de $\mathbf{N}^r$ dont les coordonnées sont nulles, sauf la i-ième qui est égale à 1. Nous définissons les *endomorphismes* T_i de $F(\mathbf{N}^r, M)$ en posant

(1.2.1.1) $$(T_i f)(\lambda) = f(\lambda + \delta_i)$$

pour tout $f \in F(\mathbf{N}^r, M)$, $\lambda \in \mathbf{N}^r$ *et* $1 \leqslant i \leqslant r$.

Les opérateurs T_i commutent deux à deux. Pour tout $\lambda = (\lambda_i)_{1 \leqslant i \leqslant r} \in \mathbf{N}^r$, nous avons un opérateur (calculé dans l'anneau des endomorphismes de $F(\mathbf{N}^r, M)$)

(1.2.1.2) $$T^\lambda = \prod_{1 \leqslant i \leqslant r} T_i^{\lambda_i},$$

et, pour tout $f \in F(\mathbf{N}^r, M)$,

(1.2.1.3) $$f(\lambda) = (T^\lambda f)(0).$$

(1.2.2) *Différences à l'origine.* — Nous définissons les opérateurs Δ_i en posant, dans l'anneau des endomorphismes de $F(\mathbf{N}^r, M)$,

(1.2.2.1) $$\Delta_i = T_i - 1.$$

Ces opérateurs commutent deux à deux. Pour $\alpha \in \mathbf{N}^r$, nous avons le monôme

(1.2.2.2) $$\Delta^\alpha = \prod_{1 \leqslant i \leqslant r} \Delta_i^{\alpha_i},$$

et, si $f \in F(\mathbf{N}^r, M)$, l'élément

(1.2.2.3) $$(\Delta^\alpha f)(0) \in M$$

est dit « *différence d'ordre* α *de* f *à l'origine* ».

Les relations (1.2.2.1) nous donnent $T_i = 1 + \Delta_i$ et

(1.2.2.4) $$T_i^{\lambda_i} = \sum_{\alpha_i \in \mathbf{N}} \binom{\lambda_i}{\alpha_i} \Delta_i^{\alpha_i};$$

(1.2.2.5) $$T^\lambda = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} \Delta^\alpha, \quad \text{où}$$

(1.2.2.6) $$\binom{\lambda}{\alpha} = \prod_{1 \leqslant i \leqslant r} \binom{\lambda_i}{\alpha_i}.$$

Si nous considérons $\binom{\lambda}{\alpha}$ comme un élément de $F(\mathbf{N}^r, \mathbf{N})$, α restant fixe, nous avons

(1.2.2.7) $$\begin{cases} \Delta^\beta \binom{\lambda}{\alpha} = \binom{\lambda}{\alpha - \beta} & \textit{si } \beta \leqslant \alpha; \\ \Delta^\beta \binom{\lambda}{\alpha} = 0 & \textit{si } \beta \not\leqslant \alpha. \end{cases}$$

La relation $\beta \leqslant \alpha$ signifie $\beta_i \leqslant \alpha_i$ pour chaque i, $1 \leqslant i \leqslant r$. Les relations (1.2.2.7) s'obtiennent, par récurrence sur $|\beta|$, à partir de la formule classique

$$\binom{\lambda + 1}{n} = \binom{\lambda}{n} + \binom{\lambda}{n-1}, \quad n \in \mathbf{N}^*.$$

(1.2.3) *Proposition.* — *(« Formule d'interpolation »). Pour chaque* $\lambda \in \mathbf{N}^r$, *les entiers* $\binom{\lambda}{\alpha}$ *sont presque tous nuls (plus précisément : sont nuls pour* $\alpha \not\leqslant \lambda$*). Une application* f *de* $\mathbf{N}^r$ *dans le groupe additif* M *est représentable, d'une manière et d'une seule, par une série*

(1.2.3.1) $$f(\lambda) = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} C_\alpha,$$

où $C_\alpha \in M$. *Les* C_α *sont les différences de* f *à l'origine :*

(1.2.3.2) $$C_\alpha = \Delta^\alpha f(0), \quad \textit{pour tout} \quad \alpha \in \mathbf{N}^r.$$

Preuve. — La formule (1.2.3.1), où les C_α ont les valeurs indiquées en (1.2.3.2), est une conséquence de (1.2.1.3) et (1.2.2.5).

Une famille quelconque d'éléments $C_\alpha \in M$ définit une fonction f par la formule (1.2.3.1). Les opérateurs Δ^α s'appliquent terme à terme à la série f, et les relations (1.2.2.7) donnent (1.2.3.2).

(1.2.4) *Théorème* (Mahler [22]). — *Soit f une application continue de $\mathbf{Z}_p^r$ dans un $\mathbf{Z}_p$-module complet* M (II, 2.2.4). *Alors les différences de f à l'origine*

(1.2.4.1) $$C_\alpha = \Delta^\alpha f(0)$$

tendent vers zéro dans M, *et, pour tout* $\lambda \in \mathbf{Z}_p^r$, $f(\lambda)$ *est égal à la somme de la série*

(1.2.4.2) $$f(\lambda) = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} C_\alpha.$$

Réciproquement, si (C_α), $\alpha \in \mathbf{N}^r$, *est une famille d'éléments tendant vers zéro dans* M, *la formule* (1.2.4.2) *définit une application continue f de $\mathbf{Z}_p^r$ dans* M, *qui vérifie* (1.2.4.1), *pour chaque* $\alpha \in \mathbf{N}^r$.

Preuve. — L'ensemble $\mathbf{N}^r$ est *dense* dans $\mathbf{Z}_p^r$, qui est compact. Une fonction *continue* f définie sur $\mathbf{Z}_p^r$ est donc déterminée par sa *restriction* à $\mathbf{N}^r$, et $f(\mathbf{Z}_p^r)$ est l'adhérence de $f(\mathbf{N}^r)$. En particulier, pour un $\alpha \in \mathbf{N}^r$, $\binom{\lambda}{\alpha}$ est une fonction continue de λ à valeurs p-adiques entières. Si les C_α, pour $\alpha \in \mathbf{N}^r$, tendent vers zéro dans M, la série (1.2.4.2) est une série uniformément convergente de fonctions continues, et définit une fonction continue f. Les relations (1.2.4.1) ne concernent que la restriction de f à $\mathbf{N}^r$, et résultent donc de (1.2.3).

Si f est donnée comme application continue de $\mathbf{Z}_p^r$ dans M, et si (1.2.4.1) définit les C_α, alors (1.2.4.2) vaut pour $\lambda \in \mathbf{N}^r$. Il nous reste seulement à prouver que les *différences à l'origine d'une fonction continue tendent vers zéro.*

(1.2.5) Donnons-nous donc la *fonction continue* $f : \mathbf{Z}_p^r \to M$ et un *sous-module ouvert* N *de* M. L'image du compact $f(\mathbf{Z}_p^r)$ dans le *groupe discret de p-torsion* M/N est *finie*. Il existe donc un entier $m \in \mathbf{N}$, tel que

(1.2.5.1) $$p^m f(\lambda) \in N, \qquad \text{pour tout } \lambda \in \mathbf{N}^r.$$

D'autre part f est *uniformément continue*, ce qui entraîne l'existence d'un entier $n \in \mathbf{N}$ tel que

(1.2.5.2) $$(T_i^{p^n} - 1) f(\lambda) \in N,$$

pour tout $\lambda \in \mathbf{Z}_p^r$ et tout i $(1 \leqslant i \leqslant r)$, les opérateurs T_i et Δ_i restant définis par les formules (1.2.1.1) et (1.2.2.1). Posons, pour simplifier l'écriture,

(1.2.5.3) $$q = p^{m+n-1},$$

et écartons le cas trivial où $m = 0$. Nous allons démontrer la relation

(1.2.5.4) $$\Delta_i^q f(\lambda) \in N, \qquad \textit{pour } \lambda \in \mathbf{Z}_p^r.$$

Nous avons en effet

(1.2.5.5) $$\Delta_i^q = (T_i - 1)^q = \sum_{0 \leqslant j \leqslant q} (-1)^{q-j} \binom{q}{j} (T_i^j - 1).$$

Distinguons deux cas relatifs aux termes de la dernière somme. Si $v(j) \geqslant n$, j est divisible par p^n et $T_i^j - 1$ est divisible par $T_i^{p^n} - 1$; nous appliquons alors (1.2.5.2). Si, par contre, $v(j) \leqslant n-1$, alors $\binom{q}{j}$ est divisible par p^m. En effet, si $h \in \mathbf{N}, j \in \mathbf{N}$, $0 \leqslant j \leqslant p^h$, nous avons $v\left(\binom{p^h}{j}\right) = h - v(j)$. Nous appliquons (1.2.5.1) dans ce deuxième cas, et (1.2.5.4) est démontré. Pour *presque tous* les $\alpha \in \mathbf{N}^r$, l'un des α_i est $\geqslant p^{m+n-1}$, l'opérateur Δ^α est divisible par Δ_i^q, et $\Delta^\alpha f(0) \in \mathrm{N}$.

(1.3) Fonctions continues et fonctions analytiques.

(1.3.1) *Séries de puissances.* — Soient $r \in \mathbf{N}$ et M un $\mathbf{Z}_p$-module complet (II, 2.2.4). A chaque famille $(d_\alpha)_{\alpha \in \mathbf{N}^r}$ d'éléments de M nous associons la *série de puissances*

(1.3.1.1)
$$\sum_{\alpha \in \mathbf{N}^r} x^\alpha . d_\alpha,$$

où $x^\alpha = \prod_{1 \leqslant i \leqslant r} x_i^{\alpha_i}$. Nous supposons que cette série converge lorsque x appartient à un voisinage V de zéro dans $\mathbf{Z}_p^r$; elle définit alors une *application* $f : \mathrm{V} \to \mathrm{M}$.

Si le module M est *sans torsion*, nous pouvons dire que (1.3.1.1) est la série de Taylor de f (à l'origine). En effet, la fonction f est alors *indéfiniment dérivable*, et, pour chaque $\alpha \in \mathbf{N}^r$, nous avons la relation

(1.3.1.2)
$$\alpha!\, d_\alpha = \mathrm{D}^\alpha f(0),$$

où $\alpha! = \prod_i \alpha_i!$ et D^α est l'opérateur de dérivation d'ordre α. Par contre, si M a de la torsion, la série (1.3.1.1) *n'est pas univoquement déterminée* par la fonction f; exemple : si $r=1$, $\mathrm{M} = \mathbf{F}_p$, la série $x - x^p$ représente la fonction nulle. Un autre aspect du même phénomène est le suivant; si $r=1$ et $\mathrm{M} = \mathbf{Z}_p$, la fonction polynôme $x \mapsto p^{-1}(x - x^p)$ n'est pas représentable par une série (1.3.1.1).

(1.3.2) *Définition des fonctions analytiques sur un ouvert de* $\mathbf{Z}_p^r$. — Soient M un $\mathbf{Z}_p$-module complet, $r \in \mathbf{N}$, V un ouvert de $\mathbf{Z}_p^r$ et f une application de V dans M. Nous disons que f est *analytique* si, *pour chaque* $y \in \mathrm{V}$, *il existe* $h \in \mathbf{N}$ *tel que la fonction*

(1.3.2.1)
$$x \mapsto f(y + p^h x)$$

soit égale à la somme d'une série de puissances en x (1.3.1), *pour tout* $x \in \mathbf{Z}_p^r$.

Cette définition transcrit celle des fonctions analytiques réelles ou complexes. Nous avons dû faire intervenir des homothéties de rapport p^h, parce que nous travaillons avec des modules (au lieu d'espaces vectoriels sur $\mathbf{Q}_p$).

Les fonctions *localement constantes* sont analytiques, ainsi que les *fonctions polynômes*, dont voici la définition.

(1.3.2.2) *Une fonction* $f : \mathbf{Z}_p^r \to \mathrm{M}$ *est dite fonction polynôme si elle est continue et si presque toutes ses différences à l'origine sont nulles.*

D'après le théorème (1.2.4), cette définition équivaut à la suivante (valable pour un $\mathbf{Z}_p$-module M quelconque, non nécessairement topologique).

(1.3.2.3) *Une fonction polynôme* $f : \mathbf{Z}_p^r \to \mathrm{M}$ *est une application qui s'écrit comme une somme finie :*

$$x \mapsto \sum_\alpha \binom{x}{\alpha} \mathrm{C}_\alpha,$$

(les C_α étant des éléments de M, *presque tous nuls*).

(1.3.3) *Variétés analytiques sur* $\mathbf{Q}_p$. — Les variétés analytiques (« molles ») sur $\mathbf{Q}_p$ se définissent en transcrivant l'une des définitions des variétés analytiques réelles ou complexes. Pour définir une variété de dimension $r \in \mathbf{N}$, il est indifférent de prendre comme « modèles » (à recoller) les ouverts de $\mathbf{Z}_p^r$ ou de $\mathbf{Q}_p^r$.

Une *variété analytique de dimension r* est un *espace topologique séparé*. Au voisinage de chaque point on peut prendre un *système de r coordonnées analytiques* et les fonctions qui font passer d'un tel système à un autre sont *analytiques*, au sens de (1.3.2). Comme dans le cas classique, on définit le *produit* de deux variétés analytiques, et les applications analytiques (ou *morphismes*) d'une variété analytique dans une autre.

(1.3.4) *Fonctions analytiques tayloriennes ; variétés analytiques tayloriennes de type* $\mathbf{Z}_p^r$. — Nous disons qu'une application $f : \mathbf{Z}_p^r \to \mathrm{M}$ est *analytique taylorienne* si f est égale à la *somme d'une série de puissances* (1.3.1.1). Cette série doit donc *converger sur* $\mathbf{Z}_p^r$ *tout entier ; ses coefficients* d_α *appartiennent à* M, *et tendent vers* 0.

Nous appelons *variété analytique taylorienne de type* $\mathbf{Z}_p^r$ la structure constituée par un *espace topologique* E et une famille non vide F d'homéomorphismes de E sur $\mathbf{Z}_p^r$ vérifiant les deux axiomes suivants

(1.3.4.1) *Si* $f_1, f_2 \in \mathrm{F}$, *alors* $f_1 \circ f_2^{-1}$ *est une application analytique taylorienne de* $\mathbf{Z}_p^r$ *sur lui-même.*

(1.3.4.2) *La famille* F *est maximale pour la propriété* (1.3.4.1).

Autrement dit (par abus de langage), E est $\mathbf{Z}_p^r$ où l'on se permet les changements de coordonnées définis par des séries de puissances convergentes à coefficients entiers.

Si E_1 et E_2 sont deux variétés analytiques tayloriennes, de types $\mathbf{Z}_p^{r_1}$ et $\mathbf{Z}_p^{r_2}$ respectivement, alors le *produit* $\mathrm{E}_1 \times \mathrm{E}_2$ possède une structure de variété analytique taylorienne, de type $\mathbf{Z}_p^{r_1+r_2}$. Nous définissons un *morphisme* $g : \mathrm{E}_1 \to \mathrm{E}_2$ comme une application analytique taylorienne, E_1 (resp. E_2) étant identifié à $\mathbf{Z}_p^{r_1}$ (resp. $\mathbf{Z}_p^{r_2}$) par l'un quelconque des homéomorphismes f de la famille F qui le définit.

(1.3.5) *Fonctions analytiques strictes ; variétés analytiques strictes de type* $\mathbf{Z}_p^r$. — Une application $f : \mathbf{Z}_p^r \to \mathrm{M}$ est dite *fonction analytique stricte* si elle est *somme d'une fonction polynôme* (1.3.2) et d'une *fonction analytique taylorienne* (1.3.4).

Lorsque $\mathrm{M} = \mathbf{Z}_p$, une application $f : \mathbf{Z}_p^r \to \mathbf{Z}_p$ est *analytique stricte* si et seulement si $i \circ f : \mathbf{Z}_p^r \to \mathbf{Q}_p$ est *analytique taylorienne*, i désignant l'injection canonique de $\mathbf{Z}_p$ dans $\mathbf{Q}_p$. Autrement dit, f est la somme d'une série $\sum_\alpha x^\alpha d_\alpha$ *à valeurs p-adiques entières* (pour $x \in \mathbf{Z}_p^r$), dont *les coefficients appartiennent à* $\mathbf{Q}_p$ (et, *presque tous*, à $\mathbf{Z}_p$, puisqu'ils tendent vers zéro).

Remplaçant « analytique taylorienne » par « analytique stricte » dans la définition des variétés analytiques tayloriennes de type $\mathbf{Z}_p^r$ (1.3.4), nous parvenons à la notion de *variété analytique stricte de type* $\mathbf{Z}_p^r$. Il s'agit (par abus de langage) de $\mathbf{Z}_p^r$ où l'on se permet les changements de coordonnées globaux définis par des séries de puissances (dont les coefficients ne sont pas nécessairement tous entiers).

Le *produit* de deux variétés analytiques strictes de type $\mathbf{Z}_p^{r_1}$ et $\mathbf{Z}_p^{r_2}$ est une variété analytique stricte de type $\mathbf{Z}_p^{r_1+r_2}$. De même un *morphisme* de variétés analytiques strictes est défini par une application analytique stricte.

Nous avons ainsi défini trois *catégories* : les variétés *analytiques*, *analytiques strictes*, et *analytiques tayloriennes.*

(1.3.6) *Critères d'analyticité stricte ou taylorienne.* — Soit $f : \mathbf{Z}_p^r \to \mathrm{M}$ une application continue.

D'après le théorème (1.2.4) nous avons

$$(1.3.6.1) \qquad f(\lambda) = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} \mathrm{C}_\alpha,$$

où les C_α sont les différences de f à l'origine.

(1.3.6.2) *Critère d'analyticité taylorienne. — Pour que l'application f de* (1.3.6.1) *soit analytique taylorienne, il faut et il suffit qu'existe, pour chaque* $\alpha \in \mathbf{N}^r$, *un élément* $\mathrm{C}'_\alpha \in \mathrm{M}$, *vérifiant* $\mathrm{C}_\alpha = \alpha!\,\mathrm{C}'_\alpha$, *et que les* C'_α *tendent vers zéro dans* M (*pour* $|\alpha| \to \infty$).

Preuve. — Pour chaque $\alpha \in \mathbf{N}^r$, $\alpha!\binom{\lambda}{\alpha}$ *est un polynôme à coefficients entiers* en λ, ce qui prouve la suffisance. Pour prouver la nécessité nous remarquons que la différence à l'origine d'ordre β de la fonction polynôme λ^α (c'est-à-dire $\prod_i \lambda_i^{\alpha_i}$) est un entier *divisible par* $\beta!$.

(1.3.6.3) *Critère d'analyticité stricte.* — C'est le critère (1.3.6.2), à ceci près que *les* C'_α *sont seulement définis pour presque tous les* $\alpha \in \mathbf{N}^r$ (ou encore pour $|\alpha|$ assez grand).

(1.3.7) *Applications analytiques d'ordre h.* — Soient $f : \mathbf{Z}_p^r \to \mathrm{M}$ une application continue et $h \in \mathbf{N}$. Nous disons que f est *analytique d'ordre* $\geqslant h$ si, *pour chaque* $y \in \mathbf{Z}_p^r$, la fonction définie par $x \mapsto f(y + p^h x)$ est *analytique stricte au sens de* (1.3.5), x parcourant $\mathbf{Z}_p^r$. Une fonction analytique d'ordre $\geqslant h$ est donc analytique, au sens de (1.3.2). Réciproquement si f est analytique, elle est analytique d'ordre h pour h assez grand, d'après (1.3.2) et la *compacité* de $\mathbf{Z}_p^r$. *L'ordre d'analyticité* de f est le plus petit entier h tel que f soit analytique d'ordre $\geqslant h$.

En particulier, les fonctions analytiques d'ordre 0 sont les fonctions analytiques strictes (1.3.5).

(1.3.8) *Critère d'analyticité d'ordre h. — Théorème (Y. Amice). Soient $h \in \mathbf{N}$ et $f : \mathbf{Z}_p^r \to \mathrm{M}$ une application continue. Notons C_α la différence d'ordre α de f à l'origine, si bien que*

$$(1.3.8.1) \qquad f(\lambda) = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} \mathrm{C}_\alpha.$$

Supposons que M *soit un* $\mathbf{Z}_p$*-module saturé* (I, 2.2.10), *ou un* $\mathbf{Z}_p$*-module valué de type fini. Notons* w *la valuation de* M *et, pour* $\alpha=(\alpha_i)\in\mathbf{N}^r$, *posons*

(1.3.8.2) $$\operatorname{Schiff}\alpha=\sum_{1\leqslant i\leqslant r}\operatorname{Schiff}\alpha_i.$$

Alors les deux assertions suivantes sont équivalentes.

(1.3.8.3) *La fonction* f *est analytique d'ordre* $\geqslant h$.

(1.3.8.4) $$w(\mathrm{C}_\alpha)-(p-1)^{-1}(p^{-h}|\alpha|-\operatorname{Schiff}\alpha)$$

tend vers $+\infty$ *avec* $|\alpha|$.

Preuve. — Pour $h=0$, c'est une conséquence de (1.3.6.3), compte tenu de (1.1.2.5).

Pour $h\geqslant 1$, cela résulte de [1], chap. III.

(1.3.9) *Corollaire* [10]. — *Les hypothèses sur* f *et* M *étant celles de* (1.3.8), *les deux assertions suivantes sont équivalentes.*

(1.3.9.1) *La fonction* f *est analytique* (1.3.2).

(1.3.9.2) $$\varliminf_{|\alpha|\to\infty}\frac{w(\mathrm{C}_\alpha)}{|\alpha|}>0.$$

Preuve. — Si nous notons $\log_p$ le logarithme de base p, nous avons, pour $n\in\mathbf{N}^*$,

(1.3.9.3) $$\operatorname{Schiff} n\leqslant(p-1)(1+\log_p n),$$

ce qui établit (1.3.9) à partir du théorème précédent et de (1.3.7).

2. GROUPES p-VALUÉS

(2.1) Groupes p-valués, p-divisibles, p-saturés.

(2.1.1) Soit G un groupe p-filtré (II, 1.2.10) vérifiant la condition suivante :

(2.1.1.1) *Pour tout* $x\in\mathrm{G}$, $\omega(x)>(p-1)^{-1}$.

Alors le gradué associé gr G est une *algèbre de Lie mixte* (II, 1.2.11) *dont les composantes homogènes de degrés* $\leqslant(p-1)^{-1}$ *sont nulles*. Les seuls axiomes de la définition (1.2.5) qui interviennent sont (II, 1.2.5.2) et (II, 1.2.5.5). L'opérateur P est donc additif, c'est-à-dire $\mathbf{F}_p$-linéaire, et homogène de degré $+1$. Nous pouvons le prolonger par linéarité à toute l'algèbre gr G, qui devient ainsi une *algèbre de Lie sur l'anneau de polynômes* $\Gamma=\mathbf{F}_p[\pi]$, étudié en (I, 1.2) : pour $\xi\in\mathrm{gr}_\nu\mathrm{G}$, nous posons $\pi x=\mathrm{P}x$.

D'après (II, 1.4.5.7), si x et y sont deux éléments de G vérifiant

(2.1.1.2) $$\omega(x)\leqslant\omega(y)<\infty,\quad\text{alors}$$

(2.1.1.3) $$\omega(y^{-p}x^{-p}(xy)^p)>\omega(y)+1.$$

Pour établir ces propriétés, il n'est pas nécessaire de disposer de l'énoncé complet du lemme (II, 1.4.3). Si (2.1.1.1) est vérifié, les relations (II, 1.4.3.5), (II, 1.4.3.7) et (II, 1.4.3.9) deviennent inutiles. Il suffirait d'avoir démontré le lemme (II, 1.4.3) sous la forme simplifiée suivante. *Soient* $\mathscr{F}$ *le groupe libre engendré par les générateurs* X *et* Y, $\mathscr{F}_i$ *le i-ième sous-groupe de la suite centrale descendante de* $\mathscr{F}$, *et* $\mathscr{F}_i^p$ *le sous-groupe engendré par les p-ièmes puissances des éléments de* $\mathscr{F}_i$. *Alors nous avons les relations :*

(2.1.1.4) $$(XY)^p \equiv X^p Y^p \quad \text{mod } \mathscr{F}_2^p . \mathscr{F}_p.$$

(2.1.1.5) $$(X^p, Y) \equiv (X, Y)^p \quad \text{mod } \mathscr{F}_3^p . \mathscr{F}_{p+1}.$$

(2.1.2) *Définition.* — Nous dirons qu'un *groupe filtré* G (II, 1.1.1) est *p-valué* s'il vérifie les trois axiomes suivants

(2.1.2.1) $$\omega(x) < \infty \quad \textit{pour} \quad x \in G,\ x \neq 1.$$

(2.1.2.2) $$\omega(x) > (p-1)^{-1} \quad \textit{pour tout} \quad x \in G.$$

(2.1.2.3) $$\omega(x^p) = \omega(x) + 1 \quad \textit{pour tout} \quad x \in G.$$

Autrement dit, une *p-valuation* ω du groupe G est une *p-filtration* (II, 1.2.10) *séparée* (II, 1.1.5) *pour laquelle* $\mathrm{gr}_\nu G = 0$ *si* $\nu \leqslant (p-1)^{-1}$, *et* gr G (qui est donc une Γ-algèbre de Lie) *est sans torsion.*

Tout *sous-groupe* d'un groupe p-valué est p-valué (pour la filtration induite). Le *complété* $\hat{G}$ d'un groupe p-valué G est p-valué.

Si nous avons une famille $(\omega_i)_{i \in I}$ de p-valuations d'un même groupe G, leur *borne inférieure* (II, 1.1.4) est encore une p-valuation si et seulement si elle vérifie la condition (2.1.2.2).

(2.1.3) *Définition.* — Soit G un groupe *p-valué* (2.1.2). Alors gr G est un Γ-module *sans torsion, donc libre* d'après le théorème (I, 1.2.3). Nous appellerons *rang* de G le rang sur Γ du Γ-module libre gr G.

(2.1.4) *Proposition.* — *Soient* x *et* y *deux éléments d'un groupe p-valué* G. *Alors, pour tout entier* $n \in \mathbf{N}$,

$$\omega(x^{-p^n} y^{p^n}) = \omega(x^{-1}y) + n.$$

Preuve. — Il nous suffit de traiter le cas où $n = 1$, l'énoncé général s'en déduisant par récurrence. Nous pouvons supposer $\omega(x) \leqslant \omega(y)$. Appliquons (2.1.1.3), où nous remplaçons x et y par x et $x^{-1}y$ respectivement, ainsi que (2.1.2.3); nous obtenons

$$\omega((x^{-1}y)^{-p} x^{-p} y^p) > \omega(x^{-1}y) + 1 = \omega((x^{-1}y)^p),$$

d'où

$$\omega(x^{-p} y^p) = \omega((x^{-1}y)^p) = \omega(x^{-1}y) + 1.$$

(2.1.5) *Définition.* — Un groupe G sera dit *p-divisible* s'il est *p-valué* et possède la propriété suivante.

Si $x \in G$ *et* $\omega(x) > p(p-1)^{-1}$, *alors il existe* $y \in G$ *tel que* $y^p = x$.

Autrement dit, un groupe p-divisible est un groupe p-valué où tout élément, auquel (2.1.2.2) et (2.1.2.3) n'interdisent pas d'être une puissance p-ième, est effectivement une puissance p-ième.

(2.1.6) *Définition.* — Nous disons qu'un groupe G est *p-saturé* s'il est *p-divisible* et *complet.*

(2.1.7) *Proposition. — Le complété* $\hat{\mathrm{G}}$ *d'un groupe p-divisible* G *est p-saturé.*

La preuve procède comme en (I, 2.2.10), compte tenu de (2.1.4).

(2.1.8) *Proposition. — Soit* G *un groupe p-valué complet dont la filtration est discrète. Alors, si* $\mathrm{gr}_{\nu+1}\mathrm{G} = \pi\, \mathrm{gr}_\nu \mathrm{G}$ *pour tout* $\nu > (p-1)^{-1}$, *le groupe* G *est p-saturé.*

Preuve. — Compte tenu de (2.1.4), on construit par approximations successives la racine p-ième d'un élément x; cf. (I, 2.3.13).

(2.1.9) *Exercice.* — Soit G un groupe p-filtré complet, de filtration discrète et vérifiant les axiomes (2.1.2.1) et (2.1.2.2) (mais non nécessairement (2.1.2.3)). Alors gr G est une Γ-algèbre de Lie (2.1.1). Supposons que $\mathrm{gr}_{\nu+1}\mathrm{G} = \pi\, \mathrm{gr}_\nu \mathrm{G}$ pour tout $\nu > (p-1)^{-1}$. Alors chaque élément de $\mathrm{G}_{\nu+1}$ est puissance p-ième d'un élément de G_ν (pour $\nu > (p-1)^{-1}$). D'autre part, s'il existe $x \in \mathrm{G}$ avec $\omega(x^p) > \omega(x) + 1$ (autrement dit si (2.1.2.3) n'est pas vérifié), alors il existe $y \in \mathrm{G}$ ayant même terme dominant que x, et tel que $y^p = 1$.

(2.1.10) *Exercice.* — Soient x et y deux éléments d'un groupe *p-saturé* G (2.1.6). Montrer que, pour tout $n \in \mathbf{N}$, il existe des éléments $u_n, v_n \in \mathrm{G}$ vérifiant

(2.1.10.1) $$u_n^{p^n} = x^{p^n} y^{p^n};$$

(2.1.10.2) $$v_n^{p^{2n}} = (x^{p^n}, y^{p^n}).$$

Montrer que les suites (u_n) et (v_n) convergent dans G. Si l'on note respectivement $x+y$ et $[x, y]$ les limites de ces suites, montrer que les deux nouvelles opérations binaires ainsi définies sur G font de cet ensemble une $\mathbf{Z}_p$-algèbre de Lie (le produit de $x \in \mathrm{G}$ par $\lambda \in \mathbf{Z}_p$ est pris égal à x^λ, défini en (II, 2.1.6)).

(2.2) Bases ordonnées.

(2.2.1) Soient G un groupe topologique, noté multiplicativement, I un ensemble totalement ordonné et $(x_i)_{i \in \mathrm{I}}$ une famille d'éléments de G. A toute partie finie J de I nous associons le *produit ordonné* fini

$$x_{\mathrm{J}} = \prod_{i \in \mathrm{J}} x_i.$$

Si la famille (x_{J}) converge vers $x \in \mathrm{G}$ suivant le filtre des sections de l'ensemble des parties finies de I, ordonnées par inclusion, nous disons que le produit ordonné $\prod_{i \in \mathrm{I}} x_i$ est convergent, et nous écrivons

(2.2.1.1) $$x = \prod_{i \in \mathrm{I}} x_i.$$

Si, en particulier, G est un groupe topologique complet, dont les sous-groupes distingués ouverts forment un système fondamental de voisinages de l'élément neutre, alors le produit (2.2.1.1) converge si et seulement si x_i tend vers l'élément neutre (suivant le filtre des complémentaires des parties finies de I).

Plus particulièrement, si G est un *groupe p-valué* (2.1.2) *complet*, si $(x_i)_{i\in I}$ est une famille totalement ordonnée d'éléments de G et $(\lambda_i)_{i\in I}$ une famille d'*entiers p-adiques*, alors le produit

(2.2.1.2)
$$\prod_{i\in I} x_i^{\lambda_i}$$

converge si et seulement si

(2.2.1.3)
$$v(\lambda_i)+\omega(x_i)\to+\infty$$

(2.2.2) *Lemme. — Soient* G *un groupe p-valué complet,* I *un ensemble totalement ordonné et* $(x_i)_{i\in I}$ *une famille d'éléments de* G, *distincts de l'élément neutre. Les deux assertions suivantes sont équivalentes.*

(2.2.2.1) *La famille des termes dominants* (1.1.7) *des* x_i *est libre sur* Γ *dans* gr G.

(2.2.2.2) *Quelles que soient les familles* $(\lambda_i)_{i\in I}$ *et* $(\mu_i)_{i\in I}$ *d'entiers p-adiques, si les produits* $y=\prod_{i\in I} x_i^{\lambda_i}$ *et* $z=\prod_{i\in I} x_i^{\mu_i}$ *convergent, alors*

(2.2.2.3)
$$\omega(y^{-1}z)=\inf_{i\in I}(\omega(x_i)+v(\lambda_i-\mu_i)).$$

Preuve. — Pour vérifier, comme en (I, 2.3.12), que (2.2.2.2) implique (2.2.2.1), il nous suffit de supposer (2.2.2.3) vérifiée lorsque tous les $\mu_i\in\mathbf{Z}_p$ sont nuls.

Pour démontrer (2.2.2.2) à partir de (2.2.2.1), nous posons

$$\nu=\inf(\omega(x_i)+v(\lambda_i-\mu_i))$$

et nous remarquons que les éléments de G_ν/G_{ν^+} sont centraux dans le groupe G/G_{ν^+}.

(2.2.3) *Lemme. — Soit* G *un groupe p-valué complet, de filtration discrète,* I *un ensemble totalement ordonné et* $(\xi_i)_{i\in I}$ *une famille de générateurs de* gr G *considéré comme* Γ*-module. Alors, si* $(x_i)_{i\in I}$ *est une famille de représentants des* ξ_i, *tout élément* $y\in G$ *peut s'écrire comme un produit ordonné*

$$y=\prod_{i\in I} x_i^{\lambda_i},\qquad \textit{où}\ \lambda_i\in\mathbf{Z}_p,\ i\in I.$$

Preuve par approximations successives.

(2.2.4) *Définition. — Soit* G *un groupe p-valué complet. Nous appellerons base ordonnée de* G *une famille d'éléments* $(x_i)_{i\in I}$, *indexée par l'ensemble totalement ordonné* I, *vérifiant les propriétés suivantes. Tout élément* $y\in G$ *s'écrit, d'une manière et d'une seule, comme un produit ordonné*

(2.2.4.1)
$$y=\prod_{i\in I} x_i^{\lambda_i}$$

où $\lambda_i\in\mathbf{Z}_p$ *pour tout* $i\in I$, *et nous avons*

(2.2.4.2)
$$\omega(y)=\inf_{i\in I}(\omega(x_i)+v(\lambda_i)).$$

La famille $(\lambda_i)_{i\in \mathrm{I}}$ est déterminée par y et peut s'appeler « coordonnées de deuxième espèce » de y, car nous avons représenté le groupe G comme un produit de groupes « à un paramètre ». Si l'ensemble I est infini, les λ_i sont assujettis à la condition

(2.2.4.3) $$\lim_i(\omega(x_i)+v(\lambda_i))=+\infty.$$

En particulier, si $\omega(x_i)\to+\infty$ *(ce qui caractérise les groupes p-valués compacts)*, aucune condition n'est imposée aux λ_i.

(2.2.5) *Proposition. — Soit* G *un groupe p-valué complet. Si* G *possède une base ordonnée* $(x_i)_{i\in \mathrm{I}}$ *alors la famille* $(\xi_i)_{i\in \mathrm{I}}$ *des termes dominants des* x_i *est une base du* Γ*-module* gr G. *Réciproquement, si la filtration de* G *est discrète, toute famille totalement ordonnée de représentants d'une base* (I, 1.1.6) *du* Γ*-module* gr G *est une base ordonnée de* G.

Preuve. — La première assertion n'est qu'une traduction. La réciproque utilise les lemmes (2.2.2) et (2.2.3).

(2.2.6) *Proposition. — Considérons les quatre propriétés suivantes d'un groupe p-valué complet* G :

(2.2.6.1) G *est de rang fini* (2.1.3).

(2.2.6.2) G *est de type fini* (II, 2.1.4).

(2.2.6.3) G *est compact.*

(2.2.6.4) *La valuation de* G *est discrète* (II, 1.1.5).

Alors nous avons les implications

$$(2.2.6.1)\Rightarrow(2.2.6.2)\Rightarrow(2.2.6.3)\Rightarrow(2.2.6.4).$$

Preuve. — Si (2.2.6.1) est vérifié, gr G est de type fini, donc de graduation discrète, ce qui implique (2.2.6.4), et G possède une *base ordonnée finie*, d'après la proposition (2.2.5), d'où (2.2.6.2). Si (2.6.6.2) est vérifié, le lemme (II, 3.1.2) établit (2.2.6.3). Enfin si G est compact, chaque G/G_ν est fini, et il n'y a donc qu'un nombre fini de $\lambda<\nu$ tels que $\mathrm{gr}_\lambda G\neq 0$, ce qui exprime (2.2.6.4).

(2.2.7) *Bases ordonnées et groupes saturés. Proposition. — Soit* G *un groupe p-valué complet, de filtration discrète. Choisissons* (2.2.5) *une base ordonnée* $(x_i)_{i\in \mathrm{I}}$.

Pour que G *soit p-saturé, il faut et il suffit que les valuations* $\omega(x_i)$ *vérifient les relations*

(2.2.7.1) $$(p-1)^{-1}<\omega(x_i)\leqslant p(p-1)^{-1},$$

pour $i\in \mathrm{I}$.

Preuve. — Nous appliquons le critère (2.1.8).

(2.2.8) *Proposition. — Soient* G *un groupe p-valué et* $(x_i)_{i\in \mathrm{I}}$ *une famille totalement ordonnée d'éléments de* G *qui est une base ordonnée du complété* $\hat{G}$ *de* G. *Soit* μ *un nombre* >0. *Déterminons, pour chaque* $i\in \mathrm{I}$, *l'entier* $k_i\in\mathbf{Z}$ *par les conditions*

(2.2.8.1) $$\omega(x_i)+k_i-1<\mu\leqslant\omega(x_i)+k_i.$$

Alors nous obtenons un système complet de représentants de G *modulo* G_μ *en prenant les éléments*

(2.2.8.2) $$x = \prod_{i\in I} x_i^{\lambda_i},$$

où (λ_i) *parcourt l'ensemble des familles d'entiers rationnels, presque tous nuls, vérifiant*

(2.2.1.3) $$0 \leqslant \lambda_i < p^{k_i}, \qquad \textit{pour chaque } i\in I.$$

Preuve. — C'est une conséquence de la définition (2.2.4) et du lemme (2.2.2).

(2.2.9) *Corollaire.* — *Considérons, dans l'algèbre* $\mathbf{Z}_p[G]$, *les produits ordonnés*

(2.2.9.1) $$z^\alpha = \prod_{i\in I} (x_i - 1)^{\alpha_i}$$

pour $\alpha = (\alpha_i)_{i\in I} \in \mathbf{N}^{(I)}$. *Formons l'algèbre* $\mathbf{F}_p[G/G_\mu]$ *et l'épimorphisme canonique*

(2.2.9.2) $$f : \mathbf{Z}_p[G] \to \mathbf{F}_p[G/G_\mu].$$

Alors $f(z^\alpha) = 0$ *si et seulement s'il existe un* $i\in I$ *tel que* $\alpha_i \geqslant p^{k_i}$. *Ceux des* $f(z^\alpha)$ *qui ne sont pas nuls forment une base de* $\mathbf{F}_p[G/G_\mu]$.

Preuve. — D'après (2.2.8) nous obtenons la base canonique de $\mathbf{F}_p[G/G_\mu]$ comme ensemble des $f(x^\alpha)$, avec

(2.2.9.3) $$x^\alpha = \prod_{i\in I} x_i^{\alpha_i},$$

et

(2.2.9.4) $$\alpha\in\mathbf{N}^{(I)};\ 0 \leqslant \alpha_i < p^{k_i} \text{ pour tout } i\in I.$$

Or nous avons les formules (« du binôme »)

(2.2.9.5) $$x^\alpha = \sum_{\beta\leqslant\alpha} \binom{\alpha}{\beta} z^\beta;$$

(2.2.9.6) $$z^\alpha = \sum_{\beta\leqslant\alpha} (-1)^{|\alpha-\beta|} \binom{\alpha}{\beta} x^\beta.$$

Il en résulte que les $f(z^\alpha)$, où α vérifie (2.2.9.4), forment eux aussi une base de $\mathbf{F}_p[G/G_\mu]$. Quant aux autres $f(z^\alpha)$, ils sont nuls, car chacun contient en facteur $f(x_i - 1)^{p^{k_i}}$ (pour un certain $i\in I$), et

$$f(x_i - 1)^{p^{k_i}} = f(x_i)^{p^{k_i}} - 1 = 0.$$

(2.3) Valuation de la Z_p-algèbre d'un groupe p-valué.

(2.3.1) *Filtration induite sur la* $\mathbf{Z}_p$*-algèbre d'un groupe p-filtré.* — Nous avons vu, en (II, 1.2.1), comment une filtration w d'une $\mathbf{Z}_p$-algèbre associative A induit une p-filtration ω (II, 1.2.10) sur certains sous-groupes G du groupe multiplicatif de A par la formule

(2.3.1.1) $$\omega(x) = w(x-1).$$

Si nous partons d'un groupe p-filtré G, et si nous cherchons à définir sa filtration par la méthode rappelée, il nous suffit de traiter le cas où A est l'algèbre $\mathbf{Z}_p[\mathrm{G}]$. En effet, l'injection de G dans A se prolonge en un homomorphisme d'algèbres $f:\mathbf{Z}_p[\mathrm{G}]\to\mathrm{A}$, et nous définissons la valuation w' de $\mathbf{Z}_p[\mathrm{G}]$ par la formule $w'=w\circ f$. Si nous avons pu obtenir la p-filtration ω à partir de w par la formule (2.3.1.1), nous l'obtenons aussi bien à partir de w'.

(2.3.1.2) *Définition. — Étant donné un groupe p-filtré* G, *nous appelons filtration induite sur l'algèbre* $\mathbf{Z}_p[\mathrm{G}]$ *la borne inférieure w des filtrations (de* $\mathbf{Z}_p$*-algèbre) qui vérifient*

$$w(x-1)\geqslant\omega(x),\qquad \textit{pour tout } x\in\mathrm{G}.$$

S'il existe une filtration w' de $\mathbf{Z}_p[\mathrm{G}]$ telle que $w'(x-1)=\omega(x)$ pour $x\in\mathrm{G}$, alors la filtration induite w possède la même propriété.

(2.3.1.3) *Soit* $f:\mathrm{G}\to\mathrm{H}$ *un morphisme* (II, 1.1.3) *de groupes p-filtrés. Le prolongement naturel* $g:\mathbf{Z}_p[\mathrm{G}]\to\mathbf{Z}_p[\mathrm{H}]$ *est un morphisme de* $\mathbf{Z}_p$*-algèbres filtrées, si* $\mathbf{Z}_p[\mathrm{G}]$ *et* $\mathbf{Z}_p[\mathrm{H}]$ *sont munies de leurs filtrations induites.*

(2.3.2) *Le morphisme fonctoriel* $\mathrm{U}_{\mathrm{mix}}\mathrm{gr}\,\mathrm{G}\to\mathrm{gr}\,\mathbf{Z}_p[\mathrm{G}]$.

Soient G un groupe p-filtré (dont la filtration est notée ω), et w la filtration induite de $\mathbf{Z}_p[\mathrm{G}]$, définie en (2.3.1.2). A son tour la filtration w induit une p-filtration de G, que nous noterons ω^* :

(2.3.2.1) $$\omega^*(x)=w(x-1),\qquad \text{pour } x\in\mathrm{G}.$$

Par définition de w et ω^*, nous avons donc

(2.3.2.2) $$\omega^*(x)\geqslant\omega(x)\qquad \text{pour } x\in\mathrm{G}.$$

Autrement dit, l'application identique Id_{G} est un morphisme de G (filtré par ω) dans G (filtré par ω^*), d'où (II, 1.2.11) un morphisme d'algèbres de Lie mixtes

(2.3.2.3) $$\mathrm{gr}\,\mathrm{G}\to\mathrm{gr}^*\mathrm{G}.$$

Mais, d'après (II, 1.1.9) et (II, 1.2.1), nous avons une représentation canonique (injective)

(2.3.2.4) $$\mathrm{gr}^*\mathrm{G}\to\mathrm{gr}\,\mathbf{Z}_p[\mathrm{G}],$$

le gradué associé $\mathrm{gr}\,\mathbf{Z}_p[\mathrm{G}]$ étant calculé pour la filtration induite w. Nous composons le morphisme (2.3.2.3) et la représentation (2.3.2.4) pour obtenir la représentation

(2.3.2.5) $$\mathrm{gr}\,\mathrm{G}\to\mathrm{gr}\,\mathbf{Z}_p[\mathrm{G}].$$

Enfin, par définition de l'algèbre enveloppante mixte (II, 1.2.7), nous obtenons le *morphisme de* Γ*-algèbres graduées* :

(2.3.2.6) $$f:\mathrm{U}_{\mathrm{mix}}\mathrm{gr}\,\mathrm{G}\to\mathrm{gr}\,\mathbf{Z}_p[\mathrm{G}],$$

dont le caractère fonctoriel s'établit comme en (2.3.1.3).

Nous n'appliquerons la définition précédente qu'au cas d'un groupe p-valué. La structure d'algèbre de Lie mixte se réduit alors à une structure de Γ-algèbre de Lie, et l'algèbre enveloppante mixte est l'algèbre enveloppante en tant que Γ-algèbre.

(2.3.3) *Théorème. — Soit* G *un groupe p-valué* (2.1.2). *Munissons son algèbre* $A = \mathbf{Z}_p[G]$ *de sa filtration induite* w (2.3.1). *Alors* w *est une valuation (de* $\mathbf{Z}_p$*-module) et le morphisme*

$$(2.3.3.1) \qquad f : \mathrm{U\,gr\,G} \to \mathrm{gr}\,\mathbf{Z}_p[G]$$

est un isomorphisme. Si G *est compact, l'algèbre* Al G (II, 2.2.1) *s'identifie, comme extension topologique de* A, *au complété* $\hat{A}$ *de* A *pour sa valuation* w.

Nous prouverons ce théorème pour les groupes de type fini, puis nous passerons au cas général, comme pour le théorème (I, 3.2.1). Démontrons d'abord deux corollaires.

(2.3.4) *Corollaire. — L'algèbre* $A = \mathbf{Z}_p[G]$ *est valuée en tant qu'anneau par la valuation* w.

Preuve. — Puisque w est séparée, le corollaire signifie (I, 2.3.6) que $\mathrm{gr}\,\mathbf{Z}_p[G]$ est sans diviseurs de zéro. Puisque (2.3.3.1) est un isomorphisme, il s'agit de prouver que U gr G est sans diviseurs de zéro. Or gr G est un Γ-module libre, et, utilisant la « filtration croissante » de U gr G ([2], § 2, nº 6), nous sommes ramenés à prouver que *l'algèbre symétrique d'un module libre est sans diviseurs de zéro*, résultat classique dans le langage des polynômes.

(2.3.5) *Corollaire. — Soient* $f : G \to H$ *une isométrie de groupes p-valués et* $g : \mathbf{Z}_p[G] \to \mathbf{Z}_p[H]$ *le prolongement naturel de f. Si les algèbres de groupes sont munies de leurs filtrations induites, g est encore une isométrie.*

Preuve. — Nous avons une injection

$$(2.3.5.1) \qquad \mathrm{gr}\,f : \mathrm{gr\,G} \to \mathrm{gr\,H},$$

qui nous permet (I, 1.2.4) de prendre des *bases adaptées* à gr H et (gr f)(gr G). Le théorème de Poincaré-Birkhoff-Witt ([2], § 2) prouve alors que le morphisme

$$\mathrm{U\,gr}\,f : \mathrm{U\,gr\,G} \to \mathrm{U\,gr\,H}$$

est injectif, ce qui (compte tenu du théorème (2.3.3)) est le corollaire cherché.

(2.3.6) *Lemme. — Si la filtration du groupe p-filtré* G *est discrète* (II, 1.1.5), *le morphisme fonctoriel* (2.3.2)

$$(2.3.6.1) \qquad f : \mathrm{U_{mix}gr\,G} \to \mathrm{gr}\,\mathbf{Z}_p[G]$$

est surjectif.

Preuve. — Notons $\mathcal{N}$ le *sous-monoïde additif* de $\mathbf{R}_+$ engendré par 1 et par les $\omega(x)$, $x \in G$. L'ensemble $\mathcal{N}$ est une *partie discrète* de $\mathbf{R}_+$ (I, 1.1.3).

Pour chaque $\nu \in \mathcal{N}$, nous définissons A_ν comme le sous-$\mathbf{Z}_p$-module de $\mathbf{Z}_p[G]$ engendré par les éléments

$$(2.3.6.2) \qquad z = p^h(y_1 - 1)\dots(y_n - 1), \qquad \text{où}$$

$$(2.3.6.3) \qquad h, n \in \mathbf{N}, \ y_1, \dots, y_n \in G, \ \text{et}$$

$$(2.3.6.4) \qquad h + \omega(y_1) + \dots + \omega(y_n) \geqslant \nu.$$

Nous avons $A_0 = \mathbf{Z}_p[G]$, $A_\nu \supset A_{\nu'}$ pour $\nu \leqslant \nu'$ et $A_\nu . A_{\nu'} \subset A_{\nu+\nu'}$. Si w est la filtration induite de $\mathbf{Z}_p[G]$, nous avons d'autre part $w(z) \geqslant \nu$ pour tout générateur z de A_ν (2.3.6.2).

Il en résulte que la *filtration* w *se définit, pour chaque* $x \in A$, *par la formule*

$$(2.3.6.5) \qquad w(x) = \sup \nu, \qquad x \in A_\nu.$$

Si nous prenons, pour chaque $y \in G$, l'image canonique de $y - 1$ dans $\mathrm{gr}_{\omega(y)} \mathbf{Z}_p[G]$, les éléments ainsi obtenus engendrent la Γ-algèbre associative gr A. Cela signifie que le morphisme f (2.3.6.1) est *surjectif*.

(2.3.7) *Lemme. — Conservons les hypothèses et les notations du lemme* (2.3.6). *Soit* μ *un nombre* > 0. *Formons l'algèbre* $\mathbf{Z}_p[G/G_\mu]$, G_μ *désignant* (II, 1.1.2) *l'ensemble des* $y \in G$ *tels que* $\omega(y) \geqslant \nu$.

Notons g *l'épimorphisme canonique de* $\mathbf{Z}_p[G]$ *sur* $\mathbf{Z}_p[G/G_\mu]$, *et* R *l'idéal engendré dans ce dernier anneau par* p *et par les éléments* $u - 1$, *où* $u \in G/G_\mu$.

Alors, si

$$(2.3.7.1) \qquad m \in \mathbf{N}, \qquad x \in \mathbf{Z}_p[G], \qquad w(x) \geqslant m . \max(\mu, 1),$$

nous avons

$$(2.3.7.2) \qquad g(x) \in \mathrm{R}^m.$$

Preuve. — D'après le lemme (2.3.6), nous pouvons nous ramener au cas où x est de la forme (2.3.6.2), avec

$$(2.3.7.3) \qquad h + \omega(y_1) + \ldots + \omega(y_n) \geqslant m . \max(\mu, 1).$$

Si l'un des y_i vérifie $\omega(y_i) \geqslant \mu$, alors $g(x) = 0$.

Sinon la relation (2.3.7.3) implique

$$(2.3.7.4) \qquad h + n \geqslant m,$$

c'est-à-dire notre lemme.

(2.3.8) *Cas d'un groupe p-valué précompact.* — Soit G un groupe p-valué précompact; sa filtration est *discrète* (2.2.6). Choisissons une *base homogène* $(\xi_i)_{i \in I}$ du Γ-module libre gr G. Nous supposons l'ensemble d'indices I *totalement ordonné*.

Nous notons J l'ensemble $\mathbf{N}^{(I)}$. A chaque $\alpha \in J$, nous associons le monôme ξ^α, défini par le *produit ordonné*

$$(2.3.8.1) \qquad \xi^\alpha = \prod_{i \in I} \xi_i^{\alpha_i},$$

calculé dans la Γ-algèbre U gr G (nous identifions gr G à son image canonique dans U gr G). D'après le théorème de Poincaré-Birkhoff-Witt, les ξ^α, $\alpha \in J$, forment une *base du Γ-module libre* U gr G.

Choisissons maintenant une *famille de représentants* $(x_i)_{i \in I}$ des ξ_i dans G (pour la filtration ω). Les x_i constituent, d'après (2.2.5), une *base ordonnée du complété* $\hat{G}$ *de* G. Posons, pour $i \in I$,

(2.3.8.2) $$\tau_i = \deg \xi_i = \omega(x_i);$$

(2.3.8.3) $$z_i = x_i - 1 \in \mathbf{Z}_p[G].$$

Pour $\alpha \in J$, nous écrivons

(2.3.8.4) $$\tau\alpha = \sum_{i \in I} \tau_i \alpha_i;$$

(2.3.8.5) $$z^\alpha = \prod_{i \in I} z_i^{\alpha_i} \qquad \text{(produit ordonné)}.$$

Puisque les ξ^α forment une base du Γ-module U gr G, la *surjectivité* du morphisme f (2.3.6) se traduit par la propriété suivante, où A désigne l'algèbre $\mathbf{Z}_p[G]$, munie de sa filtration induite (2.3.1) w.

(2.3.8.6) *Pour chaque* $\nu \in \mathbf{R}_+^*$, *le module* A_ν *est engendré, modulo* A_{ν^+}, *par les éléments* $p^h z^\alpha$, *avec* $h \in \mathbf{N}$, $\alpha \in J$, *et* $h + \tau\alpha = \nu$.

Le lemme (2.3.7) prouve que la *filtration* w *est séparée*. En effet, si $x \in A$ avec $w(x) = \infty$, nous avons $g(x) \in R^m$ pour tout $m \in \mathbf{N}$ (avec les notations de (2.3.7)), c'est-à-dire $g(x) = 0$ d'après (II, 2.1.7) puisque G/G_μ est un p-groupe *fini*.

Or, si $x \neq 0$, il existe un $\mu > 0$ tel que $g(x)$ soit non nul (II, 2.2.2).

Comme la filtration w est *discrète*, nous pouvons procéder par approximations successives à partir de (2.3.8.6), comme en (I, 2.3.13), et nous parvenons au résultat suivant.

Quel que soit l'élément $x \in A$, *il existe une famille* $(\lambda_\alpha)_{\alpha \in J}$ *d'entiers* p*-adiques* (avec $v(\lambda_\alpha) + \tau\alpha \to \infty$), *telle que*

(2.3.8.7) $$x = \sum_{\alpha \in J} \lambda_\alpha z^\alpha;$$

(2.3.8.8) $$w(x) = \inf_{\alpha \in J} (v(\lambda_\alpha) + \tau\alpha).$$

(2.3.9) *Fin de la preuve pour les groupes précompacts.* — Montrons que la famille des λ_α est univoquement déterminée par la relation (2.3.8.7).

Nous devons prouver l'énoncé suivant :

(2.3.9.1) *Si* $(\lambda_\alpha)_{\alpha \in J}$ *est une famille d'entiers* p*-adiques telle que* $\sum_{\alpha \in J} \lambda_\alpha z^\alpha$ *converge vers* 0, *alors* $\lambda_\alpha = 0$ *pour tout* α.

Supposons en effet que ces λ_α ne soient pas tous nuls. Soit $h \in \mathbf{N}$ l'entier défini par

(2.3.9.2) $$h = \inf_{\alpha \in J} v(\lambda_\alpha),$$

et soit $\beta \in J$ tel que

(2.3.9.3) $$v(\lambda_\beta) = h.$$

Nous allons appliquer le corollaire (2.2.9). Nous choisissons d'abord μ assez grand pour que $g(z^\beta) \neq 0$, g étant défini comme en (2.3.7). La série

(2.3.9.4) $$\sum_{\alpha \in J} \lambda_\alpha g(z^\alpha)$$

est convergente dans $\mathbf{Z}_p[G/G_\mu]$, d'après le lemme (2.3.7), et sa somme est nulle puisque $\sum_\alpha \lambda_\alpha z^\alpha = 0$. Mais, d'autre part, nous avons choisi h, β et μ de telle sorte que, d'après (2.2.9), la somme de la série (2.3.9.4) soit divisible par p^h mais non par p^{h+1}. Cette contradiction prouve (2.3.9.1).

Pour un groupe p-valué précompact G, la valuation induite w de $A = \mathbf{Z}_p[G]$ est séparée (2.3.8). La famille $(z^\alpha)_{\alpha \in J}$ est *filtrée-libre* (I, 2.1.16) dans A, car (2.3.8.7) implique (2.3.8.8) par *l'unicité* des λ_α, que nous venons d'établir. Les z^α engendrent un *sous-module dense* de A (existence des λ_α).

Le complété $\hat{A}$ de A pour la valuation w admet la base topologique $(z^\alpha)_{\alpha \in J}$; c'est donc une *algèbre compacte* (I, 3.1.5). Nous avons, pour chaque $\mu \in \mathbf{R}_+^*$, un homomorphisme continu $\hat{A} \to \mathbf{Z}_p[G/G_\mu]$, d'après (2.3.7). La famille de ces homomorphismes définit l'application continue $\hat{A} \to \mathrm{Al}\,\hat{G}$ qui est *surjective* (car l'image est dense et compacte) et *injective* (comme nous venons de le prouver). C'est donc un *homéomorphisme*, et toutes les assertions de (2.3.3) sont établies si G est précompact.

(2.3.10) *Fin de la preuve : cas général.* — Soit G un groupe p-valué. Ce groupe est réunion de ses sous-groupes de type fini, qui sont précompacts (2.2.6). Si H et H′ sont deux tels sous-groupes, avec $H \subset H'$, le théorème (2.3.3) *et son corollaire* (2.3.5) s'appliquent à H et H′. Autrement dit, la valuation induite de $\mathbf{Z}_p[H]$ est la *restriction* de la valuation induite de $\mathbf{Z}_p[H']$. Par passage à la réunion, nous démontrons le théorème (2.3.3) pour le groupe G.

(2.3.11) *Application : puissances dans l'algèbre de groupe.* — Soient G un *groupe p-valué complet* et $A = \mathbf{Z}_p[G]$ son algèbre munie de la filtration induite (2.3.3). Pour tout $y \in G$ et tout $\lambda \in \mathbf{Z}_p$, nous avons le développement (1.1.6).

(2.3.11.1)
$$y^\lambda = \sum_{n \in \mathbf{N}} \binom{\lambda}{n} (y-1)^n.$$

La série obtenue converge dans A, bien que cette algèbre ne soit pas complète (sauf si G se réduit à l'unité).

Par multiplication terme à terme des séries, nous obtenons le développement d'un *produit ordonné* (2.2.1). Avec les notations usuelles concernant les monômes et les produits de coefficients binomiaux, nous avons

(2.3.11.2)
$$y^\lambda = \prod_{i \in I} y_i^{\lambda_i} = \sum_{\alpha \in \mathbf{N}^{(I)}} \binom{\lambda}{\alpha} (y-1)^\alpha.$$

Plus particulièrement, supposons G de rang r fini, et reprenons les notations de (2.3.8), l'ensemble I étant formé des entiers $1, \ldots, r$. Les éléments de G sont définis par leurs « coordonnées de seconde espèce » (2.2.5), et nous avons, pour $\lambda \in \mathbf{Z}_p^r$, la formule

(2.3.11.3)
$$x^\lambda = \prod_{1 \leq i \leq r} x_i^{\lambda_i} = \sum_{\alpha \in J} \binom{\lambda}{\alpha} z^\alpha.$$

3. GROUPES ANALYTIQUES

(3.1) Pro-p-groupes analytiques; groupes p-valuables et p-saturables.

(3.1.1) *Groupes analytiques sur* $\mathbf{Q}_p$. — Soit $\mathscr{C}$ une catégorie, où les *objets* sont des ensembles et où les *morphismes* sont des applications ensemblistes. Supposons, de plus, que le *produit* de deux objets soit toujours défini dans $\mathscr{C}$ et coïncide (en tant qu'ensemble) avec le produit ensembliste. Alors nous définissons un *groupe dans la catégorie* $\mathscr{C}$ comme un objet G de $\mathscr{C}$ muni d'une structure de groupe (ensembliste), tel que l'application

(3.1.1.1) $$f : \mathrm{G}\times\mathrm{G}\to\mathrm{G}$$

définie (en notation multiplicative) par $f(x,y)=xy^{-1}$ soit un morphisme dans $\mathscr{C}$. Bien entendu l'application f peut être remplacée par les deux applications « produit » et « inverse ».

Un groupe analytique sur $\mathbf{Q}_p$ est, par définition, un groupe dans la *catégorie des variétés analytiques sur* $\mathbf{Q}_p$ (1.3.3). Nous pourrions définir de même les groupes dans la catégorie des *variétés analytiques strictes* (1.3.5) ou *tayloriennes* (1.3.4).

(3.1.2) *Première définition des pro-p-groupes analytiques.* — Un groupe analytique sur $\mathbf{Q}_p$ possède une structure sous-jacente de *groupe topologique.* Nous disons que c'est un *pro-p-groupe analytique* si c'est un pro-p-groupe (II, 2.1.2). Cette définition est provisoire, car elle suppose *donnée* une structure de variété analytique sur un groupe G, alors que cette structure de variété analytique est déterminée par la structure de *groupe topologique*, et même de simple groupe « *abstrait* ». Comme exemple de groupes analytiques sur $\mathbf{Q}_p$ qui ne sont pas des pro-p-groupes, citons les groupes non compacts, ou les groupes finis qui ne sont pas des p-groupes.

(3.1.3) *Proposition. — Soit* G *un groupe analytique sur* $\mathbf{Q}_p$, *de dimension r. Alors* G *possède un sous-groupe ouvert* H *qui peut être défini (comme groupe topologique) par une p-valuation* ω (2.1.2) *à valeurs entières, pour laquelle* H *est de rang r* (2.1.3) *et p-saturé* (2.1.6).

Preuve. — Prenons des coordonnées analytiques au voisinage de l'élément neutre de G, celui-ci ayant ses coordonnées nulles. Pour $x=(x_i)\in\mathbf{Q}_p^r$, posons $w(x)=\inf\limits_{1\leqslant i\leqslant r} v(x_i)$, v désignant la valuation p-adique du corps $\mathbf{Q}_p$. Par définition notre système de coordonnées nous permet d'*identifier* un certain voisinage de zéro dans $\mathbf{Q}_p^r$ à un voisinage de l'élément neutre dans G.

La fonction f de (3.1.1.1) s'écrivait xy^{-1}, en notation multiplicative de G. Par transport de structure, nous écrivons cette même fonction comme somme d'une série de puissances dans le système de coordonnées analytiques adopté :

(3.1.3.1) $$f(x,y)=x-y+\sum_{\alpha,\beta\in\mathbf{N}^r} a_{\alpha,\beta}x^\alpha y^\beta.$$

Quitte à donner la nouvelle coordonnée $p^{-h}x$ au point du groupe G de coordonnées x, nous pouvons (en prenant l'entier h assez grand) supposer vérifiées les propriétés suivantes.

(3.1.3.2) *Le système de coordonnées identifie* $\mathbf{Z}_p^r$ *à un voisinage de l'élément neutre dans* G.

(3.1.3.3) $w(a_{\alpha,\beta}) \geqslant 0$ *pour tous* α, $\beta \in \mathbf{N}^r$.

(3.1.3.4) *La série* (3.1.3.1) *converge vers* $f(x,y)$ *pour tous* $x, y \in \mathbf{Z}_p^r$.

Pour tout $n \in \mathbf{N}$, les $x \in \mathbf{Z}_p^r$ vérifiant $w(x) \geqslant n$ forment un sous-groupe ouvert de G.

Lorsque n varie, ces sous-groupes constituent un système fondamental de voisinages de l'élément neutre. Pour obtenir le groupe H de l'énoncé, nous pouvons prendre l'un de ces sous-groupes, correspondant à un entier $n \geqslant 2$, et poser

(3.1.3.5) $$\omega(x) = w(x) - n + 1 \quad \text{si } p > 2.$$

(3.1.3.6) $$\omega(x) = w(x) - n + 2 \quad \text{si } p = 2.$$

L'axiome (II, 1.1.1.1) a déjà été vérifié. Pour établir (II, 1.1.1.2), remarquons que le commutateur de deux éléments x et y de G est donné par une série de puissances à coefficients dans $\mathbf{Z}_p^r$ qui s'annule lorsque x *ou* y est nul : chaque terme de la série contient donc en facteur une coordonnée de x *et* une coordonnée de y. Pour démontrer (2.1.2.3), remarquons que la puissance p-ième de $x \in G$ est donnée par une série de puissances en x dont le terme linéaire est px; en effet, si nous écrivons que 0 est élément neutre, nous obtenons $a_{\alpha,\beta} = 0$ pour $|\alpha| + |\beta| \leqslant 1$ dans la formule (3.1.3.1).

Le gradué associé au groupe H pour la filtration ω *coïncide* avec le gradué associé au *groupe additif* $p^n\mathbf{Z}_p^r$ pour la filtration w, *au décalage près des degrés* de $(n-1)$ ou $(n-2)$.

(3.1.4) *Corollaire. — La topologie d'un pro-p-groupe analytique* G *est déterminée par sa structure de groupe « abstrait ». Plus précisément, nous obtenons un système fondamental de voisinages de l'élément neutre dans* G *en prenant, soit les ensembles des* p^n*-ièmes puissances d'éléments de* G, *soit les sous-groupes engendrés par ces* p^n*-ièmes puissances* (n *parcourant* $\mathbf{N}$).

Preuve. — Par définition (3.1.2) G est un groupe analytique sur $\mathbf{Q}_p$ et un pro-p-groupe. Gardons les notations de (3.1.3). Le sous-groupe ouvert H doit être d'indice (G : H) fini, égal à une puissance de p, soit p^e.

Comme H est *p-saturé* par la filtration ω *à valeurs entières*, nous voyons que, pour chaque $n \in \mathbf{N}$, l'*ensemble* E_n des p^n-ièmes puissances des éléments de H est le *sous-groupe* des éléments de *filtration* $\geqslant n+1$ *si* $p > 2$ (resp. de *filtration* $\geqslant n+2$ *si* $p = 2$).

Si E'_n désigne l'ensemble des p^n-ièmes puissances des éléments de G, nous avons (pour $n \in \mathbf{N}$) les inclusions

(3.1.4.1) $$E'_{n+e} \subset E_n \subset E'_n.$$

(3.1.5) *Lemme. — Soient* G *un groupe p-valué complet* (2.1.2) *de rang fini r* (2.1.3) *et* $(x_i)_{1 \leqslant i \leqslant r}$ *une base ordonnée* (2.2.4) *de* G. *Soit* $(y_j)_{1 \leqslant j \leqslant s}$ *une famille d'éléments de* G. *A tout* $\mu \in \mathbf{Z}_p^s$ *nous associons le produit ordonné*

(3.1.5.1) $$y^\mu = \prod_{1 \leqslant j \leqslant s} y_j^{\mu_j},$$

puis les coordonnées $\lambda \in \mathbf{Z}_p^r$ *de ce produit par rapport à la base ordonnée* (x_i), *de telle sorte que*

(3.1.5.2) $$\prod_{1 \leqslant i \leqslant r} x_i^{\lambda_i} = \prod_{1 \leqslant j \leqslant s} y_j^{\mu_j}.$$

Alors λ *est une fonction analytique stricte de* μ. *Plus précisément, les* λ_i *sont donnés par leurs séries de Mahler* (1.2.4).

(3.1.5.3) $$\lambda_i = \sum_{\beta \in \mathbf{N}^s} \binom{\mu}{\beta} c_{i,\beta},$$

avec $c_{i,\beta} \in \mathbf{Z}_p$ *et*

(3.1.5.4) $$v(c_{i,\beta}) \geqslant \Big(\sum_{1 \leqslant j \leqslant s} \beta_j \omega(y_j)\Big) - \omega(x_i).$$

Preuve. — Plaçons-nous dans l'algèbre $\mathbf{Z}_p[G]$ munie de la filtration induite (2.3.3), ou dans son complété Al G.

Pour chaque $\beta \in \mathbf{N}^s$, posons

(3.1.5.5) $$(y-1)^\beta = \prod_{1 \leqslant j \leqslant s} (y_j - 1)^{\beta_j} \qquad \text{(produit ordonné).}$$

Nous avons

(3.1.5.6) $$w((y-1)^\beta) = \sum_{1 \leqslant j \leqslant s} \beta_j \omega(y_j),$$

d'après (2.3.3) et son corollaire (2.3.4) (ce dernier est d'ailleurs inutile ici : nous pourrions remplacer, dans (3.1.5.6), le signe $=$ par $\geqslant$).

Comme en (2.3.11.2), nous avons le développement

(3.1.5.7) $$y^\mu = \sum_{\beta \in \mathbf{N}^s} \binom{\mu}{\beta} (y-1)^\beta.$$

Nous écrivons les $(y-1)^\beta$ par rapport à la *base topologique* (z^α) de Al G (2.3.8) :

(3.1.5.8) $$(y-1)^\beta = \sum_{\alpha \in \mathbf{N}^r} b_{\alpha,\beta} z^\alpha,$$

avec $b_{\alpha,\beta} \in \mathbf{Z}_p$ et

(3.1.5.9) $$w((y-1)^\beta) = \inf_\alpha (v(b_{\alpha,\beta}) + \tau\alpha).$$

Nous obtenons ainsi

(3.1.5.10) $$y^\mu = \sum_{\alpha,\beta} \binom{\mu}{\beta} b_{\alpha,\beta} z^\alpha.$$

Nous égalons y^μ à

(3.1.5.11) $$x^\lambda = \sum_{\alpha \in \mathbf{N}^r} \binom{\lambda}{\alpha} z^\alpha,$$

d'où, pour chaque $\alpha \in \mathbf{N}^r$,

(3.1.5.12) $$\binom{\lambda}{\alpha} = \sum_{\beta \in \mathbf{N}^s} \binom{\mu}{\beta} b_{\alpha,\beta}.$$

Pour $\alpha=\delta_i$ (1.2.1), nous avons $\binom{\lambda}{\alpha}=\lambda_i$ et $\tau\alpha=\tau_i=\omega(x_i)$. La formule (3.1.5.12) se réduit donc à (3.1.5.3), en posant

$$c_{i,\beta}=b_{\delta_i,\beta}, \tag{3.1.5.13}$$

et la formule (3.1.5.4) est une conséquence de (3.1.5.9). Comme les $\omega(y_j)$ sont tous strictement supérieurs à $(p-1)^{-1}$, le critère d'analyticité stricte (1.3.6.3) est vérifié.

(3.1.6) *Définitions.* — *Soit* G *un groupe « abstrait ». Nous disons que* G *est p-valuable (resp. p-saturable) s'il existe une filtration* ω *de* G *pour laquelle* G *est p-valué complet (resp. p-saturé) de rang fini* (2.1).

(3.1.7) *La catégorie des groupes p-valuables. Théorème.*

(3.1.7.1) *Un groupe p-valuable* G *possède une structure canonique de variété analytique stricte de type* $\mathbf{Z}_p^r$ (1.3.5), *pour un certain entier r, dit « rang » ou « dimension » de* G.

Le groupe G *est un groupe dans la catégorie des variétés analytiques strictes, définie comme en* (3.1.1).

Une identification de G *à* $\mathbf{Z}_p^r$ *(qui définit sa structure de variété analytique stricte) s'obtient en prenant les coordonnées (« de deuxième espèce ») par rapport à une base ordonnée quelconque pour une quelconque des filtrations dont l'existence est assurée par la définition* (3.1.6). *En particulier* G *possède une structure de pro-p-groupe analytique* (3.1.2), *et, plus particulièrement encore, de groupe topologique.*

(3.1.7.2) *Soit* $f: G \to H$ *un homomorphisme de groupes p-valuables (en tant que groupes abstraits). Alors f est un morphisme dans la catégorie des variétés analytiques strictes.*

(3.1.7.3) *Le produit direct* $G \times H$ *de deux groupes p-valuables* G *et* H *est p-valuable; la dimension de* $G \times H$ *est la somme des dimensions de* G *et de* H.

(3.1.7.4) *Tout sous-groupe fermé d'un groupe p-valuable est p-valuable.*

(3.1.7.5) *Toute chaîne ascendante de sous-groupes fermés d'un groupe p-valuable est stationnaire.*

(3.1.7.6) *Soit* H *un sous-groupe distingué fermé du groupe p-valuable* G, *tel que le quotient* G/H *soit sans torsion. Alors* G/H *est p-valuable.*

Preuve. — Les assertions (3.1.7.1) et (3.1.7.2) sont des conséquences du lemme (3.1.5).

Nous prouvons (3.1.7.3) en choisissant des p-valuations sur G et H, et en prenant leur produit direct (II, 1.1.4) sur $G \times H$. Sur les sous-groupes de G nous prenons la valuation induite (II, 1.1.3), d'où (3.1.7.4). Le gradué associé gr G est un Γ-module libre de rang fini, qui est donc *noethérien.* A une chaîne ascendante de sous-groupes fermés de G correspond la chaîne ascendante de leurs gradués associés, considérés comme sous-modules de gr G (II, 1.1.8). La chaîne des gradués associés étant stationnaire, celle des sous-groupes fermés l'est aussi, d'après (I, 2.3.15) et (II, 1.1.8).

La preuve de (3.1.7.6) sera donnée en (IV, 3.4.2).

(3.1.8) *Proposition. — Soient* G *un pro-p-groupe analytique de dimension r et, pour chaque* $n \in \mathbf{N}$, G^{p^n} *le sous-groupe engendré par les* p^n*-ièmes puissances des éléments de* G. *Nous avons*

(3.1.8.1) $$r = \lim_{n\to\infty} n^{-1}\log_p(G : G^{p^n}),$$

« $\log_p$ » *désignant le logarithme de base p.*

Preuve. — Si G est p-saturé pour la filtration ω les puissances p^n-ièmes sont les éléments x qui vérifient

(3.1.8.2) $$\omega(x) > n + (p-1)^{-1},$$

elles forment un sous-groupe, et nous avons, pour chaque $n \in \mathbf{N}$

(3.1.8.2) $$\log_p(G : G^{p^n}) = nr.$$

Dans le cas général nous appliquons la proposition (3.1.3), comme en (3.1.4).

(3.1.9) *Proposition. — Soit* ω *une p-valuation d'un groupe p-valuable* G (3.1.6). *Alors* G *est complet et de rang fini pour* ω.

Preuve. — Par définition, G est complet et de rang r pour une certaine p-valuation ω'. Les puissances p-adiques entières x^λ sont définies à partir de la filtration ω', c'est-à-dire de la topologie des p^n-ièmes puissances (3.1.4). Elles restent donc définies (et gardent les mêmes valeurs) pour la filtration ω. D'après (2.2.5), il nous suffit de montrer que G est de rang fini pour ω. Sinon le lemme (2.2.2) nous permettrait d'établir, pour chaque $s \in \mathbf{N}$, l'existence d'un nombre a_s tel que

(3.1.9.1) $$\log_p(G : G^{p^n}) \geqslant s(n - a_s), \qquad \textit{pour tout } n \in \mathbf{N},$$

contrairement à la relation (3.1.8.1) que vérifie G.

(3.1.10) *Corollaire. — Toutes les p-valuations d'un groupe p-valuable* G *peuvent être définies comme des* (x, τ, p)*-filtrations* (II, 3.2.8).

Preuve. — Si $(x_i)_{1\leqslant i\leqslant r}$ est une base ordonnée de G pour la p-valuation ω, et si $\tau_i = \omega(x_i)$, nous voyons, d'après (2.2.4), que ω est la (x, τ, p)-filtration de G. La filtration ω est la borne inférieure des p-filtrations ω' pour lesquelles

$$\omega'(x_i) \geqslant \tau_i \quad (1 \leqslant i \leqslant r).$$

Par contre une (x, τ, p)-filtration d'un groupe p-valuable G peut ne pas être une p-valuation, même si tous les τ_i sont $> (p-1)^{-1}$.

(3.1.11) *Proposition. — Un groupe p-valuable* G *possède une p-valuation à valeurs rationnelles.*

Nous prouverons ultérieurement cette assertion (IV, 3.4.3). Si l'algèbre Al G (II, 2.2.1) est valuée comme en (3.3.3), la valuation de Sat Al G (I, 2.2.11) est alors *discrète.*

(3.1.12) *Proposition. — Soit* G *un groupe p-valué complet de rang fini. Notons t (resp. t') le minimum (resp. le maximum) des filtrations des éléments d'une base ordonnée de* G.

Pour tout nombre C *vérifiant*

(3.1.12.1) $$0 < C < t - (p-1)^{-1},$$

la formule

$$\text{(3.1.12.2)}\qquad \omega'(x)=\omega(x)-\mathrm{C}$$

définit une p-valuation ω' *de* G *pour laquelle le gradué associé est abélien. Pour qu'on puisse choisir* C *de telle sorte que* G *devienne p-saturé (pour* ω'*) il faut et il suffit que*

$$\text{(3.1.12.3)}\qquad t'-t<1.$$

La condition supplémentaire imposée à C *est*

$$\text{(3.1.12.4)}\qquad t'-p(p-1)^{-1}\leqslant \mathrm{C}.$$

Preuve. — Cf. (II, 1.1.11.5) et (2.2.7).

(3.1.13) *Corollaire. — Avec les notations de* (3.1.12), *soit* ν *un nombre strictement positif, vérifiant*

$$\text{(3.1.13.1)}\qquad \nu>t'-1.$$

Alors le sous-groupe G_ν *est p-saturé pour la filtration* ω' *définie par*

$$\text{(3.1.13.2)}\qquad \omega'(x)=\omega(x)-\nu+(p-1)^{-1}+\varepsilon,$$

où ε *est un nombre strictement positif assez petit.*

Preuve. — Nous obtenons une base ordonnée de G_ν (pour ω) en appliquant (2.2.4), et (3.1.13.1) nous assure que (3.1.12.3) est vérifié par le groupe G_ν.

(3.2) Deuxième définition des pro-p-groupes analytiques ; exemples.

(3.2.1) *Lemme. — Soient* G *un groupe analytique sur* $\mathbf{Q}_p$ (3.1.2) *et* K *un sous-groupe ouvert p-valuable* (3.1.6) *de* G. *Nous avons sur* K *deux structures de variété analytique* (1.3.3) : *celle induite par la structure de* G, *et celle sous-jacente à la structure de variété analytique stricte de* K (3.1.7.1). *Ces deux structures coïncident.*

Ce lemme pourrait être admis, car il est connu que les coordonnées « de deuxième espèce » sont des coordonnées analytiques. Voici cependant comment le prouver.

Nous allons utiliser une certaine « *formule du binôme* », donnée par la proposition (6.1), p. 339, de [16]. Corrigeons d'abord une faute d'impression : au lieu de

$$g_n(x)=\sum_{1\leqslant j\leqslant i<\infty}\binom{n}{i}\mathrm{C}_{i,j}(x),$$

il faut lire

$$g_n(x)=\sum_{1\leqslant j\leqslant i<\infty}\binom{n}{j}\mathrm{C}_{i,j}(x).$$

Reprenons les notations et les hypothèses de (3.1.3), en particulier les relations (3.1.3.2) à (3.1.3.4). La fonction f à laquelle nous appliquons la proposition (6.1) de [16] *n'est pas* celle définie par (3.1.3.1), mais la fonction qui exprime le *produit* de deux éléments x et y dans le groupe G. Voici les informations que nous obtenons.

Soit x un élément de G, *identifié à un élément de* $\mathbf{Z}_p^r$ (3.1.3.2). *Pour* $\lambda \in \mathbf{N}$, *la puissance* $x^\lambda \in \mathrm{G}$ *s'écrit sous la forme* (1.2.3)

$$\sum_{n\in\mathbf{N}^*} \mathrm{C}_n(x)\binom{\lambda}{n}. \tag{3.2.1.1}$$

Les fonctions C_n *sont analytiques tayloriennes* (1.3.4). *La série qui définit* C_n *est d'ordre* $\geqslant n$, *c'est-à-dire que ses composantes homogènes de degré* $<n$ *sont nulles. Enfin le terme linéaire de* $\mathrm{C}_1(x)$ *est* x.

Prenons comme sous-groupe H (3.1.3) l'ensemble des x vérifiant $w(x)\geqslant 2$. Pour $x\in\mathrm{H}$ nous avons ainsi $w(\mathrm{C}_n(x))\geqslant 2n$, et la série (3.2.1.1) représente une fonction analytique taylorienne de $\lambda\in\mathbf{Z}_p$, d'après le critère (1.3.6). La *dérivée à l'origine* de cette série s'obtient par dérivation terme à terme. Nous trouvons que la dérivée est égale à la somme de la série

$$\sum_{n\in\mathbf{N}^*} (-1)^{n+1} n^{-1}\mathrm{C}_n(x), \tag{3.2.1.2}$$

et cet élément a *même terme dominant que* x (supposé $\neq 0$), comme nous l'avons vu en (1.1.5).

Si $x\in\mathrm{G}$ est tel que les puissances p-adiques x^λ ($\lambda\in\mathbf{Z}_p$) soient définies (ou encore si x appartient à un sous-groupe de G qui est un pro-p-groupe), l'application $\lambda\mapsto x^\lambda$ de $\mathbf{Z}_p$ dans G est *analytique*, car $x^{p^h}\in\mathrm{H}$ pour h assez grand.

Comme G est un groupe analytique (3.1.1), le produit de deux applications analytiques est analytique. Si les $(y_j)_{1\leqslant j\leqslant s}$ sont des éléments de G tels que les $y_j^{\lambda_j}$ soient définis pour tous $\lambda_j\in\mathbf{Z}_p$, l'application

$$\lambda=(\lambda_1,\ldots,\lambda_s)\mapsto y^\lambda=\prod_{1\leqslant j\leqslant s} y_j^{\lambda_j} \tag{3.2.1.3}$$

est *analytique*. De plus, si η_j est la dérivée à l'origine de l'application $\lambda\mapsto y_j^\lambda$ (rappelons que η_j est un vecteur tangent à G), la dérivée à l'origine de l'application (3.2.1.3) est

$$(\lambda_1,\ldots,\lambda_s)\mapsto \sum_{1\leqslant j\leqslant s}\lambda_j\eta_j. \tag{3.2.1.4}$$

Prenant s égal à la dimension de G, et choisissant convenablement les y_j dans le sous-groupe ouvert K, nous obtenons une dérivée (3.2.1.4) *inversible* (en tant qu'application de $\mathbf{Q}_p$-espaces vectoriels).

Choisissons une base ordonnée de K. Grâce aux coordonnées de deuxième espèce qu'elle définit, l'application $\mathbf{Z}_p^s\to\mathrm{G}$ peut se factoriser en un produit de deux applications $\mathbf{Z}_p^s\to\mathbf{Z}_p^r$ et $\mathbf{Z}_p^r\to\mathrm{G}$. Appliquant le lemme (3.1.5), nous voyons que *l'injection* canonique de K (muni de sa structure analytique sous-jacente) dans G (donné comme groupe analytique) est *analytique* et possède une *dérivée à l'origine surjective*. Cela prouve notre lemme.

(3.2.2) *Deuxième définition des pro-p-groupes analytiques; groupes profinis p-analytiques.* Un groupe G analytique sur $\mathbf{Q}_p$ (3.1.1) possède des sous-groupes ouverts

p-valuables (3.1.3). La donnée d'un sous-groupe ouvert p-valuable de G définit sa structure analytique sur $\mathbf{Q}_p$ (3.2.1).

Si, de plus, G est un pro-p-groupe, alors tous les sous-groupes ouverts sont d'indice fini, égal à une puissance de p (II, 2.1.2), et tout sous-groupe d'indice égal à une puissance de p est ouvert (3.1.4). Les sous-groupes engendrés par les puissances p^n-ièmes sont p-valuables pour n assez grand (3.1.3).

La structure analytique d'un pro-p-groupe analytique (3.1.2) se reconstruit ainsi à partir de sa structure de groupe abstrait. Nous remplaçons donc (3.1.2) par la définition suivante.

Un pro-p-groupe analytique est un groupe qui possède un sous-groupe p-valuable (3.1.6) *d'indice égal à une puissance de p.*

Nous nous intéressons surtout aux pro-p-groupes. Mais nous pouvons, plus généralement, définir les *groupes profinis p-analytiques* comme les groupes qui possèdent un *sous-groupe p-valuable d'indice fini.* Un tel groupe a une structure analytique sur $\mathbf{Q}_p$, et est compact (c'est-à-dire profini puisque totalement discontinu). Mis à part les groupes finis, qui sont p-analytiques (de dimension zéro) pour tout p, un groupe profini ne peut être p-analytique que pour un nombre premier p au plus. Pour $n \in \mathbf{N}$ assez grand, le sous-groupe engendré par les $n!$-ièmes puissances est p-valuable.

(3.2.3) *La catégorie des pro-p-groupes analytiques. Théorème. — Soient* G *et* H *deux pro-p-groupes analytiques.*

(3.2.3.1) *Tout homomorphisme* $f: \mathrm{G} \to \mathrm{H}$ *est analytique.*

(3.2.3.2) *Le produit* $\mathrm{G} \times \mathrm{H}$ *est analytique.*

(3.2.3.3) *Tout sous-groupe fermé de* G *est analytique.*

(3.2.3.4) *Toute chaîne croissante de sous-groupes fermés de* G *est stationnaire.*

(3.2.3.5) *Si* K *est un sous-groupe fermé distingué de* G, *le quotient* G/K *est un pro-p-groupe analytique.*

Preuve. — Pour $i = 1, 2, 3, 4, 5$ l'assertion (3.2.3, (i)) est une conséquence de (3.1.7, ($i+1$)), compte tenu de la définition (3.2.2) des pro-p-groupes analytiques. Précisons seulement la démonstration de (3.2.3.5). Nous prenons un sous-groupe ouvert p-valuable G′ de G, et une p-valuation ω de G′. Pour ν assez grand, les sous-groupes G'_ν et $\mathrm{G}'_\nu \cap \mathrm{K}$ sont tous deux p-saturés pour une valuation ω', déduite de ω par translation, comme en (3.1.13). Le nombre ν étant ainsi choisi, si un élément $x \in \mathrm{G}'_\nu$ a sa p-ième puissance x^p dans $\mathrm{G}'_\nu \cap \mathrm{K}$, il appartient lui-même à $\mathrm{G}'_\nu \cap \mathrm{K}$. Cela prouve que le groupe quotient $\mathrm{G}'_\nu/(\mathrm{G}'_\nu \cap \mathrm{K})$ est sans torsion; il est donc p-valuable (3.1.7.6), et il est isomorphe au groupe $(\mathrm{G}'_\nu\mathrm{K}/\mathrm{K})$ dont l'indice dans G/K est une puissance de p.

(3.2.4) *Exemple d'un groupe nilpotent de dimension quatre (exercice).* — Considérons le groupe G engendré dans la catégorie des pro-p-groupes (II, 2.1.2) par deux générateurs x_1, x_2 liés par les relations

(3.2.4.1) $$(x_3, x_2) = (x_4, x_1) = (x_4, x_2) = 1,$$

où nous avons posé

(3.2.4.2) $$x_3=(x_2, x_1);$$

(3.2.4.3) $$x_4=(x_3, x_1).$$

Un élément $y\in G$ s'écrit, d'une manière et d'une seule,

(3.2.4.4) $$y=x_1^{\lambda_1}x_2^{\lambda_2}x_3^{\lambda_3}x_4^{\lambda_4},$$

où $\lambda_1, \lambda_2, \lambda_3, \lambda_4\in\mathbf{Z}_p$. Si z est un autre élément de G, donné par

(3.2.4.5) $$z=x_1^{\mu_1}x_2^{\mu_2}x_3^{\mu_3}x_4^{\mu_4},$$

nous avons

(3.2.4.6) $$yz^{-1}=x_1^{\nu_1}x_2^{\nu_2}x_3^{\nu_3}x_4^{\nu_4},$$

(3.2.4.7) $$\begin{cases} \nu_1=\lambda_1-\mu_1; \\ \nu_2=\lambda_2-\mu_2; \\ \nu_3=\lambda_3-\mu_3+\mu_1(\mu_2-\lambda_2); \\ \nu_4=\lambda_4-\mu_4+\mu_1(\mu_3-\lambda_3)+\frac{1}{2}(\lambda_2-\mu_2)\mu_1(\mu_1+1). \end{cases}$$

Pour tout nombre $t>(p-1)^{-1}$, le groupe G est *p-valué* pour sa (t, p)-filtration ω, qui vérifie

(3.2.4.8) $$\omega(x_1)=\omega(x_2)=t;\ \omega(x_3)=2t;\ \omega(x_4)=3t,$$

et $\{x_1, x_2, x_3, x_4\}$ est une base ordonnée de G.

Pour $p=2$ ou 3, le groupe G *n'est pas p-saturable*, car l'élément x_4, qui est un commutateur de poids 3, devrait être une p-ième puissance. Par contre, pour $p>3$, le groupe G est p-saturé pour sa (t, p)-filtration, si $(p-1)^{-1}<t\leqslant\frac{1}{3}p(p-1)^{-1}$.

Les formules (3.2.4.7) sont à coefficients p-entiers pour $p\geqslant 3$. Nous verrons en (3.3) pourquoi il en est ainsi pour $p>3$.

Pour $p=2$, nous voyons que les formules donnant l'inverse d'un élément ne sont pas à coefficients p-entiers. Si nous remplaçons la base ordonnée $\{x_1, x_2, x_3, x_4\}$ par la base ordonnée $\{x_4, x_3, x_2, x_1\}$, les formules de transformation sont donc *analytiques strictes* (1.3.5), *mais non pas tayloriennes* (1.3.4).

(3.2.5) *Exemple d'un pro-p-groupe analytique sans torsion qui admet des coordonnées de deuxième espèce mais n'est pas p-valuable (exercice).*

Soit Ω l'anneau valué obtenu en adjoignant à $\mathbf{Z}_p$ une racine p-ième primitive ξ de l'unité. Rappelons [25] que la valuation v de Ω est unique et que $v(\xi-1)=(p-1)^{-1}$. L'élément $\xi^x\in\Omega$ est défini pour tout $x\in\mathbf{Z}_p$, et ne dépend que de la classe de x modulo p.

Construisons un groupe G, produit semi-direct des groupes additifs de $\mathbf{Z}_p$ et de Ω, un élément $x \in \mathbf{Z}_p$ opérant sur Ω en le multipliant par ξ^x. Les éléments de G sont les couples $\{x, y\}$, où $x \in \mathbf{Z}_p$ et $y \in \Omega$. Le produit est défini dans G par

$$\{x,y\}\{x',y'\} = \{x+x', \xi^{x'}y+y'\}. \tag{3.2.5.1}$$

Les commutateurs et les p-ièmes puissances sont donnés par les formules

$$(\{x,y\},\{x',y'\}) = \{0, (\xi^{x'}-1)y-(\xi^x-1)y'\}; \tag{3.2.5.2}$$

$$\{x,y\} = \{px, (\sum_{0 \leqslant i < p} \xi^{ix})y\}. \tag{3.2.5.3}$$

Soit δ un nombre $>(p-1)^{-1}$. Définissons une fonction ω sur G en posant

$$\omega(\{x,y\}) = \min(v(x)+(p-1)^{-1}, v(y)+\delta). \tag{3.2.5.4}$$

La fonction ω est une p-filtration, et vérifie tous les axiomes des p-valuations, à l'exception de (2.1.2.2) qui doit être remplacé par une inégalité large :

$$\omega(\{x,y\}) \geqslant (p-1)^{-1}, \qquad \text{pour tout } \{x,y\} \in \mathrm{G}. \tag{3.2.5.5}$$

Le groupe G n'est pas p-valuable. En effet la formule (3.2.5.3) montre que $\{x,y\} \mapsto \{x,y\}^p$ n'est pas une application injective dans G, contrairement aux groupes p-valués (2.1.4).

Le groupe G admet des coordonnées de deuxième espèce, c'est-à-dire s'écrit comme produit de groupes isomorphes à $\mathbf{Z}_p$, puisqu'il est produit semi-direct de deux groupes commutatifs.

D'autre part les éléments $\{x,y\}$ de G, où x est divisible par p, constituent un sous-groupe commutatif d'indice p. Du point de vue « infinitésimal » (algèbres de Lie, etc.), le groupe G ne se distingue pas des groupes commutatifs.

(3.2.6) *Groupe multiplicatif d'une algèbre (exercice).* — Soit A une $\mathbf{Z}_p$-*algèbre associative valuée complète* (I, 2.2.4). L'ensemble G des éléments $x \in \mathrm{A}$ vérifiant $w(x-1) > (p-1)^{-1}$ est un *groupe multiplicatif p-valué complet* pour la filtration ω, définie par $\omega(x) = w(x-1)$.

Dans le cas où A est *saturée* (I, 2.2.10), nous pouvons calculer les *logarithmes* (1.1.5) des éléments de G et, réciproquement, nous obtenons les éléments de G comme *exponentielles* (1.1.4) des éléments de A de filtration $>(p-1)^{-1}$. Nous voyons alors (1.1.8) que G est *p-saturé* (2.1.6).

Si la $\mathbf{Z}_p$-algèbre associative A est un $\mathbf{Z}_p$-module libre de rang fini, le groupe multiplicatif A^* des éléments inversibles de A est un *groupe profini p-analytique* (3.2.2). L'algèbre A est complète pour chacune de ses valuations w (I, 3.1.4), à laquelle correspond un *sous-groupe p-valué* G, *ouvert dans* A^* (et qui dépend, en général, du choix de w).

(3.2.7) *Les groupes* $\mathrm{GL}_n(\Omega)$ *et leurs p-sous-groupes de Sylow (exercice).* — Soit K une extension algébrique finie du corps $\mathbf{Q}_p$, munie de sa valuation p-adique v [25]. Nous notons e l'indice de ramification absolue de K. C'est le plus petit entier naturel tel que $ev(x) \in \mathbf{Z}$ pour tout $x \in \mathrm{K}$. Nous avons donc l'équivalence

$$v(x) > 0 \Leftrightarrow v(x) \geqslant e^{-1}, \qquad \textit{pour } x \in \mathrm{K}. \tag{3.2.7.1}$$

Appelons Ω l'anneau des entiers de K, et $A = M_n(\Omega)$ l'anneau des matrices $n \times n$ à coefficients dans Ω.

Le groupe *linéaire général* $GL_n(\Omega)$ est le groupe multiplicatif des éléments inversibles de A; le groupe *linéaire spécial* $SL_n(\Omega)$ est le sous-groupe de $GL_n(\Omega)$ formé des éléments de déterminant 1.

Par restriction des scalaires, la Ω-algèbre A devient une $\mathbf{Z}_p$-algèbre (de rang fini), et nous pouvons appliquer les résultats de (3.2.6). La valuation la plus simple de A est donnée par la formule

(3.2.7.2) $$w(X) = \min_{1 \leqslant i, j \leqslant n} v(x_{ij}),$$

où les x_{ij} sont les coefficients de la matrice $X \in A$.

Pour chaque nombre réel $\nu \geqslant 0$, nous avons un *sous-groupe « de congruence »* de $GL_n(\Omega)$, formé des X vérifiant $w(X-1) > \nu$. Pour $\nu = 0$, ce sous-groupe est le noyau de l'épimorphisme $GL_n(\Omega) \to GL_n(k)$, k désignant le corps résiduel de K; pour $\nu = (p-1)^{-1}$ nous obtenons le sous-groupe G de (3.2.6). Ces deux sous-groupes coïncident si $(p-1)^{-1} < e^{-1}$.

Pour obtenir un p-sous-groupe de Sylow ([29], chap. Ier, 1.4) de $GL_n(\Omega)$, nous prenons l'image réciproque d'un p-sous-groupe de Sylow de $GL_n(k)$. Comme la seule représentation irréductible d'un p-groupe fini sur un corps de caractéristique p est la représentation unité ([25], théorème 2, p. 146), les matrices triangulaires unipotentes constituent un sous-groupe de Sylow dans $GL_n(k)$. Remontons dans $GL_n(\Omega)$, et précisons les notations.

(3.2.7.3) *Nous notons* $SY_n(\Omega)$ *le p-sous-groupe de Sylow de* $GL_n(\Omega)$ *formé des matrices* $X = (x_{ij})$ *vérifiant* $v(x_{ij} - \delta_{ij}) > 0$ *pour* $1 \leqslant j \leqslant i \leqslant n$, *où* δ_{ij} *est le symbole de Kronecker.*

(3.2.7.4) *Nous notons* $SSY_n(\Omega)$ *le sous-groupe de* $SY_n(\Omega)$ *formé des matrices de déterminant* 1.

Le groupe $SSY_n(\Omega)$ est un p-sous-groupe de Sylow de $SL_n(\Omega)$.

Lorsque n est assez grand (en tout cas si $n \geqslant p-1$), le pro-p-groupe $SY_n(\Omega)$ contient des éléments d'ordre p et n'est donc pas p-valuable. Par contre, *si nous supposons vérifiée la condition*

(3.2.7.5) $$ne < p-1,$$

les groupes $SY_n(\Omega)$ *et* $SSY_n(\Omega)$ *sont p-saturables.*

En effet, la condition (3.2.7.5) équivaut à l'existence d'un nombre rationnel α vérifiant

(3.2.7.6) $$\alpha > (p-1)^{-1} \quad \textit{et} \quad (n-1)\alpha < e^{-1} - (p-1)^{-1}.$$

Choisissons un tel nombre α, puis une extension (algébrique finie) K′ de K qui contient un élément a de valuation α. Notons Ω' l'anneau des entiers de K′, w la valuation de $M_n(\Omega')$ définie par la formule (3.2.7.2), et $D \in GL_n(K')$ la *matrice diagonale* de coefficients $d_{ij} = a^i \delta_{ij}$. Appelons f *l'automorphisme intérieur* de $M_n(K')$ défini par $f(X) = D^{-1}XD$ et enfin B l'ensemble des $X \in M_n(K)$ pour lesquels $f(X) \in M_n(\Omega')$ (cette dernière définition utilise les inclusions naturelles des anneaux de matrices).

Il en résulte que B est une $\mathbf{Z}_p$-algèbre (et même une Ω-algèbre) *associative saturée pour la filtration* $w' = w \circ f$.

Le calcul montre que $SY_n(\Omega)$ *est formé des* $X \in B$ *vérifiant* $\omega(X) = w'(X - 1) > (p-1)^{-1}$. Ce groupe est donc p-saturé par la filtration ω (3.2.6).

Si $X \in SY_n(\Omega)$, nous avons $v(1 - \det X) > (p-1)^{-1}$. Il en résulte que $\det X^p = 1$ implique $\det X = 1$, ce qui prouve que $SSY_n(\Omega)$ est p-saturé par ω.

Nous avons plongé un p-sous-groupe de Sylow de $GL_n(\Omega)$ dans un sous-groupe de congruences de $GL_n(\Omega')$. Cet artifice pourrait être dissimulé par une définition directe de la filtration ω.

(3.3) Les groupes p-saturables et le foncteur Ala.

(3.3.1) *Lemme. — Reprenons les hypothèses et les notations du lemme* (3.1.5). *Supposons, de plus, que le groupe* G *soit p-saturé* (2.1.6). *Alors* λ *est une fonction analytique taylorienne de* μ (1.3.4).

Preuve. — D'après (2.2.7), l'hypothèse supplémentaire se traduit par les inégalités

$$\omega(x_i) \leqslant p(p-1)^{-1}, \tag{3.3.1.1}$$

vérifiées par les filtrations des éléments x_i de la base ordonnée de G. Si t désigne le minimum des $\omega(y_j)$, pour $1 \leqslant j \leqslant s$, la formule (3.1.5.4) nous donne

$$v(c_{i,\beta}) \geqslant t|\beta| - p(p-1)^{-1}, \tag{3.3.1.2}$$

pour tout $\beta \in \mathbf{N}^s$ et $1 \leqslant i \leqslant r$. Comme nous avons $v(\beta!) = (p-1)^{-1}(|\beta| - \text{Schiff}\,\beta)$, nous obtenons

$$v(c_{i,\beta}) - v(\beta!) \geqslant |\beta|(t - (p-1)^{-1}) + (p-1)^{-1}(\text{Schiff}\,\beta - 1) - 1. \tag{3.3.1.3}$$

D'après le critère d'analyticité taylorienne (1.3.6.2), notre lemme équivaut à affirmer que le premier membre de (3.3.1.3) est toujours $\geqslant 0$ (nous savons déjà qu'il tend vers $+\infty$ avec $|\beta|$, d'après (3.1.5)). Or, le nombre en question est entier, et il nous suffit de montrer qu'il est > -1. Comme $t > (p-1)^{-1}$, le résultat cherché est mis en évidence par la formule (3.3.1.3) si $\beta \neq 0$; si $\beta = 0$, nous avons $c_{i,\beta} = 0$.

(3.3.2) *La catégorie des groupes p-saturables. Théorème.*

(3.3.2.1) *Un groupe p-saturable* G *possède une structure canonique de variété analytique taylorienne de type* $\mathbf{Z}_p^r$ (1.3.4), *r désignant la dimension de* G. *Le groupe* G *est un groupe dans la catégorie des variétés analytiques tayloriennes, définie comme en* (3.1.1).

Une identification de G *à* $\mathbf{Z}_p^r$ *(qui définit sa structure de variété analytique taylorienne) s'obtient en prenant les coordonnées par rapport à une base ordonnée pour l'une quelconque des filtrations qui font de* G *un groupe p-saturé.*

(3.3.2.2) *Soit* $f: \mathrm{G} \to \mathrm{H}$ *un homomorphisme de groupes p-saturables. Alors f est un morphisme dans la catégorie des variétés analytiques tayloriennes.*

(3.3.2.3) *Le produit direct* $\mathrm{G} \times \mathrm{H}$ *de deux groupes p-saturables est p-saturable.*

(3.3.2.4) *Soit* H *un sous-groupe distingué fermé du groupe p-saturable* G, *tel que le quotient* G/H *soit sans torsion. Alors* G/H *est p-saturable. Plus précisément, si* ω *est une filtration pour laquelle* G *est p-saturé, le groupe* G/H *est p-saturé pour la filtration quotient de* ω (II, 1.1.4).

(3.3.3) *Preuve.* — Les assertions (3.3.2.1) et (3.3.2.2) sont des conséquences du lemme (3.3.1). Nous prouvons (3.3.2.3) en prenant sur $\mathrm{G} \times \mathrm{H}$ le produit direct de deux filtrations pour lesquelles G et H sont p-saturés. Démontrons enfin (3.3.2.4).

Appliquons le théorème des bases adaptées (I, 1.2.4) au Γ-module gr G et à son sous-module gr H (calculés pour la filtration ω de G et sa restriction à H). Alors *la base de* gr H *est une partie de la base de* gr G. Sinon il existerait un élément homogène $\xi \in \operatorname{gr} \mathrm{G}$ vérifiant $\xi \notin \operatorname{gr} \mathrm{H}$ et $\pi\xi \in \operatorname{gr} \mathrm{H}$. Un représentant x de $\pi\xi$ dans H posséderait une racine p-ième dans G, mais non dans H, contrairement à l'hypothèse que G/H est sans torsion.

D'après (2.2.5), nous pouvons prendre une base ordonnée de G, soit $(x_i)_{1 \leqslant i \leqslant r}$, de telle sorte qu'une base ordonnée de H soit formée des x_i, où $s < i \leqslant r$.

Si f désigne l'épimorphisme canonique $\mathrm{G} \to \mathrm{G/H}$, la filtration quotient de G/H est définie par la formule (I, 2.1.7.1)

(3.3.3.1)
$$\omega(\mathrm{G/H}; x) = \sup_{f(y)=x} \omega(y).$$

Parmi les $y \in \mathrm{G}$ tels que $f(y) = x$, il en existe un, et un seul, de la forme

(3.3.3.2)
$$y = \prod_{1 \leqslant i \leqslant s} x_i^{\lambda_i} \qquad (\lambda_i \in \mathbf{Z}_p)$$

et, d'après (2.2.4.2), la borne supérieure de (3.3.3.1) est atteinte en cet élément. Il en résulte que la filtration quotient est une p-valuation pour laquelle G/H admet les éléments $f(x_i)$, où $1 \leqslant i \leqslant s$, comme base ordonnée. Les relations $\omega(\mathrm{G/H}; f(x_i)) = \omega(x_i)$ montrent (2.2.7) que G/H est p-saturé.

(3.3.4) *Applications analytiques tayloriennes d'un groupe p-saturable dans un* $\mathbf{Z}_p$*-module complet.* — Soient G un groupe p-saturable (3.1.6) et M un $\mathbf{Z}_p$-module complet (II, 2.2.4). Choisissons une filtration ω de G pour laquelle ce groupe est p-saturé, et une base ordonnée $(x_i)_{1 \leqslant i \leqslant r}$ pour cette filtration. Un élément $x \in \mathrm{G}$ possède alors comme coordonnées l'élément $\lambda \in \mathbf{Z}_p^r$, selon la formule

(3.3.4.1)
$$x = \prod_{1 \leqslant i \leqslant r} x_i^{\lambda_i} \qquad \text{(produit ordonné).}$$

Une application analytique taylorienne de G *dans* M est une application $f: \mathrm{G} \to \mathrm{M}$ donnée par une série de puissances (1.3.4).

(3.3.4.2)
$$f(x) = \sum_{\alpha \in \mathbf{N}^r} \lambda^\alpha d_\alpha,$$

où les d_α *sont des éléments de* M *qui tendent vers zéro* (suivant le filtre des complémentaires des parties finies de $\mathbf{N}^r$).

D'après (3.3.2) cette définition des applications analytiques tayloriennes est *indépendante du choix de la filtration et de la base.*

Si $g : \mathrm{M} \to \mathrm{M}'$ est une application linéaire et continue de $\mathbf{Z}_p$-modules complets, l'application composée $g \circ f$ est analytique taylorienne.

Le critère d'analyticité taylorienne (1.3.6.2) entraîne la conséquence suivante.

(3.3.4.3) *Il existe un $\mathbf{Z}_p$-module complet sans torsion* M_0 *et une application analytique taylorienne* $f_0 : \mathrm{G} \to \mathrm{M}_0$, *tels que toute application analytique taylorienne* $f : \mathrm{G} \to \mathrm{M}$ *se factorise en* $f = g \circ f_0$, *où* g *est un morphisme dans la catégorie des* $\mathbf{Z}_p$*-modules complets (c'est-à-dire* (II, 2.2.4) *une application linéaire continue). La factorisation est unique si* M *est sans torsion.*

Nous pouvons prendre pour M_0 le module produit $\mathbf{Z}_p^{\mathrm{J}}$, où $\mathrm{J} = \mathbf{N}^r$. Écrivons les éléments de M_0 comme des séries : $\sum_{\alpha \in \mathrm{J}} \mu_\alpha e_\alpha$, où $\mu_\alpha \in \mathbf{Z}_p$. Définissons l'application f_0, dans un système de coordonnées de G, par la formule

$$f_0(x) = \sum_{\alpha \in \mathbf{N}^r} \alpha! \binom{\lambda}{\alpha} e_\alpha. \tag{3.3.4.4}$$

La propriété universelle explicitée en (3.3.4.3) définit le couple (M_0, f_0) à un isomorphisme canonique près.

Remarquons que, si nous remplaçons « analytique taylorienne » par « analytique stricte » (1.3.5), le problème d'application universelle n'admettrait pas de solution (sauf si G se réduit à l'élément neutre).

(3.3.5) *Le foncteur* Ala. — Conservons les notations de (3.3.4). Nous allons montrer que le module M_0 défini en (3.3.4.3) par une propriété universelle possède une *structure canonique de* $\mathbf{Z}_p$*-algèbre associative compacte, qui en fait une extension de l'algèbre complétée* Al G, définie en (II, 2.2.1).

Nous appliquons d'abord le théorème (2.3.3) : le choix de ω nous permet de considérer Al G comme une $\mathbf{Z}_p$-algèbre valuée, possédant la base topologique $(z^\alpha)_{\alpha \in \mathrm{J}}$ (avec les notations de (2.3.8)). Nous avons (2.3.11.3)

$$\prod_{1 \leqslant i \leqslant r} x_i^{\lambda_i} = \sum_{\alpha \in \mathrm{J}} \binom{\lambda}{\alpha} z^\alpha; \tag{3.3.5.1}$$

$$w(z^\alpha) = \sum_{1 \leqslant i \leqslant r} \alpha_i \omega(x_i). \tag{3.3.5.2}$$

Nous construisons (I, 2.2.11) l'algèbre Sat Al G, *saturée de l'algèbre valuée* Al G.

L'algèbre Sat Al G contient des éléments e_α vérifiant

$$z^\alpha = \alpha!\, e_\alpha \qquad (\text{pour tout } \alpha \in \mathbf{N}^r), \tag{3.3.5.3}$$

et ces éléments tendent vers zéro dans Sat Al G.

Notons Ala G le *sous-module fermé de* Sat Al G *engendré par les* e_α, $\alpha \in \mathbf{N}^r$. Nous voyons que le module Ala G s'identifie canoniquement au module M_0 de (3.3.4.3), l'application f_0 étant remplacée par l'injection canonique de G dans Ala G. Nous avons les inclusions

$$(3.3.5.4) \qquad \text{Al G} \subset \text{Ala G} \subset \text{Sat Al G}.$$

L'injection canonique (ou inclusion) de G dans Ala G est analytique taylorienne, tandis que l'injection dans Al G n'est même pas analytique stricte (sauf si $G=\{1\}$).

L'application $G\times G \to G$ définie par $x, y \mapsto xy$ est analytique taylorienne (3.3.2.1). Il en est de même de l'application composée $G\times G \to \text{Ala G}$. Identifions $G\times G$ à $\mathbf{Z}_p^r \times \mathbf{Z}_p^r$ par notre système de coordonnées, et traduisons notre dernière assertion, compte tenu du critère (1.3.6.2) et de (3.3.5.1). Nous voyons que, pour tous α, $\beta \in \mathbf{N}^r$, l'élément $(\alpha!\,\beta!)^{-1} z^\alpha z^\beta$, c'est-à-dire $e_\alpha e_\beta$, appartient à Ala G. Autrement dit Ala G est une *sous-algèbre compacte* de Sat Al G. La structure d'algèbre de Ala G est déterminée par la propriété d'être une extension de Al G. Résumons les résultats obtenus.

A chaque groupe p-saturable G *nous associons une* $\mathbf{Z}_p$*-algèbre compacte* Ala G, *qui est une extension de l'algèbre* Al G (II, 2.2.1). *L'injection canonique de* G *dans* Ala G *est analytique taylorienne. Chaque application analytique taylorienne de* G *dans un* $\mathbf{Z}_p$*-module complet* M *se prolonge en une application linéaire continue de* Ala G *dans* M; *ce prolongement est unique si* M *est sans torsion. Chaque p-valuation* ω *de* G *définit sur* Ala G *une structure de* $\mathbf{Z}_p$*-algèbre valuée, et* Ala G *s'identifie à une sous-algèbre de* Sat Al G (2.3.3).

La propriété (3.3.2.2) montre que Ala est un *foncteur covariant* défini sur la catégorie des groupes p-saturables.

Si G et H sont deux groupes p-saturables, alors $\text{Ala}(G\times H)$ s'identifie au produit tensoriel complété $\text{Ala G} \hat{\otimes}_{\mathbf{Z}_p} \text{Ala H}$ (I, 3.2.9).

(3.4) Critères d'analyticité; extensions de groupes analytiques.

(3.4.1) *Position du problème.* — Nous avons défini les pro-p-groupes analytiques comme des groupes abstraits possédant certaines propriétés (3.2.2). La vérification directe de ces propriétés est parfois malaisée; c'est pourquoi nous allons indiquer des conditions qui entraînent qu'un groupe G est un pro-p-groupe analytique. Les principaux résultats concernent le cas où G est *donné* comme un *pro-p-groupe* (II, 2.1.2) *de type fini* (II, 2.1.4).

(3.4.2) *Proposition.* — *Supposons que la p-filtration* ω *définisse la topologie du pro-p-groupe* G, *et qu'il existe un nombre* $m > (p-1)^{-1}$ *tel que, pour tout* $\nu \geqslant m$ *l'application*

$$(3.4.2.1) \qquad P : \text{gr}_\nu G \to \text{gr}_{\nu+1} G$$

définie en (II, 1.2.11) *soit surjective. Alors* G *est un pro-p-groupe analytique.*

Preuve. — Le quotient du groupe *compact* G par son sous-groupe *ouvert* G_{m+1} est *fini*. Il n'y a donc qu'un nombre fini de nombres ν vérifiant

$$(3.4.2.2) \qquad m \leqslant \nu < m+1, \quad \text{et}$$

$$(3.4.2.3) \qquad \text{gr}_\nu G \neq 0.$$

Pour ces nombres ν, le groupe $\mathrm{gr}_\nu G$ est fini, c'est-à-dire est un espace vectoriel de *dimension finie* sur le corps premier $\mathbf{F}_p$, et nous avons (par hypothèse) la suite d'*épimorphismes* ($\mathbf{F}_p$-linéaires)

(3.4.2.4) $$\mathrm{gr}_\nu G \to \mathrm{gr}_{\nu+1} G \to \ldots \to \mathrm{gr}_{\nu+i} G \to \mathrm{gr}_{\nu+i+1} G \to \ldots$$

La dimension de $\mathrm{gr}_{\nu+i} G$ est une fonction décroissante de i, à valeurs dans $\mathbf{N}$. Elle est donc stationnaire, ce qui signifie que $\mathrm{gr}_{\nu+i} G \to \mathrm{gr}_{\nu+i+1} G$ est *bijectif* pour i assez grand.

Il existe donc un nombre $m' \geqslant m$, tel que, pour $\lambda \geqslant m'$, l'application

(3.4.2.5) $$\mathrm{gr}_\lambda G \to \mathrm{gr}_{\lambda+1} G$$

soit bijective. Cela entraîne que le sous-groupe $G_{m'}$ est *p-valué de rang fini* (et même p-saturable).

(3.4.3) *Théorème. — Soient* G *un pro-p-groupe de type fini,* $(x_i)_{1 \leqslant i \leqslant r}$ *une famille de générateurs de* G, *et* $(\tau_i)_{1 \leqslant i \leqslant r}$ *une famille de nombres strictement positifs. Munissons* G *de sa* (x, τ, p)*-filtration* (II, 3.2.8). *Soient t le plus grand des τ_i et m un nombre* $>(p-1)^{-1}$. *Si les applications*

(3.4.3.1) $$P : \mathrm{gr}_\nu G \to \mathrm{gr}_{\nu+1} G$$

sont surjectives pour tous les nombres ν vérifiant

(3.4.3.2) $$m \leqslant \nu < m + t,$$

alors G *est analytique.*

Preuve. — Nous avons vu, en (II, 3.2.8), que la p-filtration ω définit la topologie de G et que l'algèbre de Lie mixte gr G est engendrée par les images respectives des x_i dans $\mathrm{gr}_{\tau_i} G$.

La proposition (II, 3.3.6) prouve que les hypothèses de la proposition précédente (3.4.2) sont vérifiées.

(3.4.4) *Un critère simple.* — Nous allons appliquer le théorème précédent dans le cas particulier de la $(1, p)$-filtration, dont nous avons précisé la construction en (II, 3.2.6.3). L'algèbre gr G est alors *graduée de type* $\mathbf{N}^*$, le nombre t figurant dans (3.4.3.2) est égal à 1, et nous n'avons à vérifier la surjectivité de P que pour un *seul degré* ν. Traduisons le théorème (3.4.3) en prenant successivement $m = 1$ (ce qui nous oblige à supposer $p > 2$), puis $m = 2$.

(3.4.4.1) *Supposons $p > 2$. Si, dans le pro-p-groupe de type fini* G, *chaque commutateur* (x, y) *est contenu dans le sous-groupe engendré par les p-ièmes puissances, le groupe* G *est analytique.*

Ce critère est évidemment en défaut si $p = 2$ (car il est vérifié par n'importe quel groupe!).

(3.4.4.2) *Si, dans le pro-p-groupe de type fini* G, *chaque commutateur de poids trois* $((x, y), z)$ *est contenu dans le sous-groupe engendré par toutes les puissances p^2-ièmes et par les puissances p-ièmes des commutateurs, alors* G *est analytique.*

Nous obtenons un critère simple, valable pour tout p, en remplaçant les hypothèses de (3.4.4.2) par une condition un peu plus forte.

(3.4.4.3) *Si, dans le pro-p-groupe de type fini* G, *chaque commutateur est contenu dans le sous-groupe engendré par les p^2-ièmes puissances, alors* G *est analytique.*

Le critère (3.4.4.3) n'est pas vérifié par tous les pro-p-groupes analytiques, mais par des sous-groupes arbitrairement petits convenables.

(3.4.4.4) *Un pro-p-groupe analytique* G *admet comme système fondamental de voisinages de l'unité ses sous-groupes qui vérifient le critère* (3.4.4.3).

Preuve. — Nous appliquons la proposition (3.1.3), en remarquant que, dans un groupe p-saturé H, le sous-groupe H_2 des éléments de filtration $\geqslant 2$ vérifie le critère (3.4.4.3).

(3.4.5) *Théorème (Serre).* — *Soient* G *un groupe topologique séparé,* N *un sous-groupe fermé de* G, *et* H *le groupe quotient* G/N. *Supposons que les topologies de* N *et de* H *soient sous-jacentes à des structures analytiques sur* $\mathbf{Q}_p$ (3.1.1). *Alors* G *possède une structure analytique sur* $\mathbf{Q}_p$, *et une seule, compatible avec sa topologie.*

Preuve. — D'après un théorème de Vilenkin [24], G est localement compact, et totalement discontinu (puisque N et H le sont). D'après [23], p. 54 et 56, G admet comme système fondamental de voisinages de l'unité ses sous-groupes *ouverts compacts*, c'est-à-dire *profinis.*

D'après (3.1.3), nous pouvons choisir un sous-groupe ouvert compact G′ de G assez petit pour que $G' \cap N$ et l'image canonique de G′ dans H (isomorphe à $G'/(G' \cap N)$) soient des pro-p-groupes analytiques (3.2.3.3). Cela entraîne que G′ est un pro-p-groupe ([29], chap. Ier, 1.3), d'où l'unicité de la structure analytique sur G′, et par conséquent sur G (3.2.2). Démontrons l'existence de cette structure, *en supposant désormais que* G *est un pro-p-groupe.*

D'après [29], chap. Ier, prop. 1, il existe une *section continue* $s : H \to G$. Pour tous $x, y \in H$, nous avons

$$s(x)s(y) = s(xy)f(x,y), \quad \text{où} \tag{3.4.5.1}$$

$$f : H \times H \to N \tag{3.4.5.2}$$

est une *fonction continue.* Quitte à translater la section, nous pouvons supposer que $s(1) = 1$, d'où

$$f(1, 1) = 1. \tag{3.4.5.3}$$

Choisissons un sous-groupe ouvert N_0 de N qui vérifie le critère (3.4.4.3), c'est-à-dire

$$(N_0, N_0) \subset N_0^{p^2}, \tag{3.4.5.4}$$

où $N_0^{p^2}$ est le sous-groupe engendré par les p^2-ièmes puissances des éléments de N_0.

Il existe un sous-groupe ouvert H_0 de H qui vérifie les trois conditions suivantes :

(3.4.5.5) $$f(x, y) \in N_0^{p^2} \quad \text{pour tous } x, y \in H_0.$$

(3.4.5.6) $$(s(x), z) \in N_0^{p^2} \quad \text{pour tous } x \in H_0, z \in N_0.$$

(3.4.5.7) $$(H_0, H_0) \subset H_0^{p^2}.$$

En effet la continuité de f et (3.4.5.3) montrent que (3.4.5.5) est vérifié pour x, y voisins de l'unité, puisque $N_0^{p^2}$ est ouvert dans N. La continuité de s et la compacité de N_0 montrent que (3.4.5.6) est vérifié pour x voisin de l'unité. Enfin (3.4.4.4) nous permet de vérifier (3.4.5.7), c'est-à-dire le critère (3.4.4.3), pour un sous-groupe ouvert H_0 arbitrairement petit.

L'ensemble G_0 des éléments de la forme $s(x)z$, où $x \in H_0$ et $z \in N_0$ est un *sous-groupe ouvert de* G *qui vérifie le critère d'analyticité* (3.4.4.3).

En effet nous avons la relation

(3.4.5.8) $$s(x)zs(y)t = s(xy)f(x, y)z(z, s(y))t,$$

valable pour tous $x, y \in H$ et z, $t \in N$. Nous en déduisons que G_0 est un sous-groupe de G; il est ouvert puisque G s'identifie topologiquement au produit $H \times N$. La même formule (3.4.5.8) nous montre enfin que le quotient $G_0/N_0^{p^2}$ s'identifie au *produit direct* $H_0 \times (N_0/N_0^{p^2})$, ce qui prouve que G_0 vérifie (3.4.4.3).

CHAPITRE IV

APPLICATIONS DIAGONALES GROUPES ET ALGÈBRES DE LIE

1. ALGÈBRES DIAGONALES

(1.1) Algèbres diagonales strictes.

(1.1.1) *Définition.* — Soit Ω un anneau commutatif. Nous appellerons *Ω-algèbre diagonale stricte* la donnée d'une *Ω-algèbre supplémentée* A et d'un *homomorphisme*

(1.1.1.1) $$\Delta_A : A \to A \otimes_\Omega A.$$

Précisons que $A \otimes_\Omega A$ est munie de sa structure de Ω-algèbre supplémentée (son augmentation est $\varepsilon \otimes \varepsilon$, si ε désigne l'augmentation de A), et l'homomorphisme Δ_A est un *morphisme de Ω-algèbres supplémentées*. Pour simplifier, nous écrirons parfois Δ au lieu de Δ_A.

(1.1.2) *Exemple : algèbre d'un monoïde.* — Soit G un monoïde multiplicatif (avec élément neutre noté 1).

Appelons A l'*algèbre* $\Omega[G]$ de ce monoïde. Définissons l'*augmentation* ε de A en posant $\varepsilon(x) = 1$ pour tout $x \in G$.

L'algèbre $\Omega[G \times G]$ du monoïde $G \times G$ s'identifie au produit tensoriel $\Omega[G] \otimes_\Omega \Omega[G]$, et l'application diagonale $x \mapsto (x, x)$ de G dans $G \times G$ se prolonge en un homomorphisme unique $\Delta_A : A \to A \otimes A$.

Nous avons ainsi défini A comme *Ω-algèbre diagonale stricte*. Notons la relation

(1.1.2.1) $$\Delta_A x = x \otimes x, \qquad \textit{pour tout } x \in G.$$

(1.1.3) *Exemple : algèbre enveloppante d'une algèbre de Lie.* — Soit L une *algèbre de Lie* sur l'anneau commutatif Ω. L'*augmentation* ε de son algèbre enveloppante UL est définie par la condition $\varepsilon \circ \sigma = 0$, σ désignant l'application canonique de L dans UL. L'algèbre enveloppante $U(L \times L)$ s'identifie canoniquement à $UL \otimes_\Omega UL$ ([2], § 2, nº 2, prop. 2). L'application diagonale de L dans $L \times L$ détermine un morphisme de Ω-algèbres supplémentées $UL \to U(L \times L)$, c'est-à-dire le morphisme

(1.1.3.1) $$\Delta_{UL} : UL \to UL \otimes_\Omega UL,$$

qui définit UL comme une *Ω-algèbre diagonale stricte*.

Notons la relation

(1.1.3.2) $$\Delta_{\mathrm{UL}}\sigma(x)=\sigma(x)\otimes 1+1\otimes\sigma(x), \qquad \textit{pour tout } x\in \mathrm{L}.$$

(1.1.4) *Morphismes de Ω-algèbres diagonales strictes.* — Soient A et A′ deux Ω-algèbres diagonales strictes (1.1.1). Nous appelons morphisme $f: \mathrm{A}\to\mathrm{A}'$ un *morphisme* pour les *structures de Ω-algèbres supplémentées qui rend commutatif le diagramme*

(1.1.4.1)
$$\begin{tikzcd} \mathrm{A} \arrow[r, "f"'] \arrow[d, "\Delta_{\mathrm{A}}"'] & \mathrm{A}' \arrow[d, "\Delta_{\mathrm{A}'}"'] \\ \mathrm{A}\otimes\mathrm{A} \arrow[r, "f\otimes f"'] & \mathrm{A}'\otimes\mathrm{A}' \end{tikzcd}$$

Par exemple, Ω[G] devient (1.1.2) un foncteur covariant à valeurs dans la catégorie des Ω-algèbres diagonales strictes, lorsque G parcourt la catégorie des monoïdes. De même la définition (1.1.3) fait de UL un foncteur covariant en L.

(1.1.5) *Définition de $\mathscr{G}$ et de $\mathscr{L}$.* — Soit A une *Ω-algèbre diagonale stricte* (1.1.1), d'augmentation ε.

(1.1.5.1) Nous notons $\mathscr{G}$A l'*ensemble des* $x\in\mathrm{A}$ *qui vérifient*

$$\Delta_{\mathrm{A}}x=x\otimes x \qquad \textit{et} \qquad \varepsilon(x)=1.$$

(1.1.5.2) Nous notons $\mathscr{L}$A l'*ensemble des* $x\in\mathrm{A}$ *qui vérifient*

$$\Delta_{\mathrm{A}}x=x\otimes 1+1\otimes x.$$

(1.1.6) *Propriétés de $\mathscr{G}$.* — Pour chaque Ω-algèbre diagonale stricte, $\mathscr{G}$A est un *sous-monoïde multiplicatif* de A. En effet, si $x, x'\in\mathscr{G}\mathrm{A}$, nous avons $\varepsilon(xx')=\varepsilon(x)\varepsilon(x')=1$ et $\Delta xx'=\Delta x.\Delta x'=(x\otimes x)(x'\otimes x')=xx'\otimes xx'$.

Si $f: \mathrm{A}\to\mathrm{A}'$ est un *morphisme* de Ω-algèbres diagonales strictes (1.1.4), alors $f(\mathscr{G}\mathrm{A})\subset\mathscr{G}\mathrm{A}'$, ce qui montre que $\mathscr{G}$ est un *foncteur covariant* en A (à valeurs dans la catégorie des monoïdes).

Enfin l'injection de $\mathscr{G}$A dans A se prolonge en une application Ω-linéaire

(1.1.6.1) $$\Omega[\mathscr{G}\mathrm{A}]\to\mathrm{A},$$

qui, d'après (1.1.2) et (1.1.4) est un *morphisme fonctoriel* de Ω-algèbres diagonales strictes.

(1.1.7) *Propriétés de $\mathscr{L}$.* — Une Ω-algèbre diagonale stricte est, en particulier, une *algèbre de Lie* pour le crochet $[a, b]=ab-ba$. L'ensemble $\mathscr{L}$A est une *sous-algèbre de Lie* de A. De plus, si Ω est un anneau de caractéristique p, A est une algèbre de Lie *restreinte* (au sens de Jacobson [13]) pour la p-application $x\mapsto x^p$, et $\mathscr{L}$A est une *sous-algèbre de Lie restreinte*. En effet, si x, x' appartiennent à $\mathscr{L}$A, c'est-à-dire vérifient (1.1.5.2), nous avons

(1.1.7.1) $$\Delta_{\mathrm{A}}xx'=xx'\otimes 1+1\otimes xx'+x\otimes x'+x'\otimes x,$$

d'où $[x, x'] \in \mathscr{L}A$. La linéarité en x de la relation (1.1.5.2) montre que $\mathscr{L}A$ est un sous-Ω-module de A.

Enfin nous avons

$$\Delta_A x^p = x^p \otimes 1 + 1 \otimes x^p + \sum_{0<i<p} \binom{p}{i} x^i \otimes x^{p-i}, \tag{1.1.7.2}$$

ce qui prouve que $x^p \in \mathscr{L}A$ si Ω est de caractéristique p.

Tout morphisme $f : A \to A'$ de Ω-algèbres diagonales strictes (1.1.4) applique $\mathscr{L}A$ dans $\mathscr{L}A'$. Ainsi $\mathscr{L}A$ est un *foncteur covariant* en A.

Les éléments de $\mathscr{L}A$ appartiennent à l'idéal d'augmentation (car la relation (1.1.5.2) implique $\varepsilon(x) = 2\varepsilon(x)$) et l'injection de $\mathscr{L}A$ dans A se prolonge en un *morphisme fonctoriel de Ω-algèbres diagonales strictes*

$$U\mathscr{L}A \to A. \tag{1.1.7.3}$$

Si Ω est de caractéristique p, nous avons de même un *morphisme fonctoriel* d'algèbres diagonales strictes

$$\widetilde{U}\mathscr{L}A \to A, \tag{1.1.7.4}$$

où $\widetilde{U}L$ désigne l'*algèbre enveloppante restreinte* de L ([13], th. 12, p. 191).

(1.1.8) *Lemme. — Soient* K *un corps commutatif,* M *un* K-*espace vectoriel et* $\Delta : M \to M \otimes_K M$ *une application* K-*linéaire. Alors les éléments* $x \in M$ *qui vérifient* $x \neq 0$ *et* $\Delta x = x \otimes x$ *sont linéairement indépendants sur* K.

Preuve. — Si ces éléments n'étaient pas indépendants, ils seraient liés par une relation primordiale de dépendance linéaire, que nous pourrions écrire sous la forme

$$x_0 = \sum_{1 \leqslant i \leqslant n} \lambda_i x_i. \tag{1.1.8.1}$$

Les $x_i \in M$ vérifieraient $\Delta x_i = x_i \otimes x_i$ pour $0 \leqslant i \leqslant n$; ils seraient *linéairement indépendants sur* K et se trouveraient *multipliés par des scalaires* $\lambda_i \in K$ *tous non nuls pour* $1 \leqslant i \leqslant n$. La relation (1.1.8.1) nous donne

$$\Delta x_0 = \sum_{1 \leqslant i \leqslant n} \lambda_i x_i \otimes x_i; \tag{1.1.8.2}$$

$$x_0 \otimes x_0 = \sum_{1 \leqslant i, j \leqslant n} \lambda_i \lambda_j x_i \otimes x_j. \tag{1.1.8.3}$$

Comme les éléments $x_i \otimes x_j$ sont linéairement indépendants dans $M \otimes M$, la comparaison de (1.1.8.2) à (1.1.8.3) nous donne $n = 1$ et $\lambda_1^2 = \lambda_1$, ce qui prouve le lemme.

(1.1.9) *Lemme. — Soient* A *une algèbre diagonale stricte sur le corps commutatif* K *de caractéristique* 0, *et* $(x_i)_{i \in I}$ *une famille d'éléments de* $\mathscr{L}A$ *linéairement indépendants sur* K. *Supposons l'ensemble d'indices* I *totalement ordonné. Alors les monômes ordonnés* x^α *sont linéairement indépendants sur* K, α *parcourant l'ensemble* $\mathbf{N}^{(I)}$.

Preuve. — Notons (m, n) le coefficient binomial $(m+n)!/m!\,n!$ $(m, n \in \mathbf{N})$ et posons

(1.1.9.1) $$(\beta, \gamma) = \prod_{i \in \mathrm{I}} (\beta_i, \gamma_i) \quad \text{pour } \beta, \gamma \in \mathbf{N}^{(\mathrm{I})}.$$

Les relations

(1.1.9.2) $$\Delta x_i = x_i \otimes 1 + 1 \otimes x_i$$

conduisent, pour chaque $\alpha \in \mathbf{N}^{(\mathrm{I})}$, à

(1.1.9.3) $$\Delta x^\alpha = \sum_{\beta+\gamma=\alpha} (\beta, \gamma) x^\beta \otimes x^\gamma$$

Démontrons, par récurrence sur n, l'indépendance linéaire des x^α pour lesquels $|\alpha| \leqslant n$. Cela est vrai, par hypothèse, pour $n=1$. Supposons une relation de dépendance linéaire

(1.1.9.4) $$y = \sum_{\alpha \in \mathbf{N}^{(\mathrm{I})}} \lambda_\alpha x^\alpha = 0.$$

En calculant l'augmentation $\varepsilon(y)$ nous trouvons $\lambda_0 = 0$. Puis nous écrivons la relation

(1.1.9.5) $$\Delta y - y \otimes 1 - 1 \otimes y = 0,$$

c'est-à-dire, d'après (1.1.9.3) et (1.1.9.4),

(1.1.9.6) $$\sum_{\beta, \gamma > 0} (\beta, \gamma) \lambda_{\beta+\gamma} x^\beta \otimes x^\gamma = 0.$$

Si n est le maximum des $|\alpha|$ correspondant aux λ_α non nuls, la relation (1.1.9.6) ne fait intervenir que des x^β et x^γ pour lesquels $|\beta|, |\gamma| < n$ (si $n > 0$) et notre hypothèse de récurrence entraîne que ces éléments $x^\beta \otimes x^\gamma$ sont linéairement indépendants dans $\mathrm{A} \otimes_{\mathrm{K}} \mathrm{A}$. Nous concluons que $\lambda_\alpha = 0$ pour $|\alpha| \neq 1$, puis pour $|\alpha| = 1$.

(1.1.9.7) *Remarque.* — Nous avons utilisé essentiellement le fait que K est de caractéristique zéro, quand nous avons déduit la relation $\lambda_{\beta+\gamma} = 0$ de $(\beta, \gamma)\lambda_{\beta+\gamma} = 0$. Si K était de caractéristique p, notre lemme resterait valable après la modification suivante : *le multidegré α ne devrait pas parcourir $\mathbf{N}^{(\mathrm{I})}$ tout entier, mais seulement la partie définie par les relations $\alpha_i < p$ pour tout $i \in \mathrm{I}$.*

(1.1.10) *Lemme. — Extension des scalaires dans une algèbre diagonale stricte.* Soient A une Ω-algèbre diagonale stricte (1.1.1) et Ω' un anneau commutatif, extension de Ω. *Notons* A′ *la Ω'-algèbre supplémentée* $\Omega' \otimes_\Omega \mathrm{A}$ (dont l'augmentation ε' est $1 \otimes \varepsilon$). Alors le produit tensoriel $\mathrm{A}' \otimes_{\Omega'} \mathrm{A}'$ s'identifie canoniquement à $\Omega' \otimes_\Omega (\mathrm{A} \otimes_\Omega \mathrm{A})$, ce qui permet de définir la *structure de Ω'-algèbre diagonale stricte de* A′, en posant $\Delta_{\mathrm{A}'} = 1 \otimes \Delta_{\mathrm{A}}$, compte tenu de l'identification rappelée.

Preuve. — Ces assertions sont banales. Plus généralement, si M et N sont deux Ω-modules, alors $(\Omega' \otimes_\Omega \mathrm{M}) \otimes_{\Omega'} (\Omega' \otimes_\Omega \mathrm{N})$ s'identifie à $\Omega' \otimes_\Omega (\mathrm{M} \otimes \mathrm{N})$, l'élément $(\lambda \otimes m) \otimes (\mu \otimes n)$ du premier module correspondant à l'élément $(\lambda\mu) \otimes (m \otimes n)$ du second.

(1.1.11) *Théorème. — Soient* Ω *un anneau intègre,* K *son corps des fractions, et* A *une* Ω*-algèbre diagonale stricte* (1.1.1).

(1.1.11.1) *Si nous supposons* A *et* $A \otimes_\Omega A$ *sans torsion, alors le morphisme* (1.1.6.1)

$$\Omega[\mathscr{G}A] \to A$$

est injectif.

(1.1.11.2) *Si, de plus, nous supposons* K *de caractéristique zéro et* $U\mathscr{L}A$ *sans torsion, alors le morphisme* (1.1.7.3)

$$U\mathscr{L}A \to A$$

est injectif.

Preuve. — Si Ω était un corps, les assertions (1.1.11.1) et (1.1.11.2) résulteraient respectivement des lemmes (1.1.8) et (1.1.9). Les hypothèses faites ont pour but de ramener les propriétés de A à celles de la K-algèbre diagonale stricte $K \otimes_\Omega A = A'$, définie en (1.1.10). Pour établir (1.1.11.2), il faut vérifier que la K-algèbre de Lie $\mathscr{L}A'$ s'identifie à $K \otimes_\Omega \mathscr{L}A$, puis que $U\mathscr{L}A'$ (algèbre enveloppante en tant que K-algèbre) s'identifie à $K \otimes_\Omega U\mathscr{L}A$. Ce dernier point est traité en [2], § 2, n° 9.

(1.1.11.3) *Remarque.* — Si le corps K était de caractéristique p, nous pourrions modifier (1.1.11.2). Nous supposerions que $\widetilde{U}\mathscr{L}A$ est sans torsion, et nous en déduirions que le morphisme (1.1.7.4)

$$\widetilde{U}\mathscr{L}A \to A$$

est injectif.

(1.2) Algèbres diagonales valuées.

(1.2.1) *Insuffisance de la notion d'algèbre diagonale stricte.* — Reprenons l'exemple (1.1.3) dans le cas où L est un Ω-module libre de rang 1. Alors UL et $UL \otimes UL$ s'identifient à des anneaux de polynômes $\Omega[T]$ et $\Omega[T, T']$, et l'application diagonale Δ est déterminée par la relation

(1.2.1.1) $$\Delta T = T + T'.$$

Il n'existe pas de prolongement « naturel » de Δ à l'algèbre de séries formelles $\Omega[[T]]$ qui fasse de cette dernière une algèbre diagonale stricte. En effet, la formule (1.2.1.1) définit encore un homomorphisme de $\Omega[[T]]$ dans $\Omega[[T, T']]$, mais nous disposons seulement d'un homomorphisme canonique

(1.2.1.2) $$\Omega[[T]] \otimes \Omega[[T]] \to \Omega[[T, T']]$$

qui n'est pas surjectif (ni même toujours injectif).

(1.2.2) *Une notion générale d'algèbre diagonale.* — Si nous voulons définir $\Omega[[T]]$ comme une algèbre diagonale par la formule (1.2.1.1), il nous suffit de remplacer, dans la définition (1.1.1), le produit tensoriel ordinaire par un « produit tensoriel complété » (« complété » signifiant parfois « séparé-complété »).

Nous parviendrions ainsi à la notion générale de Ω-algèbre diagonale. Ce serait la donnée de *deux Ω-algèbres supplémentées* A et B, et de *deux morphismes* $\Delta_A : A \to B$ et $f_A : A \otimes_A A \to B$. Nous n'étudierons qu'un cas très particulier de cette notion.

(1.2.3) *Définition des algèbres diagonales valuées.* — Faisons d'abord une première convention : quand nous parlerons d'une *algèbre diagonale valuée* sur un anneau Ω, nous sous-entendrons que Ω est un *anneau de valuation discrète complet, d'inégales caractéristiques avec* $v(p) = 1$ (I, 3.1.1). L'anneau Ω contient toujours $\mathbf{Z}_p$.

Une *Ω-algèbre diagonale valuée* est constituée par la donnée d'une *Ω-algèbre supplémentée valuée* (I, 2.2.4) *et d'un morphisme de Ω-algèbres supplémentées valuées*

(1.2.3.1) $$\Delta_A : A \to \mathrm{Sat}(A \otimes_\Omega A).$$

Rappelons (I, 3.2.8) que $\mathrm{Sat}(A \otimes A)$ est l'algèbre *saturée* de l'*algèbre valuée* $A \otimes A$.

(1.2.4) *Morphismes d'algèbres diagonales valuées.* — Soient A et A′ deux Ω-algèbres diagonales valuées (1.2.3). Un *morphisme* $f : A \to A'$ est un morphisme pour les structures de *Ω-algèbres supplémentées valuées qui rend commutatif le diagramme*

(1.2.4.1) $$\begin{tikzcd} A \arrow[r, "f"'] \arrow[d, "\Delta_A"'] & A' \arrow[d, "\Delta_{A'}"'] \\ \mathrm{Sat}(A \otimes A) \arrow[r, "\mathrm{Sat}(f \otimes f)"'] & \mathrm{Sat}(A' \otimes A') \end{tikzcd}$$

(1.2.5) *Algèbre diagonale valuée définie par une algèbre diagonale stricte.* — Soit A une Ω-algèbre supplémentée valuée, et $\Delta_A : A \to A \otimes A$ un homomorphisme qui définit une structure d'*algèbre diagonale stricte* (1.1.1). Comme $\mathrm{Sat}(A \otimes A)$ est une extension de $A \otimes A$, nous pouvons considérer Δ_A comme un morphisme de Ω-algèbres supplémentées, à valeurs dans $\mathrm{Sat}(A \otimes A)$. Pour que A devienne ainsi une *Ω-algèbre diagonale valuée*, il faut et il suffit que Δ_A soit un *morphisme de Ω-modules filtrés* (I, 2.1.4).

(1.2.6) *Proposition.* — *Soit* A *une Ω-algèbre diagonale valuée* (1.2.3). *Alors chacune des algèbres* $\hat{A}$ (I, 2.1.14), div A (I, 2.2.9) *et* Sat A (I, 2.2.11) *possède une structure de Ω-algèbre diagonale valuée, déterminée univoquement par la condition que l'injection canonique de* A *dans* $\hat{A}$ (*resp.* div A, Sat A) *est un morphisme* (1.2.4).

Cela signifie que l'application diagonale Δ_A se prolonge naturellement à chacune des algèbres considérées.

Preuve. — Si B désigne l'une des algèbres $\hat{A}$, div A et Sat A, nous avons vu en (I, 3.2.8) que $\mathrm{Sat}(B \otimes B)$ s'identifie à $\mathrm{Sat}(A \otimes A)$. Le prolongement unique de Δ_A à B résulte alors des propriétés du foncteur Sat (I, 2.2.11).

(1.2.7) *Les $\mathbf{Z}_p$-algèbres diagonales associées à un groupe p-valué.* — Soient G un groupe p-valué (III, 2.1.2) et $A = \mathbf{Z}_p[G]$. Munissons A de la valuation induite par celle de G (III, 2.3.3). Alors la structure de $\mathbf{Z}_p$-algèbre diagonale stricte de A (1.1.2) est aussi une structure de $\mathbf{Z}_p$-*algèbre diagonale valuée* (1.2.5). Si nous appliquons (1.2.6), nous obtenons les $\mathbf{Z}_p$-*algèbres diagonales valuées* $\hat{\mathrm{A}}$, div A et Sat A.

Si G est un *groupe p-saturé de rang fini*, nous avons vu (III, 3.3.5) que $\mathrm{Ala}(\mathrm{G}\times\mathrm{G})$ s'identifie au produit tensoriel complété $\mathrm{Ala}\ \mathrm{G}\hat{\otimes}\mathrm{Ala}\ \mathrm{G}$, qui est lui-même une sous-algèbre de $\mathrm{Sat}(\mathrm{Ala}\ \mathrm{G}\otimes\mathrm{Ala}\ \mathrm{G})$. Nous avons donc une structure de $\mathbf{Z}_p$-*algèbre diagonale valuée sur* Ala G.

(1.2.8) *Algèbres diagonales valuées construites à partir d'une algèbre associative libre.* — Soit A une Ω-algèbre associative, libre pour la famille de générateurs $(\mathrm{X}_i)_{i\in\mathrm{I}}$. Nous considérons A comme une algèbre supplémentée, en posant $\varepsilon(\mathrm{X}_i)=0$ pour tout $i\in\mathrm{I}$. Nous pouvons définir une structure d'algèbre diagonale stricte (1.1.1) sur A en nous donnant les éléments $\Delta\mathrm{X}_i$ dans $\mathrm{A}\otimes_\Omega\mathrm{A}$ (ces éléments doivent seulement être d'augmentation nulle). En particulier nous pouvons prendre

(1.2.8.1) $$\Delta\mathrm{X}_i=\mathrm{X}_i\otimes 1+1\otimes\mathrm{X}_i,$$

et nous retrouvons l'exemple (1.1.3), car A s'identifie à l'*algèbre enveloppante de l'algèbre de Lie libre engendrée par les* X_i. Si nous nous donnons une famille de nombres $\geqslant 0$, $(\tau_i)_{i\in\mathrm{I}}$, nous pouvons munir A de la borne inférieure des filtrations pour lesquelles $w(\mathrm{X}_i)\geqslant\tau_i$. Cette filtration est une valuation facile à expliciter, et nous obtenons A comme *algèbre diagonale valuée* (1.2.5). L'algèbre complétée $\hat{\mathrm{A}}$ est l'algèbre de Magnus étudiée en (II, 3.1.3). Nous utiliserons plus loin (3.2.1) la structure d'algèbre diagonale valuée de Sat A (1.2.6).

(1.2.9) *Structures d'algèbre diagonale valuée sur* $\mathbf{Z}_p[\mathrm{T}]$: *exercice.* — Prenons sur $\mathrm{A}=\mathbf{Z}_p[\mathrm{T}]$ la structure d'algèbre diagonale stricte définie par $\Delta\mathrm{T}=\mathrm{T}\otimes 1+1\otimes\mathrm{T}$. Les *valuations* de A pour lesquelles les monômes $(\mathrm{T}^n)_{n\in\mathbf{N}}$ constituent une *base filtrée* (I, 2.1.16) et A une *algèbre diagonale valuée* s'obtiennent comme suit. Si $(t_i)_{i\in\mathbf{N}}$ désigne une suite de nombres positifs vérifiant

(1.2.9.1) $$pt_i\leqslant t_{i+1}\leqslant pt_i+1 \quad (i\in\mathbf{N}),$$

et si $n=\sum_i a_ip^i$ est le développement de l'entier n dans le système de base p (III, 1.1.1), nous posons

(1.2.9.2) $$w(\mathrm{T}^n)=\sum_i a_it_i.$$

Pour $t_i=p^it_0$ nous retrouvons un cas particulier de (1.2.8).

(1.2.10) *Extension des scalaires dans une algèbre diagonale valuée : exercice.* — Soient A une Ω-algèbre diagonale valuée (1.2.3) et Ω' un second anneau de valuation discrète complet, contenant Ω. Alors l'algèbre $\Omega'\otimes_\Omega\mathrm{A}$, valuée comme en (I, 3.2.1), possède une structure naturelle de Ω'-algèbre diagonale valuée.

(1.3) Propriété fondamentale des algèbres diagonales saturées.

(1.3.1) *Définition de $\mathscr{L}$, $\mathscr{L}^*$, $\mathscr{G}$ et $\mathscr{G}^*$ dans les algèbres diagonales valuées.* — Soit A une Ω-algèbre diagonale valuée (1.2.3). Rappelons que le produit tensoriel saturé $\mathrm{Sat}(A\otimes A)$ est une *extension* du produit tensoriel $A\otimes A$. Nous pouvons donc définir $\mathscr{G}A$ et $\mathscr{L}A$ comme nous l'avons fait en (1.1.5) pour les algèbres diagonales strictes, c'est-à-dire par les relations

(1.3.1.1) $$x\in\mathscr{G}A \Leftrightarrow x\in A,\ \varepsilon(x)=1 \text{ et } \Delta_A x = x\otimes x.$$

(1.3.1.2) $$x\in\mathscr{L}A \Leftrightarrow x\in A \text{ et } \Delta_A x = x\otimes 1 + 1\otimes x.$$

Dans (1.3.1.1), la condition $\varepsilon(x)=1$ pourrait être remplacée par $\varepsilon(x)\neq 0$, car la dernière condition entraîne que $\varepsilon(x)$ est un idempotent de Ω.

Définissons maintenant $\mathscr{G}^*A$ et $\mathscr{L}^*A$, qui sont respectivement des parties de $\mathscr{G}A$ et $\mathscr{L}A$.

(1.3.1.3) $$x\in\mathscr{G}^*A \Leftrightarrow x\in\mathscr{G}A \text{ et } w(x-1)>(p-1)^{-1}.$$

(1.3.1.4) $$x\in\mathscr{L}^*A \Leftrightarrow x\in\mathscr{L}A \text{ et } w(x)>(p-1)^{-1}.$$

(1.3.2) *Propriétés de $\mathscr{L}$, $\mathscr{L}^*$, $\mathscr{G}$ et $\mathscr{G}^*$.* — Étendons aux algèbres diagonales valuées les résultats élémentaires de (1.1.6) et (1.1.7).

(1.3.2.1) La partie $\mathscr{G}A$ (resp. $\mathscr{G}^*A$) de A est un *sous-monoïde multiplicatif* de A. Si A est *complet*, alors $\mathscr{G}^*A$ est un *groupe*. Le *sous-Ω-module* de A engendré par $\mathscr{G}A$ (resp. $\mathscr{G}^*A$) est une *sous-algèbre supplémentée*. Cette sous-algèbre possède une structure d'*algèbre diagonale stricte*, définie par la *restriction* de Δ_A.

(1.3.2.2) La partie $\mathscr{L}A$ (resp. $\mathscr{L}^*A$) de A est une *sous-Ω-algèbre de Lie*. Si A est *divisible* (en particulier si A est saturée) $\mathscr{L}A$ s'*identifie* à $\operatorname{div}\mathscr{L}^*A$. La *sous-algèbre associative* de A engendrée par $\mathscr{L}A$ (resp. $\mathscr{L}^*A$) possède une structure d'*algèbre diagonale stricte* définie par la *restriction* de Δ_A.

(1.3.2.3) Soit $f: A\to A'$ un morphisme de Ω-algèbres diagonales valuées (1.2.4). Alors f applique $\mathscr{G}A$, $\mathscr{G}^*A$, $\mathscr{L}A$, $\mathscr{L}^*A$ respectivement dans $\mathscr{G}A'$, $\mathscr{G}^*A'$, $\mathscr{L}A'$, $\mathscr{L}^*A'$, ce qui nous permet de parler des *foncteurs covariants* $\mathscr{G}$, $\mathscr{G}^*$, $\mathscr{L}$ et $\mathscr{L}^*$.

Preuve. — Contentons-nous de préciser l'application diagonale Δ_M de l'une des algèbres diagonales strictes définies en (1.3.2.1) ou (1.3.2.2). Si M est un sous-module de A, nous savons (I, 3.2.1.4) que $M\otimes M$ s'identifie à un sous-module de $A\otimes A$, donc de $\mathrm{Sat}(A\otimes A)$. La restriction Δ_M de Δ_A est ainsi définie lorsque $\Delta_A(M)\subset M\otimes M$.

(1.3.3) *Application du théorème* (1.1.11). — Soit A une algèbre diagonale valuée. Alors les *morphismes fonctoriels*

(1.3.3.1) $$\Omega[\mathscr{G}^*A]\to\Omega[\mathscr{G}A]\to A, \quad \text{et}$$

(1.3.3.2) $$U\mathscr{L}^*A\to U\mathscr{L}A\to A,$$

sont *injectifs*.

Preuve. — Nous vérifions les hypothèses de (1.1.11). Il faut savoir que $U\mathscr{L}A$ est sans torsion, et que $U\mathscr{L}^*A \to U\mathscr{L}A$ est injectif. Nous démontrons plus loin des résultats plus forts : (2.2.5) et (2.2.6).

(1.3.4) *Définition.* — Une Ω-*algèbre diagonale saturée* est une Ω-*algèbre diagonale valuée* au sens de (1.2.3), qui est *saturée* au sens de (I, 2.2.10).

(1.3.5) *Théorème. — Soit* A *une* Ω-*algèbre diagonale saturée.*

(1.3.5.1) *La fonction exponentielle* (III, 1.1.4) *applique* $\mathscr{L}^*A$ *sur* $\mathscr{G}^*A$. *La fonction logarithme* (III, 1.1.5) *applique* $\mathscr{G}^*A$ *sur* $\mathscr{L}^*A$. *Ces fonctions, réciproques l'une de l'autre, mettent* $\mathscr{L}^*A$ *et* $\mathscr{G}^*A$ *en correspondance biunivoque et bicontinue.*

(1.3.5.2) *L'algèbre de Lie* $\mathscr{L}A$ *est saturée. L'algèbre de Lie* $\mathscr{L}^*A$ *s'identifie aux éléments de valuation* $>(p-1)^{-1}$ *de son algèbre saturée (ou divisée)* $\mathscr{L}A$.

(1.3.5.3) *Le monoïde* $\mathscr{G}^*A$ *est un groupe* p-*saturé* (III, 2.1.6) *pour la filtration* ω *induite par la filtration* w *de* A *(c'est-à-dire définie en posant* $\omega(x)=w(x-1)$, *comme en* (II, 1.1.9)).

(1.3.5.4) *Les gradués associés* gr $\mathscr{L}^*A$ *et* gr $\mathscr{G}^*A$ *sont canoniquement isomorphes.*

(1.3.5.5) *Les parties* $\mathscr{L}^*A$ *et* $\mathscr{G}^*A$ *engendrent dans* A *la même sous-algèbre associative saturée. Celle-ci possède une structure d'algèbre diagonale saturée, définie par la restriction de* Δ_A.

Preuve. — Il s'agit d'une simple vérification qui fait intervenir les définitions des fonctions exp et Log et leurs propriétés (III, 1.1) ainsi que la définition des algèbres diagonales saturées, et de $\mathscr{L}$, $\mathscr{L}^*$, $\mathscr{G}^*$. Précisons cependant la propriété (1.3.5.4). Nous munissons $\mathscr{L}^*A$ de sa valuation de sous-module; alors gr $\mathscr{L}^*A$ s'identifie à une *sous*-gr Ω-*algèbre de Lie de* gr A; par *restriction des scalaires,* nous considérons gr $\mathscr{L}^*A$ comme une Γ-algèbre de Lie, où $\Gamma = \mathrm{gr}\,\mathbf{Z}_p$. Le groupe $\mathscr{G}^*A$ est muni de sa p-valuation définie en (1.3.5.3). D'après (II, 1.1.9) et (II, 1.2.1), la Γ-algèbre de Lie gr $\mathscr{G}^*A$ s'identifie à une sous-Γ-algèbre de Lie de gr A. Si x est un élément de $\mathscr{G}^*A$ $(x\neq 1)$ alors le *terme dominant* de x dans gr $\mathscr{G}^*A$ est identifié au même élément de gr A que le *terme dominant* de $y=\mathrm{Log}\,x$ dans gr $\mathscr{L}^*A$.

(1.3.6) *Remarques.* — Le théorème (1.3.5) ne nous apprend rien sur le monoïde $\mathscr{G}A$. Nous aurions pu sans inconvénient supposer que A coïncide avec sa sous-algèbre définie en (1.3.5.5); nous définirons plus loin (3.1.5) les *algèbres diagonales saturées normales* qui vérifient une condition plus stricte.

Nous aurions pu introduire des algèbres diagonales valuées sur un anneau de valuation discrète complet, *de caractéristique zéro ainsi que son corps résiduel.* Nous avons cru préférable de ne pas allonger l'exposé.

La correspondance biunivoque établie en (1.3.5) entre $\mathscr{L}^*A$ et $\mathscr{G}^*A$ nous permettra de transporter à l'algèbre $\mathscr{L}^*A$ la structure de groupe de $\mathscr{G}^*A$, et de transporter au groupe $\mathscr{G}^*A$ la structure d'algèbre de $\mathscr{L}^*A$. C'est ce que nous ferons en (3.2). Cependant, si $\Omega\neq\mathbf{Z}_p$, nous renoncerons à transporter au groupe $\mathscr{G}^*A$ la multiplication de $\mathscr{L}^*A$ par les éléments de Ω (c'est-à-dire à définir les éléments x^λ pour $x\in\mathscr{G}^*A$, $\lambda\in\Omega$). Si Ω est une extension algébrique finie de $\mathbf{Z}_p$, et si la dimension de $\mathscr{L}^*A$ est finie, le groupe $\mathscr{G}^*A$ possède une structure analytique sur le corps des fractions K de Ω; nous ne l'étudierons pas.

Avant d'aborder les transports de structure, nous allons démontrer un théorème de Poincaré-Birkhoff-Witt pour les algèbres de Lie valuées sur un anneau de valuation discrète complet (quelconque) Ω. Cela nous permettra de construire le *foncteur* Sat U.

2. LE THÉORÈME DE POINCARÉ-BIRKHOFF-WITT

(2.1) Généralités : le cas gradué.

(2.1.1) *Algèbre enveloppante : définitions et notations.* — Soit L une algèbre de Lie sur l'anneau commutatif Ω. Dans l'*algèbre tensorielle* TL du Ω-module L (I, 3.3.1), considérons l'*idéal bilatère* J engendré par les éléments

(2.1.1.1) $$x.y-y.x-[x,y],$$

où $x, y \in \mathrm{L}$. L'*algèbre quotient* $\mathrm{UL}=\mathrm{TL}/\mathrm{JL}$ est l'*algèbre enveloppante* de l'algèbre de Lie L (cf. [2], § 2, n° 1). Nous avons ainsi la suite exacte

(2.1.1.2) $$0 \to \mathrm{JL} \to \mathrm{TL} \to \mathrm{UL} \to 0.$$

(2.1.2) *Définition de* T_n, J_n *et* U_n. — Pour chaque $n \in \mathbf{N}$, nous notons $\mathrm{T}_n\mathrm{L}$ la somme directe des puissances tensorielles $\mathrm{T}^i\mathrm{L}$ pour $0 \leqslant i \leqslant n$:

(2.1.2.1) $$\mathrm{T}_n\mathrm{L} = \coprod_{0 \leqslant i \leqslant n} \mathrm{T}^i\mathrm{L}.$$

Les sous-modules $\mathrm{T}_n\mathrm{L}$ de TL croissent avec n, et leur réunion est TL. Nous avons, pour chaque $n \in \mathbf{N}^*$, la suite exacte scindée

(2.1.2.2) $$0 \to \mathrm{T}_{n-1}\mathrm{L} \to \mathrm{T}_n\mathrm{L} \to \mathrm{T}^n\mathrm{L} \to 0.$$

Pour chaque $n \in \mathbf{N}$, *nous notons* $\mathrm{J}_n\mathrm{L}$ *le sous-Ω-module de* $\mathrm{T}_n\mathrm{L}$ *engendré par les éléments*

(2.1.2.3) $$a(x.y-y.x-[x,y])b,$$

où $$x, y \in \mathrm{L}, \quad a \in \mathrm{T}^i, \quad b \in \mathrm{T}^j, \quad et \quad i+j+2 \leqslant n.$$

Nous avons en particulier $\mathrm{J}_0\mathrm{L}=\mathrm{J}_1\mathrm{L}=0$; les modules $\mathrm{J}_n\mathrm{L}$ croissent avec n, et leur réunion est JL :

(2.1.2.4) $$\bigcup_{n \in \mathbf{N}} \mathrm{J}_n\mathrm{L} = \mathrm{JL}.$$

Si nous composons l'injection canonique de $\mathrm{J}_n\mathrm{L}$ dans $\mathrm{T}_n\mathrm{L}$ avec la projection (2.1.2.2) de $\mathrm{T}_n\mathrm{L}$ sur $\mathrm{T}^n\mathrm{L}$, nous obtenons une application $f : \mathrm{J}_n\mathrm{L} \to \mathrm{T}^n\mathrm{L}$. L'image par f d'un générateur de $\mathrm{J}_n\mathrm{L}$ écrit sous la forme (2.1.2.3) est nulle si $i+j+2<n$, ou égale à

(2.1.2.5) $$a(x.y-y.x)b$$

si $i+j+2=n$. Cela signifie que $f(\mathrm{J}_n\mathrm{L})$ est le module $\mathrm{I}^n\mathrm{L}$ défini en (I, 3.3.1), ou encore

(2.1.2.6) $$\mathrm{J}_n\mathrm{L}+\mathrm{T}_{n-1}\mathrm{L} = \mathrm{I}^n\mathrm{L}+\mathrm{T}_{n-1}\mathrm{L}.$$

Définissons enfin le module U_nL comme le quotient de T_nL par J_nL. Nous avons ainsi, pour chaque $n \in \mathbf{N}$, la suite exacte

$$0 \to J_nL \to T_nL \to U_nL \to 0. \tag{2.1.2.7}$$

Cette définition de U_nL ne coïncide pas toujours avec celle de [2], § 2, nº 6.

(**2.1.3**) *Les diagrammes* D_nL *et le théorème de Poincaré-Birkhoff-Witt.* — Pour chaque entier $n \in \mathbf{N}^*$, nous noterons D_nL le diagramme commutatif suivant, où les flèches représentent des applications Ω-linéaires.

$$(D_nL) \qquad \begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J_{n-1}L & \longrightarrow & T_{n-1}L & \longrightarrow & U_{n-1}L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J_nL & \longrightarrow & T_nL & \longrightarrow & U_nL & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^nL & \longrightarrow & T^nL & \longrightarrow & S^nL & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Les deux premières lignes sont des suites exactes (2.1.2.7), et les morphismes du carré supérieur gauche sont des inclusions.

La ligne inférieure est une suite exacte (I, 3.3.1.4). Nous avons remarqué l'existence du morphisme $J_nL \to I^nL$, qui entraîne celle du morphisme $U_nL \to S^nL$.

La deuxième colonne est une suite exacte scindée.

Nous avons donc un diagramme D_nL avec *trois* lignes et *une* colonne exactes. De plus, nous savons que l'application $J_nL \to I^nL$ est *surjective*, ce qui équivaut à la relation

$$\mathrm{Ker}(U_nL \to S^nL) = \mathrm{Im}(U_{n-1}L \to U_nL). \tag{2.1.3.1}$$

Les applications $U_{n-1}L \to U_nL$ nous permettent de construire la limite inductive des U_nL. D'après (2.1.2.4), cette dernière s'identifie à UL :

$$\varinjlim U_nL = UL. \tag{2.1.3.2}$$

La *conclusion* du théorème de Poincaré-Birkhoff-Witt est que *tous les diagrammes* D_nL *sont exacts* (c'est-à-dire ont toutes leurs lignes et leurs colonnes exactes, pour chaque $n \in \mathbf{N}^*$).

Quant à l'*hypothèse* de ce théorème, elle peut être que le Ω-module sous-jacent à L est libre [2], ou, plus généralement, est une limite inductive de sommes directes de Ω-modules monogènes [15]. Cette dernière hypothèse est vérifiée lorsque Ω est un *anneau principal*.

Pour chaque $n \in \mathbf{N}^*$, l'exactitude du diagramme $D_n L$ équivaut à l'une des deux relations suivantes

(2.1.3.3) $$\mathrm{Ker}(U_{n-1}L \to U_n L) = 0;$$

(2.1.3.4) $$J_n L \cap T_{n-1}L = J_{n-1}L.$$

Si le théorème est vérifié, les relations (2.1.3.3) nous permettent d'identifier chaque module $U_n L$ à l'image canonique de $T_n L$ dans UL : nous retrouvons alors les notations de [2].

(2.1.4) *Le cas gradué.* — Supposons que Ω soit un anneau gradué (I, 1.1.1) et L une Ω-algèbre de Lie graduée (I, 1.1.9). Nous avons vu (I, 3.3.2) que TL et SL possèdent des graduations naturelles. La forme (2.1.2.3) des générateurs du module $J_n L$ montre que celui-ci est gradué, ainsi que l'idéal JL. Nous pouvons donc prendre la *graduation quotient* sur chaque module $U_n L$, ainsi que sur l'algèbre UL. Le diagramme $D_n L$ devient alors un *diagramme dans la catégorie des Ω-modules gradués* (I, 1.1.4), et la relation (2.1.3.2) reste valable dans cette catégorie.

(2.2) Le cas filtré; algèbres de Lie valuées sur un anneau de valuation discrète complet.

(2.2.1) *Les filtrations canoniques.* — Supposons désormais que Ω soit un anneau filtré (I, 2.1.1) et L une Ω-algèbre de Lie filtrée (I, 2.1.11). Les algèbres TL et SL sont munies de leurs filtrations canoniques (I, 3.3.3).

Définissons la filtration de JL (resp. de $J_n L$) comme *induite* (I, 2.1.5) par celle de TL, puis la filtration de UL (resp. de $U_n L$) comme *filtration quotient* (I, 2.1.7) de TL (resp. de $T_n L$).

La filtration de UL peut encore être définie comme la *borne inférieure des filtrations de Ω-algèbre pour lesquelles l'application canonique de* L *dans* UL *est un morphisme.*

Chacun des diagrammes $D_n L$ (2.1.3) devient un diagramme dans la catégorie des Ω-modules filtrés (I, 2.1.4). Pour chaque nombre $\nu \in \mathbf{R}_+$, nous définissons le diagramme $(D_n L)_\nu$ à partir de $D_n L$ en appliquant le foncteur « ν en indice ». Autrement dit, nous remplaçons chacun des modules M figurant dans $D_n L$ par le sous-module M_ν des éléments de filtration $\geqslant \nu$, les morphismes de $D_n L$ étant remplacés par leurs restrictions correspondantes.

La formule (2.1.3.2) reste valable dans la catégorie des Ω-modules filtrés (I, 2.1.8).

(2.2.2) *Les morphismes fonctoriels.* — Conservons les notations précédentes. Nous avons une algèbre de Lie graduée gr L sur l'anneau gradué gr Ω (I, 2.3.11), et nous pouvons construire son algèbre enveloppante U gr L ainsi que les diagrammes $D_n$gr L dans la catégorie des gr Ω-modules gradués (2.1.4).

D'autre part, nous pouvons prendre les gradués associés des modules filtrés définis en (2.2.1).

Si nous appliquons le foncteur gr au diagramme D_nL dans la catégorie Fil(Ω), nous obtenons le diagramme gr D_nL dans la catégorie Gr(gr Ω).

Les suites exactes (2.1.1.2) et (2.1.2.7) conduisent (I, 2.3.8) aux suites exactes :

(2.2.2.1) $$0 \to \mathrm{gr}\, JL \to \mathrm{gr}\, TL \to \mathrm{gr}\, UL;$$

(2.2.2.2) $$0 \to \mathrm{gr}\, J_nL \to \mathrm{gr}\, T_nL \to \mathrm{gr}\, U_nL.$$

Le *morphisme fonctoriel* $T\,\mathrm{gr}\, L \to \mathrm{gr}\, TL$ nous donne, par restriction, les morphismes fonctoriels

(2.2.2.3) $$J\,\mathrm{gr}\, L \to \mathrm{gr}\, JL,$$

(2.2.2.4) $$J_n\mathrm{gr}\, L \to \mathrm{gr}\, J_nL,$$

puis, en complétant le diagramme exact

$$\begin{tikzcd} 0 \arrow[r] & J\,\mathrm{gr}\, L \arrow[r] \arrow[d] & T\,\mathrm{gr}\, L \arrow[r] \arrow[d] & U\,\mathrm{gr}\, L \arrow[r] & 0 \\ 0 \arrow[r] & \mathrm{gr}\, JL \arrow[r] & \mathrm{gr}\, TL \arrow[r] & \mathrm{gr}\, UL, & \end{tikzcd}$$

le morphisme fonctoriel

(2.2.2.5) $$U\,\mathrm{gr}\, L \to \mathrm{gr}\, UL,$$

et, de même, les morphismes fonctoriels

(2.2.2.6) $$U_n\mathrm{gr}\, L \to \mathrm{gr}\, U_nL.$$

Au moyen de (2.2.2.4), (2.2.2.6) et des morphismes déjà définis en (I, 3.3.1) nous obtenons les *morphismes fonctoriels de diagrammes commutatifs*

(2.2.2.7) $$D_n\mathrm{gr}\, L \to \mathrm{gr}\, D_nL.$$

(2.2.3) *Définition des suites exactement filtrées.* — Soit

(2.2.3.1) $$0 \to M' \xrightarrow[f]{} M \xrightarrow[g]{} M'' \to 0$$

une suite de morphismes de Ω-modules filtrés (I, 2.1.4). Nous disons que la suite (2.2.3.1) est *exactement filtrée* si, *pour chaque nombre* $\nu \in \mathbf{R}_+$, la suite des restrictions

(2.2.3.2) $$0 \to M'_\nu \xrightarrow[f_\nu]{} M_\nu \xrightarrow[g_\nu]{} M''_\nu \to 0$$

est une *suite exacte* (dans la catégorie des Ω-modules).

(2.2.4) *Théorème.* — *Soient* Ω *un anneau de valuation discrète complet* (I, 3.1.1) *et* L *une* Ω*-algèbre de Lie valuée* (I, 2.2.4). *Alors, pour chaque* $n \in \mathbf{N}^*$,

(2.2.4.1) *les lignes et les colonnes du diagramme* D_nL *sont exactement filtrées ;*

(2.2.4.2) *le diagramme* $D_n\mathrm{gr}\, L$ *est exact ;*

(2.2.4.3) *le morphisme fonctoriel* $D_n \operatorname{gr} L \to \operatorname{gr} D_n L$ *est un isomorphisme de diagrammes commutatifs.*

Nous prouverons ce théorème, ainsi que les corollaires qui suivent, en (2.3). Remarquons déjà que (2.2.4.2) est vérifié parce que l'anneau $\operatorname{gr} \Omega$ est principal (2.1.3).

(2.2.5) *Corollaire. — Avec les notations précédentes, l'algèbre filtrée* UL *est une* Ω*-algèbre valuée, et valuée en tant qu'anneau. Le morphisme fonctoriel* $U \operatorname{gr} L \to \operatorname{gr} UL$ *est un isomorphisme.*

(2.2.6) *Corollaire. — Si* $f: L \to L'$ *est un homomorphisme et une isométrie de* Ω*-algèbres de Lie valuées, alors* $Uf: UL \to UL'$ *est une isométrie.*

(2.2.7) *Corollaire. — Soit* $(x_i)_{i \in I}$ *une famille filtrée-libre* (I, 2.1.16) *dans une* Ω*-algèbre de Lie valuée* L. *Si nous ordonnons totalement l'ensemble d'indices* I, *les monômes ordonnés* x^α *forment une famille filtrée-libre dans* UL, α *parcourant l'ensemble* $\mathbf{N}^{(I)}$. *Si les* (x_i) *constituent une base filtrée (resp. base topologique) de* L, *alors les* (x^α) *constituent une base filtrée de* UL *(resp. une base topologique du complété* $\widehat{UL}$ *de* UL).

(2.3) Preuves du théorème (2.2.4) et de ses corollaires.

(2.3.1) *Lemme. — Soit* (2.2.3)

$$0 \to M' \to M \to M'' \to 0$$

une suite exactement filtrée (sur un anneau filtré Ω *quelconque). Alors la suite des gradués associés*

$$0 \to \operatorname{gr} M' \to \operatorname{gr} M \to \operatorname{gr} M'' \to 0$$

est exacte.

Preuve. — Pour chaque $\nu \in \mathbf{R}_+$, nous considérons le diagramme commutatif

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_{\nu+} & \longrightarrow & M_{\nu+} & \longrightarrow & M''_{\nu+} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_{\nu} & \longrightarrow & M_{\nu} & \longrightarrow & M''_{\nu} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{gr}_\nu M' & \longrightarrow & \operatorname{gr}_\nu M & \longrightarrow & \operatorname{gr}_\nu M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Les trois colonnes sont exactes, par définition du foncteur gr. La seconde ligne est exacte, par la définition (2.2.3); la première ligne est exacte (par passage à la réunion, ou limite inductive, des suites exactes pour les nombres $\nu' > \nu$). Par conséquent la troisième ligne est exacte.

(2.3.2) *Lemme. — Soit*

(2.3.2.1) $$0 \to M' \xrightarrow[f]{} M \xrightarrow[g]{} M'' \to 0$$

une suite de morphismes de Ω-modules filtrés. Pour que cette suite soit exactement filtrée (2.2.3), *il faut et il suffit que les trois conditions suivantes soient vérifiées.*

(2.3.2.2) *La suite* (2.3.2.1) *est exacte dans la catégorie des Ω-modules (non filtrés).*

(2.3.2.3) *Le morphisme* $\mathrm{gr} f$ *est injectif.*

(2.3.2.4) *Pour chaque* $\nu \in \mathbf{R}_+$, *l'application* $g_\nu : M_\nu \to M''_\nu$ *est surjective.*

Preuve. — Ces trois conditions sont nécessaires. En effet, (2.3.2.2) s'obtient en faisant $\nu = 0$ dans (2.2.3.2). L'injectivité de $\mathrm{gr} f$ résulte de (2.3.1). Enfin (2.3.2.4) est une partie de (2.2.3.2).

Réciproquement si nous supposons vérifiées les trois conditions, la seule propriété non immédiate relative à l'exactitude de la suite

$$0 \to M'_\nu \xrightarrow[f_\nu]{} M_\nu \xrightarrow[g_\nu]{} M''_\nu \to 0$$

est la relation $\mathrm{Ker}\, g_\nu \subset \mathrm{Im} f_\nu$. Or, si $x \in \mathrm{Ker}\, g_\nu$, il existe $y \in M'$ tel que $x = f(y)$, d'après (2.3.2.2) et $w(M'; y) = w(M; x)$ d'après (2.3.2.3), ce qui entraîne $y \in M'_\nu$ et $x \in \mathrm{Im} f_\nu$.

(2.3.3) *Lemme. — Considérons, dans une catégorie de modules, le diagramme commutatif suivant, dont nous supposons les lignes et les colonnes exactes*

(2.3.3.1)
$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & A'' & \longrightarrow & B'' & \longrightarrow & C'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Si l'introduction d'un morphisme $f : C' \to C$ (*resp.* $g : C \to C''$) *conserve la commutativité du diagramme, alors f est injectif (resp. g est surjectif).*

(2.3.4) *Preuve du théorème* (2.2.4). — Soient Ω un anneau de valuation discrète complet et L une Ω-algèbre de Lie valuée.

(2.3.4.1) *Pour chaque* $n \in \mathbf{N}^*$,

$$0 \to T_{n-1}L \to T_n L \to T^n L \to 0$$

est une suite exactement filtrée de Ω*-modules valués.*

En effet ces modules sont valués, d'après le théorème (I, 3.2.7) et une suite exacte scindée (dans la catégorie des Ω-modules filtrés) est exactement filtrée.

(2.3.4.2) *Pour chaque* $n \in \mathbf{N}$,

$$0 \to I^n L \to T^n L \to S^n L \to 0$$

est une suite exactement filtrée de Ω*-modules valués.*

C'est une conséquence du théorème (I, 3.2.7).

(2.3.4.3) *Pour chaque* $n \in \mathbf{N}^*$,

$$0 \to J_{n-1}L \to J_n L \to I^n L \to 0$$

est une suite exactement filtrée de Ω*-modules valués.*

En effet, la condition (2.3.2.2) du lemme (2.3.2) est vérifiée, car le théorème de Poincaré-Birkhoff-Witt est valable (l'anneau Ω étant principal). La condition (2.3.2.3) est vérifiée puisque $J_{n-1}L$ est un sous-module valué de $J_n L$. Enfin, la condition (2.3.2.4) résulte du théorème (I, 3.2.7) et de la forme (2.1.2.3) des générateurs de $J_n L$.

(2.3.4.4) *Pour chaque* $n \in \mathbf{N}$ *et chaque* $\nu \in \mathbf{R}_+$, *nous avons les suites exactes*

$$0 \to (J_n L)_\nu \to (T_n L)_\nu \to (U_n L)_\nu,$$

et

$$0 \to \operatorname{gr} J_n L \to \operatorname{gr} T_n L \to \operatorname{gr} U_n L.$$

Ces assertions résultent de la définition des filtrations canoniques (2.2.1) et de (I, 2.3.8).

(2.3.4.5) Démontrons maintenant les assertions (2.2.4.1) par récurrence sur n. Nous prouvons que la suite

$$0 \to U_{n-1}L \to U_n L \to S_n L \to 0$$

est exactement filtrée en lui appliquant le lemme (2.3.2). La condition (2.3.2.2) résulte de la validité du théorème de Poincaré-Birkhoff-Witt (2.1.3). Pour vérifier (2.3.2.3), nous montrons que l'application $\operatorname{gr} U_{n-1}L \to \operatorname{gr} U_n L$ est injective, en appliquant le lemme (2.3.3) au diagramme $\operatorname{gr} D_n L$, compte tenu de (2.3.4.1), (2.3.4.2), (2.3.4.3), de notre hypothèse de récurrence, et du lemme (2.3.1). Enfin nous vérifions (2.3.2.4) en appliquant le lemme (2.3.3) au diagramme $(D_n L)_\nu$.

Le diagramme $(D_n L)_\nu$ possède ainsi trois colonnes et deux lignes exactes, ce qui implique l'exactitude de la ligne restante. Nous venons de prouver (2.2.4.1).

(2.3.4.6) Les seules assertions de (2.2.4.3) qui ne figurent pas dans l'énoncé du théorème (I, 3.3.7) concernent les isomorphismes

$$J_n \mathrm{gr}\, L \to \mathrm{gr}\, J_n L \qquad \text{et} \qquad U_n \mathrm{gr}\, L \to \mathrm{gr}\, U_n L.$$

Nous les prouvons par récurrence sur n, à partir des diagrammes exacts

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_{n-1}\mathrm{gr}\, L & \to & J_n \mathrm{gr}\, L & \to & I^n \mathrm{gr}\, L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{gr}\, J_{n-1}L & \to & \mathrm{gr}\, J_n L & \to & \mathrm{gr}\, I^n L & \longrightarrow & 0 \end{array}$$

$$\begin{array}{ccccccccc} 0 & \to & U_{n-1}\mathrm{gr}\, L & \to & U_n \mathrm{gr}\, L & \to & S^n \mathrm{gr}\, L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{gr}\, U_{n-1}L & \to & \mathrm{gr}\, U_n L & \to & \mathrm{gr}\, S^n L & \to & 0 \end{array}$$

(2.3.5) *Lemme. — Soit*

$$0 \to M' \to M \to M'' \to 0$$

une suite exactement filtrée de Ω-modules filtrés. Si M' *et* M'' *sont valués, alors* M *est valué.*

Preuve. — Nous vérifions que M est séparé. D'après (2.3.1), le module gr M est sans torsion, comme extension de modules sans torsion.

(2.3.6) *Preuve du corollaire* (2.2.5). — Nous prouvons que les modules $U_n L$ sont valués par récurrence sur n, en appliquant le lemme (2.3.5) aux suites exactement filtrées

$$0 \to U_{n-1}L \to U_n L \to S^n L \to 0.$$

Le module UL s'obtient alors (2.2.1) comme limite inductive de modules valués, calculée pour une famille d'*isométries*. Il est donc *valué* (I, 2.3.9). Nous pouvons passer à la limite inductive dans les isomorphismes $U_n \mathrm{gr}\, L \to \mathrm{gr}\, U_n L$, et nous obtenons ainsi l'isomorphisme

(2.3.6.1) $$U\, \mathrm{gr}\, L \to \mathrm{gr}\, UL.$$

Cet isomorphisme vaut pour les structures d'anneaux (ou de gr Ω-algèbres) de U gr L et de gr UL. Pour démontrer que UL est valué en tant qu'anneau, nous sommes donc ramenés à prouver que U gr L est sans diviseurs de zéro. Or, pour sa « filtration croissante » canonique, U gr L a comme gradué associé S gr L qui est une algèbre de polynômes (I, 1.2.3).

(2.3.7) *Preuve du corollaire* (2.2.6). — D'après le théorème (I, 3.3.7), les applications

(2.3.7.1) $$S^n f : S^n L \to S^n L'$$

sont injectives. Nous en déduisons que les applications

(2.3.7.1) $$U_n f : U_n L \to U_n L'$$

sont injectives, par récurrence sur n au moyen des suites exactes

$$0 \to U_{n-1}L \to U_n L \to S^n L \to 0.$$

Cela prouve le corollaire, puisque UL est réunion (par abus de langage) des $U_n L$.

(2.3.8) *Preuve du corollaire* (2.2.7). — Nous prouvons, par récurrence sur n, que les (x^α) forment une famille filtrée-libre pour $|\alpha| \leqslant n$. Cela est vrai pour $n = 1$ (rappelons que les x_i sont d'augmentation nulle). Le passage de $(n-1)$ à n utilise le théorème (I, 3.3.7), et la suite exacte $0 \to U_{n-1}L \to U_n L \to S^n L \to 0$.

3. GROUPES ET ALGÈBRES DE LIE

(3.1) Le théorème de saturation des algèbres de Lie.

(3.1.1) *Les algèbres diagonales valuées* UL *et leurs extensions.* — Désignons de nouveau par Ω un anneau de valuation discrète complet, d'inégales caractéristiques, avec $v(p) = 1$. Soit L une Ω-algèbre de Lie valuée. Nous avons défini en (1.1.3) l'algèbre enveloppante UL comme une algèbre diagonale stricte. D'autre part l'algèbre UL est valuée (2.2.5) et son application diagonale est un morphisme de Ω-algèbres valuées. Nous avons donc une structure de Ω-*algèbre diagonale valuée* sur l'algèbre UL (1.2.5), ainsi que sur les algèbres complétée, divisée ou saturée de UL (1.2.6). Nous utiliserons surtout l'algèbre saturée Sat UL. Tout morphisme $f : L \to L'$ se prolonge en un morphisme $\operatorname{Sat} Uf : \operatorname{Sat} UL \to \operatorname{Sat} UL'$ (ce qui exprime le caractère fonctoriel de Sat U); si f est une isométrie, alors Sat Uf est une isométrie, d'après (2.2.6) et (I, 2.2.11).

(3.1.2) *Lemme. — Pour toute Ω-algèbre de Lie valuée* L, *le morphisme fonctoriel*

(3.1.2.1) $$\operatorname{Sat} UL \to \operatorname{Sat} U \operatorname{Sat} L,$$

déduit de l'injection $L \to \operatorname{Sat} L$, *est un isomorphisme.*

Preuve. — L'isométrie $L \to \operatorname{div} L$ se prolonge en une isométrie $UL \to U \operatorname{div} L$. Si nous identifions UL à un sous-module de U div L, le quotient est un Ω-module de torsion, ce qui prouve (I, 2.2.9) que le morphisme

(3.1.2.2) $$\operatorname{div} UL \to \operatorname{div} U \operatorname{div} L$$

est un isomorphisme, ainsi que le morphisme des complétés :

(3.1.2.3) $$\operatorname{Sat} UL \to \operatorname{Sat} U \operatorname{div} L.$$

Comme div L est dense dans Sat L, l'image de div U div L est dense dans div U Sat L, et le morphisme

(3.1.2.4) $$\operatorname{Sat} U \operatorname{div} L \to \operatorname{Sat} U \operatorname{Sat} L$$

est un isomorphisme. Les relations (3.1.2.3) et (3.1.2.4) prouvent notre lemme.

(3.1.3) *Théorème de saturation.* — *Soit* L *une* Ω*-algèbre de Lie valuée. Dans l'algèbre diagonale valuée* Sat UL *nous avons les relations*

$$\mathscr{L}\,\text{Sat UL} = \text{Sat L}. \tag{3.1.3.1}$$

$$\mathscr{G}\,\text{Sat UL} = \mathscr{G}^*\,\text{Sat UL}. \tag{3.1.3.2}$$

Rappelons que les foncteurs $\mathscr{L}$, $\mathscr{G}$, $\mathscr{G}^*$ ont été définis en (1.3.1), et que nous identifions Sat L à un sous-module de Sat UL. D'après le lemme (3.1.2), nous pouvons supposer que L est une algèbre saturée. Nous nous ramènerons au cas où L possède une base topologique, au moyen des lemmes (3.1.6) et (3.1.7), d'où résulteront respectivement des énoncés un peu plus précis que (3.1.3.1) et (3.1.3.2). Formulons d'abord un corollaire.

(3.1.4) *Corollaire.* — *Toute* Ω*-algèbre de Lie saturée* L *peut s'obtenir sous la forme* $\mathscr{L}$A, *où* A *est une algèbre diagonale saturée.*

Il suffit en effet de prendre $A = \text{Sat UL}$.

Soit A une Ω-algèbre diagonale saturée. Posons $L = \mathscr{L}A$ et $B = \text{Sat UL}$. Le morphisme fonctoriel (1.3.3.2)

$$\text{UL} \to \text{A} \tag{3.1.4.1}$$

se prolonge en un *morphisme de* Ω*-algèbres diagonales saturées*

$$f : \text{B} \to \text{A}. \tag{3.1.4.2}$$

Comme l'a montré l'exercice (1.2.9), le morphisme f n'est pas nécessairement une isométrie. Néanmoins sa *restriction à* $\mathscr{L}$B (resp. $\mathscr{L}^*$B, $\mathscr{G}^*$B) est un *isomorphisme* sur $\mathscr{L}$A (resp. $\mathscr{L}^*$A, $\mathscr{G}^*$A). Cela justifie la définition suivante.

(3.1.5) *Définition.* — *Une* Ω*-algèbre diagonale saturée* A *sera dite normale si le morphisme fonctoriel* $\text{Sat U}\mathscr{L}\text{A} \to \text{A}$ *est un isomorphisme.*

(3.1.6) *Lemme.* — *Soit* L *une* Ω*-algèbre de Lie valuée admettant la base topologique* $(y_i)_{i \in I}$ (I, 2.1.17). *Supposons l'ensemble d'indices* I *totalement ordonné. Notons* K *le corps des fractions de l'anneau* Ω, A *l'algèbre diagonale saturée* Sat UL, w *la valuation de* A *et* Δ *son application diagonale. Posons* $\tau_i = w(y_i)$ *pour* $i \in I$.

(3.1.6.1) *Si* $x \in A$, $x \notin \text{Sat L}$, *nous avons*

$$w(\Delta x - x \otimes 1 - 1 \otimes x) \leqslant d + 1,$$

où

$$d = \sup_{z \in \text{Sat L}} w(x - z).$$

(3.1.6.2) *Les éléments de* $\mathscr{G}$A *s'écrivent univoquement comme des produits ordonnés*

$$x = \prod_{i \in I} \exp(\lambda_i y_i)$$

où les λ_i *sont des éléments de* K *vérifiant les conditions suivantes : pour chaque* $i \in I$,

$v(\lambda_i)+\tau_i>(p-1)^{-1}$, *et* $v(\lambda_i)+\tau_i$ *tend vers l'infini* (*suivant le filtre des complémentaires des parties finies de* I). *Nous en déduisons* (III, 1.1.4)

$$\omega(x)=w(x-1)=\inf_{i\in I}(v(\lambda_i)+\tau_i),$$

et $\mathscr{G}\mathrm{A}=\mathscr{G}^*\mathrm{A}$.

Si $\Omega=\mathbf{Z}_p$, *les éléments* $\exp(p^{h_i}y_i)$ *constituent une base ordonnée du groupe p-saturé* $\mathscr{G}^*\mathrm{A}$, *les entiers* $h_i\in\mathbf{Z}$ *étant déterminés par les conditions*

$$(p-1)^{-1}<\tau_i+h_i\leqslant p(p-1)^{-1}.$$

Preuve. — Posons $\mathbf{N}^{(I)}=\mathrm{J}$, et $\tau\alpha=\sum_{i\in I}\tau_i\alpha_i$ pour $\alpha\in\mathrm{J}$. D'après (2.2.7), les *monômes ordonnés* y^α $(\alpha\in\mathrm{J})$ constituent une base topologique du complété $\hat{\mathrm{U}}\mathrm{L}$ de l'algèbre enveloppante UL, et nous avons $w(y^\alpha)=\tau\alpha$ (2.2.5). Nous obtenons donc une base topologique de A en divisant les y^α par des puissances convenables d'une uniformisante ϖ de Ω (I, 3.1.7). Il est plus simple d'écrire les éléments de A comme des séries

(3.1.6.3)
$$x=\sum_{\alpha\in J}\lambda_\alpha y^\alpha,$$

où les λ_α sont des éléments de K qui vérifient les conditions suivantes : $v(\lambda_\alpha)+\tau\alpha\geqslant 0$ pour tout $\alpha\in\mathrm{J}$, et $v(\lambda_\alpha)+\tau\alpha\to\infty$ (suivant le filtre des complémentaires des parties finies de A). Nous avons alors

(3.1.6.4)
$$w(x)=\inf_{\alpha\in J}(v(\lambda_\alpha)+\tau\alpha).$$

L'application diagonale Δ est définie, comme en (1.1.9), par les formules

(3.1.6.5)
$$\Delta y^\alpha=\sum_{\beta+\gamma=\alpha}(\beta,\gamma)y^\beta\otimes y^\gamma.$$

Pour l'élément $x\in\mathrm{A}$ donné par la série (3.1.6.3), nous obtenons

(3.1.6.6)
$$\Delta x-x\otimes 1-1\otimes x=-\lambda_0 1\otimes 1+\sum_{\beta,\gamma>0}(\beta,\gamma)\lambda_{\beta+\gamma}y^\beta\otimes y^\gamma.$$

La dernière somme est étendue aux couples β, γ d'éléments de J, avec $\beta>0$ et $\gamma>0$.

Le nombre d défini en (3.1.6.1) est égal à

(3.1.6.7)
$$d=\inf_{\alpha\in J,\,|\alpha|\neq 1}(v(\lambda_\alpha)+\tau\alpha).$$

La preuve de (3.1.6.1) s'achève en remarquant que, si $\alpha\in\mathrm{J}$ avec $|\alpha|>1$, il existe β et $\gamma\in\mathrm{J}$, avec $\beta>0$, $\gamma>0$, $\beta+\gamma=\alpha$ et $v((\beta,\gamma))\leqslant 1$.

Passons à la preuve de (3.1.6.2). Pour le même élément x (3.1.6.3), nous avons

(3.1.6.8)
$$x\otimes x-\Delta x=\sum_{\beta,\gamma\in J}(\lambda_\beta\lambda_\gamma-(\beta,\gamma)\lambda_{\beta+\gamma})y^\beta\otimes y^\gamma.$$

Pour que cet élément appartienne à $\mathscr{G}\mathrm{A}$, il faut et il suffit que $\lambda_0=1$, et que

(3.1.6.9)
$$\lambda_\beta\lambda_\gamma-(\beta,\gamma)\lambda_{\beta+\gamma}=0$$

pour tous $\beta, \gamma \in J$. Ces équations montrent que les λ_α sont déterminés par la seule donnée des $\lambda_i = \lambda_{\delta_i}$ (rappelons que δ_i est l'élément α de J vérifiant $\alpha_i = 1$ et $|\alpha| = 1$). Plus précisément, les relations (3.1.6.9) équivalent, si $\lambda_0 = 1$, à

$$\lambda_\alpha = (\alpha!)^{-1}\lambda^\alpha = (\alpha!)^{-1}\prod_i \lambda_i^{\alpha_i}, \tag{3.1.6.10}$$

pour tout $\alpha \in J$. Comme $v(\lambda_\alpha) + \tau\alpha$ doit tendre vers l'infini, nous devons avoir $v(\lambda_i) + \tau_i > (p-1)^{-1}$, d'après (III, 1.1.2), et $v(\lambda_i) + \tau_i$ tend vers l'infini. Les éléments $\exp(\lambda_i y_i)$ sont donc définis dans A (III, 1.1.4), et leur produit converge vers x.

(3.1.7) *Lemme. — Conservons les notations du lemme* (3.1.6). *Soit x un élément de* A, *d'augmentation* 1, *et vérifiant*

$$w(x-1) \leqslant (p-1)^{-1}.$$

Nous avons alors la relation

$$w(x \otimes x - \Delta x) \leqslant p(p-1)^{-1}. \tag{3.1.7.1}$$

Preuve. — Supposons d'abord que la base topologique de L se réduise au seul élément y, avec $w(y) = \tau$. Écrivons x sous la forme

$$x = \sum_{n \in \mathbf{N}} \lambda_n y^n \qquad (\lambda_n \in \mathrm{K}). \tag{3.1.7.2}$$

Posons, pour chaque $n \in \mathbf{N}$,

$$c(n) = v(\lambda_n) + \tau n. \tag{3.1.7.3}$$

Pour que x appartienne à A, nous devons avoir $c(n) \geqslant 0$ pour tout $n \in \mathbf{N}$, et $c(n)$ doit tendre vers l'infini avec n. Nous avons, par hypothèse, $\lambda_0 = 1$ et il existe un $n \in \mathbf{N}^*$ tel que

$$c(n) \leqslant (p-1)^{-1}. \tag{3.1.7.4}$$

Supposons que $w(x \otimes x - \Delta x) > p(p-1)^{-1}$. D'après la formule (3.1.6.8), cela équivaut aux relations

$$v(\lambda_m \lambda_n - (m, n)\lambda_{m+n}) + \tau(m+n) > p(p-1)^{-1} \tag{3.1.7.5}$$

pour tous $m, n \in \mathbf{N}$.

Désignons par r le plus petit entier $n \geqslant 1$ pour lequel $c(n)$ atteint son minimum. Nous avons donc $r \geqslant 1$ et

$$c(n) > c(r) \qquad \text{pour} \qquad 1 \leqslant n < r. \tag{3.1.7.6}$$

D'après (3.1.7.4), nous avons

$$c(r) \leqslant (p-1)^{-1}. \tag{3.1.7.7}$$

Supposons d'abord que r ne soit pas de la forme p^h, où $h \in \mathbf{N}$. Il existe alors $m, n \in \mathbf{N}^*$, tels que $m + n = r$ et $v((m, n)) = 0$. Nous avons, d'après (3.1.7.6)

$$c(m) + c(n) > 2c(r) \geqslant c(r). \tag{3.1.7.8}$$

Nous en déduisons la relation

(3.1.7.9) $$v(\lambda_m\lambda_n) > v(\lambda_r) = v((m, n)\lambda_r),$$

et les relations (3.1.7.5) et (3.1.7.7) sont contradictoires.

Nous sommes donc ramenés au cas où $r = p^h$. Supposons, plus généralement, que, pour un certain $h \in \mathbf{N}$, nous ayons la relation

(3.1.7.10) $$c(p^h) \leqslant (p-1)^{-1}.$$

Nous en déduisons, par récurrence sur i, à partir de (3.1.7.5),

(3.1.7.11) $$c(ip^h) = ic(p^h), \quad pour\ 1 \leqslant i < p,$$

puis la relation

(3.1.7.12) $$c(p^{h+1}) = pc(p^h) - 1.$$

Cette dernière relation s'écrit encore

(3.1.7.13) $$c(p^{h+1}) - (p-1)^{-1} = p(c(p^h) - (p-1)^{-1}).$$

La relation (3.1.7.10) reste donc valable si l'on y remplace h par $h+1$. Plus généralement, nous obtenons par récurrence sur $n \in \mathbf{N}$,

(3.1.7.14) $$c(p^{h+n}) - (p-1)^{-1} = p^n(c(p^h) - (p-1)^{-1}),$$

d'où, puisque $c(n)$ est toujours positif,

(3.1.7.15) $$c(p^{h+n}) = (p-1)^{-1} \quad \text{pour tout } n \in \mathbf{N},$$

ce qui contredit l'hypothèse que $c(n)$ tend vers l'infini avec n.

Traitons maintenant le cas général. Soit $x \in \mathrm{A}$, avec $x = \sum_{\alpha \in \mathrm{J}} \lambda_\alpha y^\alpha$, $\lambda_0 = 1$. Supposons que $w(x \otimes x - \Delta x) > p(p-1)^{-1}$. Cela équivaut aux relations

(3.1.7.16) $$v(\lambda_\beta\lambda_\gamma - (\beta, \gamma)\lambda_{\beta+\gamma}) + \tau(\beta+\gamma) > p(p-1)^{-1},$$

pour tous $\beta, \gamma \in \mathrm{J}$. Nous venons de voir que $v(\lambda_\alpha) + \tau\alpha > (p-1)^{-1}$ pour chaque $\alpha \in \mathrm{J}$ de la forme $n\delta_i$, $n \in \mathbf{N}$, $i \in \mathrm{I}$. Si nous avons $w(x-1) \leqslant (p-1)^{-1}$, choisissons $\alpha \in \mathrm{J}$ tel que $v(\lambda_\alpha) + \tau\alpha \leqslant (p-1)^{-1}$, et que le nombre d'indices $i \in \mathrm{I}$ avec $\alpha_i > 0$ soit minimum. Il existe alors β et $\gamma \in \mathrm{J}$, vérifiant les relations : $\beta + \gamma = \alpha$, $v((\beta, \gamma)) = 0$, $v(\lambda_\beta) + \tau\beta > (p-1)^{-1}$, $v(\lambda_\gamma) + \tau\gamma > (p-1)^{-1}$.

Ces relations sont incompatibles avec (3.1.7.16), et notre lemme est prouvé.

(3.1.8) *Preuve de* (3.1.3). — Supposons l'algèbre de Lie L saturée. Si $x \in \mathscr{L}$ Sat UL, $x \notin \mathrm{L}$, posons

(3.1.8.1) $$d = \sup_{z \in \mathrm{L}} w(\mathrm{Sat\ UL}; z - x).$$

Soit M une *sous-algèbre saturée* de L, engendrée par une *famille finie* d'éléments. Nous pouvons identifier Sat UM à une sous-algèbre de Sat UL (2.2.6). Lorsque M varie, les sous-algèbres Sat UM forment une famille filtrante croissante de sous-modules divisibles de Sat UL. Leur réunion contient UL, donc div UL, et est *dense* dans Sat UL. Nous pouvons donc choisir la sous-algèbre de Lie saturée de type fini M de telle sorte qu'il existe un élément $x' \in \mathrm{Sat\,UM}$, avec

$$w(\mathrm{Sat\,UL};\, x-x') > d+1. \tag{3.1.8.2}$$

La relation (3.1.8.1) implique alors

$$\sup_{z' \in \mathrm{M}} w(\mathrm{Sat\,UM};\, z'-x') \leqslant d, \tag{3.1.8.3}$$

et la relation $x \in \mathscr{L}\,\mathrm{Sat\,UL}$ implique

$$w(\mathrm{Sat\,UM};\, \Delta x' - x' \otimes 1 - 1 \otimes x') > d+1. \tag{3.1.8.4}$$

Or l'algèbre de Lie saturée M possède une base topologique, d'après (I, 3.1.10), et les relations (3.1.8.3), (3.1.8.4) sont incompatibles, d'après (3.1.6.1). Cela prouve la première assertion du théorème (3.1.3); la seconde s'établit par la même méthode, grâce au lemme (3.1.7). Nous démontrons un résultat plus précis que le théorème (3.1.3) : les lemmes (3.1.6.1) et (3.1.7) restent valables sans supposer que L possède une base topologique.

(3.2) Transport de structures.

(3.2.1) *Application du théorème de saturation à une algèbre de Lie libre.* — Soient L la $\mathbf{Z}_p$-algèbre de Lie libre engendrée par deux éléments x et y, et t un nombre $\geqslant 0$. L'algèbre enveloppante UL est une $\mathbf{Z}_p$-algèbre associative libre engendrée par x et y. Munissons L de la borne inférieure w des filtrations d'algèbre pour lesquelles $w(x) \geqslant t$ et $w(y) \geqslant t$ (ou encore pour lesquelles tous les éléments ont une filtration $\geqslant t$). Cette filtration est une *valuation*, et la structure d'*algèbre diagonale valuée* de UL définie en (3.1.1) coïncide avec une de celles définies en (1.2.8).

L'algèbre saturée Sat UL dépend de t, mais nous pouvons toujours considérer Sat UL comme un sous-anneau de l'algèbre de Magnus engendrée par x et y sur le corps $\mathbf{Q}_p$ (II, 1.1.10).

Un élément z de Sat UL (resp. de Sat L) s'écrit univoquement comme une série

$$z = \sum_{n \in \mathbf{N}} u_n(x,y) \tag{3.2.1.1}$$

où, pour tout $n \in \mathbf{N}$, $u_n(x,y)$ est un *polynôme associatif* (resp. *polynôme de Lie*) *à coefficients dans* $\mathbf{Q}_p$ *homogène de degré total* n *en* x *et* y.

Pour chaque $n \in \mathbf{N}$, notons h_n *le plus petit entier* ($\in \mathbf{Z}$) tel que $p^{h_n} u_n(x,y)$ soit un *polynôme à coefficients dans* $\mathbf{Z}_p$ (si $u_n = 0$, posons $h_n = -\infty$). Nous avons alors les relations

(3.2.1.2) $nt - h_n \geqslant 0$ pour chaque $n \in \mathbf{N}$;

(3.2.1.3) $nt - h_n$ tend vers l'infini avec n;

(3.2.1.4) $w(\mathrm{Sat\,UL};\, z) = \inf_{n \in \mathbf{N}} (nt - h_n)$.

Supposons maintenant $t > (p-1)^{-1}$. Nous avons alors $x, y \in \mathscr{L}^*\mathrm{Sat\,UL}$. Nous en déduisons, d'après (1.3.5), $\exp x, \exp y \in \mathscr{G}^*\mathrm{Sat\,UL}$, puis (1.3.2) $(\exp x)(\exp y) \in \mathscr{G}^*\mathrm{Sat\,UL}$, d'où, d'après (1.3.5) et (3.1.3), les relations

(3.2.1.5) $$z = \mathrm{Log}(\exp x)(\exp y) \in \mathrm{Sat\,L};$$

(3.2.1.6) $$w(\mathrm{Sat\,UL}; z) > (p-1)^{-1}.$$

L'élément $\mathrm{Log}(\exp x)(\exp y)$ s'écrit donc sous la forme (3.2.1.1), les u_n étant des *polynômes de Lie*. Pour calculer $u_n(x, y)$ il suffit de connaître les termes des séries logarithme et exponentielle jusqu'au degré n. Les $u_n(x, y)$ sont donc des polynômes de Lie à *coefficients rationnels*. Nous avons $u_1(x, y) = x + y$ et $u_2(x, y) = \frac{1}{2}[x, y]$.

Les relations (3.2.1.4) et (3.2.1.6) nous donnent

(3.2.1.7) $$nt - h_n > (p-1)^{-1} \quad \text{pour } t > (p-1)^{-1},$$

c'est-à-dire

(3.2.1.8) $$h_n \leqslant [(n-1)(p-1)^{-1}] \quad \textit{pour } n \in \mathbf{N}^*.$$

(3.2.2) *Théorème : la formule de Hausdorff, sa majoration p-adique, et son application aux algèbres diagonales saturées. — Dans l'algèbre des séries formelles associatives en x et y à coefficients rationnels (algèbre de Magnus), l'élément*

(3.2.2.1) $$\Phi(x, y) = \mathrm{Log}(\exp x)(\exp y)$$

s'écrit sous la forme

(3.2.2.2) $$\Phi(x, y) = x + y + \frac{1}{2}[x, y] + \ldots + u_n(x, y) + \ldots,$$

où, pour chaque $n \in \mathbf{N}^*$, $u_n(x, y)$ *est un polynôme de Lie en* x, y *à coefficients rationnels, homogène de degré total* n. *Si nous posons*

(3.2.2.3) $$h_n = [(n-1)(p-1)^{-1}],$$

les polynômes de Lie $p^{h_n} u_n(x, y)$ *sont à coefficients p-entiers.*

Si A *est une algèbre diagonale saturée* (1.3.4), *et si* x', y' *sont deux éléments de* $\mathscr{L}^*\mathrm{A}$, *alors* $u_n(x', y')$ *est, pour chaque* $n \in \mathbf{N}^*$, *un élément de* $\mathscr{L}^*\mathrm{A}$, *et nous avons*

(3.2.2.4) $$\mathrm{Log}(\exp x')(\exp y') = \sum_{n \in \mathbf{N}^*} u_n(x', y'),$$

où la série du second membre converge dans $\mathscr{L}^*\mathrm{A}$.

Preuve. — Toutes ces assertions ont été établies en (3.2.1), à l'exception de (3.2.2.4). Pour vérifier cette dernière formule, posons $t = \min(w(\mathrm{A}; x'), w(\mathrm{A}; y'))$; construisons une Ω-algèbre de Lie libre L de générateurs x et y; valuons L par la borne inférieure w des filtrations pour lesquelles $w(x) \geqslant t$, $w(y) \geqslant t$. Il existe alors un morphisme d'algèbres diagonales saturées $f : \mathrm{Sat\,UL} \to \mathrm{A}$ défini par $f(x) = x'$ et $f(y) = y'$. La formule (3.2.2.4) est vérifiée par x et y dans Sat UL; l'existence de f montre que cette formule est encore vérifiée par x' et y' dans A.

(3.2.3) *Proposition. — Inversion de la formule de Hausdorff* (cf. exercice (III, 2.1.10)). *Soient* A *une algèbre diagonale saturée, et x, y deux éléments de* $\mathscr{G}^*$A. *Nous avons alors les relations suivantes :*

(3.2.3.1) $$\exp(\mathrm{Log}\,x+\mathrm{Log}\,y)=\lim_{i\to\infty}(x^{p^i}y^{p^i})^{p^{-i}}.$$

(3.2.3.2) $$\exp[\mathrm{Log}\,x,\ \mathrm{Log}\,y]=\lim_{i\to\infty}(x^{p^i},y^{p^i})^{p^{-2i}}$$

Les racines p^i-ièmes qui figurent dans ces formules doivent être calculées dans le groupe $\mathscr{G}^*$A *où elles sont univoquement déterminées.*

Preuve. — Posons $\mathrm{Log}\,x=x'$ et $\mathrm{Log}\,y=y'$. D'après le théorème (3.2.2), nous avons

$$\mathrm{Log}(xy)=x'+y'+\sum_{n\geqslant 2}u_n(x',y'),$$

et de même, pour chaque $i\in\mathbf{N}$,

(3.2.3.3) $$\mathrm{Log}(x^{p^i}y^{p^i})=p^i(x'+y')+\sum_{n\geqslant 2}p^{ni}u_n(x',y')$$

(3.2.3.4) $$\mathrm{Log}(x^{p^i}y^{p^i})^{p^{-i}}=x'+y'+p^i\sum_{n\geqslant 2}p^{(n-2)i}u_n(x',y').$$

Nous obtenons la formule (3.2.3.1) en transformant les deux membres de (3.2.3.4) par la fonction exponentielle, qui est continue, et en passant à la limite.

Pour démontrer la formule (3.2.3.2), nous utilisons la série donnant le « commutateur de Hausdorff »

(3.2.3.5) $$\Psi(x,y)=\mathrm{Log}(e^{-x}e^{-y}e^{x}e^{y})=\sum_{n\geqslant 2}v_n(x,y).$$

Les $v_n(x,y)$ sont des polynômes de Lie à coefficients rationnels, homogènes de degré total n. A partir de (3.2.2.2), nous calculons $v_2(x,y)$ qui est égal à $[x,y]$. Nous avons, dans l'algèbre saturée A

$$\mathrm{Log}(x,y)=[x',y']+\sum_{n\geqslant 3}v_n(x',y')$$

et de même, pour chaque $i\in\mathbf{N}$,

(3.2.3.6) $$\mathrm{Log}(x^{p^i},y^{p^i})=p^{2i}[x'y']+\sum_{n\geqslant 3}p^{ni}v_n(x',y'),$$

(3.2.3.7) $$\mathrm{Log}(x^{p^i},y^{p^i})^{p^{-2i}}=[x',y']+p^i\sum_{n\geqslant 3}p^{(n-3)i}v_n(x',y').$$

Cette dernière relation nous donne la formule (3.2.3.2).

(3.2.4) *Corollaire. — Soient* A *une algèbre diagonale saturée* (1.3.4), *et* G *un sous-groupe p-saturé de* $\mathscr{G}^*$A *pour la filtration induite* ω (III, 2.1.6). *Alors l'ensemble* L *des éléments* $\mathrm{Log}\,x$, *où* $x\in$G, *est une sous-$\mathbf{Z}_p$-algèbre de Lie de* $\mathscr{L}^*$A, *et* L *s'identifie à l'ensemble des éléments de filtration* $>(p-1)^{-1}$ *de l'algèbre* Sat L (*algèbre saturée de la $\mathbf{Z}_p$-algèbre de Lie* L).

Preuve. — Soient $x,y\in$G, $x'=\mathrm{Log}\,x$ et $y'=\mathrm{Log}\,y$. Nous avons, pour chaque $i\in\mathbf{N}$, $\omega(x^{p^i}y^{p^i})>i+(p-1)^{-1}$ et $\omega((x^{p^i},y^{p^i}))>2i+2(p-1)^{-1}$. Puisque le groupe G est p-saturé, cela prouve que les éléments $(x^{p^i}y^{p^i})^{p^{-i}}$ et $(x^{p^i}, y^{p^i})^{p^{-2i}}$ appartiennent à G. Comme ce groupe est fermé, la proposition (3.2.3) nous donne

(3.2.4.1) $$x' + y' \in \mathrm{L} \quad \text{et} \quad [x', y'] \in \mathrm{L}.$$

Nous avons aussi, pour $\lambda \in \mathbf{Z}_p$,

(3.2.4.2) $$\lambda x' = \operatorname{Log}(x^\lambda) \in \mathrm{L}.$$

La $\mathbf{Z}_p$-algèbre valuée L est *complète*, car isométrique au groupe complet G. Si $z \in \mathrm{L}$, alors $w(\mathrm{L}; z) > (p-1)^{-1}$ et, si $w(\mathrm{L}; z) > p(p-1)^{-1}$, z est divisible par p dans L. Nous en déduisons la relation

(3.2.4.3) $$\operatorname{div} \mathrm{L} = \operatorname{Sat} \mathrm{L},$$

et L s'identifie à l'ensemble des éléments de filtration $> (p-1)^{-1}$ dans Sat L.

(3.2.5) *Théorème de saturation des groupes. — Soient* G *un groupe p-saturé, et* $\mathrm{A} = \operatorname{Sat} \mathbf{Z}_p[\mathrm{G}]$ *la* $\mathbf{Z}_p$*-algèbre diagonale saturée, définie en* (1.2.8). *Alors nous avons la relation*

(3.2.5.1) $$\mathscr{G}^*\mathrm{A} = \mathrm{G},$$

et A *est une* $\mathbf{Z}_p$*-algèbre diagonale saturée normale, au sens de* (3.1.5).

Preuve. — Par définition de l'algèbre A, nous avons

(3.2.5.2) $$\mathrm{G} \subset \mathscr{G}^*\mathrm{A}.$$

Soit L l'ensemble des logarithmes des éléments de G, calculés dans A. D'après le corollaire (3.2.4), L est une $\mathbf{Z}_p$-algèbre de Lie, et, si nous appliquons le théorème (3.1.3) à l'algèbre diagonale saturée $\mathrm{B} = \operatorname{Sat} \mathrm{UL}$, nous obtenons la relation

(3.2.5.3) $$\mathrm{L} = \mathscr{L}^*\mathrm{B}.$$

L'injection canonique de L dans A se prolonge en un *morphisme de* $\mathbf{Z}_p$*-algèbres diagonales saturées*

(3.2.5.4) $$f : \mathrm{B} \to \mathrm{A}.$$

Si nous posons $\mathrm{G}' = \mathscr{G}^*\mathrm{B}$, le groupe G′ est l'ensemble des exponentielles des éléments de L (calculées dans B), d'après (3.2.5.3) et le théorème (1.3.5). La restriction de f à G′ est une *isométrie* (II, 1.1.3) de G′ sur G. D'après (1.3.3), les éléments de G′ sont linéairement indépendants dans B, c'est-à-dire qu'ils engendrent la sous-algèbre $\mathrm{B}' = \mathbf{Z}_p[\mathrm{G}'] \subset \mathrm{B}$. D'après la définition de la filtration induite de $\mathbf{Z}_p[\mathrm{G}]$ (III, 2.3.1), la restriction de f à B′ est une isométrie. Comme $\mathrm{B} = \operatorname{Sat} \mathrm{B}'$ (1.3.5.5), le morphisme f est une *isométrie surjective*, ce que nous voulions prouver.

(3.2.6) *Isomorphisme de catégories.* — Nous venons de voir que n'importe quel groupe p-saturé G est de la forme $\mathscr{G}^*\mathrm{A}$, où A est une $\mathbf{Z}_p$-algèbre diagonale saturée. Nous pouvons donc définir sur le même ensemble G une structure d'algèbre de Lie, au moyen des formules de la proposition (3.2.3). Réciproquement, si L est l'ensemble des éléments de valuation $> (p-1)^{-1}$ d'une $\mathbf{Z}_p$-algèbre de Lie saturée, nous pouvons définir sur le même ensemble L une structure de groupe au moyen de la formule de Hausdorff (3.2.2).

Nous obtenons ainsi un *isomorphisme de catégories*. Rappelons les axiomes qui définissent les objets de ces deux catégories :

L'ensemble G est un groupe, et ω est une application de G dans

$$\mathbf{R}_+ \cup \{+\infty\}.$$

Pour tout $x \in G$, $\omega(x) > (p-1)^{-1}$; $\omega(x) = \infty$ équivaut à $x = 1$, et $\omega(x^p) = \omega(x) + 1$; si $\omega(x) > p(p-1)^{-1}$, il existe $y \in G$ tel que $y^p = x$.

Pour tous $x, y \in G$, nous avons

$$\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))$$

et $$\omega((x, y)) \geqslant \omega(x) + \omega(y).$$

Si G_n désigne l'ensemble des $x \in G$, avec $\omega(x) \geqslant n$, les G_n ($n \in \mathbf{N}$) constituent un système fondamental de voisinages de 1 pour une topologie de groupe. Le groupe G est complet pour cette topologie.

L'ensemble L est une algèbre de Lie, et w est une application de L dans

$$\mathbf{R}_+ \cup \{+\infty\}.$$

Pour tout $x \in L$, $w(x) > (p-1)^{-1}$; $w(x) = \infty$ équivaut à $x = 0$, et $w(px) = w(x) + 1$; si $w(x) > p(p-1)^{-1}$, il existe $y \in L$ tel que $py = x$.

Pour tous $x, y \in L$, nous avons

$$w(x-y) \geqslant \min(w(x), w(y)),$$

et $$w([x, y]) \geqslant w(x) + w(y).$$

Si L_n désigne l'ensemble des $x \in L$, avec $w(x) \geqslant n$, les L_n ($n \in \mathbf{N}$) constituent un système fondamental de voisinages de 0 pour une topologie d'algèbre de Lie. L'algèbre L est complète pour cette topologie.

(3.2.7) *Automorphismes intérieurs.* — Soient A une algèbre diagonale saturée et x un élément de $\mathscr{L}^*A$. Notons g_x (resp. d_x) l'endomorphisme de A défini par la multiplication à gauche (resp. à droite) par x :

(3.2.7.1) $$g_x.y = xy; \qquad d_x.y = yx.$$

Nous avons, par définition du crochet

(3.2.7.2) $$\operatorname{ad} x = g_x - d_x.$$

La multiplication à gauche (resp. à droite) par l'élément $\exp x \in \mathscr{G}^*A$ s'écrit encore $\exp g_x$ (resp. $\exp d_x$). L'automorphisme intérieur

(3.2.7.3) $$y \mapsto (\exp x) y (\exp x)^{-1} \quad (y \in A),$$

s'écrit donc $(\exp g_x)(\exp(-d_x))$, ou encore, puisque g_x et d_x sont des endomorphismes permutables, $\exp(\operatorname{ad} x)$. Nous obtenons la formule

(3.2.7.4) $$(\exp x) y (\exp x)^{-1} = (\exp(\operatorname{ad} x)).y,$$

pour tout $y \in A$. Nous avons en particulier, pour $y \in \mathscr{L}^*A$,

(3.2.7.5) $$\operatorname{Log}((\exp x)(\exp y)(\exp(-x))) = (\exp(\operatorname{ad} x)).y.$$

(3.2.8) *Proposition.* — *Soient* G *un groupe p-saturé et* H *un sous-groupe p-saturé de* G. *Alors le normalisateur* N *de* H *dans* G *est un sous-groupe p-saturé.*

Preuve. — Soit A la $\mathbf{Z}_p$-algèbre diagonale saturée $\operatorname{Sat}\mathbf{Z}_p[G]$ (3.2.5). Notons Log G (resp. Log H, Log N) l'ensemble des logarithmes des éléments de G (resp. de H, de N). D'après (3.2.4), Log G et Log H sont des $\mathbf{Z}_p$-algèbres de Lie complètes, *et l'algèbre des endomorphismes du module* Log H, *valuée comme en* (I, 2.2.4.1), *est saturée.*

Pour qu'un élément $x \in \operatorname{Log} G$ appartienne à Log N, il faut et il suffit, d'après (3.2.7), que Log H soit stable pour l'endomorphisme $\exp(\operatorname{ad} x)$. Comme l'algèbre des endomorphismes de Log H est saturée, cela équivaut à dire que Log H est stable pour l'endomorphisme ad x. Autrement dit, Log N est le normalisateur de la sous-algèbre Log H dans l'algèbre de Lie Log G. Notre proposition en résulte.

(3.3) Les foncteurs Sat et div dans la catégorie des groupes p-valués.

(3.3.1) *Définition du groupe saturé d'un groupe p-valué.* — Soit G un groupe p-valué (III, 2.1.2). Munissons l'algèbre $\mathbf{Z}_p[G]$ de la filtration induite (III, 2.3.3), et construisons l'algèbre diagonale saturée $\operatorname{Sat}\mathbf{Z}_p[G]$, comme en (1.2.7).

Nous appelons groupe saturé du groupe p-valué G, et nous notons Sat G le groupe

(3.3.1.1) $$\operatorname{Sat} G = \mathscr{G}^* \operatorname{Sat}\mathbf{Z}_p[G].$$

Nous *identifions* G au sous-groupe de Sat G qui lui est canoniquement isomorphe, et nous notons i_G l'injection canonique de G dans Sat G, qui est donc une *inclusion.*

(3.3.2) *Propriétés du foncteur* Sat.

(3.3.2.1) *Pour tout groupe p-valué* G, *le groupe* Sat G *est p-saturé, et l'inclusion* $i_G : G \to \operatorname{Sat} G$ *est une isométrie.*

C'est une conséquence de (III, 2.3.3) et de (1.3.5.3).

(3.3.2.2) *Si le groupe* G *est p-saturé, alors* $\operatorname{Sat} G = G$.

C'est la relation (3.2.5.1).

(3.3.2.3) *Soit* $f : G \to H$ *un morphisme de groupes p-valués. Alors* f *se prolonge en un morphisme* $\operatorname{Sat} f : \operatorname{Sat} G \to \operatorname{Sat} H$, *qui achève de définir le foncteur* Sat *dans la catégorie des groupes p-valués.*

En effet, f se prolonge en un morphisme des algèbres de groupes : $\mathbf{Z}_p[G] \to \mathbf{Z}_p[H]$, d'après (III, 2.3.1.3), puis en un morphisme d'algèbres diagonales saturées (I, 2.2.11) : $\operatorname{Sat}\mathbf{Z}_p[G] \to \operatorname{Sat}\mathbf{Z}_p[H]$, dont la restriction à Sat G donne (1.3.2.3) le morphisme cherché $\operatorname{Sat} f : \operatorname{Sat} G \to \operatorname{Sat} H$. La relation « Sat f prolonge f » s'écrit encore $i_H \circ f = \operatorname{Sat} f \circ i_G$.

(3.3.2.4) *Soient* G *un groupe p-valué,* H *un groupe p-saturé, et* $f : G \to H$ *un morphisme. Alors il existe un morphisme* $g : \operatorname{Sat} G \to H$, *et un seul, qui prolonge* f.

Nous venons de voir (3.3.2.3) la relation $i_H \circ f = \operatorname{Sat} f \circ i_G$, qui se réduit à $f = \operatorname{Sat} f \circ i_G$ puisque i_H est l'identité sur H (3.3.2.2). D'autre part, si $g : \operatorname{Sat} G \to H$ est un morphisme vérifiant $f = g \circ i_G$, nous en déduisons $\operatorname{Sat} f = \operatorname{Sat} g \circ \operatorname{Sat} i_G$, c'est-à-dire $\operatorname{Sat} f = g$.

La propriété (3.3.2.4) *définit* le foncteur Sat comme solution d'un problème d'application universelle.

(3.3.2.5) *Si* $f : \mathrm{G} \to \mathrm{H}$ *est une isométrie de groupes p-valués, alors* $\mathrm{Sat} f : \mathrm{Sat}\,\mathrm{G} \to \mathrm{Sat}\,\mathrm{H}$ *est une isométrie.*

C'est une conséquence de (III, 2.3.5) et de (I, 2.2.11).

(3.3.3) *Proposition. — Soit* H *un sous-groupe du groupe p-valué* G, *muni de sa filtration induite. Alors* Sat H *s'identifie à un sous-groupe de* Sat G. *Si* H *est distingué dans* G, Sat H *est distingué dans* Sat G.

Preuve. — La première assertion équivaut à la propriété (3.3.2.5). Supposons donc H distingué dans G, et soit $x \in \mathrm{G}$. Notons f l'automorphisme intérieur de G associé à x, et g la restriction de f à H, considérée comme application dans H. Alors Sat f est l'automorphisme intérieur de Sat G défini par x; la restriction de Sat f à Sat H et la composée de Sat g avec l'inclusion de Sat H dans Sat G coïncident, d'après (3.3.2.4). Il en résulte que l'élément x *normalise le sous-groupe* Sat H. Or le *normalisateur* de Sat H dans Sat G est *p-saturé*, d'après (3.2.8). Comme il contient G, c'est le groupe Sat G, d'après (3.3.2.4).

(3.3.4) *Définition du foncteur* div *dans la catégorie des groupes p-valués. — Soit* G *un groupe p-valué. Nous notons* div G *l'intersection des sous-groupes p-divisibles* (III, 2.1.5) *de* Sat G *qui contiennent* G.

Le sous-groupe div G est p-divisible.

Si $f : \mathrm{G} \to \mathrm{H}$ est un morphisme de groupes p-valués, alors l'image réciproque du sous-groupe div H par le morphisme Sat f (3.3.2.3) est un sous-groupe p-divisible de Sat G. Il existe donc un morphisme $\mathrm{div} f : \mathrm{div}\,\mathrm{G} \to \mathrm{div}\,\mathrm{H}$, dont le prolongement est Sat f.

(3.3.5) *Propriété du foncteur* div; *remarques.* — Le foncteur div possède toutes les propriétés analogues à celles du foncteur Sat énoncées en (3.3.2). Le groupe div G est une *extension p-divisible* du groupe p-valué G; si f est un *morphisme* de G *dans un groupe p-divisible* H, *alors il existe un morphisme unique* $g : \mathrm{div}\,\mathrm{G} \to \mathrm{H}$ *qui prolonge* f. Si $f : \mathrm{G} \to \mathrm{H}$ est un *isométrie* de groupes p-valués, alors div f est une *isométrie.*

Le groupe div G *est dense dans* Sat G (III, 2.1.7) et, par conséquent, nous obtenons Sat G en complétant div G.

Contrairement au cas des modules (I, 2.2), nous avons construit le foncteur Sat avant le foncteur div dans la catégorie des groupes p-valués.

J'ignore si les propositions (3.2.8) et (3.3.3) restent valables quand on y remplace « saturé » par « divisible » et Sat par div.

(3.3.6) *Lemme. — Soit* G *un groupe p-valué complet admettant la base ordonnée* $(x_i)_{i \in \mathrm{I}}$ (III, 2.2.4). *Alors le groupe* Sat G *admet la base ordonnée* $(\overline{x}_i)_{i \in \mathrm{I}}$, *où les* $\overline{x}_i$ *sont reliés aux* x_i *par des relations*

(3.3.6.1) $$x_i = \overline{x}_i^{\,p^{h_i}} \quad (h_i \in \mathbf{N},\ i \in \mathrm{I}).$$

Si le groupe G *est p-saturé, les éléments* $(\mathrm{Log}\, x_i)_{i\in \mathrm{I}}$ *constituent une base topologique de la* $\mathbf{Z}_p$*-algèbre de Lie valuée* $\mathscr{L}^*\,\mathrm{Sat}\,\mathbf{Z}_p[\mathrm{G}]$.

Preuve. — Nous procédons comme en (3.1.6). Notons A l'algèbre diagonale saturée $\mathrm{Sat}\,\mathbf{Z}_p[\mathrm{G}]$ et B l'adhérence de $\mathbf{Z}_p[\mathrm{G}]$ dans A, c'est-à-dire l'algèbre complétée de $\mathbf{Z}_p[\mathrm{G}]$. Posons $\mathrm{J}=\mathbf{N}^{(\mathrm{I})}$, $\tau_i=\omega(x_i)$, $\tau\alpha=\sum_{i\in\mathrm{I}}\tau_i\alpha_i$ pour $\alpha\in\mathrm{J}$.

Notons, pour $\alpha\in\mathrm{J}$, z^α le produit ordonné $z^\alpha=\prod_{i\in\mathrm{I}}(x_i-1)^{\alpha_i}$.

(3.3.6.2) *La famille* $(z^\alpha)_{\alpha\in\mathrm{J}}$ *est une base topologique de* B, *avec* $w(z^\alpha)=\tau\alpha$.

En effet les (z^α) forment une famille filtrée-libre d'après le théorème (III, 2.3.3), et le sous-module complet-libre engendré par les z^α dans B contient G, donc coïncide avec B.

Nous obtenons une base topologique de A en divisant les z^α par des puissances convenables de p, mais nous préférons écrire les éléments de A comme des séries

$$\sum_{\alpha\in\mathrm{J}}\lambda_\alpha z^\alpha=y, \tag{3.3.6.3}$$

où $\lambda_\alpha\in\mathbf{Q}_p$ et $v(\lambda_\alpha)+\tau\alpha\geqslant 0$ pour tout $\alpha\in\mathrm{J}$; $v(\lambda_\alpha)+\tau\alpha$ tend vers l'infini (suivant le filtre des complémentaires des parties finies de J), et

$$w(y)=\inf_{\alpha\in\mathrm{J}}(v(\lambda_\alpha)+\tau\alpha). \tag{3.3.6.4}$$

L'application diagonale Δ *est définie par les formules*

$$\Delta z^\alpha=\sum_{\beta,\gamma}\frac{\alpha!}{(\alpha-\beta)!\,(\alpha-\gamma)!\,(\beta+\gamma-\alpha)!}z^\beta\otimes z^\gamma \tag{3.3.6.5}$$

où la sommation est étendue aux couples β, γ d'éléments de J vérifiant

$$\beta\leqslant\alpha,\qquad \gamma\leqslant\alpha,\qquad \beta+\gamma\geqslant\alpha. \tag{3.3.6.6}$$

Ces formules résultent de l'identité

$$(x+y+xy)^n=\sum_{i,j}\frac{n!}{(n-i)!\,(n-j)!\,(i+j-n)!}x^iy^j. \tag{3.3.6.7}$$

Pour que l'élément y de (3.3.6.3) appartienne à $\mathscr{G}$A, il faut et il suffit que $\lambda_0=1$, et que

$$\lambda_\beta\lambda_\gamma-\sum_\alpha\frac{\alpha!}{(\alpha-\beta)!\,(\alpha-\gamma)!\,(\beta+\gamma-\alpha)!}\lambda_\alpha=0 \tag{3.3.6.8}$$

pour tous $\beta,\gamma\in\mathrm{J}$, la sommation s'étendant aux $\alpha\in\mathrm{J}$ vérifiant (3.3.6.6).

Les équations (3.3.6.8) montrent que les λ_α sont déterminés, quand on connaît les $\lambda_{\delta_i}=\lambda_i$ (puisque $\lambda_0=1$), par les formules

$$\lambda_\alpha=\binom{\lambda}{\alpha}=\prod_{i\in\mathrm{I}}\binom{\lambda_i}{\alpha_i}. \tag{3.3.6.9}$$

Nous sommes ramenés au cas élémentaire où G *est isomorphe* (comme groupe abstrait) *au groupe additif* $\mathbf{Z}_p$.

Pour chaque $i \in \mathrm{I}$, nous déterminons l'entier h_i par la relation

(3.3.6.10) $$(p-1)^{-1} < \tau_i - h_i \leqslant p(p-1)^{-1}.$$

Les éléments $\overline{x}_i$ sont alors bien déterminés dans $\mathscr{G}^*\mathrm{A}$ par la relation (3.3.6.1). Pour que l'élément $y \in \mathrm{A}$ donné par (3.3.6.3) appartienne à $\mathscr{G}\mathrm{A} = \mathscr{G}^*\mathrm{A}$, il faut et il suffit que les λ_α soient donnés par (3.3.6.9), où les $\lambda_i \in \mathbf{Q}_p$ doivent vérifier

(3.3.6.11) $$v(\lambda_i) + h_i \geqslant 0 \qquad \textit{pour tout } i \in \mathrm{I}.$$

L'élément y est alors égal au produit ordonné

(3.3.6.12) $$y = \prod_{i \in \mathrm{I}} \overline{x}_i^{\nu_i}, \qquad \textit{où } \nu_i = p^{h_i}\lambda_i,\ i \in \mathrm{I}.$$

Si le groupe G est p-saturé, nous avons $\overline{x}_i = x_i$ pour tout $i \in \mathrm{I}$.

Dans le cas général, les éléments de $\mathscr{L}\mathrm{A}$ sont les éléments y de la forme (3.3.6.3), où les λ_α satisfont aux équations $\lambda_0 = 0$ et

(3.3.6.13) $$\sum_\alpha \frac{\alpha!}{(\alpha-\beta)!\,(\alpha-\gamma)!\,(\beta+\gamma-\alpha)!}\lambda_\alpha = 0$$

pour tous les couples $\beta, \gamma \in \mathrm{J}$ *tels que* $\beta > 0$, $\gamma > 0$, l'indice de sommation $\alpha \in \mathrm{J}$ vérifiant (3.3.6.6). Ces équations entraînent $\lambda_\alpha = 0$ si α n'est pas de la forme $n\delta_i$ $(n \in \mathbf{N},\ i \in \mathrm{I})$. Nous sommes encore ramenés au groupe de dimension 1, où nous prouvons la dernière assertion du lemme.

(3.4) Groupes p-valués de rang fini ; remarques et exemples.

(3.4.1) *Théorème. — Soit* G *un groupe p-valué complet de rang fini r. Alors le groupe saturé* Sat G *a le même rang r. Si x est un élément de* Sat G, x^{p^n} *appartient à* G *dès que l'entier n est assez grand. Le groupe divisé* div G *coïncide avec* Sat G. *Le groupe* G *est ouvert dans* Sat G.

Preuve. — Le groupe G possède une base ordonnée $(x_i)_{1 \leqslant i \leqslant r}$ (III, 2.2.5). Notre théorème est alors une conséquence du lemme (3.3.6). Celui-ci nous donne même un énoncé plus précis : nous obtenons une base ordonnée $(\overline{x}_i)$ en prenant respectivement des racines p^{h_i}-ièmes des x_i, les entiers h_i étant déterminés à partir des relations $(p-1)^{-1} < \omega(\overline{x}_i) \leqslant p(p-1)^{-1}$.

(3.4.2) *Quotients sans torsion de groupes p-valuables : preuve de* (III, 3.1.7.6). — Soit H un sous-groupe fermé distingué du groupe p-valuable G tel que le quotient G/H soit sans torsion. Choisissons une p-valuation ω de G, qui devient ainsi un groupe p-valué de rang fini r.

Construisons le groupe saturé Sat G, dont Sat H est un sous-groupe *distingué*, d'après la proposition (3.3.3). Le groupe Sat G est encore de rang r (3.4.1).

Le groupe quotient Sat G/Sat H est *sans torsion*, puisque Sat H est saturé, et nous avons prouvé (III, 3.3.2.4) que le groupe Sat G/Sat H est *p-saturé pour la filtration quotient de* Sat G.

Or nous avons $(\mathrm{Sat}\, H) \cap G = H$, d'après (3.4.1), puisque G/H est sans torsion. Le groupe G/H est donc isomorphe au groupe *p-valué de rang fini* $(G.\mathrm{Sat}\, H)/\mathrm{Sat}\, H$.

(3.4.3) *Valuations rationnelles : preuve de* (III, 3.1.11). — Soit G un groupe p-valuable. Choisissons une p-valuation ω de G, qui devient donc p-valué de rang r. Construisons le groupe $\mathrm{Sat}\, G = H$, qui est p-saturé de rang r. Nous allons prouver que H peut être muni d'une *p-valuation à valeurs rationnelles*. La même propriété vaudra pour son sous-groupe G.

D'après le transport de structures (3.2.6), il revient au même de démontrer que la $\mathbf{Z}_p$-algèbre de Lie L associée à H (et que nous pouvons écrire Log H dans l'algèbre diagonale saturée $\mathrm{Sat}\, \mathbf{Z}_p[H]$) admet une valuation à valeurs rationnelles. L'algèbre de Lie L est de rang r sur $\mathbf{Z}_p$ (3.3.6). Soit $(x_i)_{1 \leqslant i \leqslant r}$ une base filtrée de L. Le crochet de Lie est donné par les constantes de structure $c_{ijk} \in \mathbf{Z}_p$:

(3.4.3.1) $$[x_i, x_j] = \sum_{1 \leqslant k \leqslant r} c_{ijk} x_k,$$

et les valuations $\tau_i = w(x_i)$ vérifient les inégalités

(3.4.3.2) $$\tau_i + \tau_j \leqslant v(c_{ijk}) + \tau_k,$$

pour tous i, j, k.

Réciproquement, si les τ_i sont r nombres $\geqslant 0$ vérifiant les r^3 inégalités (3.4.3.2), ils définissent une valuation de la $\mathbf{Z}_p$-algèbre L (I, 3.3.6). Cette algèbre de Lie devient, par transport de structure, un groupe p-saturé, pourvu que les τ_i vérifient en outre les r inégalités

(3.4.3.3) $$(p-1)^{-1} < \tau_i \leqslant p(p-1)^{-1}.$$

Les relations (3.4.3.2) et (3.4.3.3) constituent une *famille finie d'inégalités en les* τ_i, *à coefficients rationnels*. Si cette famille admet une *solution réelle*, elle admet une *solution rationnelle* [33]. Cela prouve notre assertion.

(3.4.4) *Structures d'algèbres de Lie sur les groupes p-saturables ; coordonnées « de première espèce ».* — Soit G un groupe p-saturé. Nous avons une structure d'algèbre de Lie sur G, définie par transport de structure (3.2.5). Les formules (3.2.3.1) et (3.2.3.2) qui définissent la somme et le crochet ne font intervenir que la *structure de groupe topologique de* G.

Un groupe *p-saturable* G (III, 3.1.6) possède donc une structure d'algèbre de Lie sur $\mathbf{Z}_p$. Notons L^* la $\mathbf{Z}_p$-algèbre de Lie ainsi associée à G. Le rang de G est égal au rang du $\mathbf{Z}_p$-module libre L^* (3.3.6). Or un $\mathbf{Z}_p$-module libre de rang r possède une structure de *variété analytique taylorienne de type* $\mathbf{Z}_p^r$: le choix d'une base définit une identification à $\mathbf{Z}_p^r$, et les fonctions de passage sont linéaires, donc analytiques tayloriennes.

Nous avons ainsi *deux structures de variété analytique taylorienne* sur le groupe p-saturable G : celle définie en (III, 3.3.2) au moyen des coordonnées « de seconde espèce », et celle définie au moyen de coordonnées par rapport à une base de L^* (identifié à G) qu'on appelle encore « *coordonnées de première espèce* ». *Ces deux structures de variété analytique taylorienne coïncident : les coordonnées de première (resp. de seconde) espèce sont fonctions analytiques tayloriennes des coordonnées de seconde (resp. première) espèce.*

(3.4.5) *Preuve de* (3.4.4). — Énonçons d'abord une généralisation de la formule de Hausdorff (3.2.2). Soit r un entier naturel; posons $J=\mathbf{N}^r$. Nous avons une identité

$$\text{(3.4.5.1)}\qquad \operatorname{Log}(\exp x_1)\ldots(\exp x_r)=\sum_{\alpha\in J}u_\alpha(x_1,\ \ldots,\ x_r),$$

où les $u_\alpha(x_1,\ \ldots,\ x_r)$ *sont des polynômes de Lie à coefficients rationnels, homogènes de multidegrés respectifs* α *en* $(x_1,\ \ldots,\ x_r)$. *Si nous posons*

$$\text{(3.4.5.2)}\qquad h_\alpha=[(|\alpha|-1)(p-1)^{-1}]$$

les polynômes de Lie $p^{h_\alpha}u_\alpha(x_1,\ \ldots,\ x_n)$ *sont à coefficients p-entiers.*

La relation (3.4.5.1) peut être considérée comme une égalité dans l'algèbre de Magnus engendrée par les x_i sur $\mathbf{Q}$, mais la formule (3.4.5.1) est encore valable quand on y remplace les x_i par des éléments de $\mathscr{L}^*A$ (A désignant une algèbre diagonale saturée); les $u_\alpha(x_1,\ \ldots,\ x_n)$ représentent alors des éléments de $\mathscr{L}^*A$.

Ces assertions s'établissent soit par récurrence sur r à partir du théorème (3.2.2), soit directement comme ce théorème.

Prenons un groupe G, p-saturé de rang r. Notons A l'algèbre diagonale saturée $\operatorname{Sat}\mathbf{Z}_p[G]$ et L (resp. L^*) l'algèbre de Lie $\mathscr{L}A$ (resp. $\mathscr{L}^*A$). Choisissons une base filtrée $(x_i)_{1\leqslant i\leqslant r}$ de L^*. Les éléments $u_\alpha(x_1,\ \ldots,\ x_n)$ appartiennent à L^* et tendent vers zéro. Nous avons des formules

$$\text{(3.4.5.3)}\qquad u_\alpha(x_1,\ \ldots,\ x_n)=\sum_{1\leqslant i\leqslant r}d_{i,\alpha}x_i,$$

où les coefficients $d_{i,\alpha}$ appartiennent à $\mathbf{Z}_p$ et tendent vers zéro (selon le filtre des complémentaires des parties finies de J).

Les éléments $(\exp x_i)_{1\leqslant i\leqslant r}$ constituent une base ordonnée du groupe G, d'après (3.1.6). L'élément x dont les coordonnées de second espèce par rapport à cette base sont $(\lambda_1,\ \ldots,\ \lambda_r)\in\mathbf{Z}_p^r$ est

$$\text{(3.4.5.4)}\qquad x=\prod_{1\leqslant i\leqslant r}(\exp\lambda_i x_i).$$

Nous avons, d'après (3.4.5.1),

$$\text{(3.4.5.5)}\qquad \operatorname{Log}x=\sum_{\alpha\in J}\lambda^\alpha u_\alpha(x_1,\ \ldots,\ x_n).$$

Les coordonnées de première espèce $(\mu_1,\ \ldots,\ \mu_r)$ de l'élément $x\in G$ sont définies par la relation

$$\text{(3.4.5.6)}\qquad \operatorname{Log}x=\sum_{1\leqslant i\leqslant r}\mu_i x_i.$$

Nous obtenons ainsi

$$\text{(3.4.5.7)}\qquad \mu_i=\sum_{\alpha\in J}\lambda^\alpha d_{i,\alpha},\qquad \textit{pour}\ 1\leqslant i\leqslant r.$$

Ces dernières formules signifient que μ *est fonction analytique taylorienne de* λ.

Prouvons maintenant que λ *est fonction analytique taylorienne de* μ.

Nous procédons comme pour le lemme (III, 3.3.1). Posons, pour $\alpha \in \mathrm{J}$,

$$z^\alpha = \prod_{1 \leqslant i \leqslant r} (\exp x_i - 1)^{\alpha_i}.$$

Nous avons

$$x = \sum_{\alpha \in \mathrm{J}} \binom{\lambda}{\alpha} z^\alpha, \tag{3.4.5.8}$$

et

$$x = \exp(\sum_i \mu_i x_i) = \sum_{n \in \mathbf{N}} (n!)^{-1} (\sum_i \mu_i x_i)^n. \tag{3.4.5.9}$$

Pour chaque $n \in \mathbf{N}$, posons

$$(n!)^{-1} (\sum_{1 \leqslant i \leqslant r} \mu_i x_i)^n = \sum_{|\beta| = n} \mu^\beta y_\beta, \tag{3.4.5.10}$$

où les éléments $y_\beta \in \mathrm{A}$ vérifient les relations

$$w(y_\beta) \geqslant |\beta| t - v(|\beta|!), \tag{3.4.5.11}$$

t désignant le plus petit des nombres $w(x_i)$. Comme les z^α, divisés par des puissances convenables de p, constituent une base topologique de A, nous avons

$$y_\beta = \sum_{\alpha \in \mathrm{J}} d'_{\alpha, \beta} z^\alpha, \tag{3.4.5.12}$$

avec $d'_{\alpha, \beta} \in \mathbf{Q}_p$ (α, $\beta \in \mathrm{J}$), et

$$v(d'_{\alpha, \beta}) + w(z^\alpha) \geqslant w(y_\beta). \tag{3.4.5.13}$$

Nous parvenons ainsi aux relations

$$\binom{\lambda}{\alpha} = \sum_{\beta \in \mathrm{J}} \mu^\beta d'_{\alpha, \beta}, \tag{3.4.5.14}$$

pour $\alpha \in \mathrm{J}$. Si $\alpha = \delta_i$, $\binom{\lambda}{\alpha}$ se réduit à λ_i, et nous avons, en posant $d'_{\delta_i, \beta} = d'_{i, \beta}$:

$$\lambda_i = \sum_{\beta \in \mathrm{J}} \mu^\beta d'_{i, \beta}. \tag{3.4.5.15}$$

Nous obtenons, à partir de (3.4.5.11), (3.4.5.13) et des relations $w(x_i) \leqslant p(p-1)^{-1}$, les inégalités

$$v(d'_{i, \beta}) \geqslant |\beta| (t - (p-1)^{-1}) + (p-1)^{-1} (\mathrm{Schiff}\, |\beta| - 1) - 1. \tag{3.4.5.16}$$

La preuve s'achève comme en (III, 3.3.1).

(3.4.6) *Les grands corps gauches.* — Rappelons ([13], théorème 6, p. 166) que l'algèbre enveloppante UL d'une algèbre de Lie L de dimension finie sur un corps possède un *corps des fractions à gauche* (ou à droite).

Le même résultat vaut pour une $\mathbf{Z}_p$-*algèbre de Lie* L *valuée de rang fini*. De plus, la *valuation* de l'algèbre UL (2.2.5) se prolonge au corps des fractions de UL (I, 2.2.5).

Nous obtenons ainsi un *corps gauche valué* K (commutatif si et seulement si L est abélienne). Le corps K contient l'algèbre divisée div UL. Si nous complétons le corps K pour la structure uniforme associée à sa valuation, nous obtenons le corps gauche $\hat{K}$, qui contient comme sous-algèbre valuée le complété Sat UL de div UL.

Soit maintenant G un groupe p-valué de rang fini. Nous construisons (1.2.7) l'algèbre diagonale saturée $\mathrm{Sat}\,\mathbf{Z}_p[G]=A$, et nous prenons l'algèbre de Lie $L=\mathscr{L}A$. C'est une $\mathbf{Z}_p$-algèbre valuée de rang fini (3.3.6), et Sat UL s'identifie à A (3.2.5). Le corps $\hat{K}$ construit à partir de L est dit le *grand corps gauche* associé à G. Il contient la $\mathbf{Z}_p$-algèbre $\mathrm{Sat}\,\mathbf{Z}_p[G]$, et c'est un *foncteur covariant* en G.

(3.4.7) *L'extension p-saturable minima d'un groupe p-valuable.* — Soit G un groupe p-valuable (III, 3.1.6). Pour chaque p-valuation ω le groupe G est complet et de rang fini r (III, 3.1.9); il lui correspond alors un groupe p-saturé que nous notons $\mathrm{Sat}_\omega G$, qui est de rang r (3.4.1). L'indice $(\mathrm{Sat}_\omega G : G)$ est donc fini.

Le groupe $\mathrm{Sat}_\omega G$ dépend en général du choix de la p-valuation ω, comme on le voit sur l'exemple du groupe $\mathbf{Z}_p$.

Si ω et ω' sont deux p-valuations de G, telles que

(3.4.7.1) $$\omega(x)\leqslant\omega'(x) \quad \text{pour chaque } x\in G,$$

alors l'application identique de G se prolonge en un morphisme

(3.4.7.2) $$\mathrm{Sat}_\omega G \to \mathrm{Sat}_{\omega'} G,$$

qui est *injectif*, d'après (3.4.1).

Convenons de dire qu'*une p-valuation du groupe* G *est minimisante si l'entier* $(\mathrm{Sat}_\omega G : G)$ *a sa valeur minima* (*pour toutes les p-valuations de* G).

Soient ω une p-valuation minimisante et ω' une p-valuation de G. Notons ω'' la borne inférieure de ω et ω'; c'est encore une p-valuation de G. Nous avons alors deux morphismes canoniques :

(3.4.7.3) $$\mathrm{Sat}_{\omega''} G \to \mathrm{Sat}_\omega G$$

(3.4.7.4) $$\mathrm{Sat}_{\omega''} G \to \mathrm{Sat}_{\omega'} G.$$

Le premier est *bijectif* (puisque ω est minimisante); le second est injectif. Nous pouvons ainsi définir le *morphisme injectif* (3.4.7.2), *sans supposer que* $\omega\leqslant\omega'$. Le groupe $\mathrm{Sat}_\omega G$ est, au sens qui vient d'être précisé, *le plus petit groupe p-saturable contenant* G. Rappelons (III, 3.1.12) que la borne inférieure des p-valuations de G *n'est pas* une p-valuation (sauf si G se réduit à l'élément neutre).

(3.4.8) *Groupes et algèbres de Lie transportables ; exercice.* — Soit G un *groupe p-valuable.* Choisissons une p-valuation ω de G et construisons la $\mathbf{Z}_p$-algèbre diagonale saturée $A=\mathrm{Sat}\,\mathbf{Z}_p[G]$ (1.2.7). La propriété suivante

(3.4.8.1) « *l'ensemble* Log G *des éléments de la forme* $\mathrm{Log}\,x$, $x\in G$, *est une sous-algèbre de Lie de* $\mathscr{L}^*A$ »

est *indépendante du choix de la p-valuation* ω. Nous dirons que le groupe G est *transportable* s'il possède la propriété (3.4.8.1) et nous dirons qu'une $\mathbf{Z}_p$-algèbre de Lie est *transportable* si elle s'obtient sous la forme Log G, où G est transportable.

Toute la théorie du transport dė structures (3.2) vaut pour les groupes et algèbres de Lie transportables.

Le groupe p-valuable étudié en (III, 3.2.4) n'est pas transportable pour $p=2$.

Voici un exemple d'algèbre de Lie transportable dont le groupe associé n'est pas saturable.

Soit $p=3$. Construisons une $\mathbf{Z}_3$-algèbre de Lie M, libre pour les générateurs x, y, z. Munissons M de sa graduation naturelle (les générateurs ont le degré 1). Formons l'idéal I de M engendré par les éléments suivants :

(3.4.8.2) tous les éléments de degré >3;

(3.4.8.3) les 6 éléments déduits de $[[x,y],y]$ par permutation des générateurs x, y, z;

(3.4.8.4) l'élément $[[x,y],z]+[[x,z],y]$.

L'algèbre quotient $L=M/I$ *est transportable.* Cependant L ne correspond pas à un groupe 3-saturable puisque l'image de $[[x,y],z]$ n'y est pas divisible par 3.

(3.4.9) *Valuation de* $\mathfrak{sl}_2(\mathbf{Z}_2)$; *exercice.* — Pour tout anneau commutatif Ω, l'algèbre de Lie $\mathfrak{sl}_2(\Omega)$ des matrices 2×2 de trace nulle à coefficients dans Ω admet la base $\{X, Y, H\}$, où

(3.4.9.1) $$X=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \quad Y=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \quad H=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Les crochets se calculent par les formules

(3.4.9.2) $$[H, X]=2X; \quad [H, Y]=-2X; \quad [X, Y]=H.$$

Nous avons repris les notations de [2], exemple, p. 85.

Prenons désormais $\Omega=\mathbf{Z}_2$; notons L^0 l'algèbre de Lie $\mathfrak{sl}_2(\mathbf{Z}_2)$ et A l'algèbre de matrices $M_2(\mathbf{Z}_2)$.

D'après (I, 3.3.6), les formules (3.4.9.2) montrent l'existence d'une *valuation* w *de* L^0 pour laquelle $\{X, Y, H\}$ est une *base filtrée*, avec

(3.4.9.3) $$w(X)=w(Y)=\frac{1}{2}; \quad w(H)=1.$$

Cette valuation w peut encore être définie comme la borne inférieure des filtrations d'algèbre de L^0 vérifiant $w(x)\geqslant\frac{1}{2}$ pour tout $x\in L^0$. *Elle est donc invariante par chaque automorphisme de* L^0.

Nous notons L l'algèbre de Lie divisée (ou saturée) de L^0 pour la valuation w. Cette algèbre a comme base filtrée les éléments X, Y et $\frac{1}{2}$H.

Nous notons L^* l'ensemble des éléments de L de valuation >1. Cette algèbre a comme base les éléments 2X, 2Y, 2H, si bien que $L^*=2L^0$.

Notons $\mathscr{A}$ l'algèbre associative des *endomorphismes du module valué* L. L'algèbre $\mathscr{A}$, valuée comme en (I, 2.2.4) est saturée.

(3.4.9.4) *L'application* $\mathrm{ad}: L \to \mathscr{A}$ *qui associe à* $x \in L$ *la dérivation intérieure* $\mathrm{ad}\, x$ *est une isométrie, et un morphisme d'algèbres de Lie* (pour le crochet $[a,b]=ab-ba$ de $\mathscr{A}$).

Nous notons Γ le groupe des automorphismes de L ($\Gamma \subset \mathscr{A}$), et Γ^* le sous-groupe de Γ formé des $u \in \Gamma$ vérifiant $w(\mathscr{A}; u-1) > 1$.

(3.4.9.5) *A chaque* $x \in L^*$ *nous associons l'automorphisme* $\exp(\mathrm{ad}\, x) \in \Gamma^*$. *L'image de* L^* *par l'application* $\exp \mathrm{ad}: L^* \to \Gamma^*$ *est un sous-groupe de* Γ^*, d'après (3.2.2).

(3.4.9.6) *En fait,* $\Gamma^* = \exp \mathrm{ad}\, L^*$, *car, si* $u \in \Gamma^*$, $\mathrm{Log}\, u \in \mathscr{A}$ *est une dérivation de* L, *donc une dérivation intérieure* $\mathrm{ad}\, x$, $x \in L^*$, d'après [2], corollaire 3, p. 73 et (3.4.9.5).

(3.4.10) *Les groupes* $GL_2(\mathbf{Z}_2)$ *et* $SL_2(\mathbf{Z}_2)$; *exercice.* — Conservons les notations de (3.4.9). Notons G le groupe $GL_2(\mathbf{Z}_2)$ et $S = SL_2(\mathbf{Z}_2)$ son sous-groupe des éléments de déterminant 1.

Le centre C de G est formé des matrices scalaires, et l'intersection $S \cap C$ se réduit au groupe $\{\pm 1\}$.

Pour $n \in \mathbf{N}^*$, notons G_n le *sous-groupe de congruence* de G (cf. III, 3.2.7) défini par

(3.4.10.1) $$x \in G_n \Leftrightarrow x \in A \text{ et } x - 1 \in 2^n . A.$$

Posons $S_n = S \cap G_n$ et $C_n = C \cap G_n$. Nous avons $C = C_1$, et la décomposition classique en produit direct : $C = \{\pm 1\} \times C_2$; le groupe multiplicatif C_2 est isomorphe au groupe additif $\mathbf{Z}_2$.

A chaque $x \in G$ correspond un automorphisme intérieur $y \mapsto xyz^{-1}$ de l'algèbre A. Cet automorphisme conserve l'algèbre de Lie L^0 et se prolonge donc en un automorphisme de l'algèbre de Lie L.

Nous obtenons ainsi un homomorphisme

(3.4.10.2) $$F: G \to \Gamma$$

de G dans le groupe des automorphismes de L. *Le noyau de* F *est le centre* C *de* G, si bien que l'image est isomorphe au groupe projectif, $G/C = PGL_2(\mathbf{Z}_2)$. L'homomorphisme F est *surjectif* (nous n'utiliserons pas cette propriété).

Les considérations de (III, 3.2.6) s'appliquent à l'algèbre A. Comme la formule

(3.4.10.3) $$\det \exp x = \exp \mathrm{Tr}\, x$$

est valable pour tout $x \in 4A$ et que l'application exponentielle est injective, nous parvenons au résultat suivant.

(3.4.10.4) *Les éléments de* G_2 (resp. de S_2) *s'obtiennent univoquement sous la forme* $\exp(4x)$, *où* $x \in A$ (resp. $x \in L^0$).

Pour $x \in A$, convenons de noter $\mathrm{ad}\, x$ l'application $y \mapsto [x,y]$, où $y \in L$, si bien que $\mathrm{ad}\, x \in \mathscr{A}$.

Les considérations de (3.2.7) sont applicables, et nous donnent la formule

(3.4.10.5) $$F\exp(4x) = \exp \operatorname{ad}(4x), \quad \textit{pour tout } x \in A.$$

Une base sur $\mathbf{Z}_2$ du module A est constituée des trois éléments X, Y, H (3.4.9.1), et de l'élément $\frac{1}{2}(H+1) = Z$. Nous avons $\operatorname{ad} Z = \frac{1}{2} \operatorname{ad} H$, d'où (3.4.10.5) :

(3.4.10.6) $$F\exp(4Z) = \exp \operatorname{ad}(2H).$$

Remarquons que l'élément $\exp 2H$ *n'existe pas dans* A ; cette affirmation peut être précisée comme suit.

(3.4.10.7) *Le groupe* S *ne contient aucun élément x vérifiant* $F(x) = \exp \operatorname{ad}(2H)$.

En effet, l'entier 2-adique exp 4 n'est pas un carré dans $\mathbf{Z}_2$ (car $v((\exp 4) - 1) = 2$).

Par contre les éléments X et Y (3.4.9.1) vérifient $X^2 = Y^2 = 0$. Pour tout $\lambda \in \mathbf{Z}_2$, nous pouvons donc calculer $\exp(\lambda X) = 1 + \lambda X$ (resp. $\exp(\lambda Y) = 1 + \lambda Y$), et nous avons

(3.4.10.8) $$\begin{cases} F\exp(\lambda X) = \exp \operatorname{ad}(\lambda X), \\ F\exp(\lambda Y) = \exp \operatorname{ad}(\lambda Y). \end{cases}$$

Notons a et b les éléments

(3.4.10.9) $$\begin{cases} a = -(1 + 2X) = -\exp(2X); \\ b = -(1 + 2Y) = -\exp(2Y). \end{cases}$$

Nous avons $a, b \in S_1$, et $F(a) = \exp \operatorname{ad}(2X)$, $F(b) = \exp \operatorname{ad}(2Y)$.

Notons K *le sous-groupe de* G *engendré par* G_2, *a et b.*

(3.4.10.10) *Le sous-groupe* K *est distingué dans* G *et* $-1 \notin K$.

En effet, nous avons $G_1 \supset K \supset G_2$, et le groupe multiplicatif G_1/G_2 s'identifie au groupe additif de l'algèbre $\overline{A} = A/2A$: à un élément de G_1/G_2, représenté par $x \in G_1$, nous associons la classe de $\frac{1}{2}(x-1)$ modulo 2A. Les éléments de K/G_2 sont ainsi associés aux éléments $0, 1+X, 1+Y, X+Y$ de $\overline{A}$ (nous notons encore X et Y les matrices (3.4.9.1) à coefficients dans $\mathbf{F}_2$). Nous obtenons alors la définition suivante de K, qui montre son invariance dans G, et la relation $-1 \notin K$.

(3.4.10.11) $$x \in K \Leftrightarrow \begin{cases} x \in G_2 \quad \textit{ou} \\ x \notin G_2,\ x \in G_1,\ x - 3 \notin 4A \quad \textit{et} \quad (x-1)^2 - 4 \in 8A. \end{cases}$$

Le sous-groupe $\exp \operatorname{ad}(4L^0)$ de Γ^* admet comme base ordonnée les éléments $\exp \operatorname{ad}(4X)$, $\exp \operatorname{ad}(4Y)$ et $\exp \operatorname{ad}(8Z)$. Nous obtenons le groupe 2-saturé $\exp \operatorname{ad} L^*$ (qui est d'ailleurs égal à Γ^*, d'après (3.4.9.6)) en adjoignant à $\exp \operatorname{ad}(4L^0)$ des racines carrées des éléments de cette base ordonnée (3.4.1).

Comme le groupe K contient S_2, ainsi que les éléments $\exp(4Z)$, a et b, nous avons

(3.4.10.12) $$F(K) = \exp \operatorname{ad} L^* = \Gamma^*.$$

Le noyau de la restriction de F à K est C_2, d'après (3.4.10.10).

Notons U *le sous-groupe* $S \cap K$.

(3.4.10.13) *La restriction de l'homomorphisme* F *au sous-groupe* U *est injective. Celui-ci est donc isomorphe au groupe 2-valué* F(U), *qui est d'indice 2 dans* Γ^*. *Le groupe* U *n'est pas transportable, au sens de* (3.4.8).

Le groupe F(U) contient en effet $F(a)$, $F(b)$, $F(S_2)$, *mais non* exp ad(2H), d'après (3.4.10.7). Si le groupe U était transportable, nous pourrions appliquer la formule de Hausdorff à l'algèbre de Lie engendrée sur $\mathbf{Z}_2$ par les éléments 2X, 2Y et 4H, ce qui est impossible.

Le groupe G/G_1 est isomorphe à $GL_2(\mathbf{F}_2)$, donc au groupe symétrique $\mathfrak{S}_3$ (le groupe $GL_2(\mathbf{F}_2)$ permute de toutes les six manières possibles les trois vecteurs non nuls du plan $\mathbf{F}_2^2$).

Le groupe S/S_1 est canoniquement isomorphe à G/G_1. Le groupe S_1 est le produit direct $U \times \{\pm 1\}$.

Enfin, le groupe S/U est produit semi-direct d'un sous-groupe distingué cyclique d'ordre 3 par un sous-groupe (non distingué) cyclique d'ordre 4.

(3.4.11) *Remarques sur les groupes libres ; exercice.* — Soit $\mathscr{F}$ le groupe libre pour une famille de générateurs $(x_i)_{1 \leqslant i \leqslant r}$. Pour chaque nombre réel $t > (p-1)^{-1}$, la (t, p)-filtration fait de $\mathscr{F}$ un groupe p-valué (III, 3.2.5); notons $G(t)$ le saturé de $\mathscr{F}$ pour sa (t, p)-filtration (3.3.1). Pour tout couple t, t', avec

(3.4.11.1) $$(p-1)^{-1} < t \leqslant t'$$

nous avons un *homomorphisme continu*

(3.4.11.2) $$f_{t',t} : G(t) \to G(t')$$

qui prolonge l'identité sur $\mathscr{F}$. Ces homomorphismes sont *injectifs*, si bien que la limite projective

(3.4.11.3) $$G = \varprojlim G(t)$$

des $G(t)$ pour les morphismes $f_{t',t}$ est une simple intersection. Le groupe G, muni de sa topologie de limite projective, est *compact*, et les formules (3.2.3) permettent de définir sur lui une structure de $\mathbf{Z}_p$-algèbre de Lie compacte.

Le groupe G possède la propriété universelle suivante : il contient une famille d'éléments $(x_i)_{1 \leqslant i \leqslant r}$, et, pour tout groupe p-saturé H et toute famille $(y_i)_{1 \leqslant i \leqslant r}$ d'éléments de H, il existe un unique homomorphisme continu $f : G \to H$ qui vérifie $f(x_i) = y_i$ pour $1 \leqslant i \leqslant r$.

Cependant aucune filtration ne fait de G un groupe p-saturé si $r > 1$.

CHAPITRE V

COHOMOLOGIE

1. COMPLEXES STANDARD ET COHOMOLOGIE CONTINUE

(1.1) Complexes filtrés et cohomologie continue.

(1.1.1) *Complexes de modules gradués ou filtrés.* — Soit A un anneau. Nous appelons *complexe de* A-*modules* la donnée d'une famille $(X^n)_{n\in\mathbf{Z}}$ de A-modules et d'une *différentielle* d, c'est-à-dire une famille d'applications A-linéaires $d^n : X^n \to X^{n+1}$, vérifiant $d^{n+1} \circ d^n = 0$. Nous notons $X^\bullet$ un tel complexe.

Un morphisme de complexes $f : X^\bullet \to Y^\bullet$ est constitué par une famille d'applications A-linéaires $f^n : X^n \to Y^n$, telles que $d_Y^n \circ f^n = f^{n+1} \circ d_X^n$.

Si A est un anneau *gradué* (resp. *filtré*), nous définissons les complexes de A-modules *gradués* (resp. *filtrés*) et leurs *morphismes* en imposant que les applications A-linéaires d^n ou f^n soient des *morphismes* de A-*modules gradués* (resp. *filtrés*) tels que nous les avons définis en (I, 1.1.4) et (I, 2.1.4). Autrement dit, nous considérons les complexes *dans la catégorie des* A-*modules gradués* (resp. *filtrés*).

Un complexe de *chaînes*, ou complexe *à gauche*, est un complexe $X^\bullet$ tel que $X^n = 0$ pour $n > 0$. Nous posons alors, selon l'usage, $X_n = X^{-n}$, et nous écrivons $X_\bullet$ pour indiquer qu'il s'agit d'un complexe de chaînes.

Il est parfois plus commode de définir un complexe $X^\bullet$ comme la somme directe des X^n; la différentielle d devient un endomorphisme de carré nul.

(1.1.2) *Foncteurs de complexes filtrés.* — Soit $X^\bullet$ un complexe filtré sur l'anneau filtré A (1.1.1). Pour chaque $\nu \in \mathbf{R}_+$ et chaque $n \in \mathbf{N}$, la différentielle d^n applique X_ν^n (resp. $X_{\nu+}^n$) dans X_ν^{n+1} (resp. $X_{\nu+}^{n+1}$). Nous obtenons ainsi, par restriction, les complexes $X_\nu^\bullet$ (resp. $X_{\nu+}^\bullet$).

De même, quand nous prenons les gradués associés, nous obtenons le complexe gradué $\operatorname{gr} X^\bullet$ sur l'anneau $\operatorname{gr} A$; il est constitué par les modules $\operatorname{gr} X^n$ et les applications $\operatorname{gr} d^n$ (I, 2.3.5).

Nous nous intéresserons au cas où A est une algèbre valuée supplémentée (I, 2.2.4) sur un anneau de valuation discrète complet Ω (I, 3.1.1); nous pourrions même supposer que $\Omega = \mathbf{Z}_p$. Soit alors $X^\bullet$ un complexe de A-modules filtrés (1.1.1), valués en tant que Ω-modules.

Nous obtenons les *complexes* de A-*modules filtrés* $\hat{X}^\bullet$ (resp. div $X^\bullet$, Sat $X^\bullet$), en remplaçant chaque X^n par $\hat{X}^n$ (resp. div X^n, Sat X^n) et d^n par $\hat{d}^n$ (resp. div d^n, Sat d^n). Dans la construction du complexe divisé ou saturé, les X^n sont considérés d'abord comme des Ω-modules (I, 2.2.9 et 2.2.11); la définition de div et de Sat comme foncteurs additifs montre que les div X^n et Sat X^n ont des structures naturelles de A-modules filtrés.

(1.1.3) *Résolutions acycliques filtrées.* — Revenons au cas général où A est un anneau filtré quelconque. Tout A-module filtré M peut être considéré comme un complexe de chaînes $M_\bullet$, comme en [4], p. 75. Une résolution acyclique de M *(loc. cit.)* est constituée par un complexe de chaînes $X_\bullet$ et un morphisme de complexes $\varepsilon : X_\bullet \to M_\bullet$ qui induit des isomorphismes par passage à l'homologie.

Cette définition possède un sens dans la catégorie des complexes de A-modules filtrés, mais nous préférons la remplacer par la définition suivante.

(1.1.3.1) *Une résolution acyclique filtrée de* M *est constituée par un* A-*complexe de chaînes filtré* $X_\bullet$ *et un morphisme* $\varepsilon : X_\bullet \to M_\bullet$ *tels que, pour chaque* $\nu \in \mathbf{R}_+$, *le morphisme* $\varepsilon_\nu : X_{\bullet\nu} \to M_{\bullet\nu}$ *induise des isomorphismes par passage aux modules d'homologie.*

Autrement dit, pour chaque $\nu \in \mathbf{R}_+$, le sous-complexe $X_{\bullet\nu}$ doit être une résolution acyclique du sous-module M_ν, au sens de [4].

(1.1.3.2) *Proposition. — Si* $X_\bullet$ *est une résolution acyclique filtrée de* M, *alors le complexe* gr $X_\bullet$ *est une résolution acyclique graduée du* gr A-*module* gr M.

La preuve est analogue à celle du lemme (IV, 2.3.1).

(1.1.4) *Résolutions scindées.* — Soient A une algèbre filtrée sur l'anneau filtré Ω, et M un A-module filtré. Donnons-nous un complexe à gauche de A-modules filtrés $X_\bullet$ et un morphisme $\varepsilon : X_\bullet \to M_\bullet$. Cela revient (par un petit abus de notations) à se donner l'application $\varepsilon : X_0 \to M$, dite *augmentation* du complexe $X_\bullet$, qui doit vérifier la condition

(1.1.4.1) $$\varepsilon \circ d_1 = 0.$$

L'augmentation ε, ainsi que les différentielles d_n, sont des applications A-linéaires.

Une résolution scindée de M *par un complexe de* A-*modules filtrés* est constituée, en plus des données précédentes, par une *application* Ω-*linéaire*.

(1.1.4.2) $$\eta : M \to X_0,$$

et par une famille d'*applications* Ω-*linéaires*

(1.1.4.3) $$s_n : X_n \to X_{n+1} \quad (n \in \mathbf{Z}),$$

qui doivent être des *morphismes* de Ω-*modules filtrés*, et vérifier les relations suivantes

(1.1.4.4) $$\varepsilon \circ \eta(x) = x \qquad \textit{pour tout } x \in M.$$

(1.1.4.5) $$s_0 \circ \eta(x) = 0 \qquad \textit{pour tout } x \in M.$$

(1.1.4.6) $$(d_{n+1} \circ s_n + s_{n-1} \circ d_n)(x) = x \qquad \textit{pour tout } n \in \mathbf{N}^* \textit{ et tout } x \in X_n.$$

(1.1.4.7) $$d_1 \circ s_0(x) = x - (\eta \circ \varepsilon)(x) \qquad \textit{pour tout } x \in X_0.$$

L'application η est une *isométrie* de M sur un *sous-Ω-module* de X_0. Si nous identifions M à son image (ce que nous ferons dans le cas où A est une Ω-algèbre supplémentée et où $M=\Omega$), l'application ε devient un *projecteur* (Ω-linéaire) de X_0 sur son sous-Ω-module M. Si nous considérons $X_\bullet$ comme une somme directe des X_n, les propriétés de l'endomorphisme A-linéaire d et des endomorphismes Ω-linéaires s et ε s'expriment par les relations

(1.1.4.8) $$dd = d\varepsilon = \varepsilon d = s\varepsilon = \varepsilon s = \varepsilon(1-\varepsilon) = 0;$$

(1.1.4.9) $$ds + sd = 1 - \varepsilon.$$

Une résolution filtrée scindée est une résolution acyclique filtrée. — Cela résulte des propriétés des complexes de modules (non filtrés), et de ce que η et s sont des morphismes de modules filtrés.

Si $X_\bullet$ est une résolution filtrée scindée de M, nous pouvons appliquer le foncteur gr aussi bien à η et s qu'à d et ε, et nous obtenons le complexe gradué gr $X_\bullet$ comme *résolution graduée scindée* de gr M.

La principale utilité des résolutions scindées résulte de la relation

(1.1.4.10) $$dsd = d.$$

Si x est un bord, c'est le bord de l'élément $s(x)$, qui a même filtration que x.

(1.1.5) *Résolutions acycliques par des modules complets-libres.* — Soit A un anneau complet. Nous avons défini en (I, 2.1.17) les A-modules complets-libres, qui sont les modules libres dans la catégorie des A-modules filtrés complets. La proposition suivante généralise la proposition 1.1 de [4] p. 76.

(1.1.5.1) *Proposition.* — *Soient* $X_\bullet$ *et* $X'_\bullet$ *deux* A-*complexes à gauche sur les* A-*modules filtrés* M *et* M' (*les augmentations sont notées* $\varepsilon : X_0 \to M$ *et* $\varepsilon' : X'_0 \to M'$). *Supposons que* $X'_\bullet$ *soit une résolution acyclique filtrée de* M' (1.3.3), *que tous les* A-*modules* X'_n *soient complets, et que tous les* A-*modules* X_n *soient complets-libres. Alors, si* $f: M \to M'$ *est un morphisme de modules filtrés, il existe un morphisme* g *de complexes filtrés* (1.1.1) *vérifiant* $\varepsilon' \circ g_0 = f \circ \varepsilon$. *Deux tels morphismes sont homotopes (dans la catégorie des complexes filtrés).*

Cette proposition justifie la définition (1.1.3.1) des résolutions acycliques filtrées.

(1.1.5.2) *Définition.* — *Nous appelons résolution acyclique complète-libre d'un* A-*module filtré complet* M *une résolution acyclique filtrée* $X_\bullet$ *de* M *dont les modules* X_n *sont complets-libres pour chaque* $n \in \mathbf{Z}$. *Nous écrirons, en abrégé, que* $X_\bullet$ *est une* racl *de* M.

Tout A-module filtré complet M possède une racl; deux racl de M sont homotopes, d'après (1.1.5.1).

Si $X_\bullet$ est une racl du A-module M, alors gr $X_\bullet$ est une résolution acyclique libre du gr A-module gr M.

(1.1.6) *Choix normaux des morphismes et des homotopies.* — Reprenons les notations de la proposition (1.1.5.1). Supposons que les modules complets-libres X_n aient des bases topologiques *données* (dont les éléments seront dits « basiques »). Supposons aussi que A soit une Ω-algèbre, et que $X'_\bullet$ soit une *résolution filtrée scindée* de M' (1.1.4), dont nous notons η' et s' les applications notées η et s en (1.1.4).

Parmi les morphismes $g : X_\bullet \to X'_\bullet$ définis en (1.1.5.1), il en existe un, que nous appellerons *normal*, déterminé par les conditions suivantes.

(1.1.6.1) *Si x est un élément basique de* X_0 *alors* $g(x) = (\eta' \circ f \circ \varepsilon)(x)$.

(1.1.6.2) *Si x est un élément basique de* X_n, *où* $n \in \mathbf{N}^*$, *alors* $g_n(x) = (s'_{n-1} \circ g_{n-1} \circ d_n)(x)$.

De même, si nous avons deux morphismes g, g' au-dessus de f, il existe une homotopie que nous appellerons *normale*, déterminée comme suit (rappelons qu'une homotopie h est une famille d'applications A-linéaires $h_n : X_n \to X'_{n+1}$ vérifiant les relations $g_n - g'_n = h_{n-1} \circ d_n + d'_{n+1} \circ h_n$).

(1.1.6.3) *Pour chaque* $n \in \mathbf{Z}$ *et chaque élément basique* $x \in X_n$,

$$h_n(x) = (s'_n \circ (g_n - g'_n - h_{n-1} \circ d_n))(x).$$

Les « choix normaux » que nous venons de définir nous serviront à construire sans ambiguïté certaines applications. Leur intérêt n'est que technique. Si $X_\bullet$ est une racl de M, si le complexe $X_\bullet$ est scindé et si les X_n ont des bases topologiques données, alors le morphisme normal $g : X_\bullet \to X_\bullet$ au-dessus de l'identité de M n'est pas toujours l'identité de $X_\bullet$ (voir aussi les deux dernières phrases de [4], chap. XI, § 6).

(1.1.7) *Cohomologie continue d'une algèbre supplémentée filtrée complète.* — Soient Ω un anneau filtré complet et A une Ω-algèbre supplémentée filtrée complète. (Il nous suffirait de prendre $\Omega = \mathbf{Z}_p$ et de supposer A valuée complète.)

Notons $\boldsymbol{C}_A$ la catégorie des A-*modules topologiques complets linéairement topologisés* (c'est-à-dire admettant leurs sous-A-modules ouverts comme système fondamental de voisinages de zéro). Les morphismes dans $\boldsymbol{C}_A$ sont les *applications* A-*linéaires continues*.

Soit X un A-module complet-libre, de base topologique $(x_i)_{i \in I}$; posons $w(X; x_i) = \tau_i$. Si $M \in \boldsymbol{C}_A$ (il nous semble superflu d'écrire $M \in \mathrm{Ob}\, \boldsymbol{C}_A$), un morphisme $f : X \to M$ est déterminé par la donnée des $y_i = f(x_i)$. Les $(y_i)_{i \in I}$ sont une famille d'éléments de M, qui doivent seulement vérifier la propriété suivante : *si* $(\lambda_i)_{i \in I}$ *est une famille d'éléments de* A *telle que* $w(A; \lambda_i) + \tau_i$ *tende vers l'infini, alors* $\lambda_i y_i$ *tend vers zéro dans* M (suivant le filtre des complémentaires des parties finies de I).

En particulier (ce sera le cas le plus important), *si* τ_i *tend vers l'infini, les* y_i *doivent tendre vers zéro dans* M, *et ils déterminent alors univoquement le morphisme* $f : X \to M$.

Choisissons une racl $X_\bullet$ (1.1.5) de Ω, considéré comme A-module. Nous pouvons sans inconvénient supposer que $X_0 = A$, ce qui nous permettra de parler sans équivoque de l'augmentation ε.

Si $M \in \boldsymbol{C}_A$, formons le *complexe de cochaînes*

(1.1.7.1) $$\mathrm{Hom}^\bullet_c(X_\bullet, M),$$

défini par les *applications* A-*linéaires continues*, c'est-à-dire par les morphismes dans la catégorie $\boldsymbol{C}_A$.

Nous appelons n-ième groupe de cohomologie continue de A *à valeurs dans* M, *et nous notons* $H_c^n(A, M)$ *le groupe*

(1.1.7.2) $$H^n(\mathrm{Hom}_c^\bullet(X_\bullet, M)), \quad \textit{où } n \in \mathbf{N} \quad (n \in \mathbf{Z}, \text{ si l'on préfère}).$$

Comme deux racl de Ω sont homotopes dans la catégorie des A-modules filtrés complets (et à plus forte raison dans $\mathcal{C}_A$) les groupes de cohomologie continue sont définis à isomorphisme canonique près, comme en [4], chap. X.

(1.1.8) *Comparaison de la cohomologie continue à la cohomologie discrète.* — Conservons les notations de (1.1.7). A tout module $M \in \mathcal{C}_A$ nous associons les groupes de cohomologie du A-module *discret* sous-jacent à M, c'est-à-dire les groupes

(1.1.8.1) $$H^n(A, M) = \mathrm{Ext}_A^n(\Omega, M).$$

Pour calculer ces derniers, nous pouvons prendre une *résolution acyclique projective* $Y_\bullet$ de Ω, et nous avons

(1.1.8.2) $$H^n(A, M) = H^n(\mathrm{Hom}^\bullet(Y_\bullet, M)).$$

Si $X_\bullet$ désigne une racl de Ω, nous avons (dans la catégorie des A-modules discrets) un morphisme $Y_\bullet \to X_\bullet$ au-dessus de l'identité de Ω. Nous en déduisons un morphisme $\mathrm{Hom}_c^\bullet(X_\bullet, M) \to \mathrm{Hom}^\bullet(Y_\bullet, M)$ qui, par passage à la cohomologie, donne les *morphismes fonctoriels*

(1.1.8.3) $$H_c^n(A, M) \to H^n(A, M),$$

qui sont indépendants du choix de $X_\bullet$ et de $Y_\bullet$.

Lorsqu'il existe une racl $X_\bullet$ de Ω dont les modules X_n sont de *rang fini* (c'est-à-dire ont des bases topologiques finies), alors $X_\bullet$ est une résolution acyclique libre de Ω, nous pouvons prendre $Y_\bullet = X_\bullet$ et, comme toutes les applications A-linéaires de X_n dans M sont continues, les morphismes fonctoriels (1.1.8.3) sont des isomorphismes : *la cohomologie continue* $H_c^*(A, M)$ *s'identifie à la cohomologie discrète* $H^*(A, M)$, *pour tout* A-*module topologique complet* $M \in \mathcal{C}_A$.

(1.2) Complexes standard complétés et cohomologie continue d'un pro-p-groupe.

(1.2.1) *Complexe standard d'une algèbre supplémentée.* — Soient Ω un anneau commutatif et A une Ω-algèbre supplémentée, dont l'augmentation est notée ε.

Le *complexe standard* de A est une *résolution acyclique scindée* $X_\bullet$ de Ω, définie comme suit.

(1.2.1.1) *Pour chaque* $n \in \mathbf{N}$, $X_n = A \otimes_\Omega T^n A$.

Autrement dit, X_n est la puissance tensorielle $(n+1)$-ième du Ω-module A; la structure de A-module de X_n s'obtient en faisant opérer à gauche A sur le premier facteur de X_n.

(1.2.1.2) *Pour chaque* $n \in \mathbf{N}^*$, *l'opérateur* $d_n : X_n \to X_{n-1}$ *est défini par la formule*

$$d_n(x_0 \otimes \ldots \otimes x_n) = \sum_{0 \leqslant i < n} (-1)^i x_0 \otimes \ldots \otimes x_i x_{i+1} \otimes \ldots \otimes x_n + (-1)^n x_0 \otimes \ldots \otimes x_{n-1} \varepsilon(x_n).$$

(1.2.1.3) *Pour chaque* $n \in \mathbf{N}$, *l'opérateur* $s_n : X_n \to X_{n+1}$ *est défini par la formule*

$$s_n(x_0 \otimes \ldots \otimes x_n) = 1 \otimes x_0 \otimes \ldots \otimes x_n.$$

Si l'on forme la somme directe des X_n, on vérifie les formules (1.1.4.8) et (1.1.4.9), qui expriment que $X_\bullet$ est une résolution acyclique scindée de Ω. Le lecteur peut se reporter à [4], chap. IX, § 6 et chap. X, § 2.

(1.2.2) *Le complexe standard normalisé d'une algèbre supplémentée.* — Conservons les notations précédentes, et désignons par I le noyau de l'augmentation ε.

Nous avons ainsi $A = I \amalg \Omega$, et $1 - \varepsilon$ est un projecteur Ω-linéaire de A sur l'idéal I.

Le *complexe standard normalisé* de A est une *résolution acyclique scindée* $X'_\bullet$ de Ω, définie comme suit.

(1.2.2.1) $$X'_n = A \otimes_\Omega T^n I, \qquad \textit{pour tout } n \in \mathbf{N}.$$

La structure de A-module est définie par l'opération de A sur le premier facteur.

(1.2.2.2) $$d_n(x_0 \otimes \ldots \otimes x_n) = \sum_{0 \leqslant i < n} (-1)^i x_0 \otimes \ldots \otimes x_i x_{i+1} \otimes \ldots \otimes x_n, \qquad \textit{pour chaque } n \in \mathbf{N}^*.$$

(1.2.2.3) $$s'_n(x_0 \otimes \ldots \otimes x_n) = 1 \otimes (x_0 - \varepsilon(x_0)) \otimes x_1 \otimes \ldots \otimes x_n, \qquad \textit{pour chaque } n \in \mathbf{N}.$$

On vérifie encore les formules (1.1.4.8) et (1.1.4.9) : cf. [4], *loc. cit.*

Le projecteur $1 - \varepsilon : A \to I$ conduit aux épimorphismes Ω-linéaires $T^n A \to T^n I$, puis aux épimorphismes A-linéaires $X_n \to X'_n$. Nous obtenons ainsi un *morphisme de complexes* $X_\bullet \to X'_\bullet$ qui commute aux opérateurs s.

De même, l'injection $I \to A$ conduit à un morphisme $X'_\bullet \to X_\bullet$ (qui ne commute pas aux opérateurs s).

En composant ces deux applications, nous obtenons le *projecteur* $P : X_\bullet \to X_\bullet$ qui applique $X_\bullet$ sur le sous-complexe identifié à $X'_\bullet$.

Il existe une *homotopie* S du complexe $X_\bullet$ (ou encore une *famille d'application* A-linéaires $S_n : X_n \to X_{n+1}$) qui vérifie

(1.2.2.4) $$P - 1 = dS + Sd.$$

(1.2.2.5) $$PS = SP = P(1 - P) = 0.$$

Nous pouvons définir S par $S_0 = 0$, et par la relation de récurrence :

(1.2.2.6) $$S_n(x_0 \otimes \ldots \otimes x_n) = x_0 . (s_n \circ (P_n - 1_n - S_{n-1} \circ d_n) \circ s_{n-1})(x_1 \otimes \ldots \otimes x_n),$$

où 1_n note l'identité sur X_n.

(1.2.3) *Cohomologie d'un groupe abstrait; cochaînes.* — Soient G un groupe, Ω un anneau commutatif, et A l'algèbre supplémentée $\Omega[G]$, avec l'augmentation ε définie par $\varepsilon(x)=1$ pour $x\in G$. Le Ω-module A (resp. I) possède alors une base canonique formée des éléments $x\in G$ (resp. des éléments $x-1$, pour $x\in G$, $x\neq 1$).

Les complexes standard $X_\bullet$ et $X'_\bullet$ de A sont alors des *résolutions acycliques libres* de Ω. Si M est un A-module, c'est-à-dire un Ω-module où G opère par automorphismes, les groupes de cohomologie des complexes $\mathrm{Hom}^\bullet(X_\bullet, M)$ et $\mathrm{Hom}^\bullet(X'_\bullet, M)$ s'identifient *aux groupes de cohomologie de* G *à valeurs dans* M. Comme $X_n = A\otimes T^n A$, le A-module X_n possède une base en correspondance bijective avec G^n, et une application A-linéaire de X_n dans M s'identifie ainsi à une application quelconque de G^n dans M, qu'on appelle une *n-cochaîne*.

La formule (1.2.1.2) conduit à l'expression suivante du cobord d'une n-cochaîne f :

(1.2.3.1)
$$\delta f(x_1, \ldots, x_{n+1}) = x_1 f(x_2, \ldots, x_{n+1}) + \\ + \sum_{1\leqslant i\leqslant n} (-1)^i f(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n).$$

Nous considérons X'_n comme un *quotient* de X_n (1.2.2), ce qui nous permet d'identifier $\mathrm{Hom}(X'_n, M)$ à un *sous-groupe* de $\mathrm{Hom}(X_n, M)$, donc à un sous-groupe du groupe des n-cochaînes. Nous obtenons ainsi les *n-cochaînes normalisées*. Ce sont les applications de G dans M qui prennent la valeur zéro si l'une des variables ($\in G$) est égale à 1.

(1.2.4) *Complexes standards d'une algèbre supplémentée filtrée.* — Soit A une algèbre supplémentée filtrée sur l'anneau filtré Ω (I, 2.1.11). Munissons les modules $X_n = A\otimes T^n A$ et $X'_n = A\otimes T^n I$ de leurs filtrations de produits tensoriels (I, 2.1.10). Alors toutes les applications d, s, s', P, S définies en (1.2.1) et en (1.2.2) sont des *morphismes de modules filtrés*. Nous obtenons ainsi des *résolutions filtrées scindées* de Ω, au sens de (1.1.4).

Supposons que Ω soit un anneau de valuation discrète complet, et A une Ω-algèbre supplémentée valuée. Alors les complexes $X_\bullet$ et $X'_\bullet$ sont formés de *Ω-modules valués* (I, 3.2.1), et nous pouvons construire les *complexes complétés* $\hat{X}_\bullet$ et $\hat{X}'_\bullet$ (1.1.2), qui sont encore des résolutions scindées de Ω. Si nous supposons en outre que I est un Ω-module *complet-libre*, alors tous les modules $\hat{X}_n$ et $\hat{X}'_n$ sont complets-libres et les complétés $\hat{X}_\bullet$, $\hat{X}'_\bullet$ nous fournissent des *résolutions acycliques complètes-libres de* Ω, dont nous avons vu l'usage en (1.1.7).

(1.2.5) *Le complexe standard complété d'un groupe p-valué complet de rang fini.* — Soit G un groupe p-valué complet de rang fini (III, 2.1.2 et 2.1.3). Notons B l'algèbre $\mathbf{Z}_p[G]$, munie de sa filtration induite. Le théorème (III, 2.3.3) affirme que B est une $\mathbf{Z}_p$-algèbre supplémentée valuée. De plus, l'algèbre complétée A de B s'identifie (en tant que $\mathbf{Z}_p$-algèbre topologique) à l'algèbre Al G, définie en (II, 2.2.1). Le choix d'une base ordonnée de G (III, 2.2.4) entraîne celui d'une base topologique de A sur $\mathbf{Z}_p$ (III, 2.3.8).

Le complexe standard de l'algèbre B permet le calcul de la cohomologie « discrète » de G opérant dans un $\mathbf{Z}_p$-module M (1.2.3). Ce complexe standard est *valué* (1.2.4) et *s'identifie à un sous-complexe dense du complexe standard de* A (I, 3.2.1). Les complexes standards de A et de B ont donc *même complexe complété* (I, 3.2.6). Ce complexe sera dit *complexe standard complété du groupe* G; notons $X_\bullet$ ce complexe.

Si M est un A-module linéairement topologisé complet, les groupes de cohomologie du complexe $\mathrm{Hom}_c^\bullet(X_\bullet, M)$ sont les groupes de cohomologie continue $H_c^*(A, M)$ définis en (1.1.7).

Rappelons qu'un A-module linéairement topologisé complet n'est qu'un $\mathbf{Z}_p$-module linéairement topologisé complet, où G opère continûment (II, 2.2.6).

Nous définissons le *complexe standard normalisé complété* de G comme le complété du complexe standard normalisé (1.2.2) de A ou de B.

(1.2.6) *Proposition.* — *Conservons les notations de* (1.2.5). *Les groupes de cohomologie continue* $H_c^*(A, M)$ *s'identifient aux groupes de cohomologie continue* $H_c^*(G, M)$, *définis au moyen des cochaînes continues et de la formule du cobord* (1.2.3.1).

Nous donnerons deux démonstrations de cette proposition : l'une est une vérification directe qui s'appuie sur le théorème de Mahler (III, 1.2.4); l'autre fait intervenir une notion plus générale de « complexe standard complété », qui s'applique à tous les pro-p-groupes.

Lorsque le module M est *discret*, les groupes de cohomologie continue $H_c^*(G, M)$ sont les groupes de cohomologie de Tate, tels qu'ils sont définis en [29], chap. I, 2.2. *Cependant nous avons supposé que* M *est un* $\mathbf{Z}_p$*-module complet.* S'il est discret, cela signifie qu'il est un *p-groupe additif* (ou groupe de *p-torsion*), non nécessairement fini. Ainsi la cohomologie continue, telle que nous l'exposons ici, n'englobe pas la cohomologie de Tate : par exemple, les groupes $H_c^*(G, \mathbf{Z})$ *ne sont pas définis.*

(1.2.7) *Preuve de* (1.2.6) *par le théorème de Mahler.* — Choisissons une base ordonnée $(x_i)_{1\leqslant i\leqslant r}$ du groupe p-valué complet G, de rang r. Posons $\omega(x_i)=\tau_i$. Notons J l'ensemble $\mathbf{N}^r$. L'algèbre de groupe $B=\mathbf{Z}_p[G]$ contient les éléments

$$z^\alpha = \prod_{1\leqslant i\leqslant r}(x_i-1)^{\alpha_i}, \tag{1.2.7.1}$$

pour $\alpha\in J$. Les $(z^\alpha)_{\alpha\in J}$ constituent une base topologique de l'algèbre complétée A de B, avec $w(A; z^\alpha)=\tau\alpha=\sum_{1\leqslant i\leqslant r}\tau_i\alpha_i$.

Le module X_n du complexe standard complété de G est égal, par définition, à $A\hat{\otimes}\hat{T}^nA$. Il admet donc comme *base topologique sur* A *les éléments* z^α *définis par la formule*

$$z^{\boldsymbol\alpha} = 1\otimes z^{\alpha^1}\otimes\ldots\otimes z^{\alpha^n}, \tag{1.2.7.2}$$

où $\boldsymbol\alpha=(\alpha^1, \ldots, \alpha^n)$ *parcourt l'ensemble* J^n.

Nous avons $w(X_n; z^{\boldsymbol\alpha})=\tau\boldsymbol\alpha=\sum_{1\leqslant j\leqslant n}\tau\alpha^j$. Les éléments $z^{\boldsymbol\alpha}$ tendent donc vers zéro dans X_n, et les *applications* A*-linéaires continues* de X_n dans un A-module linéairement topologisé complet M sont en correspondance biunivoque avec les *familles d'éléments* $(c_{\boldsymbol\alpha})_{\boldsymbol\alpha\in J^n}$ *qui tendent vers zéro dans* M. La correspondance est définie par la formule

$$c_{\boldsymbol\alpha}=f(z^{\boldsymbol\alpha}) \tag{1.2.7.3}$$

où $f\in\mathrm{Hom}_c(X_n, M)$ et $\boldsymbol\alpha\in J^n$.

Notons $Y_\bullet$ le complexe standard de B. Nous identifions Y_n à un sous-module dense de X_n, et les éléments f de $\mathrm{Hom}_c(X_n, M)$ sont ainsi déterminés par leurs restrictions à Y_n. Rappelons que $\mathrm{Hom}(Y_n, M)$ s'identifie au groupe des n-cochaînes de G (1.2.3). Si $\mathbf{y}=(y_1, \ldots, y_n)\in G_n$, la valeur en $\mathbf{y}$ de la n-cochaîne ainsi associée à $f\in\mathrm{Hom}_c(X_n, M)$ est

$$f(1\otimes y_1\otimes\ldots\otimes y_n). \tag{1.2.7.4}$$

Notons $\lambda_{(j)}\in\mathbf{Z}_p^r$ les coordonnées de y par rapport à la base ordonnée $(x_i)_{1\leqslant i\leqslant r}$ de G, et posons $\boldsymbol{\lambda}=(\lambda_{(1)}, \ldots, \lambda_{(n)})$.

Les formules (III, 2.3.11.3)

$$y_j=\sum_{\alpha\in J}\binom{\lambda_{(j)}}{\alpha}z^\alpha \tag{1.2.7.5}$$

conduisent à

$$1\otimes y_1\otimes\ldots\otimes y_n=\sum_{\boldsymbol{\alpha}\in J^n}\binom{\boldsymbol{\lambda}}{\boldsymbol{\alpha}}z^{\boldsymbol{\alpha}}, \tag{1.2.7.6}$$

où nous avons posé

$$\binom{\boldsymbol{\lambda}}{\boldsymbol{\alpha}}=\prod_{1\leqslant j\leqslant n}\binom{\lambda_{(j)}}{\alpha^j}. \tag{1.2.7.7}$$

Appliquant (1.2.7.4), nous voyons que la valeur de la n-cochaîne en $\mathbf{y}\in G^n$ est

$$\sum_{\boldsymbol{\alpha}\in J^n}\binom{\boldsymbol{\lambda}}{\boldsymbol{\alpha}}c_{\boldsymbol{\alpha}}\in M. \tag{1.2.7.8}$$

D'après le théorème (III, 1.2.4), une n-cochaîne de G à valeurs dans M, considérée comme application A-linéaire de Y_n dans M, est la restriction d'une application A-linéaire continue de X_n dans M si et seulement si elle est continue. Cela prouve notre proposition, puisque $Y_\bullet$ est un sous-complexe de $X_\bullet$.

(1.2.8) *Définition générale du complexe standard complété d'un pro-p-groupe.* — Soit G un pro-p-groupe. Pour chaque sous-groupe ouvert distingué U de G, notons $X_\bullet^U$ le complexe standard (1.2.1) de l'algèbre supplémentée $\mathbf{Z}_p[G/U]$. La forme fonctorielle des opérateurs d (1.2.1.2) et s (1.2.1.3) montre que nous pouvons construire la *limite projective* $X_\bullet=\varprojlim X_\bullet^U$ des complexes $X_\bullet^U$, et que nous obtenons ainsi une *résolution acyclique scindée de* $\mathbf{Z}_p$ *par des* A-*modules linéairement topologisés compacts*, où A désigne l'algèbre complétée $\mathrm{Al}\, G=\varprojlim \mathbf{Z}_p[G/U]$. Le complexe $X_\bullet$ sera dit *complexe standard complété du pro-p-groupe* G.

(1.2.9) *Propriété du complexe standard complété d'un pro-p-groupe, et deuxième preuve de* (1.2.6). — Conservons les notations de (1.2.8). Notons $\mathcal{C}_A$ la catégorie des A-modules linéairement topologisés complets. Soit $M\in\mathcal{C}_A$. *Alors les groupes de cohomologie du complexe* $\mathrm{Hom}^\bullet(X_\bullet, M)$ *s'identifient aux groupes de cohomologie continue de* G *à valeurs dans* M.

Précisons que, dans $\mathrm{Hom}^\bullet(X_\bullet, M)$, il s'agit de morphismes au sens de $\mathcal{C}_A$ (applications A-linéaires continues) et que la « cohomologie continue » de G est définie au moyen des cochaînes continues.

En effet, si $Y_\bullet$ désigne le complexe standard de l'algèbre supplémentée $\mathbf{Z}_p[G]$, chaque Y_n s'identifie à un sous-$\mathbf{Z}_p[G]$-module dense de X_n, ce qui permet d'identifier $\mathrm{Hom}^\bullet(X_\bullet, M)$ à un complexe de cochaînes.

D'après la proposition (I, 3.2.11), le module X_n s'identifie au *produit tensoriel topologique complété* $A\hat{\otimes}\hat{T}^n A$. Le produit tensoriel complété $\hat{T}^n A$ s'identifie à l'algèbre complétée $\mathrm{Al}(G^n)$, d'après (II, 2.2.8), et le groupe des n-cochaînes continues de G à valeurs dans M s'identifie au groupe des applications $\mathbf{Z}_p$-linéaires continues de $\mathrm{Al}(G^n)$ (ou de $\hat{T}^n A$) dans M, d'après (II, 2.2.6). Les applications A-linéaires de $A\otimes\hat{T}^n A$ dans M s'identifient aux applications $\mathbf{Z}_p$-linéaires de $\hat{T}^n A$ dans M; nous vérifions que les applications continues se correspondent, ce qui achève la démonstration.

Supposons maintenant que l'algèbre $A = \mathrm{Al}\, G$ soit *l'algèbre topologique sous-jacente à une $\mathbf{Z}_p$-algèbre valuée.* Alors la proposition (I, 3.2.10) montre que le complexe standard complété de l'algèbre valuée A, tel que nous l'avons défini en (1.2.4), possède comme complexe sous-jacent de modules topologiques le complexe standard complété de G, défini en (1.2.8). Nous voyons ainsi que, *pour un groupe p-valué complet de rang fini* G, *les deux définitions du complexe standard complété données en* (1.2.5) *et* (1.2.8) *sont compatibles.* La propriété démontrée du complexe standard complété d'un pro-p-groupe nous fournit une deuxième preuve de (1.2.6).

(1.2.10) *Remarques. — Le complexe standard normalisé complété d'un pro-p-groupe* peut se définir comme en (1.2.8).

Nous verrons plus loin comment l'algèbre complétée Al G d'un *pro-p-groupe analytique* G (III, 3.2.2) peut toujours être considérée comme l'algèbre topologique sous-jacente à une algèbre valuée.

(1.3) Aide-mémoire et compléments.

(1.3.1) *Produits tensoriels de complexes.* — Soient Ω un anneau commutatif, et $X^\bullet$, $Y^\bullet$ deux complexes de Ω-modules. Le *produit tensoriel* $Z^\bullet = X^\bullet \otimes_\Omega Y^\bullet$ est un *complexe* de Ω-*modules* défini par les formules suivantes.

(1.3.1.1)
$$Z^n = \coprod_{i+j=n} X^i \otimes_\Omega Y^j.$$

(1.3.1.2)
$$d(x\otimes y) = dx\otimes y + (-1)^i x\otimes dy,$$

pour $i, j \in \mathbf{Z}$, $x \in X^i$ *et* $y \in Y^j$.

Si A et B sont deux Ω-algèbres, et si $X^\bullet$, $Y^\bullet$ sont respectivement des complexes de A-modules et de B-modules, alors $Z^\bullet = X^\bullet \otimes Y^\bullet$ est un complexe de $A\otimes_\Omega B$-modules.

Le produit tensoriel des complexes est *associatif.*

Le produit tensoriel des complexes est *anticommutatif* (ou « commutatif au sens de l'algèbre homologique ») : nous obtenons un isomorphisme $f: X^\bullet\otimes Y^\bullet \to Y^\bullet \otimes X^\bullet$ en posant $f(x\otimes y) = (-1)^{ij} y\otimes x$ pour $i, j \in \mathbf{Z}$, $x \in X^i$, $y \in Y^j$.

(1.3.2) *Produits tensoriels de résolutions scindées.* — Soient A (resp. A′) une Ω-algèbre associative, M (resp. M′) un A-module, $X_\bullet$ (resp. $X'_\bullet$) une résolution scindée de M (resp. M′) dont les opérateurs ε, η, s (resp. ε', η', s') sont définis comme en (1.1.4).

Nous faisons du complexe $X''_\bullet = X_\bullet \otimes_\Omega X'_\bullet$ de $A\otimes A'$-modules une *résolution scindée* de $M\otimes M'$, en posant

(1.3.2.1) $$\varepsilon''(x\otimes x') = \varepsilon(x)\otimes\varepsilon(x') \qquad \textit{pour } x\in X_0 \textit{ et } x'\in X'_0.$$

(1.3.2.2) $$\eta''(x\otimes x') = \eta(x)\otimes\eta(x') \qquad \textit{pour } x\in M \textit{ et } x'\in M'.$$

(1.3.2.3) $$\begin{aligned} s''(x\otimes x') &= s(x)\otimes x', && \textit{pour } i\in \mathbf{N}^*, j\in\mathbf{N}, x\in X_i, x'\in X'_j;\\ s''(x\otimes x') &= s(x)\otimes x' + \eta\varepsilon(x)\otimes s'(x'), && \textit{pour } x\in X_0, j\in\mathbf{N}, x'\in X'_j.\end{aligned}$$

Le produit tensoriel des résolutions scindées est encore *associatif, mais il n'est pas anticommutatif* (le choix de l'opérateur s'' fait jouer des rôles différents aux facteurs $X_\bullet$ et $X'_\bullet$).

(1.3.3) *Complexe de Koszul.* — Soit M un module sur l'anneau commutatif Ω. Construisons l'algèbre symétrique SM et l'algèbre extérieure EM. Le module M s'injecte canoniquement dans SM et dans EM, mais il est ici essentiel de ne pas identifier les images canoniques dans SM et EM d'un élément x de M. Nous convenons donc d'identifier $x\in M$ à son image dans SM, et d'écrire x^* son image dans EM. Construisons le produit tensoriel

(1.3.3.1) $$\mathrm{Ko}\, M = SM\otimes_\Omega EM$$

Pour tout $n\in\mathbf{N}$, posons

(1.3.3.2) $$\mathrm{Ko}_n M = SM\otimes_\Omega E^n M, \quad \text{et}$$

(1.3.3.3) $$d_n(x_1^*\dots x_n^*) = \sum_{1\leqslant i\leqslant n}(-1)^{i+1}(x_1^*\dots x_{i-1}^* x_i x_{i+1}^*\dots x_n^*), \qquad \textit{pour tous } x_1,\dots,x_n\in M.$$

Ces définitions nous permettent de considérer Ko M comme une *algèbre associative*, ainsi que comme *un complexe de* SM-*modules sur* Ω (pour l'augmentation naturelle $\mathrm{Ko}\,M\to\Omega$).

Si M est un Ω-*module libre de rang r, où nous avons choisi une base ordonnée* $(y_i)_{1\leqslant i\leqslant r}$, nous définissons Ko M comme une *résolution scindée de* Ω par le procédé suivant.

Si $r=1$, l'opérateur $s_0 : SM\to SM\otimes E^1M$ est défini par

(1.3.3.4) $$s_0(y_1^n) = y_1^{n-1}y_1^* \qquad \textit{pour } n\in\mathbf{N}^* \textit{ et } s_0(1)=0.$$

Si $r>1$, le module M est somme directe des modules $M_i = \Omega.y_i$; nous venons de définir chaque complexe $\mathrm{Ko}\,M_i$ comme une résolution scindée de Ω par des SM_i-modules. Le *produit tensoriel des résolutions scindées* $\mathrm{Ko}\,M_i$ (calculé dans l'ordre croissant des indices, comme en (1.3.2)) *s'identifie à* Ko M.

(1.3.4) *Complexe standard d'une algèbre de Lie.* — Soient L une Ω-algèbre de Lie, A une Ω-algèbre associative et $\rho : L\to\mathscr{D}A$ un homomorphisme de L dans l'algèbre de Lie des dérivations de A (que nous faisons opérer à gauche sur A). Formons l'algèbre enveloppante UL de L; supposons, pour simplifier, que l'application canonique de L dans UL soit injective et identifions L à son image dans UL. Alors il existe sur le *module*

(1.3.4.1) $$X = UL\otimes_\Omega A$$

une *structure de* Ω-*algèbre associative*, univoquement déterminée par les conditions suivantes.

(1.3.4.2) $x \mapsto x \otimes 1$ *est un homomorphisme de* UL *dans* X.

(1.3.4.3) $y \mapsto 1 \otimes y$ *est un homomorphisme de* A *dans* X.

(1.3.4.4) $$(x \otimes 1).(1 \otimes y) = x \otimes y \qquad \textit{pour } x \in \mathrm{UL} \textit{ et } y \in \mathrm{A}.$$

(1.3.4.5) $$x \otimes y - (1 \otimes y).(x \otimes 1) = 1 \otimes \rho(x).y, \quad \textit{pour } x \in \mathrm{L} \subset \mathrm{UL} \textit{ et } y \in \mathrm{A}.$$

L'existence de l'algèbre X se prouve commodément en construisant sa représentation régulière à droite (cf. [17], Appendice).

Supposons maintenant que A soit *l'algèbre extérieure* EL. Nous n'identifions pas L à $\mathrm{E}^1\mathrm{L}$, mais nous écrivons x^* l'image canonique dans $\mathrm{E}^1\mathrm{L}$ de $x \in \mathrm{L}$. Nous prenons la représentation ρ de L dans les dérivations de $\mathrm{EL} = \mathrm{A}$ qui est définie par la relation :

(1.3.4.6) $$\rho(x).y^* = [x, y]^*, \qquad \textit{pour tous } x, y \in \mathrm{L}.$$

Posons, pour chaque $n \in \mathbf{N}$,

(1.3.4.7) $$\mathrm{X}_n = \mathrm{UL} \otimes_\Omega \mathrm{E}^n\mathrm{L};$$

(1.3.4.8) $$d_n(x_1^* \ldots x_n^*) = \sum_{1 \leqslant i \leqslant n} (-1)^{i+1}(x_1^* \ldots x_{i-1}^* x_i x_{i+1} \ldots x_n^*),$$

pour tous $x_1, \ldots, x_n \in \mathrm{L}$.

Ces formules nous permettent de définir l'algèbre X comme un *complexe de* UL-*modules*. Lorsque L est abélienne, $\mathrm{UL} = \mathrm{SL}$ et nous retrouvons le complexe de Koszul Ko L. Dans le cas général, bien que la formule (1.3.4.8) ne se distingue pas de (1.3.3.3), on doit se rappeler que X a été défini comme produit tensoriel « *gauche* » de UL et EL. Le complexe $\mathrm{X}_\bullet$ de UL-modules sera dit *complexe standard de* L. Ce n'est pas un complexe standard de UL au sens de (1.2.1) ou (1.2.2), mais le lecteur peut voir dans [4], Chap. XIII, comment $\mathrm{X}_\bullet$ s'identifie à un sous-complexe du complexe standard normalisé de UL.

(1.3.5) *Lemme. — Soient* X *un groupe additif,* A *l'anneau des endomorphismes de* X, *et* d, ε, σ *trois éléments de* A. *Supposons vérifiées les relations*

(1.3.5.1) $$\varepsilon(1 - \varepsilon - d\sigma - \sigma d) = 0, \qquad \textit{et}$$

(1.3.5.2) $$d(1 - \varepsilon - d\sigma - \sigma d) = (1 - \varepsilon - d\sigma - \sigma d)d.$$

Définissons, pour $n \in \mathbf{N}$, *les éléments* $\sigma_{(n)} \in \mathrm{A}$ *par les relations de récurrence*

(1.3.5.3) $$\sigma_{(0)} = \sigma;$$

(1.3.5.4) $$\sigma_{(n)} - \sigma_{(n-1)} = \sigma(1 - \varepsilon - d\sigma - \sigma d)^n.$$

Alors nous avons les relations

(1.3.5.5) $$1 - \varepsilon - d\sigma_{(n)} - \sigma_{(n)}d = (1 - \varepsilon - d\sigma - \sigma d)^{n+1}$$

pour chaque $n \in \mathbf{N}$.

La preuve s'obtient par récurrence sur n.

Dans les applications que nous ferons de ce lemme, nous aurons les relations (1.1.4.8)

(1.3.5.6) $$d^2 = d\varepsilon = \varepsilon d = \sigma\varepsilon = \varepsilon\sigma = \varepsilon(1-\varepsilon) = 0,$$

qui entraînent (1.3.5.1) et (1.3.5.2). Nous chercherons à définir un élément $s \in A$ comme limite de $\sigma_{(n)}$, de telle sorte que nous ayons (1.1.4.9)

(1.3.5.7) $$ds + sd = 1 - \varepsilon, \quad \textit{et}$$

(1.3.5.8) $$s\varepsilon = \varepsilon s = 0.$$

(1.3.6) *Application au complexe standard d'une algèbre de Lie.* — Soit L une Ω-algèbre de Lie; nous supposons que L est un Ω-module libre de rang r, et nous choisissons une base ordonnée $(y_i)_{1 \leqslant i \leqslant r}$ de L. Ce choix détermine un isomorphisme (de Ω-modules) de UL sur SL : si $\bar{x}$ note l'image canonique dans SL de $x \in L$, l'isomorphisme met en correspondance les bases de UL et de SL, formées respectivement des monômes ordonnés $y^\alpha = \prod_i y_i^{\alpha_i}$ et $\bar{y}^\alpha = \prod_i \bar{y}_i^{\alpha_i}$ $(\alpha \in \mathbf{N}^r)$. L'isomorphisme $UL \to SL$ se prolonge en un isomorphisme (de Ω-modules)

(1.3.6.1) $$f : X = UL \otimes_\Omega EL \to \text{Ko } L = SL \otimes_\Omega EL.$$

Le choix de la base (y_i) entraîne celui d'une homotopie $\bar{s}$ de Ko L, qui en fait une résolution scindée de Ω (1.3.3). Définissons l'opérateur Ω-linéaire $\sigma : X \to X$ par la formule :

(1.3.6.2) $$\sigma = f^{-1} \circ \bar{s} \circ f.$$

Alors nous pouvons appliquer le lemme (1.3.5) aux opérateurs d, ε, σ de X. *Pour tout $x \in X$, $\sigma_{(n)}(x)$ a une valeur constante $s(x)$ pour n assez grand, et l'opérateur s achève de définir X comme une résolution scindée de Ω par des UL-modules.*

En effet, notons $U_n L$ les modules définis en (IV, 2.1.2 et 2.1.3), que nous identifions à leurs images canoniques dans UL. Les modules $U_n L$ sont facteurs directs dans UL. Posons, pour $i \in \mathbf{N}$,

(1.3.6.3) $$X^{(i)} = \coprod_{0 \leqslant j \leqslant i} U_j L \otimes_\Omega E^{i-j} L.$$

Les $X^{(i)}$ forment une famille croissante de *sous-Ω-modules* et de *sous-complexes* de X. Leur réunion est X; on a $X^{(0)} = \Omega$. Ils sont stables pour l'opérateur σ.

Le quotient $X^{(i)}/X^{(i-1)}$ s'identifie d'après (IV, 2.1.3), à

(1.3.6.4) $$\coprod_{0 \leqslant j \leqslant i} S^j L \otimes_\Omega E^{i-j} L.$$

Ce dernier module s'identifie à un sous-complexe de Ko L, stable pour $\bar{s}$. Nous en déduisons les relations

(1.3.6.5) $$(1 - \varepsilon - d\sigma - \sigma d)(x) \in X^{(i-1)},$$

pour $i \in \mathbf{N}$ *et* $x \in X^{(i)}$, qui nous permettent d'appliquer le lemme (1.3.5). Nous avons ainsi une *homotopie s bien déterminée* sur le complexe standard d'une algèbre de Lie *dont nous connaissons une base ordonnée.*

(1.3.7) *Complexes gradués, filtrés et valués.* — Lorsqu'il s'agit d'anneaux et de modules gradués (resp. filtrés), la forme explicite des opérateurs de bord, d'augmentation et d'homotopie montre que ce sont des *morphismes de modules gradués* (resp. *filtrés*). Dans le cas des modules gradués, la base d'un module libre doit être formée d'éléments homogènes (I, 1.1.6). Dans le cas filtré, l'homotopie d'un complexe de Koszul Ko M (1.3.3) est définie à partir d'une *base filtrée* (I, 2.1.16) *ordonnée*; de même l'homotopie du complexe standard d'une algèbre de Lie L est définie à partir d'uue *base filtrée ordonnée de* L.

En particulier, si L est une algèbre de Lie valuée de rang fini r sur un anneau de valuation discrète complet Ω, nous avons vu en (I, 3.3) et en (IV, 2.2) que SL, EL, UL sont des algèbres valuées. Nous vérifions que la structure *d'algèbre* du produit tensoriel gauche $X = UL \otimes_{\Omega} EL$ est compatible avec sa structure de Ω-*module valué* (I, 3.2.1). Considéré comme UL-module, X est filtré-libre, donc valué puisque UL est valué en tant qu'anneau.

2. COHOMOLOGIE CONTINUE DES PRO-p-GROUPES ANALYTIQUES

(2.1) Un lemme de Serre.

(2.1.1) *Énoncé du lemme.* — Soient Ω un anneau commutatif *filtré complet*, et A une Ω-*algèbre supplémentée filtrée complète*, d'augmentation ε. Nous supposons que *l'idéal d'augmentation* $I (= \operatorname{Ker} \varepsilon)$ est un Ω-module *complet-libre* (I, 2.1.17). Nous notons Γ l'anneau gr Ω, B la Γ-algèbre supplémentée gr A, et $\overline{\varepsilon}$ l'augmentation gr ε de B.

Soit $Y_\bullet$ une *résolution scindée de* Γ (1.1.4) par des B-*modules* $(Y_n)_{n \in \mathbf{N}}$ *gradués libres* (I, 1.1.6) de *graduations discrètes* (I, 1.1.3). Le module Y_0 est B, *l'augmentation est* $\overline{\varepsilon}$; la *différentielle* et l'*homotopie* du complexe $Y_\bullet$ sont notées $\overline{d}$ et $\overline{s}$; ce sont des *morphismes* de B-*modules* (resp. Γ-*modules*) *gradués.*

Alors il existe une résolution scindée $X_\bullet$ *de* Ω *par des* A-*modules complets-libres, de telle sorte que*

(2.1.1.1) $$\operatorname{gr} X_\bullet = Y_\bullet.$$

Plus précisément, $X_0 = A$ et l'augmentation de la résolution scindée $X_\bullet$ est l'augmentation ε de A. Pour chaque $n \in \mathbf{N}$, il existe un isomorphisme de gr X_n sur Y_n, de telle sorte que (par transport de structure) :

(2.1.1.2) $\operatorname{gr} d = \overline{d}$, $\operatorname{gr} s = \overline{s}$, *et* $\operatorname{gr} \varepsilon = \overline{\varepsilon}$, d et s désignant la différentielle et l'homotopie de $X_\bullet$.

(2.1.1.3) *Corollaire.* — *Si, pour un entier* $n \in \mathbf{N}$, Y_n *est un* B-*module libre de rang fini, alors* X_n *est un* A-*module libre de même rang. Plus particulièrement, si* $Y_n = 0$ *pour* $n > r$, *alors* $X_n = 0$ *pour* $n > r$.

(2.1.2) *Construction des* X_n, *de* d_1 *et de* s_0. — Posons $X_0 = A$. Pour chaque $n \in \mathbf{N}^*$, choisissons une base $\overline{\mathscr{B}}_n$ du B-module gradué Y_n, prenons un ensemble $\mathscr{B}_n$ en correspondance bijective avec $\overline{\mathscr{B}}_n$ ($x \in \mathscr{B}_n$ correspondant à $\overline{x} \in \overline{\mathscr{B}}_n$) et construisons le A-*module complet-libre* X_n *de base topologique* $\mathscr{B}_n$, de telle sorte que

$$w(X_n; x) = \deg \overline{x}, \quad \textit{pour } x \in \mathscr{B}_n. \tag{2.1.2.1}$$

Alors la bijection $\mathscr{B}_n \to \overline{\mathscr{B}}_n$ détermine un isomorphisme de B-modules $\operatorname{gr} X_n \to Y_n$. Nous identifierons désormais Y_n à $\operatorname{gr} X_n$.

Pour définir les applications A-linéaires d_n, il nous suffira de donner les valeurs $d_n(x)$ pour $x \in \mathscr{B}_n$. Ces valeurs devront vérifier les relations

$$w(X_{n-1}; d_n(x)) \geqslant w(X_n; x).$$

Soit $x \in \mathscr{B}_1$. Nous avons $\overline{d}_1(\overline{x}) \in \operatorname{gr} I$, puisque $\overline{\varepsilon}\overline{d}_1 = 0$. Nous pouvons donc choisir *dans* I *un représentant de* $\overline{d}_1(\overline{x})$; appelons cet élément $d_1(x)$.

Nous définissons ainsi une application $d_1 : X_1 \to X_0$. Nous avons

$$\varepsilon d_1 = 0 \quad \textit{et} \quad \operatorname{gr} d_1 = \overline{d}_1. \tag{2.1.2.2}$$

Choisissons maintenant un *morphisme de* Ω-*modules filtrés* $\sigma_0 : X_0 \to X_1$ qui vérifie les relations

$$\sigma_0 \varepsilon = 0 \quad \textit{et} \quad \operatorname{gr} \sigma_0 = \overline{s}_0. \tag{2.1.2.3}$$

Il nous suffit de définir la restriction de σ_0 à I. Par hypothèse I est un Ω-module complet-libre. Nous choisissons une base topologique de I; si y est un élément de cette base et $\overline{y}$ le terme dominant de y, nous choisissons un représentant de $\overline{s}_0(\overline{y})$ dans X_1 et nous l'appelons $\sigma_0(y)$. Ces choix définissent σ_0.

Posons $X = X_0 \amalg X_1$. L'application $d : X \to X$ est définie par sa restriction d_i à X_i ($i = 0, 1$), et $\varepsilon : X \to X$ est la projection sur $\Omega \subset X_0$; définissons $\sigma : X \to X$, dont la restriction à X_0 est σ_0 (σ est nul sur X_1). Appliquons le lemme (1.3.5). Comme $1 - \varepsilon - d\sigma - \sigma d$ *est un endomorphisme* Ω-*linéaire* de X, que la restriction à $\operatorname{gr} X_0 = Y_0$ de l'application $\operatorname{gr}(1 - \varepsilon - d\sigma - \sigma d)$ est *nulle* (car c'est $1 - \overline{\varepsilon} - \overline{d}_1 \overline{s}_0 = 0$, par hypothèse), et que X_0 est *complet* pour une *filtration discrète*, les applications $\sigma_{(i)}$ définies en (1.3.5) convergent dans X_0. Nous posons

$$s_0(x) = \lim_{i \to \infty} \sigma_{(i)}(x), \quad \textit{pour } x \in X_0, \tag{2.1.2.4}$$

et nous avons

$$s_0 \varepsilon = 0, \quad \operatorname{gr} s_0 = \overline{s}_0 \quad \textit{et} \tag{2.1.2.5}$$

$$1 - \varepsilon - d_1 s_0 = 0 \quad \textit{sur } X_0. \tag{2.1.2.6}$$

(2.1.3) *Hypothèse de récurrence; construction de* d_{n+1}. — Nous avons construit les X_n, ainsi que d_1 et s_0. Supposons que, pour un certain entier $n \geqslant 1$, nous ayons construit les applications A-linéaires $d_i : X_i \to X_{i-1}$ pour $1 \leqslant i \leqslant n$ et les applications Ω-linéaires $s_i : X_i \to X_{i+1}$ pour $0 \leqslant i < n$, de telle sorte que

(2.1.3.1) $$d_{i-1} d_i = 0 \qquad \textit{pour } 1 < i \leqslant n;$$

(2.1.3.2) $$d_{i+1} s_i + s_{i-1} d_i = 1 \quad \textit{sur } X_i, \ \textit{pour } 1 \leqslant i < n.$$

(2.1.3.3) $$\operatorname{gr} d_i = \overline{d}_i \qquad \textit{pour } 1 \leqslant i \leqslant n.$$

(2.1.3.4) $$\operatorname{gr} s_i = \overline{s}_i \qquad \textit{pour } 0 \leqslant i < n.$$

Les relations (2.1.2.2), (2.1.2.5) et (2.1.2.6) font partie de notre hypothèse de récurrence.

La construction de d_{n+1} équivaut au choix des éléments $d_{n+1}(x)$, pour $x \in \mathscr{B}_{n+1}$ (base topologique de X_{n+1}). Le terme dominant de $d_{n+1}(x)$ doit être $\overline{d}_{n+1}(\overline{x})$ (cela équivaut à $\operatorname{gr} d_{n+1} = \overline{d}_{n+1}$). Prenons un représentant y de $\overline{d}_{n+1}(\overline{x})$. Nous n'avons pas nécessairement $d_n(y) = 0$, mais nous savons que $w(X_{n-1}; d_n(y)) > w(X_n; y)$: cela exprime la relation $\overline{d}_n \overline{d}_{n+1}(\overline{x}) = 0$. Nous pouvons donc poser

(2.1.3.5) $$d_{n+1}(x) = y - s_{n-1} d_n(y),$$

et, les choix des y étant faits pour tous les $x \in \mathscr{B}_{n+1}$, nous obtenons par prolongement une application A-linéaire $d_{n+1} : X_{n+1} \to X_n$, qui vérifie

(2.1.3.6) $$\operatorname{gr} d_{n+1} = \overline{d}_{n+1}, \qquad \textit{et}$$

(2.1.3.7) $$d_n d_{n+1} = 0.$$

Pour établir (2.1.3.7) nous utilisons (2.1.3.2), avec $i = n-1$, si $n \geqslant 2$, et (2.1.2.6) si $n = 1$.

(2.1.4) *Construction de s_n, et fin de la preuve.* — Le Ω-module $A = \Omega \amalg I$ est complet-libre. Les Ω-modules X_n, qui sont des A-modules complets-libres, sont donc des Ω-modules complets-libres. Cela nous permet de choisir une application Ω-linéaire $\sigma_n : X_n \to X_{n+1}$, telle que

(2.1.4.1) $$\operatorname{gr} \sigma_n = \overline{s}_n.$$

Posons $X = \coprod_{0 \leqslant i \leqslant n+1} X_n$. Définissons les endomorphismes ε, d, σ de X. L'endomorphisme ε est l'augmentation (projection sur $\Omega \subset X_0$) ; la restriction de d à X_i est d_i ; la restriction de σ à X_i est s_i pour $0 \leqslant i < n$, σ_n pour $i = n$, et 0 pour $i = n+1$. Ces endomorphismes sont des morphismes de Ω-modules filtrés.

Appliquons le lemme (1.3.5). Comme X est un Ω-module *complet* de filtration *discrète*, et que $\operatorname{gr}(1 - \varepsilon - d\sigma - \sigma d)$ a une restriction nulle à $\operatorname{gr} X_j$ pour $0 \leqslant j \leqslant n$, les applications $\sigma_{(i)}$ définies en (1.3.5) convergent dans X_n (si $x \in X_j$, $j < n$, $\sigma_{(i)}(x) = s_j(x)$ pour tout $i \in \mathbf{N}$). Nous posons

(2.1.4.2) $$s_n(x) = \lim_{i \to \infty} \sigma_{(i)}(x), \qquad \textit{pour } x \in X_n.$$

Nous obtenons

(2.1.4.3) $$\operatorname{gr} s_n = \overline{s}_n;$$

(2.1.4.4) $$d_{n+1} s_n + s_{n-1} d_n = 1 \qquad \textit{sur } X_n.$$

Notre hypothèse de récurrence est maintenant prouvée pour $n+1$, ce qui achève la démonstration.

(2.1.5) *Lemme. — Soient* A *un anneau filtré complet*, M *et* M′ *deux* A*-modules filtrés complets*, $X_\bullet$ *et* $X'_\bullet$ *deux complexes de* A*-modules filtrés, enfin* $\varepsilon : X_\bullet \to M_\bullet$ *et* $\varepsilon' : X'_\bullet \to M'_\bullet$ *deux morphismes* (1.1.3). *Nous supposons que les modules* X_n *sont complets-libres, que les modules* X'_n *sont complets, pour* $n \in \mathbf{N}$, *et que* $X'_\bullet$ *est une résolution acyclique filtrée de* $M'_\bullet$. *Soient* $f : M \to M'$ *un morphisme de* A*-modules filtrés et* $g : \operatorname{gr} X_\bullet \to \operatorname{gr} X'_\bullet$ *un morphisme de* gr A*-complexes gradués* (1.1.1) *tels que* $\operatorname{gr} \varepsilon' \circ g = \operatorname{gr} f \circ \operatorname{gr} \varepsilon$.

Alors il existe un morphisme de A*-complexes filtrés* $h : X_\bullet \to X'_\bullet$, *tel que* $\operatorname{gr} h = g$ *et que* $\varepsilon' \circ h = f \circ \varepsilon$.

Preuve. — Choisissons une base topologique $\mathscr{B}_0$ de X_0. Soit $x \in \mathscr{B}_0$. Prenons le terme dominant $\bar{x}$ de x dans $\operatorname{gr} X_0$, et choisissons un représentant y de $g(\bar{x})$ dans X'_0. La relation $\operatorname{gr} \varepsilon' \circ g = \operatorname{gr} f \circ \operatorname{gr} \varepsilon$ entraîne

(2.1.5.1) $$w(M'; \varepsilon'(y) - f\varepsilon(x)) > w(M; x).$$

D'après la définition des résolutions acycliques filtrées (1.1.3.1), il existe un élément $z \in X'_0$ vérifiant

(2.1.5.2) $$\varepsilon'(z) = \varepsilon'(y) - f\varepsilon(x);$$

(2.1.5.3) $$w(X'_0; z) = w(M'; \varepsilon'(y) - f\varepsilon(x)).$$

Nous posons alors

(2.1.5.4) $$h_0(x) = y - z.$$

Les choix étant faits pour tous les $x \in \mathscr{B}_0$, nous obtenons par prolongement une application

(2.1.5.5) $$h_0 : X_0 \to X'_0,$$

qui vérifie $\operatorname{gr} h_0 = g_0$ et $f \circ \varepsilon = \varepsilon' \circ h_0$.

Les morphismes h_i, $i \in \mathbf{N}^*$, se construisent de même, par récurrence sur i.

(2.1.6) *Corollaire. — Reprenons les notations du lemme* (2.1.1). *Si* $X_\bullet$ *et* $X'_\bullet$ *sont deux complexes vérifiant les conclusions de ce lemme, alors* $X_\bullet$ *et* $X'_\bullet$ *sont des* A*-complexes filtrés isomorphes* (1.1.1).

Un isomorphisme de $X_\bullet$ sur $X'_\bullet$ ne commute pas nécessairement aux homotopies de ces complexes.

(2.2) Le complexe quasi-minimal d'un groupe p-valué complet de rang fini.

(2.2.1) *Structure de l'algèbre* A = Al G. — Soit G un groupe *p-valué* (III, 2.1.2) *complet de rang fini* r (III, 2.1.3). Rappelons les propriétés principales de G et de sa $\mathbf{Z}_p$*-algèbre complétée* Al G (II, 2.2.1) que nous noterons A.

L'algèbre de Lie graduée associée gr G est une Γ*-algèbre de Lie graduée, libre de rang* r

en tant que Γ-*module*; l'anneau gradué Γ est gr $\mathbf{Z}_p$, que nous pouvons écrire $\mathbf{F}_p[\pi]$, π désignant le terme dominant de p.

Si $(x_i)_{1 \leqslant i \leqslant r}$ est une famille de représentants dans G d'une base ordonnée de gr G, alors les x_i constituent une *base ordonnée* de G (III, 2.2.4), c'est-à-dire que tout élément $y \in G$ s'écrit univoquement comme un produit ordonné $y = \prod_{1 \leqslant i \leqslant r} x_i^{\lambda_i}$, où $\lambda_i \in \mathbf{Z}_p$, et nous avons alors

$$\omega(y) = \inf_{1 \leqslant i \leqslant r} (\omega(x_i) + v(\lambda_i)).$$

L'algèbre $A = \mathrm{Al}\, G$ est la *complétée* de l'algèbre $\mathbf{Z}_p[G]$ pour la *borne inférieure des filtrations* w qui vérifient $w(x-1) \geqslant \omega(x)$ pour tout $x \in G$.

L'algèbre A est un $\mathbf{Z}_p$-*module complet-libre*, admettant la base topologique z^α, $\alpha \in \mathbf{N}^r$ (où $z^\alpha = \prod_{1 \leqslant i \leqslant r} (x_i - 1)^{\alpha_i}$ et $w(A; z^\alpha) = \sum_{1 \leqslant i \leqslant r} \alpha_i \omega(x_i)$). *La* Γ-*algèbre graduée associée* gr A *s'identifie canoniquement à l'algèbre enveloppante* U gr G (III, 2.3.3).

La $\mathbf{Z}_p$-algèbre topologique sous-jacente à A est indépendante du choix de la valuation de G. Il existe toujours des p-valuations de G pour lesquelles gr G est une algèbre de Lie abélienne (III, 3.1.12). L'algèbre gr A est alors *l'algèbre symétrique d'un* Γ-*module libre de rang r*.

(2.2.2) *Définition du complexe quasi-minimal de* G. — Conservons les notations de (2.2.1). Notons $Y_\bullet$ le complexe standard de la Γ-algèbre de Lie gr G (1.3.4) (qui se réduit au complexe de Koszul Ko gr G si gr G est abélienne). Nous savons, d'après (1.3.6) et (1.3.7), que $Y_\bullet$ est une *résolution acyclique* de Γ par des U gr G-*modules libres*. Plus précisément, le choix d'une base ordonnée de gr G détermine celui d'une homotopie qui fait de $Y_\bullet$ une *résolution scindée* de Γ.

Si nous posons $B = \mathrm{gr}\, A$ et $\Omega = \mathbf{Z}_p$, nous retrouvons les notations du lemme (2.1.1) et nous vérifions les hypothèses de ce lemme.

(2.2.2.1) *Définition. — Nous appelons complexe quasi-minimal de* G *le complexe* $X_\bullet$ *construit à partir du complexe standard* $Y_\bullet$ *de l'algèbre de Lie* gr G *par application du lemme* (2.2.1).

(2.2.2.2) *Tout groupe p-valué complet* G *de rang r possède un complexe quasi-minimal.*

(2.2.2.3) *Le complexe quasi-minimal* $X_\bullet$ *de* G *est une résolution filtrée scindée* (1.1.4) *de* $\mathbf{Z}_p$ *par des* Al G-*modules filtrés-libres* X_n (I, 2.1.16), *de rangs respectifs* $\binom{r}{n}$.

En effet Y_n est un U gr G-module libre de rang égal à celui de E^n gr G sur Γ (1.3.4.7), c'est-à-dire à $\binom{r}{n}$. Comme A est complet, les A-modules filtrés-libres de rang fini sont complets-libres.

(2.2.2.4) *Le complexe quasi-minimal* $X_\bullet$ *de* G *est déterminé à un isomorphisme* (non canonique) *près*. Il s'agit d'un isomorphisme en tant que complexe, mais non en tant que résolution scindée.

C'est une conséquence du corollaire (2.1.6).

(2.2.3) *Premières conséquences de l'existence d'un complexe quasi-minimal.* — Conservons les notations précédentes. Soit M un A-module linéairement topologisé complet, c'est-à-dire un $\mathbf{Z}_p$-module complet où G opère continûment.

L'existence du complexe quasi-minimal $X_\bullet$ montre que nous sommes dans le cas étudié en (1.1.8) : la *cohomologie continue* $H_c^*(A, M)$ *s'identifie à la cohomologie discrète* $H^*(A, M)$, *c'est-à-dire à* $H^*(\mathrm{Hom}_A^\bullet(X_\bullet, M))$.

D'autre part (1.2.6) *la cohomologie continue de* G *s'identifie à la cohomologie continue de* A. Nous obtenons donc :

(2.2.3.1) $$H_c^n(G, M) = \mathrm{Ext}_A^n(\mathbf{Z}_p, M), \qquad \textit{pour tout } n \in \mathbf{N}.$$

Ce résultat ne fait pas intervenir la valuation de G. Il est donc vrai pour un groupe p-valuable G (III, 3.1.6). Nous verrons plus loin (3.2.7) qu'il vaut pour tout pro-p-groupe analytique (III, 3.2.2).

Dans le cas du groupe G, p-valué de rang r, nous avons

(2.2.3.2) $$H_c^n(G, M) = H^n(\mathrm{Hom}_A^\bullet(X_\bullet, M)),$$

d'où

(2.2.3.3) $$H_c^n(G, M) = 0 \qquad \text{pour } n > r.$$

La dimension cohomologique de G *est donc* $\leqslant r$.

Si nous posons $M = \mathbf{F}_p$ (sur lequel G opère trivialement), nous avons, pour chaque n

(2.2.3.4) $$\dim_{\mathbf{F}_p} \mathrm{Hom}_A(X_n, \mathbf{F}_p) = \binom{r}{n},$$

d'où

(2.2.3.5) $$\dim_{\mathbf{F}_p} H_c^n(G, \mathbf{F}_p) \leqslant \binom{r}{n}.$$

(2.2.4) *Proposition.* — *Soit* G *un pro-p-groupe analytique. Alors l'algèbre* Al G *est un anneau local compact noethérien (à droite et à gauche).*

Preuve. — Nous savons que Al G est un anneau local compact, pour chaque pro-p-groupe G (II, 2.2.2). Si G est analytique, il contient un sous-groupe ouvert p-valuable U (III, 3.2.2) que nous pouvons supposer p-valué. L'algèbre Al G est un Al U-module de type fini (II, 2.2.7), et il nous suffit de prouver que Al U est noethérien. Or gr Al U est *noethérien* ([13], th. 4, p. 164) et la filtration de l'algèbre *complète* Al U est *discrète*.

(2.2.5) *Complexes minimaux.* — Soient A un anneau local noethérien et R son radical. Rappelons quelques points de la théorie des résolutions minimales d'Eilenberg [7].

Nous nous plaçons dans la *catégorie des* A-*modules de type fini*. Un *épimorphisme* $P \to M$, où P est *libre*, est dit *minimal* si le morphisme associé $P/RP \to M/RM$ est *bijectif*.

(2.2.5.1) Une résolution acyclique libre $X_\bullet$ d'un module M est dite *minimale* si les épimorphismes $\varepsilon : X_0 \to M$, $X_1 \to \mathrm{Ker}\,\varepsilon$ et $X_{i+1} \to \mathrm{Ker}\, d_i\ (i \in \mathbf{N}^*)$ sont minimaux.

(2.2.5.2) *La résolution minimale* $X_\bullet$ de M est déterminée à un *isomorphisme* (non canonique) près ([7], prop. 7). Toute résolution libre de M contient la résolution minimale comme *facteur direct* (*ibid.*, th. 8).

(2.2.5.3) *Pour qu'une résolution libre* $X_\bullet$ *de* M *soit minimale, il faut et il suffit que le complexe quotient* $X_\bullet/RX_\bullet$ *ait une différentielle nulle* (*ibid.*, prop. 9). Ce complexe peut encore s'écrire $k\otimes_A X_\bullet$, en désignant par k le *corps résiduel* A/R.

Nous appliquons ces notions à l'algèbre complétée $A = \mathrm{Al}\, G$ d'un pro-p-groupe analytique G (2.2.5).

(2.2.5.4) *Définition. — Nous appelons complexe minimal d'un pro-p-groupe analytique* G *une résolution minimale de* $\mathbf{Z}_p$ *par des* Al G-*modules libres.*

(2.2.6) *Critère de minimalité du complexe quasi-minimal.* — Soient G un groupe p-valué complet de rang r, et $X_\bullet$ un complexe quasi-minimal de G (2.2.2).

Pour que le complexe de Al G-modules $X_\bullet$ soit un *complexe minimal* du pro-p-groupe analytique G (2.2.5.4), il faut et il suffit d'après (2.2.5.3) que le complexe

(2.2.6.1) $$X_\bullet^* = \mathbf{F}_p \otimes_A X_\bullet$$

ait une différentielle nulle. Cette condition peut se mettre sous la forme suivante :

(2.2.6.2) $$\dim_{\mathbf{F}_p} H^n(\mathrm{Hom}^\bullet_{\mathbf{F}_p}(X_\bullet^*, \mathbf{F}_p)) = \dim_{\mathbf{F}_p} X_n^*,$$

pour tout $n \in \mathbf{N}$.

Or le complexe $\mathrm{Hom}^\bullet_{\mathbf{F}_p}(X_\bullet^*, \mathbf{F}_p)$ s'identifie à $\mathrm{Hom}^\bullet_A(X_\bullet, \mathbf{F}_p)$, et $\dim_{\mathbf{F}_p} X_n^* = \binom{r}{n}$. Nous obtenons donc le critère de minimalité suivant.

(2.2.6.3) *Pour que le complexe quasi-minimal du groupe p-valué* G *complet de rang* r *soit minimal, il faut et il suffit que*

$$\dim_{\mathbf{F}_p} H^n_c(G, \mathbf{F}_p) = \binom{r}{n}$$

pour tout $n \in \mathbf{N}$.

Il est aisé de construire des groupes p-valués qui ne vérifient pas le critère (2.2.6.3). En effet, l'entier $\dim_{\mathbf{F}_p} H^1_c(G, \mathbf{F}_p)$ est égal au *nombre minimum de générateurs* de G ([29], chap. Ier, corollaire de la prop. 25). Le groupe étudié en (III, 3.2.4) est de rang 4 et possède deux générateurs.

(2.2.7) *Groupes équi-p-valués.* — Nous dirons qu'un groupe G est *équi-p-valué* s'il est *p-valué complet de rang fini* et s'il possède une *base ordonnée dont tous les éléments ont la même filtration t.* Il revient au même d'exiger que le *module* gr G soit engendré par ses éléments de degré t.

(2.2.7.1) *Tout pro-p-groupe analytique contient un sous-groupe ouvert qui est équi-p-valué (pour une filtration convenable).*

C'est une conséquence de (III, 3.1.3), ou de (II, 1.1.11).

(2.2.7.2) *Le complexe quasi-minimal* $X_\bullet$ *d'un groupe équi-p-valué* G *est minimal.*

En effet le radical R de l'algèbre Al G est constitué par les éléments de valuation > 0. Si t est la valuation des générateurs de G, les éléments basiques de X_n ont tous la valuation nt (1.3.4). Nous avons donc $dX_{\bullet} \subset RX_{\bullet}$, ce qui équivaut (2.2.5.3) à la minimalité de $X_{\bullet}$.

(2.2.8) *Théorème. — La dimension cohomologique d'un groupe p-valuable de rang r est égale à r.*

Soit en effet G un groupe p-valuable de rang r. Nous avons $\mathrm{cd}\, G \leqslant r$ (2.2.3), et G contient des sous-groupes ouverts de dimension cohomologique r, d'après (2.2.6) et (2.2.7). La proposition 14 de [29], chap. Ier, achève notre preuve.

(2.3) Cohomologie continue et cohomologie analytique.

(2.3.1) *Cochaînes analytiques.* — Soit G un groupe profini p-analytique (III, 3.2.2) opérant continûment sur un $\mathbf{Z}_p$-module complet M (II, 2.2.4). Les *n-cochaînes analytiques* de G à valeurs dans M sont les applications analytiques de G^n dans M (III, 1.3.2).

Si, de plus, G est *p-valuable* (resp. *p-saturable* (III, 3.1.6)), nous savons définir les cochaînes *analytiques strictes* (III, 1.3.5) (resp. *analytiques tayloriennes* (III, 1.3.4)).

Sous certaines hypothèses, ces cochaînes analytiques (resp. analytiques strictes, analytiques tayloriennes) constituent un sous-complexe du complexe des cochaînes continues. Nous obtenons alors des groupes de cohomologie analytique (resp. stricte, taylorienne) de G à valeurs dans M, qui s'appliquent canoniquement dans les groupes de cohomologie continue.

Nous montrerons que *la cohomologie analytique s'identifie à la cohomologie continue*, lorsque G est un *groupe profini p-analytique* (III, 3.2.2) et M un *$\mathbf{Z}_p$-module sans torsion de rang fini.*

(2.3.2) *Les $\mathbf{Z}_p$-modules sans torsion de rang fini.* — Nous appelons *rang* d'un $\mathbf{Z}_p$-module M la *dimension* du $\mathbf{Q}_p$-espace vectoriel $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} M$.

Un $\mathbf{Z}_p$-module sans torsion de rang d est isomorphe à un module de la forme $\mathbf{Z}_p^s \times \mathbf{Q}_p^{s'}$, où $s + s' = d$. Un tel module M possède une topologie naturelle : c'est la topologie induite par celle de *l'espace vectoriel de dimension finie* $\mathbf{Q}_p \otimes M$ *sur le corps valué complet* $\mathbf{Q}_p$.

Il nous sera commode de parler de *valuations* des $\mathbf{Q}_p$-espaces vectoriels, ou (par restriction) de leurs sous-modules : ce sont les valuations à valeurs *réelles* (non nécessairement positives) qui prolongent les valuations positives de $\mathbf{Z}_p$-modules, comme en (I, 2.2.8).

Le théorème d'équivalence des normes prend la forme « additive » suivante.

(2.3.2.1) *Si w et w' sont deux valuations d'un $\mathbf{Q}_p$-espace vectoriel* V *de dimension finie, il existe un nombre $c \in \mathbf{R}$ tel que*

$$|w(x) - w'(x)| \leqslant c \quad \textit{pour tout } x \in V.$$

(2.3.3) *Lemme. — Soient* V *un $\mathbf{Q}_p$-espace vectoriel de dimension finie d, et* G *un pro-p-groupe qui opère continûment sur* V. *Alors* G *laisse stable un sous-$\mathbf{Z}_p$-module compact de rang d de* V. *Un tel sous-module est libre de rang d sur $\mathbf{Z}_p$.*

Preuve. — L'espace V est un Al G-module topologique (II, 2.2.6), l'algèbre Al G est compacte, et, si $(x_i)_{1\leqslant i\leqslant d}$ est une base de V sur $\mathbf{Q}_p$, le sous-Al G-module $\sum_{1\leqslant i\leqslant d} \mathrm{Al\,G}.x_i$ est compact de rang d.

(2.3.4) *Lemme. — Soit* G *un pro-p-groupe opérant continûment sur un* $\mathbf{Z}_p$*-module* M, *libre de rang d. Alors il existe une valuation w de* M *et une constante* $b\geqslant d^{-1}$, *telles que*

$$w(x.y-y)\geqslant w(y)+b \tag{2.3.4.1}$$

pour tous $x\in \mathrm{G}$ *et* $y\in \mathrm{M}$.

Preuve. — Le groupe G opère continûment sur M/pM, et tout G-module topologique fini simple est isomorphe à $\mathbf{F}_p$ (où G opère trivialement).

Si nous « remontons » une suite de Jordan-Hölder du G-module M/pM, nous obtenons une base $(e_i)_{0\leqslant i<d}$ de M vérifiant les relations

$$xe_i-e_i\in \sum_{0\leqslant j\leqslant i} p\mathbf{Z}_p.e_j+\sum_{i<j<d}\mathbf{Z}_p.e_j \tag{2.3.4.2}$$

pour tout $x\in \mathrm{G}$.

Nous vérifions les conclusions du lemme en prenant les e_i comme *base filtrée* de M, avec

$$w(e_i)=id^{-1} \qquad \text{pour } 0\leqslant i<d. \tag{2.3.4.3}$$

Remarque. — En faisant opérer convenablement le pro-p-groupe $\mathbf{Z}_p$ sur M, on voit qu'il est parfois impossible d'obtenir la relation (2.3.4.1) avec une constante $b>d^{-1}$.

(2.3.5) *Notations.* — Reprenons et complétons les notations de (2.2.1). Nous désignons par G un groupe p-valué complet de rang r, dans lequel nous avons choisi une base ordonnée $(x_i)_{1\leqslant i\leqslant r}$. Les coordonnées de deuxième espèce par rapport à cette base nous permettent d'identifier G à $\mathbf{Z}_p^r$; c'est ainsi que nous pourrons parler *d'applications analytiques d'ordre h* de G dans un module M (III, 1.3.7). Nous posons

$$\omega(x_i)=\tau_i, \qquad \text{pour } 1\leqslant i\leqslant r; \tag{2.3.5.1}$$

$$t=\min_{1\leqslant i\leqslant r}\tau_i, \tag{2.3.5.2}$$

$$t'=\max_{1\leqslant i\leqslant r}\tau_i. \tag{2.3.5.3}$$

Nous appelons $\mathrm{X}_\bullet$ le *complexe standard complété* de G, et nous reprenons les notations de (1.2.7). Pour chaque $n\in\mathbf{N}^*$, X_n possède une base topologique sur l'anneau A = Al G formé des éléments z^α, où $\boldsymbol{\alpha}$ parcourt J^n.

Nous notons $\mathrm{Y}_\bullet$ le *complexe quasi-minimal* de G, défini en (2.2.2). Pour chaque $n\in\mathbf{N}$, Y_n est un A-module filtré-libre admettant une base $\mathscr{B}_n$ formée de $\binom{r}{n}$ éléments.

Rappelons que $\mathrm{X}_0=\mathrm{Y}_0=\mathrm{A}$.

Les complexes $X_\bullet$ et $Y_\bullet$ sont deux *résolutions acycliques complètes-libres de* $\mathbf{Z}_p$ par des A-modules. Il existe donc (1.1.5) deux *morphismes* de A-*complexes filtrés* (1.1.1)

(2.3.5.4) $$\varphi : X_\bullet \to Y_\bullet,$$

(2.3.5.5) $$\psi : Y_\bullet \to X_\bullet,$$

dont les composés sont homotopes à l'identité.

Il nous suffira d'introduire l'homotopie $h : X_\bullet \to X_\bullet$ ou, plus précisément, la famille de *morphismes* de A-*modules filtrés* :

(2.3.5.6) $$h_n : X_n \to X_{n+1} \qquad (n \in \mathbf{N}),$$

qui vérifient

(2.3.5.7) $$\psi_n \circ \varphi_n - 1 = d_{n+1} \circ h_n + h_{n-1} \circ d_n.$$

Nous notons enfin M un $\mathbf{Z}_p$-*module sans torsion de rang fini sur lequel* G *opère continûment*, et nous supposons M *muni d'une valuation.*

(2.3.6) *Proposition.* — *Conservons les notations de* (2.3.5).

(2.3.6.1) *Il existe un nombre* $a > 0$ *et un nombre* $c \in \mathbf{R}$ *tels que*

$$w(M; x.y) \geqslant aw(A; x) + w(M; y) + c$$

pour tout $x \in A$ *et tout* $y \in M$. *Ces nombres a et c une fois choisis, nous notons* h_0 *le plus petit entier* $h \in \mathbf{N}$ *vérifiant*

$$at > (p-1)^{-1} p^{-h}.$$

(2.3.6.2) *Pour tout* $y \in M$, *l'application* $x \mapsto x.y$ *de* G *dans* M *est analytique d'ordre* $\geqslant h_0$ (III, 1.3.7).

(2.3.6.3) *Pour tout entier* $h \geqslant h_0$, *les cochaînes de* G *dans* M *analytiques d'ordre* $\geqslant h$ *constituent un sous-complexe.*

(2.3.6.4) *Pour tout* $f \in \mathrm{Hom}_A(Y_n, M)$, *la n-cochaîne associée à* $f \circ \varphi_n$ *est analytique d'ordre* $\geqslant h_0$.

(2.3.7) *Preuve de* (2.3.6.1). — D'après le lemme (2.3.3), le groupe G laisse invariant un sous-module M′ de M isomorphe à $\mathbf{Z}_p^d$. Il nous suffit de prouver (2.3.6.1) pour les éléments $y \in M'$. De plus, d'après (2.3.2.1) nous pouvons prendre n'importe quelle valuation sur M (ou M′), quitte à modifier la constante c. Nous supposons donc que la valuation de M′ vérifie le lemme (2.3.4), pour une certaine constante $b > 0$.

Posons, pour tout $x \in A$,

(2.3.7.1) $$w'(x) = \inf_{y \in M} (w(M; x.y) - w(M; y)).$$

Alors w' est une filtration de la $\mathbf{Z}_p$-algèbre A : cf. (I, 2.2.4.1). Le lemme (2.3.4) équivaut à la relation

(2.3.7.2) $$w'(x-1) \geqslant b \qquad \text{pour tout } x \in G.$$

Nous en déduisons

(2.3.7.3) $$w'(z^\alpha) \geqslant |\alpha| b \qquad \text{pour tout } \alpha \in J.$$

Comme d'autre part

(2.3.7.4) $$|\alpha| \geqslant \tau\alpha/t',$$

nous avons

(2.3.7.5) $$w'(z^\alpha) \geqslant (b/t')w(\mathrm{A}; z^\alpha).$$

Si nous posons

(2.3.7.6) $$a = \min(1, b/t'),$$

nous avons

(2.3.7.7) $$w'(x) \geqslant aw(\mathrm{A}; x),$$

pour tout $x \in \mathrm{A}$. C'est l'énoncé de (2.3.6.1) pour $c = 0$.

(2.3.8) *Fin de la preuve de* (2.3.6). — Si $x \in \mathrm{G}$ est donné par ses coordonnées $\lambda \in \mathbf{Z}_p^r$, nous avons, pour $y \in \mathrm{M}$,

(2.3.8.1) $$x.y = \sum_{\alpha \in \mathrm{J}} \binom{\lambda}{\alpha} z^\alpha.y.$$

Nous obtenons, d'après (2.3.6.1),

(2.3.8.2) $$w(\mathrm{M}; z^\alpha.y) \geqslant a(\tau\alpha) + w(\mathrm{M}; y) + c.$$

Comme $\tau\alpha \geqslant t|\alpha|$, le critère d'analyticité (III, 1.3.8) démontre l'assertion (2.3.6.2).

Rappelons que l'application $\mathrm{G} \times \mathrm{G} \to \mathrm{G}$, définie par le produit, est analytique stricte (III, 3.1.7), c'est-à-dire analytique d'ordre 0. Si nous prenons une n-cochaîne f, analytique d'ordre $\geqslant h$, cela prouve que tous les termes de son cobord δf, défini en (1.2.3.1), sont analytiques d'ordre $\geqslant h$, sauf éventuellement le premier terme : $x_1 f(x_2, \ldots, x_{n+1})$. Or ce dernier point résulte de (2.3.6.2).

Soit enfin $f \in \mathrm{Hom}_\mathrm{A}(\mathrm{Y}_n, \mathrm{M})$. La n-cochaîne associée à $f \circ \varphi_n$ est donnée, en fonction des coordonnées $\boldsymbol{\lambda}$ de $\mathbf{x} \in \mathrm{G}^n$, par la formule :

(2.3.8.3) $$\sum_{\alpha \in \mathrm{J}^n} \binom{\boldsymbol{\lambda}}{\boldsymbol{\alpha}} c_\alpha,$$

où

(2.3.8.4) $$c_\alpha = f(\varphi_n(z^\alpha)).$$

Comme φ_n est un *morphisme de* A-*modules filtrés*, nous avons, pour tout $\boldsymbol{\alpha} \in \mathrm{J}^n$,

(2.3.8.5) $$\varphi_n(z^\alpha) = \sum_{y \in \mathscr{B}_n} d_{\alpha,y}.y,$$

où

(2.3.8.6) $$d_{\alpha,y} \in \mathrm{A}, \quad \textit{et}$$

(2.3.8.7) $$w(\mathrm{A}; d_{\alpha,y}) + w(\mathrm{Y}_n; y) \geqslant \tau\boldsymbol{\alpha}.$$

Nous obtenons ainsi

(2.3.8.8) $$c_\alpha = \sum_{y \in \mathscr{B}_n} d_{\alpha,y}.f(y).$$

Les relations (2.3.6.1) et (2.3.8.7) conduisent aux inégalités

(2.3.8.9) $$w(\mathrm{M}; c_\alpha) \geqslant at|\boldsymbol{\alpha}| + c',$$

où

(2.3.8.10) $$c' = \min_{y \in \mathscr{B}_n} (w(\mathrm{M}; f(y)) - aw(\mathrm{Y}_n; y) + c).$$

La relation (2.3.8.9), valable pour tout $\boldsymbol{\alpha} \in \mathrm{J}^n$, prouve (2.3.6.4) d'après le critère d'analyticité.

(2.3.9) *Remarques.* — La constante a qui apparaît dans (2.3.6.1) est toujours $\leqslant 1$ (sauf si $\mathrm{M} = 0$). Comme l'application $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$ est bilinéaire et continue, l'existence d'une *norme* pour les applications *multilinéaires continues* d'espaces vectoriels normés *réels* pourrait faire croire qu'on peut toujours prendre $a = 1$. Il n'en est rien, comme le montre la remarque de (2.3.4).

La propriété (2.3.6.2) montre que toute représentation continue de G dans un $\mathbf{Z}_p$-module libre de rang fini est analytique. Nous le savions déjà, d'après (III, 3.2.3.1).

(2.3.10) *Théorème. — Soit* G *un groupe profini p-analytique* (III, 3.2.2) *opérant continûment sur un* $\mathbf{Z}_p$*-module sans torsion* M *de rang fini. Alors les cochaînes analytiques de* G *dans* M *forment un sous-complexe du complexe des cochaînes continues, et les applications canoniques des groupes de cohomologie analytique dans les groupes de cohomologie continue sont des isomorphismes.*

Preuve. — Nous allons démontrer ce théorème pour un groupe *p-valuable* G (III, 3.1.6). Nous supposons que G est p-valué, que M est valué, et nous appliquons (2.3.6).

Les cochaînes analytiques forment un sous-complexe du complexe des cochaînes continues, d'après (2.3.6.3). Nous avons donc des groupes de *cohomologie analytique* $\mathrm{H}^*_a(\mathrm{G}, \mathrm{M})$, et des homomorphismes canoniques

(2.3.10.1) $$\mathrm{H}^*_a(\mathrm{G}, \mathrm{M}) \to \mathrm{H}^*_c(\mathrm{G}, \mathrm{M}).$$

D'après (2.3.5.7) et (2.3.6.4), *un n-cocycle continu f est cohomologue au n-cocycle analytique* $f \circ \psi_n \circ \varphi_n$. Cela prouve que les applications (2.3.10.1) sont *surjectives*.

Pour montrer qu'elles sont *injectives*, nous devons prouver qu'un n-cocycle analytique f, qui est le cobord d'une $(n-1)$-cochaîne continue, est aussi le cobord d'une $(n-1)$-cochaîne analytique. D'après (2.3.5.7) et (2.3.6.4), il nous suffit de montrer que, *pour toute n-cochaîne analytique f, la* $(n-1)$*-cochaîne* $f \circ h_{n-1}$ *est analytique.*

La n-cochaîne f est définie au moyen des éléments

(2.3.10.2) $$f(z^{\boldsymbol{\alpha}}) = c_\alpha, \qquad \boldsymbol{\alpha} \in \mathrm{J}^n.$$

D'après (III, 1.3.9), l'analyticité de f équivaut à l'existence de deux nombres réels $c_1 > 0$ et c_2, tels que

(2.3.10.3) $$w(\mathrm{M}; c_\alpha) \geqslant c_1|\boldsymbol{\alpha}| + c_2,$$

pour tout $\boldsymbol{\alpha} \in \mathrm{J}^n$.

L'application h_{n-1} est définie par les formules

$$h_{n-1}(z^{\beta}) = \sum_{\alpha \in J^n} e_{\beta,\alpha} z^{\alpha}, \tag{2.3.10.4}$$

avec $e_{\beta,\alpha} \in A$ pour tous $\boldsymbol{\beta} \in J^{n-1}$, $\boldsymbol{\alpha} \in J^n$, et

$$w(A;\, e_{\beta,\alpha}) + \tau\boldsymbol{\alpha} \geqslant \tau\boldsymbol{\beta}. \tag{2.3.10.5}$$

La cochaîne $f \circ h_{n-1}$ est donc définie par

$$(f \circ h_{n-1})(z^{\beta}) = c'_{\beta} = \sum_{\alpha \in J^n} e_{\beta,\alpha} c_{\alpha} \tag{2.3.10.6}$$

pour tout $\boldsymbol{\beta} \in J^{n-1}$.

Si nous appliquons (2.3.6.1), nous obtenons

$$w(M;\, c'_{\beta}) \geqslant \min_{\alpha \in J^n} (aw(A;\, e_{\beta,\alpha}) + w(M;\, c_{\alpha}) + c). \tag{2.3.10.7}$$

Posons, pour tous $\boldsymbol{\alpha} \in J^n$ et $\boldsymbol{\beta} \in J^{n-1}$,

$$u_{\alpha,\beta} = aw(A;\, e_{\beta,\alpha}) + w(M;\, c_{\alpha}) + c. \tag{2.3.10.8}$$

Pour un $\boldsymbol{\beta} \in J^{n-1}$ fixé, considérons d'abord les $\boldsymbol{\alpha} \in J^n$ vérifiant $\tau\boldsymbol{\alpha} \geqslant \tau\boldsymbol{\beta}$. La relation (2.3.10.5) ne nous apprend rien et nous la remplaçons par

$$w(A;\, e_{\beta,\alpha}) \geqslant 0. \tag{2.3.10.9}$$

Comme $\tau\boldsymbol{\alpha} \geqslant \tau\boldsymbol{\beta}$ implique $|\boldsymbol{\alpha}| \geqslant (t/t')|\boldsymbol{\beta}|$, les relations (2.3.10.3) et (2.3.10.8) nous donnent

$$u_{\alpha,\beta} \geqslant (c_1 t/t')|\boldsymbol{\beta}| + c_2 + c. \tag{2.3.10.10}$$

Supposons maintenant que $\tau\boldsymbol{\alpha} = \theta\tau\boldsymbol{\beta}$, avec $0 \leqslant \theta < 1$. Nous obtenons, à partir de (2.3.10.3), (2.3.10.5) et (2.3.10.8) :

$$u_{\alpha,\beta} \geqslant a(1-\theta)t|\boldsymbol{\beta}| + \theta(tc_1/t')|\boldsymbol{\beta}| + c_2 + c. \tag{2.3.10.11}$$

Nous minorons le second membre de (2.3.10.11) en remplaçant θ soit par 1 (et nous retrouvons (2.3.10.10)), soit par 0, ce qui donne

$$u_{\alpha,\beta} \geqslant at|\boldsymbol{\beta}| + c_2 + c. \tag{2.3.10.12}$$

Si nous posons

$$c'_1 = \min(at,\, c_1 t/t'), \tag{2.3.10.13}$$

$$c'_2 = c_2 + c, \tag{2.3.10.14}$$

nous avons $c'_1 > 0$ et

$$w(M;\, c'_{\beta}) \geqslant c'_1|\boldsymbol{\beta}| + c'_2, \tag{2.3.10.15}$$

pour tout $\boldsymbol{\beta} \in J^{n-1}$. Cela prouve l'analyticité de la $(n-1)$-cochaîne $f \circ h_{n-1}$ (III, 1.3.9).

Nous étendrons la démonstration aux groupes profinis p-analytiques quelconques en (3.2.8).

(2.4) Cohomologie de groupes et cohomologie d'algèbres de Lie.

(2.4.1) *L'algèbre de Lie d'un groupe analytique sur* $\mathbf{Q}_p$. — Nous n'avons utilisé qu'une seule fois (III, 3.2.1) la notion *d'espace tangent* en un point à une variété analytique sur $\mathbf{Q}_p$. Il nous faut maintenant définir *l'algèbre de Lie d'un groupe analytique sur* $\mathbf{Q}_p$ (III, 3.1.1). Reconnaissons que la définition la plus simple s'obtiendrait en transcrivant l'une quelconque des définitions classiques de l'algèbre de Lie d'un groupe analytique sur le corps $\mathbf{R}$: voir, par exemple, [5], chap. IV, § 2.

L'algèbre de Lie d'un groupe analytique sur $\mathbf{Q}_p$ est donc une $\mathbf{Q}_p$*-algèbre de Lie.*

Des difficultés se présentent lorsqu'on veut étendre au cas p-adique la théorie de *l'application exponentielle* (*ibid.*, § 8). Si G est un pro-p-groupe analytique (de dimension >0) et L son algèbre de Lie, l'application exponentielle ne peut être définie que sur un voisinage de zéro dans L et non pas sur L tout entière. De plus, il n'est pas toujours possible de définir sans ambiguïté une application exponentielle « maximale », comme le montre l'exemple suivant.

Le groupe G est le pro-p-groupe *commutatif* engendré par deux générateurs x_1 et x_2 liés par la relation $x_1^p = x_2^p$. Nous pouvons identifier L à $\mathbf{Q}_p$. L'application exponentielle

$$p\mathbf{Z}_p \to \mathrm{G} \tag{2.4.1.1}$$

est alors définie par la formule

$$\lambda \mapsto x_1^\lambda = x_2^\lambda. \tag{2.4.1.2}$$

Nous pouvons *prolonger cette application à* $\mathbf{Z}_p$ *de différentes manières* (raisonnables), par exemple en appliquant $\lambda \in \mathbf{Z}_p$ sur x_1^λ *ou* x_2^λ.

Ces remarques ont pour but de justifier auprès du lecteur la définition suivante (2.4.2) de l'algèbre de Lie d'un groupe analytique.

(2.4.2) *Définition de l'algèbre de Lie d'un groupe analytique sur* $\mathbf{Q}_p$ *au moyen des sous-groupes p-saturables.* — Rappelons qu'à tout groupe *p-saturable* G (III, 3.1.6) nous avons associé une $\mathbf{Z}_p$-algèbre de Lie, que nous noterons désormais Log G. Nous renonçons à identifier G à Log G, comme nous l'avions fait en (IV, 3.2.6) et (IV, 3.4.4). Par contre nous nous permettrons d'appeler Log aussi bien le *foncteur* qui transforme G en Log G que le *morphisme fonctoriel* qui, pour chaque G, définit la bijection

$$\mathrm{Log} : \mathrm{G} \to \mathrm{Log}\,\mathrm{G}. \tag{2.4.2.1}$$

Si nous avons un *monomorphisme*

$$f : \mathrm{G} \to \mathrm{G}' \tag{2.4.2.2}$$

de groupes p-saturables de *même dimension*, nous en déduisons un *monomorphisme*

$$\mathrm{Log} f : \mathrm{Log}\,\mathrm{G} \to \mathrm{Log}\,\mathrm{G}' \tag{2.4.2.3}$$

de $\mathbf{Z}_p$-algèbres de Lie qui sont des *$\mathbf{Z}_p$-modules libres de même rang*. En construisant les produits tensoriels par $\mathbf{Q}_p$, nous obtenons une *bijection*

$$\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \operatorname{Log} G \to \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \operatorname{Log} G' \tag{2.4.2.4}$$

(que nous n'osons pas noter $\mathbf{Q}_p \otimes \operatorname{Log} f$) *de $\mathbf{Q}_p$-algèbres de Lie.*

Rappelons enfin (III, 3.1.3) qu'un groupe G, analytique sur $\mathbf{Q}_p$, admet comme système fondamental de voisinages de l'unité l'ensemble de ses *sous-groupes ouverts p-saturables.*

(2.4.2.5) *Définition. — Soit* G *un groupe analytique sur* $\mathbf{Q}_p$. *Associons à chaque sous-groupe ouvert p-saturable* H *de* G *la* $\mathbf{Q}_p$*-algèbre de Lie* $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \operatorname{Log} H$, *que nous noterons* L_H. *Si* H *et* H′ *sont deux tels sous-groupes de* G, *avec* $H \subset H'$, *nous avons* (2.4.2.4) *une bijection canonique* $L_H \to L_{H'}$. *Nous appelons algèbre de Lie de* G *la limite projective*

$$L = \varprojlim L_H \tag{2.4.2.6}$$

des algèbres L_H, *construite sur l'ensemble des sous-groupes ouverts p-saturables, ordonnés par anti-inclusion.*

Les morphismes canoniques

$$L \to L_H \tag{2.4.2.7}$$

sont donc tous des *bijections.*

(2.4.2.8) Lorsque G est un *pro-p-groupe analytique* (ou, plus généralement, un groupe compact analytique sur $\mathbf{Q}_p$), la limite projective (2.4.2.6) peut être construite sur l'ensemble des sous-groupes ouverts p-saturables *distingués* dans G, ainsi qu'il résulte du lemme suivant.

(2.4.3) *Lemme. — Soient* G *un groupe compact analytique sur* $\mathbf{Q}_p$, H *un sous-groupe fermé p-valué de* G *et* ω *la filtration de* H. *Notons* H′ *l'intersection des conjugués de* H *dans* G *et posons, pour tout* $x \in H'$,

$$\omega'(x) = \inf_{y \in G} \omega(yxy^{-1}). \tag{2.4.3.1}$$

Alors H′ *est un sous-groupe fermé distingué de* G *et* ω' *une p-valuation de* H′ *invariante par* G.

Si H *est ouvert dans* G, *il en est de même de* H′ *et, pour tout nombre* ν *assez grand, le sous-groupe* H'_ν (*formé des* $x \in H'$ *vérifiant* $\omega'(x) \geq \nu$) *est un sous-groupe p-saturable ouvert distingué dans* G.

Preuve. — Les applications $x \mapsto \omega(yxy^{-1})$ sont des p-valuations du sous-groupe distingué fermé H′ de G. Comme G est compact et ω continue (en tant qu'application dans $\overline{\mathbf{R}}$), la borne inférieure (2.4.3.1) est atteinte en un certain $y \in G$ (l'élément $x \in H'$ étant fixé). Nous avons donc

$$\omega'(x) > (p-1)^{-1} \tag{2.4.3.2}$$

pour tout $x \in H'$, ce qui prouve que ω' est une p-valuation (III, 2.1.2).

Si H est ouvert, il est d'indice fini dans G, ainsi que H'. La dernière assertion résulte de (III, 3.1.13).

(2.4.4) *Lemme. — Soit* G *un groupe profini* p*-analytique opérant continûment sur un* $\mathbf{Z}_p$*-module libre de rang fini* M. *Alors il existe un sous-groupe ouvert* U *de* G *qui possède la propriété suivante.*

Soient H *un sous-groupe de* U *et* ω *une filtration de* H, *pour laquelle ce groupe est* p*-saturé. Construisons l'algèbre saturée* Sat Al H *de l'algèbre* Al H, *valuée comme en* (III, 2.3.3). *Alors la structure de* (Al H)*-module de* M *se prolonge univoquement en une structure de* (Sat Al H)*-module topologique.*

Preuve. — Munissons M d'une valuation pour laquelle ce module est saturé. Si nous avons

$$w(\mathrm{M}; x.y) \geqslant w(\mathrm{M}; y) + w(\mathrm{Al\,H}; x) \tag{2.4.4.1}$$

pour tout $x \in \mathrm{Al\,H}$ et tout $y \in \mathrm{M}$, l'opération de Al H sur M se prolonge à div Al H, puis, par continuité, à Sat Al H.

Reprenons les notations de la proposition (2.3.6). La relation (2.4.4.1) n'est autre (après remplacement de G par H) que la relation (2.3.6.1), avec $c=0$ et $a=1$. Comme H est p-saturé, le nombre t' (2.3.5.3) vérifie

$$t' \leqslant p(p-1)^{-1}. \tag{2.4.4.2}$$

D'après (2.3.7.6), la relation (2.4.4.1) est donc vérifiée si nous avons

$$w(\mathrm{M}; x.y-y) \geqslant w(\mathrm{M}; y) + p(p-1)^{-1} \tag{2.4.4.3}$$

pour tout $x \in \mathrm{H}$ et tout $y \in \mathrm{M}$. Or cette dernière relation est vraie pour tout x assez voisin de l'élément neutre de G.

(2.4.5) *Lemme. — Soit* L *une* $\mathbf{Q}_p$*-algèbre de Lie de dimension* r *opérant sur un* $\mathbf{Q}_p$*-espace vectoriel* M *de dimension finie. Soit* L^0 *un sous-*$\mathbf{Z}_p$*-module de* L, *libre de rang* r. *Alors, pour tout entier* h *assez grand,* $p^h\mathrm{L}^0$ *est une sous-*$\mathbf{Z}_p$*-algèbre de Lie* L' *de* L *et* L' *peut être munie d'une valuation* w, *de telle sorte que l'opération de* UL' *sur* M *se prolonge en une opération continue de* Sat UL' (IV, 2.2.5).

(2.4.6) *Représentations de groupes et d'algèbres de Lie : « dérivation » et « intégrations ».* — Le lemme (2.4.4) nous montre que, si un pro-p-groupe analytique G opère continûment sur un $\mathbf{Z}_p$-module sans torsion M de rang fini, alors l'algèbre de Lie L de G opère sur $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{M}$: c'est *la* représentation « infinitésimale » associée à celle de G.

Le lemme (2.4.5) nous montre que, si l'algèbre de Lie L opère sur M, il en est de même du pro-p-groupe analytique exp L', où L' désigne une sous-$\mathbf{Z}_p$-algèbre de Lie ouverte assez petite de L. Ce sont *les* représentations « intégrales » associées à celle de L.

Pour éviter les ambiguïtés, nous préférons parler de A-modules, A désignant une $\mathbf{Z}_p$*-algèbre diagonale saturée normale* (IV, 3.1.5). Rappelons que, si nous posons $\mathrm{L} = \mathscr{L}^*\mathrm{A}$ et $\mathrm{G} = \mathscr{G}^*\mathrm{A}$, l'algèbre A s'identifie à Sat UL ainsi qu'à Sat $\mathbf{Z}_p[\mathrm{G}]$. Un A-module M est donc (par restrictions) un *module de représentation pour le groupe* G *et pour l'algèbre de Lie* L.

(2.4.7) *Lemme. — Soient* Ω *un anneau de valuation* (I, 2.2.6), K *le corps des fractions de* Ω, A *une* Ω*-algèbre associative valuée* (I, 2.2.4) *et* M *un* A*-module filtré-libre* (I, 2.1.16) *de rang fini.*

Construisons la Ω*-algèbre saturée* Sat A *et le* Sat A*-module* Sat M (I, 2.2.11). *Notons* B *la* K*-algèbre*

$$B = K \otimes_\Omega \operatorname{Sat} A. \tag{2.4.7.1}$$

Alors les modules $K \otimes_\Omega \operatorname{Sat} M$ *et* $B \otimes_A M$ *sont canoniquement isomorphes.*

Preuve. — Rappelons comment nous avons construit Sat A en (I, 2.2.8) et (I, 2.2.11). Nous avons pris l'algèbre $A' = K \otimes_\Omega A$. Les éléments de A′ s'écrivent sous la forme $\lambda^{-1} \otimes x$, avec $\lambda \in \Omega$, $\lambda \neq 0$ et $x \in A$. Nous avons prolongé la valuation de A en une application de A′ dans $\mathbf{R}$ (*et non plus dans* $\mathbf{R}_+$) définie par

$$w(A'; \lambda^{-1} \otimes x) = w(A; x) - v(\lambda). \tag{2.4.7.2}$$

Les éléments $y \in A'$ vérifiant

$$w(A'; y) \geqslant 0 \tag{2.4.7.3}$$

constituent l'algèbre div A (I, 2.2.8), et nous obtenons Sat A en complétant div A (I, 2.2.11).

Nous vérifions que l'algèbre B (2.4.7.1) s'identifie à la *complétée* $\hat{A}'$ de l'algèbre A′ pour la topologie définie par w (c'est-à-dire la topologie où div A est une sous-algèbre ouverte de A′).

Puisque le foncteur Sat, ainsi que les produits tensoriels, permutent aux sommes directes *finies*, nous pouvons supposer que M est un A-module possédant la base filtrée $\{e\}$, avec $w(M; e) = t$. Nous avons construit div M en prenant, dans le module $A'.e$ les éléments $x.e$ vérifiant

$$w(A'; x) + t \geqslant 0. \tag{2.4.7.4}$$

Nous obtenons Sat M en complétant div M. Cela équivaut à prendre le sous-module de $\hat{A}'.e$ formé des éléments $x.e$ vérifiant

$$w(\hat{A}'; x) + t \geqslant 0. \tag{2.4.7.5}$$

L'assertion du lemme résulte alors de l'identification des deux modules $K \otimes_\Omega \operatorname{Sat} M$ et $B \otimes_A M$ au $\hat{A}'$-module libre $\hat{A}'.e$.

Remarquons que Sat M n'est pas nécessairement un Sat A-module de type fini.

(2.4.8) *Lemme. — Soient* $\mathbf{\Omega}$ *un anneau de valuation complet,* K *le corps des fractions de* Ω, A *une* Ω*-algèbre supplémentée valuée* (I, 2.2.4). *Notons* B *la* K*-algèbre supplémentée* $B = K \otimes_\Omega \operatorname{Sat} A$. *Supposons qu'il existe une résolution filtrée scindée de* Ω *par un complexe* $X_\bullet$ *de* A*-modules filtrés-libres de rangs finis* (1.1.4). *Alors les hypothèses du « mapping theorem »* ([4], p. 150) *sont vérifiées par* A *et* B (*pour l'injection canonique de* A *dans* B).

Plus précisément, nous pouvons considérer le complexe $B \otimes_\Omega X_\bullet$ *comme une résolution scindée* *de* K *par des* B-*modules libres de rangs finis. Nous en déduisons, pour chaque* B-*module* M, *un isomorphisme canonique*

(2.4.8.1) $$H^*(B, M) \to H^*(A, M).$$

Preuve. — Le complexe Sat $X_\bullet$ (1.1.2) est une résolution scindée de Sat $\Omega = \Omega$ (pour les opérateurs Sat s, Sat η, avec les notations de (1.1.4)). En tensorisant par K sur Ω, nous obtenons une résolution scindée de K : $K \otimes_\Omega \mathrm{Sat}\, X_\bullet$. Or, d'après les hypothèses sur $X_\bullet$ et le lemme (2.4.7), $B \otimes_A X_\bullet$ s'identifie à $K \otimes_\Omega \mathrm{Sat}\, X_\bullet$.

Si M est un B-module, les complexes $\mathrm{Hom}_B^\bullet(B \otimes_A X_\bullet, M)$ et $\mathrm{Hom}_A^\bullet(X_\bullet, M)$ s'identifient.

Leurs groupes de cohomologie s'identifient respectivement à $H^*(B, M)$ et $H^*(A, M)$.

(2.4.9) *Théorème.* — *Soit* G *un groupe p-valué complet de rang fini. Sa* $\mathbf{Z}_p$*-algèbre complétée* Al G *est valuée comme en* (III, 2.3.3), *et nous pouvons identifier l'algèbre de Lie* L *de* G (2.4.2) *à*

(2.4.9.1) $$L = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} (\mathscr{L}\, \mathrm{Sat\, Al}\, G).$$

Soit M *un* $\mathbf{Q}_p$*-espace vectoriel muni d'une structure de* (Sat Al G)*-module topologique complet. Alors les groupes de cohomologie continue de* G *à valeurs dans* M (1.2.6)

(2.4.9.2) $$H_c^*(G, M)$$

s'identifient canoniquement aux groupes de cohomologie de L *à valeurs dans* M

(2.4.9.3) $$H^*(L, M).$$

Les opérations de G *et de* L *sur* M *sont définies naturellement à partir de l'opération de* Sat Al G.

Preuve. — Posons

(2.4.9.4) $$B = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} (\mathrm{Sat\, Al}\, G).$$

Nous allons appliquer deux fois le lemme (2.4.8). Nous prenons $\Omega = \mathbf{Z}_p$, $K = \mathbf{Q}_p$.

Posons d'abord $A = \mathrm{Al}\, G$. Alors l'existence d'un complexe quasi-minimal de G (2.2.2) montre que les hypothèses de (2.4.8) sont vérifiées par $A = \mathrm{Al}\, G$. Comme un B-module n'est pas autre chose qu'un $\mathbf{Q}_p$-espace vectoriel où opère Sat Al G, nous identifions $H^*(A, M)$ à $H^*(B, M)$. Or $H_c^*(G, M)$ s'identifie (1.2.6) à $H^*(A, M)$.

Prenons maintenant $A = UL^0$, où L^0 est la $\mathbf{Z}_p$-algèbre de Lie valuée $\mathscr{L}$ Sat Al G. Alors Sat Al G s'identifie à Sat A, car Sat Al G est une algèbre diagonale saturée normale (IV, 3.1.5 et 3.3.6), qui s'identifie d'ailleurs à Sat Al Sat G (IV, 3.3.1). D'après (1.3.6) et (1.3.7), l'algèbre $A = UL^0$ vérifie les hypothèses du lemme (2.4.8). Nous identifions ainsi $H^*(B, M)$ à $H^*(UL^0, M)$, donc à $H^*(UL, M)$ puisque M est un $\mathbf{Q}_p$-espace vectoriel. Or $H^*(UL, M)$ est, par définition, $H^*(L, M)$.

(2.4.10) *Théorème.* — *Soit* G *un groupe profini p-analytique* (III, 3.2.2) *opérant continûment sur un* $\mathbf{Q}_p$*-espace vectoriel* M *de dimension finie. Alors l'algèbre de Lie* L *de* G (2.4.2) *opère sur* M (2.4.6). *Définissons les groupes de cohomologie stable de* G *à valeurs dans* M, $H_{st}^*(G, M)$, *en posant, pour chaque* $n \in \mathbf{N}$,

(2.4.10.1) $$H_{st}^n(G, M) = \varinjlim H_c^n(H, M).$$

La limite inductive est calculée sur l'ensemble des sous-groupes ouverts H *de* G, *ordonnés par anti-inclusion. Les morphismes sont définis par la restriction de la cohomologie.*

Le groupe G *opère sur lui-même à gauche par automorphismes intérieurs, et opère sur* M. *Ces deux opérations définissent l'opération de* G *sur tout ce qui est canoniquement attaché à la structure constituée par* G *et le* G-*module* M, *en particulier* $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})$.

Nous avons les propriétés suivantes :

(i) $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})$ *s'identifie canoniquement à* $\mathrm{H}^*(\mathrm{L}, \mathrm{M})$.

(ii) *Le morphisme canonique*

$$\mathrm{H}^*_c(\mathrm{H}, \mathrm{M}) \to \mathrm{H}^*(\mathrm{L}, \mathrm{M}), \tag{2.4.10.2}$$

déduit de l'isomorphisme (i), *est un isomorphisme dès que le sous-groupe ouvert* H *est assez petit. Plus précisément l'application* (2.4.10.2) *est un isomorphisme si* H *est p-valuable et si, pour une p-valuation convenable de* H, *l'opération continue de* Al H *sur* M *se prolonge en une opération continue de* Sat Al H.

(iii) *Le stabilisateur de* $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})$ *dans* G *est un sous-groupe ouvert, et les groupes de cohomologie continue* $\mathrm{H}^*_c(\mathrm{G}, \mathrm{M})$ *s'identifient aux groupes des points fixes* $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})^{\mathrm{G}}$ *de* $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})$ *pour l'opération de* G.

Preuve. — D'après le lemme (2.4.4), nous pouvons appliquer le théorème (2.4.9) dès que H est assez petit. Nous prouvons ainsi (i) et (ii).

Prenons pour H un sous-groupe ouvert *distingué* de G, assez petit pour que (2.4.10.2) soit un isomorphisme. Alors G opère sur H par restriction des automorphismes intérieurs, et opère donc sur tout ce qui est attaché à H et M, en particulier sur $\mathrm{H}^*_c(\mathrm{H}, \mathrm{M})$. Les opérations de G sur $\mathrm{H}^*_c(\mathrm{H}, \mathrm{M})$ et $\mathrm{H}^*(\mathrm{L}, \mathrm{M})$ permutent à l'isomorphisme (2.4.10.2).

Or nous avons la suite spectrale de Hochschild-Serre (3.2.6.4)

$$\mathrm{H}^r(\mathrm{G}/\mathrm{H}, \mathrm{H}^s_c(\mathrm{H}, \mathrm{M})) \Rightarrow \mathrm{H}_c(\mathrm{G}, \mathrm{M}) \tag{2.4.10.3}$$

(r désigne le degré filtrant). Comme les groupes $\mathrm{H}^*_c(\mathrm{H}, \mathrm{M})$ sont des $\mathbf{Q}_p$-espaces vectoriels et que G/H est fini, la suite spectrale (2.4.10.3) dégénère et se réduit à

$$\begin{aligned} \mathrm{H}^n_c(\mathrm{G}, \mathrm{M}) &= \mathrm{H}^0(\mathrm{G}/\mathrm{H}, \mathrm{H}^n_c(\mathrm{H}, \mathrm{M})) \\ &= \mathrm{H}^n_c(\mathrm{H}, \mathrm{M})^{\mathrm{G}} \\ &= \mathrm{H}^n_{st}(\mathrm{G}, \mathrm{M})^{\mathrm{G}}. \end{aligned} \tag{2.4.10.4}$$

En particulier, le stabilisateur de $\mathrm{H}^*_{st}(\mathrm{G}, \mathrm{M})$ dans G contient le sous-groupe H.

(2.5) Cup-produits et dualité de Poincaré.

(2.5.1) *Cup-produits pour les algèbres diagonales strictes.* — Soient Ω un anneau commutatif, et A une Ω-algèbre diagonale stricte (IV, 1.1.1) dont nous notons Δ l'application diagonale.

Grâce à l'application Δ, chaque $(\mathrm{A}\otimes_\Omega \mathrm{A})$-module possède une structure de A-module. En particulier, si M et M′ sont deux A-modules, le $(\mathrm{A}\otimes \mathrm{A})$-module $\mathrm{M}\otimes_\Omega \mathrm{M}'$ devient un A-module.

Donnons-nous trois A-modules M, M′ et N, ainsi qu'une *application* A-*linéaire de* $M \otimes_\Omega M'$ *dans* N (nous noterons $m * m' \in N$ l'image de $m \otimes m' \in M \otimes M'$). Pour tous $r, s \in \mathbf{N}$ nous avons des *applications bilinéaires*

$$H^r(A, M) \times H^s(A, M') \to H^{r+s}(A, N) \tag{2.5.1.1}$$

appelées *cup-produits* ([4], chap. XI). Rappelons la définition du cup-produit.

Soit $X_\bullet$ une *résolution acyclique de* Ω *par des* A-*modules libres* (ou projectifs). Construisons le complexe (1.3.1)

$$Y_\bullet = X_\bullet \otimes_\Omega X_\bullet. \tag{2.5.1.2}$$

Nous obtenons une *résolution acyclique de* Ω *par des* $(A \otimes_\Omega A)$-*modules libres* (ou projectifs). Au moyen de Δ, $Y_\bullet$ peut être considérée comme une résolution acyclique de Ω par des A-modules, et nous en déduisons un morphisme de A-complexes sur Ω :

$$D : X_\bullet \to X_\bullet \otimes X_\bullet = Y_\bullet. \tag{2.5.1.3}$$

Soient $\xi \in H^r(A, M)$ et $\eta \in H^s(A, M)$, représentés respectivement par les cocycles $f : X_r \to M$ et $g : X_s \to M'$. Il est commode de considérer f (resp. g) comme une application de $X = \coprod_{n \in \mathbf{N}} X_n$ dans M (resp. M′) nulle sur X_n pour $n \neq r$ (resp. $n \neq s$). Nous définissons l'application A-linéaire

$$h : X \otimes X \to N \tag{2.5.1.4}$$

en posant

$$h(x \otimes x') = f(x) * g(x'). \tag{2.5.1.5}$$

Alors $h \circ D_{r+s} : X_{r+s} \to N$ est un $(r+s)$-cocycle dont la classe est le cup-produit $\xi \cup \eta \in H^{r+s}(A, N)$. Cette définition est indépendante des choix de $X_\bullet$, D, f et g.

(2.5.2) *Cas des groupes.* — Soient G un groupe et $A = \Omega[G]$ l'algèbre diagonale stricte associée (IV, 1.1.2). Alors M, M′ et N sont des Ω-modules où opère G, et nous devons avoir

$$x.(m * m') = (x.m) * (x.m'), \tag{2.5.2.1}$$

pour tous $x \in G$, $m \in M$ et $m' \in M'$.

Si nous désignons par $X_\bullet$ le complexe standard (1.2.1) ou le complexe standard normalisé (1.2.2) de A, nous avons une application D (2.5.1.3) définie par les formules (cf. [4], p. 221)

$$D(x_0 \otimes x_1 \ldots \otimes x_n) = \sum_{0 \leqslant i \leqslant n} (x_0 \otimes x_1 \ldots \otimes x_i) \otimes ((x_0 x_1 \ldots x_i) \otimes x_{i+1} \ldots \otimes x_n), \tag{2.5.2.2}$$

pour tous $x_0, x_1, \ldots, x_n \in G$.

Le cup-produit peut être défini au moyen du produit des cochaînes (1.2.3). Si f (resp. g) est une r-cochaîne (resp. s-cochaîne), $h = f \cup g$ est la $(r+s)$-cochaîne définie par

$$h(x_1, \ldots, x_{r+s}) = f(x_1, \ldots, x_r) * (x_1 \ldots x_r) . g(x_{r+1}, \ldots, x_{r+s}). \tag{2.5.2.3}$$

(2.5.3) *Cas des algèbres de Lie.* — Soient L une Ω-algèbre de Lie et $A = UL$ l'algèbre diagonale stricte associée (IV, 1.1.3). Alors M, M', N sont des Ω-modules où opère L, et nous devons avoir

(2.5.3.1) $$x.(m*m') = (x.m)*m' + m*(x.m'),$$

pour tous $x \in L$, $m \in M$ et $m' \in M'$.

Supposons que L soit un Ω-module libre de rang fini. Notons X le complexe standard de L (1.3.4), considéré comme Ω-*algèbre associative graduée*. Formons le produit tensoriel anticommutatif (cf. [4], p. 164)

(2.5.3.2) $$Y = X \otimes_\Omega X.$$

Si $x \in X_r$, $x' \in X_s$, nous avons

(2.5.3.3) $$x \otimes x' = (-1)^{rs} x' \otimes x$$

dans l'algèbre associative graduée Y.

Or Y s'identifie au complexe standard de l'algèbre de Lie $L \amalg L$ (somme directe de deux copies de L). Comme le complexe standard est un foncteur covariant de l'algèbre de Lie, l'application diagonale de L dans $L \amalg L$ définit le morphisme

(2.5.3.4) $$D : X \to X \otimes_\Omega X = Y.$$

Cette application nous donne le morphisme de complexes cherché (2.5.1.3).

En particulier, si

(2.5.3.5) $$M = M' = N = \Omega,$$

le complexe des cochaînes $\mathrm{Hom}^{\bullet}_\Omega(EL, \Omega)$ s'identifie, pour la multiplication définie par le cup-produit, à l'algèbre extérieure EL^* du dual $L^* = \mathrm{Hom}_\Omega(L, \Omega)$ de L.

Si l'algèbre L est *abélienne*, la différentielle du complexe EL^* est nulle, et l'*algèbre de cohomologie* $H^*(L, \Omega)$ *s'identifie canoniquement à* EL^*.

(2.5.4) *Cup-produits pour la cohomologie continue des groupes topologiques, des pro-p-groupes et des groupes p-valuables.* — Reprenons les notations de (2.5.2). Supposons que G soit un groupe topologique, opérant continûment sur les modules topologiques M, M', N, et que l'application bilinéaire $M \times M' \to N$ soit continue. Alors la formule (2.5.2.3) montre que le cup-produit de deux cochaînes continues est une cochaîne continue.

Soient G un pro-p-groupe, et $X_\bullet$ son complexe standard complété (1.2.8). La formule (2.5.2.2) et la proposition (I, 3.2.11) nous permettent de définir l'application

(2.5.4.1) $$\dot{D} : X_\bullet \to X_\bullet \hat{\otimes}_{\mathbf{Z}_p} X_\bullet,$$

par passage aux limites projectives, à partir des complexes standard des quotients finis G/U.

Si G opère continûment sur les $\mathbf{Z}_p$-modules complets M, M', N et si l'application linéaire $M \otimes M' \to N$ est continue, l'application D définit, d'après (1.2.6), un cup-produit

(2.5.4.1) $$H^*_c(G, M) \times H^*_c(G, M') \to H^*_c(G, N).$$

Ce cup-produit coïncide avec celui défini par les cochaînes continues et la formule (2.5.2.3). La preuve de cette assertion procède comme en (1.2.9).

Lorsque G est un groupe p-valué complet de rang fini, son complexe standard complété est valué (1.2.5). Plus précisément, si A désigne l'algèbre Al G, le complexe standard complété $X_\bullet$ de G est une racl (résolution acyclique complète-libre) de $\mathbf{Z}_p$ par des A-modules. Le complexe $X_\bullet \hat{\otimes}_{\mathbf{Z}_p} X_\bullet$ est une racl de $\mathbf{Z}_p$ par des $(A\hat{\otimes}A)$-modules. L'algèbre A est une *algèbre diagonale valuée* au sens de (IV, 1.2.3) et l'application diagonale Δ applique A dans $A\hat{\otimes}_{\mathbf{Z}_p}A$. D'après (1.1.5.1) et (I, 3.2.10), l'application

$$D : X_\bullet \to X_\bullet \hat{\otimes}_{\mathbf{Z}_p} X_\bullet$$

est un *morphisme de* A-*complexes filtrés, qui est défini à une homotopie près par la structure d'algèbre diagonale de* A.

(2.5.5) *Exercice.* — Énoncer et démontrer le complément au théorème (2.4.9) qui affirme la compatibilité des identifications avec les cup-produits. Compléter de même le théorème (2.4.10). Montrer en particulier que l'*algèbre de cohomologie* $H_c^*(G, \mathbf{Q}_p)$ s'identifie canoniquement à la *sous-algèbre des points fixes par* G *de* $H^*(L, \mathbf{Q}_p)$.

(2.5.6) *Calcul du cup-produit au moyen du complexe quasi-minimal; application aux groupes équi-p-valués.* — Soient G un groupe p-valué complet de rang fini et $X_\bullet$ un complexe quasi-minimal de G (2.2.2). Notons A l'algèbre Al G et $Y_\bullet = \operatorname{gr} X_\bullet$ le complexe gradué associé à $X_\bullet$. Par définition du complexe quasi-minimal, $Y_\bullet$ est le *complexe standard* (1.3.4) *de la* Γ-*algèbre de Lie* gr G.

Lorsque deux complexes sont homotopiquement équivalents, il en est de même de leur produit tensoriel ([21], p. 164). Le complexe quasi-minimal $X_\bullet$ de G peut donc nous servir à calculer les cup-produits pour la cohomologie continue au moyen d'un produit tensoriel complété, tout comme le complexe standard complété de G utilisé en (2.5.4).

Construisons donc le produit tensoriel $X_\bullet \otimes X_\bullet$, et complétons-le pour obtenir le complexe de $(A\hat{\otimes}A)$-modules $X_\bullet \hat{\otimes} X_\bullet$. Considérons ce dernier comme un complexe de A-modules, grâce à l'application diagonale $\Delta : A \to A\hat{\otimes}A$.

Nous cherchons un *morphisme de* A-*complexes filtrés* (1.1.1)

(2.5.6.1) $$D^X : X_\bullet \to X_\bullet \hat{\otimes}_{\mathbf{Z}_p} X_\bullet,$$

au-dessus des augmentations naturelles de ces complexes. D'après le lemme (2.1.5) nous pouvons nous donner $\operatorname{gr} D^X$, pourvu que ce morphisme de complexes gradués soit compatible avec les augmentations. Or la complétion ne modifie pas le gradué associé, et nous avons (I, 3.2.1) un isomorphisme canonique de $\operatorname{gr}(X_\bullet \hat{\otimes} X_\bullet)$ avec $Y_\bullet \otimes_\Gamma Y_\bullet$. Nous pouvons donc supposer que

(2.5.6.2) $$\operatorname{gr} D^X = D^Y,$$

où

(2.5.6.3) $$D^Y : Y_\bullet \to Y_\bullet \otimes_\Gamma Y_\bullet$$

est le morphisme défini en (2.5.3.4) pour le calcul du cup-produit de la cohomologie des algèbres de Lie.

Supposons maintenant que tous les éléments d'une base ordonnée de G ont la même filtration t, c'est-à-dire que G est *équi-p-valué* au sens de (2.2.7).

Pour chaque $s \in \mathbf{N}$, X_s est un A-module filtré-libre de rang $\binom{r}{s}$, r désignant le rang de G, et les générateurs de X_s ont tous la même filtration st.

Le complexe $\mathrm{Hom}_A^\bullet(X_\bullet, \mathbf{F}_p)$ a une différentielle nulle, et les groupes de cohomologie $H_c^s(G, \mathbf{F}_p)$ s'identifient aux groupes de cochaînes $\mathrm{Hom}_A(X_s, \mathbf{F}_p)$, ou encore aux espaces vectoriels $(\mathrm{gr}_{st} X_s)^*$ (où nous notons M^* le dual d'un $\mathbf{F}_p$-espace vectoriel M).

Les relations (2.5.6.1) à (2.5.6.3) nous permettent de déterminer la *structure d'algèbre* de $H_c^*(G, \mathbf{F}_p)$.

En effet, soit L la $\mathbf{F}_p$-algèbre de Lie $\mathrm{gr}\, G/\pi.\mathrm{gr}\, G$ (rappelons que π est le terme dominant de $p \in \mathbf{Z}_p$ dans $\Gamma = \mathrm{gr}\, \mathbf{Z}_p$). C'est une *algèbre de Lie abélienne et son rang sur* $\mathbf{F}_p$ *est r*. Notons $Z_\bullet$ le complexe standard de L (1.3.4). L'épimorphisme canonique de gr G sur L se prolonge en un *épimorphisme de complexes*

(2.5.6.4) $$f : Y_\bullet \to Z_\bullet,$$

et, si $D^Z : Z_\bullet \to Z_\bullet \otimes_{\mathbf{F}_p} Z_\bullet$ est l'application (2.5.3.4) correspondant à L, nous avons un diagramme commutatif.

(2.5.6.5)
$$\begin{tikzcd} Y_\bullet \arrow[r, "D^Y"] \arrow[d, "f"] & Y_\bullet \otimes_\Gamma Y_\bullet \arrow[d, "f\otimes f"] \\ Z_\bullet \arrow[r, "D^Z"] & Z_\bullet \otimes_{\mathbf{F}_p} Z_\bullet \end{tikzcd}$$

L'application $f_s : Y_s \to Z_s$ est injective sur la composante homogène de degré st de Y_s, et nulle sur les autres composantes homogènes.

L'identification de $H_c^s(G, \mathbf{F}_p)$ à $(\mathrm{gr}_{st} X_s)^*$ permet d'identifier ce même groupe à $Z_s^* = H^s(L, \mathbf{F}_p)$ et *l'identification de* $H_c^*(G, \mathbf{F}_p)$ *à* $H^*(L, \mathbf{F}_p)$ *est compatible avec les structures d'algèbres.*

(2.5.7) *Dualité de Poincaré.* — Notre dernier résultat peut s'énoncer comme suit.

(2.5.7.1) *Proposition. — Soit* G *un groupe équi-p-valué* (2.2.7) *de rang r. Alors l'algèbre de cohomologie* $H_c^*(G, \mathbf{F}_p)$ *s'identifie à l'algèbre extérieure de* $H_c^1(G, \mathbf{F}_p)$, *qui est un* $\mathbf{F}_p$*-espace vectoriel de dimension r.*

Il en résulte que G est *un groupe de Poincaré de dimension r*, au sens de [29], chap. Ier, 4.5. Recopions la définition. Le *pro-p-groupe* G est dit groupe de Poincaré de dimension r si

(i) $H^s(G) = H_c^s(G, \mathbf{F}_p)$ *est fini pour tout* $s \in \mathbf{N}$.

(ii) $\dim_{\mathbf{F}_p} H^r(G) = 1$.

(iii) *Le cup-produit* $H^s(G) \times H^{r-s}(G) \to H^r(G)$ *est une forme bilinéaire non dégénérée pour tout* $s \in \mathbf{N}$.

Ces hypothèses entraînent, d'après Serre et Tate, une « *dualité de Poincaré* » (*ibid.*, proposition 30).

Il existe sur le groupe additif $\mathbf{Q}_p/\mathbf{Z}_p$ *une structure de* G-*module topologique, soit* I, *possédant la propriété suivante.*

Le groupe $H^r_c(G, I)$ *est isomorphe à* $\mathbf{Q}_p/\mathbf{Z}_p$. *Si* M *est un p-groupe additif fini sur lequel* G *opère continûment, et si nous posons*

$$\widetilde{M} = \mathrm{Hom}_{\mathbf{Z}}(M, I), \tag{2.5.7.2}$$

le cup-produit

$$H^s_c(G, M) \times H^{r-s}_c(G, \widetilde{M}) \to H^r_c(G, I) \tag{2.5.7.3}$$

met en dualité les deux groupes finis $H^s_c(G, M)$ *et* $H^{r-s}_c(G, \widetilde{M})$ *pour tout* $s \in \mathbf{N}$.

Rappelons qu'il s'agit de la « dualité de Pontrjagin » des p-groupes additifs finis. Si l'application de $M \times \widetilde{M}$ dans I est notée $(m|\widetilde{m})$, l'opération de G sur $\widetilde{M}$ est définie par

$$x.(m|\widetilde{m}) = (x.m|x.\widetilde{m}), \tag{2.5.7.4}$$

pour tous $x \in G$, $m \in M$, $\widetilde{m} \in \widetilde{M}$.

(2.5.7.5) *Tout sous-groupe ouvert d'un groupe de Poincaré est un groupe de Poincaré de même dimension* (*ibid.*, Corollaire, p. 1, 51). — Le « *module dualisant* » I pour un sous-groupe ouvert de G s'obtient par restriction des scalaires.

(2.5.7.6) *Proposition (Serre-Tate-Verdier); cf.* [29], *chap.* V, *prop.* 4.7). — *Si un pro-p-groupe* G *est de dimension cohomologique finie et contient un sous-groupe ouvert de Poincaré, alors* G *est un groupe de Poincaré.*

(2.5.8) *Théorème.* — *Soit* G *un pro-p-groupe analytique* (III, 3.1.2) *de dimension r et de dimension cohomologique finie. Alors* G *est un groupe de Poincaré de dimension r.*

Si, pour tout $x \in G$, *nous notons* $\mathrm{Ad}(x)$ *l'automorphisme de l'algèbre de Lie* L *de* G (2.4.2.5) *induit par l'automorphisme intérieur* $(y \mapsto xyx^{-1})$ *de* G, *l'opération de x sur le module dualisant* I *de* G *est la multiplication par*

$$\chi(x) = \det \mathrm{Ad}(x). \tag{2.5.8.1}$$

Preuve. — La première assertion résulte de (2.5.7.1) et (2.5.7.6), puisque tout pro-p-groupe analytique contient des sous-groupes ouverts qui peuvent être équi-p-valués (III, 3.1.3).

Le *module dualisant* I de G est le groupe additif $\mathbf{Q}_p/\mathbf{Z}_p$ muni d'une certaine structure de G-module, c'est-à-dire d'un *homomorphisme de* G *dans le groupe des automorphismes de* $\mathbf{Q}_p/\mathbf{Z}_p$. Ce dernier groupe s'identifie canoniquement au groupe $\mathbf{U}_p$ des *unités p-adiques* (éléments inversibles de $\mathbf{Z}_p$). Tout revient donc à déterminer l'homomorphisme

$$\chi : G \to \mathbf{U}_p. \tag{2.5.8.2}$$

La donnée de χ permet de faire opérer G sur d'autres groupes additifs que $\mathbf{Q}_p/\mathbf{Z}_p$, par exemple sur $\mathbf{Q}_p$. Le lemme suivant, conséquence de la « dualité de Poincaré », donne une caractérisation de χ.

(2.5.8.3) *Lemme. — Soient* G *un pro-p-groupe de Poincaré de dimension* r *et* M *un* $\mathbf{Q}_p$*-espace vectoriel de dimension* 1. *Supposons que* G *opère continûment sur* M, *l'opération étant donnée par l'homomorphisme* $\chi' : \mathrm{G} \to \mathbf{U}_p$. *Alors* $\mathrm{H}^r_c(\mathrm{G}, \mathrm{M}) \neq 0$ *si et seulement si* $\chi' = \chi$.

Ce lemme nous permettra d'appliquer le théorème (2.4.10). Rappelons quelques résultats concernant les algèbres de Lie. Soit L une Ω-algèbre de Lie, qui est un Ω-module libre de rang r. Nous avons défini la *représentation adjointe* de L sur EL (1.3.4). L'opération d'un $x \in \mathrm{L}$ sur $\mathrm{E}^r\mathrm{L}$ est la *multiplication par* $\mathrm{Tr}\,\mathrm{ad}\,x$ (trace de l'endomorphisme $y \mapsto [x, y]$ du module L). D'autre part, avec les notations de (1.3.4.8), nous avons

$$(2.5.8.4) \qquad d(e_1^* \dots e_r^*) = \sum_{1 \leqslant i \leqslant r} (-1)^i ((\mathrm{Tr}\,\mathrm{ad}\,e_i) - e_i) e_1^* \dots e_{i-1}^* e_{i+1}^* \dots e_r^*,$$

si $\{e_1, \dots, e_r\}$ est une base de L sur Ω. Les r-cochaînes de L à valeurs dans un L-module M s'identifient aux éléments de $\mathrm{Hom}_\Omega(\mathrm{E}^r\mathrm{L}, \mathrm{M})$. Si $\mathrm{M} = \mathrm{E}^r\mathrm{L}$, la formule (2.5.8.4) montre que les r-cobords sont nuls, et nous avons un isomorphisme *canonique* de $\mathrm{H}^r(\mathrm{L}, \mathrm{E}^r\mathrm{L})$ avec Ω, l'élément basique privilégié étant la classe du r-cocycle défini par l'*application identique de* $\mathrm{E}^r\mathrm{L}$ *sur lui-même.*

Si Ω est un corps, et M un Ω-espace vectoriel de dimension 1, alors $\mathrm{H}^r(\mathrm{L}, \mathrm{M}) \neq 0$ si et seulement si M est isomorphe à $\mathrm{E}^r\mathrm{L}$.

Reprenons les notations du théorème (2.4.10). Comme la classe fondamentale de L correspond à l'application identique de $\mathrm{E}^r\mathrm{L}$, cette classe est invariante par l'opération de G. Il reste à vérifier que l'opération de G sur $\mathrm{E}^r\mathrm{L}$ est bien la multiplication par $\det \mathrm{Ad}(x)$. Cela résulte de (IV, 3.2.7).

3. LE HOCHSCHILD-SERRE SELON C. T. C. WALL

(3.1) Complexes de Wall.

(3.1.1) *Complexes doubles et complexes de Wall.* — Soient A un anneau et $\mathrm{X}_{i,j}$ une famille de A-modules; les indices i et j parcourent $\mathbf{Z}$, *mais* $\mathrm{X}_{i,j} = 0$ *pour* $i < 0$ *ou* $j < 0$. Définissons les modules X_n comme les *sommes directes* (finies)

$$(3.1.1.1) \qquad \mathrm{X}_n = \coprod_{i+j=n} \mathrm{X}_{i,j}, \qquad \text{pour } n \in \mathbf{Z}.$$

Pour obtenir un complexe de chaînes $\mathrm{X}_\bullet$, il ne nous manque plus que la différentielle d, c'est-à-dire la famille des $d_n : \mathrm{X}_n \to \mathrm{X}_{n-1}$. D'après (3.1.1.1) la donnée des d_n équivaut à celle des applications

$$(3.1.1.2) \qquad d_{i,j}^{(k)} : \mathrm{X}_{i,j} \to \mathrm{X}_{i-k,j+k-1},$$

définies comme composées des applications

$$(3.1.1.3)\qquad X_{i,j} \longrightarrow X_{i+j} \xrightarrow{d_{i+j}} X_{i+j-1} \longrightarrow X_{i-k,j+k-1}.$$

En omettant les indices inférieurs, nous pouvons écrire

$$(3.1.1.4)\qquad d = \sum_{k\in\mathbf{Z}} d^{(k)},$$

et la relation $dd=0$ équivaut à la famille de relations

$$(3.1.1.5)\qquad \sum_{h\in\mathbf{Z}} d^{(k-h)} d^{(h)} = 0,$$

pour tout $k\in\mathbf{Z}$. Si nous explicitons complètement cette formule, nous obtenons

$$(3.1.1.6)\qquad \sum_{h\in\mathbf{Z}} d^{(k-h)}_{i-h,j+h-1} \circ d^{(h)}_{i,j} = 0,$$

qui doit être vérifiée pour tous $i, j, k\in\mathbf{Z}$.

La notion usuelle de *complexe double* (de chaînes) s'obtient en supposant $d^{(k)}_{i,j}=0$ pour $k\neq 0, 1$. Nous avons alors ([4], chap. XV) deux filtrations du complexe $X_\bullet$, auxquelles correspondent deux suites spectrales.

(3.1.1.7) *Définition. — Nous appelons complexe de Wall* $X_{\bullet\bullet}$ *la donnée de la famille de* A-*modules* $X_{i,j}$ *et d'applications* A-*linéaires* $d^{(k)}_{i,j}$ (3.1.1.2) *qui sont supposées nulles pour* $k<0$. *Les relations* (3.1.1.5), (3.1.1.6), *que nous supposons vérifiées, se réduisent à*

$$(3.1.1.8)\qquad \sum_{0\leqslant h\leqslant k} d^{(k-h)} d^{(h)} = 0,$$

pour tout $k\in\mathbf{N}$, *c'est-à-dire à*

$$(3.1.1.9)\qquad \sum_{0\leqslant h\leqslant k} d^{(k-h)}_{i-h,j+h-1} \circ d^{(h)}_{i,j} = 0,$$

pour tous $i, j, k\in\mathbf{N}$.

Lorsque A est un anneau gradué (resp. filtré), nous supposons que les $X_{i,j}$ sont des modules gradués (resp. filtrés) et que les $d^{(k)}_{i,j}$ sont des *morphismes* dans la catégorie correspondante.

(3.1.2) *Complexes fibres, filtration et suite spectrale d'un complexe de Wall.* — Si nous posons, pour tous $r, n\in\mathbf{N}$,

$$(3.1.2.1)\qquad F_r X_n = \coprod_{\substack{i+j=n\\ i\leqslant r}} X_{i,j},$$

nous définissons une « *filtration croissante* » du complexe $X_\bullet$, compatible avec sa différentielle, c'est-à-dire telle que $d_n F_r X_n \subset F_r X_{n-1}$.

Plus précisément, le fait que la filtration F soit compatible avec la différentielle équivaut à la nullité des $d^{(k)}_{i,j}$ pour $k<0$, c'est-à-dire caractérise les complexes de Wall.

A la filtration canonique d'un complexe de Wall $X_{\bullet\bullet}$ correspond une suite spectrale ([4], chap. XV). Le « terme E^0 » est donné par

$$(3.1.2.2)\qquad E^0_{i,j} = X_{i,j},$$

et la différentielle d^0 du complexe E^0 s'identifie à $d^{(0)}$.

Nous obtenons ainsi, pour chaque $i \in \mathbf{N}$, un *complexe de chaînes* $X_{i,\bullet}$ pour la différentielle $d^{(0)}_{i,\bullet}$. Ces complexes seront dits les *complexes fibres* du complexe de Wall, et nous écrirons parfois d^f au lieu de $d^{(0)}$.

Le « terme E^1 » de la suite spectrale est donné par l'homologie des complexes fibres. Plus précisément nous avons

(3.1.2.3) $$E^1_{i,j} = H_j(X_{i,\bullet}).$$

La différentielle d^1 du complexe E^1 est définie à partir de $d^{(1)}$, par restriction et passage au quotient, comme dans le cas d'un complexe double.

Bien entendu la suite spectrale « converge » vers l'homologie du complexe $X_\bullet$.

Supposons maintenant vérifiées les relations

(3.1.2.3) $$H_j(X_{i,\bullet}) = 0,$$

pour tout $i \in \mathbf{N}$ et tout $j \in \mathbf{N}^*$. Posons, pour $i \in \mathbf{N}$,

(3.1.2.4) $$H_0(X_{i,\bullet}) = Y_i.$$

Alors nous pouvons considérer chaque complexe fibre $X_{i,\bullet}$ comme une *résolution acyclique du module* Y_i. Munis de la différentielle d^1, *les* Y_i *constituent un complexe* $Y_\bullet$ *que nous appelons le complexe base* (et dont nous notons parfois d^b la différentielle). La suite spectrale est dégénérée, et nous obtenons

(3.1.2.5) $$H_n(X_\bullet) = H_n(Y_\bullet) \quad \textit{pour tout } n \in \mathbf{N}.$$

En particulier, si $Y_\bullet$ est une résolution acyclique d'un module M, il en est de même de $X_\bullet$.

(3.1.3) *Théorème* [32]. — *Soient* A *un anneau gradué (resp. filtré, filtré complet) et* $Y_\bullet$ *un complexe de* A*-modules gradués (resp. filtrés, filtrés complets). Donnons-nous, pour chaque* $i \in \mathbf{N}$, *une résolution acyclique projective (resp. filtrée-libre, complète-libre)* $X_{i,\bullet}$ *du module* Y_i. *Alors il existe un complexe de Wall à suite spectrale dégénérée dont les* $X_{i,\bullet}$ *sont les complexes fibres et* $Y_\bullet$ *le complexe base.*

Preuve. — Nous construisons les applications $d^{(k)}_{i,j}$ dans l'ordre croissant des triplets (k, j, i) que nous ordonnons lexicographiquement. Pour $k=0$, $d^{(0)}$ est formé par les différentielles des complexes fibres :

(3.1.3.1) $$d^{(0)}_{i,j} = d^f_{i,j},$$

pour tous $i, j \in \mathbf{N}$.

Pour $k=1, j=0$, nous devons définir des morphismes $d^{(1)}_{i,0}$ qui rendent commutatifs les diagrammes

(3.1.3.2) $$\begin{tikzcd} X_{i,0} \arrow[r, "d^{(1)}_{i,0}"] \arrow[d, "\varepsilon^f_i"] & X_{i-1,0} \arrow[d, "\varepsilon_{i-1}"] \\ Y_i \arrow[r, "d^b_i"'] & Y_{i-1} \end{tikzcd}$$

C'est possible, d'après les hypothèses du théorème.

Dans la construction des $d_{i,j}^{(k)}$, nous n'avons plus qu'à vérifier les relations (3.2.1.9)

$$(3.1.3.3) \qquad \sum_{0\leqslant h\leqslant k} d_{i-h,j+h-1}^{(k-h)} \circ d_{i,j}^{(h)} = 0.$$

Nous écrivons cette dernière relation sous la forme

$$(3.1.3.4) \qquad d_{i-k,j+k-1}^{f} \circ d_{i,j}^{(k)} = u_{i,j}^{(k)},$$

où le morphisme

$$(3.1.3.5) \qquad u_{i,j}^{(k)} : \mathrm{X}_{i,j} \to \mathrm{X}_{i-k,j+k-2}$$

est construit au moyen des applications $d_{i',j'}^{(k')}$ telles que $(k',j',i')<(k,j,i)$, c'est-à-dire est *donné*, d'après notre hypothèse de récurrence concernant la construction des $d_{i,j}^{(k)}$ et la vérification des relations (3.1.3.3).

D'après les propriétés des résolutions acycliques projectives (resp. filtrées-libres, complètes-libres), l'existence d'un morphisme $d_{i,j}^{(k)}$ vérifiant (3.1.3.4) équivaut à

$$(3.1.3.6) \qquad d_{i-k,j+k-2}^{f} \circ u_{i,j}^{(k)} = 0 \qquad si\ j+k>2,$$

$$(3.1.3.7) \qquad \varepsilon_{i-k}^{f} \circ u_{i,j}^{(k)} = 0 \qquad si\ j+k=2.$$

La relation (3.1.3.7) ne peut se présenter que pour $k=1, j=1$, ou $k=2, j=0$. Si nous explicitons les égalités à vérifier, nous obtenons

$$(3.1.3.8) \qquad \varepsilon_{i-1}^{f} \circ d_{i,0}^{(1)} \circ d_{i,1}^{(0)} = 0,$$

$$(3.1.3.9) \qquad \varepsilon_{i-2}^{f} \circ d_{i-1,0}^{(1)} \circ d_{i,0}^{(1)} = 0,$$

qui résultent des relations de commutation (3.1.3.2).

Il ne nous reste plus qu'à vérifier (3.1.3.6). Nous avons, en omettant les indices inférieurs,

$$(3.1.3.10) \qquad u^{(k)} = -\sum_{1\leqslant h\leqslant k} d^{(h)} d^{(k-h)},$$

et nous voulons vérifier la relation

$$(3.1.3.11) \qquad d^{(0)} u^{(k)} = -\sum_{1\leqslant h\leqslant k} d^{(0)} d^{(h)} d^{(k-h)} = 0,$$

appliquée au module $\mathrm{X}_{i,j}$. D'après notre hypothèse de récurrence sur (k,j), nous pouvons remplacer dans (3.1.3.11) chacun des facteurs $d^{(0)}d^{(h)}$ par

$$(3.1.3.12) \qquad -\sum_{1\leqslant g\leqslant h} d^{(g)} d^{(h-g)} = d^{(0)} d^{(h)}.$$

La relation à vérifier devient ainsi

$$(3.1.3.13) \qquad \sum_{1\leqslant h\leqslant k} \Big(\sum_{1\leqslant g\leqslant h} d^{(g)} d^{(h-g)}\Big) d^{(k-h)} = 0.$$

L'interversion des sommations nous donne le résultat cherché, d'après l'hypothèse de récurrence sur k.

(3.1.4) *Morphismes de complexes de Wall.* — Soient $X_{\bullet\bullet}$ et $\overline{X}_{\bullet\bullet}$ deux complexes de Wall (3.1.1.7) sur un même anneau A. Nous appellerons *morphisme f de $X_{\bullet\bullet}$ dans $\overline{X}_{\bullet\bullet}$* un *morphisme des complexes (simples) associés* :

(3.1.4.1) $$f : X_{\bullet} \to \overline{X}_{\bullet}$$

compatible avec les filtrations (3.1.2.1), c'est-à-dire vérifiant

(3.1.4.2) $$f_n(F_r X_n) \subset F_r \overline{X}_n$$

pour tous $n, r \in \mathbf{N}$. La donnée de f équivaut à celle des morphismes

(3.1.4.3) $$f_{i,j}^{(k)} : X_{i,j} \to \overline{X}_{i-k,j+k},$$

définis comme composés des applications

$$X_{i,j} \longrightarrow X_{i+j} \xrightarrow{f_{i+j}} \overline{X}_{i+j} \longrightarrow \overline{X}_{i-k,j+k}.$$

La compatibilité avec les filtrations se traduit par les relations $f_{i,j}^{(k)} = 0$ pour $k < 0$. La propriété pour f d'être un morphisme de complexes se traduit (en notant $\overline{d}$ la différentielle de $\overline{X}$) par

(3.1.4.4) $$fd = \overline{d}f,$$

c'est-à-dire

(3.1.4.5) $$\sum_{0 \leqslant h \leqslant k} f^{(k-h)} d^{(h)} = \sum_{0 \leqslant h \leqslant k} \overline{d}^{(k-h)} f^{(h)},$$

pour tout $k \in \mathbf{N}$. En explicitant complètement, nous obtenons

(3.1.4.6) $$\sum_{0 \leqslant h \leqslant k} (f_{i-h,j+h-1}^{(k-h)} \circ d_{i,j}^{(h)} - \overline{d}_{i-h,j+h}^{(k-h)} \circ f_{i,j}^{(h)}) = 0,$$

pour tous $i, j, k \in \mathbf{N}$.

Le morphisme f définit un morphisme des suites spectrales de $X_{\bullet\bullet}$ et $\overline{X}_{\bullet\bullet}$. Pour chaque $i \in \mathbf{N}$, nous avons un morphisme des complexes fibres

(3.1.4.7) $$f_{i,\bullet}^{(0)} : X_{i,\bullet} \to \overline{X}_{i,\bullet},$$

que nous noterons parfois f_i^f.

Ces morphismes des complexes fibres doivent vérifier les conditions

(3.1.4.8) $$\overline{\varepsilon}_{i-1}^f \circ (f_{i-1,0}^f \circ d_{i,0}^{(1)} - \overline{d}_{i,0}^{(1)} \circ f_{i,0}^f) = 0,$$

pour tout $i \in \mathbf{N}$, en notant $\overline{\varepsilon}_i^f$ le morphisme canonique

(3.1.4.9) $$\overline{\varepsilon}_i^f : \overline{X}_{i,0} \to H_0(\overline{X}_i^f) = H_0(\overline{X}_{i,\bullet}).$$

(3.1.5) *Proposition. — Soient* $X_{\bullet\bullet}$ *et* $\overline{X}_{\bullet\bullet}$ *deux complexes de Wall sur* A, *que nous supposons gradué (resp. filtré, filtré complet). Supposons que les modules* $X_{i,j}$ *soient projectifs (resp. filtrés-libres, complets-libres), et que les complexes fibres* $\overline{X}_{i,\bullet}$ *soient acycliques (resp. acycliques filtrés, acycliques filtrés complets). Donnons-nous des morphismes des complexes fibres*

$$f_i^f : X_{i,\bullet} \to \overline{X}_{i,\bullet},$$

pour tout $i \in \mathbf{N}$, *vérifiant les conditions* (1.3.4.8). *Alors il existe un morphisme* $f: X_{\bullet\bullet} \to \overline{X}_{\bullet\bullet}$ (3.1.4) *qui induit les morphismes donnés* f_i^f *sur les complexes fibres. Ce morphisme est défini à une homotopie près.*

La preuve procède comme en (3.1.3) : nous construisons les $f_{i,j}^{(1)}$ par récurrence sur le triplet (k, j, i).

(3.1.5.1) *Corollaire. — Reprenons les notations et les hypothèses du théorème* (3.1.3). *Soient* $X_{\bullet\bullet}$ *et* $\overline{X}_{\bullet\bullet}$ *deux structures de complexe de Wall sur la famille des* $X_{i,j}$ *qui vérifient les conditions du théorème. Alors il existe un isomorphisme* $f: X_{\bullet\bullet} \to \overline{X}_{\bullet\bullet}$ *qui induit l'identité sur les complexes fibres* $X_{i,\bullet}$.

(3.1.6) *Choix normaux.* — Reprenons l'énoncé du théorème (3.1.3). Supposons que chaque complexe fibre $X_{i,\bullet}$ soit donné comme *résolution scindée* (1.1.4) de Y_i, et que les modules $X_{i,j}$ soient *libres* (resp. filtrés-libres, complets-libres) avec des *bases* (resp. bases filtrées, bases topologiques) *données*. Alors nous pouvons préciser la construction des $d_{i,j}^{(k)}$ (3.1.3), en effectuant à chaque étape le « *choix normal* » du morphisme $d_{i,j}^{(k)}$, tel que nous l'avons défini en (1.1.6). Nous obtenons ainsi un complexe de Wall *complètement déterminé.*

Supposons, de plus, que le complexe base $Y_\bullet$ soit une *résolution scindée* (1.1.4) *du module* M. Nous allons montrer que *le complexe* $X_\bullet$ *peut être défini comme une résolution scindée de* M.

Nous notons d^f, s^f, ε^f, η^f (resp. d^b, s^b, ε^b, η^b) les opérateurs des complexes fibres (resp. du complexe base). Nous omettons les indices inférieurs. L'augmentation ε^X du complexe $X_\bullet$ est

(3.1.6.1) $$\varepsilon^X = \varepsilon^b \varepsilon^f : X_0 \to M;$$

l'opérateur η^X est

(3.1.6.2) $$\eta^X = \eta^f \eta^b : M \to X_0.$$

Quant à l'opérateur s^X, nous le calculons par application du lemme (1.3.5) à partir d'un opérateur σ qui vérifie

(3.1.6.3) $$(1 - \eta^X \varepsilon^X - d\sigma - \sigma d)(x) \in F_{r-1} X_\bullet,$$

pour tout $r \in \mathbf{N}$ et tout $x \in F_r X_\bullet$. Nous définissons cet opérateur σ par la formule

(3.1.6.4) $$\sigma = s^f - \eta^f s^b \varepsilon^f - s^f d^{(1)} \eta^f s^b \varepsilon^f.$$

(3.2) Extension de groupes.

(3.2.1) *Les complexes de Wall d'une extension de groupes.* — Soient G un groupe, H un sous-groupe distingué de G et Ω un anneau commutatif. Notons respectivement A, B et C les algèbres $\Omega[G]$, $\Omega[H]$ et $\Omega[G/H]$. L'algèbre C est canoniquement isomorphe à $A \otimes_B \Omega$; l'algèbre A est un B-module libre (à gauche ou à droite).

Soit $Z_\bullet$ *une résolution acyclique de* Ω *par des* B-*modules*. Le complexe de A-modules

$$A \otimes_B Z_\bullet \tag{3.2.1.1}$$

est une *résolution acyclique de* C *par des* A-*modules*.

Si les B-modules Z_n sont libres (resp. projectifs), les A-modules $A \otimes_B Z_n$ sont libres (resp. projectifs).

Donnons-nous maintenant une *résolution acyclique libre* $Y_\bullet$ *de* Ω *par des* C-*modules*, et posons, pour tout $n \in \mathbf{N}$

$$Y_n = C \otimes_\Omega \widetilde{Y}_n, \tag{3.2.1.2}$$

où $\widetilde{Y}_n$ est un Ω-*module libre*.

Pour tous $i, j \in \mathbf{N}$, notons $X_{i,j}$ le A-module

$$A \otimes_B Z_j \otimes_\Omega \widetilde{Y}_i = X_{i,j}. \tag{3.2.1.3}$$

Si $Z_\bullet$ est une résolution acyclique *projective* de Ω, les hypothèses du théorème (3.1.3) sont vérifiées lorsque nous prenons comme complexes fibres les complexes

$$A \otimes_B Z_\bullet \otimes_\Omega \widetilde{Y}_i = X_{i,\bullet}. \tag{3.2.1.4}$$

En effet $Y_\bullet$ est un complexe de A-modules grâce à l'épimorphisme $A \to C$, et chaque $X_{i,\bullet}$ est une résolution acyclique projective de Y_i.

Nous obtenons donc un complexe de Wall $X_{\bullet\bullet}$ (3.1.3), dont le *complexe simple associé* $X_\bullet$ (3.1.1) est une *résolution acyclique projective de* Ω *par des* A-*modules*.

Supposons, de plus, que $Z_\bullet$ (resp. $Y_\bullet$) soit une *résolution scindée* de Ω par des B-*modules* (resp. C-*modules*) *libres ayant des bases données*, et donnons-nous une *section* $G/H \to G$ de l'extension de groupes (notée $\xi \mapsto \overline{\xi}$). Nous obtenons $\widetilde{Y}_n$ en prenant le sous-Ω-module de Y_n engendré par la base de ce module sur C. La section nous donne une *base de* A *sur* B, qui nous permet de définir chaque *complexe fibre* $X_{i,\bullet}$ comme une résolution scindée de Y_i. Alors, comme nous l'avons vu en (3.1.6), nous pouvons construire un complexe de Wall *déterminé* qui est une *résolution scindée de* Ω.

(3.2.2) *La suite spectrale de Hochschild-Serre pour la cohomologie des groupes discrets.* — Conservons les notations précédentes. Soit M un A-module. Nous avons, puisque $X_\bullet$ est une résolution acyclique projective de Ω par des A-modules :

$$H^*(G, M) = H^*(A, M) = H^*(\mathrm{Hom}_A^\bullet(X_\bullet, M)). \tag{3.2.2.1}$$

Le complexe $X_\bullet$ est muni de sa « filtration croissante » F (3.1.2). Le complexe $\mathrm{Hom}_A^\bullet(X_\bullet, M)$ possède donc une « filtration décroissante » associée, que nous pouvons noter encore F : le sous-complexe

$$F^r \mathrm{Hom}_A^\bullet(X_\bullet, M) \tag{3.2.2.2}$$

est constitué par les morphismes de $X_\bullet$ dans M qui s'annulent sur $F_r X_\bullet$.

A partir de cette filtration du complexe $\mathrm{Hom}_A^\bullet(X_\bullet, M)$ nous obtenons la *suite spectrale de Hochschild-Serre* [12], comme nous le montrerons par un calcul explicite (3.2.3).

(3.2.2.3) *Exercice.* — Démontrer, à partir de (3.1.5), que le terme E_2 de la suite spectrale est indépendant du choix du complexe de Wall $X_{\bullet\bullet}$.

(3.2.3) *Opération de* G *sur la cohomologie de* G/H; *calculs explicites.* — Le groupe G opère à gauche sur H (par restriction des automorphismes intérieurs) et sur M. Il opère sur les cochaînes de H dans M, selon la formule

$$(xf)(y_1, \ldots, y_n) = xf(x^{-1}y_1x, \ldots, x^{-1}y_nx), \tag{3.2.3.1}$$

pour $x \in G$, $y_1, \ldots, y_n \in H$ et $f : H^n \to M$.

Le groupe G opère sur la cohomologie $H^*(H, M)$. En fait, son sous-groupe H opère trivialement, et le quotient G/H opère sur $H^*(H, M)$. Nous retrouvons ces résultats comme suit.

Notons $Z_\bullet$ le complexe standard de B (avec les notations de (3.2.1)). Puisque M est un A-module, le complexe $\mathrm{Hom}^\bullet_B(Z_\bullet, M)$, dont la cohomologie est $H^*(H, M)$, s'identifie au complexe

$$\mathrm{Hom}^\bullet_A(A \otimes_B Z_\bullet, M). \tag{3.2.3.2}$$

Nous faisons opérer *à droite* G sur le complexe $A \otimes_B Z_\bullet$ en posant, pour

$$u = x_0 \otimes y_1 \otimes \ldots \otimes y_n \in A \otimes_B Z_n = A \otimes_\Omega T^n B, \quad \text{et} \quad x \in G, \tag{3.2.3.3}$$

$$u.x = x_0x \otimes x^{-1}y_1x \otimes \ldots \otimes x^{-1}y_nx. \tag{3.2.3.4}$$

(Les éléments y_i appartiennent à B, auquel nous prolongeons l'automorphisme $y \mapsto x^{-1}yx$ de H.)

Par l'identification de $\mathrm{Hom}_A(A \otimes_B Z_n, M)$ au module des n-cochaînes de H dans M, l'opération à droite de G sur $A \otimes_B Z_\bullet$ (3.2.3.4) conduit à l'opération à gauche de G sur les cochaînes (3.2.3.1).

Si $x \in H$, la formule (3.2.3.4) montre que la multiplication à droite par x définit un *endomorphisme du complexe* $Z_\bullet$ *compatible avec son augmentation*, donc *homotope à l'identité*. Cela prouve que G opère sur $H^*(H, M)$ par l'intermédiaire de G/H.

Prenons comme complexe $Y_\bullet$ le complexe standard de C, avec (3.2.1.2)

$$\widetilde{Y}_n = T^n C. \tag{3.2.3.5}$$

Les modules $X_{i,j}$ de notre complexe de Wall sont donc définis par

$$X_{i,j} = A \otimes_\Omega T^j B \otimes_\Omega T^i C. \tag{3.2.3.6}$$

La différentielle $d^{(0)}$ est définie, comme différentielle des complexes fibres (3.1.2), par le complexe standard de B.

Pour écrire les applications $d^{(1)}$, donnons-nous une *section* $G/H \to G$ (notée $\xi \mapsto \overline{\xi}$). Posons alors, pour tous $i, j \in \mathbf{N}$, $u \in A \otimes_\Omega T^j B$, $\xi_1, \ldots, \xi_i \in G/H$:

(3.2.3.7)
$$(-1)^j d_{i,j}^{(1)}(u \otimes \xi_1 \otimes \ldots \otimes \xi_i) = (u\overline{\xi}_1) \otimes \xi_2 \otimes \ldots \otimes \xi_i + \\ + \sum_{1 \leqslant k < i} (-1)^k u \otimes \xi_1 \otimes \ldots \otimes \xi_k \xi_{k+1} \otimes \ldots \otimes \xi_i + (-1)^i u \otimes \xi_1 \otimes \ldots \otimes \xi_{i-1}.$$

Si nous notons généralement $C^n(K, M)$ le module des n-cochaînes d'un groupe K dans un module M (où K n'opère pas nécessairement) le terme $E_0^{i,j}$ de la suite spectrale s'identifie à

(3.2.3.8)
$$E_0^{i,j} = C^i(G/H, C^j(H, M)).$$

Le terme $E_1^{i,j}$ est donné par

(3.2.3.9)
$$E_1^{i,j} = C^i(G/H, H^j(H, M)),$$

et enfin le terme $E_2^{i,j}$ est

(3.2.3.10)
$$H^i(G/H, H^j(H, M)).$$

Lorsque G est *produit semi-direct* de H et G/H, c'est-à-dire lorsque nous pouvons supposer $\overline{\xi_1\xi_2} = \overline{\xi}_1\overline{\xi}_2$ pour tous $\xi_1, \xi_2 \in G/H$, l'application $d^{(1)}$ définie en (3.2.3.7) vérifie $d^{(1)}d^{(1)} = 0$. Nous posons alors $d^{(k)} = 0$ pour $k > 1$, et notre complexe de Wall est un *complexe double*. Par le choix d'un homomorphisme section de G/H dans G, $A \otimes_B Z_\bullet$ devient un complexe de C-modules à droite, et nous avons

$$X_\bullet = (A \otimes_B Z_\bullet) \otimes_C Y_\bullet.$$

(3.2.4) *Valuation de l'algèbre complétée d'un groupe profini p-analytique.* — Soient G un groupe profini p-analytique (III, 3.2.2), H un sous-groupe ouvert de G et A (resp. B) la $\mathbf{Z}_p$-algèbre complétée Al G (resp. Al H). Nous étendons la définition de Al (II, 2.2.1), si bien que A est encore (II, 2.2.7) un B-module libre de rang fini (G : H), à gauche et à droite.

Supposons maintenant que H soit *p-valuable* (III, 3.1.6) et *distingué* dans G. D'après le lemme (2.4.3), nous pouvons supposer H muni d'une *p-valuation* ω *invariante par* G.

Prenons alors sur A la *borne inférieure* ω *des filtrations d'algèbre qui vérifient*

(3.2.4.1)
$$\omega(x-1) \geqslant \omega(x) \qquad \textit{pour tout } x \in H.$$

Alors la restriction de w à B *est la valuation induite par* ω (III, 2.3.3). *Une famille de représentants* $(\overline{\xi}_i)_{1 \leqslant i \leqslant s}$ *de* G/H *dans* G *est une base filtrée du* B-*module* A *(à gauche ou à droite), avec* $\omega(\overline{\xi}_i) = 0$ *pour* $1 \leqslant i \leqslant s$. *L'algèbre topologique* A *devient ainsi une* $\mathbf{Z}_p$*-algèbre supplémentée valuée complète pour la filtration* w.

En effet, notons w' la valuation du B-module A définie par la valuation de B (III, 2.3.3) et le choix des représentants $(\overline{\xi}_i)$. Nous avons

(3.2.4.2)
$$w'(x) \leqslant w(x) \qquad \text{pour tout } x \in A,$$

et il nous suffit de montrer que w' est compatible avec la structure d'*algèbre* de A, ce qui résulte de l'invariance de ω par G.

(3.2.5) *Complexe standard complété d'un groupe profini p-analytique.* — Conservons les notations de (3.2.4) et construisons le complexe standard (1.2.1) de l'algèbre supplémentée A. Ce complexe standard est *valué* (1.2.4). Son complété, que nous notons $X_\bullet$, est une *résolution acyclique complète-libre (et scindée) de* $\mathbf{Z}_p$ *par des* A-*modules.*

Explicitons les bases topologiques. Reprenons, pour le sous-groupe ouvert distingué H de G, les notations de (1.2.7). Notons $\overline{J}$ l'ensemble produit

(3.2.5.1) $$(G/H)\times J = \overline{J}.$$

Ayant choisi la section $\xi \mapsto \overline{\xi}$ de G/H dans G, posons

(3.2.5.2) $$z^{\overline{\alpha}} = \overline{\xi}.z^{\alpha} \in A$$

pour tout $\overline{\alpha} = (\xi, \alpha) \in \overline{J}$.

Les éléments $z^{\overline{\alpha}}$, $\overline{\alpha} \in \overline{J}$, constituent une *base topologique de* A *sur* $\mathbf{Z}_p$, avec

(3.2.5.3) $$w(A; z^{\overline{\alpha}}) = \tau\overline{\alpha} = \tau\alpha.$$

Nous obtenons, comme en (1.2.7), une *base topologique de* X_n *sur* A en prenant les éléments

(3.2.5.4) $$z^{\overline{\boldsymbol{\alpha}}} = 1 \otimes z^{\overline{\alpha}^1} \otimes \ldots \otimes z^{\overline{\alpha}^n},$$

où $\overline{\boldsymbol{\alpha}} = (\overline{\alpha}^1, \ldots, \overline{\alpha}^n) \in \overline{J}^n$. Nous avons

(3.2.5.5) $$w(X_n; z^{\overline{\boldsymbol{\alpha}}}) = \tau\overline{\boldsymbol{\alpha}}, \qquad \text{avec}$$

(3.2.5.6) $$\tau\overline{\boldsymbol{\alpha}} = \sum_{1 \leqslant j \leqslant n} \tau\overline{\alpha}^j.$$

La proposition (1.2.6) s'étend sans modification. *Si* M *est un* A-*module linéairement topologisé complet, les groupes de cohomologie continue* (1.1.7) $H_c^*(A, M)$ *s'identifient aux groupes de cohomologie continue de* G, $H_c^*(G, M)$.

Les notations que nous avons introduites permettent d'étendre la démonstration exposée en (1.2.7). Une application A-linéaire continue

(3.2.5.7) $$f : X_n \to M$$

est donnée par la famille des éléments

(3.2.5.8) $$c_{\overline{\boldsymbol{\alpha}}} = f(z^{\overline{\boldsymbol{\alpha}}}), \qquad \overline{\boldsymbol{\alpha}} \in \overline{J}^n,$$

qui doivent tendre vers zéro dans M (suivant le filtre des complémentaires des parties finies de $\overline{J}^n$).

Les éléments $c_{\overline{\boldsymbol{\alpha}}}$ nous donnent d'autre part les coefficients de Mahler de la n-cochaîne associée $G^n \to M$, ou, plus précisément, de ses restrictions aux classes à gauche de G^n suivant H^n (ces classes étant identifiées à $\mathbf{Z}_p^{rn}$ par la section de G/H et la base ordonnée de H).

Le critère d'analyticité (III, 1.3.9) nous donne le résultat suivant.

(3.2.5.9) *Soit* M *un* $\mathbf{Z}_p$*-module sans torsion de rang fini sur lequel* G *opère continûment, que nous supposons valué* (2.3.2). *Pour que la n-cochaîne associée à l'application* A*-linéaire* $f: X_n \to M$ *donnée par ses coefficients* $c_{\bar{\alpha}}$ (3.2.5.8) *soit analytique, il faut et il suffit que*

$$\varliminf_{|\bar{\alpha}|\to\infty} \frac{w(c_{\bar{\alpha}})}{|\bar{\alpha}|} > 0.$$

(Nous posons $|\bar{\boldsymbol{\alpha}}| = \sum_j |\bar{\alpha}^j|$ pour $\bar{\boldsymbol{\alpha}} \in \bar{J}^n$, et $|\bar{\alpha}| = |\alpha|$ pour $\bar{\alpha} = (\xi, \alpha) \in \bar{J}$).

(3.2.6) *Résolutions acycliques complètes-libres de* $\mathbf{Z}_p$. — Conservons les notations de (3.2.4) et cherchons comment il convient de modifier les considérations de (3.2.1) pour construire des résolutions acycliques complètes-libres de $\mathbf{Z}_p$ par des A-modules. Nous posons de nouveau $C = \mathbf{Z}_p[G/H]$.

Nous prenons maintenant comme complexe $Z_\bullet$ une *résolution acyclique complète-libre de* $\mathbf{Z}_p$ *par des* B*-modules*. Le complexe $A \otimes_B Z_\bullet$ est formé de A*-modules complets libres* : pour chaque $n \in \mathbf{N}$, une base topologique de Z_n sur B nous donne une base topologique de $A \otimes_B Z_n$ sur A. Le complexe

(3.2.6.1) $$A \otimes_B Z_\bullet$$

est donc une *résolution acyclique complète-libre de* C *par des* A*-modules*.

Nous prendrons comme C-complexe $Y_\bullet$ un complexe dont les modules sont donnés sous la forme

(3.2.6.2) $$Y_n = C \otimes_{\mathbf{Z}_p} \widetilde{Y}_n,$$

où les $\widetilde{Y}_n$ sont des $\mathbf{Z}_p$-modules libres de rangs finis. Chaque $\widetilde{Y}_n$ est valué par sa valuation p-adique (une base sur $\mathbf{Z}_p$ est une base filtrée dont les éléments ont la filtration 0).

Nous construisons enfin les produits tensoriels valués

(3.2.6.3) $$X_{i,j} = (A \otimes_B Z_j) \otimes_{\mathbf{Z}_p} \widetilde{Y}_i,$$

et nous avons satisfait aux conditions du théorème (3.1.3), qui nous donne un complexe de Wall $X_{\bullet\bullet}$ et une résolution acyclique complète-libre $X_\bullet$ de $\mathbf{Z}_p$ par des A-modules.

Si nous prenons pour $Y_\bullet$ (resp. $Z_\bullet$) le complexe standard (resp. complété) de C (resp. B), nous pouvons encore définir l'opération à droite de G sur $A \otimes_B Z_\bullet$ par la formule (3.2.3.4), puis définir $d^{(1)}$ par (3.2.3.7) après avoir choisi une section. Nous obtenons explicitement la suite spectrale

(3.2.6.4) $$H^i(G/H, H^j_c(H, M)) \Rightarrow H^\bullet_c(G, M).$$

(3.2.7) *Théorème.* — *Soit* G *un groupe profini p-analytique* (III, 3.2.2). *Supposons que l'algèbre* $A = \mathrm{Al}\, G$ *soit munie d'une valuation, comme en* (3.2.4). *Alors il existe une résolution acyclique complète-libre de* $\mathbf{Z}_p$ *par des* A*-modules de rangs finis. Pour tout* A*-module linéairement topologisé complet* M, *les groupes* $H^n_c(G, M)$, $H^n_c(A, M)$ *et* $\mathrm{Ext}^n_A(\mathbf{Z}_p, M)$ *s'identifient canoniquement* ($n \in \mathbf{N}$).

Preuve. — Avec les notations de (3.2.6), prenons comme complexe $Z_\bullet$ le *complexe quasi-minimal de* H (2.2.2). Alors Z_n est un B-module filtré-libre de rang $\binom{r}{n}$. Comme nous prenons des $\mathbf{Z}_p$-modules $\widetilde{Y}_n$ libres de rangs finis, les $X_{i,j}$ (3.2.6.3) sont des A-modules filtrés-libres de rangs finis, ainsi que les X_n (3.1.1.1). Les dernières assertions du théorème se prouvent comme en (2.2.3).

(3.2.8) *Fin de la preuve du théorème* (2.3.10). — Nous avons prouvé ce théorème pour un groupe p-valuable G. Nous avons valué l'algèbre $A = \mathrm{Al}\ G$, et nous avons utilisé deux résolutions acycliques complètes-libres de $\mathbf{Z}_p$ par des A-modules : $X_\bullet$ et $Y_\bullet$. Le complexe $X_\bullet$ était le complexe standard complété de l'algèbre supplémentée valuée A. Il nous a servi à *traduire la définition des cochaînes analytiques* et à formuler un *critère d'analyticité*. Le complexe $Y_\bullet$ était le complexe quasi-minimal de G, mais il intervenait par la *seule propriété que les* Y_n *sont des* A-*modules filtrés-libres de rangs finis*. Nous avons étendu toutes ces notions aux groupes profinis p-analytiques généraux en (3.2.4), (3.2.5) et (3.2.7), et nous étendons de même la démonstration du théorème (2.3.10).

APPENDICE

A.1. Commutateurs, puissances et critères d'analyticité dans les pro-p-groupes de type fini.

(1.1) *Définition.* — *Soient* G *un groupe,* n *et* h *deux entiers positifs. Nous noterons*

(1.1.1) $$\mathrm{CP}(\mathrm{G}; n; h)$$

l'assertion suivante :

« *tout commutateur de poids* n *dans le groupe* G *est une* p^h*-ième puissance* ».

Dans la notation $\mathrm{CP}(\mathrm{G}; n; h)$ le nombre premier p est sous-entendu. Quand il n'y aura pas d'équivoque possible sur le groupe G, nous écrirons

(1.1.2) $$\mathrm{CP}(n; h)$$

au lieu de $\mathrm{CP}(\mathrm{G}; n; h)$. Rappelons que les commutateurs de poids n sont définis par récurrence sur n : tout élément de G est un commutateur de poids 1 ; si u et v sont deux commutateurs de poids i et j respectivement, alors $(u, v) = u^{-1}v^{-1}uv$ est un commutateur de poids $(i+j)$.

(1.2) *Théorème.* — *Soit* G *un pro-p-groupe analytique de dimension* r (>0). *Alors il existe un entier* $a \in \mathbf{N}$ *tel que, pour tout* $n \in \mathbf{N}$,

(1.2.1) $$\mathrm{CP}(\mathrm{G}; n; [(n-a)r^{-1}]).$$

Rappelons que le crochet désigne la partie entière.

Preuve. — Appliquons à G le lemme (V, 2.4.3) en partant d'un sous-groupe ouvert p-valué H dont nous supposons la filtration à valeurs entières (III, 3.1.3). Alors, avec les notations de (V, 2.4.3), la valuation invariante ω' du sous-groupe distingué H' est encore à valeurs entières.

Il en résulte que, pour n assez grand, le groupe $\mathrm{H}'_n/\mathrm{H}'_{n+1}$ est abélien élémentaire d'ordre p^r (III, 3.1.13). Soit ν le plus petit entier n pour lequel cette propriété est vérifiée ; posons, pour tout $h \in \mathbf{N}$,

(1.2.2) $$\mathrm{K}_h = \mathrm{H}'_{\nu+h}.$$

Les groupes K_h sont tous distingués dans G et K_h coïncide avec l'*ensemble* des p^h-ièmes puissances des éléments du groupe K_0. Les automorphismes intérieurs de G définissent (par restriction et passage au quotient) des automorphismes des p-groupes abéliens $\mathrm{K}_h/\mathrm{K}_{h+1}$. Nous pouvons intercaler entre K_h et K_{h+1} des sous-groupes distingués K_i, où $i = h + r^{-1}, h + 2r^{-1}, \ldots, h + (r-1)r^{-1}$, de telle sorte que G *opère trivia-*

lement sur les quotients $K_i/K_{i+r^{-1}}$ pour $i=h,\ h+r^{-1}, \ldots, h+(r-1)r^{-1}$: cf. (II, 2.1.7) et (V, 2.3.4).

Il en résulte, par l'identité de P. Hall (II, 1.1.6.3), que, si x est un commutateur de poids n dans G et y un élément de K_i $(i\in r^{-1}\mathbf{N})$, alors le commutateur (x,y) appartient au groupe $K_{i+nr^{-1}}$.

Nous achevons la preuve en définissant a comme le plus petit entier n tel que les commutateurs de poids n dans G appartiennent à K_0.

(1.3) *Exemple.* — Soit Ω l'anneau obtenu en adjoignant à $\mathbf{Z}_p$ une racine p-ième primitive ξ de l'unité. Construisons le *produit semi-direct des groupes additifs*

(1.3.1) $$G=\mathbf{F}_p\times\Omega.$$

L'image canonique $\overline{n}$ dans $\mathbf{F}_p$ d'un élément $n\in\mathbf{Z}$ opère sur le sous-groupe distingué Ω de G en multipliant ses éléments par ξ^n.

Le pro-p-groupe G est de dimension $(p-1)$. C'est un quotient du groupe construit en (III, 3.2.5).

Utilisant les formules (III, 3.2.5.2) et (III, 3.2.5.3) qui restent valables, on voit que l'énoncé du théorème (1.2) est « le meilleur possible ».

(1.4) *Notations.* — Jusqu'à la fin de ce paragraphe, G désignera un pro-p-groupe engendré par des éléments x_i $(1\leqslant i\leqslant r)$ auxquels sont associés des nombres strictement positifs τ_i. Nous posons

(1.4.1) $$t=\max_i \tau_i,$$

(1.4.2) $$\theta=\min_i \tau_i.$$

Le groupe G *est muni de sa* (x,τ,p)*-filtration* (II, 3.2.2), qui se réduit à la (t,p)-filtration (II, 3.2.1) si $t=\theta$. Nous posons $L=\operatorname{gr} G$; rappelons (II, 3.2.4) que L est engendrée, en tant qu'*algèbre de Lie mixte*, par les images canoniques ξ_i des éléments x_i dans les composantes homogènes de L de degrés respectifs τ_i. Nous notons L^* la sous-algèbre de Lie *(non mixte)* de L engendrée par les ξ_i $(1\leqslant i\leqslant r)$. Nous écrivons L_ν (resp. L^*_ν) la composante homogène de L (resp. L^*) de degré ν.

Nous notons $\log_p$ le logarithme de base p et φ la fonction définie en (II, 1.2.2) : $\varphi(\nu)=\min(\nu+1, p\nu)$. Pour $h\in\mathbf{N}$, φ^h désignera la h-ième itérée de φ :

$$\varphi^0(\nu)=\nu, \qquad \varphi^{h+1}(\nu)=\varphi(\varphi^h(\nu)).$$

(1.5) *Lemme.* — (i) *Soit* $m>0$; *si l'on a* $L^*_\nu=0$ *pour tout* ν *vérifiant*

(1.5.1) $$m\leqslant\nu<m+t,$$

alors $L^*_\nu=0$ *pour tout* $\nu\geqslant m$.

(ii) *Si* $t=\theta$, *et si* $L^*_{nt}=0$ *pour un entier* $n>0$, *alors* $L^*_\nu=0$ *pour tout* $\nu\geqslant nt$.

Preuve. — C'est une conséquence du lemme (II, 3.3.3).

(1.6) *Proposition.* — *S'il existe* $m>0$ *tel que* $L^*_\nu=0$ *pour* $m\leqslant\nu<m+t$, *ou si* $t=\theta$ *et s'il existe un entier* $n>0$ *tel que* $L^*_{nt}=0$, *alors* G *est analytique.*

Preuve. — D'après (1.5) et le lemme (II, 3.3.5), les hypothèses de la proposition (III, 3.4.2) sont vérifiées.

(1.7) *Lemme.* — *Soient* ν *un nombre* >0, *et* n, h *deux entiers* $\geqslant 0$. *Alors les relations*

(1.7.1) $$\mathrm{CP}(G; n; h),$$

(1.7.2) $$(n-1)t<\nu\leqslant nt, \quad \textit{et}$$

(1.7.3) $$\varphi^h(\theta)>\nu$$

impliquent

(1.7.4) $$L^*_\nu=0.$$

Preuve. — La composante homogène L^*_ν est engendrée, en tant que groupe additif, par les images modulo $G_{\nu+}$ de certains commutateurs de poids $\geqslant n$: c'est une conséquence de (1.7.2) et de la définition de L^*. D'après (1.7.1) ces commutateurs sont des p^h-ièmes puissances, et leur filtration vaut au moins $\varphi^h(\theta)$.

(1.8) *Critères de nullité de* L^*_ν. — Pour appliquer le lemme précédent nous allons expliciter la condition (1.7.3). *Chacune des relations suivantes implique* (1.7.3) :

(1.8.1) $$h+\theta>\nu.$$

Cette relation vaut quel que soit θ, mais elle peut être améliorée, *sauf si* $\theta\geqslant(p-1)^{-1}$.

(1.8.2) $$p(p-1)^{-1}\geqslant\theta p^h>\nu.$$

Cette relation correspond à la plus rapide croissance de la fonction φ.

(1.8.3) $$\theta<(p-1)^{-1} \quad \textit{et} \quad h-[\log_p(\theta(p-1))^{-1}]-(p-2)(p-1)^{-1}\geqslant\nu.$$

Posons en effet
$$i=1+[\log_p(\theta(p-1))^{-1}],$$
ce qui équivaut à
$$\theta p^{i-1}\leqslant(p-1)^{-1}<\theta p^i.$$
Nous avons alors, pour $h\geqslant i$,
$$\varphi^h(\theta)=\theta p^i+h-i.$$

La relation (1.8.3) peut s'écrire sous la forme
$$h-i\geqslant\nu-(p-1)^{-1}.$$
Comme le premier membre de cette dernière relation est entier et que ν est strictement positif, nous avons bien $h\geqslant i$ et $\varphi^h(\theta)>\nu$.

Lorsque $t=\theta$, nous pouvons remplacer la relation (1.7.2) par
$$\nu=nt,$$
car $L^*_\nu=0$ si ν n'est pas multiple entier de t.

Indiquons encore une relation qui précise un peu (1.8.3) dans un cas particulier.

(1.8.4) $$t=\theta=(p-1)^{-1}p^{-j} \quad \textit{pour un } j\in\mathbf{N}, \quad \textit{et} \quad h>n(p-1)^{-1}p^{-j}+j-(p-1)^{-1}.$$

(1.9) *Théorème. — Pour que* G *soit analytique, il faut et il suffit qu'existent deux entiers n, h tels que*

(1.9.1) $$\mathrm{CP}(G; n; h), \quad et$$

(1.9.2) $$p^h > n.$$

Preuve. — Si G est analytique, le théorème (1.2) nous permet de vérifier (1.9.1) et (1.9.2) dès que n est assez grand. Réciproquement, supposons ces deux relations vérifiées et choisissons $t(=\theta)$ assez petit pour que

$$tp^h \leqslant p(p-1)^{-1}.$$

Alors la proposition (1.6) établit l'analyticité de G, compte tenu du lemme (1.7) et de (1.8.2).

(1.10) *Corollaire. — Supposons le groupe* G *analytique. Alors, pour tout nombre* $m>0$ (*resp.* $m>(p-1)^{-1}$), *les hypothèses de la proposition* (1.6) (*resp. du théorème* (III, 3.4.3)) *sont vérifiées par la* (t, p)*-filtration dès que le nombre t est assez petit.*

(1.11) *Proposition. — Si le groupe* G *est analytique de dimension* r (>0) *et si*

(1.11.1) $$tr<1,$$

alors les hypothèses de la proposition (1.6) *et du théorème* (III, 3.4.3) *sont vérifiées pour tout nombre m assez grand.*

Preuve. — Nous appliquons le critère (1.8.3).

A.2. Filtrations restreintes de groupes et algèbres de Lie restreintes.

(2.1) *Anneaux filtrés de caractéristique p.* — Développons des considérations analogues à celles de (II, 1.2) pour des anneaux de caractéristique p, c'est-à-dire pour des $\mathbf{F}_p$-algèbres associatives.

Soient A un tel anneau, filtré par w, et G un sous-groupe du groupe multiplicatif des éléments inversibles de A, tel que

(2.1.1) $$w(x-1)>0 \quad \textit{pour tout } x\in G.$$

Nous posons

(2.1.2) $$\omega(x)=w(x-1), \quad \textit{pour tout } x\in G$$

et nous obtenons ainsi une *filtration* de G; de plus nous avons une *injection canonique*

(2.1.3) $$\iota : \mathrm{gr}\, G \to \mathrm{gr}\, A$$

de l'algèbre de Lie graduée associée à G dans l'anneau gradué associé à A (II, 1.9.9).

L'identité

(2.1.4) $$x^p-1=(x-1)^p,$$

valable dans tous les anneaux de caractéristique p, entraîne

(2.1.5) $$\omega(x^p) \geqslant p\omega(x) \quad \text{pour tout } x\in G.$$

L'algèbre de Lie gr G possède une structure canonique de $\mathbf{F}_p$-*algèbre de Lie restreinte* au sens de Jacobson [13]. La p-application $(\xi \mapsto \xi^{[p]})$ est définie, pour les éléments *homogènes*, par passage aux quotients à partir de la p-ième puissance dans G. L'injection ι (2.1.3) se prolonge en un homomorphisme

$$\tilde{\iota} : \tilde{\mathrm{U}}\,\mathrm{gr}\,\mathrm{G} \to \mathrm{gr}\,\mathrm{A} \tag{2.1.6}$$

de l'*algèbre enveloppante restreinte* $\tilde{\mathrm{U}}$ gr G *de* gr G dans gr A. Le morphisme d'anneaux gradués (2.1.6) n'est pas nécessairement injectif, ni surjectif.

(2.2) *Définition. — Nous appellerons filtration restreinte d'un groupe* G *une filtration* ω (II, 1.1.1) *qui vérifie l'axiome suivant.*

$$\omega(x^p) \geqslant p\omega(x) \quad \textit{pour tout } x \in \mathrm{G}. \tag{2.2.1}$$

La terminologie correcte serait « filtration p-restreinte ».

Toute filtration restreinte est une p-filtration (II, 1.2.10). Plus précisément, filtrations restreintes et p-filtrations satisfont aux mêmes axiomes tant qu'il ne s'agit que d'éléments de filtration $<(p-1)^{-1}$. En fait, nous pouvons presque ramener l'étude des filtrations restreintes à celle des p-filtrations grâce à la propriété suivante.

Soient ω une filtration restreinte d'un groupe G et t un nombre >0. Alors l'application ω' définie par

$$\omega'(x) = t\omega(x) \quad \text{pour tout } x \in \mathrm{G} \tag{2.2.2}$$

est encore une filtration restreinte.

(2.3) *Théorème. — Soit* G *un groupe muni d'une filtration restreinte* ω (2.2). *Pour tout* $\nu \in \mathbf{R}_+^*$ *et tout* $\xi \in \mathrm{gr}_\nu \mathrm{G}$, *prenons un représentant* x *de* ξ, *puis l'élément* $x^p \in \mathrm{G}_{p\nu}$, *et enfin l'image de* x^p *dans* $\mathrm{gr}_{p\nu}\mathrm{G}$.

Ce dernier élément ne dépend que de ξ; *nous le notons* $\xi^{[p]}$. *L'application* $\xi \mapsto \xi^{[p]}$ *se prolonge univoquement à tous les éléments de* gr G, *de telle sorte que* gr G *devienne une* $\mathbf{F}_p$-*algèbre de Lie restreinte.*

Preuve. — Quitte à remplacer ω par $\omega' = t\omega$ pour un nombre t assez petit, l'existence et les propriétés de l'élément $\xi^{[p]}$ (pour un $\xi \in \mathrm{gr}\,\mathrm{G}$ homogène donné) figurent parmi les assertions du théorème (II, 1.2.11), prouvé en (II, 1.4). Nous concluons en appliquant [13], chap. V, th. 11, p. 190.

(2.4) *Corollaire. — Si* $f : \mathrm{G} \to \mathrm{H}$ *est un morphisme* (II, 1.1.3) *de groupes munis de filtrations restreintes, alors l'application* $\mathrm{gr} f : \mathrm{gr}\,\mathrm{G} \to \mathrm{gr}\,\mathrm{H}$ *est un morphisme d'algèbres de Lie restreintes.*

(2.5) *Définitions des filtrations induites et d'un morphisme fonctoriel.* — Soient G un groupe muni d'une filtration restreinte ω et $\mathrm{A} = \mathbf{F}_p[\mathrm{G}]$ son algèbre à coefficients dans le corps premier $\mathbf{F}_p$.

Munissons A de la *borne inférieure des filtrations d'algèbre* qui vérifient

$$w(x-1) \geqslant \omega(x) \quad \textit{pour tout } x \in \mathrm{G}. \tag{2.5.1}$$

La filtration w de A sera dite *induite* par ω. Nous noterons ω^* la filtration restreinte de G induite par w comme en (2.1), c'est-à-dire que nous posons

(2.5.2) $$\omega^*(x) = w(x-1) \quad \textit{pour tout } x \in G.$$

L'application identique est donc un morphisme de G filtré par ω dans G filtré par ω^*; nous en déduisons (2.4) un morphisme des gradués associés

(2.5.3) $$\mathrm{gr}\, G \rightarrow \mathrm{gr}^* G,$$

qui se prolonge en un morphisme des *algèbres enveloppantes restreintes* :

(2.5.4) $$\widetilde{U}\, \mathrm{gr}\, G \rightarrow \widetilde{U}\, \mathrm{gr}^* G.$$

Nous avons d'autre part le morphisme canonique défini en (2.1.6) :

(2.5.5) $$\widetilde{U}\, \mathrm{gr}^* G \rightarrow \mathrm{gr}\, A = \mathrm{gr}\, \mathbf{F}_p[G].$$

Nous composons les morphismes (2.5.4) et (2.5.5) pour obtenir le morphisme de $\mathbf{F}_p$-*algèbres associatives graduées*

(2.5.6) $$j : \widetilde{U}\, \mathrm{gr}\, G \rightarrow \mathrm{gr}\, \mathbf{F}_p[G],$$

qui est un *morphisme fonctoriel* (sur la catégorie des groupes filtrés par une filtration restreinte).

(2.6) *Théorème.* — *Soit* G *un groupe muni d'une filtration restreinte. Alors le morphisme fonctoriel* (2.5)

(2.6.1) $$j : \widetilde{U}\, \mathrm{gr}\, G \rightarrow \mathrm{gr}\, \mathbf{F}_p[G]$$

est bijectif. De plus, si la filtration de G *est séparée* (II, 1.1.5), *alors la filtration de* $\mathbf{F}_p[G]$ *est séparée.*

(2.6.2) *Corollaire.* — *Si* $f: G \rightarrow H$ *est une isométrie* (II, 1.1.3) *de groupes munis de filtrations restreintes, alors le prolongement canonique* $g : \mathbf{F}_p[G] \rightarrow \mathbf{F}_p[H]$ *de* f *aux algèbres de groupes est une isométrie pour les filtrations induites* (cf. (III, 2.3.5)).

(2.7) *Preuve.* — Lorsque la filtration restreinte ω du groupe G est *discrète* (1.1.5), la filtration induite (2.5) sur $\mathbf{F}_p[G] = A$ peut être explicitée comme suit (cf. (III, 2.3.6)).

Pour tout $\nu > 0$, le groupe additif A_ν des éléments de filtration $\geqslant \nu$ dans A est engendré par ses éléments de la forme

(2.7.1) $$z = (y_1 - 1) \ldots (y_n - 1),$$

où $y_1, \ldots, y_n \in G$, $n \in \mathbf{N}^*$ et

(2.7.2) $$\omega(y_1) + \ldots + \omega(y_n) \geqslant \nu.$$

Il en résulte que le morphisme j (2.6.1) est *surjectif.*

Supposons, de plus, que G soit un groupe *fini*, d'ordre p^r, et que la filtration ω soit *séparée*. Nous avons alors

(2.7.3) $$\dim \mathrm{gr}\, G = r,$$

ce qui implique ([13], th. 12, p. 191)

(2.7.4) $$\dim \widetilde{\mathrm{U}} \operatorname{gr} \mathrm{G} = p^r.$$

Le signe « dim » note ici la dimension d'un espace vectoriel sur $\mathbf{F}_p$.

Comme nous avons

(2.7.5) $$\dim \mathbf{F}_p[\mathrm{G}] = p^r,$$

la relation

(2.7.6) $$\dim \operatorname{gr} \mathbf{F}_p[\mathrm{G}] = p^r$$

est vérifiée si et seulement si la filtration de $\mathbf{F}_p[\mathrm{G}]$ est *séparée*. Quand nous aurons prouvé ce dernier point, nous saurons que j est un épimorphisme d'espaces vectoriels de mêmes dimensions (finies), donc un isomorphisme.

Or, puisque l'idéal d'augmentation de $\mathbf{F}_p[\mathrm{G}]$ est nilpotent (II, 2.1.7), l'élément z de (2.7.1) ne peut être différent de zéro que si

(2.7.7) $$n \leqslant t,$$

où t désigne un certain entier. Si λ est le maximum des $\omega(x)$, pour $x \in \mathrm{G}$ et $x \neq 1$, nous voyons que

(2.7.8) $$w(z) > \lambda t \quad \text{implique} \quad z = 0,$$

ce qui prouve que w est séparé (cf. (III, 2.3.7)).

Le théorème (2.6) est donc prouvé dans le cas des groupes finis munis de filtrations restreintes séparées.

Si G est un groupe de *type fini* muni d'une filtration restreinte ω, alors tous les quotients $\mathrm{G}/\mathrm{G}_\nu$ $(\nu > 0)$ sont des p-groupes *finis*, car, d'après (2.2), le lemme (II, 3.1.2) s'applique aux filtrations restreintes. Cela nous permet d'étendre la démonstration de (2.6) aux groupes de type fini, par la considération des quotients finis séparés $\mathrm{G}/\mathrm{G}_\nu$. Nous prouvons alors le corollaire (2.6.2) pour les groupes de type fini : cf. (III, 2.3.5).

Nous atteignons enfin le cas général par passage aux limites inductives (I, 2.3.8).

A.3. Filtrations de Zassenhaus et séries de Golod-Chafarévitch.

(3.1) *Définition du foncteur* Alp *sur la catégorie des pro-p-groupes.* — Soit d'abord G un pro-p-groupe *discret*, c'est-à-dire *fini*. Nous notons Alp G *l'algèbre* $\mathbf{F}_p[\mathrm{G}]$ et (pour tout $n \in \mathbf{N}$) $\mathrm{Alp}_n \mathrm{G}$ la *n-ième puissance de l'idéal d'augmentation* de Alp G.

Pour un pro-p-groupe quelconque G, nous posons

(3.1.1) $$\mathrm{Alp}\,\mathrm{G} = \varprojlim \mathrm{Alp}\,\mathrm{G}/\mathrm{U},$$

(3.1.2) $$\mathrm{Alp}_n \mathrm{G} = \varprojlim \mathrm{Alp}_n \mathrm{G}/\mathrm{U},$$

les limites projectives étant prises sur l'ensemble des *sous-groupes distingués ouverts* U de G.

Nous considérons les $\mathrm{Alp}_n\mathrm{G}$ et G comme des *parties* de Alp G.

(3.2) *Proposition. — Soit* G *un pro-p-groupe. Considérons les algèbres* Alp G (3.1) *et* Al G (II, 2.2.1); *nous avons la suite exacte*

(3.2.1) $$0 \to p \text{ Al G} \to \text{Al G} \to \text{Alp G} \to 0.$$

L'algèbre Alp G *est un anneau local compact de radical* $\mathrm{Alp}_1 \mathrm{G}$; *elle contient* $\mathbf{F}_p[\mathrm{G}]$ *comme sous-algèbre dense et* G *comme sous-espace compact. Les* $\mathrm{Alp}_n \mathrm{G}$ *sont des idéaux fermés de* Alp G. *Ils définissent la filtration canonique w : c'est la filtration de* Alp G *à valeurs entières telle que*

(3.2.2) $$w(y) \geqslant n \Leftrightarrow y \in \mathrm{Alp}_n \mathrm{G},$$

pour tous $y \in \mathrm{Alp\,G}$, $n \in \mathbf{N}$.

Le pro-p-groupe G *est de type fini* (II, 2.1.4) *si et seulement si*

(3.2.3) $$\dim \mathrm{gr}_1 \mathrm{Alp\,G} = d < \infty.$$

Dans ce cas, d est le nombre minimum de générateurs de G, $\mathrm{Alp}_n \mathrm{G}$ *est la n-ième puissance du radical de* Alp G, *tous les* $\mathrm{gr}_n \mathrm{Alp\,G}$ *sont de dimension finie, et la topologie de* Alp G *est définie par sa filtration canonique.*

Preuve. — Nous avons les *suites exactes de groupes compacts*

$$0 \to p \text{ Al G/U} \to \text{Al G/U} \to \text{Alp G/U} \to 0,$$

et nous obtenons (3.2.1) par passage aux limites projectives. Cela permet de ramener les propriétés de Alp à celles de Al (II, 2.2.2); on peut aussi bien les prouver directement. La caractérisation de d (3.2.3) comme nombre minimum de générateurs de G résulte de (II, 2.1.9), qui montre que $\mathrm{gr}_1 \mathrm{Alp\,G}$ est canoniquement isomorphe au quotient de G par son sous-groupe de Frattini (adhérence du sous-groupe engendré par les commutateurs et les p-ièmes puissances).

(3.3) *Définition. — Filtration de Zassenhaus d'un pro-p-groupe.* Soit G un pro-p-groupe. Considérons les *filtrations restreintes* (2.2) ω de G qui vérifient les conditions suivantes :

(3.3.1) $\omega(x) \geqslant 1$ *pour tout* $x \in \mathrm{G}$;

(3.3.2) *pour tout* $\nu > 0$, *le sous-groupe* G_ν (des $x \in \mathrm{G}$ vérifiant $\omega(x) \geqslant \nu$) *est fermé.*

La borne inférieure de ces filtrations est encore une filtration restreinte qui vérifie ces deux conditions; nous l'appelons *filtration de Zassenhaus de* G.

(3.4) *Lemme. — Soient* G, G′ *deux pro-p-groupes,* ω, ω′ *leurs filtrations de Zassenhaus respectives, et* $f : \mathrm{G} \to \mathrm{G}'$ *un homomorphisme continu. Alors f est un morphisme* (II, 1.1.3) *pour* ω *et* ω′; *de plus, si f est surjectif,* ω′ *est la filtration quotient de* ω (II, 1.1.4).

Preuve. — La fonction $\omega' \circ f$ est une filtration restreinte de G vérifiant les conditions (3.3), d'où $\omega(x) \leqslant \omega'(f(x))$ pour tout $x \in \mathrm{G}$, d'après la minimalité de ω.

Supposons f surjectif, et notons ω^* la filtration quotient de ω. Nous avons $\omega^*(x) \leqslant \omega'(x)$ pour tout $x \in \mathrm{G}'$, et, d'après la minimalité de ω′, il nous suffit de prouver que ω^* vérifie les conditions (3.3). La filtration ω^* est restreinte et satisfait à (3.3.1). Pour vérifier (3.3.2), il faut établir que, pour tout $\nu > 0$, le sous-groupe

(3.4.1) $$\bigcap_{\lambda < \nu} f(\mathrm{G}_\lambda)$$

est fermé dans G' : cf. (I, 2.1.7). Cela résulte de la compacité de G, de la continuité de f et de ce que les G_λ sont fermés. En même temps nous prouvons que le sous-groupe (3.4.1) se réduit à $f(G_\nu)$.

(3.5) *Théorème. — Soient* G *un pro-p-groupe et* ω *sa filtration de Zassenhaus* (3.3). *Alors* ω *est induite par la filtration canonique de* Alp G (3.2). *Autrement dit,* ω *est à valeurs entières et*

(3.5.1) $$\omega(x) \geqslant n \Leftrightarrow x - 1 \in \mathrm{Alp}_n \mathrm{G},$$

pour tous $x \in \mathrm{G}$, $n \in \mathbf{N}$.

Si le pro-p-groupe G *est de type fini* (II, 2.1.4), *sa topologie est définie par* ω (II, 1.1.5), *l'algèbre de Lie restreinte* gr G *est engendrée par ses éléments de degré* 1, *et le morphisme* (2.1.6)

(3.5.2) $$\widetilde{\mathrm{U}}\,\mathrm{gr}\,\mathrm{G} \to \mathrm{gr}\,\mathrm{Alp}\,\mathrm{G}$$

est bijectif.

Preuve. — Supposons d'abord G *fini*. Notons w' la filtration de $\mathbf{F}_p[\mathrm{G}] = \mathrm{Alp}\,\mathrm{G}$ induite (2.5) par ω, et w la filtration canonique de Alp G (3.2).

Comme nous avons $w'(x-1) \geqslant 1$ pour tout $x \in \mathrm{G}$, nous en déduisons

(3.5.3) $$w'(y) \geqslant w(y) \quad \text{pour tout } y \in \mathrm{Alp}\,\mathrm{G}.$$

Nous avons d'autre part, d'après (3.2) et (3.3), $w(x-1) \geqslant \omega(x)$ pour tout $x \in \mathrm{G}$, d'où nous tirons

(3.5.4) $$w(y) \geqslant w'(y) \quad \text{pour tout } y \in \mathrm{Alp}\,\mathrm{G}.$$

Les relations (3.5.3) et (3.5.4) équivalent à $w = w'$. Le théorème (2.6) entraîne alors (3.5.1) et (3.5.2). Comme $\widetilde{\mathrm{U}}$ gr G est engendrée par ses éléments de degré 1, d'après (3.5.2) et la définition de la filtration de Alp G, la théorie des algèbres enveloppantes restreintes ([13], chap. V, § 7) montre qu'il en est de même de gr G.

Si G est maintenant un pro-p-groupe quelconque, notons, pour chaque sous-groupe ouvert distingué U de G, ω_{U} la filtration de Zassenhaus de G/U, et x_{U} l'image canonique dans G/U d'un élément x de G. Nous avons alors, d'après (3.4), $\omega(x) \leqslant \omega_{\mathrm{U}}(x_{\mathrm{U}})$ pour tous x, U. Comme (3.5.1) a été prouvé pour les groupes finis G/U, la relation (3.5.1) dans G équivaut à

(3.5.5) $$\omega(x) = \inf_{\mathrm{U}} \omega_{\mathrm{U}}(x_{\mathrm{U}}), \quad \text{pour tout } x \in \mathrm{G}.$$

Si (3.5.5) n'était pas vrai, il existerait $x \in \mathrm{G}$ et $\nu \in \mathbf{R}$ tels que

(3.5.6) $$\omega(x) < \nu < \inf_{\mathrm{U}} \omega_{\mathrm{U}}(x_{\mathrm{U}}).$$

Comme le sous-groupe G_ν des éléments de filtration $\geqslant \nu$ dans G est fermé (3.3.2), il existe un U tel que $\omega(y) < \nu$ pour tout $y \in x\mathrm{U}$. Or, d'après (3.4), nous avons

(3.5.7) $$\omega_{\mathrm{U}}(x_{\mathrm{U}}) = \sup_{y \in x\mathrm{U}} \omega(y),$$

ce qui contredit (3.5.6).

Enfin si G est de type fini, une partie de nos assertions est contenue dans (3.2); pour le reste, nous nous ramenons aux groupes finis par la considération des quotients G/G_n.

(3.6) *Proposition. — Soient* G *un pro-p-groupe de type fini, t un nombre* >0, ω *la filtration de Zassenhaus de* G (3.3) *et* ω_t *sa* (t, p)*-filtration* (II, 3.2.8). *Nous avons alors*

(3.6.1) $$\omega_t(x) \leqslant t\omega(x) \quad \textit{pour tout } x \in G, \quad \textit{et}$$

(3.6.2) $$\textit{si} \quad \omega_t(x) < p(p-1)^{-1}, \quad \omega_t(x) = t\omega(x).$$

Preuve. — La fonction $x \mapsto t\omega(x)$ est une p-filtration de G (2.2) vérifiant les mêmes conditions que ω_t, exception faite de la minimalité : cela entraîne (3.6.1).

Posons $\omega'(x) = t^{-1}\omega_t(x)$ si $\omega_t(x) < p(p-1)^{-1}$, et $\omega'(x) = +\infty$ si $\omega_t(x) \geqslant p(p-1)^{-1}$. Alors ω' est une filtration restreinte de G vérifiant les mêmes conditions que ω, mise à part la minimalité, d'où (3.6.2).

(3.6.3) *Corollaire. — Soient* gr G (resp. gr^t G) *l'algèbre de Lie graduée associée à* G *pour* ω *(resp.* ω_t*). Prenons le quotient de* gr G *(resp.* gr^t G*) par l'idéal qu'engendrent les éléments homogènes de degré* $\geqslant t^{-1}p(p-1)^{-1}$ *(resp.* $\geqslant p(p-1)^{-1}$*), et multiplions les degrés par t* (I, 1.1.10). *Les deux algèbres obtenues sont canoniquement isomorphes.*

(3.7) *Théorème. — Soient* G *un pro-p-groupe de type fini,* $L = \mathrm{gr}\, G$ *l'algèbre de Lie restreinte associée à* G *pour sa filtration de Zassenhaus, et* L^* *la sous-algèbre de Lie (non restreinte) engendrée dans* L *par* $\mathrm{gr}_1 G$. *Alors les deux assertions suivantes sont équivalentes.*

(3.7.1) *Le groupe* G *est analytique.*

(3.7.2) *Il existe un entier* $n \in \mathbf{N}^*$ *tel que la composante homogène de degré n de* L^* *soit nulle.*

Preuve. — Le théorème (1.9) prouve que (3.7.1) implique (3.7.2). Pour établir l'implication réciproque, nous utilisons (3.6.3) et la proposition (1.6).

Nous allons maintenant traduire diversement le théorème (3.7). Remarquons d'abord que, pour une $\mathbf{F}_p$-algèbre de Lie graduée L engendrée par L_1 (L_n désignant la composante homogène de degré n), les deux assertions suivantes sont équivalentes d'après (II, 3.3.3) :

(i) $$L_n = 0 \quad (\text{pour un } n \in \mathbf{N}^*);$$

(ii) $$L_{n+h} = 0 \quad \text{pour tout } h \in \mathbf{N}.$$

(3.8) *Théorème. — Soient* G *un pro-p-groupe de type fini et, pour chaque* $n \in \mathbf{N}$, G^{p^n} *l'adhérence du sous-groupe engendré par les* p^n*-ièmes puissances des éléments de* G. *Alors* G *est analytique si et seulement si*

(3.8.1) $$\varliminf_{n \to \infty} n^{-1} \log_p(G : G^{p^n}) < \infty.$$

Dans ce cas la dimension r est donnée par la formule

(3.8.2) $$r = \lim_{n \to \infty} n^{-1} \log_p(G : G^{p^n}).$$

Preuve. — Si G est analytique, nous appliquons (III, 3.1.8). Sinon nous avons $\mathrm{gr}_n \mathrm{G} \neq 0$ pour tout $n \in \mathbf{N}^*$, gr G désignant le gradué associé à la filtration de Zassenhaus, ce qui entraîne

(3.8.3) $$\log_p(\mathrm{G} : \mathrm{G}^{p^n}) \geqslant p^n$$

pour tout $n \in \mathbf{N}^*$.

(3.9) *Définitions.* — Pour chaque entier $n \geqslant 1$ nous notons P_n le polynôme

(3.9.1) $$\mathrm{P}_n(\mathrm{T}) = (1 - \mathrm{T}^{pn})(1 - \mathrm{T}^n)^{-1}.$$

Si G est un pro-p-groupe de type fini muni de sa filtration de Zassenhaus, nous posons

(3.9.2) $$a_n(\mathrm{G}) = \dim \mathrm{Alp}_n \mathrm{G}/\mathrm{Alp}_{n+1} \mathrm{G},$$

(3.9.3) $$b_n(\mathrm{G}) = \dim \mathrm{gr}_n \mathrm{G},$$

(3.9.4) $$\mathrm{gocha}(\mathrm{G}; \mathrm{T}) = \sum_{n=0}^{\infty} a_n(\mathrm{G}) \mathrm{T}^n.$$

La série (3.9.4) est dite série de Golod-Chafarévitch de G : cf. [8], [19].

(3.10) *Proposition.* — *Pour un pro-p-groupe de type fini* G *nous avons la relation*

(3.10.1) $$\mathrm{gocha}(\mathrm{G}; \mathrm{T}) = \prod_{n=1}^{\infty} \mathrm{P}_n(\mathrm{T})^{b_n(\mathrm{G})}.$$

Preuve. — Cette relation est une conséquence de (3.5.2) et de la structure d'une algèbre enveloppante restreinte. Si $(x_i)_{i \in \mathrm{I}}$ est une *base homogène* de gr G, l'ensemble I étant totalement ordonné, nous pouvons prendre comme base de $\widetilde{\mathrm{U}}$ gr G les monômes ordonnés x^α, où $\alpha \in \mathbf{N}^{(\mathrm{I})}$ et $\alpha_i < p$ pour tout $i \in \mathrm{I}$. Le dénombrement de ces monômes suivant leurs degrés s'exprime précisément par (3.10.1).

(3.11) *Théorème.* — *L'alternative des gocha. Soit* G *un pro-p-groupe de type fini. Alors deux cas seulement sont possibles :*

1° *Le groupe* G *est analytique de dimension* $r \geqslant 0$. *Alors la série* gocha(G; T) *représente une fraction rationnelle en* T *qui admet au point* 1 *un pôle d'ordre r. Cette fraction peut s'écrire comme un produit fini*

(3.11.1) $$\prod_{i=1}^{r} (1 - \mathrm{T}^{n_i})^{-1} . \prod_{j=1}^{s} \mathrm{P}_{m_j}(\mathrm{T}),$$

où les n_i *et* m_j *sont des entiers positifs (non nécessairement distincts).*

2° *Le groupe* G *n'est pas analytique. Alors nous avons la relation*

(3.11.2) $$\varliminf_{n \to \infty} n^{-\frac{1}{2}} \log a_n(\mathrm{G}) \geqslant \pi(2(p-1)/3p)^{\frac{1}{2}}.$$

Plus précisément

(3.11.3) $$\mathrm{gocha}(\mathrm{G}; \mathrm{T}) \geqslant \mathrm{P}_1(\mathrm{T}) \mathrm{F}(\mathrm{T}) \mathrm{F}(\mathrm{T}^p)^{-1},$$

où F *est la série des partitions*

(**3.11.4**) $$\mathrm{F}(\mathrm{T}) = \prod_{n=1}^{\infty} (1-\mathrm{T}^n)^{-1}.$$

(**3.12**) *Corollaire. — Pour qu'un pro-p-groupe* G *de type fini soit analytique, il faut et il suffit qu'il vérifie la relation*

(**3.12.1**) $$\overline{\lim_{n\to\infty}}\,(\log n)^{-1}\log a_n(\mathrm{G}) < \infty.$$

(**3.13**) *Preuve du théorème* (3.11). — Supposons d'abord G analytique et appliquons (3.7). Si la composante homogène L_n^* est nulle pour $n \geqslant n_0$, les lemmes (II, 3.3.4) et (II, 3.3.5) donnent les résultats suivants.

(**3.13.1**) $\mathrm{L}_n = 0$ *pour* $n \geqslant n_0$ *et* $p \nmid n$;

(**3.13.2**) *la p-application* $\mathrm{L}_{p^{-1}n} \to \mathrm{L}_n$ *est surjective et additive si* $n \geqslant n_0$ *et* $p \mid n$.

Comme il s'agit d'espaces vectoriels de dimension finie sur $\mathbf{F}_p$, les p-applications (3.13.2) deviennent *bijectives* pour les degrés assez grands. Autrement dit, il existe un entier n_1 tel que

(**3.13.3**) $$b_n(\mathrm{G}) = 0 \qquad \text{pour } n \geqslant n_1 \text{ et } p \nmid n.$$

(**3.13.4**) $$b_n(\mathrm{G}) = b_{p^{-1}n}(\mathrm{G}) \qquad \text{pour } n \geqslant n_1 \text{ et } p \mid n.$$

Comme nous avons (3.9)

(**3.13.5**) $$\prod_{i=0}^{\infty} \mathrm{P}_{np^i}(\mathrm{T}) = (1-\mathrm{T}^n)^{-1},$$

la formule (3.11.1) résulte de (3.10). Il reste à montrer que l'entier r figurant dans (3.11.1) est la dimension du groupe G. C'est une conséquence du théorème (3.8).

Supposons maintenant G non analytique. Nous avons alors (3.7)

(**3.13.6**) $$b_n(\mathrm{G}) \geqslant 1 \qquad \text{pour tout } n \geqslant 1,$$

et

(**3.13.7**) $$b_1(\mathrm{G}) \geqslant 2$$

(sinon G serait un quotient de $\mathbf{Z}_p$, donc analytique). Nous obtenons ainsi la formule (3.11.3), d'où nous déduisons (3.11.2) en appliquant [9], p. 113 et 116.

(**3.14**) *Exemples (exercices).* — Soit $\overline{\mathscr{F}}$ un pro-p-groupe libre pour les générateurs X_i^* $(1 \leqslant i \leqslant r)$. Alors l'algèbre Alp $\overline{\mathscr{F}}$ s'identifie à l'algèbre de Magnus sur $\mathbf{F}_p$ engendrée par les $\mathrm{X}_i = \mathrm{X}_i^* - 1$, d'après (II, 3.1.4). Nous avons

(**3.14.1**) $$\mathrm{gocha}(\overline{\mathscr{F}}; \mathrm{T}) = (1-r\mathrm{T})^{-1},$$

et gr $\overline{\mathscr{F}}$ est une algèbre de Lie restreinte *libre* pour les images canoniques des X_i^* dans $\mathrm{gr}_1 \overline{\mathscr{F}}$.

Si G est un pro-p-groupe admettant r générateurs, nous avons

(**3.14.2**) $$a_n(\mathrm{G}) \leqslant r^n \qquad (\text{pour tout } n \in \mathbf{N}),$$

l'égalité n'ayant lieu pour tout n que si G est libre. Plus généralement, si $f: G \to G'$ est un *épimorphisme continu* de pro-p-groupes de type fini, alors

$$\text{gocha}(G;T) \geqslant \text{gocha}(G';T), \tag{3.14.3}$$

ce qui signifie, par définition, $a_n(G) \geqslant a_n(G')$ pour tout n. L'égalité ne peut avoir lieu dans (3.14.3) que si f est un isomorphisme.

Soient G un pro-p-groupe de type fini, ω sa filtration de Zassenhaus, G_n l'ensemble des $x \in G$ tels que $\omega(x) \geqslant n$ (pour $n \in \mathbf{N}^*$), et Γ_n l'adhérence du n-ième sous-groupe de la suite centrale descendante de G. Le gradué associé $L = \text{gr}\, G$ est calculé pour ω, L^* est défini comme en (3.7) et L_n^* est la composante de degré n de L^*. Choisissons, pour chaque $n \in \mathbf{N}^*$, une *partie* A_n de G, contenue dans G_n, et telle que l'image de A_n modulo G_{n+1} contienne L_n^*. Nous pouvons, par exemple, prendre $A_n = \Gamma_n$. Notons $A_n^{p^j}$ l'ensemble des p^j-ièmes puissances des éléments de A_n. Soient n un entier $\geqslant 1$, et

$$n = mp^h, \quad \text{avec } m, h \in \mathbf{N}, p \nmid m. \tag{3.14.4}$$

Nous avons alors

$$G_n = A_m^{p^h} \dots A_{mp^i}^{p^{h-i}} \dots A_{mp^h} G_{n+1}. \tag{3.14.5}$$

Cela résulte de ce que gr G est engendré par $\text{gr}_1\, G$.

Notons G^0 le produit semi-direct

$$G^0 = \mathbf{Z}_p \times A, \tag{3.14.6}$$

où A est l'algèbre de séries formelles $\mathbf{F}_p[[x]]$; le générateur canonique de $\mathbf{Z}_p$ opère sur A en multipliant ses éléments par $(1+x)$. Nous avons

$$\text{gocha}(G^0;T) = (1-T)^{-1}F(T)F(T^p)^{-1}, \tag{3.14.7}$$

où F est défini comme en (3.11.4). Cela entraîne [9],

$$\lim_{n\to\infty} n^{-\frac{1}{2}} \log a_n(G^0) = \pi(2(p-1)/3p)^{\frac{1}{2}}. \tag{3.14.8}$$

Appelons maintenant G^1 le groupe nilpotent de classe 3 et de dimension 4 étudié en (III, 3.2.4). Nous avons :

$$\text{gocha}(G^1;T) = (1-T)^{-2}(1-T^2)^{-1}(1-T^3)^{-1}. \tag{3.14.9}$$

Si nous prenons le quotient G^2 de G^1 par le troisième sous-groupe de sa suite centrale descendante nous avons

$$\text{gocha}(G^2;T) = (1-T)^{-2}(1-T^2)^{-1}. \tag{3.14.10}$$

Si $p=2$, et si nous posons

$$G^3 = G^2 \times (\mathbf{Z}/2\mathbf{Z}), \tag{3.14.11}$$

nous avons

$$\text{gocha}(G^3;T) = (1-T)^{-3}. \tag{3.14.12}$$

Cela résulte de la formule

$$\text{gocha}(G \times G'; T) = \text{gocha}(G; T)\text{gocha}(G'; T), \tag{3.14.13}$$

valable pour les produits directs. Nous sommes ainsi obligés de constater un résultat regrettable, à savoir

$$\text{gocha}(\mathbf{Z}_2^3; T) = \text{gocha}(G^3; T). \tag{3.14.14}$$

Enfin notons G^4 le groupe G de (1.4), pour un p quelconque. Nous obtenons

$$\text{gocha}(G^4; T) = P_1(T) . \prod_{i=1}^{p-1} (1 - T^i)^{-1}. \tag{3.14.15}$$

INDEX DES NOTATIONS

INDEX TERMINOLOGIQUE

BIBLIOGRAPHIE

[1] AMICE (Y.), Interpolation p-adique, *Bull. Soc. math. France*, 92 (1964), p. 117-180.

[2] BOURBAKI (N.), *Groupes et algèbres de Lie*, chap. Ier (A.S.I., 1285, Paris, 1960).

[3] — *Algèbre commutative*, chap. III et IV (A.S.I., 1293, Paris, 1961).

[4] CARTAN (H.) et EILENBERG (S.), *Homological algebra* (Princeton math. series, nº 19).

[5] CHEVALLEY (C.), *Theory of Lie groups* (I) (Princeton math. series, nº 8).

[6] DYNKIN (E. B.), Algèbres de Lie normées et groupes analytiques (en russe) : *Uspekhi Mat. Nauk*, n.s. 5 (1950), p. 135-186; traduction : *Am. Mat. Soc. Transl.*, sér. 1, 9, p. 471-534.

[7] EILENBERG (S.), Homological dimension and syzygies, *Ann. of Math.*, 64 (1956), p. 328-336.

[8] GOLOD (E. S.) et CHAFARÉVITCH (I. R.), Sur la tour des corps de classes (en russe) : *Izvestia A.N.S.S.S.R.*, sér. mat. 28 (1964), p. 13-24.

[9] HARDY (G. H.), *Ramanujan*, New York, Chelsea.

[10] HILY (J.), Séries d'interpolation pour les fonctions de plusieurs variables p-adiques, *C.R. Acad. Sc. Paris*, 256 (1963), p. 2985-2987.

[11] HOCHSCHILD (G.), Cohomology of algebraic linear groups, *Illinois J. of Math.*, 5 (1961), p. 492-519.

[12] HOCHSCHILD (G.) et SERRE (J.-P.), Cohomology of group extensions, *Trans. A.M.S.*, 74 (1953), p. 110-134.

[13] JACOBSON (N.), *Lie algebras*, New York, Interscience 1962.

[14] LAZARD (M.), Sur les groupes nilpotents et les anneaux de Lie, *Annales E.N.S.*, 71 (1954), p. 101-190.

[15] — Sur les algèbres enveloppantes universelles de certaines algèbres de Lie, *Alger Mathématiques*, 1 (1954), p. 281-294.

[16] — Lois de groupes et analyseurs, *Annales E.N.S.*, 72 (1955), p. 299-400.

[17] — Groupes, anneaux de Lie et problème de Burnside, *Centro Internazionale Matematico Estivo*, Roma, 1960.

[18] — Quelques calculs concernant la formule de Hausdorff, *Bull. Soc. math. France*, 91 (1963), p. 435-451.

[19] — Sur les séries de Golod-Chafarévitch des pro-p-groupes de type fini, *C.R. Acad. Sc. Paris*, 258 (1964), p. 4403-4406.

[20] — Sur la cohomologie d'une algèbre de puissances divisées (à paraître aux *Actes du Colloque de Clermont-Ferrand*, C.N.R.S., avril 1964).

[21] MAC LANE (S.), *Homology*, Springer Verlag, 1963.

[22] MAHLER (K.), An interpolation series for continuous fonctions of a p-adic variable, *Journ. f. reine u. ang. Math.*, 199 (1958), p. 23-34; *ibid.*, 208 (1961), p. 70-72.

[23] MONTGOMERY (D.) et ZIPPIN (S.), *Topological transformation groups*, New York, Interscience, 1955.

[24] SERRE (J.-P.), Compacité locale des espaces fibrés, *C.R. Acad. Sc. Paris*, 229 (1949), p. 1295-1297.

[25] — *Corps locaux* (A.S.I., 1296, Paris, 1962).

[26] — Endomorphismes complètement continus des espaces de Banach p-adiques, *Publications Math. de l'I.H.E.S.* nº 12, 1962.

[27] — Structure de certains pro-p-groupes, *Sémin. Bourbaki*, 252 (février 1963).

[28] — Groupes analytiques p-adiques, *Sémin. Bourbaki*, 270 (février 1964).

[29] — *Cohomologie galoisienne*, Collège de France, 1963.

[30] — Classification des variétés analytiques p-adiques compactes, à paraître dans *Topology*.

[31] — Sur la dimension cohomologique des groupes profinis, *ibid.*

[32] WALL (C. T. C.), Resolutions for extensions of groups, *Proc. Camb. Phil. Soc.*, 57 (1961), p. 251-255.

[33] WEYL (H.), Elementare Theorie der konvexen Polyeder, *Comm. Math. Helv.*, 7 (1935), p. 290-306.

TABLE DES MATIÈRES

Manuscrit reçu entre le 1er octobre 1963 et le 1er juillet 1964.