JEAN-MARC FONTAINE

Groupes p-divisibles sur les corps locaux

Astérisque, tome 47-48 (1977)

<http://www.numdam.org/item?id=AST_1977__47-48__1_0>

Je voudrais remercier le département de mathématiques de Queen's University, Kingston, Ontario, en particulier P. Ribenboim, de m'avoir donné l'occasion d'éclaircir mes idées sur les schémas en groupes finis et plats lors d'un cours que j'y fis à l'automne 1974.

Les résultats annoncés dans [20], [21] et [22] (dont les démonstrations constituent une partie du chapitre III et du § 1 du chapitre IV du présent mémoire, ainsi qu'une partie de [23]) ont été exposés lors d'un cours au Collège de France (Fondation Peccot) au printemps 1975. Les démonstrations étaient différentes car on utilisait au maximum les résultats connus. Je voudrais remercier la fondation Peccot de son hospitalité et les auditeurs de ce cours de leur patience et de leurs interventions.

Je voudrais aussi remercier tous ceux qui m'ont aidé aux différents stades de ce travail. Tout particulièrement P. Berthelot et W. Messing, mais aussi P. Cartier, P. Deligne, L. Illusie, N. Katz, M. Lazard, B. Mazur, M. Raynaud. Et enfin et surtout J.-P. Serre sans lequel ce travail n'aurait jamais vu le jour.

Ces remerciements seraient incomplets si je n'exprimais ici ma reconnaissance à Mme Guttin-Lombard et à Mlle Marchand qui ont réalisé la frappe du manuscrit.

TABLE DES MATIÈRES

INTRODUCTION

0.1. Soit p un nombre premier, soit k un corps parfait de caractéristique p, soit $A = W(k)$ l'anneau des vecteurs de Witt à coefficients dans k, soit A' l'anneau des entiers d'une extension finie totalement ramifiée du corps des fractions de A et soit e le degré de cette extension.

Le présent mémoire a pour objet

- la classification, à isomorphisme près, des (schémas en) groupes formels commutatifs sur k ;
- la classification, à isomorphisme près, des (schémas en) groupes formels, lisses et de dimension finie, sur A et sur A' si $e \leq p-1$;
- la classification, à isogénie près, des groupes de Barsotti-Tate (ou groupes p-divisibles) sur A'.

0.2. Ce mémoire a été conçu pour pouvoir être lu par les non-spécialistes : il suffit, en principe, de connaître un peu d'algèbre commutative (par exemple celle de Bourbaki) et les rudiments du langage des catégories (par exemple, [40]). On a essayé d'être aussi "élémentaire" que possible. On a systématiquement négligé le point de vue "géométrique" au profit du point de vue "fonctoriel" (et on a escamoté les difficultés d'ordre logique : les "catégories" de foncteurs que l'on considère ne sont de "vraies" catégories qu'à condition de se restreindre à un univers convenable, ce qui est implicitement supposé). Dans cet esprit, donnons, dès maintenant, quelques définitions (nous les reprendrons dans un cadre plus général au chapitre I) : soit B un anneau qui est soit k, soit A, soit A' :

- on appelle B-<u>anneau fini</u> toute B-algèbre associative, commutative et unitaire qui est un B-module de longueur finie ;
- un B-<u>foncteur formel</u> est un foncteur covariant de la catégorie des B-anneaux finis dans celle des ensembles ; on dit que c'est un <u>schéma fini sur</u> B

s'il est représentable, que c'est un <u>schéma formel sur</u> B si c'est une limite inductive de schémas finis ;

- un B-<u>foncteur en groupes formels</u> (<u>commutatifs</u>) est un objet en groupes (commutatifs) dans la catégorie des B-foncteurs formels ; autrement dit c'est un foncteur covariant de la catégorie des B-anneaux finis dans celle des groupes (commutatifs) ; un <u>groupe formel sur</u> B (resp. un <u>groupe fini sur</u> k) est un foncteur en groupes formels dont le foncteur formel sous-jacent est un schéma formel (resp. fini) ;
- un groupe formel G sur B est <u>lisse</u> si, pour tout B-anneau fini R et tout idéal I de R de carré nul, l'homomorphisme canonique de $G(R)$ dans $G(R/I)$ est surjectif ;
- un p-<u>groupe formel</u> G sur B est un groupe formel commutatif de p-torsion (i.e. G s'identifie à $\varinjlim \operatorname{Ker} p^n|G)$;
- un p-<u>groupe fini</u> sur k est un p-groupe formel qui est un groupe fini ;
- un groupe p-<u>divisible</u>, ou de <u>Barsotti-Tate</u>, sur k est un p-groupe formel tel que la multiplication par p est un épimorphisme, à noyau fini ; un groupe p-divisible, ou de Barsotti-Tate sur A ou A' est un p-groupe formel lisse qui, par restriction aux k-anneaux finis, définit un groupe p-divisible sur k (en fait, il y a seulement équivalence entre la catégorie des groupes formels que l'on vient de définir et celle des groupes p-divisibles).

0.3. Il nous a semblé utile de rassembler dans un chapitre préliminaire (chap.I) les résultats classiques et élémentaires sur les groupes formels qui sont utilisés dans la suite. Il ne contient aucune idée vraiment nouvelle, tout au plus quelques variantes de résultats bien connus ([13] , [14] , [15] , [27] , [28] , [36]). Sa lecture est vivement déconseillée aux spécialistes qui l'utiliseront comme un chapitre de références.

0.4. Les quatre premiers paragraphes du chapitre II ont pour objet l'étude et la construction des covecteurs de Witt.

Soit m un entier ≥ 1 . On sait ce que c'est que le schéma en anneaux commutatifs W_m des vecteurs de Witt : pour tout anneau commutatif R ,

$W_m(R)$ est formé des éléments de la forme $(a_0, a_1, \dots, a_{m-1})$, avec les a_i dans R ; l'addition et la multiplication sont données par des polynômes convenables à coefficients entiers rationnels (cf. n° II.1).

Le morphisme de schémas $V_m : W_m \to W_{m+1}$, qui, à $(a_0, \dots, a_{m-1}) \in W_m(R)$, associe $(0, a_0, \dots, a_{m-1}) \in W_{m+1}(R)$, est compatible avec l'addition. Par passage à la limite, il nous permet de définir le $\mathbb{Z}$-foncteur en groupes commutatifs $CW^u = \varinjlim W_m$, que nous appelons le <u>groupe des covecteurs de Witt unipotents</u>.

Pour tout anneau commutatif R , on peut munir le groupe $CW^u(R)$ d'une structure de groupe topologique (telle que si $\varphi : R \to S$, l'homomorphisme $CW^u(\varphi)$ est continu). On note $CW(R)$ le complété séparé de $CW^u(R)$ pour cette topologie. En tant qu'ensemble, $CW(R)$ s'identifie à l'ensemble des covecteurs de Witt

$$\underline{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0) ,$$

où les a_{-n} sont des éléments de R vérifiant la condition

(ψ) $\left\{\begin{array}{l}\underline{\text{il existe un entier}}\ r \geq 0\ \underline{\text{tel que l'idéal de}}\ R\ \underline{\text{engendré par les}}\ a_{-n} ,\\ \underline{\text{pour}}\ n \geq r\ ,\ \underline{\text{est nilpotent}}.\end{array}\right.$

Le groupe $CW^u(R)$ s'identifie au sous-groupe de $CW(R)$ formé des $\underline{a}$ tels que les a_{-n} sont presque tous nuls ; c'est un sous-groupe dense de $CW(R)$.

Cette construction est faite au § 1 . Les endomorphismes du groupe CW sont étudiés au § 2 . Par restriction à la catégorie des k-anneaux finis, CW définit un p-groupe formel lisse $\widehat{CW}_k$ sur k qui est introduit au § 4. Le § 3 a pour but de donner une description de l'algèbre affine de $\widehat{CW}_k$ et de certain de ses sous-groupes et ne joue qu'un rôle tout à fait secondaire.

0.5. Soit σ le Frobenius absolu sur A (i.e. l'unique automorphisme continu de A tel que $\sigma(a) \equiv a^p \pmod{pA}$, pour tout $a \in A$) et soit $D_k = A[\underline{F}, \underline{V}]$ l'anneau (non commutatif si $k \neq \mathbb{F}_p$) engendré par A et deux éléments $\underline{F}$ et $\underline{V}$ soumis aux relations $\underline{F}\,\underline{V} = \underline{V}\,\underline{F} = p$, $\underline{F}a = \sigma(a)\underline{F}$ et $a\underline{V} = \underline{V}\sigma(a)$, pour tout $a \in A$.

Appelons <u>D_k-module $A[\underline{F}]$-profini</u> tout D_k-module à gauche qui est un

A[$\underline{F}$] -module profini sur lequel $\underline{V}$ opère continûment. On montre que, si G est un p-groupe formel sur k, le groupe $\mathrm{Hom}(G, \widehat{CW}_k)$ des morphismes (dans la catégorie des groupes formels sur k) de G dans $\widehat{CW}_k$ a une structure naturelle de D_k-module A[$\underline{F}$] -profini ; on le note $\underline{M}(G)$ et on l'appelle le <u>module de Dieudonné</u> de G. Il est clair que $\underline{M}$ peut être considéré comme un foncteur contravariant additif de la catégorie des p-groupes formels sur k dans celle des D_k-modules A[$\underline{F}$] -profinis. Les quatre premiers paragraphes du chapitre III ont pour objet la démonstration des deux théorèmes suivants :

THÉORÈME 1.- <u>Le foncteur</u> $\underline{M}$ <u>est pleinement fidèle et induit une anti-équivalence entre la catégorie des</u> p-<u>groupes formels sur</u> k <u>et celle des</u> D_k-<u>modules</u> A[$\underline{F}$] -<u>profinis</u>.

THÉORÈME 2.- <u>Le groupe</u> $\widehat{CW}_k$ <u>est un objet injectif de la catégorie des groupes formels commutatifs sur</u> k .

On construit, en outre, un foncteur quasi-inverse $\underline{G}$ du foncteur $\underline{M}$: si M est un D_k-module A[$\underline{F}$] -profini

- pour tout k-anneau fini R, le groupe $\underline{G}(M)(R)$ est le groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R))$ des applications D_k-linéaires continues de M dans $\widehat{CW}_k(R)$,
- si $\varphi : R \to S$ est un morphisme de k-anneaux finis, l'application $\underline{G}(M)(\varphi)$ est la flèche évidente.

0.6. Appelons D_k-<u>module fini</u> tout D_k-module à gauche qui est de longueur finie en tant que A-module. On a une notion de dualité dans la catégorie des D_k-modules finis (cf. n° III.5) et nous notons M' le dual d'un D_k-module fini M .

Si G est un p-groupe fini sur k, notons $\mathbb{D}(G)$ son dual de Cartier ; c'est un p-groupe fini sur k et $\underline{M}(G)$ et $\underline{M}(\mathbb{D}(G))$ sont des D_k-modules finis. L'objet du § 5 du chapitre III est de montrer que les foncteurs $G \mapsto \underline{M}(\mathbb{D}(G))$ et $G \mapsto (\underline{M}(G))'$ sont naturellement équivalents. On y utilise, de façon essentielle, le § 6 du chapitre II qui a pour objet l'étude de l'exponentielle d'Artin-Hasse, la construction d'un anneau un peu compliqué, noté $C\Lambda(k) = \mathcal{C}_k$, et l'étude des covecteurs de Witt à coefficients dans $\mathcal{C}_k$.

On déduit facilement de ce résultat le fait que le foncteur "module de Dieudonné des p-groupes finis sur k" construit dans ce mémoire est naturellement équivalent au foncteur "module de Dieudonné traditionnel" (qui nécessite la décomposition du groupe considéré en le produit d'un groupe unipotent par un groupe de type multiplicatif).

La construction de l'équivalence naturelle entre $G \mapsto \underline{M}(\mathbb{D}(G))$ et $G \mapsto (\underline{M}(G))'$ utilise un intermédiaire : la construction d'un foncteur covariant $\underline{M}'$ de la catégorie des p-groupes finis sur k dans celle des D_k-modules finis, qui est l'analogue, pour ces groupes, du module des courbes typiques de Cartier pour les groupes formels lisses et connexes sur k : en tant que groupe $\underline{M}'(G)$ est le sous-groupe de $G(\mathcal{C}_k)$ formé des α tels que $u_\ell(\alpha) = 0$, pour tout nombre premier $\ell \neq p$ (où u_ℓ est l'analogue de l'opérateur $F_\ell \circ V_\ell$ de Cartier). Si G est un groupe connexe tel que $F_G^m = 0$, on a $G(\mathcal{C}_k) = G(k[T]/T^{p^m})$ et la construction de $\underline{M}'(G)$ se simplifie considérablement.

0.7. Le § 6 du chapitre III a pour objet de donner une autre description du module de Dieudonné d'un p-groupe formel sur k lorsque celui-ci est lisse. C'est en fait le point de départ du chapitre IV et on y utilise de façon essentielle l'étude du "relèvement des covecteurs" faite au § 5 du chapitre II.

0.8. Le but du chapitre IV est la classification des p-groupes formels lisses sur A', à isomorphisme près, lorsque $e \leq p-1$ et des groupes p-divisibles sur A', à isogénie près, pour e quelconque.

Le § 1 correspond au cas $e = 1$, autrement dit $A = A'$, que nous avons préféré traiter séparément afin de ne pas mélanger les difficultés.

Soit G un p-groupe formel lisse de dimension finie sur A et soit $\mathfrak{R}$ son algèbre affine. Par extension des scalaires, G définit un p-groupe formel lisse G_k sur k dont l'algèbre affine est $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. Soit K le corps des fractions de A et soit $\mathfrak{R}_K = \mathfrak{R} \otimes_A K$. Avec des notations évidentes, soit $P^u(\mathfrak{R})$ le sous-A-module de $\mathfrak{R}_K$ formé des α tels que $d\alpha \in \Omega_A(\mathfrak{R})$, module des A-différentielles continues de l'anneau $\mathfrak{R}$, identifié à un sous-module de $\Omega_K(\mathfrak{R}_K)$. On munit $P^u(\mathfrak{R})$ d'une topologie A-linéaire convenable et on note $P(\mathfrak{R})$ le séparé complété de $P^u(\mathfrak{R})$ pour cette topologie (si G est connexe et si $(X_1, X_2, \dots, X_d)$ est un système de coordonnées pour $\mathfrak{R}$, i.e. si $\mathfrak{R} = A[[X_1, X_2, \dots, X_d]]$, $P(\mathfrak{R})$ s'identifie au module des séries formelles en les X_j , à coefficients dans K , qui vérifient $\frac{\partial \alpha}{\partial X_j} \in \mathfrak{R}$, pour tout j). On construit au §5 du chapitre II une application A-linéaire continue $w_{\mathfrak{R}} : \widehat{CW}_k(\mathfrak{R}_k) \to P(\mathfrak{R})/p\mathfrak{R}$ qui est, en fait, un isomorphisme.

Soit $\Delta : \mathfrak{R} \to \mathfrak{R} \hat{\otimes}_A \mathfrak{R}$ le coproduit. Cette application se prolonge en une application, encore notée Δ , de $P(\mathfrak{R})$ dans $P(\mathfrak{R} \hat{\otimes}_A \mathfrak{R})$. Soit

$$\mathcal{M}\mathcal{H}(G) = \{\alpha \in P(R) \mid \Delta\alpha - \alpha \hat{\otimes} 1 - 1 \hat{\otimes} \alpha \in p\mathfrak{R} \hat{\otimes}_A \mathfrak{R}\} .$$

On démontre au §6 du chapitre III que $w_{\mathfrak{R}}$ induit un isomorphisme de $\underline{M}(G_k)$ sur $MH(G) = \mathcal{M}\mathcal{H}(G)/p\mathfrak{R}$.

Notons $\mathfrak{L}(G)$ le sous-A-module de $P(R)$ formé des α tels que $\Delta\alpha = \alpha \hat{\otimes} 1 + 1 \hat{\otimes} \alpha$. Soit $\rho(G)$ l'application A-linéaire composée

$$\mathfrak{L}(G) \xrightarrow{\text{incl.can.}} \mathcal{M}\mathcal{H}(G) \xrightarrow{\text{proj.can.}} MH(G) \xrightarrow{\text{iso.can.}} \underline{M}(G_k) \ ;$$

on démontre que l'application $\tilde{\rho}(G) : \mathfrak{L}(G)/p\mathfrak{L}(G) \to \underline{M}(G_k)/\underline{F}\,\underline{M}(G_k)$, induite par passage aux quotients, est un isomorphisme.

Soit Λ_A^{ℓ} la catégorie dont les objets sont les triplets $(\mathfrak{L}, M, \rho)$

- où M est un D_k-module profini, tel que l'action de $\underline{F}$ sur M est injective et $M/\underline{F}M$ est un espace vectoriel sur k de dimension finie,
- où $\mathfrak{L}$ est un A-module libre de rang fini,
- où $\rho : \mathfrak{L} \to M$ est une application A-linéaire qui induit, par passage aux quotients, un isomorphisme $\tilde{\rho} : \mathfrak{L}/p\mathfrak{L} \to M/\underline{F}M$;

et dont les flèches sont évidentes.

On voit que l'on peut considérer la correspondance

$$G \mapsto \mathfrak{L}M(G) = (\mathfrak{L}(G), \underline{M}(G_k), \rho(G))$$

comme un foncteur contravariant additif $\mathfrak{L}M$ de la catégorie des p-groupes formels lisses sur A dans Λ_A^{ℓ} . Le but du §1 du chapitre IV est de montrer que, si $p \neq 2$, ce foncteur est pleinement fidèle et induit une anti-équivalence entre les deux catégories. On a des résultats analogues pour $p = 2$ à condition de se restreindre soit aux groupes "unipotents" soit aux groupes connexes.

Soit G un p-groupe formel lisse et de dimension finie sur A et soit $\mathcal{S}$ un A-anneau qui est un A-module libre de rang fini. On donne aussi une description du groupe $G(\mathcal{S})$ à l'aide du triplet $(\mathcal{L}, M, \rho) = \mathcal{L}M(G)$: soit $\mathcal{S}_k = \mathcal{S} \otimes_A k$, $\mathcal{S}_K = \mathcal{S} \otimes_A K$, soit $N_{\mathcal{L}}(\mathcal{S})$ le groupe des applications A-linéaires de $\mathcal{L}$ dans $\mathcal{S}$ et soit $G_M(\mathcal{S})$ le groupe des applications D_k-linéaires continues de M dans $\widehat{CW}_k(\mathcal{S}_k)$; si $p \neq 2$ ou si G est unipotent le groupe $G(\mathcal{S})$ s'identifie canoniquement, et fonctoriellement en $\mathcal{S}$, au sous-groupe de $N_{\mathcal{L}}(\mathcal{S}) \times G_M(\mathcal{S})$ formé des $(x_{\mathcal{L}}, x_M)$ tels que le diagramme

$$\begin{tikzcd} \mathcal{L} \arrow[r, "x_{\mathcal{L}}"] \arrow[d, "\rho"'] & \mathcal{S}_K \arrow[dr, "\text{proj.}"] & \\ & & \mathcal{S}_K/p\mathcal{S} \\ M \arrow[r, "x_M"] & \widehat{CW}_k(\mathcal{S}_k) \arrow[ur, "w_{\mathcal{S}}"'] & \end{tikzcd}$$

(où $w_{\mathcal{S}}$ est une application A-linéaire construite au § 5 du chapitre II) est commutatif.

Dans le cas des groupes p-divisibles, l'application $\rho(G)$ est injective ; soit $L(G)$ l'image de $\mathcal{L}(G)$ par $\rho(G)$. En associant à G le couple $(L(G), \underline{M}(G_k))$, on obtient une anti-équivalence entre la catégorie des groupes p-divisibles sur A et une catégorie H_A^d dont les objets sont des couples (L, M) , où M est un D_k-module et L un sous-A-module de M , avec des propriétés convenables.

0.9. Pour pouvoir obtenir, sur A' , des résultats analogues à ceux que l'on a sur A , on est conduit à introduire un foncteur $M \mapsto M_{A'}$ de la catégorie des D_k-modules dans celle des A'-modules, et c'est l'objet du § 2 du chapitre IV.

Soit M un D_k-module. Pour tout entier j , soit $M^{(j)}$ le D_k-module déduit de M par l'extension des scalaires σ^j (où σ est le Frobenius absolu). Le décalage (resp. le Frobenius) induit une application D_k-linéaire $v_j : M^{(j)} \to M^{(j+1)}$ (resp. $f_j : M^{(j)} \to M^{(j-1)}$) . Soit $\mathfrak{m}$ l'idéal maximal de A' . Alors $M_{A'}$ est la limite inductive d'un diagramme (assez compliqué) dont les objets sont certains des $\mathfrak{m}^i \otimes_A M^{(j)}$ et les flèches sont construites à partir des v_j et des f_j . Lorsque $e \leq p-1$, $M_{A'}$ est la limite inductive du diagramme

$$\begin{tikzcd} & \mathfrak{m}\otimes_A M \arrow[dl, "\psi_0"'] \arrow[dr, "\chi_0"] & \\ A'\otimes_A M & & p^{-1}\mathfrak{m}\otimes_A M^{(1)} \\ & A'\otimes_A M^{(1)} \arrow[ul, "\varphi_0"] \arrow[ur, "\psi'_0"'] & \end{tikzcd}$$

où $\psi_0(\lambda\otimes\underline{a}) = \lambda\otimes\underline{a}$, $\chi_0(\lambda\otimes\underline{a}) = p^{-1}\lambda\otimes v_0(\underline{a})$, $\psi'_0(\lambda\otimes\underline{a}) = \lambda\otimes\underline{a}$, $\varphi_0(\lambda\otimes\underline{a}) = \lambda\otimes f_1(\underline{a})$.

Dans le cas particulier où M est un A-module libre de type fini (i.e. où $M = \underline{M}(G_k)$, avec G_k un groupe p-divisible sur k), on a une application A'-linéaire de $M_{A'}$ sur un réseau de $M_{K'} = M\otimes_A K'$ (où $K' = \mathrm{Frac}(A')$) que l'on peut décrire très simplement. Le noyau de cette application est la partie de torsion $(M_{A'})_{tor}$ de $M_{A'}$; celle-ci est nulle si $e\leq p-1$, mais est un A'-module fini, non nul, en général, si $e\geq p$.

0.10. Dans le § 3 du chapitre IV, on utilise les constructions du § 2 pour étendre aux A'-algèbres les résultats sur les relèvements des covecteurs dans les A-algèbres obtenus au § 5 du chapitre II :

- soit G un p-groupe formel lisse et de dimension finie sur A' et soit $\mathcal{R}$ son algèbre affine. On définit, comme dans le cas $e = 1$ (n° 0.8) un A'-module topologique $P(\mathcal{R})$. On note $P'(\mathcal{R})$ l'adhérence du sous-A'-module de $P(\mathcal{R})$ engendré par les éléments de la forme $p^{-n}\alpha^{p^n}$, avec $\alpha\in\mathfrak{m}\mathcal{R}$ et $n\in\mathbb{N}$ (si $e\leq p-1$, on a $P'(\mathcal{R}) = \mathfrak{m}\mathcal{R}$) . Soit $\mathcal{R}_k = \mathcal{R}\otimes_{A'} k$. On construit un isomorphisme $w_{\mathcal{R}}$ du A'-module $\widehat{CW}_{k,A'}(\mathcal{R}_k) = (\widehat{CW}_k(\mathcal{R}_k))_{A'}$ sur $P(\mathcal{R})/P'(\mathcal{R})$.
- soit $\mathcal{S}$ un A'-anneau qui est un A'-module libre de rang fini. Soit $\mathcal{S}_K = \mathcal{S}\otimes_A K = \mathcal{S}\otimes_{A'} K'$, $\mathcal{S}_k = \mathcal{S}\otimes_{A'} k = \mathcal{S}/\mathfrak{m}\mathcal{S}$. On définit, comme pour $\mathcal{R}$, un sous-A'-module $P'(\mathcal{S})$ de $\mathcal{S}_K$. On construit alors une application A'-linéaire $w_{\mathcal{S}}$ de $\widehat{CW}_{k,A'}(\mathcal{S}_k) = (\widehat{CW}_k(\mathcal{S}_k))_{A'}$ dans $\mathcal{S}_K/P'(\mathcal{S})$.

0.11. Conservons les hypothèses et les notations du n° précédent pour décrire les résultats du § 4 du chapitre IV .

Le coproduit $\Delta : \mathcal{R}\to\mathcal{R}\hat{\otimes}_A\mathcal{R}$ se prolonge en une application encore notée Δ de $P(\mathcal{R})$ dans $P(\mathcal{R}\hat{\otimes}_A\mathcal{R})$. Nous notons $\mathcal{M}\mathcal{H}_{A'}(G)$ le sous-A'-module fermé de $P(\mathfrak{R})$ formé des α tels que $\Delta\alpha - \alpha\hat{\otimes}1 - 1\hat{\otimes}\alpha \in P'(\mathfrak{R}\hat{\otimes}_A\mathfrak{R})$ et $MH_{A'}(G) = \mathcal{M}\mathcal{H}_{A'}(G)/P'(\mathfrak{R})$. On démontre que l'application $w_{\mathfrak{R}}$ induit un isomorphisme canonique de $M_{A'}(G_k) = (\underline{M}(G_k))_{A'}$ sur $MH_{A'}(G)$.

Soit $\mathfrak{L}_{A'}(G) = \{\alpha \in P(\mathfrak{R}) \mid \Delta\alpha = \alpha\hat{\otimes}1 + 1\hat{\otimes}\alpha\}$ et soit $\rho_{A'}(G)$ l'application A'-linéaire composée

$$\mathfrak{L}_{A'}(G) \xrightarrow{\text{incl.}} \mathcal{M}\mathcal{H}_{A'}(G) \xrightarrow{\text{proj. can.}} MH_{A'}(G) \xrightarrow{\text{iso.can.}} M_{A'}(G_k) \ .$$

On définit alors une catégorie $\Lambda^{\ell}_{A'}$, dont les objets sont des triplets $(\mathfrak{L}, M, \rho)$ où M est un D_k-module, $\mathfrak{L}$ un A'-module et ρ une application A'-linéaire de $\mathfrak{L}$ dans $M_{A'}$ vérifiant des propriétés convenables. La correspondance $G \to (\mathfrak{L}_{A'}(G), \underline{M}(G_k), \rho_{A'}(G))$ définit un foncteur contravariant additif $\mathfrak{L}M_{A'}$ de la catégorie des p-groupes formels lisses et de dimension finie sur A' dans $\Lambda^{\ell}_{A'}$.

On montre que, si $e < p-1$, le foncteur $\mathfrak{L}M_{A'}$ induit une anti-équivalence entre ces deux catégories. Pour tout G et pour tout A'-anneau $\mathfrak{S}$ qui est un A'-module libre de rang fini, on peut donner une description du groupe $G(\mathfrak{S})$, à l'aide du triplet $\mathfrak{L}M_{A'}(G)$ et de l'application $w_{\mathfrak{S}}$, qui est du même genre que ce qui a été fait pour $e = 1$.

Si $e = p-1$, on a des résultats analogues, à condition de se restreindre soit aux groupes unipotents, soit aux groupes connexes.

Lorsque e est quelconque, $\mathfrak{L}M_{A'}$ n'est pas pleinement fidèle (du moins si $e \geq 2p-1$) et je ne sais pas décrire l'image essentielle. Toutefois, à tout objet $(\mathfrak{L}, M, \rho)$ de la catégorie $\Lambda^{\ell}_{A'}$, on peut associer un foncteur en groupes $G_{(\mathfrak{L},M,\rho)}$ sur la catégorie des A'-anneaux qui sont des A'-modules libres de rang fini. Si $(\mathfrak{L}, M, \rho) = \mathfrak{L}M_{A'}(G)$, où G est un p-groupe formel lisse et de dimension finie sur A' , on peut construire deux morphismes de foncteurs en groupes $\varphi_G : G \to G_{(\mathfrak{L},M,\rho)}$ et $\psi_G : G_{(\mathfrak{L},M,\rho)} \to G$ vérifiant $\psi_G \circ \varphi_G = p^t . \mathrm{id}_G$ et $\varphi_G \circ \psi_G = p^t . \mathrm{id}_{G_{(\mathfrak{L},M,\rho)}}$ (où t est un entier qui ne dépend que de e : c'est le plus grand entier tel que $p^t - te \leq p^n - ne$, pour tout entier $n \geq 0$).

0.12. Dans le § 5 du chapitre IV, on applique les résultats du § 4 aux groupes p-divisibles : si G est un groupe p-divisible sur A' , l'application $\rho(G)$

est injective et on note $L_{A'}(G)$ son image. En associant à G le couple $(L_{A'}(G), \underline{M}(G_k))$, on obtient un foncteur contravariant additif $LM_{A'}$ de la catégorie des groupes p-divisibles sur A' dans une catégorie, notée $H^d_{A'}$ dont les objets sont formés de couples (L,M) , avec M un D_k-module et L un sous-A'-module de $M_{A'}$, jouissant de propriétés convenables.

Si $e < p-1$, ce foncteur induit une anti-équivalence.

Si $e \geq p-1$, il n'en est plus de même. Cependant, si G est un groupe p-divisible sur A' , notons $G_{\mathfrak{m}}$ le plus petit sous-schéma en groupes fermé de G tel que, pour tout A'-anneau $\mathcal{S}$ qui est un A'-module libre de rang fini, $G_{\mathfrak{m}}(\mathcal{S})$ soit le noyau de la flèche canonique de $G(\mathcal{S})$ dans $G(\mathcal{S}/\mathfrak{m}\mathcal{S}) = G_k(\mathcal{S}_k)$. On constate que $G_{\mathfrak{m}}$ est un schéma en groupes fini et plat sur A' annulé par p^t et que le quotient $G/G_{\mathfrak{m}}$ est un groupe p-divisible sur A' , isogène à G . On peut donner une description de $G/G_{\mathfrak{m}}$, considéré comme foncteur en groupes sur la catégorie des A'-anneaux qui sont des A'-modules libres de rang fini, à l'aide du couple $LM_{A'}(G)$.

Ceci implique aussi une classification à isogénie près des groupes p-divisibles sur A' : notons $H^d_{K'}$ la catégorie dont les objets sont les couples (L,M) , avec M un $(D_k \otimes_A K)$-module et L un sous-K'-espace vectoriel de $M_{K'} = M \otimes_K K'$, avec une définition évidente pour les flèches.

En associant à G le couple $LM_{K'}(G) = (L_{K'}(G), M_K(G_k))$, avec $M_K(G_k) = \underline{M}(G_k) \otimes_A K$ et $L_{K'}(G) = L_{A'}(G) \otimes_{A'} K'$, on obtient un foncteur contravariant additif pleinement fidèle $LM_{K'}$ de la catégorie "des groupes p-divisibles sur A' , à isogénie près" dans $H^d_{K'}$.

0.13. Soit G un groupe p-divisible sur A' et soit $\mathcal{S}$ un A'-anneau qui est un A'-module libre de rang fini. Les méthodes développées au chapitre IV permettent de décrire le groupe $G(\mathcal{S})$ (où, du moins, si $e \geq p-1$, le groupe $(G/G_{\mathfrak{m}})(\mathcal{S}))$ à l'aide du couple $(L,M) = LM_{A'}(G)$. On doit donc pouvoir décrire les modules galoisiens $T_p(G)$, module de Tate de G (ou $T_p(G/G_{\mathfrak{m}})$ si $e \geq p-1$) et, pour e quelconque, $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$. C'est ce que l'on fait au § 1 du chapitre V .

Cette description est assez compliquée : soit A_C l'anneau des entiers du complété C d'une clôture algébrique $\overline{K}'$ de K' . Soit $\mathrm{Res}(A_C) = \varprojlim_{n \in \mathbb{N}} R_n$, où $R_n = A_C/pA_C$, l'application de transition de R_{n+1} dans R_n étant la flèche $x \mapsto x^p$. On définit le groupe $BW(Res(A_C))$ des "bivecteurs de Witt à coefficients dans $Res(A_C)$" ; si $\mathcal{G} = Gal(\overline{K}'/K')$, on montre que l'on peut considérer $BW(Res(A_C))$ aussi bien comme un D_k-module à gauche que comme un $K[\mathcal{G}]$-module à gauche ; on peut en outre définir une application $K[\mathcal{G}]$-linéaire $bw_{A_C} : BW(Res(A_C)) \to C$ et on note $bw_{A_C,K'} : K' \otimes_K BW(Res(A_C)) \to C$ l'application K'-linéaire déduite de bw_{A_C} par extension des scalaires.

Soit G un groupe p-divisible sur A' et soit $(L_{K'}, M_K) = LM_{K'}(G)$. Pour tout $u \in Hom_{D_k}(M_K, BW(Res(A_C)))$, notons $u_{K'} : K' \otimes_K M_K \to K' \otimes_K BW(Res(A_C))$ l'application K'-linéaire déduite de u par extension des scalaires. Alors $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$ s'identifie au sous-$\mathbb{Q}_p[\mathcal{G}]$-module de $Hom_{D_k}(M_K, BW(Res(A_C)))$ formé des u tels que $u_{K'}(L_{K'}) \subset \ker bw_{A_C,K'}$.

Nous étudierons ailleurs ([24]) le D_k-module $Hom_{\mathbb{Q}_p[\mathcal{G}]}(U, BW(Res(A_C)))$ lorsque U est un $\mathbb{Q}_p[\mathcal{G}]$-module admettant une décomposition de Hodge-Tate. Cela devrait nous permettre en particulier de montrer que, réciproquement, on peut reconstruire le couple $(L_{K'}, M_K)$ associé à un groupe p-divisible G sur A' à partir de la seule connaissance du $\mathbb{Q}_p[\mathcal{G}]$-module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$ (par exemple, M_K devrait s'identifier à $Hom_{\mathbb{Q}_p[\mathcal{G}]}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G), BW(Res(A_C)))$).

0.14. Dans le § 3 du chapitre V, on explique comment on peut retrouver les résultats de Cartier sur la classification des groupes formels lisses et connexes, de dimension finie sur k au moyen de courbes typiques ([7]).

Dans le § 2 , on explique comment on retrouve les résultats de Honda ([32]) sur les mêmes groupes et sur leurs relèvements sur $W(k)$.

0.15. On a compris que ce mémoire repose sur la construction des covecteurs de Witt. C'est Barsotti ([1] , [2] , [3]) qui en a entrepris le premier une étude systématique (pour classifier les groupes formels commutatifs, lisses et connexes, de dimension finie sur k , et, au moins lorsque k est algébriquement clos, les groupes p-divisibles sur k). Notre construction est différente de celle de Barsotti et nous semble plus commode (Barsotti défini les covecteurs à coefficients dans un anneau qui est une algèbre sur $\mathbb{F}_p$ ou sur $\mathbb{Q}$

et dont le groupe additif est muni d'une topologie $\mathbb{Z}_{(p)}$-linéaire ; la somme de deux covecteurs n'est alors pas partout définie et, pour obtenir un groupe additif, il faut se restreindre à une partie convenable de l'ensemble des covecteurs, qu'il faut préciser à chaque fois).

0.16. On a vu que beaucoup des résultats contenus dans ce mémoire se rapprochent de résultats connus et que nous expliquons (not. au chap. V) les rapports avec certains d'entre eux. L'avantage le plus net de nos méthodes nous semble être qu'à chaque fois on obtient une description du groupe formel étudié, <u>considéré comme foncteur en groupes commutatifs</u> sur une catégorie convenable, à l'aide de l'objet qui le classifie (à ma connaissance, le seul cas où ceci avait pu être fait est celui des p-groupes finis unipotents sur k, Grothendieck [30]).

Je voudrais maintenant dire quelques mots sur la construction "traditionnelle" du module de Dieudonné.

C'est Dieudonné qui, le premier, a montré que l'on pouvait classifier certains groupes formels commutatifs sur k, à l'aide de D_k-modules à gauche. Au langage près, il obtient ([16], voir surtout IV) une équivalence entre la catégorie des groupes formels commutatifs, lisses et connexes, de dimension finie sur k et celle des D_k-modules d'un type particulier. Il utilise pour cela le "groupe hyperexponentiel" dont il démontre [17] qu'il est isomorphe au groupe additif des vecteurs de Witt.

Les idées de Dieudonné ont été reprises par de nombreux auteurs (Cartier, Gabriel, Barsotti, Manin,...). Soit Fcu_k la catégorie des p-groupes finis connexes uipotents sur k ; Gabriel [27] a utilisé ses propres travaux sur les catégories pro-artiniennes [26] pour construire une anti-équivalence entre cette catégorie et celle des D_k-modules finis, sur lesquels l'action de $\underline{F}$ et celle de $\underline{V}$ sont nilpotentes : la catégorie Fcu_k a un seul objet simple, le groupe α_p (d'algèbre affine $k[X]/X^p$, avec $\Delta X = X\otimes 1 + 1\otimes X$, $\varepsilon X = 0$) ; on construit son enveloppe injective dans la catégorie $\varinjlim Fcu_k$ (qui se trouve être le groupe formel que nous notons $\widehat{CW}_k^{u,c}$ au § 4 du chapitre II) et on montre que l'anneau des endomorphismes de $\widehat{CW}_k^{u,c}$ est, à peu de chose près, l'anneau D_k.

Il est alors facile d'en déduire une classification complète des p-groupes finis sur k : un peu de cohomologie galoisienne permet de se débarrasser des groupes étales, et les groupes de type multiplicatif se ramènent aux groupes étales par la dualité de Cartier (voir, entre autres, [37] , chap.I, [15] , chap. III, [14] , chap. V). Cette classification se trouve être naturellement équivalente à la notre (cf. cor. 3 à la prop. 5.3 du chap.III) et s'étend, bien sûr, par passage à la limite, aux groupes formels qui sont limite inductive de p-groupes finis. Outre le fait d'être un peu plus générale, notre classification présente l'avantage de ne pas recourir à la dualité de Cartier pour la partie de type multiplicatif. C'est très commode, aussi bien pour décrire le groupe des points d'un groupe formel à l'aide de son module de Dieudonné que pour l'étude des relèvements en caractéristique 0 .

Signalons en passant, bien que ce type de problèmes ne soit pas du tout étudié dans ce mémoire que divers auteurs ont tenté, à juste titre, de rendre cette classification plus précise en étudiant les D_k-modules eux-mêmes (cf. Dieudonné ([16] , VII) pour les groupes formels lisses et connexes, de dim. finie, à isogénie près, Manin [37] pour les mêmes groupes, à isomorphisme près lorsque k est algébriquement clos, Kraft [33] , pour les groupes finis tués par p).

0.17. C'est Grothendieck qui, le premier, a pensé que l'on devait pouvoir classifier les groupes p-divisibles sur A' (à isomorphisme près si $e < p-1$, à isogénie près pour e quelconque) au moyen d'un couple formé du module de Dieudonné M de la fibre spéciale et d'un sous-module d'une extension des scalaires convenable de M . Les premiers résultats ont été annoncés par Cartier ([8] , via l'étude des courbes typiques) et Grothendieck ([29] , [30] , via la construction des cristaux de Dieudonné). Les travaux de Grothendieck ont été repris systématiquement par Messing ([39]) qui obtient une classification complète pour $e < p-1$ ([39] , chap. V, th.1.6), puis par Mazur et Messing ([38]) avec une étude détaillée des extensions universelles des groupes p-divisibles et des schémas abéliens. Le lecteur regrettera, à juste titre, que ne soit pas explicité ici comment ces résultats se relient aux nôtres. Cela nous aurait emmené trop loin.

Nous indiquons toutefois brièvement et sans démonstration (chap. V, n° 3.7, rem. 2) comment on peut construire l'extension universelle d'un groupe p-divisible G sur k (resp. sur A), connaissant son module de Dieudonné (resp. le module de Dieudonné de la fibre spéciale), à l'aide du groupe des covecteurs de Witt. Nous espérons pouvoir généraliser cette construction.

0.18. A l'origine de ce travail, il y a une question que m'avait posée Serre : déterminer l'image de Galois dans la représentation p-adique définie par une courbe elliptique sur $K = \mathrm{Frac}(A)$, avec bonne réduction supersingulière. J'avais fait les calculs "à la main" en me servant des travaux de Hazewinkel [31]. Le contraste entre la simplicité du résultat [19] et la complexité des calculs donnait envie de comprendre ce qui était caché derrière. Dans un premier temps, cela m'a conduit à interpréter les résultats de Honda [32] en termes de modules de Dieudonné "à la Gabriel". D'où ce mémoire qui contient finalement un peu plus que cela.

Dans un deuxième temps, cela m'a conduit à donner une classification des schémas en groupes finis et plats sur A, du même type que celle qui est donnée ici pour les groupes p-divisibles. Les résultats ont été annoncés dans [22] et seront démontrés dans [23]. [23] contiendra aussi les résultats sur les courbes elliptiques et une classification, au moins partielle, des schémas en groupes finis et plats sur A' lorsque $e \leq p-1$.

CHAPITRE I

THÉORIE ÉLÉMENTAIRE DES SCHÉMAS EN GROUPES AFFINES COMMUTATIFS

§ 1.- Schémas affines.

Dans ce paragraphe et dans le suivant, k est un anneau commutatif quelconque.

1.1. On appelle k-anneau toute k-algèbre associative, commutative et unitaire. En d'autres termes un k-anneau est un couple (R, i_R) où R est un anneau commutatif et i_R un homomorphisme de k dans R (par abus de langage, on parlera le plus souvent du k-anneau R, l'application i_R étant sous-entendue). Les k-anneaux forment une catégorie, avec comme flèches les morphismes unitaires de k-algèbres.

1.2. Par définition, un k-foncteur est un foncteur covariant de la catégorie des k-anneaux dans celle des ensembles. Se donner un k-foncteur X revient donc à se donner, pour tout k-anneau R, un ensemble $X(R)$, et, pour tout morphisme $\xi : R \to S$ de k-anneaux, une application $X(\xi) : X(R) \to X(S)$, de manière que, si $\xi : R \to S$ et $\eta : S \to T$ sont des morphismes de k-anneaux, on ait $X(\eta \circ \xi) = X(\eta) \circ X(\xi)$.

Les k-foncteurs forment (à condition de se restreindre à un univers convenable) une catégorie : si X et Y sont deux k-foncteurs, un morphisme $\varphi : X \to Y$ est la donnée d'une famille d'application $\varphi_R : X(R) \to Y(R)$, pour tout k-anneau R, fonctorielle en R (i.e. si $\xi : R \to S$ est un morphisme de k-anneaux, le diagramme

$$\begin{array}{ccc} X(R) & \xrightarrow{\varphi_R} & Y(R) \\ {\scriptstyle X(\xi)}\downarrow & & \downarrow{\scriptstyle Y(\xi)} \\ X(S) & \xrightarrow{\varphi_S} & Y(S) \end{array}$$

est commutatif).

1.3. Si A est un k-anneau, on note $Sp_k A$ le k-foncteur défini par :

- pour tout k-anneau R, $Sp_k A(R) = Hom_k(A,R)$, ensemble des morphismes du k-anneau A dans R ;
- pour tout morphisme de k-anneaux $\xi : R \to S$, $Sp_k A(\xi)$ est l'application qui, à $x : A \to R$, associe $\xi \circ x : A \to S$.

On voit que Sp_k peut être considéré comme un foncteur contravariant de la catégorie des k-anneaux dans celle des k-foncteurs : si $\eta : A \to B$ est un morphisme de k-anneaux, $Sp_k \eta : Sp_k B \to Sp_k A$ est défini par

$$(Sp_k \eta)_R \; : \; x \in Sp_k B(R) = Hom_k(B,R) \mapsto x \circ \eta \in Hom_k(A,R) = Sp_k A(R) \; .$$

1.4. Si X est un k-foncteur et si A est un k-anneau, il existe (lemme de Yoneda) une bijection de l'ensemble $Hom_{k\text{-foncteurs}}(Sp_k A, X)$ des morphismes du k-foncteur $Sp_k A$ dans X sur l'ensemble $X(A)$. Celle-ci s'obtient en associant à $\varphi : Sp_k A \to X$ l'élément $\varphi_A(id_A)$ de $X(A)$. La bijection réciproque associe à $x \in X(A)$ le morphisme $\varphi : Sp_k A \to X$ défini par :

> pour tout k-anneau R, φ_R associe à $\eta : A \to R$ l'élément $X(\eta)(x) \in X(R)$.

En particulier, on voit que si A et B sont des k-anneaux, le lemme de Yoneda définit une bijection entre $Hom_{k\text{-foncteurs}}(Sp_k A, Sp_k B)$ et $Hom_k(B,A)$; autrement dit, le foncteur Sp_k est pleinement fidèle.

1.5. Si X est un k-foncteur, on note $\mathcal{O}_k(X)$ ou, plus simplement, $\mathcal{O}(X)$ l'algèbre affine de X : c'est un k-anneau. En tant qu'ensemble, $\mathcal{O}(X)$ est l'ensemble des morphismes du k-foncteur X dans la droite affine (i.e. le k-foncteur D_k défini par $D_k(R) = R$, qui est visiblement isomorphe à $Sp_k k[T]$). Se donner un élément f de $\mathcal{O}(X)$ revient donc à se donner une famille d'applications $f_R : X(R) \to R$, pour tout k-anneau R, fonctorielle en R. La structure de k-anneaux sur $\mathcal{O}(X)$ est définie par (si $f,g \in \mathcal{O}(X)$, $\lambda \in k$) :

$$\left.\begin{aligned} (f+g)_R(x) &= f_R(x) + g_R(x) \\ (fg)_R(x) &= f_R(x) g_R(x) \\ (\lambda f)_R(x) &= \lambda f_R(x) \end{aligned}\right\} \text{ pour tout k-anneau } R \text{ et tout } x \in X(R) \; .$$

Il y a un morphisme canonique $\alpha_X : X \to Sp_k \mathcal{O}(X)$: pour tout k-anneau R, $(\alpha_X)_R : X(R) \to Hom_k(\mathcal{O}(X), R)$ associe à $x \in X(R)$ l'application $f \mapsto f_R(x)$ de

$\mathcal{O}(X)$ dans R .

On voit que la correspondance $X \mapsto \mathcal{O}(X)$ définit, de manière évidente, un foncteur contravariant $\mathcal{O}_k$ de la catégorie des k-foncteurs dans celle des k-anneaux et que, si $\varphi : X \to Y$ est un morphisme de k-foncteurs, le diagramme

$$\begin{tikzcd} X \arrow[r, "\alpha_X"] \arrow[d, "\varphi"'] & \mathrm{Sp}_k\mathcal{O}(X) \arrow[d, "\mathrm{Sp}_k\mathcal{O}_k(\varphi)"] \\ Y \arrow[r, "\alpha_Y"] & \mathrm{Sp}_k\mathcal{O}(Y) \end{tikzcd}$$

est commutatif.

1.6. On appelle k-<u>schéma affine</u> (ou schéma affine sur k) tout k-foncteur qui est représentable. Autrement dit un k-foncteur X est un k-schéma affine si et seulement s'il existe un k-anneau A tel que $X \simeq \mathrm{Sp}_k A$. On voit immédiatement que ceci est équivalent à dire que la flèche canonique $\alpha_X : X \to \mathrm{Sp}_k\mathcal{O}(X)$ est un isomorphisme. On voit également que :

- le foncteur Sp_k induit une anti-équivalence entre la catégorie des k-anneaux et celle des k-schémas affines (i.e. la sous-catégorie pleine de la catégorie des k-foncteurs dont les objets sont les k-schémas affines) ;
- si X est un k-foncteur et si Y est un k-schéma affine, tout morphisme $\varphi : X \to Y$ se factorise, de manière unique, à travers le morphisme canonique $\alpha_X : X \to \mathrm{Sp}_k\mathcal{O}(X)$.

1.7. La catégorie des k-foncteurs a des limites projectives. En particulier :

- si X et Y sont des k-foncteurs, le k-foncteur $X \times Y$ est défini par $(X \times Y)(R) = X(R) \times Y(R)$; si X et Y sont affines, $X \times Y$ l'est aussi et $\mathcal{O}(X \times Y)$ s'identifie à $\mathcal{O}(X) \otimes_k \mathcal{O}(Y)$;
- plus généralement, si X , Y et Z sont des k-foncteurs et si $\varphi : X \to Z$ et $\psi : Y \to Z$ sont des morphismes de k-foncteurs, le k-foncteur $X \times_Z Y$ est défini par $(X \times_Z Y)(R) = \{(x,y) \in X(R) \times Y(R) \mid \varphi_R(x) = \psi_R(y)\}$; si X , Y et Z sont affines, $X \times_Z Y$ l'est aussi et $\mathcal{O}(X \times_Z Y)$ s'identifie à $\mathcal{O}(X) \otimes_{\mathcal{O}(Z)} \mathcal{O}(Y)$.

1.8. Soit k' un k-anneau. Pour tout k'-anneau R , nous notons $R_{[k]}$ le k-anneau déduit de R par restriction des scalaires.

Si X est un k-foncteur, nous notons $X_{k'}$ le k'-foncteur défini par $X_{k'}(R) = X(R_{[k]})$, pour tout k'-anneau R , et les flèches évidentes. La correspondance $X \mapsto X_{k'}$ définit, de manière évidente, un foncteur covariant de la catégorie des k-foncteurs dans celle des k'-foncteurs, que l'on appelle le <u>changement de base</u> ou l'<u>extension des scalaires</u>. On voit que

- le changement de base commute aux limites projectives ;
- si X est un k-schéma affine, $X_{k'}$ est un k'-schéma affine dont l'algèbre affine s'identifie à $k' \otimes_k \mathcal{O}_k(X)$.

§ 2.- <u>Groupes affines</u>.

2.1. On appelle k-<u>foncteur en groupes</u> tout objet en groupes dans la catégorie des k-foncteurs. Il revient au même de dire qu'un k-foncteur en groupes est un foncteur covariant de la catégorie des k-anneaux dans celle des groupes.

Si G est un k-foncteur, se donner une loi de composition interne sur chaque $G(R)$ (pour R décrivant les k-anneaux), fonctorielle en R , revient à se donner un morphisme de k-foncteurs $m_G : G \times G \to G$. On laisse au lecteur le soin d'écrire toutes les propriétés que doit vérifier m_G pour que chaque $G(R)$ soit un groupe.

Les k-foncteurs en groupes forment une catégorie : un morphisme $\varphi : G \to H$ de k-foncteurs en groupes est un morphisme des k-foncteurs sous-jacents, compatible avec la structure de groupe, i.e. tel que le diagramme

$$\begin{tikzcd} G \times G \arrow[r, "m_G"] \arrow[d, "\varphi \times \varphi"'] & G \arrow[d, "\varphi"] \\ H \times H \arrow[r, "m_H"] & H \end{tikzcd}$$

soit commutatif.

2.2. On appelle k-<u>schéma en groupes affine</u> ou, plus simplement, k-<u>groupe affine</u> (ou encore groupe affine sur k) tout k-foncteur en groupes dont le k-foncteur sous-jacent est un k-schéma affine.

Si G est un k-schéma affine et si $B = \mathcal{O}(G)$, se donner un morphisme

$m_G : G \times G \to G$ revient, d'après le lemme de Yoneda, à se donner un morphisme de k-anneaux $\Delta_G = \Delta_B : B \to B \otimes_k B$.

On vérifie alors que, si R est un k-anneau et si $x, y : B \to R$ sont des éléments de $G(R)$, le composé de x et y est l'application

$$B \xrightarrow{\Delta_B} B \otimes_k B \xrightarrow{x \otimes y} R \otimes_k R \xrightarrow{\text{produit}} R .$$

Si B est un k-anneau et si $\Delta_B : B \to B \otimes B$ est un morphisme de k-anneaux, on voit facilement que pour que $Sp_k \Delta_B$ munisse $G = Sp_k B$ d'une structure de k-groupe affine, il faut et il suffit que les trois propriétés suivantes soient vérifiées :

(B_1) (associativité) le diagramme

$$\begin{tikzcd}
B \arrow[r, "\Delta_B"] \arrow[d, "\Delta_B"'] & B \otimes B \arrow[d, "id_B \otimes \Delta_B"] \\
B \otimes B \arrow[r, "\Delta_B \otimes id_B"] & B \otimes B \otimes B
\end{tikzcd}$$

est commutatif ;

(B_2) (existence d'un élément-neutre) il existe un morphisme de k-anneaux $\epsilon_B : B \to k$ tel que le diagramme

$$\begin{tikzcd}
 & B \otimes B \arrow[r, "id_B \otimes \epsilon_B"] & B \otimes k \arrow[d, "\wr"] \\
B \arrow[ur, "\Delta_B"] \arrow[rr, "id_B"] \arrow[dr, "\Delta_B"'] & & B \arrow[d, "\wr"] \\
 & B \otimes B \arrow[r, "\epsilon_B \otimes id_B"'] & k \otimes B
\end{tikzcd}$$

est commutatif ;

(B_3) (existence d'un inverse) il existe un endomorphisme σ_B du k-anneau B tel que le diagramme

$$\begin{tikzcd}
 & B \otimes B \arrow[r, "id_B \otimes \sigma_B"] & B \otimes B \arrow[dr, "\text{produit}"] & \\
B \arrow[ur, "\Delta_B"] \arrow[r, "\epsilon_B"] \arrow[dr, "\Delta_B"'] & k \arrow[rr, "i_B"] & & B \\
 & B \otimes B \arrow[r, "\sigma_B \otimes id_B"'] & B \otimes B \arrow[ur, "\text{produit}"'] &
\end{tikzcd}$$

est commutatif.

Remarque : il résulte de l'unicité de l'élément-neutre et de l'inverse dans un ensemble muni d'une loi de composition interne associative que, étant donné Δ_B vérifiant (B_1) , les applications ε_B et σ_B vérifiant (B_2) et (B_3) , si elles existent, sont uniques.

2.3. Nous appelons k-bigèbre la donnée d'un couple (B,Δ_B) où B est un k-anneau et $\Delta_B : B \to B \otimes_k B$ est un morphisme de k-anneaux vérifiant les axiomes (B_1) , (B_2) et (B_3) . Par abus de langage, nous parlerons de la k-bigèbre B , l'application Δ_B étant sous-entendue. L'application Δ_B s'appelle le coproduit, ε_B s'appelle l'augmentation et σ_B l'antipodisme. On note B^+ l'idéal d'augmentation, i.e. le noyau de ε_B .

Soit B une k-bigèbre. On voit que le composé $\varepsilon_B \circ i_B$ est l'identité sur k . En particulier, l'application i_B est injective et nous l'utilisons pour identifier k à un sous-anneau de B ; on voit que, en tant que k-module, $B = k \oplus B^+$.

Pour tout $f \in B$, posons $\delta f = 1 \otimes f - \Delta_B f + f \otimes 1$. Il résulte de (B_2) que si $f \in B^+$, alors $\delta f \in B^+ \otimes B^+$.

Les k-bigèbres forment une catégorie : un morphisme $\eta : B \to C$ de k-bigèbres est un morphisme des k-anneaux sous-jacents tel que le diagramme

$$\begin{array}{ccc} B & \xrightarrow{\Delta_B} & B \otimes_k B \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta \otimes \eta} \\ C & \xrightarrow{\Delta_C} & C \otimes_k C \end{array}$$

est commutatif.

On voit que le foncteur Sp_k peut encore être considéré comme un foncteur contravariant de la catégorie des k-bigèbres dans celle des k-foncteurs en groupes et qu'il induit une anti-équivalence entre les catégorie des k-bigèbres et celle des k-groupes affines (i.e. la sous-catégorie pleine de la catégorie des k-foncteurs en groupes dont les objets sont les k-groupes affines). Un foncteur quasi-inverse consiste à associer à tout k-groupe affine G son algèbre affine $\mathcal{O}(G)$; le produit tensoriel $\mathcal{O}(G) \otimes_k \mathcal{O}(G)$ s'identifie à l'algèbre affine de $G \times G$ et le coproduit $\Delta_G = \Delta_{\mathcal{O}(G)} : \mathcal{O}(G) \to \mathcal{O}(G) \otimes_k \mathcal{O}(G)$ est défini par :

si $f \in \mathcal{O}(G)$, pour tout k-anneau R , $(\Delta_G f)_R((x,y)) = f_R(xy)$ si $(x,y) \in G(R) \times G(R) = (G \times G)(R)$.

Si G est un k-groupe affine et si B est une k-bigèbre, l'ensemble des morphismes de k-foncteurs de $\mathrm{Sp}_k B$ dans G s'identifie, par le lemme de Yoneda, à $G(B)$. On voit que, dans cette identification, un élément $x \in G(B)$ est un morphisme de k-foncteurs en groupes si et seulement s'il vérifie

$$G(\Delta_B)(x) = G(i_1)(x) . G(i_2)(x) ,$$

où i_1 et $i_2 : B \to B \otimes_k B$ sont définies par $i_1(f) = f \otimes 1$ et $i_2(f) = 1 \otimes f$.

2.4. La catégorie des k-foncteurs en groupes admet des limites projectives et celle des k-bigèbres a des limites inductives. En particulier :

- la catégorie des k-foncteurs en groupes a un objet nul : le groupe e_k défini par $e_k(R) = \{1\}$, pour tout k-anneau R ; c'est un k-groupe affine dont l'algèbre affine s'identifie à k ;

- si G et G' sont deux k-foncteurs en groupes, le k-foncteur en groupes $G \times G'$ est défini par $(G \times G')(R) = G(R) \times G'(R)$, pour tout k-anneau R ; si G et G' sont affines d'algèbres affines B et B' , $G \times G'$ est affine, d'algèbre affine $B \otimes_k B'$; on voit que le coproduit $\Delta_{B \otimes B'} : B \otimes B' \to B \otimes B' \otimes B \otimes B'$ est le composé
$$B \otimes B' \xrightarrow{\Delta_B \otimes \Delta_{B'}} B \otimes B \otimes B' \otimes B' \xrightarrow{id_B \otimes t \otimes id_{B'}} B \otimes B' \otimes B \otimes B'$$
où $t : B \otimes B' \to B' \otimes B$ est définie par $t(f \otimes f') = f' \otimes f$;

- plus généralement, si G , G' et H sont trois k-foncteurs en groupes et si $\varphi : G \to H$ et $\psi : G' \to H$ sont des morphismes de k-foncteurs en groupes, le produit fibré $G \times_H G'$ est le k-foncteur en groupes défini par $(G \times_H G')(R) = G(R) \times_{H(R)} G'(R)$, pour tout k-anneau R ; si G , G' et H sont affines, il en est de même de $G \times_H G'$ et son algèbre affine s'identifie à $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G')$.

2.5. Si $G = \mathrm{Sp}_k B$ est un k-groupe affine, on voit que G est commutatif (i.e., pour tout k-anneau R , $G(R)$ est un groupe abélien) si et seulement si la bigèbre B est "<u>co-commutative</u>", i.e. si l'image par Δ_B de tout élément de B est un tenseur symétrique, ou encore si B vérifie l'axiome

(B_4) (commutativité) le diagramme

$$\begin{tikzcd} & B\otimes_k B \arrow[dr, "t"] & \\ B \arrow[ur, "\Delta_B"] \arrow[rr, "\Delta_B"] & & B\otimes_k B \end{tikzcd}$$

(où $t(f\otimes g) = g\otimes f)$ est commutatif.

Dans toute la suite de ce mémoire, tous les k-foncteurs en groupes considérés (et, par conséquent, tous les k-groupes affines) sont supposés commutatifs, et le mot "commutatif" sera sous-entendu. De même, par k-bigèbre nous entendons désormais k-bigèbre co-commutative. Pour tout k-foncteur en groupes G, nous notons additivement le groupe abélien $G(R)$.

On voit immédiatement que les catégories des k-foncteurs en groupes, des k-groupes affines et des k-bigèbres sont additives. La première d'entre elles est abélienne, mais les deux autres (qui sont anti-équivalentes) ne le sont pas en général (cf. § 6).

§ 3.- Anneaux et modules profinis.

Les résultats de ce paragraphe sont énoncés sans démonstration et sont empruntés, pour l'essentiel à [28], chap. 0, n° 7.1 et 7.7 (pour les n° 3.1 et 3.2) et à [13], exposé VII_B, §0 (pour les n° suivants ; voir aussi [26], p. 390 et suivantes, et [14], chap. V, §2).

Dans ce paragraphe, tous les anneaux sont supposés commutatifs.

3.1. On dit qu'un anneau topologique A est linéairement topologisé s'il existe un système fondamental de voisinages de 0 formé d'idéaux (ceux-ci sont alors ouverts).

Si A est un anneau linéairement topologiqé, on note Ω_A l'ensemble des idéaux ouverts de A et $\hat{A}$ le séparé complété de A ; on voit que $\hat{A}$ s'identifie à $\varprojlim_{\mathfrak{a}\in\Omega_A} A/\mathfrak{a}$, chaque quotient étant muni de la topologie discrète et que $\hat{A}$ est lui-même un anneau linéairement topologisé.

Si A est un anneau topologique, on appelle A-anneau topologique la donnée d'un couple (B, i_B) où B est un anneau topologique et $i_B : A \to B$

un homomorphisme continu. Par abus de langage, on parle du A-anneau topologique B, l'application i_B étant sous-entendue.

Si A est un anneau linéairement topologisé, un A-<u>anneau linéairement topologisé</u> est donc un couple (B, i_B) où B est un anneau linéairement topologisé et $i_B : A \to B$ un homomorphisme continu.

Si A est un anneau linéairement topologisé et si M est un A-module topologique, on dit que M est <u>linéairement topologisé</u> s'il existe un système fondamental de voisinages de 0 formé de sous-modules (ceux-ci sont alors ouverts).

Si M est un A-module linéairement topologisé, on note Λ_M l'ensemble des sous-modules ouverts de M et $\hat{M}$ le séparé complété de M ; on voit que $\hat{M}$ s'identifie à $\varprojlim_{N \in \Lambda_M} M/N$, chaque quotient M/N étant muni de la topologie discrète, et que $\hat{M}$ a une structure naturelle de $\hat{A}$-module linéairement topologisé.

3.2. Soit A un anneau linéairement topologisé, séparé et complet, et soient M et N deux A-modules linéairement topologisés, séparés et complets. Le produit tensoriel $M \otimes_A N$ peut être considéré comme un A-module linéairement topologisé en prenant comme système fondamental de voisinages de 0 les sous-modules de la forme $\mathrm{Im}(M' \otimes_A N) + \mathrm{Im}(M \otimes_A N')$, pour $M' \in \Lambda_M$ et $N' \in \Lambda_N$. On appelle cette topologie le <u>produit tensoriel des topologies</u> de M et de N, et on note $M \hat{\otimes}_A N$ le séparé complété de $M \otimes_A N$ pour cette topologie. On voit facilement que $M \hat{\otimes}_A N$ s'identifie à $\varprojlim (M/M') \otimes_{A/\mathfrak{a}} (N/N')$, pour $\mathfrak{a} \in \Omega_A$, $M' \in \Lambda_M$, $N' \in \Lambda_N$ tels que $\mathfrak{a}M \subset M'$ et $\mathfrak{a}N \subset N'$, chaque quotient étant muni de la topologie discrète.

Soit A un anneau linéairement topologisé, séparé et complet et soit M, N, M', N' quatre A-modules linéairement topologisés, séparés et complets. Si $u : M \to M'$ et $v : N \to N'$ sont des applications A-linéaires continues, il est clair que l'application $u \otimes v$ définit par passage aux produits tensoriels complétés une application A-linéaire continue de $M \hat{\otimes}_A N$ dans $M' \hat{\otimes}_A N'$; on la note $u \hat{\otimes} v$.

On définit de la même manière le produit tensoriel complété d'un nombre fini quelconque de A-modules linéairement topologisés. Les propriétés usuelles d'associativité et commutativité sont vérifiées.

Si B et C sont deux A-anneaux linéairement topologisés, séparés et complets, on voit que la topologie du produit tensoriel sur $B \otimes_A C$ admet un système fondamental de voisinages de 0 formé des idéaux $\mathrm{Im}(\mathfrak{b} \otimes_A C) + \mathrm{Im}(B \otimes_A \mathfrak{c})$, pour $\mathfrak{b} \in \Omega_B$ et $\mathfrak{c} \in \Omega_C$. On en déduit que $B \hat{\otimes}_A C$ peut être considéré comme un A-anneau linéairement topologisé, séparé et complet. Les applications $b \mapsto b \otimes 1$ et $c \mapsto 1 \otimes c$ de B et C dans $B \otimes_A C$ induisent des applications continues de B et C dans $B \hat{\otimes}_A C$. On voit que celles-ci permettent de considérer $B \hat{\otimes}_A C$ comme "la" somme directe de B et C dans la catégorie des A-anneaux linéairement topologisés, séparés et complets.

3.3. On appelle <u>anneau pseudo-compact</u> tout anneau linéairement topologisé, séparé et complet, A, tel que, pour tout $\mathfrak{a} \in \Omega_A$, l'anneau $A/\mathfrak{a}$ est artinien.

Les anneaux pseudo-compacts forment une sous-catégorie pleine de la catégorie des anneaux linéairement topologisés, séparés et complets. Si A est un anneau pseudo-compact, on voit que tout idéal ouvert de A est fermé et que l'adhérence $\bar{\mathfrak{a}}$ d'un idéal quelconque $\mathfrak{a}$ de A est l'intersection des idéaux ouverts qui contiennent $\mathfrak{a}$. Notons $\mathfrak{M}_A$ l'ensemble des idéaux maximaux ouverts de A et, pour tout $\mathfrak{m} \in \mathfrak{M}_A$, posons $A_\mathfrak{m} = \varprojlim (A/\mathfrak{a})_{\mathfrak{m}/\mathfrak{a}}$, pour tous les idéaux ouverts $\mathfrak{a}$ de A contenus dans $\mathfrak{m}$. On voit facilement que chaque $A_\mathfrak{m}$ est un anneau local pseudo-compact et que A s'identifie à $\prod_{\mathfrak{m} \in \mathfrak{M}_A} A_\mathfrak{m}$.

Nous notons $\mathfrak{r}_A$ le radical de Jacobson de A. C'est un idéal fermé qui est l'intersection des idéaux maximaux ouverts de A ; c'est aussi l'ensemble des $x \in A$ qui sont topologiquement nilpotents. Soit $x \in A$ et soit, pour tout $\mathfrak{m} \in \mathfrak{M}_A$, $x_\mathfrak{m}$ la projection de x sur $A_\mathfrak{m}$; on voit que $x \in \mathfrak{r}_A$ si et seulement si chaque $x_\mathfrak{m}$ est dans l'idéal maximal de $A_\mathfrak{m}$. Enfin, si l'on note $k_\mathfrak{m}$ le corps résiduel de $A_\mathfrak{m}$, il est clair que $A/\mathfrak{r}_A$ s'identifie à $\prod_{\mathfrak{m} \in \mathfrak{M}_A} k_\mathfrak{m}$.

3.4. Dans toute la suite de ce paragraphe, on désigne par k un anneau pseudo-compact.

On appelle k-module pro-artinien (resp. k-module profini) tout k-module linéairement topologisé, séparé et complet tel que, pour tout $M' \in \Lambda_M$, le quotient M/M' est un k-module artinien (resp. de longueur finie). Les k-modules pro-artiniens forment une catégorie, avec comme flèches les applications k-linéaires continues.

Si M est un k-module pro-artinien et si M' est un sous-module fermé, M' et M/M' , munis de la topologie induite, sont des k-modules pro-artiniens. De plus, si $u : M \to N$ est un morphisme de k-modules pro-artiniens, l'image (ensembliste) de u est un sous-k-module fermé de N . On en déduit que la catégorie des k-modules pro-artiniens est abélienne et on voit que la catégorie des k-modules profinis en est une sous-catégorie épaisse (elle est donc aussi abélienne).

Si $(M_i)_{i\in I}$ est un système projectif de k-modules pro-artiniens (resp. profinis), la limite projective des M_i (dans la catégorie des k-modules), munie de la topologie de la limite projective, est un k-module pro-artinien (resp. profini) et s'identifie à la limite projective des M_i dans la catégorie des k-modules pro-artiniens.

Si de plus I est un ensemble ordonné filtrant, le foncteur $\varprojlim_{i\in I}$ est exact. En particulier, si $(M_i)_{i\in I}$ est un système projectif filtrant de k-modules pro-artiniens, et si les applications de transition sont surjectives, l'application canonique de $\varprojlim_{i\in I} M_i$ dans chaque M_i est surjective.

Si M et N sont deux k-modules pro-artiniens (resp. profinis), il en est de même du produit tensoriel complété $M \hat{\otimes}_A N$. En outre, le produit tensoriel complété est exact à droite et commute aux produits infinis. En particulier, si $k = \prod_{\mathfrak{m}\in\mathfrak{M}_k} k_{\mathfrak{m}}$, tout k-module pro-artinien M s'identifie au produit $\prod_{\mathfrak{m}\in\mathfrak{M}_k} M_{\mathfrak{m}}$ de ses composantes locales $M_{\mathfrak{m}} = k_{\mathfrak{m}} \hat{\otimes}_k M$.

Nous appelons k-module fini tout k-module profini qui est de longueur finie. Si M est un k-module fini, la topologie de M est donc la topologie discrète. Si M est un k-module fini et si N est un k-module profini, on voit que l'application canonique de $M \otimes_k N$ dans $M \hat{\otimes}_k N$ est bijective.

Dans le cas où k est un produit fini d'anneaux locaux nœthériens (nécessairement séparés et complets), tout idéal de k est fermé et tout k-module, muni de la topologie discrète, devient un k-module topologique. Les k-modules finis ne sont alors rien d'autre que les k-modules de longueur finie munis de la topologie discrète.

3.5. Pour tout ensemble I , le k-module k^I , muni de la topologie produit est un k-module profini. On dit qu'un k-module profini M est <u>topologiquement libre</u> s'il est isomorphe à un module de la forme k^I . On voit qu'il revient au même de dire qu'il existe une famille $(e_i)_{i\in I}$ d'éléments de M tels que

- d'une part, pour tout $M' \in \Lambda_M$, presque tous les e_i sont dans M' ;
- d'autre part, tout élément de M s'écrit d'une manière et d'une seule sous la forme $\sum_{i\in I} a_i e_i$, avec les a_i dans k .

Une telle famille $(e_i)_{i\in I}$ est appelée une <u>base topologique</u> de M .

On a le résultat suivant :

PROPOSITION 3.1. - <u>Soit</u> P <u>un</u> k-<u>module profini</u>. <u>Les assertions suivantes sont équivalentes</u> :

i) <u>le</u> k-<u>module</u> P <u>est projectif</u> ;

ii) <u>le foncteur</u> $M \mapsto M \hat{\otimes}_k P$ <u>(de la catégorie des</u> k-<u>modules profinis dans elle-même)</u> <u>est exact</u> ;

iii) <u>pour tout idéal maximal ouvert</u> $\mathfrak{m}$ <u>de</u> k , <u>la composante locale</u> $P_{\mathfrak{m}} = k_{\mathfrak{m}} \hat{\otimes}_k P$ <u>de</u> P <u>est un</u> $k_{\mathfrak{m}}$-<u>module topologiquement libre</u>.

On appelle k-<u>module topologiquement plat</u> tout k-module profini vérifiant les conditions équivalentes de la proposition 3.1.

3.6. Si N est un k-module (sans topologie), nous notons N' le k-module topologique des applications linéaires de N dans k (la topologie étant celle de la convergence simple). Il est clair que l'on peut considérer la correspondance $N \mapsto N'$ comme un foncteur contravariant de la catégorie des k-modules dans celle des k-modules topologiques.

De même, si M est un k-module topologique, nous notons M^* le k-module des applications linéaires continues de M dans k . La correspondance $M \mapsto M^*$ est, ici encore, fonctorielle.

Lorsque k est artinien (en particulier lorsque k est un corps), on voit que $M \mapsto M^*$ induit une anti-équivalence entre la catégorie des k-modules profinis projectifs (resp. topologiquement libres) et celle des k-modules projectifs (resp. libres), et que $N \mapsto N'$ est un quasi-inverse de $M \mapsto M^*$. Si N est un k-module libre et si $(e_i)_{i\in I}$ est une base de N, on voit que les e'_i, définis par $e'_i(e_j) = \delta_{i,j}$ forment une base topologique de N' ; on l'appelle la base duale de celle des e_i et réciproquement.

Toujours lorsque k est artinien, on voit que, si M et P sont des k-modules profinis et si P est projectif, les k-modules $(M \hat{\otimes}_k P)^*$ et $M^* \otimes_k P^*$ sont isomorphes. De même, si N et Q sont des k-modules et si Q est projectif, $(N \otimes_k Q)'$ et $N' \hat{\otimes}_k Q'$ sont isomorphes.

3.7. On appelle k-<u>anneau profini</u> tout k-anneau topologique dont le k-module sous-jacent est profini.

Si A est un k-anneau profini et si N est un sous-k-module de A, on montre qu'il existe un idéal ouvert $\mathfrak{a}$ de A contenu dans N. On en déduit que A est un anneau pseudo-compact.

La catégorie des k-anneaux profinis (les flèches sont les homomorphismes continus de k-anneaux) admet des limites projectives : si $(A_i)_{i\in I}$ est un système projectif de k-anneaux profinis, le k-module sous-jacent à la limite projective des A_i est la limite projective des k-modules sous-jacents et la structure d'anneau est évidente.

Cette catégorie admet aussi des limites inductives finies. En particulier :

- si A et B sont deux k-anneaux profinis, il en est de même de $A \hat{\otimes}_k B$ et $A \hat{\otimes}_k B$ s'identifie à la somme directe de A et de B ;
- plus généralement, si A, B et C sont trois k-anneaux profinis et si $\xi : C \to A$ et $\eta : C \to B$ sont des morphismes de k-anneaux profinis, la somme amalgamée de A et de B au-dessous de C s'identifie au k-anneau profini $A \hat{\otimes}_C B$.

On appelle k-<u>anneau fini</u> tout k-anneau profini dont le k-module sous-jacent est de longueur finie. Dans le cas où k est un produit fini d'anneaux locaux nœthériens, un k-anneau fini n'est rien d'autre qu'un k-anneau artinien muni de la topologie discrète.

§ 4.- Schémas formels.

Dans tout ce paragraphe, k désigne un anneau commutatif pseudo-compact.

4.1. On appelle k-foncteur formel tout foncteur covariant de la catégorie des k-anneaux finis dans celle des ensembles.

Comme les k-foncteurs (cf. § 1) les k-foncteurs formels forment une catégorie.

Soit X un k-foncteur formel. Pour tout k-anneau profini R, on pose $X(R) = \varprojlim_{\mathfrak{a}\in\Omega_R} X(R/\mathfrak{a})$. Il est clair que l'on a ainsi prolongé X en un foncteur covariant de la catégorie des k-anneaux profinis dans celle des ensembles. On voit facilement que le foncteur ainsi défini commute aux limites projectives filtrantes. Il suffit en effet de le montrer lorsque $(R_i)_{i\in I}$ est un système projectif filtrant de k-anneaux finis. Soit, pour tout couple $i \leq j$ d'éléments de I, $f_{ij} : R_j \to R_i$ l'application de transition. Pour tout i, soit $R'_i = \bigcap_{j\geq i} f_{ij}(R_j)$. Comme R_i est un k-anneau fini, il existe $j_i \in I$ tel que $R'_i = f_{ij_i}(R_{j_i})$; on en déduit que l'application évidente de $\varprojlim X(R'_i)$ dans $\varprojlim X(R_i)$ est une bijection. Si $R = \varprojlim R_i$, on a aussi $R = \varprojlim R'_i$ et l'application canonique $R \to R'_i$ est surjective (cf. n° 3.4) ; soit $\mathfrak{a}_i$ son noyau ; on voit que l'ensemble des $\mathfrak{a}_i$ est cofinal dans l'ensemble des idéaux ouverts de R et on en déduit que $X(R) = \varprojlim_{\mathfrak{a}\in\Omega_R} X(R/\mathfrak{a})$ s'identifie à $\varprojlim X(R'_i)$.

Aussi, dans toute la suite, un k-foncteur formel sera considéré aussi bien comme un foncteur de la catégorie des k-anneaux finis dans les ensembles que comme un foncteur de la catégorie des k-anneaux profinis dans les ensembles, qui commute aux limites projectives filtrantes.

4.2. Si A est un k-anneau profini, on note $\mathrm{Spf}_k A$ le k-foncteur formel défini par :

- pour tout k-anneau fini R, $\mathrm{Spf}_k A(R) = \mathrm{Hom}_k^{\mathrm{cont}}(A,R)$, ensemble des morphismes (de k-anneaux profinis) de A dans R ;
- pour tout morphisme de k-anneaux finis $\xi : R \to S$, $\mathrm{Spf}_k A(\xi)$ est l'application qui, à $x : A \to R$, associe $\xi \circ x : A \to S$.

De la même manière qu'au n° 1.3, on voit que l'on peut considérer Spf_k comme un foncteur contravariant de la catégorie des k-anneaux profinis dans celle des k-foncteurs formels.

Si $(A_i)_{i \in I}$ est un système projectif filtrant de k-anneaux finis et si $A = \varprojlim A_i$, un raisonnement analogue à celui fait au n° 4.1 montre que, pour tout k-anneau fini R, $\mathrm{Spf}_k A(R) = \varinjlim \mathrm{Spf}_k A_i(R)$, autrement dit que $\mathrm{Spf}_k A = \varinjlim \mathrm{Spf}_k A_i$.

Soient A et R deux k-anneaux profinis. Il est clair que $\mathrm{Spf}_k A(R) = \varprojlim_{\mathfrak{a} \in \Omega_R} \mathrm{Hom}_k^{\mathrm{cont}}(A, R/\mathfrak{a})$ s'identifie à l'ensemble $\mathrm{Hom}_k^{\mathrm{cont}}(A,R)$ des morphisme (de k-anneaux profinis) de A dans R. On prendra garde toutefois que, si R n'est pas un k-anneau fini et si $A = \varprojlim A_i$, $\mathrm{Spf}_k A(R)$ ne s'identifie pas en général à $\varinjlim \mathrm{Spf}_k A_i(R)$.

4.3. Si X est un k-foncteur formel et si A est un k-anneau fini, il existe une bijection naturelle entre l'ensemble $\mathrm{Hom}_{k\text{-ff}}(\mathrm{Spf}_k A, X)$ des morphismes de k-foncteurs formels de $\mathrm{Spf}_k A$ dans X et l'ensemble $X(A)$ (lemme de Yoneda). Celle-ci se construit comme au n° 1.4.

Si maintenant X est un k-foncteur formel et si A est un k-anneau profini, on a $\mathrm{Hom}_{k\text{-ff}}(\mathrm{Spf}_k A, X) = \mathrm{Hom}(\varinjlim_{\mathfrak{a} \in \Omega_A} \mathrm{Spf}_k(A/\mathfrak{a}), X) = \varprojlim \mathrm{Hom}(\mathrm{Spf}_k(A/\mathfrak{a}, X)$.
Ce dernier ensemble s'identifie, par le lemme de Yoneda, à $\varprojlim X(A/\mathfrak{a}) = X(A)$ et on a encore une bijection entre $\mathrm{Hom}_{k\text{-ff}}(\mathrm{Spf}_k A, X)$ et $X(A)$. En particulier si A et B sont des k-anneaux profinis, on a une bijection entre $\mathrm{Hom}_{k\text{-ff}}(\mathrm{Spf}_k A, \mathrm{Spf}_k B)$ et $\mathrm{Hom}_k^{\mathrm{cont}}(A,B)$; autrement dit, le foncteur Spf_k est pleinement fidèle.

4.4. Tout k-foncteur X définit, par restriction à la catégorie des k-anneaux finis, un k-foncteur formel noté $\hat{X}$ (on a donc $\hat{X}(R) = X(R)$ pour tout k-anneau fini R) et appelé le complété formel de X.

Par exemple, le complété formel $\hat{D}_k$ de la droite affine D_k est défini par $\hat{D}_k(R) = R$, pour tout k-anneau fini R, et les flèches évidentes (dans ce cas particulier, on voit que l'on a aussi $\hat{D}_k(R) = R$, pour tout k-anneau profini R). On prendra garde de ne pas confondre $\hat{D}_k$ avec la "droite formelle" qui est le k-foncteur formel $\hat{D}_k^o$ qui associe à tout k-anneau fini son radical.

4.5. Si X est un k-foncteur formel, on note $\mathcal{O}_k^f(X)$ ou, plus simplement, $\mathcal{O}^f(X)$ l'algèbre affine de X. En tant qu'ensemble, $\mathcal{O}^f(X)$ est l'ensemble des morphismes du k-foncteur formel X dans $\hat{D}_k$. Un élément f de $\mathcal{O}^f(X)$ est donc une famille d'applications $f_R : X(R) \to R$, pour tout k-anneau fini R, variant fonctoriellement en R. La structure d'anneau sur $\mathcal{O}^f(X)$ est définie comme au n° 1.5. La topologie est celle de la convergence simple. Autrement dit, pour tout k-anneau fini R et tout $x \in X(R)$, soit $\varphi_{x,R}$ l'application de $\mathcal{O}^f(X)$ dans R définie par $\varphi_{x,R}(f) = f_R(x)$; la topologie de $\mathcal{O}^f(X)$ est la topologie la moins fine rendant toutes ces applications continues. Il est clair que $\mathcal{O}^f(X)$ est ainsi un anneau linéairement topologisé dont les idéaux ouverts sont les idéaux qui contiennent une intersection finie d'idéaux de la forme $\ker \varphi_{x,R}$. On voit que $\mathcal{O}^f(X)$ est séparé et complet pour cette topologie ; comme chaque quotient $\mathcal{O}^f(X)/\ker \varphi_{x,R}$ est un k-anneau fini, $\mathcal{O}^f(X)$ est bien un k-anneau profini.

Ici encore, il y a un morphisme canonique $\alpha_X : X \to \mathrm{Spf}_k\mathcal{O}(X)$, défini comme au n° 1.5, la correspondance $X \mapsto \mathcal{O}(X)$ peut être considérée comme un foncteur contravariant $\mathcal{O}_k^f$ de la catégorie des k-foncteurs formels dans celle des k-anneaux profinis et, si $\varphi : X \to Y$ est un morphisme de k-foncteurs formels, le diagramme

$$\begin{tikzcd} X \arrow[r, "\alpha_X"] \arrow[d, "\varphi"'] & \mathrm{Spf}_k\mathcal{O}^f(X) \arrow[d, "\mathrm{Spf}_k\mathcal{O}_k^f(\varphi)"] \\ Y \arrow[r, "\alpha_Y"] & \mathrm{Spf}_k\mathcal{O}^f(Y) \end{tikzcd}$$

est commutatif.

4.6. On dit qu'un k-foncteur formel X est un k-<u>schéma formel</u> (ou un schéma formel sur k) s'il existe un k-anneau profini A tel que $X \simeq \mathrm{Spf}_k A$. Comme $\mathrm{Spf}_k A = \varinjlim_{\mathfrak{a}\in\Omega_A} \mathrm{Spf}_k(A/\mathfrak{a})$, il revient au même de dire que X est limite inductive filtrante de k-foncteurs formels représentables.

On voit immédiatement qu'un k-foncteur formel X est un k-schéma formel si et seulement si la flèche canonique $\alpha_X : X \to \mathrm{Spf}_k \mathcal{O}^f(X)$ est un isomorphisme. On voit également que :

- le foncteur Spf_k induit une anti-équivalence entre la catégorie des k-anneaux profinis et celle des k-schémas formels (i.e. la sous-catégorie pleine de la catégorie des k-foncteurs formels dont les objets sont les k-schémas formels) ;
- si X est un k-foncteur formel et si Y est un k-schéma formel, tout morphisme $\varphi : X \to Y$ se factorise, de manière unique, à travers le morphisme canonique $\alpha_X : X \to \mathrm{Spf}_k \mathcal{O}^f(X)$.

4.7. On peut caractériser les k-schémas formels parmi les k-foncteurs formels de la manière suivante :

PROPOSITION 4.1. - <u>Un k-foncteur formel est un schéma formel si et seulement s'il est exact à gauche</u>.

Il est clair que la condition est nécessaire. Indiquons pourquoi elle est suffisante : soit X un k-foncteur formel exact à gauche. Si R est un k-anneau fini et si R' est un sous-k-anneau de R, R' s'identifie à $R' \times_R R'$ et l'application canonique $X(R') \to X(R)$ est injective et nous permet d'identifier $X(R')$ à un sous-ensemble de $X(R)$. Si R_1 et R_2 sont deux sous-k-anneaux d'un k-anneau fini R, $R_1 \cap R_2$ s'identifie à $R_1 \times_R R_2$ et on a donc $X(R_1 \cap R_2) = X(R_1) \cap X(R_2)$. A tout k-anneau fini R, et à tout $x \in X(R)$, on peut donc associer le plus petit sous-k-anneau R_x de R tel que $x \in X(R_x)$; c'est l'intersection des sous-k-anneaux R' de R tels que $x \in X(R')$.

Appelons couple minimal tout couple (R,x) formé d'un k-anneau fini R et d'un élément $x \in X(R)$ tel que $R_x = R$. Les couples minimaux forment une catégorie, une flèche $\xi : (R,x) \to (R',y)$ étant un morphisme de k-anneaux finis de R dans R' tel que $X(\xi)(x) = y$.

On voit que cette catégorie est "filtrante à gauche" : si (R,x) et (R',y) sont deux couples minimaux, il est clair que $((R\times R')_{(x,y)},(x,y))$ est un couple minimal qui s'envoie à la fois sur (R,x) et sur (R',y) . On voit que l'on peut parler du k-anneau profini $A = \varprojlim R$, pour (R,x) parcourant les couples minimaux.

On a un morphisme $f : X \to X' = \mathrm{Spf}_k A$ défini par :

- pour tout k-anneau fini R , $f_R : X(R) \to X'(R)$ est l'application qui à $x \in X(R)$ associe l'application composée

$$A \xrightarrow{\text{can.}} R_x \xrightarrow{\text{incl.}} R$$

et on vérifie facilement que f est un isomorphisme.

4.8. Soit X un k-schéma affine et soit $A = \mathcal{O}(X)$ son algèbre affine. Il est clair que le complété formel $\hat{X}$ de X est un k-schéma formel ; on voit que $\mathcal{O}^f(\hat{X})$ s'identifie à $\hat{A} = \varprojlim A/\mathfrak{a}$, pour $\mathfrak{a}$ parcourant les idéaux de A tels que le quotient $A/\mathfrak{a}$, muni de la topologie discrète, soit un k-anneau fini. Nous appelons $\hat{A}$ la <u>complétion profinie</u> de A .

De même, soit A un k-anneau linéairement topologisé et soit X le k-foncteur formel défini par $X(R) = \mathrm{Hom}_k^{\mathrm{cont}}(A,R)$, pour tout k-anneau fini R; il est clair que X est un k-schéma formel et on voit que son algèbre affine s'identifie à $\hat{A} = \varprojlim A/\mathfrak{a}$, pour $\mathfrak{a}$ parcourant les idéaux ouverts de A de codimension finie. Nous appelons encore $\hat{A}$ la <u>complétion profinie</u> de A .

Appelons k-<u>schéma fini</u> tout k-foncteur formel qui est représentable, autrement dit tout k-schéma formel dont l'algèbre affine est un k-anneau fini. Les k-schémas finis forment une sous-catégorie pleine de la catégorie des k-schémas formels. Dans le cas où k est un produit fini d'anneaux locaux nœthériens, tout k-anneau artinien, muni de la topologie discrète est un k-anneau fini (autrement dit on a $\hat{A} = A$, pour tout k-anneau fini A) et la catégorie des k-schémas finis s'identifie aussi à une sous-catégorie pleine de la catégorie des k-schémas affines.

4.9. La catégorie des k-foncteurs formels a des limites inductives. Une limite inductive de k-schémas formels est encore un k-schéma formel et son algèbre affine s'identifie à la limite projective des algèbres affines.

La catégorie des k-foncteurs formels a aussi des limites projectives. Une limite projective finie de k-schémas formels est encore un k-schéma formel. Par exemple :

- si X et Y sont deux k-schémas formels, l'algèbre affine de $X \times Y$ s'identifie à $\mathcal{O}^f(X) \hat{\otimes}_k \mathcal{O}^f(Y)$;
- plus généralement, si $\varphi : X \to Z$ et $\psi : Y \to Z$ sont des morphismes de de k-schémas formels, l'algèbre affine de $X \times_Z Y$ s'identifie à $\mathcal{O}^f(X) \hat{\otimes}_{\mathcal{O}^f(Z)} \mathcal{O}^f(Y)$.

4.10. Soit k' un k-anneau fini. Si R est un k'-anneau fini, le k-anneau $R_{[k]}$ déduit de R par restriction des scalaires est un k-anneau fini. Ceci permet de définir un foncteur changement de base $X \mapsto X_{k'}$, comme au n°1.8. Si X est un k-schéma formel, on voit que $X_{k'}$ est un k'-schéma formel dont l'algèbre affine s'identifie à $k' \otimes_k \mathcal{O}^f(X) = k' \hat{\otimes}_k \mathcal{O}^f(X)$.

Soit maintenant k' un anneau pseudo-compact et $\xi : k \to k'$ un homomorphisme continu. On voit que ξ munit k' d'une structure de k'-anneau linéairement topologisé et que, si A est un k-anneau profini, $k' \hat{\otimes}_k A$ est un k'-anneau profini. Si X est un k-schéma formel, on note $X_{k'}$, le k'-schéma formel $\mathrm{Spf}_{k'}(k' \hat{\otimes}_k \mathcal{O}^f(X))$; dans le cas où k' est un k-anneau fini, les deux définitions de $X_{k'}$ coïncident.

§ 5.- Groupes formels et dualité de Cartier.

5.1. Soit k un anneau commutatif pseudo-compact.

On appelle k-foncteur en groupes formels (sous-entendu commutatif) tout objet en groupes abéliens dans la catégorie des k-foncteurs formels. Il revient au même de dire qu'un k-foncteur en groupes formels est un foncteur covariant de la catégorie des k-anneaux finis dans celle des groupes abéliens. Tout k-foncteur en groupes formels G se prolonge, de manière unique, en un foncteur covariant de la catégorie des k-anneaux profinis dans celle des groupes abéliens, qui commute aux limites projectives filtrantes, en posant,

$G(R) = \varprojlim_{\mathfrak{a} \in \Omega_R} G(R/\mathfrak{a})$, pour tout k-anneau profini R .

On appelle k-schéma en groupes formels (sous-entendu commutatif) ou, plus simplement, k-groupe formel, ou groupe formel sur k , tout k-foncteur en groupes formels dont le k-foncteur formel sous-jacent est un k-schéma formel.

On appelle k-bigèbre formelle (sous-entendu co-commutative) la donnée d'un couple (B, Δ_B) où B est un k-anneau profini et où $\Delta_B : B \to B \hat{\otimes}_k B$ est un morphisme de k-anneaux profinis satisfaisant les quatre axiomes suivants:

(B_1^f) le diagramme

$$\begin{tikzcd} B \arrow[r, "\Delta_B"] \arrow[d, "\Delta_B"'] & B \hat{\otimes} B \arrow[d, "id_B \hat{\otimes} \Delta_B"] \\ B \hat{\otimes} B \arrow[r, "\Delta_B \hat{\otimes} id_B"] & B \hat{\otimes} B \hat{\otimes} B \end{tikzcd}$$

est commutatif ;

(B_2^f) il existe un morphisme de k-anneaux profinis $\epsilon_B : B \to k$ tel que le diagramme

$$\begin{tikzcd} & B \hat{\otimes} B \arrow[r, "id_B \hat{\otimes} \epsilon_B"] & B \hat{\otimes} k \arrow[d, "\wr"] \\ B \arrow[ur, "\Delta_B"] \arrow[rr, "id_B"] \arrow[dr, "\Delta_B"'] & & B \arrow[d, "\wr"] \\ & B \hat{\otimes} B \arrow[r, "\epsilon_B \hat{\otimes} id_B"'] & k \hat{\otimes} B \end{tikzcd}$$

est commutatif ;

(B_3^f) il existe un endomorphisme σ_B du k-anneau profini B tel que le diagramme

$$\begin{tikzcd} & B \hat{\otimes} B \arrow[rr, "id_B \hat{\otimes} \sigma_B"] & & B \hat{\otimes} B \arrow[dr, "\text{produit}"] & \\ B \arrow[ur, "\Delta_B"] \arrow[r, "\epsilon_B"] \arrow[dr, "\Delta_B"'] & & k \arrow[rr, "i_B"] & & B \\ & B \hat{\otimes} B \arrow[rr, "\sigma_B \hat{\otimes} id_B"'] & & B \hat{\otimes} B \arrow[ur, "\text{produit}"'] & \end{tikzcd}$$

est commutatif ;

(B_4^f) le diagramme

$$\begin{tikzcd} & B \hat{\otimes} B \arrow[dr, "t"] & \\ B \arrow[ur, "\Delta_B"] \arrow[rr, "\Delta_B"] & & B \hat{\otimes} B \end{tikzcd}$$

(où $t(f\hat{\otimes}g) = g\hat{\otimes}f$) est commutatif.

5.2. On adopte la même terminologie qu'au n°2.3 ; en particulier, si B est une k-bigèbre formelle, B s'écrit $B = k\oplus B^+$, avec B^+ l'idéal d'augmentation. Ici encore, si $f \in B$, on pose $\delta f = 1\hat{\otimes}f - \Delta_B f + f\hat{\otimes}1$; si $f \in B^+$, alors $\delta f \in B^+\hat{\otimes}B^+$.

De la même manière qu'au paragraphe 2, on voit que les k-foncteurs en groupes formels, les k-groupes formels et les k-bigèbres formelles forment trois catégories additives. La deuxième est une sous-catégorie pleine de la première et le foncteur Spf_k induit une anti-équivalence entre la troisième et la seconde, le foncteur $\mathcal{O}_k^f$ étant un quasi-inverse.

5.3. Nous disons qu'une k-bigèbre formelle est <u>topologiquement plate</u> si le k-module profini sous-jacent est topologiquement plat, i.e. projectif. Nous disons qu'un k-groupe formel est <u>topologiquement plat</u> si son algèbre affine l'est.

De même, si k' est un anneau commutatif quelconque, nous disons qu'une k'-bigèbre est <u>plate</u> si le k'-module sous-jacent est plat ; nous disons qu'un k'-groupe affine est <u>plat</u> si son algèbre affine l'est ; dans le cas où k' est artinien, il revient au même de dire que l'algèbre affine est un k'-module projectif.

5.4. Soit maintenant k un anneau commutatif artinien.

Soit B une k-bigèbre formelle topologiquement plate. Alors (cf. n°3.6) le k-module B' des applications linéaires continues de B dans k est projectif, donc plat. Par transposition, le coproduit $\Delta_B : B \to B\hat{\otimes}B$ définit une application $\Delta'_B : (B\hat{\otimes}B)' \simeq B'\otimes B' \to B'$ qui munit B' d'une structure de k-anneau. Soit $\pi_B : B\hat{\otimes}B \to B$ l'application définie par $\pi_B(f\hat{\otimes}g) = fg$; elle induit une application $\pi'_B : B \to (B\hat{\otimes}B)' \simeq B'\otimes B'$, i.e. un coproduit. On vérifie que l'on a ainsi muni B' d'une structure de k-bigèbre. Il est clair que la correspondance $B \mapsto B'$ définit en fait un foncteur contravariant de la catégorie des k-bigèbres formelles topologiquement plates dans celle des k-bigèbres plates.

Si G est un k-groupe formel topologiquement plat, et si B est son algèbre affine, nous notons $\mathbb{D}(G)$ et appelons dual de Cartier de G le k-groupe affine $Sp_k B'$. Il est clair que la correspondance $G \mapsto \mathbb{D}(G)$ définit un foncteur contravariant de la catégorie des k-groupes formels topologiquement plats dans celle des k-groupes affines plats.

Si C est une k-bigèbre plate, on munit de la même manière le k-module topologique C^* des applications linéaires de C dans k d'une structure de k-bigèbre formelle topologiquement plate. Si H est un k-groupe affine plat d'algèbre affine C, nous notons $\hat{\mathbb{D}}(H)$ et appelons dual de Cartier de H le k-groupe formel $Spf_k C^*$. Il est clair que l'on peut considérer $\hat{\mathbb{D}}$ comme un foncteur contravariant de la catégorie des k-groupes affines plats dans celle des k-groupes formels topologiquement plats.

On voit immédiatement que le foncteur $\mathbb{D}$ induit en fait une anti-équivalence entre la catégorie des k-groupes formels topologiquement plats et celle des k-groupes affines plats et que $\hat{\mathbb{D}}$ est un quasi-inverse.

Dans le cas particulier où k est un corps, on a ainsi obtenu une anti-équivalence entre la catégorie des k-groupes formels et celle des k-groupes affines.

5.5. Soit maintenant k un anneau commutatif nœthérien.

Tout k-module de type fini est alors de présentation finie. On en déduit (cf. [4], chap.II, §3) qu'un k-module de type fini est plat si et seulement s'il est projectif, ou encore si et seulement s'il est localement libre. En particulier, le dual d'un k-module plat de type fini est encore plat de type fini.

On appelle k-groupe fini tout k-groupe affine dont l'algèbre affine est un k-module de type fini.

On peut définir, exactement comme au n° précédent, une dualité de la catégorie des k-groupes finis et plats dans elle-même. On note encore $\mathbb{D}(G)$ et on appelle encore dual de Cartier de G le dual d'un k-groupe fini et plat ainsi construit. Il est clair que $\mathbb{D}(\mathbb{D}(G))$ s'identifie canoniquement à G.

Soit G un k-groupe fini et plat et soit B son algèbre affine. Soit B' la bigèbre duale. Pour tout k-anneau R l'ensemble sous-jacent à $\mathbb{D}(G)(R)$ est formé des homomorphismes du k-anneau B' dans R et c'est un sous-ensemble du k-module des applications k-linéaires de B' dans R. Comme ce dernier est canoniquement isomorphe à $B \otimes_k R$, $\mathbb{D}(G)(R)$ s'identifie à un sous-ensemble de $B \otimes_k R$. On vérifie facilement que, dans cette identification, $\mathbb{D}(G)(R)$ est formé des α vérifiant $\Delta\alpha = \alpha \otimes \alpha$ et $\varepsilon\alpha = 1$ (on a noté $\Delta : B \otimes_k R \to (B \otimes_k R) \otimes_R (B \otimes_k R)$ l'application qui prolonge le coproduit $\Delta : B \to B \otimes_k B$ et $\varepsilon : B \otimes_k R \to R$ l'application qui prolonge l'augmentation $\varepsilon : B \to k$) et que la loi de groupe est induite par la multiplication dans l'anneau. Il résulte alors du lemme de Yoneda que $\mathbb{D}(G)(R)$ n'est autre que le groupe $\mathrm{Mor}(G_R, \mu_R)$ des morphismes dans la catégorie des R-foncteurs en groupes (ou des R-groupes affines) de G_R dans μ_R (on désigne par μ_R le groupe multiplicatif sur R , i.e. on a $\mu_R(S) = S^{\times}$, groupe multiplicatif des éléments inversibles du R-anneau S ; c'est un R-groupe affine, dont l'algèbre affine s'identifie à $R[X, X^{-1}]$).

Si maintenant k est un anneau commutatif nœthérien pseudo-compact, il est clair que toute k-algèbre qui est un k-module de type fini peut être considérée comme une k-algèbre profinie. Ceci permet de considérer la catégorie des k-groupes finis et plats comme une sous-catégorie pleine aussi bien de la catégorie des k-groupes affines que de celle des k-groupes formels. Il est clair que les notions de dualité définies au n°5.4 et dans ce n° coïncident.

§ 6.- Noyaux et conoyaux.

6.1. Soit k un anneau commutatif.

On sait (n°2.5) que la catégorie des k-foncteurs en groupes (commutatifs) est abélienne. Soit $\varphi : G \to H$ un morphisme de k-groupes affines et soit N le noyau de φ dans la catégorie des k-foncteurs en groupes (pour tout k-anneau R , $N(R)$ est donc le noyau de $\varphi_R : G(R) \to H(R)$). Soit B (resp. C) l'algèbre affine de G (resp. H) et soit $\varphi^* : C \to B$ le morphisme correspondant à φ . Soit C^+ l'idéal d'augmentation de C . Il est clair que $N(R)$ s'identifie au sous-groupe de $G(R)$ formé des $u : B \to R$ tels que $\varphi(C^+) \subset \ker u$. En tant qu'ensemble, $N(R)$ s'identifie donc à l'ensemble des homomorphismes du k-anneau $B/B\varphi^*(C^+)$ dans R et N est un k-groupe affine. C'est donc aussi le noyau de φ dans la catégorie des k-groupes affines.

On voit, de la même manière, que, si k est un anneau commutatif pseudo-compact, la catégorie des k-groupes formels a des noyaux. Si $\varphi : G \to H$ est un morphisme de k-groupes formels, le noyau N de φ, dans la catégorie des k-groupes formels, est le noyau de φ dans la catégorie des k-foncteurs en groupes formels. Si B (resp. C) est l'algèbre affine de G (resp. H) et si $\varphi^* : C \to B$ est le morphisme correspondant à φ, l'algèbre affine de N s'identifie au quotient de B par l'adhérence de l'idéal de B engendré par $\varphi^*(C^+)$.

<u>Remarque</u> : en revanche, si $\varphi : G \to H$ est un morphisme de k-groupes affines (resp. formels), il n'est pas vrai en général que le conoyau de φ dans la catégorie des k-foncteurs en groupes (resp. formels) est un k-groupe affine (resp. formel).

Dans toute la suite de ce paragraphe, <u>on suppose que</u> k <u>est un corps</u>.

6.2. Si B et B' sont deux k-espaces vectoriels profinis (i.e. des k-espaces vectoriels topologiques, topologiquement libres) et si C (resp. C') est un sous-espace vectoriel fermé de B (resp. B'), on voit que $C \hat{\otimes}_k C'$ s'identifie canoniquement à un sous-espace vectoriel fermé de $B \hat{\otimes}_k B'$.

Si B est une k-bigèbre formelle, nous appelons <u>sous-k-bigèbre formelle</u> de B tout sous-k-anneau fermé C de B tel que $\sigma_B(C) \subset C$ et $\Delta_B(C) \subset C \hat{\otimes} C$. Il est clair que Δ_B induit alors une structure de k-bigèbre formelle sur C.

Soit B une k-bigèbre formelle et soit A une partie fermée de B contenant k. L'ensemble des sous-k-bigèbres formelles de B contenues dans A est non vide (il contient k) et il est clair que la réunion $b_B(A)$ des sous k-bigèbres formelles de B contenues dans A est encore une sous-k-bigèbre formelle.

Soit alors $\varphi : G \to H$ un morphisme de k-groupes formels. Soit B (resp. C) l'algèbre affine de G (resp. H) et soit $\varphi^* : C \to B$ le morphisme correspondant à φ. Soit $\mathfrak{a}$ l'idéal fermé de C, noyau de φ^*. Si $\psi : H \to H'$ est un morphisme de k-groupes formels correspondant à un morphisme $\psi^* : C' \to C$ de k-bigèbres formelles, on voit que $\psi \circ \varphi = 0$ si et seulement si $\psi^*(C')$ est contenu dans $k \oplus \mathfrak{a}$. Il est clair que $\psi^*(C')$ est une sous-k-bigèbre formelle de C. On voit donc que $\psi \circ \varphi = 0$ si et seulement si $\psi^*(C') \subset b_C(k \oplus \mathfrak{a})$. On en déduit que φ admet un conoyau J et que l'algèbre affine de J s'identifie à $b_C(k \oplus \mathfrak{a})$.

On définit de la même manière la notion de sous-k-bigèbre d'une k-bigèbre. Si B est une k-bigèbre et si A est une partie de B contenant k, on peut encore parler de la plus grande sous-k-bigèbre $b_B(A)$ de B contenue dans A. On montre de la même façon que la catégorie des k-groupes affines admet des conoyaux.

6.3. PROPOSITION 6.1.- <u>Soit</u> $\varphi : G \to H$ <u>un morphisme de</u> k-<u>groupes affines</u> (<u>resp</u>. <u>formels</u>) <u>et soit</u> C <u>l'algèbre affine de</u> H. <u>L'algèbre affine du conoyau de</u> φ, <u>dans la catégorie des</u> k-<u>groupes affines</u> (<u>resp</u>. <u>formels</u>), <u>s'identifie au sous-anneau de</u> C <u>formé des</u> f <u>tels que</u>, <u>pour tout</u> k-<u>anneau</u> (<u>resp</u>. <u>tout</u> k-<u>anneau fini</u>) R, <u>tout</u> $u \in H(R)$ <u>et tout</u> $v \in G(R)$, <u>on ait</u> $f_R(u+\varphi_R(v)) = f_R(u)$.

<u>Démonstration</u> : la démonstration est la même dans les deux cas. Supposons, par exemple, que G et H sont des k-groupes formels.

Soit J le conoyau de φ et soit B (resp. E) l'algèbre affine de G (resp. J). Notons $\eta : C \to B$ le morphisme de k-bigèbres formelles correspondant à φ. Le morphisme $\mathbb{D}(\varphi) : \mathbb{D}(H) \to \mathbb{D}(G)$ des k-groupes affines duaux correspond à un morphisme $\eta' : B' \to C'$ des k-bigèbres duales. Il est clair que la bigèbre duale E' de E s'identifie à l'algèbre affine du noyau de $\mathbb{D}(\varphi)$. Soit F la sous-k-bigèbre $\eta'(B')$ de C'. Il résulte du n° 6.1 que E' s'identifie au quotient de C' par l'idéal $\mathfrak{b}$ de C' engendré par F^+ ; par conséquent, E s'identifie à l'orthogonal de $\mathfrak{b}$ dans C. Autrement dit, $E = \{f \in C \mid (xy^+)(f) = 0 \text{ pour } x \in C', y^+ \in F^+\}$. Par définition du produit dans C', on a encore, $E = \{f \in C \mid (x \otimes y^+)(\Delta f) = 0 \text{ pour } x \in C', y^+ \in F^+\}$, en notant Δ le coproduit dans C.

L'élément-unité de C' n'est autre que l'augmentation ε_C de C et on voit que tout $y \in F$ s'écrit sous la forme $y = y(1)\varepsilon_C + y^+$, avec $y^+ \in F^+$. On a donc, pour $x \in C'$, $y \in F$,

$$\begin{aligned}(x \otimes y)(\Delta f) &= (x \otimes y(1)\varepsilon_C)(\Delta f) + (x \otimes y^+)(\Delta f) = x(f)y(1) + (x \otimes y^+)(\Delta f) \\ &= (x \otimes y)(f \hat{\otimes} 1) + (x \otimes y^+)(\Delta f) .\end{aligned}$$

On voit donc que $E = \{f \in C \mid (x \otimes y)(\Delta f - f \hat{\otimes} 1) = 0 \text{ si } x \in C', y \in F\}$, i.e.

que E est formé des $f \in C$ tels que $\Delta f - f \hat{\otimes} 1$ appartient à l'orthogonal $(C' \otimes F)^{\perp}$ de $C' \otimes F$ dans $C \hat{\otimes} C$; si on désigne par $\mathfrak{a}$ le noyau de η, on voit que $(C' \otimes F)^{\perp}$ n'est autre que $C \hat{\otimes} \mathfrak{a}$. On en déduit que $E = \{f \in C \mid \Delta f - f \hat{\otimes} 1 \in C \hat{\otimes} \mathfrak{a}\}$.

Il est immédiat que la condition $\Delta f - f \hat{\otimes} 1 \in C \hat{\otimes} \mathfrak{a}$ équivaut à $f_R(u + \varphi_R(v)) = f_R(u)$, pour tout k-anneau fini R, tout $u \in H(R)$ et tout $v \in G(R)$.

<u>Remarque</u> : on voit que la proposition 6.1 revient à dire que l'algèbre affine du conoyau de φ, dans la catégorie des k-groupes affines (resp. formels), s'identifie à l'algèbre affine du conoyau de φ dans la catégorie des k-foncteurs en groupes (resp. formels).

6.4. PROPOSITION 6.2.- <u>Soit</u> B <u>une</u> k-<u>bigèbre</u> (<u>resp</u>. k-<u>bigèbre formelle</u>) <u>et soit</u> C <u>une sous</u>-k-<u>bigèbre</u> (<u>resp</u>. <u>formelle</u>) <u>de</u> B. <u>Alors</u>

i) <u>l'algèbre</u> $B \otimes_C B$ (<u>resp</u>. $B \hat{\otimes}_C B$) <u>est un</u> B-<u>module libre</u> (<u>resp</u>. <u>topologiquement libre</u>) <u>pour l'action de</u> B <u>définie par multiplication à gauche</u> ;

ii) <u>soit</u> G (<u>resp</u>. H) <u>le</u> k-<u>groupe affine</u> (<u>resp</u>. <u>formel</u>) <u>correspondant à</u> B (<u>resp</u>. C) <u>et soit</u> $\varphi : G \to H$ <u>le morphisme correspondant à l'inclusion de</u> C <u>dans</u> B ; <u>l'ensemble</u> C' <u>des</u> $f \in B$ <u>tels que</u> $f \otimes_C 1 = 1 \otimes_C f$ <u>dans</u> $B \otimes_C B$ (<u>resp</u>. $f \hat{\otimes}_C 1 = 1 \hat{\otimes}_C f$ <u>dans</u> $B \hat{\otimes}_C B$) <u>est une sous</u>-k-<u>bigèbre</u> (<u>resp</u>. <u>formelle</u>) <u>de</u> B <u>contenant</u> C <u>et s'identifie à l'algèbre affine de la coimage de</u> φ.

<u>Démonstration</u> : la démonstration est la même dans les deux cas. Supposons par exemple que B est une k-bigèbre. Si on note $\mathfrak{a}$ l'idéal de B engendré par C^+, il résulte du n° 6.1 que l'algèbre affine du noyau N de φ s'identifie à $B/\mathfrak{a}$.

Considérons le produit fibré $G \times_H G$; on voit que, pour tout k-anneau R, $(G \times_H G)(R)$ est formé des $(x,y) \in G(R) \times G(R)$ tels que $\varphi_R(x) = \varphi_R(y)$. D'autre part, $(G \times N)(R)$ est formé des $(u,v) \in G(R) \times G(R)$ tels que $\varphi_R(v) = 0$. On voit donc que l'on définit un isomorphisme ψ de $G \times_H G$ sur $G \times N$ en posant, pour tout k-anneau R et tout $(x,y) \in (G \times_H G)(R)$, $\psi_R(x,y) = (x, y-x)$.

L'isomorphisme ψ induit un isomorphisme η de $\mathcal{O}(G \times N) \simeq \mathcal{O}(G) \otimes_k \mathcal{O}(N) = B \otimes_k B/\mathfrak{a}$ sur $\mathcal{O}(G \times_H G) \simeq \mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G) = B \otimes_C B$: on voit que η est l'application qui à $f \otimes_k g \in B \otimes_k B/\mathfrak{a}$ associe la fonction h définie sur $G \times_H G$ par $h_R(x,y) = f_R(x)\, g_R(y-x)$, pour tout k-anneau R et tout $(x,y) \in (G \times_H G)(R)$.

On voit que η est aussi une application B-linéaire, pour la structure de B-module définie par la multiplication à gauche sur $B \otimes_k B/\mathfrak{a}$ et sur $B \otimes_C B$. La première assertion de la proposition résulte alors de ce que $B \otimes_k B/\mathfrak{a}$ est un B-module libre.

On voit que C' est formé des $f \in B$ tels que $f_R(x) = f_R(y)$, pour tout k-anneau fini R et tout $(x,y) \in (G \times_H G)(R)$; comme tout élément $(x,y) \in (G \times_H G)(R)$ s'écrit sous la forme $(u, u+v)$, avec $(u,v) \in (G \times N)(R)$, et réciproquement, on voit que C' est aussi l'ensemble des $f \in B$ tels que, pour tout k-anneau fini R et pour tout $(u,v) \in (G \times N)(R)$, $f_R(u) = f_R(u+v)$. D'après la proposition 6.1, c'est donc l'algèbre affine du conoyau de $N \to G$, autrement dit de la coimage de φ .

6.5. PROPOSITION 6.3.- <u>Soit</u> B <u>une</u> k-<u>bigèbre formelle et soit</u> C <u>une sous</u>-k-<u>bigèbre formelle</u>. <u>Alors</u> B <u>est un</u> C-<u>module topologiquement plat et</u> C <u>est facteur direct de</u> B <u>en tant que</u> C-<u>module</u>.

Commençons par établir un lemme :

LEMME 6.4.- <u>Soit</u> C <u>un</u> k-<u>anneau pseudo-compact et soient</u> B <u>un</u> C-<u>anneau profini et</u> M <u>un</u> C-<u>module profini</u>. <u>Si</u> $B \hat{\otimes}_C M$ <u>est un</u> B-<u>module topologiquement libre</u>, M <u>est un</u> C-<u>module topologiquement plat</u>.

<u>Démonstration du lemme</u> : soit $C = \prod C_{\mathfrak{m}}$ la décomposition de C en le produit de ses composantes locales et soient $B = \prod B_{\mathfrak{m}}$ et $M = \prod M_{\mathfrak{m}}$ les décompositions correspondantes des C-modules B et M . Il est clair que $B \hat{\otimes}_C M$ s'identifie au produit des $B_{\mathfrak{m}} \hat{\otimes}_{C_{\mathfrak{m}}} M_{\mathfrak{m}}$ et que chacun d'entre eux est un $B_{\mathfrak{m}}$-module topologiquement libre. On est donc ramené à montrer que, pour tout $\mathfrak{m}$, $M_{\mathfrak{m}}$ est un $C_{\mathfrak{m}}$-module topologiquement libre, autrement dit on peut supposer que C est un anneau local.

Soit alors $\mathfrak{m}$ l'idéal maximal de C et soient $\tilde{C} = C/\mathfrak{m}$ et $\tilde{B} = B/\overline{\mathfrak{m}B}$. Au diagramme commutatif d'anneaux pseudo-compacts

$$\begin{array}{ccc} C & \longrightarrow & B \\ \downarrow & & \downarrow \\ \tilde{C} & \longrightarrow & \tilde{B} \end{array}$$

correspond un diagramme commutatif

$$\begin{array}{ccc} M & \longrightarrow & B\hat{\otimes}_C M \\ \downarrow & & \downarrow \\ \tilde{C}\hat{\otimes}_C M & \longrightarrow & \tilde{B}\hat{\otimes}_C M \end{array} .$$

Soit $(\tilde{u}_i)_{i\in I}$ une base topologique du $\tilde{C}$-espace vectoriel profini $\tilde{C}\hat{\otimes}_C M$ et soit $(u_i)_{i\in I}$ les images des $\tilde{u}_i$ par une section $\tilde{C}$-linéaire continue. Comme $\mathfrak{m}$ est topologiquement nilpotent, on voit que M est l'adhérence du sous-module engendré par les u_i. Comme $\tilde{B}\hat{\otimes}_C M$ s'identifie à $\tilde{B}\hat{\otimes}_{\tilde{C}}(\tilde{C}\hat{\otimes}_C M)$, on voit que les $1\hat{\otimes}_C \tilde{u}_i$ forment une base topologique du $\tilde{B}$-module topologiquement libre $\tilde{B}\hat{\otimes}_C M$. Comme $B\hat{\otimes}_C M$ est un B-module topologiquement libre, on en déduit que les $1\hat{\otimes}_C u_i$ forment une base topologique de $B\hat{\otimes}_C M$ sur B. Par conséquent, les u_i sont "topologiquement linéairement indépendants" sur C et M est un C-module topologiquement libre admettant $(u_i)_{i\in I}$ comme base topologique.

Démontrons maintenant la proposition 6.3 : il suffit d'appliquer le lemme précédent à $M = B$ car on sait (prop.6.2) que $B\hat{\otimes}_C B$ est un B-module topologiquement libre. Le fait que C est facteur direct de B provient de ce que chaque $C_{\mathfrak{m}}$ est facteur direct de $B_{\mathfrak{m}} = M_{\mathfrak{m}}$, comme on le voit en remarquant que dans la démonstration du lemme on peut choisir la base topologique $(u_i)_{i\in I}$ pour qu'elle contienne 1 .

6.6. PROPOSITION 6.5.- La catégorie des k-groupes formels et celle des k-groupes affines sont abéliennes.

Remarquons que, grâce à la dualité entre ces deux catégories, il suffit de la démontrer pour l'une d'entre elles. Nous admettrons ce résultat classique (cf. [13] , exposé VII_B, § 2) dont nous ne connaissons pas de démonstration suffisamment élémentaire pour rentrer dans le cadre de ce chapitre.

Remarques :

1.- Comme on sait que la catégorie des k-groupes affines (resp. formels) admet des noyaux et conoyaux, il suffit, pour montrer que cette catégorie est abélienne de vérifier que pour tout morphisme φ, le morphisme canonique de la coimage de φ dans l'image de φ est un isomorphisme. On voit très facilement que cela revient à démontrer les deux résultats suivants : soit $\varphi : G \to H$ un morphisme de k-groupes affines (resp. formels) correspondant à un morphisme $\varphi^* : C \to B$ de k-bigèbres (resp. formelles) :

(P_1) si φ^* est injective, la coimage de φ est H ;

(P_2) si φ^* est surjective, l'image de φ est G .

Il résulte en outre de la dualité entre groupes affines et groupes formels que la propriété (P_1) (resp. (P_2)) pour les groupes affines est équivalente à la propriété (P_2) (resp. (P_1)) pour les groupes formels.

2.- Montrons la propriété (P_1) pour les groupes formels : si on identifie C à une sous-k-bigèbre formelle de B, on sait (prop. 6.2) que l'algèbre affine de la coimage de φ est l'ensemble C' des $f \in B$ tels que $f \hat{\otimes}_C 1 = 1 \hat{\otimes}_C f$ dans $B \hat{\otimes}_C B$. Comme C est facteur direct de B en tant que C-module (prop. 6.3), on voit que $C' = C$, donc que H s'identifie bien à la coimage de φ .

3.- En particulier, on a une démonstration complète du fait que la catégorie des k-groupes finis est abélienne : la propriété (P_1) est vérifiée, car il suffit de considérer G et H comme des groupes formels ; la propriété (P_2) est vérifiée car (P_1) est vérifiée pour $\mathbb{D}(H) \to \mathbb{D}(G)$.

4.- Nous avons préféré pouvoir utiliser librement dans la suite la proposition 6.5, afin de ne pas alourdir les démonstrations. Le lecteur consciencieux pourra remarquer que, moyennant quelques précautions supplémentaires, nous aurions pu ne pas utiliser ce résultat (la prop. 6.3, en revanche, sera utilisée de façon essentielle). Pour les corps parfaits de caractéristique non nulle, la proposition 6.5 serait alors apparue comme un corollaire de la classification des groupes formels par leurs modules de Dieudonné (chap.III).

§ 7.- Groupes étales et connexes.

Dans ce paragraphe, k est un corps parfait, on note $\bar{k}$ une clôture algébrique de k et $\mathfrak{G}$ le groupe de Galois de $\bar{k}/k$.

7.1. On appelle $\mathfrak{G}$-<u>module discret</u> tout groupe abélien Γ sur lequel $\mathfrak{G}$ opère linéairement et continûment (le groupe Γ étant muni de la topologie discrète). Les $\mathfrak{G}$-modules discrets forment, de manière évidente, une catégorie abélienne.

Un k-groupe formel est dit étale si son algèbre affine est un k-anneau pro-étale, i.e. un produit d'extensions finies de k .

Si G est un k-groupe formel quelconque, on note $G(\bar{k})$ la limite inductive des $G(k')$, pour k' parcourant les extensions finies de k contenues dans $\bar{k}$. Il est clair que l'on a ainsi défini un foncteur covariant additif de la catégorie des k-groupes formels dans celle des $\mathfrak{G}$-modules discrets.

Si Γ est un $\mathfrak{G}$-module discret, le k-anneau B des fonctions sur Γ , à valeurs dans $\bar{k}$, qui commutent à l'action de Galois, muni de la topologie de la convergence simple, est un k-anneau profini pro-étale et a une structure naturelle de k-bigèbre formelle (le coproduit est défini par $(\Delta f)(\gamma,\gamma') = f(\gamma+\gamma')$). C'est l'algèbre affine d'un k-groupe formel étale $G(\Gamma)$. Il est clair que l'on a ainsi défini un foncteur covariant additif de la catégorie des $\mathfrak{G}$-modules discrets dans celle des k-groupes formels étales.

On vérifie immédiatement que le foncteur $G \mapsto G(\bar{k})$, restreint à la catégorie des k-groupes formels étales, induit une équivalence entre cette catégorie et celle des $\mathfrak{G}$-modules discrets et que le foncteur $\Gamma \mapsto G(\Gamma)$ est un quasi-inverse.

7.2. Un k-groupe formel G est dit <u>connexe</u> si son algèbre affine est un anneau local. On voit qu'il revient au même de dire que $G(k') = 0$, pour toute extension finie k' de k , ou encore que $G(\bar{k}) = 0$.

Soit G un k-groupe formel et soit B son algèbre affine. Pour tout k-anneau fini R , notons r_R son radical. Soit $G^{et}(R) = G(R/r_R)$ et soit $G^c(R)$ le noyau de $G(R) \to G^{et}(R)$.

On voit qu'un élément $u : B \to R$ de $G(R)$ est dans $G^c(R)$ si et seulement si $u(B^+) \subset r_R$ (où B^+ est l'idéal d'augmentation). On en déduit que G^c est un k-groupe formel dont l'algèbre affine B^c s'identifie à la composante locale de B correspondant à l'idéal maximal B^+ ; c'est donc un k-groupe formel connexe et nous l'appelons la <u>composante connexe</u> ou la <u>composante neutre</u> de G (l'expression correcte serait "la composante connexe de l'élément neutre").

Comme k est parfait, on voit que tout k-anneau fini R peut s'écrire sous la forme $R = R^{et} \oplus r_R$, où R^{et} est la plus grande sous-algèbre étale de R (et est canoniquement isomorphe à R/r_R) . On voit donc que $G^{et}(R)$ s'identifie à $G(R^{et})$ et que c'est aussi le groupe des homomorphismes continus du k-anneau profini pro-étale $B^{et} = B/r_B$ (où r_B désigne le radical de B) dans R . On en déduit que G^{et} est un k-groupe formel étale. Comme $G^{et}(\bar{k}) = G(\bar{k})$, on voit que, si l'on pose $\Gamma = G(\bar{k})$, on a, avec les notations du n°7.1, $G^{et} = G(\Gamma)$.

On voit enfin que la suite $0 \to G^c(R) \to G(R) \to G^{et}(R)$ est scindée et que G s'identifie canoniquement au produit direct de G^c par G^{et} (et aussi que B s'identifie canoniquement à $B^{et} \hat{\otimes}_k B^c$). Nous appelons G^{et} <u>la composante étale de</u> G .

Finalement, l'étude des groupes formels sur un corps k <u>parfait</u> se décompose en deux parties : celle des groupes formels étales (ou, ce qui revient au même, des $\mathfrak{G}$-modules discrets) et celle des groupes formels connexes.

7.3. Soit A un anneau local pseudo-compact dont le corps résiduel est k (toujours supposé parfait).

On dit qu'un A-groupe formel topologiquement plat G est <u>connexe</u> (resp. <u>étale</u>) si son algèbre affine est un anneau local (resp. un produit de A-algèbres étales).

On voit immédiatement que le foncteur $G \mapsto G_k$ induit une équivalence entre la catégorie des A-groupes formels topologiquement plats étales et celle des k-groupes formels étales (en fait, G_k étant donné, il existe un A-groupe formel G topologiquement plat, unique à isomorphisme unique près, qui relève G_k , et G est étale).

Soit G un A-groupe formel topologiquement plat et soit B son algèbre affine. Pour tout A-anneau fini R , notons r_R son radical. Posons $G^{et}(R) = G(R/r_R)$ et soit $G^c(R)$ le noyau de $G(R) \to G^{et}(R)$.

On voit que G^c est encore un A-groupe formel topologiquement plat dont l'algèbre affine B^c s'identifie à la composante locale de B correspondant à l'unique idéal maximal de B contenant l'idéal d'augmentation. En particulier G^c est connexe et nous l'appelons la <u>composante connexe</u> ou <u>neutre</u> de G .

Soit $\mathfrak{m}$ l'idéal maximal de A . Pour tout A-anneau fini R , soit $\tilde{R}$ le k-anneau fini $R/\mathfrak{m}R$. Il est clair que R/r_R s'identifie à $\tilde{R}/r_{\tilde{R}}$; on a donc $G^{et}(R) = G(R/r_R) = G_k(\tilde{R}/r_{\tilde{R}}) = (G_k)^{et}(\tilde{R})$. On en déduit que G^{et} s'identifie au A-groupe formel topologiquement plat relevant $(G_k)^{et}$. Nous l'appelons le <u>quotient étale</u> de G .

On déduit immédiatement de l'exactitude la suite

$$0 \longrightarrow G_k^c \longrightarrow G_k \longrightarrow G_k^{et} \longrightarrow 0$$

celle de la suite

$$0 \longrightarrow G^c \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

(ceci signifiant que G^c s'identifie au noyau de $G \to G^{et}$ et que l'algèbre affine de G est un module fidèlement topologiquement plat sur l'algèbre affine de G^{et}).

7.4. Si τ est un automorphisme du corps k et si G est un k-groupe affine (resp. formel) d'algèbre affine B , nous notons G^τ le k-groupe affine (resp. formel) déduit de G par l'extension des scalaires $\tau : k \to k$ et $B^{(\tau)}$ son algèbre affine. On voit que l'on peut (et c'est ce que nous ferons toujours dans la suite) identifier l'anneau (resp. topologique) sous-jacent à $B^{(\tau)}$ à B et que le coproduit est le même ; seule la multiplication par les scalaires change : le produit de $\lambda \in k$ par $b \in B^{(\tau)}$ (identifié à B) est $\tau^{-1}(\lambda)b$ (produit calculé dans B) .

Supposons maintenant que k est de caractéristique $p \neq 0$ et soit σ le Frobenius absolu sur k (on a donc $\sigma(\lambda) = \lambda^p$, pour tout $\lambda \in k$).

Pour tout k-groupe affine (resp. formel) G d'algèbre affine B , nous notons F_B l'application de B dans B définie par $F_B(b) = b^p$. Il est clair que F_B peut être considéré comme un morphisme de la k-bigèbre (resp. formelle) $B^{(\sigma)}$ dans B et définit donc un morphisme $F_G : G \to G^\sigma$, appelé le <u>Frobenius</u>.

Plus généralement, pour tout entier $n \geq 0$, on voit que F_B^n peut être considéré comme un morphisme de la k-bigèbre (resp. formelle) $B^{(\sigma^n)}$ dans B et définit donc un morphisme de G dans G^{σ^n} ; par abus d'écriture, nous le notons F^n_G : si, pour tout $i \in \mathbb{N}$, on pose $G_i = G^{\sigma^i}$ et $F_i = F_{G_i}$, on voit que $F^n_G = F_{n-1} \circ F_{n-2} \circ \ldots \circ F_0$.

Pour tout k-anneau fini R, on voit que le radical de R est formé des x tels que $x^{p^n} = 0$, pour n suffisamment grand. Les assertions suivantes sont évidentes :

- si G est un k-groupe formel, $G^c = \varinjlim \operatorname{Ker} F^n_G$; en particulier G est connexe si et seulement si $G = \varinjlim \operatorname{Ker} F^n_G$;
- si G est un k-groupe formel, G est étale si et seulement si F_G est un monomorphisme ; s'il en est ainsi, c'est un isomorphisme.

7.5. Supposons toujours k de caractéristique $p \neq 0$. Comme le foncteur "dual de Cartier" commute au changement de base, on voit que, si G est un k-groupe affine (resp. formel), le k-groupe formel (resp. affine) $\hat{\mathbb{D}}(G)^{\sigma}$ (resp. $\mathbb{D}(G)^{\sigma}$) s'identifie à $\hat{\mathbb{D}}(G^{\sigma})$ (resp. $\mathbb{D}(G^{\sigma})$). Le morphisme $F_{\hat{\mathbb{D}}(G)} : \hat{\mathbb{D}}(G) \to \hat{\mathbb{D}}(G)^{\sigma}$ (resp. $F_{\mathbb{D}(G)} : \mathbb{D}(G) \to \mathbb{D}(G)^{\sigma}$) induit, par dualité, un morphisme $V_G : G^{\sigma} \to G$, appelé <u>Verschiebung</u> ou <u>décalage</u>. Si B est l'algèbre affine de G, nous notons V_B l'application de B dans $B^{(\sigma)}$ (identifiée à B) correspondante. On définit de la même manière, et avec les mêmes abus de notations que pour le Frobenius, les applications $V^n_B : B \to B$ et $V^n_G : G^{\sigma^n} \to G$.

Donnons maintenant une description "explicite" de V_B. Soit G un k-groupe formel et soit B son algèbre affine. Pour tout entier $m \geq 1$, notons $\Delta_m : B \to \hat{\otimes}^m B$ le m-ième itéré du coproduit (on a donc $\Delta_1 = id_B$, $\Delta_2 = \Delta$, le coproduit, $\Delta_m = (\Delta \hat{\otimes} id_{\hat{\otimes}^{m-2} B}) \circ \Delta_{m-1}$ si $m \geq 2$).

Notons $TS^p B$ le sous-k-espace vectoriel fermé des tenseurs symétriques de $\hat{\otimes}^p B$. Soit s l'application k-linéaire continue de $\hat{\otimes}^p B$ dans $TS^p B$ qui, à $b_1 \hat{\otimes} b_2 \hat{\otimes} \ldots \hat{\otimes} b_p$ associe $\sum_{g \in \mathfrak{S}_p} b_{g(1)} \hat{\otimes} b_{g(2)} \hat{\otimes} \ldots \hat{\otimes} b_{g(p)}$ et soit $TS^p_0 B$ l'image de s . On voit facilement que tout élément de $TS^p B$ s'écrit d'une manière et d'une seule sous la forme $w = (b(w))^{\hat{\otimes} p} + w_0$, avec $b(w) \in B$ et $w_0 \in TS^p_0 B$.

Pour tout $c \in B$, $\Delta_p(c) \in TS^p B$. Nous allons montrer que $V_B(c) = b(\Delta_p(c))$.

Soit B' l'algèbre affine de $\mathbb{D}(G)$. Notons $\langle\ ,\ \rangle$ l'application k-bilinéaire canonique de $B \times B'$ dans k et $\langle\ ,\ \rangle_\sigma$ l'application k-bilinéaire canonique de $B^{(\sigma)} \times (B')^{(\sigma)}$ dans k . On voit tout de suite que si l'on identifie l'anneau $B^{(\sigma)}$ à B et l'anneau $(B')^{(\sigma)}$ à B' , on a $\langle b,x\rangle_\sigma = (\langle b,x\rangle)^p$, pour $b \in B$, $x \in B'$.

Si $c \in B$, et si l'on pose $b = b(\Delta_p(c))$, on a, pour tout $x \in (B')^{(\sigma)}$, $\langle V_B c,x\rangle_\sigma = \langle c,F_B x\rangle = \langle c,x^p\rangle = \langle \Delta_p c,x^{\otimes p}\rangle = \langle (b(\Delta_p c))^{\hat{\otimes} p},x^{\otimes p}\rangle + \langle (\Delta_p c)_o,x^{\otimes p}\rangle$ $= (b^{\hat{\otimes} p},x^{\otimes p}\rangle = (\langle b,x\rangle)^p = \langle b,x\rangle_\sigma$, d'où $V_B c = b$.

On a, bien sûr, la même description de V_B dans le cas où G est un k-groupe affine.

Il résulte immédiatement de ce qui précède que, pour toute k-bigèbre (resp. toute k-bigèbre formelle) B , on a $V_B \circ F_B = F_B \circ V_B = p \cdot id_B$, ou encore que, pour tout k-groupe formel (resp. affine) G , on a $V_G \circ F_G = p \cdot id_G$ et $F_G \circ V_G = p \cdot id_{G^\sigma}$.

7.6. Supposons toujours k de caractéristique $p \neq 0$. Nous disons qu'un k-groupe formel G est <u>unipotent</u> si $G = \varinjlim \operatorname{Ker} V^n_{G^{\sigma^n}}$.

Pour tout k-groupe formel G , nous appelons <u>composante unipotente de G</u> le k-groupe formel $\varinjlim \operatorname{Ker} V^n_{G^{\sigma^n}}$. Il est clair que c'est un k-groupe formel unipotent, invariant par tout automorphisme de G .

7.7. Un k-groupe affine G est dit <u>unipotent</u> (resp. <u>de type multiplicatif</u>) si son dual de Cartier est un k-groupe formel connexe (resp. étale). Tout k-groupe affine s'écrit donc, d'une manière et d'une seule, comme le produit direct d'un groupe unipotent et d'un groupe de type multiplicatif.

Dans le cas où la caractéristique de k est non nulle et où G est un k-groupe fini, on voit que G est unipotent, en tant que k-groupe affine, si et seulement s'il est unipotent en tant que k-groupe formel (avec la définition du n° 7.6).

On voit enfin que la catégorie des k-groupes finis se décompose en quatre sous-catégories :

- la catégorie des k-groupes finis étales de type multiplicatif,
- celle des k-groupes finis étales unipotents,
- celle des k-groupes finis connexes de type multiplicatif,
- celle des k-groupes finis connexes unipotents.

On laisse au lecteur le soin de décrire, lorsque la caractéristique de k est non nulle, chacune de ces sous-catégories en terme de l'action du Frobenius et du décalage.

Si G est un k-groupe fini, nous appelons <u>ordre de</u> G (on dit aussi <u>rang de</u> G) la dimension de son algèbre affine comme espace vectoriel sur le corps k.

Si G est un k-groupe fini étale, on voit que l'ordre de G est égal à celui du groupe fini $G(\bar{k})$.

Montrons que, si

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

est une suite exacte de k-groupes finis, l'ordre de G est le produit de l'ordre de G' par celui de G'' :

- en utilisant la décomposition d'un k-groupe fini en le produit direct d'un k-groupe fini connexe par un k-groupe fini étale, on voit que l'on peut supposer soit que les trois groupes considérés sont connexes, soit qu'ils sont étales ;
- le résultat est évident si les k-groupes finis considérés sont étales puisque l'ordre de chacun d'entre eux n'est autre que l'ordre du groupe de ses points à valeurs dans $\bar{k}$;
- supposons donc les trois groupes connexes et soit B l'algèbre affine de G, soit B^+ son idéal d'augmentation. L'algèbre affine C de G'' s'identifie à une sous-k-bigèbre (formelle) de B ; c'est un anneau local dont l'idéal maximal n'est autre que l'idéal d'augmentation $C^+ = C \cap B^+$. On voit que l'algèbre affine $\tilde{B}$ de G' s'identifie au quotient B/BC^+, ou encore à $(C/C^+) \otimes_C B$. Comme C est local, il résulte de la proposition 6.3 que B est un C-module libre ; il est clair que l'on obtient une base

de B sur C en relevant une base de $\tilde{B}$ sur k. La dimension de B sur k est donc égale au produit de celle de $\tilde{B}$ par celle de C, ce qui achève la démonstration.

En particulier, on voit que, pour qu'une suite

$$0 \to G' \to G \to G'' \to 0$$

de k-groupes finis soit exacte, il faut et il suffit que les deux conditions suivantes soient réalisées :

i) pour tout k-anneau fini R, la suite

$$0 \to G'(R) \to G(R) \to G''(R)$$

est exacte ;

ii) l'ordre de G est égal au produit de l'ordre de G' par celui de G''.

§ 8.- Espaces tangent et cotangent.

Dans ce paragraphe, k est un anneau commutatif.

8.1. Soit G un k-groupe affine, soit B son algèbre affine ; notons B^+ l'idéal d'augmentation et $B_2^+ = (B^+)^2$. Pour tout k-anneau R, nous appelons espace cotangent de G à valeurs dans R, et notons $t_G^*(R)$ le R-module $(B^+/B_2^+) \otimes_k R$; nous appelons espace tangent de G à valeurs dans R, et notons $t_G(R)$ le R-module des applications k-linéaires de B^+/B_2^+ dans R.

8.2. Soit toujours G un k-groupe affine d'algèbre affine B et soit $\Omega_k(B)$ le B-module des k-différentielles de l'anneau B. Il résulte du lemme de Yoneda que se donner un $\omega \in \Omega_k(B)$ revient à se donner, pour tout k-anneau R et tout $u \in G(R)$, un élément $\omega_R(u)$ de $\Omega_k(R)$ de manière que, si $\varphi : R \to S$ est un morphisme de k-anneaux, on ait $\omega_S(G(\varphi)(u)) = \Omega_k(\varphi)(\omega_R(u))$ (si $\omega = \sum a_i db_i \in \Omega_k(B)$ et si $u : B \to R$ est un élément de $G(R)$, on a $\omega_R(u) = \sum u(a_i)du(b_i)$).

On dit qu'une différentielle $\omega \in \Omega_k(B)$ est invariante si, pour tout k-anneau R et pour $u,v \in G(R)$, on a $\omega_R(u+v) = \omega_R(u) + \omega_R(v)$. On note

$\omega_{G/k}$ le sous-k-module de $\Omega_k(B)$ formé des différentielles invariantes.

Notons $\Delta : B \to B \otimes_k B$ le coproduit et i_1 (resp. i_2) : $B \to B \otimes_k B$ l'application $b \mapsto b \otimes 1$ (resp. $b \mapsto 1 \otimes b$) . Toujours par Yoneda, on voit que $\omega_{G/k}$ est formé des $\omega \in \Omega_k(B)$ tels que $\Omega_k(\Delta)(\omega) = (\Omega_k(i_1) + \Omega_k(i_2))(\omega)$. Comme $\Omega_k(B)$ est un B-module, l'extension des scalaires définit un homomorphisme de $B \otimes_k \omega_{G/k}$ dans $\Omega_k(B)$.

PROPOSITION 8.1.- <u>Le</u> k-<u>module</u> $\omega_{G/k}$ <u>est canoniquement isomorphe à</u> $t^*_G(k)$ <u>et l'homomorphisme canonique de</u> $B \otimes_k \omega_{G/k}$ <u>dans</u> $\Omega_k(B)$ <u>est un isomorphisme</u>.

<u>Démonstration</u> : soit I le noyau de l'application de $B \otimes_k B$ dans B définie par le produit. On sait que $\Omega_k(B)$ s'identifie à I/I^2 .

Considérons le morphisme $\eta : G \times G \to G \times G$ qui, pour tout k-anneau R, associe à $(x,y) \in G(R) \times G(R)$ l'élément $(x, x-y)$. Il est clair que η est un automorphisme de $G \times G$ induisant l'identité sur la première composante. Par conséquent η induit un automorphisme η^* de $B \otimes_k B$ qui est B-linéaire (pour la structure de B-module sur $B \otimes_k B$ définie par la multiplication à gauche).

On voit que le diagramme

$$\begin{array}{ccc} G & \xrightarrow{\text{id}} & G \\ \delta \downarrow & & \downarrow \nu \\ G \times G & \xrightarrow{\eta} & G \times G \end{array}$$

où $\delta_R(x) = (x,x)$ et $\nu_R(x) = (x,0)$, est commutatif. Il induit, sur les bigèbres, un autre diagramme commutatif

$$\begin{array}{ccc} B & \xleftarrow{\text{id}} & B \\ \text{prod.} \uparrow & & \uparrow \text{id}_B \otimes \varepsilon_B \\ B \otimes_k B & \xleftarrow{\eta^*} & B \otimes_k B \end{array}$$

où les flèches horizontales sont des isomorphismes et les flèches verticales sont surjectives ; les noyaux de ces dernières, i.e. I et $B \otimes_k B^+$ (car B^+ est facteur direct de B en tant que k-module) s'identifient donc canoniquement. On en déduit que I/I^2 s'identifie à $B \otimes_k (B^+/B^+_2)$, donc à $B \otimes_k t^*_G(k)$.

Enfin, on vérifie facilement que, dans cette identification, $\omega_{G/k}$ s'identifie à $t^*_G(k)$.

8.3. Soit toujours G un k-groupe affine d'algèbre affine B . Pour tout B-anneau R , notons $Der_k(B,R)$ le R-module des k-dérivations de B dans R (remarquons que tout k-anneau R peut être considéré comme un B-anneau au moyen de l'application composée $B \xrightarrow{\epsilon_B} k \xrightarrow{can} R$).

Il résulte de la propriété universelle du module des différentielles que $Der_k(B,R)$ s'identifie canoniquement au R-module des applications B-linéaires de $\Omega_k(B)$ dans R . Comme $\Omega_k(B)$ est canoniquement isomorphe à $B \otimes_k (B^+/B^+_2)$, $Der_k(B,R)$ s'identifie au R-module des applications k-linéaires de B^+/B^+_2 dans R , i.e. à $t_G(R)$.

Soit $Der_k(B) = Der_k(B,B)$ le module des k-dérivations de B dans B . Si $D \in Der_k(B)$, nous notons D_1 l'élément de $Der_k(B \otimes_k B)$ défini par $D_1(x \otimes_k y) = D(x) \otimes_k y$. Nous disons qu'un élément de $Der_k(B)$ est une k-<u>dérivation invariante</u> si, pour tout $x \in B$, $\Delta(Dx) = D_1(\Delta x)$, où Δ est le coproduit. On vérifie immédiatement que, lorsque l'on identifie $Der_k(B)$ à $t_G(B)$, le k-module des dérivations invariantes s'identifie à $t_G(k)$.

8.4. Pour tout k-anneau R , notons $R(t) = R \otimes_k k(t)$ l'<u>algèbre des nombres duaux</u> à valeurs dans R , i.e. l'algèbre $R[T]/T^2$ (on a noté t l'image de T). Pour tout k-groupe affine G , on note $\mathrm{Lie}\,G(R)$ le noyau de l'homomorphisme canonique de $G(R(t))$ dans $G(R)$ (provenant de l'application R-linéaire de $R(t)$ dans R qui envoie t sur 0). Dire qu'un élément $u \in G(R(t))$ est dans $\mathrm{Lie}\,G(R)$ revient à dire que $u(B^+) \subset tR(t)$. Comme $t^2 = 0$, le noyau de u contient alors B^+_2 et u induit une application k-linéaire $\tilde{u} : B^+/B^+_2 \to R$; on vérifie immédiatement que l'application $u \mapsto \tilde{u}$ définit un isomorphisme du groupe $\mathrm{Lie}\,G(R)$ sur $t_G(R)$.

8.5. Tout ce qui précède se transpose, de manière évidente, au cas des groupes formels. Supposons maintenant que k est un anneau commutatif pseudo-compact. Soit G un k-groupe formel, d'algèbre affine B , soit B^+ l'idéal d'augmentation et soit B^+_2 l'adhérence de $(B^+)^2$ dans B . Pour tout k-anneau fini ou profini R , l'espace cotangent de G à valeurs dans R est le R-module topologique $t^*_G(R) = (B^+/B^+_2) \hat{\otimes}_k R$ et l'espace tangent est le R-module $t_G(R)$ des applications k-linéaires continues de B^+/B^+_2 dans R . Le B-module $\Omega_k(B)$ des k-différentielles continues de l'anneau B s'identifie à $B \hat{\otimes}_k t^*_G(k)$, le k-module des différentielles invariantes $\omega_{G/k}$ s'identifiant à $t^*_G(k)$; le B-module des k-dérivations continues de B à valeurs dans B s'identifie encore à $t_G(B)$ et celui des k-dérivations invariantes à $t_G(k)$. Enfin, pour tout k-anneau fini ou profini R , $t_G(R)$ s'identifie à $\mathrm{Lie}\, G(R)$.

Remarque : supposons k local et soit G un k-groupe formel topologiquement plat. Si G est étale, on a évidemment $B^+_2 = B^+$ et $t_G(R) = t^*_G(R) = 0$, pour tout k-anneau fini ou profini R ; dans le cas général, on voit que $t_G(R)$ (resp. $t^*_G(R)$) s'identifie canoniquement à $t_{G^c}(R)$ (resp. $t^*_{G^c}(R)$) .

8.6. Supposons maintenant que k est un anneau commutatif artinien. Soit G un k-groupe formel topologiquement plat et soit $\hat{G}_a$ le complété formel du groupe additif (on a donc $\hat{G}_a(R) = R$, muni de l'addition, pour tout k-anneau fini R). Comme k s'identifie, de manière évidente, à un sous-anneau de l'anneau des endomorphismes de $\hat{G}_a$, le groupe $\mathrm{Hom}(G,\hat{G}_a)$ des morphismes (de k-groupes formels) de G dans $\hat{G}_a$ a une structure naturelle de k-module topologique (la topologie étant celle de la convergence simple). On voit que $\mathrm{Hom}(G,\hat{G}_a)$ s'identifie, grâce à Yoneda, au sous-k-module fermé de l'algèbre affine B de G formé des u tels que $\Delta u = u\hat{\otimes}1 + 1\hat{\otimes}u$ (en notant Δ le coproduit).

Soit $\mathbb{D}(G)$ le dual de Cartier de G et soit B' son algèbre affine. Notons $\langle\ ,\ \rangle$ l'application k-bilinéaire canonique de $B \times B'$ dans k . Comme $\langle u,xy\rangle = \langle \Delta u, x\otimes y\rangle$, on voit qu'un élément u de B est dans $\mathrm{Hom}(G,\hat{G}_a)$ si et seulement si $\langle u,xy\rangle = \langle u\hat{\otimes}1 + 1\hat{\otimes}u, x\otimes y\rangle$, pour $x,y \in B'$, i.e. si et seulement si $\langle u,xy\rangle = \langle u,x\rangle\varepsilon(y) + \varepsilon(x)\langle u,y\rangle$, pour $x,y \in B'$ (où $\varepsilon : B' \to k$ est l'augmentation).Si l'on munit k de sa structure de B'-anneau provenant de l'augmentation, on voit que ceci revient à dire que l'application k-linéaire u de B' dans k est une dérivation. Par conséquent, $\mathrm{Hom}(G,\hat{G}_a)$ s'identifie au k-module topologique des k-dérivations de B' dans k , donc à $t_{\mathbb{D}(G)}(k)$ (la topologie étant encore celle de la convergence simple).

De la même manière, si G est un k-groupe affine plat, on voit que le k-module $\mathrm{Hom}(G,G_a)$ s'identifie canoniquement à $t_{\hat{\mathbb{D}}(G)}(k)$.

8.7. Supposons maintenant que k est un corps parfait de caractéristique $p \neq 0$.

Nous notons $k[\underline{V}]$ (resp. $k[\underline{F}]$) l'anneau (non commutatif si $k \neq \mathbb{F}_p$) engendré par k et un élément $\underline{V}$ (resp. $\underline{F}$) soumis aux relations $\lambda\underline{V} = \underline{V}\sigma(\lambda) = \underline{V}\lambda^p$ (resp. $\underline{F}\lambda = \sigma(\lambda)\underline{F} = \lambda^p\underline{F}$) pour tout $\lambda \in k$. On appelle $k[\underline{V}]$-module topologique (resp. $k[\underline{F}]$-module topologique) tout $k[\underline{V}]$-module (resp. $k[\underline{F}]$-module) qui est un k-espace vectoriel topologique sur lequel $\underline{V}$ (resp. $\underline{F}$) opère continûment.

Soit G un k-groupe formel et soit B son algèbre affine. Il est clair que V_B est un endomorphisme continu de l'anneau B, que $V_B(B^+) \subset B^+$ et $V_B(B_2^+) \subset B_2^+$. Par passage au quotient, V_B opère donc continûment sur $t_G^*(k) = B^+/B_2^+$. En posant $\underline{V}u = V_B(u)$, pour tout $u \in t_G^*(k)$, on voit que l'on munit le k-espace vectoriel topologiquement libre $t_G^*(k)$ d'une structure de $k[\underline{V}]$-module topologique.

Il est clair que $G \mapsto t_G^*(k)$ peut ainsi être considéré comme un foncteur contravariant de la catégorie des k-groupes formels dans celle des $k[\underline{V}]$-modules topologiques qui sont des k-espaces vectoriels topologiquement libres.

De la même manière, dans le cas des k-groupes affines, on voit que la correspondance $G \mapsto t_G^*(k)$ peut être considérée comme un foncteur contravariant de la catégorie des k-groupes affines dans celle des $k[\underline{V}]$-modules.

Soit, de nouveau, G un k-groupe formel et B son algèbre affine. Si l'on identifie $\mathrm{Hom}(G,\hat{G}_a)$ à un sous-k-espace vectoriel fermé de B, on voit que, si $u \in \mathrm{Hom}(G,\hat{G}_a)$, $F_B(u) = u^p$ aussi. En posant $\underline{F}u = F_B(u)$, pour tout $u \in \mathrm{Hom}(G,\hat{G}_a)$, on voit que l'on munit le k-espace vectoriel topologiquement libre $\mathrm{Hom}(G,\hat{G}_a)$ d'une structure de $k[\underline{F}]$-module topologique.

Si maintenant M est un $k[\underline{V}]$-module, on munit le k-espace vectoriel topologique dual $M' = \mathrm{Hom}(M,k)$ d'une structure de $k[F]$-module topologique en posant $(\underline{F}\eta)(x) = \sigma(\eta(\underline{V}x))$, pour tout $\eta \in M'$ et tout $x \in M$.

En particulier, si G est un k-groupe formel, on a deux structures naturelles de $k[F]$-module topologique sur $t_{\mathbb{D}(G)}(k)$: celle provenant de l'isomorphisme canonique entre $\mathrm{Hom}(G,\hat{G}_a)$ et $t_{\mathbb{D}(G)}(k)$ et celle obtenue par dualité, à partir de la structure de $k[V]$-module sur $t^*_{\mathbb{D}(G)}(k)$; on vérifie immédiatement que ces deux structures coïncident.

Il est clair que la correspondance $G \mapsto \mathrm{Hom}(G,\hat{G}_a) \simeq t_{\mathbb{D}(G)}(k)$ peut être considérée comme un foncteur contravariant de la catégorie des k-groupes formels dans celle des $k[\underline{F}]$-modules topologiques.

Ceci se transpose aux groupes affines et la correspondance $G \mapsto \mathrm{Hom}(G,G_a) \simeq t_{\hat{\mathbb{D}}(G)}(k)$ peut être considérée comme un foncteur contravariant de la catégorie des k-groupes affines dans celle des $k[\underline{F}]$-modules.

§ 9.- Structure des groupes formels connexes sur un corps.

Dans tout ce paragraphe, k est un corps parfait.

9.1. Commençons par introduire la définition suivante :

- si k est de caractéristique 0, on dit qu'un k-anneau profini local est <u>élémentaire</u> si c'est un anneau de séries formelles à coefficients dans k ;
- si k est de caractéristique $p \neq 0$, on dit qu'un k-anneau profini local est <u>élémentaire</u> s'il existe un ensemble J et des éléments $\nu(j) \in \mathbb{N}^* \cup \{+\infty\}$ tels que cet anneau soit isomorphe au quotient de l'anneau des séries formelles $k[[(X_j)_{j\in J}]]$ par l'adhérence de l'idéal engendré par les $X_j^{p^{\nu(j)}}$, pour $\nu(j) \neq +\infty$.

Le but de ce paragraphe est d'établir le résultat suivant :

THÉORÈME 1.- <u>Soit</u> G <u>un</u> k-<u>groupe formel connexe</u>. <u>Son algèbre affine est un</u> k-<u>anneau profini local élémentaire</u>.

<u>Démonstration</u> : soit B l'algèbre affine de G, soit B^+ l'idéal d'augmentation et soit B_2^+ l'adhérence, dans B, de $(B^+)^2$.

Soit s une section k-linéaire continue de $t_G^*(k) = B^+/B_2^+$ dans B^+. L'image de s est un sous-espace vectoriel fermé de B^+, canoniquement isomorphe à $t_G^*(k)$. Soit $(y_j)_{j\in J}$ une base topologique de cet espace vectoriel topologiquement libre. Il est clair qu'il existe un homomorphisme continu θ du k-anneau profini $A = k[[(Y_j)_{j\in J}]]$ dans B et un seul tel que $\theta(Y_j) = y_j$. On voit que θ est surjectif et, comme les images des y_j dans $t_G^*(k)$ forment une base topologique de $t_G^*(k)$, que le noyau $\mathfrak{a}$ de θ est un idéal fermé de A contenu dans l'adhérence du carré de l'idéal maximal de A.

Soit $\Omega_k(A)$ le A-module topologique des k-différentielles continues de l'anneau A. Il est clair que $\Omega_k(A)$ est un A-module topologiquement libre admettant les dY_j comme base topologique. De même, si $\Omega_k(B)$ désigne le B-module topologique des k-différentielles continues de l'anneau B, on voit (cf. n° 8.5) que $\Omega_k(B)$ est un B-module topologiquement libre admettant les dy_j comme base topologique. On en déduit que si $a \in \mathfrak{a}$, on a $\frac{\partial a}{\partial Y_j} \in \mathfrak{a}$, pour tout j.

Notons enfin, pour tout entier $n \geq 1$, I_n l'adhérence de la puissance n-ième de l'idéal maximal de A. On a vu que $\mathfrak{a} \subset I_2$.

9.2. Supposons que k est de caractéristique 0 et montrons que θ est injectif. Si ce n'était pas le cas, il existerait un entier $n \geq 2$ tel que $\mathfrak{a} \subset I_n$ et $\mathfrak{a} \not\subset I_{n+1}$. Si a était un élément de $\mathfrak{a}$ n'appartenant pas à I_{n+1}, on voit que l'on pourrait trouver j tel que $\frac{\partial a}{\partial Y_j} \notin I_n$. On aurait donc $\frac{\partial a}{\partial Y_j} \notin \mathfrak{a}$, d'où une contradiction.

Dans toute la suite, nous supposons donc que k est de caractéristique $p \neq 0$.

9.3. Supposons que $F_G = 0$, autrement dit que, pour tout $x \in B^+$, on a $x^p = 0$. Alors $\mathfrak{a}$ contient l'adhérence $\mathfrak{a}_0$ de l'idéal de A engendré par les Y_j^p. Montrons que $\mathfrak{a} = \mathfrak{a}_0$. Sinon, il existerait un entier n tel que $\mathfrak{a} \subset I_n + \mathfrak{a}_0$ et $\mathfrak{a} \not\subset I_{n+1} + \mathfrak{a}_0$. Si $a \in \mathfrak{a}$ et $\notin I_{n+1} + \mathfrak{a}_0$, on pourrait écrire $a = a' + a''$, avec a' série formelle homogène non nulle de degré n en les Y_j, dont le degré par rapport à chaque variable est $< p$ et $a'' \in I_{n+1} + \mathfrak{a}_0$. Il est clair que, pour tout j, $\frac{\partial I_{n+1}}{\partial Y_j} \subset I_n$ et que $\frac{\partial \mathfrak{a}_0}{\partial Y_j} \subset \mathfrak{a}_0$; on en déduit que $\frac{\partial a''}{\partial Y_j} \in I_n + \mathfrak{a}_0$. On voit que l'on pourrait choisir j pour que $\frac{\partial a'}{\partial Y_j} \notin I_n + \mathfrak{a}_0$; on aurait donc $\frac{\partial a}{\partial Y_j} \notin I_n + \mathfrak{a}_0$, d'où $\frac{\partial a}{\partial Y_j} \notin \mathfrak{a}$, d'où une contradiction.

9.4. Passons maintenant au cas général. Pour tout entier $r \geq 0$, soit $V_r = \{a \in A \mid a^{p^r} \in \mathfrak{a}\}$. Il est clair que les V_r forment une suite croissante d'idéaux fermés de A. Pour chaque r, le quotient $\tilde{V}_r = V_r/(V_r \cap I_2)$ est un sous-k-espace vectoriel fermé de I/I_2, lui-même canoniquement isomorphe à $B^+/B_2^+ = t_G^*(k)$:

$$\begin{array}{ccccccccccccc}
\mathfrak{a} = V_0 & \subset & V_1 & \subset & V_2 & \subset & \dots & \subset & V_r & \subset & \dots & \subset & I \\
\downarrow & & \downarrow & & \downarrow & & & & \downarrow & & & & \downarrow \\
0 = \tilde{V}_0 & \subset & \tilde{V}_1 & \subset & \tilde{V}_2 & \subset & \dots & \subset & \tilde{V}_r & \subset & \dots & \subset & I/I_2 \simeq t_G^*(k) .
\end{array}$$

Pour tout $a \in I$, notons $\tilde{a}$ son image dans I/I_2. Appelons <u>bon système de coordonnées pour</u> A <u>relativement à</u> G <u>et</u> θ tout système de coordonnées $\underline{X} = (X_j)_{j \in J}$ de A tel que, pour tout entier $r \geq 0$, les images $\tilde{X}_j$ des X_j qui sont dans V_r forment une base topologique de $\tilde{V}_r$. On voit facilement qu'un tel système existe toujours.

Soit $\underline{X} = (X_j)_{j \in J}$ un bon système de coordonnées pour A relativement à G et θ. Pour tout $j \in J$, posons

$$\nu(j) = \nu^{\underline{X}}(j) = \begin{cases} +\infty & \text{si } X_j \notin \bigcup_{r \geq 0} V_r , \\ r & \text{si } X_j \in V_r - V_{r-1} . \end{cases}$$

Notons $\mathfrak{b} = \mathfrak{b}(\theta, \underline{X})$ l'adhérence de l'idéal de A engendré par les $X_j^{p^{\nu(j)}}$, pour les j tels que $\nu(j) \neq +\infty$. Il est clair que $\mathfrak{b} \subset \mathfrak{a}$. Pour achever la démonstration du théorème, on voit qu'il suffit d'établir le lemme :

LEMME 9.1.- <u>Soit</u> $\underline{X} = (X_j)_{j \in J}$ <u>un bon système de coordonnées pour</u> A <u>relativement à</u> G <u>et</u> θ . <u>Le noyau</u> $\mathfrak{a}$ <u>de</u> θ <u>est l'idéal</u> $\mathfrak{b}(\theta, \underline{X})$.

<u>Démonstration</u> : pour tout $j \in J$, soit x_j l'image de X_j dans B et, pour tout entier $r \geq 1$, soit $\mathfrak{f}_r$ (resp. $\mathfrak{f}_r^A$) l'adhérence de l'idéal de B (resp. A) engendré par les $x_j^{p^r}$ (resp. les $X_j^{p^r}$). On voit que $\mathfrak{a} = \bigcap_{r \geq 1} (\mathfrak{a} + \mathfrak{f}_r^A)$ et il suffit donc de montrer que, pour tout entier $r \geq 1$, on a $\mathfrak{b} + \mathfrak{f}_r^A = \mathfrak{a} + \mathfrak{f}_r^A$.

On voit que $B_r = B/\mathfrak{f}_r$ s'identifie à l'algèbre affine du groupe $G_r = \mathrm{Ker}\, F_G^r$ et que, si l'on note θ_r l'application composée

$$A \xrightarrow{\theta} B \xrightarrow{\text{proj.}} B/\mathfrak{f}_r ,$$

$\underline{X} = (X_j)_{j \in J}$ est un bon système de coordonnées pour A relativement à G_r et θ_r. On voit aussi que le noyau de θ_r est $\mathfrak{a} + \mathfrak{f}_r^A$ et que $\mathfrak{b}(\theta_r, \underline{X}) = \mathfrak{b} + \mathfrak{f}_r^A$.

Il suffit donc de démontrer le lemme dans le cas où il existe un entier $r \geq 1$ tel que $F_G^r = 0$, i.e. dans le cas où $\nu(j) \leq r$, pour tout $j \in J$. Nous allons procéder par récurrence sur r :

- si $r = 1$, cela résulte du n° 9.3 ;
- dans le cas général, soit $C = \{b^p \mid b \in B\}$. Il est clair que C est une sous-k-bigèbre formelle de B ; elle correspond à un quotient H de G qui est un k-groupe formel connexe vérifiant $F_H^{r-1} = 0$ et qui n'est autre que la co-image de F_G. L'idéal d'augmentation C^+ de C n'est autre que son idéal maximal ; c'est aussi $C \cap B^+$. On voit que $\tilde{B} = (C/C^+) \hat{\otimes}_C B$ s'identifie à l'algèbre affine du noyau de F_G. Il résulte du n° 9.3 que le noyau de la projection de A sur B est l'idéal $\mathfrak{r}_1^A$, adhérence de l'idéal engendré par les X_j^p. On en déduit que les images, dans B, des éléments de la forme $\prod_{j \in J} x_j^{n_j}$, avec les n_j des entiers presque tous nuls vérifiant $0 \leq n_j < p$, forment une base topologique de B sur $k = C/C^+$.

D'après la proposition 6.3, B est un C-module topologiquement plat, donc topologiquement libre puisque C est local. Ce qui précède montre donc que les éléments de B de la forme $\prod_{j \in J} x_j^{n_j}$, avec les n_j des entiers presque tous nuls vérifiant $0 \leq n_j < p$, forment une base topologique de B sur C.

Soit, d'autre part, J' l'ensemble des $j \in J$ tels que $\nu(j) \geq 2$ et soit $A' = k[[(X_j^p)_{j \in J'}]]$. La restriction de θ à A' est un homomorphisme continu θ' de A' sur C dont le noyau est $\mathfrak{a} \cap A'$. On voit que $\underline{X}' = (X_j^p)_{j \in J'}$ est un bon système de coordonnées pour A' relativement à H et θ' et que $\mathfrak{b}(\theta', \underline{X}') = \mathfrak{b}(\theta, \underline{X}) \cap A'$. L'hypothèse de récurrence appliquée à H implique que $\mathfrak{b}(\theta, \underline{X}) \cap A' = \mathfrak{a} \cap A'$.

Soit $A_C = k[[(X_j^p)_{j \in J}]]$. Si $j \in J - J'$, $X_j^p \in \mathfrak{b}(\theta, \underline{X}) \cap A_C$; on en déduit que $\mathfrak{b}(\theta, \underline{X}) \cap A_C = \mathfrak{a} \cap A_C$.

Soit $\tilde{A} = A/\mathfrak{b}(\theta, \underline{X})$ et soit $\tilde{X}_j$ l'image de X_j dans $\tilde{A}$. On voit que θ induit une application surjective $\tilde{\theta} : \tilde{A} \to B$ (on a $\tilde{\theta}(\tilde{X}_j) = x_j$) et que la restriction de θ à $\tilde{A}' = k[[(\tilde{X}_j^p)_{j \in J}]]$ est injective et a pour image C ; on peut donc identifier C à un sous-anneau fermé de A et θ devient alors une application C-linéaire continue.

On voit que $\tilde{A}$ est un C-module topologiquement libre admettant les éléments de la forme $\prod_{j\in J} \tilde{X}_j^{n_j}$, avec les n_j des entiers presque tous nuls vérifiant $0 \leq n_j < p$, comme base topologique. On a vu que les images de ces éléments par $\tilde{\theta}$ forment une base de B sur C . On en déduit que $\tilde{\theta}$ est bijective, ce qui achève la démonstration.

9.5. Remarques :

1.- Supposons k de caractéristique 0 . Le théorème implique que, si G est un k-groupe fini connexe, G est trivial ; autrement dit, tout k-groupe fini est étale.

2.- Supposons k de caractéristique $p \neq 0$. Si G est un k-groupe fini connexe non trivial, le théorème implique qu'il existe des entiers $d, \nu(1), \nu(2), \ldots, \nu(d) \geq 1$ tels que l'algèbre affine de G est isomorphe à $k[X_1, X_2, \ldots, X_d] / \left(X_1^{p^{\nu(1)}}, X_2^{p^{\nu(2)}}, \ldots, X_d^{p^{\nu(d)}}\right)$. En particulier, tout k-groupe fini connexe est d'ordre une puissance de p .

9.6. On dit qu'un k-groupe formel est lisse si son algèbre affine est "formellement lisse", i.e. si, pour tout k-anneau fini R et tout idéal I de R de carré nul, l'application canonique de $G(R)$ dans $G(R/I)$ est surjective.

On voit que tout k-groupe formel étale est lisse et on en déduit qu'un k-groupe formel G est lisse si et seulement si G^c l'est. Un k-groupe formel connexe est lisse si et seulement si son algèbre affine est un anneau de séries formelles à coefficients dans k . Un k-groupe formel est lisse si et seulement si son algèbre affine est un anneau de séries formelles à coefficients dans un produit d'extensions finies du corps k .

Si k est de caractéristique 0 , il résulte du théorème que tout k-groupe formel connexe est lisse et, par conséquent, tout k-groupe formel est lisse.

Si k est de caractéristique $p \neq 0$, il résulte du théorème que, pour qu'un k-groupe formel connexe G soit lisse, il faut et il suffit que F_G soit un épimorphisme. On en déduit qu'un k-groupe formel G , d'algèbre affine B , est lisse si et seulement si F_G est un épimorphisme, ou encore si et seulement si l'application F_B est injective.

Si G est un k-groupe formel lisse, on appelle dimension de G la dimension du k-espace vectoriel $t_G(k)$. On voit que la dimension de G est égale à celle de G^c .

Lorsque k est de caractéristique $p \neq 0$, on voit qu'un k-groupe formel lisse G est de dimension finie si et seulement si $\mathrm{Ker}\, F_G$ est un groupe fini. Dans ce cas, si G est de dimension d , on voit que $\mathrm{Ker}\, F_G$ est d'ordre p^d et, plus généralement, que, pour tout entier $n \geq 0$, $\mathrm{Ker}\, F_G^n$ est un k-groupe fini d'ordre p^{nd} . En particulier $G^c = \varinjlim \mathrm{Ker}\, F_G^n$ est limite inductive de k-groupes finis.

9.7. Soit A un anneau local pseudo-compact dont le corps résiduel est k . On dit encore qu'un A-groupe formel G est <u>lisse</u> si, pour tout A-anneau fini R et tout idéal I de R de carré nul, l'application canonique de $G(R)$ dans $G(R/I)$ est surjective.

On démontre facilement qu'un A-groupe formel lisse est topologiquement plat et que, si G est un A-groupe formel topologiquement plat, G est lisse si et seulement si $G_k^c = (G_k)^c \simeq (G^c)_k$ l'est, ou encore si et seulement si l'algèbre affine de G^c est un anneau de séries formelles à coefficients dans A . Supposons qu'il en est ainsi et notons B , B^c , B^{et} , B_k , B_k^c , B_k^{et} les algèbres affines respectives de G , G^c , G^{et} , G_k , G_k^c , G_k^{et} . On a vu que B_k s'identifie canoniquement à $B_k^{et} \hat{\otimes}_k B_k^c$; l'homomorphisme canonique de B_k^c dans B_k se relève (non canoniquement) en un homomorphisme continu de B^c dans B et B est donc isomorphe à $B^{et} \hat{\otimes}_A B^c$. En particulier, pour tout A-anneau fini R , la suite

$$0 \longrightarrow G^c(R) \longrightarrow G(R) \longrightarrow G^{et}(R) \longrightarrow 0$$

est exacte.

§10.- <u>Cohomologie de Hochschild</u>.

Dans tout ce paragraphe, k est un corps parfait de caractéristique 0 ou p (où p est un nombre premier fixé).

10.1. Pour tout entier $r \geq 2$, soit $B_r(X,Y) = (X+Y)^r - X^r - Y^r \in \mathbb{Z}[X,Y]$, soit η_r le pgcd des coefficients de $B_r(X,Y)$ et soit $C_r(X,Y) = \eta_r^{-1} B_r(X,Y)$; c'est donc un polynôme à deux variables, homogène de degré r, dont les coefficients sont des entiers premiers entre eux.

Commençons par rappeler le résultat suivant, dû à Lazard ([36], p.44) à qui nous renvoyons pour la démonstration :

PROPOSITION 10.1.- Soit A un groupe abélien et soit r un entier ≥ 2. Soit $P(X,Y) = \sum_{i+j=r} a_{i,j} X^i Y^j$ un polynôme homogène de degré r, en deux variables X et Y, à coefficients dans A. On suppose que $P(Y,X) = P(X,Y)$ et $P(Y,Z) - P(X+Y,Z) + P(X,Y+Z) - P(X,Y) = 0$. Il existe alors un $c \in A$ et un seul tel que $P(X,Y) = cC_r(X,Y)$.

On en déduit facilement le résultat suivant :

PROPOSITION 10.2.- Soit $\Lambda(X,Y) = p^{-1}((X+Y)^p - X^p - Y^p) \in \mathbb{Z}[X,Y]$ et soit r un entier ≥ 2.

i) Soit $P(X) = aX^r$ un polynôme homogène, non nul, de degré r en une variable X, à coefficient dans k. On a $P(Y) - P(X+Y) + P(X) \neq 0$, sauf si et seulement si k est de caractéristique p et r est une puissance de p.

ii) Soit $P(X,Y) = \sum_{i+j=r} a_{i,j} X^i Y^j$ un polynôme homogène de degré r, en deux variables X et Y, à coefficients dans k, vérifiant $P(Y,X) = P(X,Y)$ et $P(Y,Z) - P(X+Y,Z) + P(X,Y+Z) - P(X,Y) = 0$. Alors

- si k est de caractéristique 0, ou si r n'est pas une puissance de p, il existe un $c \in k$ et un seul tel que $P(X,Y) = c((X+Y)^r - X^r - Y^r)$;

- si k est de caractéristique p et si $r = p^s$ (avec s entier ≥ 1), il existe un $c \in k$ et un seul tel que $P(X,Y) = c\Lambda(X^{p^{s-1}}, Y^{p^{s-1}})$.

Démonstration : on vérifie facilement que les coefficients de $B_r(X,Y) = (X+Y)^r - X^r - Y^r$ sont des entiers premiers entre eux sauf si, et seulement si, r est une puissance d'un nombre premier ℓ, auquel cas le pgcd est ℓ.

L'assertion (i) est alors triviale.

L'assertion (ii) résulte alors de la proposition 10.1, si l'on remarque que

$C_{p^s}(X,Y) = p^{-1}((X+Y)^{p^s} - X^{p^s} - Y^{p^s})$ est un polynôme, à coefficients dans $\mathbb{Z}$, congru modulo p, à $\Lambda(X^{p^{s-1}}, Y^{p^{s-1}})$.

10.2. On sait (cf. [14], p. 185) ce que c'est que la cohomologie de Hochschild des k-foncteurs en groupes. On définit de la même manière la cohomologie de Hochschild des foncteurs en groupes formels. Nous ne nous intéresserons en fait qu'au cas où les k-foncteurs en groupes formels considérés sont des k-groupes formels commutatifs et où la loi d'opération est triviale : soient G et J deux k-groupes formels (commutatifs). Pour tout entier $n \geq 0$, <u>le groupe des</u> n-<u>cochaînes de</u> G <u>à valeurs dans</u> J est l'ensemble $C^n(G,J)$ des morphismes de k-foncteurs formels (ou de k-schémas formels) de G^n dans J, muni de la loi de groupe abélien induite par J.

Se donner un élément f de $C^n(G,J)$ revient donc à se donner, pour tout k-anneau fini R, une application $f_R : (G(R))^n \to J(R)$, variant fonctoriellement par rapport à R.

On définit un opérateur bord $\partial^n : C^n(G,J) \to C^{n+1}(G,J)$ par la formule

$$(\partial_R^n f_R)(u_1, u_2, \dots, u_{n+1}) = f_R(u_2, \dots, u_{n+1}) + \sum_{i=1}^{n} (-1)^i f_R(u_1, \dots, u_i + u_{i+1}, \dots, u_{n+1})$$
$$+ (-1)^{n+1} f_R(u_1, \dots, u_n) .$$

On vérifie immédiatement que $\partial^n \circ \partial^{n-1} = 0$, pour $n \geq 1$; on note $C^{\cdot}(G,J)$ le complexe $(C^n(G,J), \partial^n)_{n \in \mathbb{N}}$; on note $Z^n(G,J)$ le noyau de ∂^n et $B^n(G,J)$ l'image de ∂^{n-1}, pour $n \geq 1$, $B^0(G,J) = 0$; on note $H_0^n(G,J)$ le groupe quotient $Z^n(G,J)/B^n(G,J)$ et on l'appelle le n-<u>ième groupe de Hochschild de</u> G <u>à valeurs dans</u> J. Enfin, nous écrirons ∂ au lieu de ∂^n lorsqu'il n'y aura pas de confusions possible sur l'entier n.

On voit, en particulier, que $H_0^0(G,J)$ s'identifie à $J(k)$ et que $H_0^1(G,J)$ s'identifie au groupe $\mathrm{Hom}(G,J)$ des morphismes de G dans J, dans la catégorie des k-groupes formels.

Nous notons $C_s^2(G,J)$ le groupe des 2-cocycles symétriques, i.e. le sous-groupe de $C^2(G,J)$ formé des f tels que $f_R(u,v) = f_R(v,u)$, pour tout k-anneau fini R et pour $u,v \in G(R)$. On pose $Z_s^2(G,J) = C_s^2(G,J) \cap Z^2(G,J)$. Il est clair que $B^2(G,J) \subset Z_s^2(G,J)$ et on note $H_s^2(G,J)$ le sous-groupe $Z_s^2(G,J)/B^2(G,J)$ de $H_0^2(G,J)$.

On vérifie par des procédés standards (cf., par exemple, [14], II, § 3, n° 2) que $H^2_s(G,J)$ s'identifie canoniquement au groupe des classes d'extensions E de G par J qui sont encore des k-groupes formels commutatifs et qui sont scindées en tant qu'extensions de k-schémas formels (cette dernière condition revenant, en fait, à dire que, pour tout k-anneau fini R, la suite

$$0 \to J(R) \to E(R) \to G(R) \to 0$$

est exacte).

10.3. PROPOSITION 10.3.- <u>Soit</u> $(G_i)_{i \in I}$ <u>une famille de</u> k-<u>groupes formels et soit</u> J <u>un</u> k-<u>groupe formel</u>. <u>Alors</u>

i) <u>les groupes</u> $H^1_0(\oplus G_i, J)$ <u>et</u> $\Pi H^1_0(G_i, J)$ <u>sont canoniquement isomorphes</u>;

ii) <u>les groupes</u> $H^2_s(\oplus G_i, J)$ et $\Pi H^2_s(G_i, J)$ <u>sont canoniquement isomorphes</u>.

<u>Démonstration</u> : on voit que $H^1_0(\oplus G_i, J)$ s'identifie canoniquement à $\mathrm{Hom}(\oplus G_i, J) \simeq \Pi\, \mathrm{Hom}(G_i, J) \simeq \Pi\, H^1_0(G_i, J)$, d'où (i).

Soit $\mathrm{Res}_i : H^2_s(\oplus G_j, J) \to H^2_s(G_i, J)$ le morphisme de restriction et soit $\mathrm{Res} : H^2_s(\oplus G_i, J) \to \Pi\, H^2_s(G_i, J)$ le produit des Res_i. Nous allons montrer que Res est un isomorphisme.

Soit $e \in H^2_s(\oplus G_i, J)$ et soit E un représentant de la classe d'extensions de $\oplus G_i$ par J définie par e. Soit π la projection de E sur $\oplus G_i$. Pour tout $i \in I$ et tout k-anneau fini R, notons $E_i(R)$ l'image réciproque de $G_i(R)$ par π_R. On voit que la suite

$$0 \to J(R) \to E_i(R) \to G_i(R) \to 0$$

est exacte ; le k-foncteur formel E_i est donc un k-groupe formel, extension de G_i par J, scindée en tant qu'extension de schémas formels, et on voit facilement que la classe de cette extension correspond à l'élément $e_i = \mathrm{Res}_i(e)$ de $H^2_s(G_i, J)$.

On voit, tout aussi facilement, que, pour tout k-anneau fini R, $E(R)$ s'identifie à la somme amalgamée (dans la catégorie des groupes abéliens) des $E_i(R)$ sous $J(R)$, autrement dit au quotient de $\oplus E_i(R)$ par le sous-groupe de $(J(R))^{(I)}$ formé des $u = (u_i)_{i \in I}$ tels que $\sum u_i = 0$ (comme E est un k-groupe formel, E est lui-même la somme amalgamée des E_i sous J, dans la catégorie des k-groupes formels).

Si tous les e_i sont nuls, chaque E_i s'identifie à $J\times G_i$ et, par conséquent, E s'identifie à $J\times(\oplus G_i)$, donc $e=0$ et l'application Res est bien injective.

Donnons-nous maintenant, pour chaque i, un élément $e_i \in H^2_s(G_i,J)$ et un représentant E_i de la classe d'extensions de G_i par J correspondante. Pour tout k-anneau fini R, notons $E(R)$ la somme amalgamée des $E_i(R)$ sous $J(R)$. On voit que l'on a ainsi défini un k-foncteur en groupes formels E. Comme pour tout R, la suite

$$0 \longrightarrow J(R) \longrightarrow E(R) \longrightarrow \oplus G_i(R) \longrightarrow 0$$

est exacte, E est un k-groupe formel extension de $\oplus G_i$ par J, scindée en tant qu'extensions de k-schémas formels. Il est clair que si e désigne l'élément de $H^2_s(\oplus G_i,J)$ défini par E, on a $\mathrm{Res}_i(e) = e_i$, pour tout i. La surjectivité de l'application Res en résulte.

10.4. Soit G et J deux k-groupes formels et soit B l'algèbre affine de G. Par Yoneda, $C^n(G,J)$ s'identifie au groupe $J(\mathcal{O}^f_k(G^n)) = J(\hat{\otimes}^n B)$.

Supposons maintenant que $J = \hat{G}_a$ est le complété formel du groupe additif. On voit que $\hat{G}_a(\hat{\otimes}^n B)$ s'identifie au groupe additif de $\hat{\otimes}^n B$ et a une structure naturelle de k-espace vectoriel topologique, topologiquement libre. Il est clair que les applications ∂^n sont k-linéaires continues, ce qui permet de considérer les $Z^n(G,\hat{G}_a)$, $B^n(G,\hat{G}_a)$, $H^n_0(G,\hat{G}_a)$ comme des k-espaces vectoriels topologiquement libres ; il en est de même de $C^2_s(G,\hat{G}_a)$ (qui s'identifie à l'espace vectoriel des tenseurs symétriques de $B\hat{\otimes}B$), $Z^2_s(G,\hat{G}_a)$ et $H^2_s(G,\hat{G}_a)$.

Avec l'identification qui précède, si $\Delta : B \to B\hat{\otimes}B$ est le co-produit, on voit que

$$\partial^n(b_1\hat{\otimes}\ldots\hat{\otimes}b_n) = 1\hat{\otimes}b_1\hat{\otimes}\ldots\hat{\otimes}b_n + \sum_{i=1}^{n}(-1)^i b_1\hat{\otimes}\ldots\hat{\otimes}\Delta b_i\hat{\otimes}b_{i+1}\hat{\otimes}b_n$$
$$+ (-1)^{n+1}b_1\hat{\otimes}b_2\hat{\otimes}\ldots\hat{\otimes}b_n\hat{\otimes}1 .$$

Supposons maintenant que G est la somme directe d'une famille, indexée par un ensemble I, de copies du groupe formel additif $\hat{G}^c_a$; en d'autres termes, l'algèbre affine de G est un anneau de séries formelles $k[[(X_i)_{i\in I}]] \simeq \hat{\bigotimes}_{i\in I} k[[X]]$ et le coproduit Δ est défini par $\Delta X_i = X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i$, pour tout $i \in I$.

Pour tout entier $n \geq 0$, tout élément de $\hat{\otimes}^n B$ s'écrit, d'une manière et d'une seule, sous la forme $\sum_{r=0}^{\infty} u_r$, où u_r est une série formelle homogène de degré r en les $1 \hat{\otimes} \ldots 1 \hat{\otimes} X_i \hat{\otimes} 1 \hat{\otimes} \ldots \hat{\otimes} 1$. Ceci nous permet de considérer $C^n(G,\hat{G}_a)$ comme un espace vectoriel topologique gradué, i.e. $C^n(G,\hat{G}_a)$ s'identifie à $\prod_{r=0}^{\infty} C^{n,r}(G,\hat{G}_a)$, où $C^{n,r}(G,\hat{G}_a)$ est le sous-k-espace vectoriel fermé de $C^n(G,\hat{G}_a)$ formé des séries formelles homogènes de degré r.

On voit que cette graduation est compatible avec l'opérateur bord et induit donc une graduation sur la cohomologie. Avec des notations évidentes, on a $H_0^n(G,\hat{G}_a) = \prod_{r=0}^{\infty} H_0^{n,r}(G,\hat{G}_a)$ et $H_s^2(G,\hat{G}_a) = \prod_{r=0}^{\infty} H_s^{2,r}(G,\hat{G}_a)$.

Rappelons que l'on a noté $\Lambda(X,Y)$ le polynôme, à coefficients dans $\mathbb{Z}$, $p^{-1}((X+Y)^p - X^p - Y^p)$.

PROPOSITION 10.4.- Conservons les hypothèses et notations qui précèdent et soit r un entier ≥ 2.

i) Si k est de caractéristique 0 ou si r n'est pas une puissance de p, on a $H_0^{1,r}(G,\hat{G}_a) = 0$ et $H_s^{2,r}(G,\hat{G}_a) = 0$.

ii) Si k est de caractéristique p et si $r = p^t$, avec $t \geq 1$, on a $H_0^{1,r}(G,\hat{G}_a) \simeq k^I$, les X_i^r, pour $i \in I$, forment une base topologique de $H_0^{1,r}(G,\hat{G}_a) = Z^{1,r}(G,\hat{G}_a)$ sur k ;

- on a $H_s^{2,r}(G,\hat{G}_a) \simeq k^I$, les images des $\Lambda(X_i^{p^{t-1}} \hat{\otimes} 1, 1 \hat{\otimes} X_i^{p^{t-1}})$ dans $H_s^{2,r}(G,\hat{G}_a)$, pour $i \in I$, forment une base topologique de $H_s^{2,r}(G,\hat{G}_a)$ dans k.

Démonstration : comme $G = \oplus G_i$, avec $G_i = \hat{G}_a^c$, la proposition 10.3 nous ramène au cas où G est de dimension 1, i.e. au cas où $B = k[[X]]$, avec $\Delta X = X \hat{\otimes} 1 + 1 \hat{\otimes} X$.

Si aX^r, avec $a \in k$, est un 1-cocycle homogène de degré r, on a $\partial(aX^r) = a\partial(X^r) = a(1 \hat{\otimes} X^r - (X \hat{\otimes} 1 + 1 \hat{\otimes} X)^r + X^r \hat{\otimes} 1)$; d'après la proposition 10.2, si $a \neq 0$, cette expression est nulle, si et seulement si k est de caractéristique p et r est une puissance de p , d'où le résultat pour $H_0^{1,r}(G,\hat{G}_a)$.

Toute 2-cochaîne homogène de degré r s'écrit, d'une manière et d'une seule comme un polynôme $P(X\hat{\otimes}1, 1\hat{\otimes}X)$ homogène de degré r ; c'est une 2-cochaîne symétrique si et seulement si $P(Y\ X) = P(X,Y)$. On voit que c'est un 2-cocycle si et seulement si $P(Y,Z) - P(X+Y,Z) + P(X,Y+Z) - P(X,Y) = 0$.

Si k est de caractéristique 0 , ou si r n'est pas une puissance de p , il résulte de la proposition 10.2 qu'il existe $c \in k$ tel que $P(X,Y) = c((X+Y)^r - X^r - Y^r)$. On voit donc que $P(X\hat{\otimes}1, 1\hat{\otimes}X) = \partial(-cX^r)$ et l'assertion (i) en résulte.

Si k est de caractéristique p et si $r = p^t$, avec t entier ≥ 1 , il résulte de la proposition 10.2 qu'il existe $c \in k$ tel que $P(X,Y) = c\Lambda(X^{p^{t-1}}, Y^{p^{t-1}})$. Comme on a $\partial b = 0$, pour tout $b \in B$, homogène de degré p^t , on voit bien que l'image de $\Lambda(X^{p^{t-1}}\hat{\otimes}1, 1\hat{\otimes}X^{p^{t-1}})$ forme une base du k-espace vectoriel $H_s^{2,r}(G,\hat{G}_a)$.

10.5. Soit G un k-groupe formel connexe quelconque et soit B son algèbre affine. Pour $n, r \in \mathbb{N}$, avec $r \geq 1$, notons $C_r^n(G,\hat{G}_a)$ l'adhérence de la puissance r-ième de l'idéal maximal de $\hat{\otimes}^n B = C^n(G,\hat{G}_a)$. On obtient ainsi une filtration des k-espaces vectoriels topologiques $C^n(G,\hat{G}_a)$ qui est visiblement compatible avec l'opérateur bord. Nous notons $H_r^n(G,\hat{G}_a)$ (resp. $H^2_{s,r}(G,\hat{G}_a)$) la composante homogène de degré r du gradué associé à $H_o^n(G,\hat{G}_a)$ (resp. $H_s^2(G,\hat{G}_a)$) .

Choisissons maintenant un anneau de séries formelles $A = k[[(X_i)_{i\in I}]]$, un homomorphisme continu surjectif θ du k-anneau A sur B et des $\nu(i) \in \mathbb{N} \cup \{+\infty\}$, avec $\nu(i) \geq 2$, tels que le noyau $\mathfrak{a}$ de θ soit l'adhérence de l'idéal engendré par les $X_i^{p^{\nu(i)}}$, pour $\nu(i) \neq +\infty$ (cela est toujours possible d'après le théorème 1 du § 9 ; si k est de caractéristique 0 , on a $\nu(i) = +\infty$, pour tout i , et θ est un isomorphisme). Posons $x_i = \theta(X_i)$.

PROPOSITION 10.5.- Conservons les hypothèses et notations qui précèdent et soit r un entier ≥ 2 . Alors

i) si k est de caractéristique 0 ou si r n'est pas une puissance

<u>de</u> p , <u>on a</u> $H^1_r(G,\hat{G}_a) = 0$ <u>et</u> $H^2_{s,r}(G,\hat{G}_a) = 0$;

ii) <u>si</u> k <u>est de caractéristique</u> p <u>et si</u> $r = p^t$, <u>avec</u> t <u>entier</u> ≥ 1 ,

- <u>les images des</u> $x_i^{p^t}$, <u>pour</u> i <u>parcourant les éléments de</u> I <u>tels que</u> $\nu(i) > t$, <u>forment une base topologique de</u> $H^1_r(G,\hat{G}_a)$ <u>sur</u> k ;
- <u>les images des</u> $\Lambda(x_i^{p^{t-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_i^{p^{t-1}})$, <u>pour</u> i <u>parcourant les éléments de</u> I <u>tels que</u> $\nu(i) \geq t$, <u>forment une base topologique de</u> $H^2_{s,r}(G,\hat{G}_a)$ <u>sur</u> k .

<u>Démonstration</u> : en posant $\Delta X_i = X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i$, on voit que l'on peut identifier $A = k[[(X_i)_{i\in I}]]$ à l'algèbre affine du k-groupe formel $G' = (\hat{G}_a^c)^{(I)}$. On voit que, pour tout i , $\Delta x_i \equiv x_i \hat{\otimes} 1 + 1 \hat{\otimes} x_i$ modulo l'adhérence du carré de l'idéal maximal de $B \hat{\otimes} B$. On en déduit que θ induit un homomorphisme continu surjectif du complexe gradué associé au complexe $C^{\cdot}(G',\hat{G}_a)$ sur le complexe gradué associé au complexe $C^{\cdot}(G,\hat{G}_a)$. On voit aussi (par exemple, en relevant de manière évidente la base topologique de B sur k formée des $\prod x_i^{n_i}$, avec les n_i des entiers presque tous nuls, vérifiant $0 \leq n_i < p^{\nu(i)}$) que cet homomorphisme est scindé. L'assertion résulte alors de la proposition 10.4.

10.6. PROPOSITION 10.6.- <u>Si</u> k <u>est de caractéristique</u> 0 , <u>tout</u> k-<u>groupe formel connexe est isomorphe à une somme directe de copies du groupe formel additif</u> $\hat{G}_a^c$.

<u>Démonstration</u> : soit G un k-groupe formel connexe. On sait (théorème 1 du § 9) que l'algèbre affine B de G est de la forme $k[[(X_i)_{i\in I}]]$. Tout revient donc à montrer que l'on peut choisir les coordonnées X_i pour que $\Delta X_i = X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i$.

Pour tout entier $r \geq 1$, soit J_r (resp. J'_r) l'adhérence de la puissance r-ième de l'idéal maximal de B (resp. $B \hat{\otimes} B$). Il est clair que, quel que soit le choix des X_i , on a $\Delta X_i \equiv X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i \pmod{J'_2}$. On en déduit qu'il suffit de prouver le lemme suivant :

LEMME 10.7.- <u>Soit</u> r <u>un entier</u> ≥ 2 <u>et soit</u> $(X_i)_{i\in I}$ <u>un système de coordonnées de</u> B <u>telles que</u> $\Delta X_i \equiv X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i \pmod{J'_r}$, <u>pour tout</u> i . <u>Il existe un système de coordonnées</u> $(X'_i)_{i\in I}$ <u>de</u> B <u>telles que</u>, <u>pour tout</u> i ,

$X'_i \equiv X_i \pmod{J_r}$ <u>et</u> $\Delta X'_i \equiv X'_i \hat{\otimes} 1 + 1 \hat{\otimes} X'_i \pmod{J'_{r+1}}$.

Démonstration : posons $\Delta X_i = X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i + b_i$, avec $b_i \in J'_r$. On voit que b_i est un tenseur symétrique et que, comme $b_i = -\partial X_i$, $\partial b_i = 0$. Il résulte de la proposition 10.5 qu'il existe $c_i \in J_r$ tel que $\partial c_i \equiv b_i \pmod{J'_{r+1}}$; il est clair que l'on peut choisir c_i pour que ce soit un polynôme homogène de degré r en les X_j , et la proposition 10.5 montre alors que ce choix est unique. Posant $X'_i = X_i + c_i$, on vérifie immédiatement que $\Delta X'_i \equiv X'_i \hat{\otimes} 1 + 1 \hat{\otimes} X'_i$ $\pmod{J'_{r+1}}$. Enfin, on vérifie facilement que la continuité de l'application Δ et le fait que l'on a choisi pour les c_i des polynômes homogènes en les X_j impliquent que les $X'_i = X_i + c_i$ forment encore un système de coordonnées pour B (ces précautions n'étant utiles que lorsque la dimension est infinie).

CHAPITRE II

COVECTEURS DE WITT

Dans tout ce chapitre, p est un nombre premier fixé.

§ 1.- Vecteurs et covecteurs de Witt.

1.1. Pour tout entier $n \geq 0$, soit Φ_n le polynôme, à coefficients entiers rationnels, en les variables $X_0, X_1, \ldots, X_n$ défini par

$$\Phi_n(X_0, X_1, \ldots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n .$$

Rappelons (cf, par exemple, [43], p. 50) que, pour tout polynôme ψ dans $\mathbb{Z}[X,Y]$, il existe une suite et une seule de polynômes

$$\psi_0 \in \mathbb{Z}[X_0, Y_0] ,$$

$$\psi_1 \in \mathbb{Z}[X_0, X_1, Y_0, Y_1] ,$$

$$\ldots$$

$$\psi_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n, Y_0, Y_1, \ldots, Y_n] ,$$

$$\ldots$$

tels que, pour tout entier $n \geq 0$,

$$\psi(\Phi_n(X_0, X_1, \ldots, X_n), \Phi_n(Y_0, \ldots, Y_n)) = \Phi_n(\psi_0, \psi_1, \ldots, \psi_n) .$$

En particulier, au polynôme $\psi = S = X + Y$ correspond des polynômes $S_0 = X_0 + Y_0$, $S_1 = X_1 + Y_1 + (X_0^p + Y_0^p - (X_0 + Y_0)^p)/p, \ldots, S_n, \ldots$ et au polynôme $\psi = P = XY$ correspond des polynômes $P_0 = X_0 Y_0$, $P_1 = X_1 Y_0^p + Y_1 X_0^p + pX_1 Y_1, \ldots, P_n, \ldots$

Les S_n et les P_n définissent un schéma en anneaux commutatifs, affine sur $\operatorname{Spec} \mathbb{Z}$, d'algèbre affine $\mathbb{Z}[X_0, X_1, \ldots, X_n, \ldots ; Y_0, \ldots, Y_n, \ldots]$. D'où un foncteur covariant W de la catégorie des anneaux commutatifs dans elle-même. Si R est un anneau commutatif, $W(R)$ est l'anneau des vecteurs de Witt à coefficients dans R (sous-entendu relatifs au nombre premier p). Un vecteur $\underline{a} \in W(R)$ s'écrit

$$\underline{a} = (a_0, a_1, \ldots, a_n, \ldots) , \text{ avec les } a_i \in R .$$

Si $\underline{a} = (a_0, \ldots, a_n, \ldots)$ et $\underline{b} = (b_0, \ldots, b_n, \ldots) \in W(R)$, on a

$\underline{a} + \underline{b} = \underline{s} = (s_0,\dots,s_n,\dots)$ et $\underline{a}.\underline{b} = \underline{p} = (p_0,\dots,p_n,\dots)$ avec

$$s_n = S_n(a_0,a_1,\dots,a_n ; b_0,b_1,\dots,b_n) ,$$
$$p_n = P_n(a_0,a_1,\dots,a_n ; b_0,b_1,\dots,b_n) .$$

1.2. Pour tout entier $m \geq 1$, on peut considérer le schéma en anneaux W_m des vecteurs de Witt de longueur m. Pour tout anneau commutatif R, $W_m(R)$ est l'ensemble des $\underline{a} = (a_0,a_1,\dots,a_{m-1})$, avec les $a_i \in R$, l'addition et la multiplication étant définies par les mêmes formules que pour $W(R)$.

Pour m entier ≥ 1 et $\underline{a} = (a_0,a_1,\dots,a_n,\dots) \in W(R)$, posons $\underline{a}^{(m)} = (a_0,a_1,\dots,a_{m-1}) \in W_m(R)$. Il est clair que l'application qui à $\underline{a}$ associe $\underline{a}^{(m)}$ est un homomorphisme de l'anneau $W(R)$ sur $W_m(R)$.

On voit que $W(R)$ s'identifie à la limite projective des $W_m(R)$, ce qui permet de considérer $W(R)$ comme un anneau commutatif linéairement topologisé, séparé et complet.

Soit k un anneau commutatif et soit R un k-anneau. L'application canonique de $W(k)$ dans $W(R)$ munit $W(R)$ d'une structure de W(k)-anneau. Pour tout entier $m \geq 1$, l'application canonique composée $W(k) \to W_m(k) \to W_m(R)$ munit $W_m(R)$ d'une structure de W(k)-anneau. On voit que $W(R)$ s'identifie encore à $\varprojlim W_m(R)$, en tant que W(k)-anneau. En particulier, $W(R)$ peut être considéré comme un W(k)-anneau linéairement topologisé, séparé et complet.

1.3. Pour tout anneau commutatif R, et pour tout $x \in R$, notons $[x]$ l'élément de $W(R)$ défini par $[x] = (x,0,\dots,0,\dots)$. On appelle $[x]$ le <u>représentant multiplicatif</u> ou le <u>représentant de Teichmüller</u> de x dans $W(R)$. Il résulte de la définition des polynômes P_n que l'application $x \mapsto [x]$ est multiplicative (i.e., on a $[x][y] = [xy]$, si $x,y \in R$). On voit aussi que, si $x \in R$ et si $\underline{a} = (a_0,\dots,a_n,\dots) \in W(R)$, on a $[x]\underline{a} = (xa_0,x^pa_1,\dots,x^{p^n}a_n,\dots)$.

Soit alors k un anneau commutatif parfait de caractéristique p. Soit σ le Frobenius absolu sur k et sur $W(k)$ (on a donc $\sigma x = x^p$ si $x \in k$, et $\sigma\underline{a} = (a_0^p,a_1^p,\dots,a_n^p,\dots)$ si $\underline{a} = (a_0,a_1,\dots,a_n,\dots) \in W(k)$. On voit facilement que, dans $W(k)$, $p = (0,1,0,\dots,0,\dots)$, que

$W_m(k) = W(k)/p^m W(k)$ et que, si $\underline{a} = (a_0, a_1, \ldots, a_n, \ldots) \in W(k)$, on a $\underline{a} = \sum_{n=0}^{\infty} p^n[\sigma^{-n}(a_n)] = \sum_{n=0}^{\infty} p^n \sigma^{-n}([a_n])$. Dans le cas particulier où k est un corps, $W(k)$ est un anneau de valuation discrète, complet, de caractéristique 0 , de corps résiduel $W_1(k) = k$, aboslument non ramifié (i.e. p engendre l'idéal maximal de $W(k)$).

Soit maintenant A un anneau linéairement topologisé, séparé et complet, et soit Ω_A l'ensemble de ses idéaux ouverts. Pour tout entier m , $W_m(A)$ s'identifie à $\varprojlim_{\mathfrak{a} \in \Omega_A} W_m(A/\mathfrak{a})$, ce qui permet de considérer les $W_m(A)$ et $W(A) = \varprojlim W_m(A)$ comme des anneaux linéairement topologisés, séparés et complets.

Ceci s'applique en particulier au cas où $A = W(k) = \varprojlim W_m(k)$, avec k anneau parfait de caractéristique p . On vérifie alors facilement que l'application qui à $[x]$ (représentant multiplicatif, dans $W(k)$, de $x \in k$) associe $[[x]]$ (représentant multiplicatif, dans $W(W(k))$, de $[x] \in W(k)$) se prolonge de manière unique en un homomorphisme continu de la structure d'anneau de $W(k)$ dans $W(W(k))$: si $\underline{x} \in W(k)$, on voit que son image dans $W(W(k))$ est $(\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_n, \ldots)$ où les $\underline{x}_n$ se calculent par récurrence au moyen de la formule $\sigma^n(\underline{x}) = \underline{x}_0^{p^n} + p\underline{x}_1^{p^{n-1}} + \ldots + p^n \underline{x}_n$.

En particulier, si R est un $W(k)$-anneau, on peut considérer $W(R)$ et les $W_m(R)$ comme des $W(k)$-anneaux. On voit que $W(R)$ s'identifie encore à la limite projective des $W_m(R)$, en tant que $W(k)$-anneau. Si $x \in k$ et si $\underline{a} = (a_0, a_1, \ldots, a_n, \ldots) \in W(R)$, on voit que $[x]\underline{a} = ([x]a_0, \ldots, [\sigma^n(x)]a_n, \ldots)$; on a des formules analogues pour les $W_m(R)$. Si on suppose R séparé et complet pour la topologie p-adique, on voit qu'il en est de même des $W_m(R)$ et de $W(R)$.

Dans le cas particulier où R est un k-anneau, on peut aussi le considérer comme un $W(k)$-anneau et on voit que les deux structures de $W(k)$-anneau définies sur $W(R)$ coïncident.

1.4. Le morphisme de schémas affines $V_m : W_m \to W_{m+1}$, qui à $(a_0, a_1, \ldots, a_{m-1}) \in W_m(R)$ associe $(0, a_0, a_1, \ldots, a_{m-1}) \in W_{m+1}(R)$, est compatible avec l'addition. Par passage à la limite, on définit ainsi un $\mathbb{Z}$-foncteur en groupes $CW^u = \varinjlim W_m$ que nous appelons <u>le groupe des covecteurs de</u>

Witt unipotents.

On voit que, pour tout anneau commutatif R, un élément $\underline{a} \in CW^u(R)$ peut se représenter comme un "covecteur unipotent" :

$$\underline{a} = (a_{-n})_{n\in\mathbb{N}} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$$

où les $a_{-n} \in R$ et sont presque tous (i.e. tous sauf un nombre fini) nuls. La somme de deux covecteurs $\underline{a} = (\ldots, a_{-n}, \ldots, a_0)$ et $\underline{b} = (\ldots, b_{-n}, \ldots, b_0)$ de $CW^u(R)$ est le covecteur $\underline{c} = (\ldots, c_{-n}, \ldots, c_0)$ où

$$c_{-n} = S_m(a_{-m-n}, \ldots, a_{-n-1}, a_{-n} ; b_{-m-n}, \ldots, b_{-n-1}, b_{-n}) ,$$

pour m suffisamment grand.

1.5. Nous allons maintenant définir un $\mathbb{Z}$-foncteur en groupes que nous appellerons le groupe CW des covecteurs de Witt et qui contiendra CW^u comme sous-foncteur en groupes.

En tant que $\mathbb{Z}$-foncteur, pour tout anneau commutatif R, $CW(R)$ est formé de l'ensemble des "covecteurs" $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$, avec les $a_{-n} \in R$, vérifiant

(Ψ) $\begin{cases} \text{\underline{il existe un entier } } r \geq 0 \text{ \underline{tel que l'idéal de} } R \text{ \underline{engendré par les} } a_{-n}, \\ \text{\underline{pour} } n \geq r \text{ , \underline{est nilpotent}.} \end{cases}$

Si $\varphi : R \to S$ est un homomorphisme d'anneaux, l'application $CW(\varphi)$ est définie de manière évidente, composante par composante.

Si r et s sont des entiers ≥ 0, notons, pour tout anneau commutatif R, $CW_{r,s}(R)$ l'ensemble des $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$, avec les $a_{-n} \in R$, vérifiant

$(\Psi_{r,s})$ $\begin{cases} \text{\underline{la puissance} } s\text{-\underline{ième de l'idéal engendré par les} } a_{-n} \text{ , \underline{pour} } n \geq r \text{ ,} \\ \text{\underline{est nulle}.} \end{cases}$

On voit que $CW_{r,s}$, qui est un schéma affine, est un sous-$\mathbb{Z}$-foncteur de CW et que CW est la réunion des $CW_{r,s}$.

Pour définir la loi de groupe sur CW, nous aurons besoin de la proposition suivante :

PROPOSITION 1.1. - *Soit* R *un anneau commutatif et soit* $\underline{a} = (\ldots, a_{-n}, \ldots, a_0)$ *et* $\underline{b} = (\ldots, b_{-n}, \ldots, b_0)$ *des éléments de* CW(R) . *Alors*

i) *pour tout entier* $n \geq 0$, *la suite des*

$S_m(a_{-n-m}, \ldots, a_{-n-1}, a_{-n} ; b_{-n-m}, \ldots, b_{-n-1}, b_{-n})$ *est stationnaire* ;

ii) *pour tout* $n \in \mathbb{N}$, *soit* s_{-n} *la limite de la suite précédente* ; *l'élément* $\underline{s} = (\ldots, s_{-n}, \ldots, s_0) \in CW(R)$ (*i.e. les* s_{-n} *vérifient la condition* (Ψ)).

Commençons par démontrer deux lemmes :

LEMME 1.2. - *Soit* t *un entier* ≥ 0 *et soit* $w_0, w_1, \ldots, w_t$ *des entiers* ≥ 0 *tels que* $w_0 \neq 0$ *et* $w_0 + pw_1 + \ldots + p^t w_t$ *est divisible par* p^{t+1} . *Alors* $w_0 + w_1 + \ldots + w_t \geq t(p-1) + p$.

La démonstration se fait par récurrence sur t :

- c'est clair si $t = 0$;
- si $t \geq 1$, on voit que w_0 doit être divisible par p et s'écrit donc $w_0 = vp$, avec v entier ≥ 1 . Posons $w'_0 = v + w_1$ et $w'_i = w_{i+1}$ pour $1 \leq i \leq t-1$. Alors $w'_0 \neq 0$ et $w'_0 + pw'_1 + \ldots + p^{t-1} w'_{t-1}$ est divisible par p^t . L'hypothèse de récurrence implique que $w'_0 + w'_1 + \ldots + w'_{t-1} \geq (t-1)(p-1) + p$, ou $v + w_1 + \ldots + w_t \geq (t-1)(p-1) + p$ donc $w_0 + w_1 + \ldots + w_t \geq (t-1)(p-1) + p + v(p-1) \geq t(p-1) + p$.

LEMME 1.3. - *Pour tout entier* $r \geq 0$, *soit* $\mathfrak{b}_r$ *l'idéal de l'anneau des polynômes* $\mathbb{Z}[(X_{-n})_{n\in\mathbb{N}}, (Y_{-n})_{n\in\mathbb{N}}]$ *engendré par les* X_{-n} *et les* Y_{-n} , *avec* $n \geq r$. *Soit* r *et* s *des entiers* ≥ 1 . *Alors*

$$S_m(X_{-m}, \ldots, X_0 ; Y_{-m}, \ldots, Y_0) \equiv S_{m+1}(X_{-m-1}, X_{-m}, \ldots, X_0 ; Y_{-m-1}, Y_{-m}, \ldots, Y_0) \pmod{\mathfrak{b}_r^s}$$

pour tout entier $m \geq \begin{cases} r-1 & \text{si } s < p , \\ r-1+(s-p)/(p-1) & \text{si } s \geq p . \end{cases}$

Démonstration : observons qu'il résulte de la définition des polynômes S_n que, si l'on donne aux variables X_i et Y_i le poids p^i , le polynôme $S_n(X_0, X_1, \ldots, X_n ; Y_0, Y_1, \ldots, Y_n)$ est isobare de poids p^n ; et que $S_{m+1}(0, X_0, \ldots, X_m ; 0, Y_0, \ldots, Y_m) = S_m(X_0, X_1, \ldots, X_m ; Y_0, Y_1, \ldots, Y_m)$.

On en déduit que $T_m = S_{m+1}(X_{-m-1}, \ldots, Y_0) - S_m(X_{-m}, \ldots, Y_0)$ s'écrit comme combinaison linéaire à coefficients entiers rationnels de termes de la forme

$$X_{-m-1}^{u_0} Y_{-m-1}^{v_0} X_{-m}^{u_1} Y_{-m}^{v_1} \ldots X_0^{u_{m+1}} Y_0^{v_{m+1}} ,$$

où les u_i et les v_i sont des entiers ≥ 0 et où, si l'on pose

$w_i = u_i + v_i$, on a $w_0 \neq 0$ et $w_0 + pw_1 + \ldots + p^{m+1}w_{m+1} = p^{m+1}$.

En particulier, pour tout entier t vérifiant $0 \leq t \leq m$, $w_0 + pw_1 + \ldots + p^t w_t$ est divisible par p^{t+1} et le lemme 1.2 implique que $w_0 + w_1 + \ldots + w_t \geq t(p-1) + p$, donc que $T_m \in \mathfrak{b}_{m+1-t}^{t(p-1)+p}$.

Pour $t = 0$, on voit que $T_m \in \mathfrak{b}_{m+1}^{p}$, ce qui démontre le lemme, pour $s < p$.

Si $s \geq p$, et si $m \geq r - 1 + (s-p)/(p-1)$, posons $t = m + 1 - r$. On a $0 \leq t \leq m$ et $T_m \in \mathfrak{b}_r^{t(p-1)+p} \subset \mathfrak{b}_r^s$ car $t(p-1) + p \geq s$.

<u>Démonstration de la proposition 1.1</u> : soit r' et s' (resp. r'' et s'') des entiers tels que $\underline{a} \in CW_{r',s'}(R)$ (resp. $b \in CW_{r'',s''}(R)$). Posons $r = \max\{1,r',r''\}$ et $s = \max\{p,s'+s''\}$. On voit que l'idéal engendré par les a_{-n} et les b_{-n} , avec $n \geq r$, a sa puissance s-ième nulle. Il résulte du lemme précédent que, quel que soit l'entier $n \geq 0$, pour tout $m \geq r - 1 + (s-p)/(p-1)$, on a

$$S_m(a_{-m-n},\ldots,a_{-n};b_{-m-n},\ldots,b_{-n}) = S_{m+1}(a_{-m-n-1},\ldots,a_{-n};b_{-m-n-1},\ldots,b_{-n}) ,$$

d'où l'assertion (i).

La deuxième assertion est évidente. Plus précisément, on voit que si $\underline{a} \in CW_{r',s'}(R)$ et $\underline{b} \in CW_{r'',s''}(R)$, alors $\underline{s} \in CW_{\max\{r',r''\},s'+s''}(R)$.

La proposition 1.1 donne un sens à l'énoncé suivant :

PROPOSITION 1.4.- <u>Soit</u> R <u>un anneau commutatif. Si</u> $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ <u>et</u> $\underline{b} = (\ldots,b_{-n},\ldots,b_0) \in CW(R)$, <u>posons</u> $\underline{a} + \underline{b} = \underline{s} = (\ldots,s_{-n},\ldots,s_0)$ <u>avec</u>

(2) $\quad s_{-n} = \lim_{m\to\infty} S_m(a_{-n-m},\ldots,a_{-n-1},a_{-n} ; b_{-n-m},\ldots,b_{-n-1},b_{-n})$.

<u>La loi</u> + <u>est une loi de groupe abélien sur</u> CW(R) .

<u>Démonstration</u> : la commutativité et l'existence d'un élément-neutre $0 = (\ldots,0,\ldots,0,0)$ sont évidentes. Montrons que si $\underline{a}$, $\underline{b}$, $\underline{c} \in CW(R)$, $\underline{a} + (\underline{b}+\underline{c}) = (\underline{a}+\underline{b}) + \underline{c}$. Pour $i = 1,2,3$, soit r_i et s_i des entiers tels que $\underline{a} \in CW_{r_1,s_1}(R)$, $\underline{b} \in CW_{r_2,s_2}(R)$, $\underline{c} \in CW_{r_3,s_3}(R)$. Posons $r = \max\{1,r_1,r_2,r_3\}$ et $s = \max\{p,s_1+s_2+s_3\}$ et soit m un entier vérifiant $m \geq r-1 + (s-p)/(p-1)$. Comme $\underline{a} + \underline{b} \in CW_{r_1+r_2,s_1+s_2}(R)$ et

$\underline{b} + \underline{c} \in CW_{r_2+r_3, s_2+s_3}(R)$, on voit tout de suite, en appliquant le lemme 1.3, que les composantes d'indice $-n$ de $\underline{a} + (\underline{b}+\underline{c})$ et de $(\underline{a}+\underline{b}) + \underline{c}$ ne dépendent que des a_{-i} , b_{-i} , c_{-i} avec $i < n+m$. On peut pour les calculer remplacer les a_{-i} , b_{-i} , c_{-i} pour $i \geq n+m$ par 0 . Elles sont donc égales, d'après l'associativité dans $CW^u(R)$.

L'existence d'un inverse se démontre de manière analogue.

Il est clair que si $\varphi : R \to S$ est un homomorphisme d'anneaux commutatifs, l'application $CW(\varphi) : CW(R) \to CW(S)$ est un homomorphisme de groupes. On a donc bien muni CW d'une structure de $\mathbb{Z}$-foncteur en groupes.

1.6. Pour tout anneau commutatif R , notons $\mathfrak{N}_R$ l'ensemble des idéaux nilpotents de R . Pour tout $\mathfrak{n} \in \mathfrak{N}_R$ et tout entier $r \geq 0$, soit $CW(R,\mathfrak{n},r)$ le sous-groupe de $CW(R)$ formé des éléments $\underline{a} = (\dots, a_{-n}, \dots, a_0)$ tels que $a_{-n} \in \mathfrak{n}$ si $n \geq r$. On voit que $CW(R,\mathfrak{n},r)$ s'identifie à l'ensemble des applications de $\{0,-1,\dots,-n,\dots\}$ dans R qui sont telles que l'image de $-n$ appartient à $\mathfrak{n}$ si $n \geq r$. On munit cet espace de la topologie de la convergence simple. Autrement dit, lorsque l'on identifie, de manière évidente, $CW(R,\mathfrak{n},r)$ à $R^r \times \mathfrak{n}^{\mathbb{N}}$, on obtient la topologie du produit direct (chaque facteur étant muni de la topologie discrète).

On voit immédiatement que $CW(R,\mathfrak{n},r)$ devient ainsi un groupe topologique.

Le groupe $CW(R)$ s'identifie à la limite inductive des $CW(R,\mathfrak{n},r)$, pour $\mathfrak{n} \in \mathfrak{N}_R$ et $r \in \mathbb{N}$. On appelle <u>topologie naturelle</u> de $CW(R)$ la topologie de la limite inductive.

Il est immédiat que $CW(R)$ est séparé et complet pour cette topologie et que $CW^u(R)$ est un sous-groupe dense de $CW(R)$.

Enfin, il est clair que si $\varphi : R \to S$ est un homomorphisme d'anneaux commutatifs, l'application $CW(\varphi)$ est continue ; autrement dit, on peut considérer CW comme un foncteur covariant de la catégorie des anneaux commutatifs dans celle des groupes topologiques.

<u>Remarque</u> : pour tout $\mathfrak{n} \in \mathfrak{N}_R$, soit $CW(R,\mathfrak{n}) = \varinjlim_{r \in \mathbb{N}} CW(R,\mathfrak{n},r)$. C'est le sous-groupe de $CW(R)$ formé des éléments dont les composantes sont presque

toutes dans $\mathfrak{n}$. On voit que la topologie du sous-groupe $CW(R,\mathfrak{n})$ est celle du produit direct restreint (cf. par exemple [34], p. 138) $R^{\mathbb{N}}$ relativement à $\mathfrak{n}$ pour chaque composante.

Pour tout entier $s \geq 0$, soit $U(R,\mathfrak{n},s)$ l'ensemble des $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0)$ tels que $a_{-n} \in \mathfrak{n}$, pour tout n , et $a_{-n} \in \mathfrak{n}^{p^{s-n}}$, si $n \leq s$. Il est clair que les $U(R,\mathfrak{n},s)$, pour $s \in \mathbb{N}$, forment un système fondamental de voisinages ouverts de 0 dans $CW(R,\mathfrak{n})$. En utilisant le caractère isobare des polynômes qui définissent l'addition dans les vecteurs de Witt (cf. n° 1.5), on voit que les $U(R,\mathfrak{n},s)$ sont des sous-groupes. Le groupe $CW(R,\mathfrak{n})$ admet donc un système fondamental de voisinages ouverts de 0 formé de sous-groupes.

1.7. Comme tout $\mathbb{Z}$-foncteur en groupes, CW s'étend, de manière évidente à la catégorie des anneaux commutatifs, linéairement topologisés, séparés et complets : si R est un tel anneau, on pose $CW(R) = \varprojlim_{\mathfrak{a}\in\Omega_R} CW(R/\mathfrak{a})$ (où Ω_R désigne l'ensemble des idéaux ouverts de R). Les éléments de $CW(R)$ peuvent encore se représenter comme des covecteurs $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0)$, avec les $a_{-n} \in R$, vérifiant

(Ψ_t) $\left\{\right.$ <u>pour tout idéal ouvert</u> $\mathfrak{a}$ <u>de</u> R , <u>il existe des entiers</u> r <u>et</u> s <u>tels que la puissance</u> s-<u>ième de l'idéal de</u> R <u>engendré par les</u> a_{-n} , <u>avec</u> $n \geq r$, <u>est contenue dans</u> $\mathfrak{a}$.

On évitera, bien sûr, de confondre $CW(R)$ avec $CW(R_{dis})$, où R_{dis} désigne l'anneau (sans topologie) sous-jacent à l'anneau topologique R : l'inclusion évidente $CW(R_{dis}) \subset CW(R)$ est, en général, stricte (sauf si la topologie de R est la topologie discrète !).

<u>Remarque</u> : soit R un anneau commutatif, linéairement topologisé, séparé et complet. Dans la suite, nous notons encore $CW^u(R)$ le groupe $\varinjlim W_m$ formé des covecteurs dont presque toutes les composantes sont nulles. On prendra garde que l'inclusion de $CW^u(R)$ dans $\varprojlim_{\mathfrak{a}\in\Omega_R} CW^u(R/\mathfrak{a})$ est, en général, stricte. Toutefois $CW^u(R)$ est encore un sous-groupe dense de $CW(R)$.

§ 2.- Endomorphismes.

Dans tout ce paragraphe, on désigne par k un corps parfait de caractéristique p. On pose $A = W(k)$ et on suppose A muni de la topologie p-adique. On désigne par σ le Frobenius absolu sur k et sur A.

2.1. Par restriction à la catégorie des k-anneaux, CW (resp. CW^u) définit un k-foncteur en groupes CW_k (resp. CW_k^u). Ici encore, pour tout k-anneau R, le groupe topologique $CW_k(R)$ est le séparé complété de $CW_k^u(R)$ pour la topologie naturelle.

Soit R un k-anneau et soit m un entier ≥ 1. On sait (cf. n° 1.2) que $W_m(R)$ a une structure naturelle de A-anneau : si $\underline{x} = (x_0, x_1, \ldots, x_n, \ldots) \in W(k) = A$ et si $\underline{a} = (a_0, a_1, \ldots, a_{m-1}) \in W_m(R)$, on voit que $\underline{x}\,\underline{a} = (b_0, b_1, \ldots, b_{m-1})$, avec $b_i = P_i(x_0, x_1, \ldots, x_i\,;\, a_0, a_1, \ldots, a_i)$.

En particulier, on voit que, si $\underline{a} = (a_0, \ldots, a_{m-1}) \in W_m(R)$, on a

(1) $\quad [x]\underline{a} = (xa_0, \sigma(x)a_1, \ldots, \sigma^{m-1}(x)a_{m-1})$, pour $x \in k$,

(2) $\quad p\underline{a} = (0, a_0^p, a_1^p, \ldots, a_{m-1}^p)$,

(3) $\quad p^m\underline{a} = 0$.

En particulier, on déduit de (1) que si $x \in k$ et si $\underline{a} = (a_0, a_1, \ldots, a_{m-1}) \in W_m(R)$, on a

$$V_m([x]\underline{a}) = (0, xa_0, \ldots, \sigma^{m-1}(x)a_{m-1}) = \sigma^{-1}([x])V_m(a) .$$

Comme les $[x]$, pour $x \in k$, engendrent un sous-groupe dense de A et comme, d'après (3), $W_m(R)$ est tué par p^m, on en déduit que, pour tout $\underline{x} \in A$ et tout $\underline{a} \in W_m(R)$, on a $V_m(\underline{x}\,\underline{a}) = \sigma^{-1}(\underline{x})V_m(\underline{a})$.

Pour tout entier $m \geq 1$, l'application de $A \times W_m(R)$ qui à $(\underline{x}, \underline{a})$ associe $\sigma^{1-m}(\underline{x})\underline{a}$ munit le groupe additif de $W_m(R)$ d'une structure de A-module. Ces structures sont maintenant compatibles avec les V_m et, par passage à la limite, on en déduit une structure de A-module sur $CW^u(R)$. Comme $W_m(R)$ est tué par p^m, on voit que $CW^u(R)$ est un A-module de torsion. On déduit immédiatement de la définition que, pour tout $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW^u(R)$, on a les formules suivantes :

(4) $\quad$ si $\underline{x} = (x_0, x_1, \ldots, x_n, \ldots) \in A = W(k)$, on a $\underline{x}\,\underline{a} = (\ldots, b_{-n}, \ldots, b_0)$ avec

$b_{-n} = P_m(\sigma^{-n-m}(x_0), \sigma^{-n-m}(x_1), \dots, \sigma^{-n-m}(x_m); a_{-n-m}, \dots, a_{-n-1}, a_{-n})$, si m est tel que $a_{-i} = 0$, pour $i > n+m$;

(5) si $x \in k$, $[x]\underline{a} = (\dots, \sigma^{-n}(x)a_{-n}, \dots, \sigma^{-1}(x)a_{-1}, xa_0)$;

(6) on a $p\underline{a} = (\dots, a^p_{-n-1}, \dots, a^p_{-2}, a^p_{-1})$.

Nous allons voir que A opère continûment sur $CW^u(R)$ muni de la topologie naturelle, ce qui va nous permettre de munir $CW(R)$ d'une structure de A-module topologique. Pour cela, commençons par établir un lemme :

LEMME 2.1.- Pour tout entier $r \geq 0$, soit $\mathfrak{d}_r$ l'idéal de l'anneau des polynômes $k[(Y_{-n})_{n\in\mathbb{N}}]$ engendré par les Y_{-n} , avec $n \geq r$. Soit r et s des entiers ≥ 1 . Alors, pour tout $\underline{x} = (x_0, x_1, \dots, x_n, \dots) \in A$, on a

$$P_m(\sigma^{-m}(x_0), \dots, \sigma^{-m}(x_m); Y_{-m}, \dots, Y_0)$$
$$\equiv P_{m+1}(\sigma^{-m-1}(x_0), \dots, \sigma^{-m-1}(x_{m+1}); Y_{-m-1}, \dots, Y_{-1}, Y_0) \pmod{\mathfrak{d}_r^s}$$

pour tout entier $m \geq \begin{cases} r-1 & \text{si } s < p \\ r-1+(s-p)/(p-1) & \text{si } s \geq p \end{cases}$.

Démonstration : soit $R = k[(Y_{-n})_{n\in\mathbb{N}}]$. Il résulte de la formule (4) appliquée au covecteur $(0, \dots, 0, Y_{-m}, Y_{-m+1}, \dots, Y_0) \in CW^u(R)$ que

$$P_m(\sigma^{-m}(x_0), \dots, \sigma^{-m}(x_m); Y_{-m}, \dots, Y_0)$$
$$= P_{m+1}(\sigma^{-m-1}(x_0), \dots, \sigma^{-m-1}(x_{m+1}); 0, Y_{-m}, \dots, Y_0) .$$

On voit facilement sur la définition des P_i que, si l'on donne aux variables Y_{-i} le poids p^{m+1-i} les deux polynômes qui interviennent dans l'énoncé du lemme sont isobares de poids p^{m+1} . On déduit donc de l'égalité précédente qu'ils diffèrent par des combinaisons linéaires de monômes de la forme $Y_{-m-1}^{w_0} Y_{-m}^{w_1} \dots Y_{-1}^{w_m} Y_0^{w_{m+1}}$, où les w_i sont des entiers ≥ 0 , vérifiant $w_0 \neq 0$ et $w_0 + pw_1 + \dots + p^{m+1}w_{m+1} = p^{m+1}$. La démonstration du lemme se termine alors comme celle du lemme 1.3.

PROPOSITION 2.2.- Soit R un k-anneau.

i) Soit $\underline{x} = (x_0, x_1, \dots, x_n, \dots) \in A$ et soit $\underline{a} = (\dots, a_{-n}, \dots, a_0) \in CW(R)$. Pour tout entier $n \geq 0$, la suite des $P_m(\sigma^{-n-m}(x_0), \dots, \sigma^{-n-m}(x_m); a_{-m-n}, \dots, a_{-n})$ est stationnaire.

ii) Soit b_{-n} la limite de la suite ci-dessus. On a

$\underline{b} = (\ldots, b_{-n}, \ldots, b_{-1}, b_0) \in CW(R)$.

iii) L'application de $A \times CW(R)$ qui à $(\underline{x}, \underline{a})$ associe $\underline{x}\,\underline{a} = \underline{b}$ munit le groupe topologique $CW(R)$ d'une structure de A-module topologique, de torsion, séparé et complet et $CW^u(R)$ en est un sous-A-module dense.

iv) Les formules (5) et (6) restent valables pour tout $\underline{a} \in CW(R)$.

Démonstration : on sait (cf. n° 1.6) que $CW(R)$ est réunion de ses sous-groupes $CW(R, \mathfrak{n}, r)$, pour $\mathfrak{n}$ parcourant l'ensemble des idéaux nilpotents de R et r l'ensemble des entiers ≥ 0 .

Il résulte du lemme 2.1 que si $\underline{a} \in CW(R, \mathfrak{n}, r)$, et si s est un entier $\geq p$ tel que $\mathfrak{n}^s = 0$, on a, pour tout $\underline{x} = (x_0, \ldots, x_n, \ldots) \in A$, $P_m(\sigma^{-n-m}(x_0), \ldots, a_{-n}) = P_{m+1}(\sigma^{-n-m-1}(x_0), \ldots, a_{-n})$ si $m \geq r-1+(s-p)/(p-1)$, d'où i) ; on voit aussi que $b_{-n} \in \mathfrak{n}$ si $n \geq r$, donc que $\underline{b} \in CW(R, \mathfrak{n}, r)$, d'où, a fortiori, ii) ; on a donc en fait, par restriction, une application de $A \times CW(R, \mathfrak{n}, r)$ dans $CW(R, \mathfrak{n}, r)$. La continuité de cette restriction est maintenant triviale, d'où la continuité de l'application de $A \times CW(R)$ dans $CW(R)$ puisque la topologie de $CW(R)$ est celle de la limite inductive des $CW(R, \mathfrak{n}, r)$.

Compte-tenu de ce que la restriction de $A \times CW(R) \to CW(R)$ à $A \times CW^u(R)$ n'est autre que l'application qui définie la structure de A-module déjà considérée sur $CW^u(R)$, les autres assertions de la proposition sont triviales.

2.2. Soit R un k-anneau. Pour tout $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW(R)$, posons

(7) $\underline{F}\underline{a} = (\ldots, a_{-n}^p, \ldots, a_{-1}^p, a_0^p)$ et $\underline{V}\underline{a} = (\ldots, a_{-n-1}, \ldots, a_{-2}, a_{-1})$.

On vérifie immédiatement que les applications $\underline{F}$ et $\underline{V}$ sont des endomorphismes continus du groupe $CW(R)$ et que, si $\underline{a} \in CW(R)$ et $\underline{x} \in A$,

$$\underline{F}(\underline{x}\,\underline{a}) = \sigma(\underline{x})\underline{F}\underline{a} ,$$
$$\underline{x}\,\underline{V}\underline{a} = \underline{V}(\sigma(\underline{x})\underline{a}) ,$$
$$\underline{F}(\underline{V}\underline{a}) = \underline{V}(\underline{F}\underline{a}) = p\underline{a} .$$

Notons alors D_k l'anneau de Dieudonné de k , i.e. l'anneau (non commutatif si $k \neq \mathbb{F}_p$) engendré par A et deux éléments $\underline{F}$ et $\underline{V}$ soumis aux relations

$$(8)\quad \begin{cases} \underline{F}\underline{x} = \sigma(\underline{x})\underline{F} \ , & \text{pour tout} \quad \underline{x} \in A \ , \\ \underline{x}\underline{V} = \underline{V}\sigma(\underline{x}) \ , & \text{pour tout} \quad \underline{x} \in A \ , \\ \underline{V}\,\underline{F} = \underline{F}\,\underline{V} = p \ . \end{cases}$$

Si l'on munit l'anneau D_k de la topologie p-adique, on voit que l'action de A définie par la proposition 2.2 et les formules (7) munissent $CW(R)$ d'une structure de D_k-module topologique.

Il est clair que la structure de D_k-module à gauche qui vient d'être définie sur chaque $CW_k(R)$ est fonctorielle en R . Elle définit donc un homomorphisme de l'anneau D_k dans l'anneau $End(CW_k)$ des endomorphismes (dans la catégorie des k-foncteurs en groupes) de CW_k . On vérifie facilement que cet homomorphisme est injectif. Dans la suite, nous utilisons cet homomorphisme pour identifier D_k à un sous-anneau de $End(CW_k)$.

Remarques :

1.- Si on note $\hat{D}_k = \varprojlim D_k/p^m D_k$ le séparé complété de D_k pour la topologie p-adique, on voit que la structure de D_k-module à gauche sur $CW_k(R)$ se prolonge en une structure de $\hat{D}_k$-module topologique séparé et complet, et qu'en particulier $\hat{D}_k$ s'identifie à un sous-anneau de $End(CW_k)$.

2.- Si R est un k-anneau linéairement topologisé, séparé et complet, on voit que $CW_k(R) = \varprojlim_{\mathfrak{a}\in\Omega_R} CW_k(R/\mathfrak{a})$ peut aussi être muni d'une structure de D_k-module topologique, séparé et complet, limite projective des D_k-modules $CW_k(R/\mathfrak{a})$. Si l'on représente les éléments de $CW_k(R)$ comme des covecteurs, on voit que les formules (5), (6) et (7) sont encore valables et que

(4') si $x = (x_0, x_1, \dots, x_n, \dots) \in A$ et $\underline{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0) \in CW_k(R)$, on a $\underline{x}\underline{a} = (\dots, b_{-n}, \dots, b_{-1}, b_0)$ avec
$$b_{-n} = \lim_{m\to+\infty} P_m(\sigma^{-n-m}(x_0), \sigma^{-n-m}(x_1), \dots, \sigma^{-n-m}(x_m) ; a_{-n-m}, \dots, a_{-n-1}, a_{-n}) \ .$$

3.- Le plongement canonique de D_k dans $End(CW_k)$ donné ici n'est pas le seul possible. Soit en effet τ un automorphisme du corps k . Par fonctorialité, il se relève de manière unique en un automorphisme de $A = W(k)$; celui-ci se prolonge en un automorphisme de D_k , encore noté τ en posant $\tau(\underline{F}) = \underline{F}$ et $\tau(\underline{V}) = \underline{V}$. Si on compose le plongement construit ici avec τ on obtient un autre plongement de D_k dans $End(CW_k)$.

2.3. Soit k' un corps parfait contenant k. Il est clair que $CW_k(k') = CW^u_k(k') = CW_{k'}(k')$ est muni de la topologie discrète. Soit $A' = W(k')$ et soit K' le corps des fractions de A'. Tout élément de K' s'écrit d'une manière et d'une seule sous la forme $\underline{a} = \sum_{n \gg -\infty}^{+\infty} p^n \sigma^{-n}([a_n])$, avec les $a_n \in k'$; on voit que l'application qui à $\underline{a} \in K'$ associe le covecteur $(\ldots, a_{-n}, \ldots, a_{-1}, a_0)$ est A-linéaire continue, surjective et que son noyau est pA'. Le A-module K'/pA' s'identifie donc à $CW_k(k')$. Par transport de structure, on en déduit une structure de D_k-module à gauche sur K'/pA' ; on voit que l'action de $\underline{F}$ et $\underline{V}$ est donnée par $\underline{F}\underline{a} = \sigma(\underline{a})$, $\underline{V}\underline{a} = p\sigma^{-1}(\underline{a})$, pour tout $\underline{a} \in K'/pA'$. Comme la division par p définit un isomorphisme de K'/pA' sur K'/A', on peut dire aussi que $CW_k(k')$ est isomorphe à K'/A'.

2.4. Notons CW_A la restriction de CW, considéré comme foncteur sur la catégorie des anneaux commutatifs linéairement topologisés, séparés et complets, à la catégorie des A-anneaux de ce type.

Nous nous proposons de montrer que l'on peut identifier le sous-anneau $A[\underline{V}]$ de D_k à un sous-anneau de l'anneau $\mathrm{End}(CW_A)$ des endomorphismes du foncteur en groupes topologiques CW_A.

Soit R un A-anneau linéairement topologisé, séparé et complet. On sait (cf. n° 1.3) que le plongement canonique de $A = W(k)$ dans $W(A) = W(W(k))$ est continu et nous permet de considérer les anneaux $W_m(R)$ comme des A-anneaux linéairement topologisés, séparés et complets ; en outre, si $x \in k$ et si $\underline{a} = (a_0, a_1, \ldots, a_{m-1}) \in W_m(R)$, on a

$$[x]\underline{a} = ([x]a_0, [\sigma(x)]a_1, \ldots, [\sigma^{m-1}(x)]a_{m-1}) \;;$$

on en déduit que

$$V_m([x]\underline{a}) = (0, [x]a_0, \ldots, [\sigma^{m-1}(x)]a_{m-1}) = \sigma^{-1}([x])V_m\underline{a} .$$

Comme les $[x]$, pour $x \in k$, engendrent un sous-groupe dense de A, on voit que, pour tout $\underline{x} \in A$ et tout $\underline{a} \in W_m(R)$, on a $V_m(\underline{x}\,\underline{a}) = \sigma^{-1}(\underline{x})V_m\underline{a}$.

Pour tout entier $m \geq 1$, l'application de $A \times W_m(R)$ dans $W_m(R)$ qui à $(\underline{x}, \underline{a})$ associe $\sigma^{1-m}(\underline{x})\underline{a}$ munit le groupe additif de $W_m(R)$ d'une structure de A-module topologique, séparé et complet. Ces structures sont maintenant compatibles avec les V_m et, par passage à la limite, on en déduit une structure de A-module topologique sur $CW^u(R)$.

On déduit immédiatement de la définition que, pour tout $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW^u(R)$, on a les formules suivantes :

(4") si $\underline{x} \in A$ et si $(\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_n, \ldots)$ désigne l'image de $\underline{x}$ dans $W(A)$, on a $\underline{x}\underline{a} = (\ldots, b_{-n}, \ldots, b_{-1}, b_0)$, avec $b_{-n} = P_m(\sigma^{-n-m}(\underline{x}_0), \ldots, \sigma^{-n-m}(\underline{x}_m) ; a_{-n-m}, \ldots, a_{-n})$ si m est un entier tel que $a_{-i} = 0$ si $i > n+m$;

(5") si $x \in k$, on a $[x]\underline{a} = (\ldots, \sigma^{-n}([x])a_{-n}, \ldots, \sigma^{-1}([x])a_{-1}, [x]a_0)$.

PROPOSITION 2.3.- <u>Soit</u> R <u>un A-anneau linéairement topologisé, séparé et complet. L'action de</u> A <u>sur</u> $CW^u(R)$ <u>définie ci-dessus est continue pour la topologie naturelle et se prolonge en une action de</u> A <u>sur</u> $CW(R)$ <u>qui munit</u> $CW(R)$ <u>d'une structure de A-module topologique, séparé et complet</u>.

<u>Si</u> $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW_A(R)$,

i) <u>on a</u> $[x]\underline{a} = (\ldots, \sigma^{-n}([x])a_{-n}, \ldots, \sigma^{-1}([x])a_{-1}, [x]a_0)$, <u>pour tout</u> $x \in k$;

ii) <u>si</u> $\underline{x} \in A$ <u>et si</u> $(\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_n, \ldots)$ <u>désigne l'image de</u> $\underline{x}$ <u>dans</u> $W(A)$, <u>on a</u> $\underline{x}\underline{a} = (\ldots, b_{-n}, \ldots, b_{-1}, b_0)$, <u>avec</u> $b_{-n} = \lim_{m \to +\infty} P_m(\sigma^{-n-m}(\underline{x}_0), \ldots, \sigma^{-n-m}(\underline{x}_m) ; a_{-n-m}, \ldots, a_{-1}, a_0)$.

<u>Démonstration</u> : il s'agit d'une généralisation de la proposition 2.2 (tout k-anneau, muni de la topologie discrète devient un A-anneau linéairement topologisé, séparé et complet) et la démonstration est analogue :

on commence par considérer le A-anneau profini $R = A[[(Y_{-n})_{n \in \mathbb{N}}]]$ des série formelles en les Y_{-n} . En appliquant la formule (4") à $(\ldots, 0, \ldots, 0, Y_{-m}, \ldots, Y_{-1}, Y_0) \in CW^u(R)$, on voit que, dans R ,

$$P_m(\sigma^{-m}(\underline{x}_0), \ldots, \sigma^{-m}(\underline{x}_m) ; Y_{-m}, \ldots, Y_0)$$
$$= P_{m+1}(\sigma^{-m-1}(\underline{x}_0), \ldots, \sigma^{-m-1}(\underline{x}_{m+1}) ; 0, Y_{-m}, \ldots, Y_0) .$$

Si l'on note encore $\mathfrak{d}_r$ l'idéal de R engendré par les Y_{-n} , avec $n \geq r$, le même raisonnement que celui fait pour prouver le lemme 2.1 montre que

$$P_m(\sigma^{-m}(\underline{x}_0), \ldots, \sigma^{-m}(\underline{x}_m) ; Y_{-m}, \ldots, Y_0)$$
$$\equiv P_{m+1}(\sigma^{-m-1}(\underline{x}_0), \ldots, \sigma^{-m-1}(\underline{x}_{m+1}) ; Y_{-m-1}, \ldots, Y_{-1}, Y_0) \pmod{\mathfrak{d}_r^s}$$

si m est un entier satisfaisant les inégalités indiquées dans ce lemme.

En utilisant cette congruence, on en déduit le résultat dans le cas où la topologie de R est la topologie discrète par le même raisonnement que celui fait pour prouver la proposition 2.2. Le cas général s'en déduit par passage à la limite.

2.5. Soit R un A-anneau, linéairement topologisé, séparé et complet. Pour tout $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_0) \in CW_A(R)$, posons

(7") $\underline{V}\underline{a} = (\dots,a_{-n-1},\dots,a_{-2},a_{-1})$.

Il est clair que $\underline{V}$ est un endomorphisme continu de $CW_A(R)$. On voit que l'action de A définie par la proposition 2.3 et celle de $\underline{V}$ qui vient d'être définie munissent $CW_A(R)$ d'une structure de $A[\underline{V}]$-module topologique (en désignant par $A[\underline{V}]$ le sous-anneau de D_k engendré par A et $\underline{V}$).

Il est clair que la structure de $A[\underline{V}]$-module à gauche qui vient d'être définie sur chaque $CW_A(R)$ est fonctorielle en R . Elle définit donc un homomorphisme de l'anneau $A[\underline{V}]$ dans l'anneau $\mathrm{End}(CW_A)$ du foncteur en groupes topologiques CW_A . Ici encore, on voit facilement que cet homomorphisme est injectif et nous l'utilisons pour identifier $A[\underline{V}]$ à un sous-anneau de $\mathrm{End}(CW_A)$.

§ 3.- Quelques séries formelles.

3.1. Soit S un anneau commutatif, que l'on suppose muni de la topologie discrète. Soit $\underline{X} = (X_0,X_{-1},\dots,X_{-n},\dots)$ une famille d'indéterminées indexée par les entiers ≤ 0 . Notons $S[\underline{X}]$ l'anneau des polynômes, à coefficients dans S , en les X_{-n} . On peut considérer $S[\underline{X}]$ comme un S-anneau topologique pour la topologie discrète.

Soit $S[[\underline{X}]]$ le S-anneau topologique des séries formelles en les X_{-n} . Si $\mathbb{I} = \mathbb{N}^{(-\mathbb{N})}$ est l'ensemble des $\underline{i} = (i_0,i_{-1},\dots,i_{-n},\dots)$, avec les $i_{-n} \in \mathbb{N}$, presque tous nuls, $S[[\underline{X}]]$ est un S-module, topologiquement libre, isomorphe à $S^{\mathbb{I}}$, avec une base topologique canonique, celle des $\underline{X}^{\underline{i}} = X_0^{i_0}X_{-1}^{i_{-1}}\dots X_{-n}^{i_{-n}}\dots$, pour $\underline{i} \in \mathbb{I}$. Tout élément de $S[[\underline{X}]]$ s'écrit, de manière unique, sous la forme

$$\sum_{\underline{i}\in\mathbb{I}} a_{\underline{i}}\underline{X}^{\underline{i}} \text{ , avec les } a_{\underline{i}} \in S \text{ , arbitraires.}$$

Pour tout entier $r \geq 0$, soit $\mathfrak{d}_r$ l'idéal de $S[\underline{X}]$ engendré par les X_{-n} , pour $n \geq r$. On voit que $S[[\underline{X}]]$ s'identifie au séparé complété de $S[\underline{X}]$ pour la topologie définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux de la forme $\mathfrak{d}_r + \mathfrak{d}_0^s$, pour r et s entiers ≥ 0 . En d'autres termes

$$S[[\underline{X}]] = \varprojlim S[\underline{X}]/(\mathfrak{d}_r + \mathfrak{d}_0^s) ,$$

et $S[\underline{X}]$ est un sous-anneau dense de $S[[\underline{X}]]$.

Considérons maintenant les trois S-anneaux topologiques suivant :

$$S^0[[\underline{X}]] = \varprojlim S[\underline{X}]/\mathfrak{d}_r^s ,$$

$$S^u[[\underline{X}]] = \varprojlim S[\underline{X}]/\mathfrak{d}_r ,$$

$$S^c[[\underline{X}]] = \varprojlim S[\underline{X}]/\mathfrak{d}_0^s .$$

On constate facilement qu'ils s'identifient à des sous-anneaux de $S[[\underline{X}]]$ contenant $S[\underline{X}]$: si, pour tout $\underline{i} = (i_0, i_{-1}, \dots, i_{-n}, \dots) \in \mathbb{I}$, et pour tout entier $r \geq 0$, on pose $|\underline{i}|_r = \sum_{n \geq r} i_{-n}$, on a :

$$S^0[[\underline{X}]] = \left\{ \sum_{\underline{i} \in \mathbb{I}} a_{\underline{i}} \underline{X}^{\underline{i}} \;\middle|\; \begin{array}{l} \text{pour tout } (r,s) \in \mathbb{N}^2 \text{, les } a_{\underline{i}} \text{, avec } |\underline{i}|_r < s \\ \text{sont presque tous nuls} \end{array} \right\} ,$$

$$S^u[[\underline{X}]] = \left\{ \sum_{\underline{i} \in \mathbb{I}} a_{\underline{i}} \underline{X}^{\underline{i}} \;\middle|\; \begin{array}{l} \text{pour tout } r \in \mathbb{N} \text{, les } a_{\underline{i}} \text{, avec } |\underline{i}|_r = 0 \text{,} \\ \text{sont presque tous nuls} \end{array} \right\} ,$$

$$S^c[[\underline{X}]] = \left\{ \sum_{\underline{i} \in \mathbb{I}} a_{\underline{i}} \underline{X}^{\underline{i}} \;\middle|\; \begin{array}{l} \text{pour tout } s \in \mathbb{N} \text{, les } a_{\underline{i}} \text{, avec } |\underline{i}|_0 < s \text{,} \\ \text{sont presque tous nuls} \end{array} \right\} .$$

On a un diagramme commutatif :

$$\begin{tikzcd} & & S^u[[\underline{X}]] \arrow[dr] & \\ S[\underline{X}] \arrow[r] & S^0[[\underline{X}]] \arrow[ur] \arrow[dr] & & S[[\underline{X}]] \\ & & S^c[[\underline{X}]] \arrow[ur] & \end{tikzcd} ,$$

où toutes les flèches sont injectives et continues, à image dense.

3.2. Le produit tensoriel $S[\underline{X}] \otimes_S S[\underline{X}]$ s'identifie à l'anneau $S[\underline{X},\underline{Y}]$ des polynômes en les indéterminées $X_0, X_{-1}, \dots, X_{-n}, \dots$ et $Y_0, Y_{-1}, \dots, Y_{-n}, \dots$ en posant $X_{-n} \otimes 1 = X_{-n}$ et $1 \otimes X_{-n} = Y_{-n}$.

Notons $S[[\underline{X},\underline{Y}]]$ (resp. $S^0[[\underline{X},\underline{Y}]]$) le produit tensoriel complété

$S[[\underline{X}]] \hat{\otimes}_S S[[\underline{X}]]$ (resp. $S^0[[\underline{X}]] \hat{\otimes}_S S^0[[\underline{X}]]$) . Si l'on note encore $\mathfrak{d}_r$ l'idéal de $S[\underline{X},\underline{Y}]$ engendré par les X_{-n} et les Y_{-n} , avec $n \geq r$, on voit que l'on a aussi

$$S[[\underline{X},\underline{Y}]] = \varprojlim S[\underline{X},\underline{Y}]/(\mathfrak{d}_r + \mathfrak{d}_0^s) \quad \text{et} \quad S^0[[\underline{X},\underline{Y}]] = \varprojlim S[\underline{X},\underline{Y}]/\mathfrak{d}_r^s .$$

Il est clair que $S[[\underline{X},\underline{Y}]]$ est l'anneau des séries formelles, à coefficients dans S , en les X_{-n} et les Y_{-n} . Avec des notations évidentes, tout élément de $S[[\underline{X},\underline{Y}]]$ s'écrit, de manière unique, sous la forme $\sum_{\underline{i},\underline{j}\in \mathrm{I}} a_{\underline{i}\,\underline{j}} \underline{X}^{\underline{i}} \underline{Y}^{\underline{j}}$, avec les $a_{\underline{i}\,\underline{j}} \in S$, arbitraires. Ici encore $S^0[[\underline{X},\underline{Y}]]$ s'identifie à un sous-anneau de $S[[\underline{X},\underline{Y}]]$.

3.3. Nous allons voir que le $\mathbb{Z}$-foncteur en groupes CW peut se décrire à l'aide d'une structure de "bigèbre topologique" sur l'anneau $\mathbb{Z}^0[[X]]$.

Soit R un anneau commutatif. On a une bijection naturelle entre l'ensemble des familles $\underline{a} = (\dots,a_{-n},\dots,a_0)$ d'éléments de R indexées par les entiers ≤ 0 et l'ensemble des homomorphismes de l'anneau $\mathbb{Z}[\underline{X}]$ dans R : à tout $\underline{a}$ correspond l'homomorphisme $\varphi_{\underline{a}}$ défini par $\varphi_{\underline{a}}(X_{-n}) = a_{-n}$.

L'élément $\underline{a}$ appartient à $CW(R)$ si et seulement s'il existe des entiers r et s tels que l'idéal engendré par les a_{-n} , avec $n \geq r$, a sa puissance s-ième nulle. Il revient au même de dire que le noyau de l'application $\varphi_{\underline{a}}$ contient l'idéal $\mathfrak{d}_r^s$.

Par conséquent, si l'on munit R de la topologie discrète, on voit que $CW(R)$ s'identifie à l'ensemble des homomorphismes continus de l'anneau $\mathbb{Z}[\underline{X}]$ dans R , pour la topologie de $\mathbb{Z}[\underline{X}]$ définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux $\mathfrak{d}_r^s$. Autrement dit,

$$CW(R) = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}^0[[\underline{X}]],R) .$$

Remarquons maintenant que le lemme 1.3 peut se réénoncer

LEMME 3.1.- <u>La suite des</u> $S_m(X_{-m},\dots,X_{-1},X_0;Y_{-m},\dots,Y_{-1},Y_0)$ <u>converge dans</u> $\mathbb{Z}^0[[\underline{X},\underline{Y}]]$.

Notons $S = S(\dots,X_{-n},\dots,X_{-1},X_0;\dots,Y_{-n},\dots,Y_{-1},Y_0)$ la limite de cette suite et posons

$S_0 = S = S(\ldots,X_{-n},\ldots,X_{-1},X_0\,;\ldots,Y_{-n},\ldots,Y_{-1},Y_0)$,

$S_{-1} = S(\ldots,X_{-n-1},\ldots,X_{-2},X_{-1}\,;\ldots,Y_{-n-1},\ldots,Y_{-2},Y_{-1})$,

...

$S_{-m} = S(\ldots,X_{-n-m},\ldots,X_{-m-1},X_{-m}\,;\ldots,Y_{-n-m},\ldots,Y_{-m-1},Y_{-m})$

...

On voit que ce sont tous des éléments de $\mathbb{Z}^0[[\underline{X},\underline{Y}]]$ (ne pas confondre $S_0 = S$ avec le polynôme $S_0(X_0\,;Y_0) = X_0 + Y_0$!).

PROPOSITION 3.2.-

i) <u>Il existe un homomorphisme d'anneaux continu et un seul</u> $\Delta : \mathbb{Z}^0[[\underline{X}]] \to \mathbb{Z}^0[[\underline{X}]] \hat{\otimes} \mathbb{Z}^0[[\underline{X}]] = \mathbb{Z}^0[[\underline{X},\underline{Y}]]$ <u>tel que</u> $\Delta(X_{-n}) = S_{-n}$, <u>pour tout</u> n .

ii) <u>L'application</u> Δ <u>munit l'anneau</u> $\mathbb{Z}^0[[\underline{X}]]$ <u>d'une structure de "bigèbre topologique", linéairement topologisée, séparée et complète</u>.

iii) <u>Pour tout anneau linéairement topologisé, séparé et complet</u> R , <u>le groupe</u> $CW(R)$ <u>s'identifie à</u> $\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}^0[[\underline{X}]],R)$ (<u>la structure de groupe sur ce dernier ensemble étant induite, de manière évidente</u>, <u>par</u> Δ .

<u>Démonstration</u> : c'est clair !

<u>Remarques</u> :

1.- On voit de même que, pour tout anneau R (sans topologie), le groupe $CW^u(R)$ s'identifie à $\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}^u[[\underline{X}]],R)$, où l'on a mis sur R la topologie discrète.

2.- Soit k un corps parfait de caractéristique p . Il est clair que, pour tout k-anneau R , $CW_k(R)$ s'identifie aussi à l'ensemble des homomorphismes continus du k-anneau $k^0[[\underline{X}]]$ dans R ; le plongement de D_k dans $\mathrm{End}(CW_k)$ induit un homomorphisme de l'anneau opposé à D_k dans l'anneau des endomorphismes continus de la bigèbre topologique $k^0[[\underline{X}]]$. On peut faire le même genre de remarque en remplaçant k par $A = W(k)$ et D_k par $A[\underline{V}]$.

3.4. Pour tout anneau topologique S et tout S-anneau topologique B , nous notons $\Omega_S(B)$ le module des S-différentielles continues de l'anneau B et $d = d_{B/S}$ l'application canonique de B dans $\Omega_S(B)$.

Il est clair que $\mathbb{Z}^0[[\underline{X}]]$ s'identifie à un sous-anneau topologique de $\mathbb{Q}^0[[\underline{X}]]$ et que $\Omega_{\mathbb{Z}}(\mathbb{Z}^0[[\underline{X}]])$ s'identifie à un sous-$\mathbb{Z}^0[[\underline{X}]]$-module topologique de $\Omega_{\mathbb{Q}}(\mathbb{Q}^0[[\underline{X}]])$. Posons

$$P(\mathbb{Z}^0[[\underline{X}]]) = \{\alpha \in \mathbb{Q}^0[[\underline{X}]] \mid d\alpha \in \Omega_{\mathbb{Z}}(\mathbb{Z}^0[[\underline{X}]])\} .$$

On voit que $P(\mathbb{Z}^0[[\underline{X}]])$ est fermé dans $\mathbb{Q}^0[[\underline{X}]]$. C'est le sous-$\mathbb{Z}^0[[\underline{X}]]$-module de $\mathbb{Q}^0[[\underline{X}]]$ formé des séries formelles $\sum a_{\underline{i}} X^{\underline{i}}$ (la sommation étant étendue aux $\underline{i} = (i_0, i_{-1}, \ldots, i_{-n}, \ldots) \in \mathbb{N}^{(\{0,-1,\ldots,-n,\ldots\})}$) à coefficients dans $\mathbb{Q}$ qui, d'une part, sont dans $\mathbb{Q}^0[[\underline{X}]]$ (i.e. on a un nombre fini de $a_{\underline{i}} \neq 0$ avec $|\underline{i}|_r < s$, pour tout couple $(r,s) \in \mathbb{N}^2$) et, d'autre part, satisfont $i_{-n} a_{\underline{i}} \in \mathbb{Z}$, pour tout $\underline{i}$ et tout entier $n \geq 0$.

On définit de la même manière

$$P(\mathbb{Z}^0[[\underline{X},\underline{Y}]]) = \{\alpha \in \mathbb{Q}^0[[\underline{X},\underline{Y}]] \mid d\alpha \in \Omega_{\mathbb{Z}}(\mathbb{Z}^0[[\underline{X},\underline{Y}]])\} .$$

Nous allons établir le résultat suivant :

PROPOSITION 3.3.- <u>Soit</u> $S_0, S_{-1}, \ldots, S_{-n}, \ldots$ <u>les éléments de</u> $\mathbb{Z}^0[[\underline{X},\underline{Y}]]$ <u>qui définissent la structure de bigèbre topologique de</u> $\mathbb{Z}^0[[\underline{X}]]$. <u>Alors</u>

i) <u>les séries de terme général</u> $p^{-n}X_{-n}^{p^n}$, $p^{-n}Y_{-n}^{p^n}$, $p^{-n}S_{-n}^{p^n}$ <u>convergent dans</u> $P(\mathbb{Z}^0[[\underline{X},\underline{Y}]])$ <u>et l'on a</u>

$$\sum_{n=0}^{\infty} p^{-n}X_{-n}^{p^n} + \sum_{n=0}^{\infty} p^{-n}Y_{-n}^{p^n} = \sum_{n=0}^{\infty} p^{-n}S_{-n}^{p^n} ;$$

ii) <u>les séries de terme général</u> $X_{-n}^{p^n-1}dX_{-n}$, $Y_{-n}^{p^n-1}dY_{-n}$, $S_{-n}^{p^n-1}dS_{-n}$ <u>convergent dans</u> $\Omega_{\mathbb{Z}}(\mathbb{Z}^0[[\underline{X},\underline{Y}]])$ <u>et l'on a</u>

$$\sum_{n=0}^{\infty} X_{-n}^{p^n-1}dX_{-n} + \sum_{n=0}^{\infty} Y_{-n}^{p^n-1}dY_{-n} = \sum_{n=0}^{\infty} S_{-n}^{p^n-1}dS_{-n} .$$

<u>Démonstration</u> : la proposition résulte trivialement du lemme suivant :

LEMME 3.4.- <u>Pour tout entier</u> $r \geq 0$, <u>soit</u> $\mathfrak{b}_r$ <u>l'idéal de</u> $\mathbb{Q}[\underline{X},\underline{Y}]$ <u>engendré par les</u> X_{-n} <u>et les</u> Y_{-n} , <u>pour</u> $n \geq r$. <u>Quels que soient les entiers</u> r <u>et</u> $s \geq 0$, <u>il existe un entier</u> $m(r,s)$ <u>tel que, si</u> $m \geq m(r,s)$, <u>alors</u>

$$\sum_{n=0}^{m} p^{-n}X_{-n}^{p^n} + \sum_{n=0}^{m} p^{-n}Y_{-n}^{p^n} \equiv \sum_{n=0}^{m} p^{-n}S_{-n}^{p^n} \pmod{\overline{\mathfrak{b}_r^s}} ,$$

<u>où</u> $\overline{\mathfrak{b}_r^s}$ <u>désigne l'adhérence, dans</u> $\mathbb{Q}^0[[\underline{X},\underline{Y}]]$, <u>de l'idéal</u> $\mathfrak{b}_r^s$ <u>de</u> $\mathbb{Q}[\underline{X},\underline{Y}]$.

<u>Démonstration</u> : il est clair qu'il suffit de démontrer ce lemme lorsque les entiers r et s satisfont $r \geq 1$, $s \geq p$ et $s \leq p^r$. Montrons qu'alors la

congruence annoncée est vérifiée dès que $m \geq r-1+(s-p)/(p-1)$:

il résulte de la définition des polynômes S_n que l'on a

$$\sum_{n=0}^{m} p^{-n} X_{-n}^{p^n} + \sum_{n=0}^{m} p^{-n} Y_{-n}^{p^n} = \sum_{n=0}^{m} p^{-n} T_{-n}^{p^n} ,$$

en posant $T_{-n} = S_{m-n}(X_{-m}, X_{-m+1}, \dots, X_{-n} ; Y_{-m}, Y_{-m+1}, \dots, Y_{-n})$. Il suffit donc de montrer que, pour $0 \leq n \leq m$, on a $T_{-n}^{p^n} \equiv S_{-n}^{p^n} \pmod{\overline{\mathfrak{v}_r^s}}$.

- Si $n \geq r$, on voit que T_{-n} et S_{-n} appartiennent à l'adhérence de $\mathfrak{v}_r$, donc que $T_{-n}^{p^n}$ et $S_{-n}^{p^n}$ appartiennent tous deux à $\overline{\mathfrak{v}_r^{p^n}} \subset \overline{\mathfrak{v}_r^{p^r}} \subset \overline{\mathfrak{v}_r^{s}}$, puisque $s \leq p^r$.

- Si $n < r$, on a, d'après le lemme 1.3,

  $S_{m'-n}(X_{-m'}, \dots, X_{-n} ; Y_{-m'}, \dots, Y_{-n})$

  $\equiv S_{m'+1-n}(X_{-m'-1}, \dots, X_{-n} ; Y_{-m'-1}, \dots, Y_{-n}) \pmod{\overline{\mathfrak{v}_{r-n+n}^{s}}}$,

  pourvu que $m'-n \geq (r-n)-1+(s-p)/(p-1)$. C'est donc le cas si $m' \geq m$ et, par passage à la limite, on en déduit $T_{-n} \equiv S_{-n} \pmod{\overline{\mathfrak{v}_r^s}}$; donc, a fortiori, $T_{-n}^{p^n} \equiv S_{-n}^{p^n} \pmod{\overline{\mathfrak{v}_r^s}}$.

§4.- Le groupe formel des covecteurs.

4.1. Soit k un anneau commutatif. Par restriction à la catégorie des k-anneaux, CW définit un k-foncteur en groupes CW_k .

Soit k un anneau commutatif pseudo-compact. Par restriction à la catégorie des k-anneaux finis, CW définit un k-foncteur formel en groupes que nous notons $\widehat{CW}_k$ car c'est la complétion formelle du k-foncteur CW_k .

Soit R un k-anneau fini. C'est un anneau artinien et son radical $\mathfrak{r}_R$ est nilpotent. On en déduit que $\widehat{CW}_k(R) = CW(R)$ s'identifie à l'ensemble des covecteurs $\underline{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0)$, avec les $a_{-n} \in R$ vérifiant

(ψ') pour presque tout n , $a_{-n} \in \mathfrak{r}_R$.

4.2. Soit toujours k un anneau commutatif pseudo-compact. Si R est un k-anneau fini, que l'on munit de la topologie discrète, on a $\widehat{CW}_k(R) = CW(R) = \mathrm{Hom}_{cont}(\mathbb{Z}^0[[\underline{X}]], R)$. Considérons le produit tensoriel topologique $B_k^0 = \mathbb{Z}^0[[\underline{X}]] \hat{\otimes}_{\mathbb{Z}} k = \varprojlim (\mathbb{Z}^0[[\underline{X}]]/\mathfrak{b}_r^s) \otimes_{\mathbb{Z}} (k/\mathfrak{a})$, pour r et s entiers ≥ 0 et $\mathfrak{a}$ idéal ouvert de k ; c'est un k-anneau topologique, linéairement topologisé, et $\widehat{CW}_k(R)$ s'identifie à l'ensemble $\mathrm{Hom}_{cont}(B_k^0, R)$ des homomorphismes continus du k-anneau topologique B_k^0 dans R . Par conséquent (cf. n° I.4.8) $\widehat{CW}_k$ est un k-groupe formel dont l'algèbre affine s'identifie à la complétion profinie de B_k^0 .

Si $\varphi : R \to S$ est un épimorphisme de k-anneaux finis, l'application $\widehat{CW}_k(\varphi) : \widehat{CW}_k(R) \to \widehat{CW}_k(S)$ est clairement surjective ; par conséquent, le k-groupe formel $\widehat{CW}_k$ est lisse.

De la même manière, par restriction aux k-anneaux finis, CW^u définit un k-foncteur formel en groupes $\widehat{CW}_k^u$. On voit que c'est un k-groupe formel lisse dont l'algèbre affine s'identifie à la complétion profinie de $B_k^u = \mathbb{Z}^u[[\underline{X}]] \hat{\otimes}_{\mathbb{Z}} k$. Il est clair que $\widehat{CW}_k^u$ s'identifie de manière naturelle à un sous-groupe de $\widehat{CW}_k$.

<u>Remarques</u> :

1.- Soit $\widehat{CW}_k^c$ (resp. $\widehat{CW}_k^{u,c}$) la composante connexe de $\widehat{CW}_k$ (resp. $\widehat{CW}_k^u$) . On voit facilement que, pour tout k-anneau fini R , de radical $\mathfrak{r}_R$, on a

$$\widehat{CW}_k^c(R) = \{\underline{a} = (\dots, a_{-n}, \dots, a_0) | a_{-n} \in \mathfrak{r}_R \text{ , pour tout } n \geq 0\} ,$$

$$\widehat{CW}_k^{u,c}(R) = \widehat{CW}_k^u(R) \cap \widehat{CW}_k^c(R) =$$

$$\{\underline{a} = (\dots, a_{-n}, \dots, a_0) \mid \text{les } a_{-n} \text{ sont tous dans } \mathfrak{r}_R \text{ et presque tous nuls}\} ,$$

et que l'algèbre affine de $\widehat{CW}_k^c$ (resp. $\widehat{CW}_k^{u,c}$) s'identifie à la complétion profinie de $B_k^c = \mathbb{Z}^c[[\underline{X}]] \hat{\otimes}_{\mathbb{Z}} k$ (resp. $B_k = \mathbb{Z}[[\underline{X}]] \hat{\otimes}_{\mathbb{Z}} k$) ; on voit d'ailleurs que B_k est déjà profinie et s'identifie au k-anneau topologique $k[[\underline{X}]]$ des séries formelles en les X_{-n} à coefficients dans k .

2.- Si k est artinien, la topologie de k est la topologie discrète, et alors $B_k^0 = k^0[[\underline{X}]]$, $B_k^u = k^u[[\underline{X}]]$, $B_k^c = k^c[[\underline{X}]]$, $B_k = k[[\underline{X}]]$.

4.3. Supposons maintenant que l'anneau commutatif pseudo-compact k est parfait de caractéristique p . On a un homomorphisme évident de l'anneau $\mathrm{End}(CW_k)$ dans l'anneau $\mathrm{End}(\widehat{CW}_k)$ des endomorphismes du k-groupe formel $\widehat{CW}_k$. On vérifie facilement que la restriction de cet homomorphisme à D_k est injective. Ceci nous permet <u>d'identifier</u> D_k <u>à un sous-anneau de</u> $\mathrm{End}(\widehat{CW}_k)$.

Remarques : supposons que k est un corps parfait de caractéristique p .

1.- Soit B l'algèbre affine de l'un des quatre k-groupes formels $\widehat{CW}_k$, $\widehat{CW}_k^u$, $\widehat{CW}_k^c$, $\widehat{CW}_k^{u,c}$. L'image canonique de $\mathbb{Z}[\underline{X}]$ dans B s'identifie à l'anneau $k[\underline{X}]$ des polynômes en les X_{-n} à coefficients dans k et est dense dans B . Soit τ un automorphisme du corps k et soit φ un endomorphisme continu de la structure d'anneau de B , τ-semi-linéaire (i.e. tel que $\varphi(\lambda x) = \tau(\lambda)\varphi(x)$, si $\lambda \in k$, $x \in B$). Comme $k[\underline{X}]$ est dense dans B , φ est complètement déterminé par les $\varphi(X_{-n})$, pour $n \geq 0$.

Le Frobenius F_B est σ-semi-linéaire et l'on a évidemment $F_B(X_{-n}) = X_{-n}^p$. L'endomorphisme de multiplication par p est linéaire et il résulte de la formule (6) du paragraphe 2 que $p(X_{-n}) = X_{-n-1}^p$.

Le décalage V_B est σ^{-1}-semi-linéaire et vérifie $F_BV_B = p$. Soit V'_B l'unique endomorphisme continu, σ^{-1}-semi-linéaire, de B tel que $V'_B(X_{-n}) = X_{-n-1}$, pour tout $n \geq 0$. On voit que $F_BV'_B$ est linéaire et vérifie $F_BV'_B(X_{-n}) = X_{-n-1}^p$. On a donc $F_BV'_B = p = F_BV_B$, d'où $V'_B = V_B$, puisque F_B est injectif. En particulier

(1) $\quad V_B(X_{-n}) = X_{-n-1}$.

2.- La formule précédente implique que $\widehat{CW}_k^u$ est la "composante unipotente" de $\widehat{CW}_k$ (cf. n° I. 7.6).

3.- Par complétion, on voit que $\hat{D}_k = \varprojlim D_k/p^mD_k$ s'identifie encore à un sous-anneau de $\mathrm{End}(\widehat{CW}_k)$. On voit qu'en fait $\hat{D}_k$ s'identifie à un sous-anneau de l'anneau $\mathrm{End}_{cont}(\widehat{CW}_k)$ des endomorphismes "continus" de $\widehat{CW}_k$ (i.e. des endomorphismes qui opèrent continûment sur chaque groupe topologique $\widehat{CW}_k(R)$). On peut montrer que l'on a $\hat{D}_k = \mathrm{End}_{cont}(\widehat{CW}_k)$. L'idée de la démonstration est la suivante : comme $\widehat{CW}_k^u$ est "dense" dans $\widehat{CW}_k$, pour connaître un élément de $\mathrm{End}_{cont}(\widehat{CW}_k)$ il suffit de connaître sa restriction à $\widehat{CW}_k^u$; c'est un endomorphisme de $\widehat{CW}_k^u$, d'après la remarque précédente (qui implique que $\widehat{CW}_k^u$ est un sous-groupe "caractéristique" de $\widehat{CW}_k$) ; on vérifie que $\mathrm{End}(\widehat{CW}_k^u) = \varprojlim \mathrm{End}((W_m)_k) = \varprojlim D_k/\underline{V}^mD_k = \hat{D}_k^V$; il reste alors à constater que $\hat{D}_k$ s'identifie à un sous-anneau de $\hat{D}_k^V$ et qu'un élément de $\hat{D}_k^V$ définit un endomorphisme continu de $\widehat{CW}_k^u$ si et seulement s'il appartient à $\hat{D}_k$.

4.4. Soit k un corps parfait de caractéristique p . Si R est un k-anneau profini, c'est un k-anneau linéairement topologisé, séparé et complet et l'on a encore $\widehat{CW}_k(R) = CW_k(R) = CW(R)$. C'est encore un D_k-module topologique. Lorsque l'on représente les éléments de $\widehat{CW}_k(R)$ comme des covecteurs, on voit que

- si R est un k-anneau profini local, son idéal maximal $\mathfrak{m}$ est topologiquement nilpotent et

$$\widehat{CW}_k(R) = \left\{ \underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \;\middle|\; \begin{array}{l} a_{-n} \in R \text{ , pour tout } n \text{ ,} \\ a_{-n} \in \mathfrak{m} \text{ , pour presque tout } n \end{array} \right\} \;;$$

- dans le cas général, le k-anneau profini R s'écrit comme un produit $\prod_{j \in J} R_j$ de k-anneaux profinis locaux et $\widehat{CW}_k(R)$ est le produit des $\widehat{CW}_k(R_j)$; on a donc

$$\widehat{CW}_k(R) = \left\{ \underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \;\middle|\; \begin{array}{l} a_{-n} \in R \text{ , pour tout } n \text{ ,} \\ \text{pour } j \text{ fixé, } a_{-n,j} \in \mathfrak{m}_j \text{ pour presque} \\ \text{tout } n \end{array} \right\},$$

  où l'on a noté $a_{-n,j}$ la projection de a_{-n} sur R_j et $\mathfrak{m}_j$ l'idéal maximal de R_j .

4.5 On suppose toujours que k est un corps parfait de caractéristique p et on pose $A = W(k)$, $D_k = A[\underline{F}, \underline{V}]$. Nous allons étudier la structure du D_k-module topologique $\widehat{CW}_k(R)$ lorsque R est un k-anneau fini ou profini. Pour cela, introduisons quelques définitions :

soit M un D_k-module topologique. On suppose M profini (resp. pro-artinien) en tant que A-module topologique (cf. n° I.3.4) :

- nous disons que M est <u>un D_k-module $A[\underline{F}]$-profini</u> (resp. <u>$A[\underline{F}]$-pro-artinien</u>) si les sous-$A[\underline{F}]$-modules ouverts forment un système fondamental de voisinages de 0 ;

- de même, nous disons que M est un D_k-module <u>D_k-profini</u> (resp. <u>D_k-pro-artinien</u>) si les sous-D_k-modules ouverts forment un système fondamental de voisinages de 0 .

PROPOSITION 4.1.- <u>Soit</u> R <u>un k-anneau fini ou profini</u>.

i) <u>Muni de sa topologie naturelle</u>, $\widehat{CW}_k(R)$ <u>est un D_k-module $A[\underline{F}]$-pro-artinien</u>.

ii) Le sous-module $\widehat{CW}_k^c(R)$, qui est ouvert dans $\widehat{CW}_k(R)$, est un D_k-module $A[\underline{F}]$-profini ; il est formé des $\underline{a} \in \widehat{CW}_k(R)$ tels que la suite des $\underline{F}^n\underline{a}$ tend vers 0 .

iii) Le sous-module $\widehat{CW}_k^{et}(R)$, qui est fermé dans $\widehat{CW}_k(R)$, est un D_k-module D_k-pro-artinien, discret si R est fini ; on a

$$\widehat{CW}_k^{et}(R) = \bigcap_{n=0}^{\infty} \underline{F}^n\widehat{CW}_k(R) = \bigcap_{n=0}^{\infty} p^n\widehat{CW}_k(R) .$$

Démonstration : par passage à la limite, on voit qu'il suffit de démontrer cette proposition lorsque R est un k-anneau fini. Soit alors r_R son radical et R^{et} la partie étale de R , de sorte que $R = R^{et} \oplus r_R$.

Montrons (iii). Il est clair que $\widehat{CW}_k^{et}(R) = \widehat{CW}_k(R^{et})$ est fermé dans $\widehat{CW}_k(R)$. Comme R^{et} est réduit, il n'a pas d'idéaux nilpotents non triviaux et on en déduit que $\widehat{CW}_k^{et}(R) = CW_k(R^{et})$ s'identifie à $CW^u(R^{et})$ et est muni de la topologie discrète. L'anneau R^{et} s'écrit comme le produit d'un nombre fini d'extensions finies k_i du corps k . On voit que $CW_k(R^{et})$ s'identifie à la somme directe des $CW_k(k_i)$; si l'on pose $A_i = W(k_i)$ et si l'on note K_i le corps des fractions de A_i , on sait (cf. n° 2.3) que $CW_k(k_i)$ s'identifie, au A-module K_i/A_i , l'action de $\underline{F}$ étant donnée par $\underline{F}\underline{a} = \sigma(\underline{a})$, pour tout $\underline{a} \in K_i/A_i$; on en déduit que $\widehat{CW}_k^{et}(R)$, isomorphe à la somme directe des K_i/A_i est artinien et divisible, donc que

$$\bigcap_{n=0}^{\infty} p^n\widehat{CW}_k^{et}(R) = \bigcap_{n=0}^{\infty} \underline{F}^n\widehat{CW}_k^{et}(R) = \widehat{CW}_k^{et}(R) \quad ;$$

si n est un entier tel que $r_R^{p^n} = 0$, on voit que

$$p^n\widehat{CW}_k(R) = \underline{F}^n\widehat{CW}_k(R) = \widehat{CW}_k^{et}(R) ,$$

ce qui achève de prouver (iii).

Le D_k-module $\widehat{CW}_k^c(R)$ est formé des $\underline{a} = (\dots,a_{-n},\dots,a_0)$ tels que $a_{-n} \in r_R$, pour tout n et est isomorphe, en tant qu'espace topologique au produit direct $r_R^{\mathbb{N}}$. On voit que les

$$U(R,r_R,s)$$
$$= \{\underline{a} = (\dots,a_{-n},\dots,a_0) \mid a_{-n} \in r_R \text{ , pour tout } n \text{ , et } a_{-n} \in r_R^{p^{s-n}} \text{ , si } n<s\},$$

pour $s \in \mathbb{N}$, forment un système fondamental de voisinages ouverts de 0 dans $\widehat{CW}_k^c(R)$ et sont des sous-$A[\underline{F}]$-modules.

Soit $\{y_1, y_2, \dots, y_{d'}\}$ une base de r_R sur k. Pour $n \in \mathbb{N}$ et $1 \leq j \leq d'$, soit $\underline{v}_{n,j}$ l'élément de $\widehat{CW}_k^c(R)$ dont toutes les composantes sont nulles, sauf celle d'indice $-n$ qui est égale à y_j. On voit tout de suite que le quotient $\widehat{CW}_k^c(R)/U(R, r_R, s)$ est engendré, en tant que A-module, par les images des $\underline{v}_{n,j}$, pour $n < s$. C'est donc un A-module de type fini. Comme $\widehat{CW}_k^c(R)$ est un groupe de p-torsion, on en déduit que les $A[\underline{F}]$-modules $\widehat{CW}_k^c(R)/U(R, r_R, s)$ sont des A-modules de longueur finie. Par conséquent, $\widehat{CW}_k^c(R)$ est un D_k-module $A[\underline{F}]$-profini.

Soit m un entier tel que $r_R^{p^m} = 0$. On a $\underline{F}^m\underline{a} = 0$, pour tout $\underline{a} \in \widehat{CW}_k^c(R)$. Réciproquement, si $\underline{a} \in CW_k(R)$ est tel que la suite des $\underline{F}^n\underline{a}$ tend vers 0, on a $\underline{F}^n\underline{a} \in \widehat{CW}_k^{et}(R)$, pour $n \geq m$. Comme $\widehat{CW}_k^{et}(R)$ est discret, on a $\underline{F}^n\underline{a} = 0$, pour n suffisamment grand, et toutes les composantes de $\underline{a}$ sont dans r_R, donc $\underline{a} \in \widehat{CW}_k^c(R)$. Par conséquent, $\widehat{CW}_k^c(R)$ est bien l'ensemble des $\underline{a} \in \widehat{CW}_k(R)$ tels que la suite des $\underline{F}^n\underline{a}$ tend vers 0.

Comme $\widehat{CW}_k(R) = \widehat{CW}(R, r_R)$, les $U(R, r_R, s)$, pour $s \in \mathbb{N}$, forment encore un système fondamental de voisinages ouverts de 0 dans $\widehat{CW}_k(R)$. En particulier, $\widehat{CW}_k^c(R) = U(R, r_R, 0)$ est ouvert dans $\widehat{CW}_k(R)$, ce qui achève de prouver l'assertion (ii).

Comme $\widehat{CW}_k(R) = \widehat{CW}_k^c(R) \oplus \widehat{CW}_k^{et}(R)$, l'assertion (i) résulte des deux autres.

§5.- Relèvement des covecteurs.

Dans ce paragraphe et dans le suivant, k désigne un corps parfait de caractéristique p, on pose $A = W(k)$ et on note K le corps des fractions de A ; on note σ le Frobenius absolu opérant sur k, $W(k) = A$ et K.

5.1. Appelons <u>anneau</u> p-<u>adique</u> (cf. Lazard, [35] p. 69 ; Serre dit " p-anneau strict" dans [43] p. 46) tout anneau $\mathcal{R}$ linéairement topologisé, séparé et complet, dont la topologie est la topologie p-adique (autrement dit $\mathcal{R} = \varprojlim \mathcal{R}/p^n\mathcal{R}$, chaque quotient étant muni de la topologie discrète), et qui est tel que p est non diviseur de zéro dans $\mathcal{R}$.

De même, nous appelons A-<u>anneau</u> p-<u>adique</u> tout A-anneau linéairement topologisé qui est un anneau p-adique.

Si $\mathfrak{R}$ est un A-anneau p-adique et si l'on pose $\mathfrak{R}_K = \mathfrak{R} \otimes_A K$, on voit que $\mathfrak{R}$ s'identifie à un sous-anneau de $\mathfrak{R}_K$ et que le A-module $\mathfrak{R}_K$, muni de la topologie p-adique, est linéairement topologisé, séparé et complet : on a $\mathfrak{R}_K = \varprojlim \mathfrak{R}_K/p^m\mathfrak{R}$, chaque quotient étant muni de la topologie discrète.

PROPOSITION 5.1.- Soit $\mathfrak{R}$ un A-anneau p-adique. Soit $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$. La série de terme général $p^{-n}\hat{a}_{-n}^{p^n}$ converge, dans $\mathfrak{R}_K = \mathfrak{R} \otimes_A K$, pour la topologie p-adique. Notons $\hat{w}_{\mathfrak{R}}(\underline{\hat{a}})$ la somme de cette série. L'application $\hat{w}_{\mathfrak{R}} : CW_A(\mathfrak{R}) \to \mathfrak{R}_K$ ainsi définie est une application A-linéaire continue.

Démonstration : on a $CW_A(\mathfrak{R}) = CW(\mathfrak{R}) = \varprojlim CW(\mathfrak{R}/p^m\mathfrak{R})$. Posons $R = \mathfrak{R}/p\mathfrak{R}$, et, pour tout $\hat{a} \in \mathfrak{R}$, notons a son image dans R. Si on se donne une suite d'éléments $\hat{a}_{-n}$, pour $n \in \mathbb{N}$, de $\mathfrak{R}$, on voit facilement que $(\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$ si et seulement si $(\ldots,a_{-n},\ldots,a_{-1},a_0) \in CW(R)$.

Soit $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$. Alors $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0) \in CW(R)$ et il existe des entiers r et s tel que l'idéal $\mathfrak{n}$ de R engendré par les a_{-n}, avec $n \geq r$, est nilpotent. Si t est un entier tel que $\mathfrak{n}^{p^t} = 0$, on en déduit, en particulier, que $\hat{a}_{-n}^{p^t} \in p\mathfrak{R}$, pour tout $n \geq r$; si $n \geq r$ et $n \geq t$, on a donc $\hat{a}_{-n}^{p^n} = (\hat{a}_{-n}^{p^t})^{p^{n-t}} \in p^{p^{n-t}}\mathfrak{R}$ ou encore $p^{-n}\hat{a}_{-n}^{p^n} \in p^{p^{n-t}-n}\mathfrak{R}$; la convergence de la série de terme général $p^{-n}\hat{a}_{-n}^{p^n}$ résulte alors de ce que, pour t fixé, la suite des $p^{n-t}-n$ tend vers l'infini.

Considérons une suite $(\underline{\hat{a}}_m)_{m\in\mathbb{N}}$ convergente d'éléments de $CW_A(\mathfrak{R})$ et soit $\underline{\hat{a}}$ sa limite. Posons $\underline{\hat{a}}_m = (\ldots,\hat{a}_{m,-n},\ldots,\hat{a}_{m,0})$ et $\hat{a} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_0)$. On voit que la suite des $\underline{a}_m = (\ldots,a_{m,-n},\ldots,a_{m,0})$ converge, dans $CW(R)$ vers $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$.

Comme la topologie de $CW(R)$ est celle de la limite inductive des $CW(R,\mathfrak{n},r)$ (cf. n° 1.6), il existe un idéal nilpotent $\mathfrak{n}$ de R et un entier r tel que $a_{-n} \in \mathfrak{n}$ et $a_{-n,m} \in \mathfrak{n}$ pour tout $n \geq r$ (et ceci quel que soit m). Choisissons un entier t tel que $\mathfrak{n}^{p^t} = 0$. Le même raisonnement que celui que l'on vient de faire montre que, si $n \geq r$ et $n \geq t$, on a

$p^{-n}\hat{a}_{-n}^{p^n} \in p^{p^{n-t}-n}\mathfrak{R}$ et $p^{-n}\hat{a}_{m,-n}^{p^n} \in p^{p^{n-t}-n}\mathfrak{R}$, quel que soit m .

Soit u un entier ≥ 1 . Soit n_0 un entier vérifiant $n_0 \geq r$ et $n_0 \geq t$ tel que $p^{n-t}-n \geq u$ si $n \geq n_0$. On voit que l'on a

$$p^{-n}\hat{a}_{m,-n}^{p^n} \equiv p^{-n}\hat{a}_{-n}^{p^n} \pmod{p^u\mathfrak{R}} \text{ , pour tout } n \geq n_0 \text{ et tout } m \text{ .}$$

La convergence de la suite des $\underline{\hat{a}}_m$ dans $CW_A(\mathfrak{R})$ vers $\underline{\hat{a}}$ implique la convergence, pour tout n fixé, de la suite des $\hat{a}_{m,-n}$ dans $\mathfrak{R}$ vers $\hat{a}_{-n}$. Il existe donc un entier m_0 tel que si $m \geq m_0$ et $n \geq n_0$, on a $\hat{a}_{-n,m} \equiv \hat{a}_{-n} \pmod{p^u\mathfrak{R}}$. Avec les mêmes conditions sur m et sur n , on a donc

$$a_{-n,m}^{p^n} \equiv \hat{a}_{-n}^{p^n} \pmod{p^{up^n}\mathfrak{R}} \text{ ,}$$

ou encore

$$p^{-n}\hat{a}_{-n,m}^{p^n} \equiv p^{-n}\hat{a}_{-n}^{p^n} \pmod{p^{up^n-n}\mathfrak{R}} \text{ ,}$$

d'où

$$p^{-n}\hat{a}_{-n,m}^{p^n} \equiv p^{-n}\hat{a}_{-n}^{p^n} \pmod{p^u\mathfrak{R}}$$

car $up^n-n \geq u$ si $n \geq 0$.

On voit donc, finalement, que si $m \geq m_0$, on a $\hat{w}_{\mathfrak{R}}(\underline{\hat{a}}_m) = \sum_{n=0}^{\infty} p^{-n}\hat{a}_{m,-n}^{p^n}$ est congru (mod $p^u\mathfrak{R}$) à $\sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n} = \hat{w}_{\mathfrak{R}}(\underline{\hat{a}})$, ce qui implique la continuité de $\hat{w}_{\mathfrak{R}}$.

Il résulte immédiatement de la définition des polynômes S_n que la restriction de $\hat{w}_{\mathfrak{R}}$ à $CW^u(\mathfrak{R})$ est additive. Comme on voit que $CW^u(\mathfrak{R})$ est un sous-groupe dense de $CW_A(\mathfrak{R})$, le fait que $\hat{w}_{\mathfrak{R}}$ est additive s'en déduit par continuité.

Comme le sous-groupe de A engendré par les $[x]$, pour $x \in k$, est dense dans A , il suffit alors, pour montrer que $\hat{w}_{\mathfrak{R}}$ est A-linéaire, de vérifier que $\hat{w}_{\mathfrak{R}}([x]\underline{a}) = [x]\hat{w}_{\mathfrak{R}}(\underline{a})$, pour tout $x \in k$ et tout $\underline{a} \in CW_A(\mathfrak{R})$; ceci résulte immédiatement de l'assertion (i) de la proposition 2.3 et du fait que $(\sigma^{-n}([x]))^{p^n} = [x]$.

<u>Remarque</u> : on aurait pu aussi déduire cette proposition de la proposition 3.3.

5.2. Soit toujours $\mathfrak{R}$ un A-anneau p-adique. Posons $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. Il est clair que l'application canonique de $\mathfrak{R}$ sur $\mathfrak{R}_k$ induit une application A-linéaire continue de $CW_A(\mathfrak{R})$ dans $CW_k(\mathfrak{R}_k)$; on voit que cette application est surjective et que son noyau est le sous-A-module fermé $CW_A(p\mathfrak{R})$ de $CW_A(\mathfrak{R})$ formé des covecteurs dont toutes les composantes sont dans $p\mathfrak{R}$. Comme $p^n - n \geq 1$, pour tout entier $n \geq 0$, on voit que l'image par $\hat{w}_{\mathfrak{R}}$ de $CW_A(p\mathfrak{R})$ est $p\mathfrak{R}$. Par passage au quotient, on en déduit une application A-linéaire continue, que nous notons $w_{\mathfrak{R}}$ de $CW_k(\mathfrak{R}_k)$ dans le module quotient $\mathfrak{R}_K/p\mathfrak{R}$.

On voit que cette application $w_{\mathfrak{R}}$ peut se construire ainsi : si $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0) \in CW_k(R_k)$, on choisit, pour tout n, un relèvement $\hat{a}_{-n}$ de a_{-n} dans $\mathfrak{R}$; alors la série de terme général $p^{-n}\hat{a}_{-n}^{p^n}$ converge dans $\mathfrak{R}_K$ et son image dans $\mathfrak{R}_K/p\mathfrak{R}$ ne dépend pas du choix des relèvements des a_{-n} : c'est $w_{\mathfrak{R}}(\underline{a})$.

Remarques.

1.- Il est clair que $\hat{w}$ et w sont des transformations naturelles au sens suivant : soit $\mathfrak{R}$ et $\mathfrak{S}$ deux A-anneaux p-adiques et soit φ un homomorphisme du A-anneau $\mathfrak{R}$ dans $\mathfrak{S}$; il est clair que φ s'étend de manière unique en un morphisme φ_K de $\mathfrak{R}_K$ dans $\mathfrak{S}_K = \mathfrak{S} \otimes_A K$ et induit, par passage au quotient une application A-linéaire $\tilde{\varphi}_K$ de $\mathfrak{R}_K/p\mathfrak{R}$ dans $\mathfrak{S}_K/p\mathfrak{S}$; de même, φ induit un morphisme φ_k de $\mathfrak{R}_k$ dans $\mathfrak{S}_k = \mathfrak{S} \otimes_A k$; il est immédiat que les diagrammes

$$(1)\quad \begin{array}{ccc} CW_A(\mathfrak{R}) & \xrightarrow{\hat{w}_{\mathfrak{R}}} & \mathfrak{R}_K \\ {\scriptstyle CW(\varphi)}\downarrow & & \downarrow{\scriptstyle \varphi_K} \\ CW_A(\mathfrak{S}) & \xrightarrow{\hat{w}_{\mathfrak{S}}} & \mathfrak{S}_K \end{array} \qquad (1')\quad \begin{array}{ccc} CW_k(\mathfrak{R}_k) & \xrightarrow{w_{\mathfrak{R}}} & \mathfrak{R}_K/p\mathfrak{R} \\ {\scriptstyle CW(\varphi_k)}\downarrow & & \downarrow{\scriptstyle \tilde{\varphi}_K} \\ CW_k(\mathfrak{S}_k) & \xrightarrow{w_{\mathfrak{S}}} & \mathfrak{S}_K/p\mathfrak{S} \end{array}$$

sont commutatifs.

2.- L'application $w_{\mathfrak{R}}$ n'est, en général, ni injective, ni surjective. Toutefois, dans le cas où $\mathfrak{R}_k = k'$ est un corps parfait contenant k, on voit que $w_{\mathfrak{R}}$ n'est autre que l'application réciproque de K'/pA' (où $A' = W(k')$, $K' = \mathrm{Frac}(A')$) dans $CW_k(k')$ construite au n° 2.3 ; en particulier $w_{\mathfrak{R}}$ est alors un isomorphisme. Ceci reste, bien sûr, encore vrai dans le cas où $\mathfrak{R}_k$ est le produit d'un nombre fini de corps parfait contenant k.

5.3. Soit $\mathfrak{R}$ un anneau linéairement topologisé. Nous disons qu'un idéal I de $\mathfrak{R}$ est un <u>idéal co-p-adique</u> s'il est fermé et si l'anneau R/I, muni de la topologie quotient, est un anneau p-adique.

Nous disons qu'un anneau (resp. un A-anneau) est un <u>anneau pro-p-adique</u> (resp. un A-<u>anneau pro</u>-p-<u>adique</u>) si, en tant qu'anneau topologique, il s'identifie à $\varprojlim R/I$, pour I parcourant l'ensemble des idéaux co-p-adiques de $\mathfrak{R}$. En particulier, tout A-anneau pro-p-adique est un A-module topologique, sans torsion.

Soit $\mathfrak{R}$ un A-anneau pro-p-adique. Nous disons qu'une famille $\mathfrak{J}$ d'idéaux co-p-adiques de $\mathfrak{R}$ détermine la topologie de $\mathfrak{R}$ si les $I + p^n\mathfrak{R}$, pour $I \in \mathfrak{J}$ et $n \in \mathbb{N}$, forment un système fondamental de voisinages de 0 dans $\mathfrak{R}$. Il revient au même de dire que tout idéal ouvert de $\mathfrak{R}$ contient un idéal de la forme $I + p^n\mathfrak{R}$, avec $I \in \mathfrak{J}$ et $n \in \mathbb{N}$. S'il en est ainsi, $\mathfrak{R}$ s'identifie à $\varprojlim_{I\in\mathfrak{J}} \mathfrak{R}/I$.

Il est clair que, si $\mathfrak{R}$ est un A-anneau pro-p-adique, l'ensemble $\mathfrak{J}_{\mathfrak{R}}$ de tous les idéaux co-p-adiques de $\mathfrak{R}$ détermine la topologie de $\mathfrak{R}$.

Soit $\mathfrak{R}$ un A-anneau pro-p-adique et soit $\mathfrak{J}$ une famille d'idéaux co-p-adiques de $\mathfrak{R}$ qui détermine la topologie de $\mathfrak{R}$. Nous posons $\mathfrak{R}_K = \mathfrak{R} \otimes_A K$ et $\hat{\mathfrak{R}}_K^{\mathfrak{J}} = \varprojlim_{I\in\mathfrak{J}} (\mathfrak{R}/I) \otimes_A K = \varprojlim_{I\in\mathfrak{J}} (\mathfrak{R}_K/I\mathfrak{R}_K)$.

Si l'on munit chaque quotient $\mathfrak{R}_K/I\mathfrak{R}_K$, qui est un espace vectoriel sur K , de la topologie p-adique, $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$ devient un K-anneau topologique ; en tant que A-module, il est linéairement topologisé : c'est le séparé complété de $\mathfrak{R}_K$ pour la topologie définie en prenant comme système fondamental de voisinages de 0 les sous-A-modules de la forme $I\mathfrak{R}_K + p^n\mathfrak{R}$, pour $I \in \mathfrak{J}$, $n \in \mathbb{N}$. L'injection canonique de $\mathfrak{R}$ dans $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$ est continue.

Pour tout $I \in \mathfrak{J}$, on a, d'après la proposition 5.1, une application A-linéaire continue $\hat{w}_{\mathfrak{R}/I}$ de $CW_A(\mathfrak{R}/I)$ dans $(\mathfrak{R}/I)_K$. La commutativité du diagramme (1) permet de passer à la limite et on en déduit une application A-linéaire continue

$$\hat{w}_{\mathfrak{R}}^{\mathfrak{J}} : CW_A(\mathfrak{R}) \to \hat{\mathfrak{R}}_K^{\mathfrak{J}} .$$

Ici encore, si $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$, $\hat{w}_{\mathfrak{R}}^{\mathfrak{J}}(\underline{\hat{a}})$ est la somme de la série convergente de terme général $p^{-n}\hat{a}_{-n}^{p^n}$.

De même, si l'on pose $\mathfrak{R}_k = \mathfrak{R}/p\mathfrak{R}$, on définit, par passage au quotient, ou par passage à la limite en utilisant la commutativité du diagramme (1'), une application A-linéaire continue

$$w_{\mathfrak{R}}^{\mathfrak{J}} : CW_k(\mathfrak{R}_k) \to \hat{\mathfrak{R}}_K^{\mathfrak{J}}/p\mathfrak{R} .$$

Si $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW_k(\mathfrak{R}_k)$ et si $\hat{a}_{-n}$ est un relèvement de a_{-n} dans $\mathfrak{R}$, $w_{\mathfrak{R}}^{\mathfrak{J}}(\underline{a})$ est l'image dans $\mathfrak{R}_K^{\mathfrak{J}}/p\mathfrak{R}$ de la somme de la série de terme général $p^{-n}\hat{a}_{-n}^{p^n}$.

5.4. La construction de l'anneau $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$, associé à un A-anneau pro-p-adique $\mathfrak{R}$ et à une famille $\mathfrak{J}$ d'idéaux co-p-adiques de $\mathfrak{R}$ qui détermine la topologie de $\mathfrak{R}$, présente deux inconvénients :

- la structure de $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$ dépend, en général, de manière considérable, du choix de la famille $\mathfrak{J}$;
- si on choisit pour $\mathfrak{J}$ l'ensemble de tous les idéaux co-p-adiques de $\mathfrak{R}$, l'anneau $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$ obtenu est en général "énorme" et peu maniable.

On est alors conduit à remplacer $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$ par un anneau plus agréable, l'anneau $\hat{\mathfrak{R}}_K^{an}$ des "fonctions analytiques", qui s'identifie à un sous-anneau de chacun des $\hat{\mathfrak{R}}_K^{\mathfrak{J}}$.

Pour simplifier, nous n'allons donner la construction de $\hat{\mathfrak{R}}_K^{an}$ que dans le cas particulier où nous en aurons effectivement besoin :

dans toute la fin de ce paragraphe, on note K' une extension finie totalement ramifiée du corps K , e le degré de l'extension, A' l'anneau des entiers de K' , π une uniformisante de A' .

Nous allons définir l'anneau $\hat{\mathfrak{R}}_K^{an}$ lorsque $\mathfrak{R}$ est un A'-anneau profini, formellement lisse, "localement de dimension finie", autrement dit, $\mathfrak{R}$ est un A'-anneau profini et chaque composante locale de $\mathfrak{R}$ est isomorphe à un anneau de séries formelles, à un nombre fini d'indéterminées, à coefficients dans l'anneau des entiers d'une extension finie non ramifiée de K' . Pour alléger l'écriture, un tel anneau est appelé, dans la fin de ce paragraphe, un A'-<u>anneau spécial</u>.

Soit $\mathfrak{R}$ un A'-anneau spécial et soit $\mathfrak{R}_K = \mathfrak{R} \otimes_A K = \mathfrak{R} \otimes_{A'} K'$.

- Supposons d'abord que $\mathfrak{R}$ est un anneau local et soit $\mathfrak{m}_{\mathfrak{R}}$ son idéal maximal. Pour tout entier $s \geq 1$, soit J_s le sous-A'-module de $\mathfrak{R}_K$ défini par $J_s = \sum_{n=1}^{\infty} \pi^{-n+1} \mathfrak{m}_{\mathfrak{R}}^{ns}$. On note $\hat{\mathfrak{R}}_K^{an}$ le séparé complété du A'-module R_K pour la topologie linéaire définie en prenant les J_s comme système fondamental de voisinages ouverts de 0 ; on a donc $\hat{\mathfrak{R}}_K^{an} = \varprojlim \mathfrak{R}_K/J_s$, chaque quotient étant muni de la topologie discrète. On voit tout de suite que $J_s . J_s \subset J_s$ et que $\pi^{-t} J_s \subset J_{s'}$ si $(t+1)s' \leq s$; on en déduit immédiatement que le produit dans $\mathfrak{R}_K$ est continu, d'où une structure de K'-anneau topologique sur $\hat{\mathfrak{R}}_K^{an}$ (la topologie de K' étant la topologie p-adique ; on voit que $\hat{\mathfrak{R}}_K^{an}$ est linéairement topologisé en tant que A'-module, mais pas en tant qu'anneau).

- Si $\mathfrak{R}$ est un A'-anneau spécial quelconque, et si $\mathfrak{R} = \prod \mathfrak{R}_{\mathfrak{m}}$ est la décomposition de $\mathfrak{R}$ en produits d'anneaux locaux, on pose $\hat{\mathfrak{R}}_K^{an} = \prod (\mathfrak{R}_{\mathfrak{m}})_K^{an}$. C'est donc un K'-anneau topologique, séparé et complet, et c'est un A'-module linéairement topologisé.

PROPOSITION 5.2.-

i) <u>Si $\mathfrak{R}$ est un A'-anneau spécial, l'application canonique de $\mathfrak{R}$ dans $\hat{\mathfrak{R}}_K^{an}$ est continue et injective</u>.

ii) <u>Si $\mathfrak{R}$ et $\mathfrak{S}$ sont deux A'-anneaux spéciaux</u>, $(\mathfrak{R} \hat{\otimes}_{A'} \mathfrak{S})_K^{an}$ <u>s'identifie canoniquement à</u> $\hat{\mathfrak{R}}_K^{an} \hat{\otimes}_{A'} \hat{\mathfrak{S}}_K^{an}$ (<u>ce qui a un sens car</u> $\hat{\mathfrak{R}}_K^{an}$ <u>et</u> $\hat{\mathfrak{S}}_K^{an}$ <u>sont des A'-modules linéairement topologisés</u>).

iii) <u>La correspondance $\mathfrak{R} \mapsto \hat{\mathfrak{R}}_K^{an}$ est fonctorielle ; plus précisément, si $\varphi : \mathfrak{R} \to \mathfrak{S}$ est un homomorphisme continu de A'-anneaux spéciaux, il existe un homomorphisme continu et un seul de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{S}}_K^{an}$ qui prolonge</u> φ .

Nous allons d'abord donner une description "explicite" de $\hat{\mathfrak{R}}_K^{an}$ lorsque le A'-anneau spécial $\mathfrak{R}$ est un anneau local. Dans ce cas, soit I un idéal de $\mathfrak{R}$ qui est un élément maximal de l'ensemble des idéaux co-p-adiques de $\mathfrak{R}$ et soit A" l'anneau-quotient $\mathfrak{R}/I$. On voit que A" est l'anneau des entiers d'une extension finie non ramifiée K" de K' et que, si l'on choisit un système minimal de générateurs $X_1, X_2, \dots, X_d$ de I , l'anneau $\mathfrak{R}$ s'identifie à $A''[[\underline{X}]] = A''[[X_1, X_2, \dots, X_d]]$. Soit $\hat{\mathfrak{R}}_K^I$ le K'-anneau topologique $\varprojlim \mathfrak{R}_K / I^m \mathfrak{R}_K$, chaque quotient, qui est un espace vectoriel de dimension finie sur le corps K' étant muni de la topologie p-adique (dans la terminologie du n° 5.3, on a $\hat{\mathfrak{R}}_K^I = \hat{\mathfrak{R}}_K^{\mathfrak{J}}$, avec $\mathfrak{J} = (I^m)_{m \in \mathbb{N}}$). Il est clair que $\hat{\mathfrak{R}}_K^I$ s'identifie à l'anneau

$K''[[\underline{X}]] = K''[[X_1,X_2,\dots,X_d]]$.

LEMME 5.3.- Reprenons les hypothèses et les notations qui précèdent. La topologie de $\mathfrak{R}_K$ définie par les J_s est plus fine que celle qui est définie par les $I^m + p^n\mathfrak{R}$. On en déduit une application continue de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^{I}$. Celle-ci est injective et son image est formée des éléments de $\hat{\mathfrak{R}}_K^{I}$ qui peuvent s'écrire sous la forme $\sum_{n=0}^{\infty} \pi^{-\nu_n} u_n$, avec $u_n \in I^n$, pour tout n , et les ν_n sont des entiers tels que, pour tout $\epsilon > 0$, la suite des $-\nu_n + n\epsilon$ tend vers l'infini.

Remarque : la dernière assertion signifie que l'image de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^{I}$ est formée des séries formelles $f(X_1,\dots,X_d)$, à coefficients dans K'' , qui sont telles, que pour tout d-uple $(x_1,x_2,\dots,x_d)$ formé d'éléments appartenant à l'idéal maximal de l'anneau des entiers du complété C d'une clôture algébrique de K'' , la série $f(x_1,x_2,\dots,x_d)$ est convergente dans C .

Démonstration du lemme : pour tout $\underline{i} = (i_1,i_2,\dots,i_d) \in \mathbb{N}^d$, posons $\underline{X}^{\underline{i}} = X_1^{i_1}X_2^{i_2}\dots X_d^{i_d}$ et $|\underline{i}| = i_1 + i_2 + \dots + i_d$. On voit que tout élément de $\hat{\mathfrak{R}}_K^{I}$ s'écrit, d'une manière et d'une seule sous la forme

$$\sum_{\underline{i}\in\mathbb{N}^d} a_{\underline{i}}\underline{X}^{\underline{i}} ,$$

avec les $a_{\underline{i}} \in K''$, et que $\mathfrak{R}$ (resp. $\mathfrak{R}_K$) s'identifie au sous-anneau de $\hat{\mathfrak{R}}_K^{I}$ formé des $\sum a_{\underline{i}}\underline{X}^{\underline{i}}$ tels que $a_{\underline{i}} \in A''$ pour tout $\underline{i}$ (resp. tels que les $a_{\underline{i}}$ sont à dénominateurs bornés).

On voit aussi que l'idéal maximal de $\mathfrak{R}$ est $\mathfrak{m}_{\mathfrak{R}} = (\pi,I) = (\pi,X_1,\dots,X_d)$ et on en déduit que, pour tout entier $r \geq 1$, $\mathfrak{m}_{\mathfrak{R}}^r$ est l'idéal engendré par les $\pi^{r-|\underline{i}|}\underline{X}^{\underline{i}}$, pour $0 \leq |\underline{i}| \leq r$; autrement dit $\mathfrak{m}_{\mathfrak{R}}^r$ est un sous-A"-module fermé de $\mathfrak{R}$, topologiquement libre, admettant comme base topologique les $\pi^{r-|\underline{i}|}\underline{X}^{\underline{i}}$, pour $0 \leq |\underline{i}| \leq r$, et les $\underline{X}^{\underline{i}}$, pour $|\underline{i}| > r$.

Soit maintenant s un entier ≥ 1 ; si $n \geq 1$, on voit que $\pi^{-n+1}\mathfrak{m}_{\mathfrak{R}}^{ns}$ est un sous-A"-module fermé de $\hat{\mathfrak{R}}_K^{I}$, topologiquement libre, admettant comme base topologique les $\pi^{ns-|\underline{i}|-n+1}\underline{X}^{\underline{i}}$, pour $0 \leq |\underline{i}| \leq ns$, et les $\pi^{-n+1}\underline{X}^{\underline{i}}$, pour $|\underline{i}| > ns$. On en déduit facilement que J_s est formé des éléments $\sum a_{\underline{i}}\underline{X}^{\underline{i}}$ de $\mathfrak{R}_K$ vérifiant

$$\begin{cases} (1_a) \quad \text{si} \quad |\underline{i}| \leq s , \quad v(a_{\underline{i}}) \geq s - |\underline{i}| , \\ (1_b) \quad \text{si} \quad ms \leq |\underline{i}| < (m+1)s , \quad v(a_{\underline{i}}) \geq -m+1 , \text{ pour } m \text{ entier } \geq 1 , \end{cases}$$

où l'on a noté v la valuation de K'' normalisée par $v(\pi) = 1$.

Soit $u_j = \sum a_{\underline{i},j} \underline{X}^{\underline{i}}$, pour $j \in \mathbb{N}$, une suite d'éléments de $\mathfrak{R}_K$ qui est une suite de Cauchy pour la topologie définie par les J_s . La condition (1_a) implique que, pour $\underline{i}$ fixé , la suite des $a_{\underline{i},j}$ converge dans K'' ; ceci signifie que la suite des u_j est aussi une suite de Cauchy pour la topologie définie par les $I^m + p^n\mathfrak{R}$; par conséquent, la première topologie est plus fine que la seconde, et on voit immédiatement que l'application de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^I$ que l'on en déduit est injective.

Soit $\overline{J}_s$ l'adhérence de J_s dans $\hat{\mathfrak{R}}_K^I$ (pour la topologie définie par les $I^m + p^nR$) : il est clair que $\overline{J}_s$ est formé des $\sum a_{\underline{i}} \underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^I$ qui vérifient les conditions (1_a) et (1_b) . Un élément $\sum a_{\underline{i}} \underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^I$ est dans l'image de $\hat{\mathfrak{R}}_K^{an}$ si et seulement s'il est congru, modulo chaque $\overline{J}_s$, à un élément de $\mathfrak{R}_K$.

On voit facilement que tout élément de $\hat{\mathfrak{R}}_K^I$ qui n'est pas dans $\mathfrak{R}_K$ peut s'écrire sous la forme $\sum_{j=0}^{\infty} \pi^{-\lambda_j} u_{n_j}$ où

- les λ_j forment une suite strictement croissante d'entiers ≥ 0 ,
- les n_j forment une suite strictement croissante d'entiers ≥ 0 ,
- pour tout j , $u_{n_j} \in I^{n_j}$, et, si $j \geq 1$, le terme homogène de degré n_j en $X_1,\ldots,X_d$ de u_{n_j} n'a pas tous ses coefficients divisibles par π .

Supposons qu'un tel élément soit dans l'image de $\hat{\mathfrak{R}}_K^{an}$; on voit que, pour tout $s \geq 1$, presque tous les $\pi^{-\lambda_j} u_{n_j}$ sont dans $\overline{J}_s$. Mais, pour $j \geq 1$, $\pi^{-\lambda_j} u_{n_j} \in \overline{J}_s$ implique que $-\lambda_j \geq -m+1$ si $n_j < (m+1)s$ donc que $-\lambda_j + (n_j/s) > 2$. Par conséquent, pour tout $s \geq 1$, on a $-\lambda_j + (n_j/s) > 2$, pour presque tout j ; il est clair que ceci implique que, pour tout $\epsilon > 0$, la suite des $-\lambda_j + n_j\epsilon$ tend vers l'infini, et l'élément considéré est bien de la forme indiquée dans le lemme.

Réciproquement, soit $\alpha = \sum_{n=0}^{\infty} \pi^{-\nu_n} u_n$ un élément de $\hat{\mathfrak{R}}_K^I$ avec $u_n \in I^n$, pour tout n , et $-\nu_n + n\epsilon$ tend vers l'infini, pour tout $\epsilon > 0$ fixé. On a alors, pour s fixé, $-\nu_n \geq -(n/s)+1$, pour presque tout n ; ce qui, d'après (1_b) implique que $\pi^{-\nu_n} u_n \in \overline{J}_s$; on en déduit que l'élément considéré est bien dans l'image de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^I$.

Compte-tenu du lemme précédent, la proposition 5.2, est essentiellement triviale lorsque les A'-anneaux spéciaux qui interviennent sont des anneaux locaux ; le cas général s'en déduit en décomposant les anneaux spéciaux qui interviennent en produits d'anneaux locaux.

5.5. Soit $\mathfrak{R}$ un A'-anneau spécial. Notons $\Omega_{A'}(\mathfrak{R})$ (resp. $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$) le A'-module des A'-différentielles continues de $\mathfrak{R}$ (resp. $\hat{\mathfrak{R}}_K^{an}$) . L'injection canonique de $\mathfrak{R}$ dans $\hat{\mathfrak{R}}_K^{an}$ induit une application A'-linéaire de $\Omega_{A'}(\mathfrak{R})$ dans $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$; on voit que celle-ci est injective, et nous l'utilisons pour identifier $\Omega_{A'}(\mathfrak{R})$ à un sous-module de $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$. Si d désigne l'application canonique de $\hat{\mathfrak{R}}_K^{an}$ dans $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$, nous notons $P(\mathfrak{R})$ l'ensemble des éléments $\alpha \in \hat{\mathfrak{R}}_K^{an}$ tels que $d\alpha \in \Omega_{A'}(\mathfrak{R})$. Il est clair que c'est un sous-A'-module fermé de $\hat{\mathfrak{R}}_K^{an}$.

Supposons $\mathfrak{R}$ local et choisissons des coordonnées $X_1, X_2, \ldots, X_d$. Alors $\mathfrak{R}$ s'identifie à l'anneau $A''[[X_1, X_2, \ldots, X_d]]$ des séries formelles en les X_i à coefficients dans A'' , anneau des entiers d'une extension finie non ramifiée K'' de K' . Utilisons le lemme 5.3 pour identifier $\hat{\mathfrak{R}}_K^{an}$ à un sous-anneau de $K''[[X_1, X_2, \ldots, X_d]] = \hat{\mathfrak{R}}_K^I$.

Soit $\alpha = \sum a_{\underline{i}} \underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^I$. On voit que $\alpha \in P(\mathfrak{R})$ si et seulement si les deux conditions suivantes sont satisfaites :

$$\left\{\begin{array}{ll} (2_a) & \text{on a } \alpha \in \hat{\mathfrak{R}}_K^{an} , \\ (2_b) & \text{pour tout } \underline{i} = (i_1, i_2, \ldots, i_d) \in \mathbb{N}^d \text{ et tout } j \in \{1, 2, \ldots, d\} , \text{ on a} \\ & i_j a_{\underline{i}} \in A'' . \end{array}\right.$$

Soit v_n la composante homogène de degré n en les X_j de α . La condition (2_b) implique que si r_n est le plus grand entier tel que $p^{r_n} \leq n$, alors $p^{r_n} v_n \in \mathfrak{R}$; si on pose $u_n = p^{r_n} v_n$, on voit que $\alpha = \sum_{n=0}^{\infty} p^{-r_n} u_n$, avec $u_n \in I^n$; comme il est clair que, pour tout $\varepsilon > 0$, la suite des $-r_n + n\varepsilon$ tend vers l'infini, il résulte du lemme 5.3 que la condition (2_b) implique la condition (2_a) .

Pour tout $\underline{i} = (i_1, i_2, \ldots, i_d) \in \mathbb{N}^d$, $\neq 0 = (0, 0, \ldots, 0)$, notons $h(\underline{i})$ le plus grand entier h tel que p^h divise tous les i_j . On voit que $P(\mathfrak{R})$ est la somme directe de K'' et d'un A''-module topologiquement libre admettant comme base topologique les $p^{-h(\underline{i})} \underline{X}^{\underline{i}}$, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$.

Si nous revenons maintenant au cas où $\mathfrak{R}$ est un A'-anneau spécial quelconque, et si $\mathfrak{R} = \prod \mathfrak{R}_m$ représente la décomposition de $\mathfrak{R}$ en le produit de ses composantes locales, on voit que $P(\mathfrak{R}) = \prod P(\mathfrak{R}_m)$.

5.6. PROPOSITION 5.4.- <u>Soit</u> $\mathfrak{R}$ <u>un A'anneau spécial. Soit</u> $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$. <u>La série de terme général</u> $p^{-n}\hat{a}_{-n}^{p^n}$ <u>converge dans</u> $\hat{\mathfrak{R}}_K^{an}$. <u>Notons</u> $\hat{w}_{\mathfrak{R}}(\underline{\hat{a}})$ <u>la somme de cette série. L'application</u> $\hat{w}_{\mathfrak{R}} : CW_A(\mathfrak{R}) \to \hat{\mathfrak{R}}_K^{an}$ <u>ainsi définie est A-linéaire continue et son image est contenue dans</u> $P(\mathfrak{R})$.

<u>Remarque</u> : la notation $\hat{w}_{\mathfrak{R}}$ ne crée pas de risque de confusion avec la notation employée pour la proposition 5.1 : si $\mathfrak{R}$ est un A'-anneau spécial qui est aussi un A-anneau-p-adique, $\mathfrak{R}$ est un produit fini d'extensions finies non ramifiées de K' , $\mathfrak{R}_K$ s'identifie à $\hat{\mathfrak{R}}_K^{an}$ et les deux définitions de $\hat{w}_{\mathfrak{R}}$ coïncident.

<u>Démonstration</u> : en décomposant $\mathfrak{R}$ en le produit de ses composantes locales, on se ramène au cas où l'anneau spécial est local. Supposons qu'il en est ainsi et reprenons les notations qui précèdent.

Si $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathfrak{R})$, on voit que, pour n suffisamment grand, $\hat{a}_{-n} \in \mathfrak{m}_{\mathfrak{R}}$, donc que $p^{-n}\hat{a}_{-n}^{p^n} \in p^{-n}\mathfrak{m}_{\mathfrak{R}}^{p^n} \subset p^{-n}\mathfrak{m}_{\mathfrak{R}}^{(n+1)s} \subset J_s$, si $p^n > (n+1)s$; pour s fixé, ceci est vrai pour tout n suffisamment grand ; la convergence de la série en résulte.

Si $\underline{\hat{a}}_m = (\ldots,\hat{a}_{m,-n},\ldots,\hat{a}_{m,0})$, pour $m \in \mathbb{N}$, est une suite d'éléments de $CW_A(\mathfrak{R})$ convergent vers un élément $\underline{\hat{a}} = (\ldots,\hat{a}_{-n},\ldots,\hat{a}_0)$, on voit que

- d'une part, il existe un entier r , indépendant de m , tel que les $\hat{a}_{m,-n}$ et $\hat{a}_{-n}$ sont dans $\mathfrak{m}_{\mathfrak{R}}$, pour $n \geq r$;
- d'autre part, pour n fixé, la suite des $\hat{a}_{m,-n}$ converge, dans $\mathfrak{R}$, vers $\hat{a}_{-n}$.

Soit s un entier ≥ 1 . La première condition montre qu'il existe un entier n_0 , indépendant de m , tel que les $p^{-n}\hat{a}_{m,-n}^{p^n}$ et $p^{-n}\hat{a}_{-n}^{p^n}$ sont dans J_s , pour $n \geq n_0$. La deuxième implique qu'il existe un entier m_0 tel que, si $m \geq m_0$, $p^{-n}\hat{a}_{m,-n}^{p^n} \equiv p^{-n}\hat{a}_{-n}^{p^n} \pmod{J_s}$, pour $n < n_0$. La continuité de l'application $\hat{w}_{\mathfrak{R}}$ s'en déduit.

On voit que $CW^u(\mathfrak{R})$ est dense dans $CW_A(\mathfrak{R})$. Le fait que la restriction de $\hat{w}_{\mathfrak{R}}$ à $CW^u(\mathfrak{R})$ est A-linéaire résulte immédiatement des définitions ; la linéarité de $\hat{w}_{\mathfrak{R}}$ s'en déduit, par continuité.

Tout élément α de $\hat{\mathfrak{R}}_K^{an}$ qui est dans l'image de $\hat{w}_{\mathfrak{R}}$ s'écrit sous la forme $\sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n}$; on a donc $d\alpha = \sum \hat{a}_{-n}^{p^n-1} d\hat{a}_{-n} \in \Omega_{A'}(\mathfrak{R})$ et $\alpha \in P(\mathfrak{R})$, d'où la proposition.

5.7. Revenons sur les vecteurs de Witt : soit $\mathfrak{R}$ un A-anneau spécial. Posons $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. C'est un k-anneau profini. L'application canonique de $\mathfrak{R}$ sur $\mathfrak{R}_k$ induit une application de $CW_A(\mathfrak{R}) = CW(\mathfrak{R})$ dans $CW(\mathfrak{R}_k) = \widehat{CW}_k(\mathfrak{R}_k)$. Il est clair que c'est une application A-linéaire continue surjective et que son noyau $CW_A(p\mathfrak{R})$ est formé des covecteurs dont toutes les composantes sont dans l'idéal $p\mathfrak{R}$.

Si $a \in \mathfrak{R}$, pour tout entier $n \geq 0$, $p^{-n}(pa)^{p^n} \in p^{p^n-n}\mathfrak{R} \subset p\mathfrak{R}$; on en déduit que l'image de $CW_A(p\mathfrak{R})$ par $\hat{w}_{\mathfrak{R}}$ est contenue dans $p\mathfrak{R}$. L'application $\hat{w}_{\mathfrak{R}}$ définit donc, par passage aux quotients, une application A-linéaire continue $w_{\mathfrak{R}}$ de $CW_k(\mathfrak{R}_k)$ dans $P(\mathfrak{R})/p\mathfrak{R}$.

PROPOSITION 5.5.- <u>Soit</u> $\mathfrak{R}$ <u>un A-anneau spécial. L'application A-linéaire continue</u> $w_{\mathfrak{R}} : CW_k(\mathfrak{R}_k) \to P(\mathfrak{R})/p\mathfrak{R}$ <u>définie ci-dessus est un isomorphisme</u>.

<u>Démonstration</u> : en décomposant $\mathfrak{R}$ en le produit de ses composantes locales, on se ramène au cas où $\mathfrak{R}$ est local. En reprenant les notations du n° 5.5, on voit que, si l'on choisit des coordonnées, $\mathfrak{R}$ s'identifie à $A''[[X_1,X_2,\dots,X_d]]$ où A'' est l'anneau des entiers d'une extension non ramifiée K'' de K .

On sait (cf. n° 5.5) qu'une fois les coordonnées choisies, $P(\mathfrak{R})$ est la somme directe de K'' et d'un A''-module topologiquement libre $P^c(\mathfrak{R})$ admettant comme base topologique les $p^{-h(\underline{i})}\underline{X}^{\underline{i}}$, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$. En particulier $P(\mathfrak{R})$ est un A''-module pro-artinien, et il en est de même de $P(\mathfrak{R})/p\mathfrak{R}$ qui est la somme directe de K''/pA'' et de $P^c(\mathfrak{R})/(p\mathfrak{R}) \cap P^c(\mathfrak{R})$.

Si k'' désigne le corps résiduel de A'' , on voit que $\mathfrak{R}_k$ s'identifie à $k''[[X_1,X_2,\dots,X_d]]$; on a donc $\widehat{CW}_k(\mathfrak{R}_k) = \widehat{CW}_{k''}(\mathfrak{R}_k)$ et c'est aussi un A''-module pro-artinien (cf. prop. 4.1). On voit que $\widehat{CW}_k^{et}(\mathfrak{R}_k) = \widehat{CW}_k(k'')$ s'identifie par $w_{\mathfrak{R}}$ à K''/pA'' (cf. n° 2.3) ; d'autre part, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$, posons $\underline{i}' = p^{-h(\underline{i})}\underline{i}$; on voit que l'image par $w_{\mathfrak{R}}$ du covecteur $(\dots,0,\dots,0,\underline{X}^{\underline{i}'},0,\dots,0)$ (où la seule composante non nulle est celle d'indice

$-h(\underline{i})$) est l'image dans $P(\mathfrak{R})/p\mathfrak{R}$ de $p^{-h(\underline{i})}\underline{X}^{\underline{i}}$. On en déduit que l'image de $w_{\mathfrak{R}}$ est dense dans $P(\mathfrak{R})/p\mathfrak{R}$, donc que $w_{\mathfrak{R}}$ est surjective puisque c'est une application A"-linéaire continue d'un A"-module pro-artinien dans un autre.

Montrons l'injectivité. Pour cela, si $a = \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}} \in \mathfrak{R}_k$ (avec les $a_{\underline{i}} \in k"$), notons $\hat{a}$ le relèvement de a dans $\mathfrak{R}$ défini par $\hat{a} = \sum [a_{\underline{i}}] \underline{X}^{\underline{i}}$ (où $[a_{\underline{i}}]$ désigne le représentant multiplicatif de $a_{\underline{i}}$ dans $A" = W(k")$). Si l'on note v la valuation $\underline{X}$-adique dans $\mathfrak{R}_k$ et $\hat{v}$ la valuation $\underline{X}$-adique dans $\mathfrak{R}$ et dans $K"[[X_1,\dots,X_d]]$, on a donc, pour tout $a \in \mathfrak{R}_k$, $\hat{v}(\hat{a}) = v(a)$.

On a déjà dit que $w_{\mathfrak{R}}$ induit un isomorphisme de $\widehat{CW}_k^{et}(\mathfrak{R}_k)$ sur $K"/pA"$; on a $\widehat{CW}_k(\mathfrak{R}_k) = \widehat{CW}_k^{et}(\mathfrak{R}_k) \oplus \widehat{CW}_k^{c}(\mathfrak{R}_k)$ et l'on voit que $\widehat{CW}_k^{c}(\mathfrak{R}_k)$ est formé des covecteurs $\underline{a} = (\dots,a_{-n},\dots,a_0)$ vérifiant $v(a_{-n}) \geq 1$, pour tout n ; pour un tel covecteur, on voit que $\alpha = \sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n} \in P^c(\mathfrak{R})$; pour achever la démonstration de l'injectivité, il suffit donc de montrer que si $\underline{a} \neq 0$, alors $\alpha \notin p\mathfrak{R}$. Pour cela, commençons par établir un lemme :

LEMME 5.6.- <u>Avec les hypothèses et les notations qui précèdent, si</u> $\alpha \in p\mathfrak{R}$, <u>pour tout</u> $m \in \mathbb{N}$ <u>tel que</u> $a_{-m} \neq 0$, <u>il existe</u> $m' \in \mathbb{N}$ <u>tel que</u> $v(a_{-m'}) \leq p^{-1}v(a_{-m})$.

<u>Démonstration du lemme</u> : il est clair que $\alpha \equiv \sum_{n=m}^{\infty} p^{-n}\hat{a}_{-n}^{p^n} \pmod{p^{-m+1}\mathfrak{R}}$. On a $\hat{v}\left(\hat{a}_{-m}^{p^m}\right) = p^m\hat{v}(\hat{a}_{-m}) = p^m v(a_{-m})$ et $p^{-m}\hat{a}_{-m}^{p^m}$ "commence" par un polynôme homogène en les X_j , de degré $p^m v(a_{-m})$, à coefficients dans $K"$, dont les coefficients ne sont pas tous dans $p^{-m+1}A"$. Il doit donc exister un entier $m' > m$ tel que $\hat{v}\left(p^{-m'}\hat{a}_{-m'}^{p^{m'}}\right) \leq p^m\hat{v}(a_{-m})$, i.e. tel que $p^{m'}v(a_{-m'}) \leq p^m v(a_{-m})$; comme $m' \geq m+1$, on a donc $v(a_{-m'}) \leq p^{-1}v(a_{-m})$.

<u>Fin de la démonstration de la proposition</u> : si, avec les notations qui précèdent, il existait $\underline{a} \in \widehat{CW}_k^{c}(\mathfrak{R}_k)$, $\underline{a} \neq 0$, tel que $\alpha \in p\mathfrak{R}$, l'hypothèse $\underline{a} \neq 0$ impliquerait l'existence d'un entier m_0 tel que $a_{-m_0} \neq 0$; on pourrait alors construire par récurrence, en utilisant le lemme, une suite d'entiers $m_0, m_1, \dots, m_i, \dots$ telle que $v\left(a_{-m_{i+1}}\right) \leq p^{-1}v\left(a_{-m_i}\right)$, pour tout i , ce qui contredit le fait que $v(a_{-n}) \geq 1$, pour tout n .

<u>Remarque</u> : soit σ le Frobenius absolu sur k et sur $A = W(k)$ et soit $\tau = \sigma^{-1}$. Pour tout k-anneau fini ou profini R , notons $\widehat{CW}_k^{\tau}(R)$ le A-module déduit de $\widehat{CW}_k(R)$ par l'extension des scalaires $\tau : A \to A$ (autrement dit $\widehat{CW}_k^{\tau}(R)$ s'identifie à $\widehat{CW}_k(R)$ comme groupe abélien et, si $\lambda \in A$ et

$\underline{a} \in \widehat{CW}_k(R)$, multiplier λ par $\underline{a}$ dans $\widehat{CW}_k^{\tau}(R)$ revient à multiplier $\tau(\lambda)$ par $\underline{a}$ dans $\widehat{CW}_k(R)$). On voit que l'on peut aussi décrire $\widehat{CW}_k^{\tau}(R)$ comme étant l'ensemble des covecteurs $(\ldots,a_{-n},\ldots,a_{-1})$ où les a_{-n} (indexés par les entiers strictement négatifs) vérifient les mêmes conditions que celles demandées pour $\widehat{CW}_k(R)$, l'addition et la multiplication par un scalaire étant données par les mêmes formules. On voit aussi que, avec ces conventions, l'application

$$(\ldots,a_{-n},\ldots,a_{-1},a_0) \longmapsto (\ldots,a_{-n},\ldots,a_{-1})$$

permet d'identifier le A-module $\widehat{CW}_k^{\tau}(R)$ au quotient de $\widehat{CW}_k(R)$ par le sous-module formé des covecteurs de la forme $(\ldots,0,\ldots,0,a_0)$, i.e. le noyau de $\underline{V}$.

Si R est réduit (en particulier si $R = \mathfrak{R}_k$ où $\mathfrak{R}$ est un A'-anneau spécial), on voit que le noyau de $\underline{V}$ est aussi le noyau de p .

Dans le cas où $R = \mathfrak{R}_k$, avec $\mathfrak{R}$ un A-anneau spécial, on voit donc que l'application $w_{\mathfrak{R}}$ induit un isomorphisme $w_{\mathfrak{R}}^{\tau}$ de $\widehat{CW}_k^{\tau}(R_k)$ sur $P(\mathfrak{R})/\mathfrak{R}$.

§ 6.- Groupe de Cartier et exponentielle d'Artin-Hasse.

6.1. Pour tout anneau commutatif R , nous notons $\Lambda(R) = R[[T]]$ l'anneau des séries formelles en une variable T , à coefficients dans R , et $C(R)$ le groupe multiplicatif des éléments de $\Lambda(R)$ congrus à 1 modulo l'idéal engendré par T .

On voit que C est, de manière naturelle, un $\mathbb{Z}$-foncteur en groupes ; il est clair que c'est un $\mathbb{Z}$-groupe affine lisse.

Soit $\mu : \mathbb{N}^* \to \{0,-1,+1\}$ la fonction de Möbius :

$$\mu(n) = \begin{cases} 1 & \text{si } n=1 , \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts,} \\ 0 & \text{dans les autres cas.} \end{cases}$$

Soit $\mathbb{Z}_{(p)}$ le localisé en p de l'anneau $\mathbb{Z}$. Nous notons $F(T)$ l'élément de l'anneau $\Lambda(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}[[T]]$ défini par

$$F(T) = \prod_{\substack{n\geq 1 \\ (n,p)=1}} (1-T^n)^{n^{-1}\mu(n)} .$$

Soit R un $\mathbb{Z}_{(p)}$-anneau. Pour tout $\underline{a} = (a_0,a_1,\ldots,a_n,\ldots) \in W(R)$, notons $E_R(\underline{a})$ l'élément de $C(R)$ défini par

$$E_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_n T^{p^n}) \ .$$

On sait (cf. par exemple, [15], chap. III, § 1) que E_R est un homomorphisme injectif du groupe $W(R)$ dans le groupe $C(R)$ et il est clair que E_R est fonctoriel en R . Autrement dit les E_R , pour R décrivant les $\mathbb{Z}_{(p)}$-anneaux, définissent un monomorphisme

$$E : W_{\mathbb{Z}_{(p)}} \longrightarrow C_{\mathbb{Z}_{(p)}}$$

de $\mathbb{Z}_{(p)}$-groupes affines.

6.2. Soit m un entier ≥ 1 . Notons $C^{(m)}(R)$ le sous-groupe de $C(R)$ formé des séries formelles congrues à 1 modulo l'idéal engendré par T^{p^m} . Il est clair que $C^{(m)}$ est un sous-$\mathbb{Z}$-groupe affine de C et que le quotient $C_m = C/C^{(m)}$ est encore un $\mathbb{Z}$-groupe affine lisse.

Si R est un $\mathbb{Z}_{(p)}$-anneau et si $\underline{a} = (a_0, \dots, a_n, \dots) \in W(R)$ est tel que $a_0 = a_1 = \dots = a_{m-1} = 0$, on voit que $E_R(\underline{a}) \in C^{(m)}(R)$. Par passage au quotient, on déduit donc de E un morphisme de $\mathbb{Z}_{(p)}$-groupes affines

$$E_m : (W_m)_{\mathbb{Z}_{(p)}} \longrightarrow (C_m)_{\mathbb{Z}_{(p)}} \ .$$

Pour tout anneau commutatif R et tout entier $m \geq 1$, notons $\Lambda_m(R)$ l'anneau quotient $\Lambda(R)/T^{p^m}\Lambda(R)$ et T_{-m+1} l'image de T dans $\Lambda_m(R)$. On voit que $C_m(R)$ s'identifie au groupe multiplicatif des éléments de l'anneau $\Lambda_m(R)$ qui sont congrus à 1 modulo l'idéal engendré par T_{-m+1} .

Si on identifie T_{-m+1} à T_{-m}^p , $\Lambda_m(R)$ s'identifie à un sous-anneau de $\Lambda_{m+1}(R)$; on en déduit un monomorphisme de C_m dans C_{m+1} ; nous notons CC^u le $\mathbb{Z}$-foncteur en groupes $\varinjlim C_m$. On voit que, pour tout anneau commutatif R , $CC^u(R)$ s'identifie au groupe multiplicatif des éléments de l'anneau $C\Lambda^u(R) = \varinjlim \Lambda_m(R)$ qui sont congrus à 1 modulo l'idéal engendré par les T_{-m} .

Il est clair que, pour tout m , le diagramme

$$\begin{array}{ccc}
(W_m)_{\mathbb{Z}_{(p)}} & \xrightarrow{E_m} & (C_m)_{\mathbb{Z}_{(p)}} \\
{\scriptstyle V_m}\downarrow & & \downarrow \\
(W_{m+1})_{\mathbb{Z}_{(p)}} & \xrightarrow{E_{m+1}} & (C_{m+1})_{\mathbb{Z}_{(p)}}
\end{array}$$

est commutatif. Par passage à la limite, on en déduit un morphisme de $\mathbb{Z}_{(p)}$-foncteurs en groupes

$$CE^u : CW^u_{\mathbb{Z}_{(p)}} \longrightarrow CC^u_{\mathbb{Z}_{(p)}} .$$

Si R est un $\mathbb{Z}_{(p)}$-anneau et si $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW^u(R)$, on voit que

$$CE^u_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_{-n}T_{-n})$$

expression qui a un sens car, pour n assez grand, $a_{-n} = 0$, donc $F(a_{-n}T_{-n}) = 1$.

6.3. Soit $S = \mathbb{N}[1/p]$ l'ensemble des nombres rationnels ≥ 0 dont le dénominateur est une puissance de p . Soit R un anneau commutatif. Tout élément du R-module R^S s'écrit, avec des notations évidentes, d'une manière et d'une seule, sous la forme

$$\sum_{s \in S} a_s \theta_s \ , \text{ avec les } a_s \in R .$$

Notons $B\Lambda(R)$ le sous-R-module de R^S formé des éléments $\sum a_s \theta_s$ qui satisfont la propriété suivante :

$$(\Phi) \qquad \begin{cases} \underline{\text{pour tout nombre réel}} \ r > 0 \ , \ \underline{\text{il existe}} \ \epsilon > 0 \ \underline{\text{tel que}} \ a_s = 0 \ , \\ \underline{\text{si}} \ r - \epsilon \leq s < r \ . \end{cases}$$

Soit $\alpha = \sum a_s \theta_s$ et $\beta = \sum b_s \theta_s$ deux éléments de $B\Lambda(R)$; on voit facilement que (Φ) implique, d'une part, que, pour tout $s \in S$, les $a_{s'} b_{s''}$ avec $s' + s'' = s$ sont presque tous nuls et, d'autre part, que, pour tout $r > 0$ il existe $\epsilon > 0$ tel que $a_{s'} b_{s''} = 0$ si $r - \epsilon \leq s' + s'' < r$; on peut donc définir un produit dans $B\Lambda(R)$ en posant

$$\alpha\beta = \sum_{s', s'' \in S} a_{s'} b_{s''} \theta_{s'+s''} .$$

On voit que l'on a ainsi muni $B\Lambda(R)$ d'une structure de R-anneau

Soit $C\Lambda(R)$ le quotient de l'anneau $B\Lambda(R)$ par l'idéal engendré par θ_p . Si l'on note $\overline{\theta}_s$ l'image de θ_s dans $C\Lambda(R)$, tout élément de $C\Lambda(R)$ s'écrit d'une manière et d'une seule sous la forme $\sum_{s \in S, s < p} a_s \overline{\theta}_s$, où les a_s sont dans R et vérifient (Φ) .

Nous notons $CC(R)$ le groupe multiplicatif des éléments de $C\Lambda(R)$ congrus à 1 modulo l'idéal engendré par les $\overline{\theta}_s$, pour $s > 0$. On voit que CC est de manière naturelle un $\mathbb{Z}$-foncteur en groupes.

Si l'on identifie T_{-n} et $\overline{\theta}_{1/p^n}$, on voit que $C\Lambda^u(R)$ s'identifie au sous-anneau de $C\Lambda(R)$ formé des $\sum a_s \overline{\theta}_s$ tels que les a_s sont presque tous nuls. En particulier CC^u s'identifie à un sous-$\mathbb{Z}$-foncteur en groupes de CC .

PROPOSITION 6.1.- Soit R un $\mathbb{Z}_{(p)}$-anneau commutatif.

i) Pour tout $\underline{a} = (\dots, a_{-n}, \dots, a_0) \in CW(R)$, le produit infini $\prod_{n=0}^{\infty} F(a_{-n}T_{-n})$ converge "ponctuellement" dans CC(R) (i.e. si $\prod_{n=0}^{m} F(a_{-n}T_{-n}) = \sum b_{m,s}\overline{\theta}_s$, la suite des $b_{m,s}$, pour s fixé est stationnaire).

ii) Pour tout $\underline{a} \in CW(R)$, posons $CE_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_{-n}T_{-n})$. L'application CE_R est un homomorphisme injectif du groupe CW(R) dans CC(R) .

Pour tout $\underline{i} = (i_n)_{n\in\mathbb{Z}} \in \mathbb{N}^{(\mathbb{Z})}$, posons $|\underline{i}| = \sum i_n$; pour tout $s \in S$, soit h(s) la somme des chiffres de s écrit "en base p ". Commençons par établir quelques lemmes élémentaires :

LEMME 6.2.- Soit m un entier > 0 et soit $s \in S$. Il n'y a qu'un nombre fini de $\underline{i} \in \mathbb{N}^{(\mathbb{Z})}$ tels que $\sum p^{-n} i_n = s$ et $|\underline{i}| < m$.

Démonstration : quitte à multiplier s par une puissance de p , on peut supposer que $s \in \mathbb{N}$. Soit r un entier tel que $s < p^{r+1}$; on a nécessairement $i_n = 0$ pour $n < -r$. Soit t le plus grand entier tel que $i_t \neq 0$. Si $t > 0$, $p^{-t}i_t + \dots + p^{-2}i_2 + p^{-1}i_1 \in \mathbb{N}$, donc $i_t + \dots + p^{t-2}i_2 + p^{t-1}i_1$ est divisible par p^t et, d'après le lemme 1.2, $i_t + \dots + i_2 + i_1 \geq (t-1)(p-1) + p$; on en déduit que $t < (m-1)/(p-1)$. On a donc nécessairement $i_n = 0$ si $n < -r$ ou si $n \geq (m-1)/(p-1)$. Le lemme est alors évident.

LEMME 6.3.- Soit $\underline{i} \in \mathbb{N}^{(\mathbb{Z})}$ et soit $s = \sum p^{-n} i_n$. Alors $|\underline{i}| \geq h(s)$.

Démonstration : soit $s = \sum p^{-n} j_n$, avec $0 \leq j_n < p$, l'écriture de s en base p . Il faut montrer que $\sum i_n \geq \sum j_n$. Quitte à multiplier par une puissance de p , on peut supposer que $i_n = j_n = 0$, pour $n > 0$. Procédons par récurrence sur le plus grand entier r tel que $j_{-r} \neq 0$:

- si $r = 0$, c'est clair ;
- dans le cas général, on voit que $i_0 = j_0 + pu$, avec $u \in \mathbb{N}$; on a donc

$j_{-1} + pj_{-2} + \ldots + p^{r-1} j_{-r} = (u+i_{-1}) + pi_{-2} + \ldots + p^{m-1} i_{-m} + \ldots$ et l'hypothèse de récurrence implique que $(u+i_{-1}) + i_{-2} + \ldots + i_{-m} + \ldots \geq j_{-1} + j_{-2} + \ldots + j_{-r}$; l'inégalité $i_0 + i_{-1} + \ldots + i_{-m} + \ldots \geq j_0 + j_{-1} + \ldots + j_{-r}$ s'en déduit immédiatement.

LEMME 6.4.- Soit $s, t \in S$. On a $h(s+t) \leq h(s) + h(t)$.

C'est une conséquence triviale du lemme précédent.

LEMME 6.5.- Soit m un entier > 0 et soit S_m l'ensemble des $s \in S$ vérifiant $h(s) < m$. Pour tout nombre réel $r > 0$, il existe $\varepsilon > 0$ tel que, si $s \in S_m$ vérifie $s < r$, alors $s \leq r - \varepsilon$.

Démonstration : il est clair qu'il suffit de montrer que, si

$s_1 < s_2 < \ldots < s_n < \ldots$

est une suite strictement croissante d'éléments de S tendant vers r, alors les $h(s_n)$ ne sont pas bornés.

Considérons l'écriture en base p de chacun des s_n :

$$s_n = \sum_{t \in \mathbb{Z}} p^{-t} c_{n,t}, \quad \text{avec les } c_{n,t} \text{ entiers presque tous nuls vérifiant } 0 \leq c_{n,t} < p.$$

On voit facilement que, pour t fixé, la suite des $c_{n,t}$ est stationnaire et que, si on note c_t sa limite, le nombre réel $r = \sum_{t \geq -\infty} p^{-t} c_t$ est égal à la limite des s_n. Comme la suite des s_n est strictement croissante, il y a une infinité de t tels que $c_t \neq 0$. La série de terme général c_t est donc divergente et les $h(s_n)$ ne sont pas bornés.

Démonstration de la proposition 6.1. : pour tout $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW(R)$, notons $r_{\underline{a}} = r$ le plus petit entier tel que l'idéal de R engendré par les a_{-n}, avec $n \geq r$, est nilpotent ; notons $\mathfrak{d}_{\underline{a}} = \mathfrak{d}$ cet idéal et $m_{\underline{a}} = m$ le plus petit entier ≥ 1 tel que $\mathfrak{d}^m = 0$.

Supposons d'abord que $r_{\underline{a}} = 0$. On voit que $F(a_{-n} T_{-n})$ est un polynôme de degré $< m$ en T_{-n} et que le coefficient de T^i_{-n} appartient à $\mathfrak{d}^i$. On en déduit que les monômes non nuls intervenant dans le développement du produit infini sont de la forme

$$a_{\underline{i}} . \prod_{n \in \mathbb{N}} T_{-n}^{i_n}, \quad \text{avec } |\underline{i}| = \sum i_n < m \text{ et } a_{\underline{i}} \in \mathfrak{d}_{\underline{a}}^{|\underline{i}|}.$$

On a $\prod T_{-n}^{i_n} = \overline{\theta}_s$, si $s = \sum p^{-n} i_n$. Pour s fixé, le coefficient de

$\overline{\theta}_s$ dans le produit infini est donc la somme $a'_s = \sum a_{\underline{i}}$, la sommation étant étendue aux $\underline{i}$ tel que $\sum p^{-n} i_n = s$ et $|\underline{i}| < m$; c'est une somme finie, d'après le lemme 6.2, d'où la convergence ponctuelle dans $R^{\overline{S}}$ (si $\overline{S} = \{s \in S \mid s < p\}$) ; de plus $a_{\underline{i}} \in \mathfrak{d}_{\underline{a}}^{|\underline{i}|} \subset \mathfrak{d}_{\underline{a}}^{h(s)}$, d'après le lemme 6.3, et on peut donc écrire

$$CE_R(\underline{a}) = \sum_{s \in S_m} a'_s \overline{\theta}_s \quad , \text{ avec } a'_s \in \mathfrak{d}_{\underline{a}}^{h(s)} ,$$

et c'est un élément de $CC(R)$, d'après le lemme 6.5.

Soit maintenant $\underline{a} = (\dots, a_{-n}, \dots, a_0)$ un élément quelconque de $CW(R)$ et soit $r = r_{\underline{a}}$, $m = m_{\underline{a}}$. En appliquant ce qui précède au covecteur $\underline{b} = (\dots, a_{-n}, \dots, a_{-r}, 0, 0, \dots, 0)$ on voit que le produit infini $\prod_{n=r}^{\infty} F(a_{-n} T_{-n})$ converge dans $CC(R)$ vers un élément de la forme $\sum_{s \in S_m} b'_s \overline{\theta}_s$, avec les b'_s dans R .

D'autre part, on voit que $\prod_{n=0}^{r-1} F(a_{-n} T_{-n})$ est un polynôme de degré $< p^r$ en T_{-r+1} (car $T_{-r+1}^{p^r} = 0$) ; pour tout entier j vérifiant $0 \leq j < p^r$, on a $T_{-r+1}^j = \overline{\theta}_{j/p^{r-1}}$ et $h(j/p^{r-1}) \leq (p-1)r$; on en déduit que $\prod_{n=0}^{r-1} F(a_{-n} T_{-n})$ s'écrit comme une somme finie de la forme $\sum_{\substack{s \in S \\ h(s) \leq (p-1)r}} c'_s \overline{\theta}_s$, avec les c'_s dans R .

La finitude de cette dernière somme implique que le produit infini

$$\prod_{n=0}^{\infty} F(a_{-n} T_{-n}) = \left(\prod_{n=0}^{r-1} F(a_{-n} T_{-n})\right) . \left(\prod_{n=r}^{\infty} F(a_{-n} T_{-n})\right) = (\sum c'_s \overline{\theta}_s) . (\sum b'_t \overline{\theta}_t)$$

converge dans $CC(R)$, ce qui achève de prouver l'assertion (i). On voit en outre que l'inégalité $h(s+t) \leq h(s) + h(t)$ (lemme 6.4) implique que l'on peut écrire, en posant $m' = m + (p-1)r$,

$$CE_R(a) = \sum_{s \in S_{m'}} a'_s \overline{\theta}_s \quad , \text{ avec les } a'_s \in R .$$

Montrons que si $\underline{a}$ et $\underline{b} \in CW(R)$, alors $CE_R(\underline{a}+\underline{b}) = CE_R(\underline{a}) . CE_R(\underline{b})$.

a) Si $\underline{a}$ et $\underline{b}$ sont dans $CW^u(R)$, cela résulte du n° 6.2.

b) Dans le cas général, il suffit de montrer que pour chaque $u \in S$ fixé, les coefficients de $\overline{\theta}_u$ dans $CE_R(\underline{a}+\underline{b})$ et dans $CE_R(\underline{a}) . CE_R(\underline{b})$ sont égaux. Compte-tenu de (a) il suffit de montrer que pour un u donné, on peut trouver un entier t tel que si l'on remplace

$\underline{a} = (\dots,a_{-n},\dots,a_0)$ par $(\dots,0,\dots,0,a_{-t},a_{-t+1},\dots,a_0)$ et

$\underline{b} = (\dots,b_{-n},\dots,b_0)$ par $(\dots,0,\dots,0,b_{-t},b_{-t+1},\dots,b_0)$,

cela ne change le coefficient de $\overline{\theta}_u$ ni dans $CE_R(\underline{a}+\underline{b})$ ni dans $CE_R(\underline{a}).CE_R(b)$. Or, il existe des entiers m_1 et m_2 tels que $CE_R(\underline{a})$ et $CE_R(\underline{b})$ peuvent s'écrire

$$CE_R(\underline{a}) = \sum_{s\in S_{m_1}} a'_s\overline{\theta}_s \quad \text{et} \quad CE_R(\underline{b}) = \sum_{s\in S_{m_2}} b'_s\overline{\theta}_s \ .$$

Il résulte facilement du lemme 6.5 qu'il n'existe qu'un nombre fini de couples $(s,s') \in S_{m_1} \times S_{m_2}$ tels que $s+s' = u$. L'assertion résulte alors de ce que, si $\underline{d}$ est un élément quelconque de $CW(R)$, le calcul du coefficient d'un $\overline{\theta}_s$ donné dans $CE_R(\underline{d})$ ne dépend que d'un nombre fini des composantes d_{-n} du covecteur $\underline{d}$.

Il reste à démontrer l'injectivité. Soit $\underline{a}$ un élément non nul de $CW(R)$. Si $\underline{a} \in CW^u(R)$, il existe un entier t tel que $a_{-t} \neq 0$ et $a_{-n} = 0$, pour $n > t$; le coefficient de T_{-t} dans $CE_R(\underline{a})$ est a_{-t} et $CE_R(\underline{a}) \neq 0$. Supposons donc que $\underline{a} \notin CW^u(R)$ et soit i le plus grand entier tel que $a_{-n} \in \mathfrak{d}^i_{\underline{a}}$, pour tout $n \geq r_{\underline{a}}$; on a $1 \leq i < m_{\underline{a}}$. Soit t un entier tel que $a_{-t} \notin \mathfrak{d}^{i+1}_{\underline{a}}$. On voit que le coefficient de T_{-t} dans $CE_R(\underline{a})$ est congru à $-a_{-t}$ modulo $\mathfrak{d}^{i+1}_{\underline{a}}$ et est donc $\neq 0$; par conséquent $CE_R(\underline{a}) \neq 0$.

6.4. Il est clair que l'application CE_R qui vient d'être construite est fonctorielle en R .

Soit k un $\mathbb{Z}_{(p)}$-anneau. Par restriction aux k-anneaux, CC définit un k-foncteur en groupes que nous notons CC_k . La famille des CE_R , pour tout k-anneau R , définit un monomorphisme de k-foncteurs en groupes que nous notons $CE_{(k)}$ ou simplement $CE : CW_k \to CC_k$.

Remarque : si k a de plus une structure d'anneau pseudo-compact, notons $\widehat{CC}_k$ le complété formel de CC_k (on a donc $\widehat{CC}_k(R) = CC_k(R)$, pour tout k-anneau fini R). On vérifie facilement que $\widehat{CC}_k$ est un k-groupe formel : soit $\overline{S} = \{s\in S \mid s<p\}$ et soit $\mathfrak{S}$ l'ensemble des parties S' de $\overline{S}$ qui vérifient :

(Φ') pour tout $r > 0$, il existe $\varepsilon > 0$ tel que $[r-\varepsilon,r[\cap \overline{S} \subset S'$.

Soit $\mathcal{C} = k[(X_s)_{s\in\overline{S}}]$ l'anneau des polynômes en les X_s à coefficients dans k ; pour tout $S' \in \mathfrak{S}$, notons $I_{S'}$ l'idéal de $\mathcal{C}$ engendré par les X_s , pour $s \in S'$. On voit que, pour tout k-anneau fini R , $\widehat{CC}_k(R)$ s'identifie à l'ensemble des homomorphismes continus du k-anneau $\mathcal{C}$ dans R , pour la topologie de $\mathcal{C}$ définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux de la forme $\mathfrak{a}\mathcal{C} + I_{S'}$, pour $\mathfrak{a}$ idéal ouvert de k et $S' \in \mathcal{S}$. L'algèbre affine de $\widehat{CC}_k$ s'identifie donc à la complétion profinie de $\mathcal{C}$ pour cette topologie (cf. n° 4.8).

6.5. Supposons maintenant que k est un corps parfait de caractéristique p . Nous allons caractériser l'image de CE_R dans $CC(R)$ lorsque R est un k-anneau.

Soit $\bar{k}$ une clôture algébrique de k . Si $a \in \bar{k}$ et si s est un élément de S de la forme $p^{-r}t$, avec r et t entiers, nous notons a^s l'unique élément b de $\bar{k}$ tel que $b^{p^r} = a^t$ (autrement di $b = \sigma^{-r}(a^t)$).

Soit ℓ un nombre premier $\neq p$. Notons μ_ℓ le groupe des racines ℓ-ièmes de l'unité dans $\bar{k}$; posons $k_\ell = k(\mu_\ell)$ et, pour tout k-anneau R , $R_\ell = R \otimes_k k_\ell$. Si $\alpha = \sum a_s \bar{\theta}_s \in CC(R)$, pour tout $\eta \in \mu_\ell$,

$$\sum a_s \eta^s \bar{\theta}_s \in CC(R_\ell)$$

et $\prod_{\eta \in \mu_\ell} (\sum a_s \eta^s \bar{\theta}_s)$ est invariant par l'action de $Gal(k_\ell/k)$ et appartient donc à $CC(R)$. On a donc ainsi défini, pour tout k-anneau R , un endomorphisme U_ℓ du groupe $CC(R)$:

$$U_\ell(\sum a_s \bar{\theta}_s) = \prod_{\eta \in \mu_\ell} (\sum a_s \eta^s \bar{\theta}_s) .$$

Soit, pour tout k-anneau R ,

$$CCT(R) = \{\alpha \in CC(R) \mid U_\ell \alpha = 1 \text{ , pour tout } \ell \neq p\} .$$

Pour tout k-anneau R , notons $CC'(R)$ l'ensemble des éléments $\sum a_s \bar{\theta}_s$ de $CC(R)$ vérifiant :

(Ψ') $\left\{\begin{array}{l}\underline{\text{il existe}}\ \varepsilon > 0\ \underline{\text{tel que l'idéal de}}\ R\ \underline{\text{engendré par les}}\ a_s ,\\ \underline{\text{avec}}\ s < \varepsilon\ ,\ \underline{\text{est nilpotent}}.\end{array}\right.$

Il est clair que $CC'(R)$ est un sous-groupe de $CC(R)$. Si $\alpha = \sum a_s \bar{\theta}_s \in CC(R)$, on a, pour r entier ≥ 1 ,

$$\alpha^{p^r} = \sum a_s^{p^r} \bar{\theta}_s^{p^r} = \sum_{0 \leq s < p^{-r+1}} a_s^{p^r} \bar{\theta}_{sp^r} .$$

On en déduit que $CC'(R)$ est contenu dans le sous-groupe $CC_{p^\infty}(R)$ de $CC(R)$ formé des éléments d'ordre une puissance de p .

Remarque 1 : si R est un k-anneau fini, le radical $\mathbf{r}_R$ de R est nilpotent, et la condition (Ψ') est équivalente à la suivante

(Ψ'') il existe $\varepsilon > 0$ tel que $a_s \in \mathbf{r}_R$, pour $s < \varepsilon$.

En particulier, on voit que $CC'(R) = CC_{p^\infty}(R)$.

Enfin, nous posons $CCT'(R) = CCT(R) \cap CC'(R)$.

PROPOSITION 6.6.- Soit R un k-anneau. L'application CE_R est un isomorphisme du groupe $CW_k(R)$ sur $CCT'(R)$.

Pour montrer que l'image est contenue dans $CCT'(R)$, nous aurons besoin du lemme suivant :

LEMME 6.7.- Soit $F(T) = \prod_{(n,p)=1} (1-T^n)^{\mu(n)/n} \in \mathbb{Z}[[T]]$ et soit ℓ un nombre premier $\neq p$. Dans $\mathbb{Z}(\sqrt[\ell]{1})[[T]]$, on a

$$\prod_{\eta\in\mu_\ell} F(\eta T) = 1 .$$

Démonstration du lemme : comme $\mu(n) = 0$ si ℓ^2 divise n , on peut écrire

$$F(T) = \left(\prod_{(n,p\ell)=1} (1-T^n)^{\mu(n)/n}\right).\left(\prod_{(n,p\ell)=1} (1-T^{n\ell})^{\mu(n\ell)/n\ell}\right)$$

$$= \prod_{(n,p\ell)=1} \left(\frac{(1-T^n)^\ell}{(1-T^{n\ell})}\right)^{\mu(n)/n\ell}$$

puisque $\mu(n\ell) = -\mu(n)$ si $(n,\ell) = 1$. On a donc

$$\prod_{\eta\in\mu_\ell} F(\eta T) = \prod_{(n,p\ell)=1} \left(\prod_{\eta\in\mu_\ell} \frac{(1-\eta^n T^n)^\ell}{(1-\eta^{n\ell}T^{n\ell})}\right)^{\mu(n)/n\ell}$$

$$= \prod_{(n,p\ell)=1} \left(\frac{\prod_{\eta\in\mu_\ell} (1-\eta^n T^n)}{(1-T^{n\ell})}\right)^{\mu(n)/n} = 1$$

puisque $\prod_{\eta\in\mu_\ell} (1-\eta^n T^n) = 1 - T^{n\ell}$ si $(n,\ell) = 1$.

Démonstration de $\operatorname{Im} CE_R \subset CCT'(R)$: soit $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW_k(R)$. On a $CE_R(\underline{a}) = \prod F(a_{-n} T_{-n})$.

Soit ℓ un nombre premier $\neq p$. Il est clair que

$$U_\ell(CE_R(\underline{a})) = \prod_{n=0}^{\infty} U_\ell(F(a_{-n}T_{-n})) = \prod_{n=0}^{\infty}\left(\prod_{\eta\in\mu_\ell} F(a_{-n}\eta^{p^{-n}}T_{-n})\right) .$$

Comme $(\ell,p) = 1$, on a $\prod_{\eta\in\mu_\ell} F(a_{-n}\eta^{p^{-n}}T_{-n}) = \prod_{\eta\in\mu_\ell} F(\eta a_{-n}T_{-n}) = 1$, d'après le lemme 6.7. Par conséquent, $CE_R(\underline{a}) \in CCT(R)$.

Le fait que les composantes de $\underline{a}$ vérifient la condition (Ψ) (cf. n° 1.5) implique trivialement que les coefficients de $CE_R(\underline{a})$ vérifient (Ψ') donc que $CE_R(\underline{a}) \in CC'(R)$. Finalement, pour tout $\underline{a} \in CW_k(R)$,

$CE_R(\underline{a}) \in CCT(R) \cap CC'(R) = CCT'(R)$.

Si $\mathfrak{d}$ est un idéal de R et si ℓ est un nombre premier $\neq p$, nous notons $\mathfrak{d}_\ell$ l'idéal $\mathfrak{d} \otimes_k k_\ell$ de $R_\ell = R \otimes_k k_\ell$. Etant donnés deux éléments α et β de $CC(R_\ell)$ et un $\varepsilon > 0$,

- on pose $\alpha \equiv \beta \mod(\mathfrak{d},\varepsilon)$ si le coefficient de $\overline{\theta}_s$ dans $\alpha - \beta$ appartient à $\mathfrak{d}_\ell$, pour $0 < s < \varepsilon$;
- on pose $\alpha \equiv \beta \mod \varepsilon$ si $\alpha \equiv \beta \mod(0,\varepsilon)$.

LEMME 6.8.- <u>Soit</u> $\overline{S} = \{s\in S \mid s<p\}$ <u>et soit</u> $\delta = \sum_{s\in\overline{S}} d_s\overline{\theta}_s$ <u>un élément de</u> $CCT'(R)$.

i) <u>Soit</u> $\mathfrak{d}$ <u>un idéal de</u> R <u>et soit</u> ε <u>un nombre réel</u> > 0 <u>tels que</u> $\delta \equiv 1 \mod(\mathfrak{d},\varepsilon)$. <u>On a</u> $d_s \in \mathfrak{d}^2$, <u>pour tout</u> $s \in \overline{S}$ <u>vérifiant</u> $0 < s < \varepsilon$ <u>qui n'est pas de la forme</u> $s = p^{-n}$, <u>avec</u> n <u>entier</u>.

ii) <u>Soit</u> ε' <u>un nombre réel</u> >0 <u>tel que</u> $\delta \equiv 1 \mod \varepsilon'$. <u>On a</u> $d_s = 0$ <u>pour tout</u> $s \in \overline{S}$ <u>vérifiant</u> $0 < s < 2\varepsilon'$ <u>qui n'est pas de la forme</u> $s = p^{-n}$, <u>avec</u> n <u>entier</u>.

<u>Démonstration du lemme</u> : commençons par prouver (i). Il est clair que si α et β sont deux éléments de $CC(R_\ell)$ vérifiant $\alpha \equiv \beta \equiv 1 \mod(\mathfrak{d},\varepsilon)$, on a $\alpha\beta \equiv \alpha + \beta - 1 \mod(\mathfrak{d}^2,\varepsilon)$. Par conséquent, si $\delta \equiv 1 \mod(\mathfrak{d},\varepsilon)$, on a

$$U_\ell\delta = \prod_{\eta\in\mu_\ell}(\Sigma d_s\eta^s\overline{\theta}_s) \equiv 1 + \sum_{\eta\in\mu_\ell}\sum_{0<s<\varepsilon} \eta^s d_s\overline{\theta}_s$$

$$\equiv 1 + \sum_{0<s<\varepsilon}\left(\sum_{\eta\in\mu_\ell}\eta^s\right)d_s\overline{\theta}_s \mod(\mathfrak{d}^2,\varepsilon) .$$

Soit $s \in S$ vérifiant $0 < s < \varepsilon$ et $s \neq p^{-n}$ pour tout n . Il existe un $\ell \neq p$ tel que $\eta^s = 1$ pour tout $\eta \in \mu_\ell$. Le coefficient de $\overline{\theta}_s$ dans

$U_\ell\delta$ est donc $\equiv \ell d_s \mod \mathfrak{d}^2$. Comme ℓ est premier à p , si $U_\ell\delta = 1$, on a $d_s \in \mathfrak{d}^2$.

La preuve de (ii) est analogue à celle de (i) si l'on remarque que, α et β étant deux éléments de $CC(R_\ell)$ vérifiant $\alpha \equiv \beta \equiv 1 \mod \varepsilon'$, on a $\alpha\beta \equiv \alpha + \beta - 1 \mod 2\varepsilon'$.

<u>Fin de la démonstration de la proposition 6.6</u> : soit $\alpha \in CCT'(R)$. Comme $\alpha \in CC'(R)$, il existe un $\varepsilon > 0$ et un idéal nilpotent $\mathfrak{d}$ de R tel que $\alpha \equiv 1 \mod(\mathfrak{d},\varepsilon)$.

Montrons, par récurrence sur i , que pour tout entier $i \geq 0$, il existe un $\beta_i \in \mathrm{Im}\, CE_R$ tel que $\alpha \equiv \beta_i \mod(\mathfrak{d}^{2^i},\varepsilon)$:

- pour $i = 0$, on peut prendre $\beta_0 = 1$;
- si $\alpha \equiv \beta_i \mod(\mathfrak{d}^{2^i},\varepsilon)$, on a $\alpha\beta_i^{-1} \equiv 1 \mod(\mathfrak{d}^{2^i},\varepsilon)$; si $\alpha\beta_i^{-1} = \sum c_s\overline{\theta}_s$ et si $\mathfrak{d}^{2^i} = \mathfrak{d}'$, on a $c_s \in \mathfrak{d}'$ pour $0 < s < \varepsilon$ et, en particulier, $c_{p^{-n}} \in \mathfrak{d}'$ si $p^{-n} < \varepsilon$; donc $\underline{c} = (\dots,c_{p^{-n}},\dots,c_{p^{-1}},c_1) \in CW_k(R)$. On voit que $\gamma = CE_R(\underline{c}) \equiv 1 - \sum c_{p^{-n}}T_{-n} \mod(\mathfrak{d}'^2,\varepsilon)$. Posons $\delta = \alpha\beta_i^{-1}\gamma$; il est clair que le coefficient de $T_{-n} = \overline{\theta}_{p^{-n}}$ dans δ appartient à $\mathfrak{d}'^2$ et que $\delta \equiv 1 \mod(\mathfrak{d}',\varepsilon)$; il résulte de l'assertion (i) du lemme 6.8 que $\delta \equiv 1 \mod(\mathfrak{d}'^2,\varepsilon)$ ou encore que $\alpha \equiv \beta_i\gamma^{-1} \mod(\mathfrak{d}^{2^{i+1}},\varepsilon)$ et la récurrence est établie.

En appliquant ceci à un entier i tel que $\mathfrak{d}^{2^i} = 0$, on se ramène à montrer que, si $\alpha \in CCT'(R)$ vérifie $\alpha \equiv 1 \mod \varepsilon$ (pour un ε donné > 0), alors $\alpha \in \mathrm{Im}\, CE_R$. En prodédant par récurrence sur ε' , on voit qu'il suffit de montrer que, pour tout nombre réel $\varepsilon' > 0$, si $\alpha \in CCT'(R)$ vérifie $\alpha \equiv 1 \mod \varepsilon'$, il existe $\beta \in \mathrm{Im}\, CE_R$ tel que $\alpha \equiv \beta \mod 2\varepsilon'$:

- s'il n'existe pas d'entier n tel que $\varepsilon' \leq p^{-n} < 2\varepsilon'$, il résulte de l'assertion (ii) du lemme 6.8 que $\alpha \equiv 1 \mod 2\varepsilon'$ et on peut prendre $\beta = 1$;
- s'il existe un entier n tel que $\varepsilon' \leq p^{-n} < 2\varepsilon'$, il résulte de l'assertion (ii) du lemme 6.8 que $\alpha \equiv 1 - aT_{-n} \mod 2\varepsilon'$, pour un $a \in k$ convenable; on voit qu'il suffit alors de prendre $\beta = F(aT_{-n})$.

<u>Remarque 2</u> : soit R un k-anneau. Par transport de structure, l'isomorphisme CE_R munit $CCT'(R)$ d'une structure de D_k-module à gauche. Si $\alpha = \sum a_s\overline{\theta}_s \in CCT'(R)$, on voit que

$$\underline{F}^{\alpha} = \Sigma a_s^p \overline{\theta}_s \ ,$$

$$\underline{V}^{\alpha} = \Sigma a_s \overline{\theta}_{sp} \ ,$$

$[x]\alpha = \Sigma a_s x^s \overline{\theta}_s$, pour tout $x \in k$ (on a noté $[x]$ le représentant multiplicatif de x dans $A = W(k)$).

Remarque 3 : pour tout k-anneau R , soit $BC(R)$ le groupe multiplicatif des éléments de $B\Lambda(R)$ congrus à 1 modulo l'idéal engendré par les θ_s , pour $s > 0$. Pour tout nombre premier ℓ , notons $B\Lambda(R)_\ell$ l'anneau $B\Lambda(R)[X]/(X^\ell - \theta_1)$. On voit que c'est un $B\Lambda(R)$-module libre de rang ℓ et que, si l'on note τ l'image de X , pour tout $s \in S$, il existe un élément $\theta_{s/\ell}$ de $B\Lambda(R)_\ell$ et un seul, de la forme $\tau^i \theta_t$, tel que $(\theta_{s/\ell})^\ell = \theta_s$. Pour tout $\alpha = \Sigma a_s \theta_s \in BC(R)$, posons

$$F_\ell(\alpha) = \prod_{\eta \in \mu_\ell} (\Sigma a_s \eta^s \theta_{s/\ell})$$

$$V_\ell(\alpha) = \Sigma a_s \theta_{s\ell} \ .$$

On voit que F_ℓ et V_ℓ définissent des endomorphismes du groupe $BC(R)$ et que $F_\ell V_\ell(\alpha) = \alpha^\ell$.

On voit aussi que le sous-groupe $C(R)$ de $BC(R)$, formé des éléments de la forme $\sum_{s \in \mathbb{N}} a_s \theta_s$ (autrement dit le groupe multiplicatif des séries formelles, de terme constant égal à 1 , en la variable $\theta_1 = T_0$), est stable par V_ℓ et F_ℓ . Par restriction V_ℓ et F_ℓ définissent des endomorphismes de $C(R)$; ce sont les opérateurs du même nom introduits par Cartier ([6], § 2).

Le noyau de la projection canonique de $BC(R)$ sur $CC(R)$ n'est pas stable par V_ℓ , mais l'est par $V_\ell F_\ell$; par conséquent $V_\ell F_\ell$ opère sur $CC(R)$; on voit que, dans $CC(R)$, $V_\ell F_\ell = U_\ell$.

6.6. Supposons encore que k est un corps parfait de caractéristique p . Nous posons $A = W(k)$ et nous notons K le corps des fractions de A . Comme au numéro précédent, nous posons $S = \mathbb{N}[1/p]$ et $\overline{S} = \{s \in S \mid 0 \leq s < p\}$. Nous allons, pour terminer ce paragraphe, utiliser ce qui a été fait au § 5 pour donner une interprétation du module des covecteurs de Witt à coefficients dans $C\Lambda(k)$.

Pour tout anneau commutatif R , muni de la topologie discrète, munissons l'anneau $B\Lambda(R)$ de la topologie définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux (θ_{p^m}), pour $m \in \mathbb{N}$. Il est clair que $B\Lambda(R)$ est un R-anneau linéairement topologisé, séparé et complet pour cette topologie.

Soit $\mathcal{B}_A = \varprojlim B\Lambda(A/p^n)$. Il est clair que, si A est muni de la topologie p-adique, $\mathcal{B}_A$ est un A-anneau linéairement topologisé, séparé et complet. On voit que $\mathcal{B}_A$ s'identifie au sous-A-module de A^S formé des éléments $\sum_{s \in S} a_s \theta_s$, avec les a_s dans A vérifiant

(Φ_1) $\left\{ \begin{array}{l} \underline{\text{pour tout entier}}\ n \geq 0\ \underline{\text{et tout nombre réel}}\ r > 0\ ,\ \underline{\text{il existe}} \\ \varepsilon > 0\ \underline{\text{tel que}}\ a_s \in p^n A\ ,\ \underline{\text{si}}\ r-\varepsilon \leq s < r\ . \end{array} \right.$

Les idéaux (θ_{p^m}, p^n), pour m, $n \in \mathbb{N}$, forment un système fondamental de voisinages ouverts de 0 dans $\mathcal{B}_A$. On en déduit, avec la terminologie du n° 5.3, que $\mathcal{B}_A$ est un A-anneau pro-p-adique et que l'ensemble $\mathfrak{J}$ des idéaux de $\mathcal{B}_A$ de la forme (θ_{p^m}), pour m entier, est une famille d'idéaux co-p-adiques de $\mathcal{B}_A$ qui détermine sa topologie.

Posons $\mathcal{B}_K = (\mathcal{B}_A)_K = \mathcal{B}_A \otimes_A K$ et $\hat{\mathcal{B}}_K = \hat{\mathcal{B}}_K^{\mathfrak{J}}$. Il est clair que $\hat{\mathcal{B}}_K$ s'identifie, en tant que K-anneau topologique à la limite projective des $\mathcal{B}_K/\theta_{p^m}\mathcal{B}_K$, chaque quotient étant muni de la topologie p-adique.

On vérifie facilement que tout élément de $\hat{\mathcal{B}}_K$ s'écrit d'une manière et d'une seule sous la forme $\sum a_s \theta_s$, avec les $a_s \in K$ vérifiant (Φ_1) et

(Φ_2) $\left\{ \begin{array}{l} \underline{\text{pour tout}}\ r > 0\ ,\ \underline{\text{il existe un entier}}\ m\ \underline{\text{tel que}}\ p^m a_s \in A\ ,\ \underline{\text{si}} \\ s < r\ . \end{array} \right.$

Enfin, nous notons $\mathcal{B}'_K$ le sous-espace vectoriel de $\hat{\mathcal{B}}_K$ formé des $\sum a_s \theta_s$ qui vérifient

(Φ_3) $\left\{ \begin{array}{l} \underline{\text{pour tout}}\ r > 0\ ,\ \underline{\text{il existe}}\ c > 0\ \underline{\text{tel que}}\ |a_s|_p \leq cs\ ,\ \underline{\text{si}} \\ s \geq r\ \ (\underline{\text{en notant}}\ |\ |_p\ \underline{\text{la valeur absolue p-adique sur}}\ K\ ). \end{array} \right.$

On voit enfin que le k-anneau linéairement topologisé $\mathcal{B}_k = \mathcal{B}_A \otimes_A k = \mathcal{B}_A/p\mathcal{B}_A$ s'identifie canoniquement à $B\Lambda(k)$.

On a défini au n° 5.3 une application A-linéaire continue $w_{\mathcal{B}_A}^{\mathfrak{J}}$ de $CW_k(\mathcal{B}_k)$ dans $\hat{\mathcal{B}}_K/p\mathcal{B}_A$. En composant avec la multiplication par $1/p$ on en déduit une application A-linéaire continue $\varpi_k = p^{-1} w_{\mathcal{B}_A}^{\mathfrak{J}} : CW_k(\mathcal{B}_k) \to \hat{\mathcal{B}}_K/\mathcal{B}_A$.

Si $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in CW_k(\mathcal{B}_k)$ et si $\hat{a}_{-n}$ désigne un relèvement de a_{-n} dans $\mathcal{B}_A$, on voit que $\varpi_k(\underline{a})$ est l'image, dans $\hat{\mathcal{B}}_K/\mathcal{B}_A$ de la somme de la série de terme général $p^{-n-1}\hat{a}^{p^n}_{-n}$.

PROPOSITION 6.9.- L'application A-linéaire continue $\varpi_k : CW_k(\mathcal{B}_k) \to \hat{\mathcal{B}}_K/\mathcal{B}_A$ est injective. Son image est $\mathcal{B}'_K/\mathcal{B}_A$.

Démonstration : on voit que $CW_k(\mathcal{B}_k)$ est formé des $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0)$, avec les $a_{-n} \in \mathcal{B}_k$ vérifiant

$$(\Psi'')\quad \begin{cases} \text{il existe des entiers } m \text{ et } n_0 \text{ tels que } a_{-n} \in \theta_{p^{-m}}\mathcal{B}_k \text{, si} \\ n \geq n_0 . \end{cases}$$

En procédant comme pour démontrer l'injectivité de $w_{\mathfrak{R}}$ dans la proposition 5.5, on voit facilement que si $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ était un élément non nul de $CW_k(\mathcal{B}_k)$ tel que $\varpi_k(\underline{a}) = 0$, il existerait un entier m et une suite infinie $n_1,n_2,\ldots,n_i,\ldots$ telle que $a_{-n_i} \notin \theta_{p^{m-n_i}}\mathcal{B}_k$, ce qui contredirait (Ψ''). L'application ϖ_k est donc injective.

Soit $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in CW_k(\mathcal{B}_k)$ et soit m et n_0 des entiers tels que $a_{-n} \in \theta_{p^{-m}}\mathcal{B}_k$, si $n \geq n_0$. On peut choisir les relèvements $\hat{a}_{-n}$ des a_{-n} dans $\mathcal{B}_A$ pour que $\hat{a}_{-n} \in \theta_{p^{-m}}\mathcal{B}_A$, si $n \geq n_0$. Si on pose

$$\alpha = \sum_{n=0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n} \in \hat{\mathcal{B}}_K ,$$

on a alors

$$\alpha = \sum_{n=0}^{n_0-1} p^{-n}\hat{a}^{p^n}_{-n} + \sum_{n=n_0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n} = p^{-n_0+1}\beta + \gamma ,$$

avec $\beta \in \mathcal{B}_A$ et $\gamma = \sum_{n=n_0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n}$.

On voit que, pour tout $s \in S$, le coefficient c_s de θ_s dans γ vérifie $|c_s|_p \leq p^n$ si $s < p^{-m+n+1}$; donc, si $p^{-m+n} \leq s < p^{-m+n+1}$, on a $s^{-1}|c_s|_p \leq p^m$.

Pour tout $s \in S$, le coefficient b_s de θ_s dans $p^{-n_0+1}\beta$ vérifie $|b_s|_p \leq p^{n_0-1}$; si r est un nombre réel > 0, on a donc

$$s^{-1}|b_s|_p \leq r^{-1}p^{n_0-1} \quad \text{si} \quad s \geq r .$$

On en déduit que pour tout $r > 0$, le coefficient a_s de θ_s dans α vérifie $|a_s|_p \leq c(r)s$, pour tout $s \geq r$, si l'on pose $c(r) = \max(p^m, r^{-1}p^{n_0-1})$.

Par conséquent α, donc $p^{-1}\alpha$, vérifie (Φ_3) et appartient à $\mathcal{B}'_K$. On a donc montré que l'image de ϖ_k est contenue dans $\mathcal{B}'_K/\mathcal{B}_A$.

Si $\alpha = \sum a_s\theta_s$ est un élément quelconque de $\mathcal{B}_A$, nous posons, pour tout entier $n \geq 0$, $\alpha^{(n)} = \sum \sigma^{-n}(a_s)\theta_{sp^{-n}}$ (rappelons que σ est le Frobenius absolu). On voit que

$$(\alpha^{(n)})^{p^n} \equiv \alpha \pmod{p\mathcal{B}_A} \quad \text{ou encore que}$$

$$p^{-n-1}(\alpha^{(n)})^{p^n} \equiv p^{-n-1}\alpha \pmod{p^{-n}\mathcal{B}_A}.$$

On en déduit facilement que l'image par ϖ_k de $CW^u(\mathcal{B}_k)$ (sous-groupe de $CW_k(\mathcal{B}_k)$ formé des covecteurs dont presque toutes les composantes sont nulles) est $\mathcal{B}_K/\mathcal{B}_A$.

Soit maintenant $\alpha = \sum a_s\theta_s$ un élément de $\mathcal{B}'_K$. Nous allons chercher un élément $\underline{a}$ de $CW_k(\mathcal{B}_k)$ tel que $\varpi_k(\underline{a})$ soit égal à l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$. La condition (Φ_2) montre que $\sum_{0\leq s<1} a_s\theta_s \in \mathcal{B}_K$. Comme $\mathcal{B}_K/\mathcal{B}_A$ est contenu dans l'image de ϖ_k, on voit que l'on peut supposer $a_s = 0$ pour $s < 1$. D'après (Φ_3) il existe donc un $c > 0$ tel que $|a_s|_p \leq cs$, pour tout $s \in S$.

Pour $s < c^{-1}p$, on a $|a_s|_p < p$, donc $|a_s|_p \leq 1$ et $a_s \in A$; pour tout entier $n \geq 0$ et pour $c^{-1}p^{n+1} \leq s < c^{-1}p^{n+2}$, on a $|a_s|_p < p^{n+2}$, donc $|a_s|_p \leq p^{n+1}$. On a donc

$$\alpha \equiv \sum_{n=0}^{\infty}\left(\sum_{c^{-1}p^{n+1}\leq s<c^{-1}p^{n+2}} a_s\theta_s\right) \pmod{\mathcal{B}_A},$$

avec $p^{n+1}a_s \in A$ si $c^{-1}p^{n+1} \leq s < c^{-1}p^{n+2}$. Soit $m \in \mathbb{Z}$ tel que $p^m \leq c^{-1}p$. On voit que l'on peut réécrire α sous la forme

$$\alpha \equiv \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n \pmod{\mathcal{B}_A},$$

les β_n étant des éléments de $\mathcal{B}_A$.

Pour achever la démonstration de la proposition il suffit donc d'établir le lemme suivant :

LEMME 6.10.- <u>Soit</u> $m \in \mathbb{Z}$ <u>et soit</u> $\beta_0, \beta_1, \ldots, \beta_n, \ldots$ <u>des éléments de</u> $\mathcal{B}_A$. <u>Il existe</u> $\underline{a} \in CW_k(\mathcal{B}_k)$ <u>tel que</u> $\varpi_k(\underline{a})$ <u>soit égal à l'image dans</u> $\mathcal{B}'_K/\mathcal{B}_A$ <u>de</u> $\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n$.

Démonstration : soit $m' \in \mathbb{Z}$ et soit $\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots$ des éléments de $\mathcal{B}_A$. Pour tout $n \geq 0$, on a $\left(\gamma_n^{(n)}\right)^{p^n} \equiv \gamma_n \pmod{p\mathcal{B}_A}$; par conséquent

$$\gamma'_n = p^{-1}\left(\gamma_{n+1} - \left(\gamma_{n+1}^{(n+1)}\right)^{p^{n+1}}\right) \in \mathcal{B}_A \text{ , pour tout } n \geq 0$$

et
$$\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m'+n}}\gamma_n = \sum_{n=0}^{\infty} p^{-n-1}\left(\theta_{p^{m'}}\gamma_n^{(n)}\right)^{p^n} + \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m'+1)+n}}\gamma'_n .$$

On voit donc que l'image de $\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m'+n}}\gamma_n$ dans $\mathcal{B}'_K/\mathcal{B}_A$ est égale à la somme de l'image de $\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m'+1)+n}}\gamma'_n$ et de $\varpi_k(\underline{b})$ où $\underline{b} = (\ldots, b_{-n}, \ldots, b_0)$ est un élément de $CW_k(\mathcal{B}_k)$ tel que $b_{-n} \in \theta_{p^m}\mathcal{B}_k$, pour tout n.

En appliquant ceci successivement à $m' = m, m+1, \ldots, m+t, \ldots$, on voit que l'on peut construire des éléments $\underline{b}_m, \underline{b}_{m+1}, \ldots, \underline{b}_{m+t}, \ldots$ de $CW(\mathcal{B}_k)$ vérifiant, pour tout $t \geq 0$,

- les coefficients de $\underline{b}_{m+t}$ appartiennent à $\theta_{p^{m+t}}\mathcal{B}_k$,
- si α_t est un relèvement dans $\mathcal{B}'_K$ de $\varpi_k(\underline{b}_m + \underline{b}_{m+1} + \ldots + \underline{b}_{m+t})$, on a $\alpha = \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n \equiv \alpha_t + \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m+t)+n}}\delta_{n,t} \pmod{\mathcal{B}_A}$, où les $\delta_{n,t}$ sont dans $\mathcal{B}_A$.

On voit donc que la suite des α_t converge vers l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$; le fait que les coefficients de $\underline{b}_{m+t}$ sont dans $\theta_{p^{m+t}}\mathcal{B}_k$ implique que la série de terme général $\underline{b}_{m+t}$ converge, dans $CW_k(\mathcal{B}_k)$, vers un élément $\underline{a}$; la continuité de ϖ_k implique que $\varpi_k(\underline{a})$ est égal à l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$

6.7. On conserve les hypothèses et les notations du numéro précédent. Posons $\mathcal{C}_k = C\Lambda(k)$; rappelons que c'est le quotient de l'anneau $\mathcal{B}_k = B\Lambda(k)$ par l'idéal engendré par θ_p. Notons $CW_k(\theta_p\mathcal{B}_k)$ le sous-A-module fermé de $CW_k(\mathcal{B}_k)$ formé des covecteurs dont toutes les composantes sont dans $\theta_p\mathcal{B}_k$. Il est clair que l'on a une suite exacte de A-modules topologiques

$$0 \longrightarrow CW_k(\theta_p\mathcal{B}_k) \longrightarrow CW_k(\mathcal{B}_k) \longrightarrow CW_k(\mathcal{C}_k) \longrightarrow 0 .$$

Soit $$\mathcal{B}''_K = \left\{ \Sigma a_s\theta_s \in \hat{\mathcal{B}}_K \;\middle|\; \begin{array}{l} a_s = 0 \quad \text{si} \quad s < p \\ |a_s|_p \leq s \quad \text{pour tout} \quad s \in S \end{array} \right\} .$$

On voit que $\mathcal{B}''_K \subset \mathcal{B}'_K$ et qu'un élément α de $\hat{\mathcal{B}}_K$ de la forme $\sum_{s\geq p} a_s \theta_s$ est dans $\mathcal{B}''_K$ si et seulement si $p^n a_s \in A$, si $p^n \leq s < p^{n+1}$. Il est clair que $\mathcal{B}''_K$ est aussi l'ensemble des éléments de $\hat{\mathcal{B}}_K$ qui peuvent s'écrire sous la forme

$$\sum_{n=0}^{\infty} p^{-n-1} \theta_{p^{n+1}} \beta_n \text{ , avec des } \beta_n \in \mathcal{B}_A .$$

On voit facilement (cf. la démonstration du lemme 6.10) que l'image par ϖ_k de $CW_k(\theta_p \mathcal{B}_k)$ est formé des éléments de $\mathcal{B}'_K/\mathcal{B}_A$ que l'on peut relever, dans $\mathcal{B}'_K$, en un élément de $\mathcal{B}''_K$. Par passage au quotient, on en déduit un isomorphisme

$$\overline{\varpi}_k : CW_k(\mathcal{C}_k) \longrightarrow \mathcal{B}'_K/(\mathcal{B}''_K + \mathcal{B}_A) .$$

On peut énoncer ce résultat sous la forme suivante :

PROPOSITION 6.11.- <u>Notons</u> Θ_k <u>le A-module formé des éléments</u> $\sum a_s \theta_s$, <u>avec</u>

$$a_s \in \begin{cases} K/A \ \underline{\text{si}} \ s < p , \\ K/p^{-n}A \ \underline{\text{si}} \ p^n \leq s < p^{n+1} \ (\underline{\text{pour}} \ n \geq 1) , \end{cases}$$

<u>vérifiant les conditions</u> (Φ_1), (Φ_2) <u>et</u> (Φ_3). <u>L'application</u> ϖ_k <u>définit, par passage au quotient, un isomorphisme</u> $\overline{\varpi}_k$ <u>du A-module</u> $CW_k(\mathcal{C}_k)$ <u>sur</u> Θ_k.

<u>Remarque</u> : en particulier, la structure de D_k-module à gauche sur $CW_k(\mathcal{C}_k)$ se transporte sur Θ_k. On voit que l'action de $\underline{F}$ et de $\underline{V}$ sont définies par

$$\underline{F}(\sum a_s \theta_s) = \sum \sigma(a_s) \theta_{sp} \quad \text{et} \quad \underline{V}(\sum a_s \theta_s) = \sum p \sigma^{-1}(a_s) \theta_{s/p} .$$

CHAPITRE III

MODULE DE DIEUDONNÉ

Dans tout ce chapitre et dans les suivants, on note k un corps parfait de caractéristique p, on note $A = W(k)$ l'anneau des vecteurs de Witt à coefficients dans k et $D_k = A[\underline{F},\underline{V}]$ l'anneau de Dieudonné de k. Si τ est un automorphisme de k, on note encore τ son relèvement à A ainsi que le prolongement de ce relèvement à D_k (avec $\tau(\underline{F}) = \underline{F}$, $\tau(\underline{V}) = \underline{V}$). Nous appliquerons ceci en particulier au Frobenius absolu σ (on a $\sigma(x) = x^p$, pour tout x dans k).

§ 1.- Classification des p-groupes formels.

1.1. Nous disons qu'un groupe formel (commutatif) G sur k est un <u>p-groupe formel</u> s'il s'identifie à la limite inductive, pour $n \to \infty$, des noyaux de la multiplication par p^n.

Les assertions suivantes sont évidentes :

- tout k-groupe formel connexe est un p-groupe formel ;
- si $G = G^c \times G^{et}$, avec G^c connexe et G^{et} étale, est un k-groupe formel, G est un p-groupe formel si et seulement si G^{et} l'est ;
- un k-groupe formel G est un p-groupe formel si et seulement si $G(k')$ est un groupe de p-torsion, pour toute extension finie k' du corps k ;
- un k-groupe formel G est un p-groupe formel si et seulement si $G(R)$ est un groupe de p-torsion, pour tout k-anneau fini R ;
- la catégorie des p-groupes formels sur k est une sous-catégorie épaisse de la catégorie des k-groupes formels ;
- le groupe $\widehat{CW}_k$ est un p-groupe formel.

1.2. Soit G un k-groupe formel et soit B_G son algèbre affine. L'ensemble des morphismes de k-schémas formels de G dans $\widehat{CW}_k$ s'identifie, par le lemme de Yoneda, à $\widehat{CW}_k(B_G)$ et a donc une structure naturelle de D_k-module $A[\underline{F}]$-pro-artinien (chap.II, prop.4.1).

Soit $\underline{M}(G) = \mathrm{Hom}(G, \widehat{CW}_k)$ le groupe des morphismes (de k-groupes formels) de G dans $\widehat{CW}_k$. L'identification précédente permet de considérer $\underline{M}(G)$ comme un sous-D_k-module topologique fermé de $\widehat{CW}_k(B_G)$. Plus précisément, considérons les trois applications continues suivantes de B_G dans $B_G \hat{\otimes} B_G$: le coproduit Δ_G, l'application $a \mapsto a \hat{\otimes} 1$, l'application $a \mapsto 1 \hat{\otimes} a$; par fonctorialité, elles induisent des applications continues de $\widehat{CW}_k(B_G)$ dans $\widehat{CW}_k(B_G \hat{\otimes} B_G)$ que nous notons de la même manière ; on voit que $\underline{M}(G)$ s'identifie au sous-D_k-module fermé de $\widehat{CW}_k(B_G)$ formé des éléments $\underline{a}$ vérifiant $\Delta_G(\underline{a}) = \underline{a} \hat{\otimes} 1 + 1 \hat{\otimes} \underline{a}$.

Si $\varphi : G \to H$ est un morphisme de k-groupes formels, il est clair que l'application évidente $\underline{M}(\varphi) : \underline{M}(H) = \mathrm{Hom}(H, \widehat{CW}_k) \to \underline{M}(G) = \mathrm{Hom}(G, \widehat{CW}_k)$ est continue.

Si maintenant G est un p-groupe formel et si, pour tout $n \in \mathbb{N}$, G_n désigne le noyau de la multiplication par p^n dans G, on voit que $\underline{M}(G)$ s'identifie à la limite projective des $\underline{M}(G_n)$ et que chaque $\underline{M}(G_n)$ est tué par p^n. On en déduit que $\bigcap_{n=0}^{\infty} p^n \underline{M}(G) = \{0\}$ et il en résulte facilement que $\underline{M}(G)$ est un D_k-module $A[\underline{F}]$-profini.

On a donc ainsi défini un foncteur contravariant $\underline{M}$, que nous appelons le foncteur <u>module de Dieudonné</u>, de la catégorie des p-groupes formels sur k dans celle des D_k-modules $A[\underline{F}]$-profinis. Il est immédiat que $\underline{M}$ est additif et exact à gauche.

1.3. A tout D_k-module $A[\underline{F}]$-profini M, on associe un k-foncteur en groupes formels $\underline{G}(M)$ en posant

- pour tout k-anneau fini R, $\underline{G}(M)(R) = \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M, \widehat{CW}_k(R))$ est le groupe des applications D_k-linéaires continues de M dans $\widehat{CW}_k(R)$ (où $\widehat{CW}_k(R)$ est muni de sa topologie naturelle, cf. n°II.1.6) ;
- si $\eta : R \to S$ est un morphisme de k-anneaux finis, $\underline{G}(M)(\eta)$ est l'application qui, à $\varphi : M \to \widehat{CW}_k(R)$, associe $\widehat{CW}_k(\eta) \circ \varphi : M \to \widehat{CW}_k(S)$.

Soit M un D_k-module $A[\underline{F}]$-profini . Comme $\widehat{CW}_k$ est un k-groupe formel, c'est un foncteur exact à gauche et on en déduit que $\underline{G}(M)$ est un foncteur exact à gauche, donc que c'est un k-groupe formel (chap.I, prop.4.1).

Soit R un k-anneau fini. On sait (n°II.4.5) que le A-module topologique $\widehat{CW}_k(R)$ est le produit direct de $\widehat{CW}_k^c(R)$ qui est tué par p^m , pour m suffisamment grand, et de $\widehat{CW}_k^{et}(R)$ qui est discret. Comme M est $A[\underline{F}]$-profini, on en déduit que le groupe $\mathrm{Hom}_A^{cont}(M, \widehat{CW}_k(R))$ des applications A-linéaires continues de M dans $\widehat{CW}_k(R)$ est de p-torsion. Il en est a fortiori de même de $\underline{G}(M)(R) = \mathrm{Hom}_{D_k}^{cont}(M, \widehat{CW}_k(R))$. Par conséquent $\underline{G}(M)$ est un p-groupe formel.

On peut considérer $\underline{G}$ comme <u>un foncteur contravariant de la catégorie des</u> D_k-<u>modules</u> $A[\underline{F}]$-<u>profinis dans celle des</u> p-<u>groupes formels sur</u> k : si $\varphi : M \to N$ est un morphisme de D_k-modules $A[\underline{F}]$-profinis, $\underline{G}(\varphi)$ est le morphisme de $\underline{G}(N)$ dans $\underline{G}(M)$ défini par :

$$\begin{cases} \text{pour tout k-anneau fini } R \text{ , } \underline{G}(\varphi)_R : \underline{G}(N)(R) \to \underline{G}(M)(R) \text{ est l'application} \\ \text{qui, à } \psi : N \to \widehat{CW}_k(R) \text{ , associe } \psi \circ \varphi : M \to \widehat{CW}_k(R) \text{ .} \end{cases}$$

Il est clair que $\underline{G}$ est un foncteur additif exact à gauche.

1.4. L'objet essentiel de ce chapitre est de démontrer le résultat suivant :

THEOREME 1.-

i) <u>Les foncteurs</u> $\underline{M}$ <u>et</u> $\underline{G}$ <u>sont adjoints à gauche</u>.

ii) <u>Le foncteur</u> $\underline{M}$ <u>induit une anti-équivalence entre la catégorie des</u> p-<u>groupes formels sur</u> k <u>et celle des</u> D_k-<u>modules</u> $A[\underline{F}]$-<u>profinis, et</u> $\underline{G}$ <u>est un quasi-inverse</u>.

iii) <u>Si</u> G <u>est un groupe fini sur</u> k <u>d'ordre</u> p^r , $\underline{M}(G)$ <u>est un</u> A-<u>module de longueur finie</u> r .

On voit que ce théorème implique que le foncteur $\underline{M}$ est exact, donc que le groupe $\widehat{CW}_k$ est un objet injectif dans la catégorie des p-groupes formels sur k . On a en fait un peu plus :

THEOREME 2.- <u>Le groupe</u> $\widehat{CW}_k$ <u>est un objet injectif dans la catégorie des</u> k-<u>groupes formels</u>.

Comme tout k-groupe formel se décompose de manière unique en le produit direct d'un groupe connexe par un groupe étale, et comme tout k-groupe formel connexe est un p-groupe formel, on voit que la seule chose à démontrer, en sus du théorème 1, est la proposition suivante :

PROPOSITION 1.1.- Le groupe $\widehat{CW}_k^{et}$ est un objet injectif de la catégorie des k-groupes formels étales.

Ce résultat sera démontré au § 2.

Remarque : appelons D_k-module fini tout D_k-module à gauche qui est de longueur finie en tant que A-module. On voit que, muni de la topologie discrète, tout D_k-module fini est $A[\underline{F}]$-profini et même D_k-profini. Le théorème précédent montre donc en particulier, par restriction à des catégories convenables, que

- le foncteur $\underline{M}$ induit une anti-équivalence entre p-groupes finis sur k et D_k-modules finis ;
- il induit aussi une anti-équivalence entre les groupes formels sur k qui sont des limites inductives de p-groupes finis et les D_k-modules profinis.

1.5. Soit G un p-groupe fini sur k . On peut le considérer aussi bien comme un k-groupe affine que comme un k-groupe formel. En particulier, le groupe $G(R)$ est défini pour tout k-anneau R (pas nécessairement fini). Nous nous proposons de déduire du théorème 1 une description de $G(R)$ à l'aide de $\underline{M}(G)$.

PROPOSITION 1.2.- Soit G un p-groupe fini sur k et soit $M = \underline{M}(G)$. Pour tout k-anneau R , le groupe $G(R)$ s'identifie canoniquement (et fonctoriellement en R) au groupe $\mathrm{Hom}_{D_k}(M, CW_k(R))$ des applications D_k-linéaires de M dans $CW_k(R)$.

Démonstration : comme G est fini, M est un D_k-module fini et la topologie de M est la topologie discrète. Si R est un k-anneau fini, on a, d'après le théorème 1, $G(R) = \mathrm{Hom}_{D_k}^{cont}(M, \widehat{CW}_k(R)) = \mathrm{Hom}_{D_k}(M, \widehat{CW}_k(R))$ (car la topologie de M est la topologie discrète) $= \mathrm{Hom}_{D_k}(M, CW_k(R))$ (car $\widehat{CW}_k(R) = CW_k(R)$) et la proposition est vraie.

Dans le cas général, soit $\mathfrak{F}(R)$ l'ensemble des sous-k-anneaux finis de

R . Comme l'algèbre affine de G est un k-anneau fini, on a $G(R) = \varinjlim_{S \in \mathfrak{F}(R)} G(S)$; par conséquent, $G(R)$ s'identifie canoniquement (et fonctoriellement en R) à $\varinjlim_{S \in \mathfrak{F}(R)} \mathrm{Hom}_{D_k}(M, CW_k(S))$. Tout revient donc à montrer que, si u est une application D_k-linéaire de M dans $CW_k(R)$, elle se factorise à travers un $CW_k(S)$, pour un $S \in \mathfrak{F}(R)$ convenable.

Pour cela, choisissons des éléments $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_r$ qui engendrent M en tant que A-module et posons $u(\underline{a}_i) = (\ldots, a_{-n,i}, \ldots, a_{0,i})$. Il est clair qu'il suffit de montrer que le sous-k-anneau S de R engendré par les $a_{-n,i}$, pour $n \in \mathbb{N}$ et $i = 1, 2, \ldots, r$, est fini.

Supposons d'abord G unipotent. Il existe donc un entier s tel que $\underline{V}^s M = 0$. On a donc $a_{-n,i} = 0$, pour $n \geq s$, et il n'y a qu'un nombre fini de $a_{-n,i}$ non nuls. Si, d'autre part, on a, pour $i = 1, 2, \ldots, r$, $\underline{F}\,\underline{a}_i = \sum \lambda_{i,j} \underline{a}_j$, avec les $\lambda_{i,j} \in A$, on doit avoir

$$(\ldots, a^p_{-n,i}, \ldots, a^p_{0,i}) = \sum_{j=1}^{r} \lambda_{i,j}(\ldots, a_{-n,j}, \ldots, a_{0,j}) .$$

Si l'on note $\tilde{\lambda}_{i,j}$ l'image de $\lambda_{i,j}$ dans k , on en déduit facilement que l'on peut écrire

$$a^p_{-n,i} = \sum_{j-1}^{r} \tilde{\lambda}_{i,j} a_{-n,j} + P_{n,i}((a_{-m,j})_{n<m<s\ ,\ 1\leq j\leq r}) ,$$

où les $P_{n,i}$ sont des polynômes à coefficients dans k . On voit alors, que S est engendré, en tant que k-espace vectoriel, par les monômes en les $a_{-n,j}$, pour $0 \leq n < s$ et $1 \leq i \leq r$, de degré $< p$ en chacun d'eux ; c'est donc bien un k-anneau fini.

Supposons maintenant G connexe et soit $\mathfrak{a}$ l'idéal de S engendré par les $a_{-n,i}$. Il existe un entier s tel que $\underline{F}^s M = 0$; on a donc $a^{p^s}_{-n,i} = 0$, pour tout n et tout i , d'où $\mathfrak{a}^{p^s} = 0$. Si, d'autre part, on a, pour $i = 1, 2, \ldots, r$, $\underline{V}\,\underline{a}_i = \sum \mu_{i,j} \underline{a}_j$, on doit avoir

$$(\ldots, a_{-n-1,i}, \ldots, a_{-1,i}) = \sum_{j=1}^{r} \mu_{i,j}(\ldots, a_{-n,j}, \ldots, a_{0,j}) .$$

Si l'on note $\tilde{\mu}_{i,j}$ l'image de $\mu_{i,j}$ dans k , on en déduit facilement que l'on peut écrire

$$a_{-n-1,i} = \sum_{j=1}^{r} \tilde{\mu}_{i,j} a_{-n,j} + P_{n,i}((a_{-m,j})) ,$$

où les $P_{n,i}$ sont des polynômes, à coefficients dans k, sans terme constant, ni termes du premier degré. Comme l'idéal $\mathfrak{a}$ est nilpotent, on en déduit que l'on peut exprimer les $a_{-n,i}$ comme des polynômes en les $a_{0,j}$. Comme $a_{0,j}^{p^s} = 0$, l'anneau S est bien un k-anneau fini.

Le cas général s'en déduit en remarquant que tout p-groupe fini sur k est le produit d'un groupe étale (donc unipotent) par un groupe connexe.

1.6. Montrons que les foncteurs $\underline{M}$ et $\underline{G}$ sont adjoints à gauche. Soit G un p-groupe formel sur k et soit M un D_k-module $A[\underline{F}]$-profini. D'après le lemme de Yoneda, l'ensemble des morphismes de k-foncteurs formels de G dans $\underline{G}(M)$ s'identifie à $\underline{G}(M)(B_G)$ (où B_G désigne l'algèbre affine de G). Si $B_G = \varprojlim_{i\in I} R_i$, avec les R_i des k-anneaux finis, on a

$$\underline{G}(M)(B_G) = \varprojlim \underline{G}(M)(R_i) = \varprojlim \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M, \widehat{CW}_k(R_i)) = \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M, \widehat{CW}_k(B_G))$$

ensemble des applications D_k-linéaires continues de M dans $\widehat{CW}_k(B_G)$. On voit immédiatement que, dans cette identification, une application D_k-linéaire continue de M dans $\widehat{CW}_k(B_G)$ est un morphisme de k-groupes formels si et seulement si son image est contenue dans $\underline{M}(G)$. On a donc ainsi construit une bijection entre le groupe $\mathrm{Hom}(G, \underline{G}(M))$ des morphismes du k-groupe formel G dans $\underline{G}(M)$ et le groupe $\mathrm{Hom}_{D_k}(M, \underline{M}(G))$ des applications D_k-linéaires continues de M dans $\underline{M}(G)$. On vérifie immédiatement que cette bijection est compatible avec les structures de groupe et est fonctorielle en G et M. Les foncteurs $\underline{G}$ et $\underline{M}$ sont donc bien adjoints à gauche.

1.7. Soit M un D_k-module $A[\underline{F}]$-pro-artinien. Nous disons que M est <u>étale</u> (resp. <u>connexe</u>) si $\underline{F}M = M$ (resp. si pour tout $\underline{a} \in M$, la suite des $F^n\underline{a}$ tend vers 0).

PROPOSITION 1.3.- <u>Tout D_k-module $A[\underline{F}]$-pro-artinien s'écrit d'une manière et d'une seule comme la somme directe d'un module étale et d'un module connexe.</u>

<u>Démonstration</u> : soit M un tel module. Soit $M^{et} = \bigcap_{n=0}^{\infty} \underline{F}^n M$ et soit M^c l'ensemble des $\underline{a}$ dans M tels que la suite des $F^n\underline{a}$ tend vers 0.

Il est clair que M^{et} et M^c sont des sous-D_k-modules fermés de M, que M^c est connexe, et que, si N est un sous-D_k-module étale (resp. connexe) de M, alors $N \subset M^{et}$ (resp. $N \subset M^c$). On voit donc qu'il suffit de montrer que $M = M^{et} \oplus M^c$ et que M^{et} est étale.

Remarquons que les définitions de M^{et} et M^c gardent leur signification si M est seulement un $A[\underline{F}]$-module pro-artinien (i.e. si l'action de $\underline{V}$ n'est pas définie). Comme les limites projectives filtrantes sont exactes dans la catégorie des A-modules pro-artiniens, on voit qu'il suffit de démontrer le lemme suivant :

LEMME 1.4.- Soit M un $A[\underline{F}]$-module à gauche, qui est artinien en tant que A-module. Posons $M^{et} = \bigcap_{n=0}^{\infty} \underline{F}^n M$ et soit M^c l'ensemble des $a \in M$ tels que $\underline{F}^n a = 0$, pour n suffisamment grand. Alors $M = M^{et} \oplus M^c$ et $\underline{F}M^{et} = M^{et}$.

Démonstration : comme M est artinien, la suite des $\underline{F}^n M$ est stationnaire. Soit m un entier tel que $\underline{F}^m M = \bigcap_{n=0}^{\infty} \underline{F}^n M$. On a alors $M^{et} = \underline{F}M^{et} = \underline{F}^m M$ et M^c est le noyau de $\underline{F}^m$. Le lemme s'en déduit.

Si M est un D_k-module $A[\underline{F}]$-pro-artinien, et si $M = M^{et} \oplus M^c$, avec M^{et} étale et M^c connexe, nous appelons M^{et} la composante étale de M et M^c la composante connexe de M.

Il résulte de la proposition 4.1 du chapitre II, que si R est un k-anneau fini ou profini, $\widehat{CW}_k^c(R)$ est la composante connexe de $\widehat{CW}_k(R)$ et $\widehat{CW}_k^{et}(R)$ sa composante étale. On en déduit immédiatement que

- si G est un k-groupe formel étale (resp. connexe), $\underline{M}(G)$ est étale (resp. connexe) ;
- si M est un D_k-module $A[\underline{F}]$-profini étale (resp. connexe), le p-groupe formel $\underline{G}(M)$ est étale (resp. connexe).

On voit donc que la démonstration du théorème 1 se décompose en deux parties : le cas étale et le cas connexe. En fait, nous procéderons en trois étapes :

1ère étape : on commence par démontrer l'exactitude de $\underline{M}$ restreint aux k-groupes formels étales, autrement dit, la proposition 1.1 : ce sera fait au

§ 2 , comme conséquence de l'étude du comportement de $\underline{M}$ vis à vis de l'extension des scalaires ;

<u>2e étape</u> : on montre (§ 3) que le noyau de $\underline{V}$ dans $\underline{M}(G)$ s'identifie à l'espace tangent du dual de G et on en déduit le théorème 1 dans le cas étale (proposition 3.4) ;

<u>3e étape</u> : on montre (§ 4) que le quotient $\underline{M}(G)/\underline{F}\,\underline{M}(G)$ s'identifie à l'espace cotangent de G et on en déduit le théorème 1 dans le cas connexe (proposition 4.5).

§ 2.- <u>Extension des scalaires</u>.

2.1. Commençons par établir le résultat suivant :

PROPOSITION 2.1.- <u>Soit</u> k' <u>une extension finie galoisienne de</u> k . <u>Soit</u> M <u>un</u> $W(k')$-<u>module pro-artinien sur lequel</u> $\mathfrak{G} = \mathrm{Gal}(k'/k)$ <u>opère continûment et semi-linéairement</u> (i.e. M <u>est un</u> $W(k)[\mathfrak{G}]$-<u>module et si</u> $g \in \mathfrak{G}$, $a \in W(k')$, $x \in M$, <u>on a</u> $g(ax) = g(a)\,g(x))$. <u>Alors</u>

i) <u>l'application de</u> $W(k') \otimes_{W(k)} M^{\mathfrak{G}}$ <u>dans</u> M <u>qui à</u> $a \otimes x$ <u>associe</u> ax <u>est un isomorphisme</u> ;

ii) <u>le</u> $\mathfrak{G}$-<u>module</u> M <u>est cohomologiquement trivial</u>.

<u>Démonstration</u> : posons $A = W(k)$ et $A' = W(k')$.

Comme A' est un $A[\mathfrak{G}]$-module libre de rang 1 , le $\mathfrak{G}$-module $A' \otimes_A M^{\mathfrak{G}}$ est induit, donc cohomologiquement trivial et la deuxième assertion résulte de la première.

Désignons par $g_1, g_2, \dots, g_n$ les éléments de $\mathfrak{G}$ et par $e_1, e_2, \dots, e_n$ des éléments de A' qui relèvent une base de k' sur k . Il est clair que les e_j forment une base du A-module libre A' et que la matrice des $g_i(e_j)$ est inversible dans A' .

Tout élément de $A' \otimes_A M^{\mathfrak{G}}$ s'écrit, de manière unique, sous la forme $\sum_{j=1}^{n} e_j \otimes a_j$, avec les $a_j \in M^{\mathfrak{G}}$. Si $\sum_{j=1}^{n} e_j a_j = 0$, on a, pour tout i , $0 = g_i(\sum_j e_j a_j) = \sum_j g_i(e_j)\,g_i(a_j) = \sum_j g_i(e_j)\,a_j$. Comme la matrice des $g_i(e_j)$ est inversible dans A' , ceci implique que les a_j sont tous nuls, et l'application considérée est injective.

Montrons que, si $M \neq 0$, alors $M^{\mathcal{G}} \neq 0$: soit en effet x un élément non nul de M . Pour tout j , l'élément $u_j(x) = \sum_{i=1}^{n} g_i(e_j x) = \sum_{i=1}^{n} g_i(e_j) g_i(x)$ appartient à $M^{\mathcal{G}}$. Comme les $g_i(x)$ ne sont pas nuls et comme la matrice des $g_i(e_j)$ est inversible dans A' , les $u_j(x)$ ne sont pas tous nuls.

Montrons la surjectivité dans le cas où M est de longueur finie (en tant que A'-module) : il est clair qu'il suffit de montrer que $\lg_A(M^{\mathcal{G}}) = \lg_{A'}(M)$; on le fait par récurrence sur $\lg_{A'}(M)$:

- c'est clair si $\lg_{A'}(M) = 1$, car alors $M^{\mathcal{G}} \neq 0$ implique que $M^{\mathcal{G}}$ est isomorphe à k et M à k' ;
- supposons $\lg_{A'}(M) > 1$. On sait qu'il existe un élément non nul $x \in M^{\mathcal{G}}$ et il est clair que l'on peut choisir x tel que $px = 0$.

On a alors une suite exacte de A'-modules sur lesquels $\mathcal{G}$ opère semi-linéairement

$$0 \to k' \to M \to M' \to 0$$

à laquelle correspond une suite exacte de A-modules

$$0 \to k \to M^{\mathcal{G}} \to M'^{\mathcal{G}} \to 0$$

car $H^1(\mathcal{G}, k') = 0$. On a donc $\lg_A(M^{\mathcal{G}}) = \lg_A(M'^{\mathcal{G}})+1 = \lg_{A'}(M')+1$ (par hypothèse de récurrence) $= \lg_{A'}(M)$.

La surjectivité dans le cas où M est artinien s'en déduit en remarquant que M est alors la réunion des noyaux de la multiplication par p^r , pour $r \in \mathbb{N}$, et que le noyau de la multiplication par p^r est de longueur finie.

Enfin, si M est pro-artinien et si N est un sous-A'-module ouvert, on voit que $\bigcap_{i=1}^{n} g_i(N)$, qui est stable par $\mathcal{G}$, est encore un sous-A'-module ouvert. Par conséquent, M admet un système fondamental de voisinages ouverts de 0 formés de sous-A'-modules stables par $\mathcal{G}$ et la surjectivité de l'application se déduit, par passage à la limite, de la surjectivité dans le cas artinien.

2.2. Soit k' une extension finie de k ; posons encore $A = W(k)$ et $A' = W(k')$.

Si M est un D_k-module topologique, l'action de $\underline{F}$ et de $\underline{V}$ se prolonge au A'-module $A' \otimes_A M$ en posant

$$\begin{cases} \underline{F}(a \otimes x) = \sigma(a) \otimes \underline{F}x \\ \underline{V}(a \otimes x) = \sigma^{-1}(a) \otimes \underline{V}x \end{cases} \quad \text{si} \quad a \in A' \ , \ x \in M \ ,$$

et $A' \otimes_A M$ devient ainsi un $D_{k'}$-module topologique qui est $A'[\underline{F}]$-profini (resp. pro-artinien) si M est $A[\underline{F}]$-profini (resp. pro-artinien).

Supposons k'/k galoisienne et soit $\mathcal{G} = \mathrm{Gal}(k'/k)$. Si R est un k-anneau profini, $\mathcal{G}$ opère continûment et semi-linéairement sur le k'-anneau profini $k' \otimes_k R$ et l'on a $(k' \otimes_k R)^{\mathcal{G}} = R$.

D'autre part, il est clair que $\widehat{CW}_{k'} = \widehat{CW}_k \otimes_k k'$. Par fonctorialité, $\mathcal{G}$ opère continûment et semi-linéairement sur le A'-module pro-artinien $\widehat{CW}_{k'}(k' \otimes_k R)$. Si $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_o) \in \widehat{CW}_{k'}(k' \otimes_k R)$, on voit que $\underline{a} \in (\widehat{CW}_{k'}(k' \otimes_k R))^{\mathcal{G}}$ si et seulement si chaque $a_{-n} \in (k' \otimes_k R)^{\mathcal{G}} = R$. Donc $(\widehat{CW}_{k'}(k' \otimes_k R))^{\mathcal{G}}$ s'identifie à $\widehat{CW}_k(R)$.

Pour tout p-groupe formel G' sur k' , notons $\underline{M}'(G')$ le $D_{k'}$-module $A'[\underline{F}]$-profini $\mathrm{Hom}(G', \widehat{CW}_{k'})$. Si G est un p-groupe formel sur k d'algèbre affine B_G , on a (cf. n° 1.2), avec des notations évidentes,

$$\underline{M}'(G_{k'}) = \{\underline{a} \in \widehat{CW}_{k'}(k' \otimes_k B_G) \mid \Delta\underline{a} = \underline{a} \hat{\otimes} 1 + 1 \hat{\otimes} \underline{a}\}$$

et

$$\underline{M}(G) = \{\underline{a} \in \widehat{CW}_k(B_G) \mid \Delta\underline{a} = \underline{a} \hat{\otimes} 1 + 1 \hat{\otimes} \underline{a}\} \ .$$

Par conséquent, $\underline{M}(G) = (\underline{M}'(G_{k'}))^{\mathcal{G}}$.

La proposition 2.1 implique alors que $\underline{M}'(G_{k'})$ s'identifie à $A' \otimes_A \underline{M}(G)$. Le même résultat reste vrai si l'extension finie k'/k n'est pas galoisienne comme on le voit en plongeant k' dans une extension finie galoisienne k'' de k et en regardant l'action de $\mathrm{Gal}(k''/k)$.

On a donc démontré le résultat suivant :

PROPOSITION 2.2.- <u>Soit</u> k' <u>une extension finie de</u> k <u>et soit</u> G <u>un p-groupe formel sur</u> k . <u>Posons</u> $M = \underline{M}(G)$ <u>et</u> $M' = \underline{M}'(G_{k'}) = \mathrm{Hom}(G_{k'}, \widehat{CW}_{k'})$.

i) <u>L'application naturelle de</u> $W(k') \otimes_{W(k)} M$ <u>dans</u> M' <u>est un isomor-</u>

phisme.

ii) Supposons l'extension k'/k galoisienne et soit $\mathcal{G} = \mathrm{Gal}(k'/k)$. Le groupe $\mathcal{G}$ opère semi-linéairement et continûment sur M' et $M = (M')^{\mathcal{G}}$.

2.3. Nous allons maintenant démontrer la proposition 1.1 (cf. n°1.4).

Soit $\bar{k}$ une clôture algébrique de k. Si G est un k-groupe formel étale, notons $G(\bar{k})$ la réunion des $G(k')$ pour k' parcourant les extensions finies de k contenues dans $\bar{k}$. Si $\mathcal{G}_k = \mathrm{Gal}(\bar{k}/k)$, $G(\bar{k})$ est un $\mathcal{G}_k$-module discret et le foncteur $G \mapsto G(\bar{k})$ induit une équivalence entre la catégorie des k-groupes formels étales et celle des $\mathcal{G}_k$-modules discrets (n°I.7.1).

Rappelons (n°II.2.3) que, si l'on note A_{nr} la limite inductive des $W(k')$, pour k' parcourant les extensions finies de k contenues dans $\bar{k}$, et K_{nr} le corps des fractions de A_{nr}, le $\mathcal{G}_k$-module $\widehat{CW}_k^{et}(\bar{k}) = \widehat{CW}_k(\bar{k})$ s'identifie à K_{nr}/A_{nr}. La proposition 1.1 est donc équivalente à la proposition suivante :

PROPOSITION 2.3.- Le module K_{nr}/A_{nr} est un objet injectif de la catégorie des $\mathcal{G}_k$-modules discrets.

Démonstration : Soit $\mathcal{U}$ un sous-groupe invariant ouvert de $\mathcal{G}_k$ et soit k' le corps fixe de $\mathcal{U}$. Soit $A' = W(k')$ et soit K' le corps des fractions de A'. On voit que $(K_{nr}/A_{nr})^{\mathcal{U}}$ s'identifie à K'/A'. Posons $\mathcal{G} = \mathrm{Gal}(k'/k) = \mathcal{G}_k/\mathcal{U}$. Nous allons commencer par montrer que K'/A' est un $\mathcal{G}$-module injectif.

Soit Γ un $\mathcal{G}$-module quelconque. On voit facilement que le groupe $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, K'/A')$ peut être considéré comme un A'-module pro-artinien sur lequel $\mathcal{G}$ opère continûment et semi-linéairement (la structure de A'-module et l'action de $\mathcal{G}$ sont évidentes ; la topologie est celle de la convergence simple ; comme $\mathcal{G}$ est un groupe fini, Γ est réunion de ses sous-$\mathbb{Z}[\mathcal{G}]$-modules Γ_f qui sont de type fini sur $\mathbb{Z}$; chaque $\mathrm{Hom}_{\mathbb{Z}}(\Gamma_f, K'/A')$ est visiblement un A'-module artinien et $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, K'/A')$, qui est la limite projective des $\mathrm{Hom}_{\mathbb{Z}}(\Gamma_f, K'/A')$ est pro-artinien).

Considérons alors une suite exacte de $\mathcal{G}$-modules

$$0 \to \Gamma' \to \Gamma \to \Gamma'' \to 0 .$$

Comme K'/A' est divisible, il lui correspond une suite exacte

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma'',K'/A') \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma,K'/A') \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma',K'/A') \to 0 .$$

D'après la proposition 2.1, $\mathrm{Hom}_{\mathbb{Z}}(\Gamma'',K'/A')$ est cohomologiquement trivial et la suite

$$0 \to \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma'',K'/A') \to \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma,K'/A') \to \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma',K'/A') \to 0$$

est encore exacte. Et K'/A' est bien un $\mathcal{G}$-module injectif.

Pour achever la démonstration de la proposition, il suffit alors d'établir l'assertion suivante :

PROPOSITION 2.4.- Soit Δ un $\mathcal{G}_k$-module discret. Pour que Δ soit injectif (dans la catégorie des $\mathcal{G}_k$-modules discrets) il faut et il suffit que, pour tout sous-groupe ouvert invariant $\mathcal{U}$ de $\mathcal{G}_k$, $\Delta^{\mathcal{U}}$ soit un $(\mathcal{G}_k/\mathcal{U})$-module injectif.

Commençons par établir un lemme :

LEMME 2.5.- Soit R un anneau et soit M un R-module à gauche. Soient Δ et N deux sous-modules de M tels que $\Delta \cap N = \{0\}$. On suppose Δ injectif. Alors il existe un sous-module N' de M contenant N tel que $M = \Delta \oplus N'$.

Démonstration du lemme : soit $\overline{M} = M/N$. Le sous-module Δ s'envoie injectivement sur son image $\overline{\Delta}$ dans $\overline{M}$. Comme Δ, donc $\overline{\Delta}$, est injectif, il existe un sous-module $\overline{N}'$ de $\overline{M}$ tel que $\overline{M} = \overline{\Delta} \oplus \overline{N}'$. On voit que l'image réciproque N' de $\overline{N}'$ dans M répond à la question.

Démonstration de la prop. 2.4 : si $\mathcal{U}$ est un sous-groupe ouvert invariant de $\mathcal{G}_k$, et si on pose $\mathcal{G} = \mathcal{G}_k/\mathcal{U}$, tout $\mathcal{G}$-module peut être considéré comme un $\mathcal{G}_k$-module discret sur lequel $\mathcal{U}$ opère trivialement. Pour un tel module M, on voit que $\mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(M,\Delta^{\mathcal{U}}) = \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}_k]}(M,\Delta)$ et on en déduit que $\Delta^{\mathcal{U}}$ est injectif si Δ l'est.

Réciproquement, soit M un $\mathcal{G}_k$-module discret contenant Δ et soit N un sous-$\mathcal{G}_k$-module de M tel que $N \cap \Delta = 0$ et qui est maximal pour cette propriété. Pour tout sous-groupe ouvert invariant $\mathcal{U}$ de $\mathcal{G}_k$, on voit que $N^{\mathcal{U}}$ est un sous-$(\mathcal{G}_k/\mathcal{U})$-module de $M^{\mathcal{U}}$ vérifiant $N^{\mathcal{U}} \cap \Delta^{\mathcal{U}} = 0$. Supposons $\Delta^{\mathcal{U}}$ injectif. D'après le lemme précédent, il existe un sous-$(\mathcal{G}_k/\mathcal{U})$-module N' de

$M^{\mathcal{U}}$ contenant $N^{\mathcal{U}}$ tel que $M^{\mathcal{U}} = \Delta^{\mathcal{U}} \oplus N'$. Si, avec des notations évidentes, $n+n' = \delta \in (N+N') \cap \Delta$, on a, pour tout $g \in \mathcal{U}$, $(g-1)n = (g-1)\delta = 0$, puisque $N \cap \Delta = 0$; par conséquent $\delta \in \Delta^{\mathcal{U}}$ et $n \in N'$. On a donc $(N+N') \cap \Delta = 0$, d'où $N+N' = N$, ce qui implique $N' = N$. Si les $\Delta^{\mathcal{U}}$ sont tous injectifs, on a donc $M^{\mathcal{U}} = \Delta^{\mathcal{U}} \oplus N^{\mathcal{U}}$, pour tout $\mathcal{U}$, d'où $M = \Delta \oplus N$, car $M = \varinjlim M^{\mathcal{U}}$.

2.4. Conservons les notations du n°2.3. Nous allons établir un résultat qui ramène la démonstration du théorème 1 dans le cas étale au cas fini :

PROPOSITION 2.6.-

i) <u>Tout</u> p-<u>groupe étale</u> G <u>est réunion de ses sous-groupes finis et le</u> D_k-<u>module topologique</u> $\underline{M}(G)$ <u>s'identifie à</u> $\varprojlim \underline{M}(G_f)$, <u>pour</u> G_f <u>parcourant les sous-groupes finis de</u> G.

ii) <u>Tout</u> D_k-<u>module</u> $A[\underline{F}]$-<u>profini étale est</u> D_k-<u>profini</u> (i.e. <u>admet un système fondamental de voisinages ouverts de</u> 0 <u>formé de sous</u>-D_k-<u>modules</u>). <u>Si</u> M <u>est un tel module</u>, <u>le</u> p-<u>groupe formel étale</u> $\underline{G}(M)$ <u>s'identifie à</u> $\varinjlim \underline{G}(M/N)$, <u>pour</u> N <u>parcourant les sous</u>-D_k-<u>modules ouverts de</u> M.

<u>Démonstration</u> :

i) Soit Γ un $\mathcal{G}_k$-module discret de p-torsion, soit $\mathcal{U}$ un sous-groupe invariant ouvert de $\mathcal{G}_k$ et soit $\mathcal{G} = \mathcal{G}_k/\mathcal{U}$. Comme $\mathcal{G}$ est un groupe fini, le $\mathcal{G}$-module $\Gamma^{\mathcal{U}}$ est réunion de ses sous-$\mathcal{G}$-modules qui sont de type fini sur $\mathbb{Z}$; comme Γ est de torsion, un tel sous-module est un groupe fini. Comme Γ est la réunion des $\Gamma^{\mathcal{U}}$, pour $\mathcal{U}$ parcourant les sous-groupes invariants ouverts de $\mathcal{G}_k$, on voit que Γ est la réunion de ses sous-$\mathcal{G}$-modules qui sont des groupes finis. L'équivalence de catégorie entre p-groupes formels étales et $\mathcal{G}_k$-modules discrets qui sont de p-torsion montre que si G est un p-groupe formel étale, G est la réunion de ses sous-groupes finis G_f. On a alors $\underline{M}(G) = \mathrm{Hom}(G, \widehat{CW}_k) = \mathrm{Hom}(\varinjlim G_f, \widehat{CW}_k) = \varprojlim \mathrm{Hom}(G_f, \widehat{CW}_k) = \varprojlim \underline{M}(G_f)$.

ii) Soit M un D_k-module $A[\underline{F}]$-profini et soit Ω_M l'ensemble des sous-$A[\underline{F}]$-modules ouverts de M. On sait que Ω_M est un système fondamental de voisinages ouverts de 0. Pour tout $N \in \Omega_M$, le quotient M/N est un $A[\underline{F}]$-module, de longueur finie en tant que A-module. Si M est étale, on a $\underline{F}M = M$ et on en déduit que $\underline{F}$ est surjectif sur le quotient, donc aussi injectif. Si $x \in N$, x s'écrit $\underline{F}y$, pour un certain $y \in M$; comme l'image de $\underline{F}y$ dans le quotient est nulle, $y \in N$, donc $\underline{V}x = py$ aussi. Les éléments de Ω_M sont donc tous des sous-D_k-modules.

On sait (cf. n° 1.7) que si M est étale, $\underline{G}(M)$ est un p-groupe formel étale. Pour montrer que $\underline{G}(M) = \varinjlim_{N \in \Omega_M} \underline{G}(M/N)$, il suffit donc de montrer que, pour toute extension finie k' de k , $\underline{G}(M)(k') = \varinjlim_{N \in \Omega_M} \underline{G}(M/N)(k')$. Or $\underline{G}(M)(k') = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(k')) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, K'/A')$, groupe des applications D_k-linéaires continues de M dans K'/A' . Comme K'/A' est discret, la continuité implique que le noyau d'une telle application est ouvert et $\underline{G}(M)(k') = \varinjlim_{N \in \Omega_M} \mathrm{Hom}_{D_k}(M/N, K'/A') = \varinjlim_{N \in \Omega_M} \underline{G}(M/N)(k')$.

§ 3.- Module de Dieudonné et espace tangent.

3.1. Soit G un p-groupe formel sur k , soit B_G son algèbre affine et soit I_G l'idéal d'augmentation de B_G . Soit $V_B = V_{B_G}$ le décalage comme endomorphisme de l'anneau B_G (n° I.7.5). Il est clair que $V_B(I_G) \subset I_G$. Si G est étale, pour tout $a \in I_G$, la suite des $V_B^n(a)$ tend vers 0 . Autrement dit, pour tout $a \in I_G$ et pour chaque composante locale B_i de B_G , les projections des $V_B^n(a)$ dans B_i sont nulles pour n suffisamment grand. Dans le cas où G est quelconque, ceci implique que, pour tout $a \in I_G$ et pour chaque composante locale B_i de B , les projections des $V_B^n(a)$ dans B_i sont presque toutes dans l'idéal maximal de B_i . Par conséquent (n° II.4.4), le covecteur

$$a^w = (\ldots, a_{-n}, \ldots, a_{-1}, a_o) \text{ , avec } a_{-n} = V_B^n(a) \text{ pour } n \in \mathbb{N} \text{ ,}$$

est un élément de $\widehat{CW}_k(B_G)$.

Nous notons B_G^w l'ensemble des éléments de $\widehat{CW}_k(B_G)$ qui sont de la forme a^w , pour un $a \in I_G$. On voit que B_G^w est un sous-D_k-module fermé de $\widehat{CW}_k(B_G)$.

L'application $a \mapsto a^w$ définit une bijection de I_G sur B_G^w . On voit que c'est en fait un homéomorphisme (si I_G est muni de la topologie induite par celle de B_G).

Soit maintenant $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_o)$ un élément de $\underline{M}(G)$. On voit facilement que l'égalité $\Delta_G(a) = a\hat{\otimes}1 + 1\hat{\otimes}a$ implique que tous les a_{-n} sont dans I_G . Comme dans l'algèbre affine de $\widehat{CW}_k$, le décalage envoie X_{-n} sur X_{-n-1} (n°II.4.3, remarque 1), on voit que

$$\underline{V}\underline{a} = (\dots,a_{-n-1},\dots,a_{-2},a_{-1}) = (\dots,V_B(a_{-n}),\dots,V_B(a_{-1}),V_B(a_o)) .$$

Donc, pour tout n , $V_B(a_{-n}) = a_{-n-1}$ et $\underline{a} \in B_G^W$. On a donc démontré le résultat suivant :

PROPOSITION 3.1.- Si G est un p-groupe formel sur k et si B_G est son algèbre affine, $\underline{M}(G)$ est un sous-D_k-module fermé de B_G^W . En particulier, l'application qui à $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_o) \in \underline{M}(G)$ associe $a_o \in I_G$ est injective et continue.

3.2. Regardons maintenant quel est le noyau de $\underline{V}$ dans $\underline{M}(G)$. C'est l'ensemble des $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_o) \in \underline{M}(G)$ tels que $a_{-n}=0$ si $n\geq 1$. Par conséquent, le noyau de $\underline{V}$ s'identifie à l'ensemble des $a_o \in I_G$ tels que $\Delta_G(a_o) = a_o\hat{\otimes}1 + 1\hat{\otimes}a_o$, ou encore (n°I.8.6) à l'ensemble $\mathrm{Hom}(G,\hat{G}_a)$ des morphismes du k-groupe formel G dans le complété formel du groupe additif. Le noyau de $\underline{V}$ dans $\underline{M}(G)$ est, d'autre part, un sous-D_k-module fermé N de $\underline{M}(G)$ tel que $\underline{V}N = 0$. C'est donc un $D_k/\underline{V}D_k = k[\underline{F}]$-module topologique. On a vu au n°I.8.7 que $\mathrm{Hom}(G,\hat{G}_a)$ a une structure naturelle de $k[\underline{F}]$-module topologique. On vérifie immédiatement que, dans l'identification qui précède les deux structures de $k[\underline{F}]$-modules topologiques coïncident.

Si $\mathbb{D}(G)$ désigne le dual de Cartier de G , on sait (n°I.8.7) que $\mathrm{Hom}(G,\hat{G}_a)$ s'identifie au $k[\underline{F}]$-module topologique $t_{\mathbb{D}(G)}(k)$. On peut donc énoncer :

PROPOSITION 3.2.- Soit G un p-groupe formel sur k . L'application, qui à $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_o)$ associe a_o , définit, par restriction au noyau de $\underline{V}$, un isomorphisme du noyau de $\underline{V}$ dans $\underline{M}(G)$ sur le $k[\underline{F}]$-module topologique $\mathrm{Hom}(G,\hat{G}_a) \simeq t_{\mathbb{D}(G)}(k)$.

3.3. La démonstration du théorème 1 dans le cas étale utilise le résultat suivant :

PROPOSITION 3.3.-

i) Soit G un p-groupe fini sur k, d'ordre p^r, tel que $V_G = 0$. Alors $\underline{M}(G)$ est un D_k-module fini vérifiant $\underline{V}\,\underline{M}(G) = 0$ dont la longueur sur A est égale à r.

ii) Soit M un D_k-module fini, de longueur sur A égale à r, vérifiant $\underline{V}\,M = 0$. Alors $\underline{G}(M)$ est un groupe fini sur k, d'ordre p^r, tel que $V_G = 0$.

Démonstration :

i) Posons $M = \underline{M}(G)$. Il est clair que $\underline{V}\,M = 0$. Par conséquent, d'après la proposition 3.2, M s'identifie à $t_{\mathbb{D}(G)}(k)$. Le fait que $V_G = 0$ implique que $F_{\mathbb{D}(G)} = 0$; comme $\mathbb{D}(G)$ a le même ordre que G, on voit que l'algèbre affine de $\mathbb{D}(G)$ est de la forme $k[x_1,x_2,\dots,x_r]/(x_1^p,x_2^p,\dots,x_r^p)$. En particulier, $t^*_{\mathbb{D}(G)}(k) = I_{\mathbb{D}(G)}/I^2_{\mathbb{D}(G)}$ est un espace vectoriel sur k de dimension r, donc aussi son dual $t_{\mathbb{D}(G)}(k)$.

ii) Si $\underline{V}\,M = 0$, on a $pM = 0$ et M est un $k[\underline{F}]$-module, de dimension r sur k. Soit $G = \underline{G}(M)$. Pour tout k-anneau fini R, on a $G(R) = \mathrm{Hom}_{D_k}(M, CW_k(R))$. Comme $\underline{V}\,M = 0$ et comme le noyau de $\underline{V}$ dans $CW_k(R)$ est formé des covecteurs $(\dots,0,\dots,0,a_o)$, on voit que $G(R)$ s'identifie à $\mathrm{Hom}_{k[\underline{F}]}(M,R)$ (où R est muni de sa structure évidente de $k[\underline{F}]$-module à gauche, $\underline{F}$ opérant par $\underline{F}y = y^p$, pour tout $y \in R$).

Soit $(u_i)_{1\le i\le r}$ une base de M sur k. Pour tout j compris entre 1 et r, posons $\underline{F}u_j = \sum_{i=1}^{r} a_{i,j}u_i$, avec les $a_{i,j} \in k$. Si η est une application k-linéaire de M dans R, et si $\eta(u_i) = y_i$, on voit que η est un élément de $G(R)$ si et seulement si, pour tout j, $\eta(\underline{F}u_j) = \underline{F}\eta(u_j)$, i.e. si $y_j^p = \sum_i a_{i,j}y_i$. Par conséquent, l'algèbre affine de G s'identifie au quotient B_G de l'anneau $k[x_1,x_2,\dots,x_r]$ par l'idéal engendré par les $x_j^p - \sum_i a_{i,j}x_i$. Les images des $x_1^{i_1}x_2^{i_2}\dots x_r^{i_r}$, pour $0 \le i_j < p$, forment une base de B_G sur k, donc B_G est un espace vectoriel sur k de dimension p^r, autrement dit G est d'ordre p^r. Comme l'addition dans $G(R)$ est induite par l'addition dans R, on voit que le coproduit dans B_G est défini par $\Delta x_i = x_i\hat{\otimes}1 + 1\hat{\otimes}x_i$. Par conséquent $V_G = 0$.

3.4. Nous allons terminer ce paragraphe en démontrant le théorème 1 dans le cas étale. On sait (cf. n° 1.6) que les foncteurs $\underline{M}$ et $\underline{G}$ sont adjoints à gauche. Il suffit donc de prouver la proposition suivante :

PROPOSITION 3.4.-

i) Si G est un p-groupe fini étale d'ordre p^r, $M(G)$ est un A-module de longueur r.

ii) Pour tout p-groupe formel étale G, le morphisme de G dans $\underline{G}\,\underline{M}(G)$ provenant de l'adjonction est un isomorphisme.

iii) Pour tout D_k-module $A[\underline{F}]$-profini étale M, l'homomorphisme de M dans $\underline{M}\underline{G}(M)$ provenant de l'adjonction est un isomorphisme.

Démonstration :

i) Si G est un p-groupe fini étale simple, on a $V_G = 0$, et l'assertion (i) est vraie, d'après la proposition 3.3. Le cas général s'en déduit par récurrence sur la longueur de G, en utilisant le fait (cf. n° 2.3) que $\underline{M}$, restreint aux k-groupes formels étales, est exact.

ii) D'après la proposition 2.6, on voit, par passage à la limite, qu'il suffit de démontrer l'assertion (ii) dans le cas où G est fini. Notons $u_G : G \to \underline{G}\,\underline{M}(G)$ le morphisme défini par l'adjonction.

- Si G est simple, d'ordre p^r, on a $V_G = 0$. Par conséquent, d'après la proposition 3.3, $\underline{M}(G)$ vérifie $\underline{V}\,\underline{M}(G) = 0$ et est un A-module de longueur r, donc $\underline{G}\underline{M}(G)$ est encore d'ordre p^r. Si u_G n'était pas un isomorphisme, on aurait donc $u_G = 0$, donc $\underline{M}(u_G) = 0$. C'est impossible, puisque $\underline{M}(u_G) : \underline{M}\,\underline{G}\,\underline{M}(G) \to \underline{M}(G)$ est un épimorphisme et $\underline{M}(G) \neq 0$.

- Le cas général s'en déduit par récurrence sur la longueur de G : En effet, comme $\underline{M}$ restreint aux k-groupes formels étales est exact, à toute suite exacte de p-groupes finis étales de la forme

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

correspond une suite exacte

$$0 \longrightarrow \underline{M}(G'') \longrightarrow \underline{M}(G) \longrightarrow \underline{M}(G') \longrightarrow 0\ ,$$

d'où un diagramme commutatif

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\
 & & \downarrow u_{G'} & & \downarrow u_G & & \downarrow u_{G''} & & \\
0 & \longrightarrow & \underline{G}\underline{M}(G') & \longrightarrow & \underline{G}\underline{M}(G) & \longrightarrow & \underline{G}\underline{M}(G'') & &
\end{array}$$

où les lignes sont exactes. On en déduit que u_G est un isomorphisme si $u_{G'}$ et $u_{G''}$ en sont.

iii) De même, par passage à la limite, en utilisant la proposition 2.6, on voit qu'il suffit de démontrer l'assertion (iii) dans le cas où M est de longueur finie sur A.

Notons $v_M : M \to \underline{M}\underline{G}(M)$ le morphisme défini par l'adjonction.

- Si M est simple, le même raisonnement qu'en (ii) montre que v_M est un isomorphisme.

- Le cas général s'en déduit par récurrence sur la longueur de M (en tant que D_k-module) : A toute suite exacte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

de D_k-modules finis étales, correspond une suite exacte

$$0 \longrightarrow \underline{G}(M'') \longrightarrow \underline{G}(M) \longrightarrow \underline{G}(M') .$$

Comme les groupes $\underline{G}(M'')$, $\underline{G}(M)$ et $\underline{G}(M')$ sont étales et comme M restreint aux groupes étales est exact, on a un diagramme commutatif

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow v_{M'} & & \downarrow v_M & & \downarrow v_{M''} & & \\
 & & \underline{M}\underline{G}(M') & \longrightarrow & \underline{M}\underline{G}(M) & \longrightarrow & \underline{M}\underline{G}(M'') & \longrightarrow & 0
\end{array}$$

où les lignes sont exactes. On en déduit que, si $v_{M'}$ et $v_{M''}$ sont des isomorphismes, v_M est un épimorphisme. Soit N le noyau de v_M . Comme $\underline{G}$ est exact à gauche et comme $\underline{G}(v_M)$ est un épimorphisme, on voit que $\underline{G}(N) = 0$.

Supposons $N \neq 0$. Comme N est étale, $\underline{V}N = \underline{V}\underline{F}N = pN$ et $N/\underline{V}N = N/pN \neq 0$. D'après la proposition 3.3, on aurait donc $\underline{G}(N/\underline{V}N) \neq 0$, d'où, a fortiori, $\underline{G}(N) \neq 0$. Par conséquent, $N = 0$ et v_M est un isomorphisme.

§ 4.- Module de Dieudonné et espace cotangent.

4.1. Rappelons (cf. n°3.1) que, si G est un p-groupe formel sur k, tout élément de $\underline{M}(G)$ est de la forme b_0^w, pour un b_0 appartenant à l'idéal d'augmentation de l'algèbre affine de G.

PROPOSITION 4.1.- Soit G un p-groupe formel sur k. Soit B_G son algèbre affine et soit I_G l'idéal d'augmentation. Pour tout $b \in I_G$ il existe $b_o \in I_G$ vérifiant $b_o \equiv b$ modulo l'adhérence de I_G^2 tel que $b_0^w \in \underline{M}(G)$.

Démonstration : comme ce résultat est trivialement vrai si G est étale, on peut supposer G connexe non réduit à 0.

Pour tout entier $m \geq 0$, notons $B_m = \hat{\otimes}^m B$ l'algèbre affine de G^m et I_m son idéal d'augmentation ; notons aussi, pour tout entier $r \geq 1$, $I_{m,r}$ l'adhérence de I_m^r dans B_m.

Soit $\hat{G}_a$ le complété formel du groupe additif sur k. Si l'on considère le complexe $C^\cdot(G,\hat{G}_a)$ (n°I.10.4), on voit que le groupe des m-cochaînes $C^m(G,\hat{G}_a)$ s'identifie à B_m. Nous notons $\partial_a : B_m \to B_{m+1}$ l'opérateur bord correspondant. Il est clair que $\partial_a(I_m) \subset I_{m+1}$.

Considérons d'autre part le complexe $C^\cdot(G,\widehat{CW}_k)$. Le groupe des m-cochaînes s'identifie à $\widehat{CW}_k(B_m)$ et contient B_m^w (i.e. l'ensemble des $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_o) \in \widehat{CW}_k(B_m)$ tels que $a_o \in I_m$ et $a_{-n} = V_{B_m}^n(a_o)$, pour tout n). On voit que les B_m^w forment un sous-complexe de $C^\cdot(G,\widehat{CW}_k)$, i.e. que l'image par l'opérateur bord de B_m^w est contenue dans B_{m+1}^w. Lorsque l'on identifie B_m^w à I_m (en envoyant $\underline{a} = (\ldots,a_{-n},\ldots,a_o)$ sur a_o) l'opérateur bord induit une application, que nous notons ∂_w, de I_m dans I_{m+1} (on a donc $(\partial_w a)^w = \partial(a^w)$ si ∂ est l'opérateur bord).

On a donc $\partial_w \circ \partial_w = 0$, mais l'application ∂_w n'est pas en général k-linéaire, ni même additive. Toutefois, si $c \in I_{m,r}$, on a $c^w = (\ldots,c_{-n},\ldots,c_o)$, avec $c_o = c$ et $c_{-n} = V_{B_m}^n(c_o) \in I_{m,r}$, et on en déduit immédiatement que

(1_1) si $a \in I_m$ et $c \in I_{m,r}$, alors $\partial_w(a-c) \equiv \partial_w a - \partial_w c \pmod{I_{m+1,r+1}}$,

(1_2) si $c \in I_{m,r}$, alors $\partial_w c \equiv \partial_a c \pmod{I_{m+1,r+1}}$.

On voit que, si $b_0 \in I_1$, on a $b_0^w \in \underline{M}(G)$ si et seulement si $\partial_w(b_0)=0$.

Pour tout $b \in I_1$, on voit que $\partial_w b \equiv \partial_a b \equiv 0 \pmod{I_{2,2}}$; comme G est connexe, I_1 et I_2 sont topologiquement nilpotents et, compte-tenu de (1_1), pour démontrer la proposition, il suffit de prouver le lemme suivant :

LEMME 4.2.- Soit r un entier ≥ 2 et soit $b \in I_1$ tel que $\partial_w b \in I_{2,r}$. Il existe $c \in I_{1,r}$ tel que $\partial_w b \equiv \partial_w c \pmod{I_{2,r+1}}$.

Démonstration : posons $b' = \partial_w b$. On voit que b' est un tenseur symétrique de $I_{2,r}$ et que $\partial_w b' = \partial_w(\partial_w b) = 0$. D'après (1_2), on a $\partial_a b' \equiv 0 \pmod{I_{3,r+1}}$.

Si r n'est pas une puissance de p, il résulte de la proposition 10.5 du chapitre I qu'il existe $c \in I_{1,r}$ tel que $b' \equiv \partial_a c \pmod{I_{2,r+1}}$. D'après (1_2) on a $\partial_a c \equiv \partial_w c \pmod{I_{2,r+1}}$ donc $\partial_w b \equiv \partial_w c \pmod{I_{2,r+1}}$.

Supposons donc que $r = p^s$, avec $s \geq 1$. Choisissons (cf. n° I.9.1) un k-homomorphisme continu θ d'un anneau de séries formelles $k[[(X_j)_{j\in J}]]$ sur B_G tel que le noyau de θ soit l'adhérence de l'idéal engendré par les $X_j^{p^{\nu(j)}}$, pour $\nu(j) \neq +\infty$ (où les $\nu(j)$ sont des éléments convenables de $\mathbb{N}^* \cup \{+\infty\}$, vérifiant $\nu(j) \geq 2$) et posons $\theta(X_j) = x_j$. Si $\Lambda(X,Y) = p^{-1}((X+Y)^p - X^p - Y^p)$, la proposition 10.5 du chapitre I montre qu'il existe $c \in I_{1,r}$ et des $\lambda_j \in k$ tels que

$$b' \equiv \partial_a c + \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}} ,$$

la sommation étant étendue aux $j \in J$ tels que $s \leq \nu(j)$.

Les formules (1_1) et (1_2) montrent que

$$(2) \qquad \partial_w(b-c) \equiv \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}}$$

et, pour achever la démonstration du lemme, il suffit de vérifier que ceci implique la nullité de tous les λ_j.

Pour tout entier $m \geq 2$, posons

$$T_m(X_1, X_2, \dots, X_m) = p^{-1}((X_1+X_2+\dots+X_m)^p - X_1^p - X_2^p - \dots - X_m^p) ;$$

c'est un polynôme à coefficients entiers rationnels. On voit que $T_2(X,Y) = \Lambda(X,Y)$ et que, pour tout entier $m \geq 2$,

(3) $\quad \Lambda(X_1,X_2) + T_m(X_1+X_2,X_3,\dots,X_{m+1}) = T_{m+1}(X_1,X_2,\dots,X_{m+1})$.

Pour $u_1,u_2 \in I_m$, notons $u_1 \oplus u_2$ l'unique $v \in I_m$ tel que $u_1^w + u_2^w = v^w$. Il est clair que $\oplus$ munit I_m d'une loi de groupe abélien et que

(4) $\quad$ si $u_1 \in I_m$ et $u_2 \in I_{m,r}$, $u_1 \oplus u_2 \equiv u_1 + u_2 \pmod{I_{m,r+1}}$.

Si on pose $a = b-c$, la formule (2) se réécrit

(2') $\quad \partial_w(a) \equiv \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}}$.

On voit tout de suite que $\Delta a = (a \hat{\otimes} 1) \oplus (1 \hat{\otimes} a) \ominus \partial_w(a)$; on a donc, d'après (4) ,

(5) $\quad \Delta a \equiv ((a \hat{\otimes} 1) \oplus (1 \hat{\otimes} a)) - \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}}$.

Pour tout $m \geq 2$, soient α_m et β_m les éléments de I_m définis par

$$\alpha_m = (a \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1) \oplus (1 \hat{\otimes} a \hat{\otimes} \dots \hat{\otimes} 1) \oplus \dots \oplus (1 \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} a) ,$$

$$\beta_m = \sum \lambda_j T_m(x_j^{p^{s-1}} \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1, 1 \hat{\otimes} x_j^{p^{s-1}} \hat{\otimes} \dots \hat{\otimes} 1, \dots, 1 \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} x_j^{p^{s-1}}) .$$

Notons Δ_m le m-ième itéré de Δ (on a $\Delta_2 = \Delta$, $\Delta_3 = (\Delta \hat{\otimes} 1) \circ \Delta$,...). Par récurrence, on montre que, pour tout $m \geq 2$,

(6) $\quad \Delta_m a \equiv \alpha_m - \beta_m \pmod{I_{m,r+1}}$:

pour $m = 2$, c'est la formule (5) ; on voit que

$$(\Delta \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1)(\alpha_m) = \alpha_{m+1} \ominus (\partial_w(a) \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1)$$

$$\equiv \alpha_{m+1} - \partial_w(a) \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1 \pmod{I_{m+1,r+1}} \quad \text{(d'après (4))}$$

$$\equiv \alpha_{m+1} - \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}} \hat{\otimes} \dots \hat{\otimes} 1) \pmod{I_{m+1,r+1}} ;$$

et que

$$(\Delta \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1)(\beta_m) \equiv \sum \lambda_j T_m\Big(x_j^{p^{s-1}} \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1 + 1 \hat{\otimes} x_j^{p^{s-1}} \hat{\otimes} \dots \hat{\otimes} 1 ,$$
$$1 \hat{\otimes} 1 \hat{\otimes} x_j^{p^{s-1}} \hat{\otimes} \dots \hat{\otimes} 1, \dots, 1 \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} x_j^{p^{s-1}}\Big) \pmod{I_{m+1,r+1}} ;$$

on voit donc, en utilisant (3), que

$$(\Delta \hat{\otimes} 1 \hat{\otimes} \dots \hat{\otimes} 1)(\alpha_m - \beta_m) \equiv \alpha_{m+1} - \beta_{m+1} \pmod{I_{m,r+1}} ,$$

ce qui achève de prouver (6) .

Soit alors $TS^p I_1$ le sous-groupe de I_p formé des tenseurs symétriques et soit s l'opérateur de symétrisation (on a donc

$$s(u_1 \hat{\otimes} u_2 \hat{\otimes} \dots \hat{\otimes} u_p) = \sum_{g \in \mathfrak{S}_p} u_{g(1)} \hat{\otimes} u_{g(2)} \hat{\otimes} \dots \hat{\otimes} u_{g(p)}).$$

Tout élément u de $TS^p I_1$ s'écrit d'une manière et d'une seule sous la forme $b(u)^{\hat{\otimes}p} + u_0$, avec $b(u) \in I_1$ et $u_0 \in s(I_p)$. On sait (cf. n°I.7.6) que $\Delta_p a = V_B(a)^{\hat{\otimes}p} + (\Delta_p a)_0$, avec $V_B(a) = b(\Delta_p a)$.

Soit B_k l'algèbre affine de $\widehat{CW}_k$. Notons encore Δ_p le p-ième itéré du coproduit dans B_k. Comme $V_{B_k}(X_0) = X_{-1}$ (cf. n°II.4.3, remarque 1), on a, de la même manière, avec des notations évidentes, $\Delta_p X_0 = X_{-1}^{\hat{\otimes}p} + (\Delta_p X_0)_0$.

Notons φ l'homomorphisme de l'algèbre B_k dans B_G défini par le covecteur a^W et $\psi = \varphi^{\hat{\otimes}p} : \hat{\otimes}^p B_k \to \hat{\otimes}^p B_G$. On voit que $\psi(\Delta_p X_0) = \alpha_p$. On a donc $\alpha_p = \psi(X_{-1}^{\hat{\otimes}p}) + \psi((\Delta_p X_0)_0) = \varphi(X_{-1})^{\hat{\otimes}p} + (\psi(\Delta_p X_0))_0 = V_B(a)^{\hat{\otimes}p} + (\psi(\Delta_p X_o))$ et $b(\alpha_p) = V_B(a)$.

D'après (6), on a $\Delta_p a \equiv \alpha_p - \beta_p \pmod{I_{p,r+1}}$. Comme $b(\Delta_p a) = b(\alpha_p) = V_{B_G}(a)$, on en déduit que $b(\beta_p)^{\hat{\otimes}p} \equiv 0 \pmod{I_{p,r+1} = I_{p,p^s+1}}$ ou que $b(\beta_p) \equiv 0 \pmod{I_{1,p^{s-1}+1}}$. Un calcul simple montre que $b(\beta_p) = \sum \sigma^{-1}(\lambda_j) x_j^{p^{s-1}}$; les λ_j doivent donc être tous nuls, ce qui achève la démonstration du lemme.

4.2. Soit G un p-groupe formel sur k, soit B_G son algèbre affine, soit I_G l'idéal d'augmentation et soit $\overline{I_G^2}$ l'adhérence de I_G^2. Rappelons (cf. n°I.8.7) que l'espace cotangent $t_G^*(k) = I_G/\overline{I_G^2}$ de G a une structure naturelle de $k[\underline{V}]$-module topologique, autrement dit de D_k-module topologique annulé par $\underline{F}$.

PROPOSITION 4.3. - Soit G un p-groupe formel sur k. Soit η_G l'application de $\underline{M}(G)$ dans $t_G^*(k)$ qui à $\underline{b} = (\dots, b_{-n}, \dots, b_{-1}, b_o) \in \underline{M}(G)$ associe l'image de b_o dans $t_G^*(k)$. L'application η_G est D_k-linéaire continue surjective. Son noyau est $\underline{F}\underline{M}(G)$.

Démonstration : ici encore ce résultat est trivialement vrai si G est étale et nous supposons G connexe non réduit à 0. On conserve les notations utilisées dans le n°4.1.

La linéarité et la continuité sont évidentes. La surjectivité n'est autre que la proposition 4.1.

Il est clair que $\underline{F}\underline{M}(G)$ est contenu dans le noyau de η_G . Comme l'idéal d'augmentation est topologiquement nilpotent, on voit que, pour achever la démonstration de la proposition, il suffit de démontrer que, pour tout entier $r \geq 2$, si b est un élément de $I_{1,r}$ tel que $b^w \in \underline{M}(G)$, il existe $c \in I_{1,r}$ tel que $b \equiv c \pmod{I_{1,r+1}}$ et $c^w \in \underline{F}\underline{M}(G)$.

Soit donc $b \in I_{1,r} - I_{1,r+1}$ tel que $b^w \in \underline{M}(G)$. On a donc $\partial_w b = 0$ donc, d'après (1_2) , $\partial_a b \equiv 0 \pmod{I_{1,r+1}}$. D'après la proposition 10.5 du chapitre I ceci implique que $r = p^s$, avec s entier ≥ 1 et que

$$b \equiv \sum_j \lambda_j x_j^{p^s} \pmod{I_{1,r+1}} ,$$

les λ_j étant des éléments de k , la sommation étant étendue aux $j \in J$ tels que $s < \nu(j)$. On a donc $b \equiv d^{p^s} \pmod{I_{1,r+1}}$, avec $d = \sum \sigma^{-s}(\lambda_j)x_j$. D'après la proposition 4.1, il existe $d_0 \in I_1$ vérifiant $d_0 \equiv d \pmod{I_{1,2}}$ et $d_0^w \in \underline{M}(G)$. Posons $c = d_0^{p^s}$. On voit que $c \in I_{1,r}$ et vérifie $c \equiv b \pmod{I_{1,r+1}}$ et $c^w \in \underline{F}^s\underline{M}(G) \subset \underline{F}\underline{M}(G)$.

COROLLAIRE 1.- <u>Si</u> G <u>est un p-groupe formel sur</u> k <u>tel que</u> $F_G = 0$, <u>on a</u> $\underline{F}\underline{M}(G) = 0$ <u>et</u> $\underline{M}(G)$ <u>s'identifie canoniquement à</u> $t_G^*(k)$. <u>En particulier</u>, <u>si</u> G <u>est un</u> p-<u>groupe fini d'ordre</u> p^r <u>tel que</u> $F_G = 0$, $\underline{M}(G)$ <u>est un espace vectoriel sur</u> k <u>de dimension</u> r .

C'est clair !

COROLLAIRE 2.- <u>Le foncteur</u> $\underline{M}$, <u>restreint à la catégorie des</u> k-<u>groupes formels connexes</u>, <u>est exact</u>.

Il suffit en effet de montrer que, si $G' \to G$ est un monomorphisme de k-groupes formels connexes, l'application correspondante $\underline{M}(G) \to \underline{M}(G')$ est surjective. Comme $M' = \underline{M}(G')$ est un D_k-module $A[\underline{F}]$-profini connexe, on voit que si N est un sous-D_k-module fermé de M' , on aura $N = M'$ si et seulement si $N/(\underline{F}M' \cap N) = M'/\underline{F}M'$.

Le fait que $G' \to G$ soit un monomorphisme implique que l'application correspondante sur les algèbres affines est surjective, donc que l'application canonique $t_G^*(k) \to t_{G'}^*(k)$ est surjective.

Il est clair que le diagramme

$$\begin{array}{ccc} \underline{M}(G) & \longrightarrow & \underline{M}(G') \\ \downarrow{\scriptstyle \eta_G} & & \downarrow{\scriptstyle \eta_{G'}} \\ t^*_G(k) & \longrightarrow & t^*_{G'}(k) \end{array}$$

est commutatif. On en déduit que l'application de $\underline{M}(G)$ dans $t^*_{G'}(k) \simeq \underline{M}(G')/\underline{F}\underline{M}(G')$ est surjective, d'où le corollaire.

4.3. Soit M un D_k-module $A[\underline{F}]$-profini et soit $G = \underline{G}(M)$. On sait (cf. n°I.8.4) que l'espace tangent $t_G(k)$ de G s'identifie au noyau de $G(\varepsilon) : G(k[t]/t^2) \to G(k)$ où $\varepsilon : k[t]/t^2 \to k$ est définie par $\varepsilon(\lambda+\mu t) = \lambda$, si $\lambda, \mu \in k$.

On voit que $\widehat{CW}_k(k[t]/t^2)$ est l'ensemble des covecteurs de la forme $(\ldots, \lambda_{-n}+\mu_{-n}t, \ldots, \lambda_{-1}+\mu_{-1}t, \lambda_o+\mu_o t)$, avec les λ_{-n} et les μ_{-n} dans k et les λ_{-n} presque tous nuls. On voit aussi que le noyau de $\widehat{CW}_k(\varepsilon)$ s'identifie à $\widehat{CW}^c_k(k[t]/t^2)$ et est formé des covecteurs de la forme $(\ldots, \mu_{-n}t, \ldots, \mu_{-1}t, \mu_0 t)$.

En particulier, $t_G(k)$ s'identifie à $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}^c_k(k[t]/t^2))$. Comme il est clair que $\underline{F}\widehat{CW}^c_k(k[t]/t^2) = 0$, on voit que l'on peut encore identifier $t_G(k)$ à $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M/\underline{F}M, \widehat{CW}^c_k(k[t]/t^2))$.

Soit $u \in t_G(k)$ et soit $\hat{u}$ son image dans $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M/\underline{F}M, \widehat{CW}^c_k(k[t]/t^2))$. Pour tout $\underline{a} \in M/\underline{F}M$, $\hat{u}(\underline{a}) = (\ldots, \mu_{-n}t, \ldots, \mu_{-1}t, \mu_o t)$, où $\mu_{-n} = \mu_{-n}(u, \underline{a})$ est un élément de k qui dépend de u et de $\underline{a}$. Posons $\xi_M(u)(\underline{a}) = \mu_0(u, \underline{a})$.

PROPOSITION 4.4.- <u>Soit</u> M <u>un</u> D_k-<u>module</u> $A[\underline{F}]$-<u>profini et soit</u> $G = \underline{G}(M)$.

i) <u>Pour tout</u> $u \in t_G(k)$, <u>l'application</u> $\xi_M(u) : M/\underline{F}M \to k$ <u>définie ci-dessus est</u> k-<u>linéaire continue</u>.

ii) <u>L'application</u> $\xi_M : t_G(k) \to \mathcal{L}^{\mathrm{cont}}_k(M/\underline{F}M, k)$, <u>espace des applications</u> k-<u>linéaires continues de</u> $M/\underline{F}M$ <u>dans</u> k, <u>ainsi définie</u>, <u>est un isomorphisme de</u> k-<u>espaces vectoriels</u>.

<u>Démonstration</u> : il résulte immédiatement du fait que le carré de l'idéal maximal de $k[t]/t^2$ est nul que l'application qui à $(\ldots, \mu_{-n}t, \ldots, \mu_{-1}t, \mu_0 t)$

associe $(\mu_{-n})_{n\in\mathbb{N}}$ définit un isomorphisme du k-espace vectoriel topologique $\widehat{CW}_k^c(k[t]/t^2)$ sur $k^{\mathbb{N}}$. La première assertion de la proposition, ainsi que le fait que ξ_M est une application k-linéaire en résultent.

Soit $(\underline{a}_i)_{i\in I}$ une base topologique du k-espace vectoriel profini $M/\underline{F}M$. Se donner une application k-linéaire continue $\theta : M/\underline{F}M \to \widehat{CW}_k^c(k[t]/t^2)$ revient à se donner une famille $(\mu_{-n,i})_{n\in\mathbb{N},i\in I}$ d'éléments de k telle que, pour n fixé, presque tous les $\mu_{-n,i}$ sont nuls : l'application θ est alors définie par $\theta(\underline{a}_i) = (\ldots,\mu_{-n,i}t,\ldots,\mu_{-1,i}t,\mu_{0,i}t)$.

Pour tout $j \in I$, $\underline{V}\underline{a}_j$ s'écrit sur la base des $\underline{a}_i$ sous la forme $\underline{V}\underline{a}_j = \sum_{i\in I} \lambda_{i,j}\underline{a}_i$, avec les $\lambda_{i,j} \in k$; le fait que $\underline{V}$ est continue implique que, pour i fixé, presque tous les $\lambda_{i,j}$ sont nuls.

Il est clair que l'application k-linéaire continue θ définie ci-dessus sera D_k-linéaire si et seulement si, pour tout $j\in I$, $\theta(\underline{V}\underline{a}_j) = \underline{V}(\theta(\underline{a}_j))$, ou encore si

$$\Big(\ldots,(\sum_i \lambda_{i,j}\mu_{-n,i})t,\ldots,(\sum_i \lambda_{i,j}\mu_{-1,i})t,(\sum_i \lambda_{i,j}\mu_{0,i})t\Big) =$$

$$= (\ldots,\mu_{-n-1,j}t,\ldots,\mu_{-2,j}t,\mu_{-1,j}t) \text{ , pour tout } j \in I .$$

Si les $\mu_{0,j}$, presque tous nuls, sont donnés, on voit que les $\mu_{-n-1,j}$ se calculent, de proche en proche, par la formule

$$\mu_{-n-1,j} = \sum_i \lambda_{i,j}\mu_{-n,i} \ ;$$

le fait que les $\lambda_{i,j}$ sont presque tous nuls, pour i fixé, implique que si les $\mu_{-n,j}$ sont presque tous nuls (n fixé), les $\mu_{-n-1,j}$ le sont aussi. On voit donc que les $\mu_{0,j}$, presque tous nuls, étant donnés, il existe un élément u de $t_G(k)$ et un seul tel que $\xi_M(u)(\underline{a}_i) = \mu_{0,i}$, pour tout i, ce qui montre que l'application ξ_M est bijective.

4.4. Nous sommes maintenant en mesure de démontrer le théorème 1 dans le cas connexe. Compte-tenu de ce qui a été fait au § 1, il suffit d'établir le résultat suivant :

PROPOSITION 4.5.-

i) Si G est un p-groupe fini connexe d'ordre p^r , $\underline{M}(G)$ est un A-module de longueur r .

ii) Pour tout k-groupe formel connexe G , le morphisme de G dans $\underline{G}\,\underline{M}(G)$ provenant de l'adjonction est un isomorphisme.

iii) Pour tout D_k-module $A[\underline{F}]$-profini connexe M , l'homomorphisme de M dans $\underline{M}\underline{G}(M)$ provenant de l'adjonction est un isomorphisme.

Démonstration : montrons (i) : si G est un p-groupe fini connexe simple, on a $F_G = 0$ et (i) résulte du corollaire 1 de la proposition 4.3. Le cas général s'en déduit par récurrence sur la longueur de G en utilisant le fait que $\underline{M}$ est exact (cor.2 de la prop.4.3).

Pour tout k-groupe formel connexe G , notons G_n le sous-groupe de G noyau de F_G^n . On sait que $G = \varinjlim G_n$. On a donc

$$\underline{M}(G) = \mathrm{Hom}(G,\widehat{CW}_k) = \mathrm{Hom}(\varinjlim G_n,\widehat{CW}_k) = \varprojlim \mathrm{Hom}(G_n,\widehat{CW}_k) = \varprojlim \underline{M}(G_n).$$

L'exactitude de $\underline{M}$ implique en outre que $\underline{M}(G_n) = \underline{M}(G)/\underline{F}^n\underline{M}(G)$.

De même, pour tout D_k-module $A[\underline{F}]$-profini connexe M , posons $M_n = M/\underline{F}^n M$. Il est clair que $M = \varprojlim M_n$.

Si R est un k-anneau fini, le radical de R est nilpotent et on en déduit qu'il existe un entier r tel que $\underline{F}^r\widehat{CW}_k^c(R) = 0$. On a donc $\underline{G}(M)(R) =$ $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M,\widehat{CW}_k(R)) = \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M,\widehat{CW}_k^c(R))$ (car M est connexe) $=$ $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M/\underline{F}^r M,\widehat{CW}_k^c(R)) = \varinjlim \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M_n,\widehat{CW}_k^c(R))$, donc $\underline{G}(M) = \varinjlim \underline{G}(M_n)$. En outre, comme $\underline{G}$ est exact à gauche, on voit que $\underline{G}(M_n) = (\underline{G}(M))_n$.

Ces considérations ramènent en particulier la démonstration de l'assertion (ii) (resp. (iii)) au cas où $F_G^n = 0$ (resp. $\underline{F}^n M = 0$).

L'assertion (ii) se démontre alors par récurrence sur l'entier n tel que $F_G^n = 0$:

- soit G un groupe tel que $F_G = 0$; On voit que $\underline{F}\underline{M}(G) = 0$ et on en déduit que $F_{\underline{G}\,\underline{M}(G)} = 0$. Il suffit donc de montrer que le morphisme canonique $u_G : G \to \underline{G}\,\underline{M}(G)$ induit un isomorphisme des espaces tangents. D'après le corollaire 1 à la proposition 4.3, $\underline{M}(G)$ s'identifie canoniquement à $t^*_G(k)$; la proposition 4.4 définit un isomorphisme canonique de $t_{\underline{G}\underline{M}(G)}(k)$ sur le dual topologique de $\underline{M}(G)$; on a donc un isomorphisme de $t_G(k)$ sur $t_{\underline{G}\underline{M}(G)}(k)$ et on vérifie facilement que c'est bien la flèche provenant de l'adjonction.

- Soit G un groupe tel que $F^n_G = 0$. On considère la suite exacte

$$0 \longrightarrow \operatorname{Ker} F_G \longrightarrow G \longrightarrow \operatorname{Im} F_G \longrightarrow 0 .$$

L'assertion (ii) se déduit de l'exactitude de $\underline{M}$ (cor. 2 à la prop. 4.3) et de l'hypothèse de récurrence appliquée à $\operatorname{Ker} F_G$ et $\operatorname{Im} F_G$ (exactement comme pour la démonstration de l'assertion (ii) de la proposition 3.4).

L'assertion (iii) se démontre de manière analogue :

- Soit M un D_k-module $A[\underline{F}]$-profini tel que $\underline{F}M = 0$. On voit que $F_{\underline{G}(M)} = 0$, donc que $\underline{F}\,\underline{M}\,\underline{G}(M) = 0$. Comme $\underline{F}M = 0$, $t_{\underline{G}(M)}(k)$ s'identifie (prop. 4.4) au dual topologique de M , donc $t^*_{\underline{G}(M)}(k)$ s'identifie à M . Comme $F_{\underline{G}(M)} = 0$, $\underline{M}\underline{G}(M)$ s'identifie (cor.1 à la prop. 4.3) à $t^*_G(k)$ donc à M et on vérifie encore que cette identification n'est autre que la flèche provenant de l'adjonction.

- Le cas d'un module M tel que $\underline{F}^n M = 0$ s'en déduit par récurrence sur n (exactement comme pour la démonstration de l'assertion (iii) de la proposition 3.4) : il suffit de considérer la suite exacte

$$0 \longrightarrow \underline{F}M \longrightarrow M \longrightarrow M/\underline{F}M \longrightarrow 0 ;$$

on applique l'hypothèse de récurrence à $\underline{F}M$ et à $M/\underline{F}M$, et on utilise l'exactitude de $\underline{M}$ et le fait que si N est un D_k-module $A[\underline{F}]$-profini non nul, $\underline{G}(M) \neq 0$, ce qui est une conséquence triviale de la proposition 4.4.

§ 5.- Dualité.

5.1. Rappelons que le k-anneau $C_k = C\Lambda(k)$ a été défini au n°II.6.7 comme étant l'anneau des éléments de la forme $\sum_{s\in\overline{S}} a_s\overline{\theta}_s$ (où $\overline{S} = \{s\in\mathbb{Z}[1/p] \mid 0\leq s<p\}$), les a_s étant des éléments de k vérifiant

(Φ) <u>pour tout</u> $r > 0$, <u>il existe</u> $\varepsilon > 0$ <u>tel que</u> $a_s = 0$ <u>si</u> $r-\varepsilon \leq s < r$.

Soit $\bar{k}$ une clôture algébrique de k . Pour tout $x \in \bar{k}$, notons ν_x l'application de $\mathcal{C}_k$ dans $\mathcal{C}_{k(x)} = C\Lambda(k(x))$ définie par $\nu_x(\sum a_s \bar{\theta}_s) = \sum a_s x^s \bar{\theta}_s$; il est clair que ν_x est un homomorphisme de k-anneaux.

Soit G un p-groupe fini sur k . Les éléments de $G(\mathcal{C}_k)$ sont les k-homomorphismes de l'algèbre affine B_G de G dans le k-anneau $\mathcal{C}_k$.

Pour tout nombre premier $\ell \neq p$, soit μ_ℓ le groupe des racines ℓ-ièmes de l'unité dans $\bar{k}$ et soit $k_\ell = k(\mu_\ell)$. Si $\varphi \in G(\mathcal{C}_k)$, nous posons $u_\ell(\varphi) = \sum_{\varepsilon \in \mu_\ell} \nu_\varepsilon \circ \varphi$; on voit que, si $\varepsilon \in \mu_\ell$, $\nu_\varepsilon \circ \varphi : B_G \to \mathcal{C}_{k_\ell}$ est un élément de $G(\mathcal{C}_{k_\ell})$; il en est donc de même de $u_\ell(\varphi)$, mais, comme il est clair que l'image de $u_\ell(\varphi)$ est contenue dans $\mathcal{C}_k$, on peut considérer $u_\ell(\varphi)$ comme un élément de $G(\mathcal{C}_k)$. Il est clair que u_ℓ est un endomorphisme du groupe $G(\mathcal{C}_k)$.

Pour tout automorphisme τ de k notons $\langle\tau\rangle$ l'application de $\mathcal{C}_k$ dans lui-même définie par $\langle\tau\rangle(\sum a_s \bar{\theta}_s) = \sum \tau(a_s)\bar{\theta}_s$. Il est clair que c'est un endomorphisme de l'anneau (et non du k-anneau) $\mathcal{C}_k$.

Notons F_{B_G} (resp. V_{B_G}) : $B_G \to B_G$ l'endomorphisme (de l'anneau B_G) définissant le Frobenius (resp. le décalage). Pour tout $\varphi \in G(\mathcal{C}_k)$, posons

$$F_p \cdot \varphi = \langle\sigma\rangle \circ \varphi \circ V_{B_G} \quad \text{et} \quad V_p \cdot \varphi = \langle\sigma^{-1}\rangle \circ \varphi \circ F_{B_G} .$$

Il est clair que $F_p \cdot \varphi$ et $V_p \cdot \varphi$ sont des éléments de $G(\mathcal{C}_k)$ et que F_p et V_p sont des endomorphismes de $G(\mathcal{C}_k)$.

PROPOSITION 5.1.- <u>Pour tout</u> p-<u>groupe fini</u> G <u>sur</u> k <u>soit</u> $\underline{M}'(G)$ <u>le sous-groupe de</u> $G(\mathcal{C}_k)$ <u>formé des éléments</u> φ <u>vérifiant</u> $u_\ell(\varphi) = 0$, <u>pour tout nombre premier</u> $\ell \neq p$.

i) <u>Il existe une structure de</u> D_k-<u>module à gauche et une seule sur</u> $\underline{M}'(G)$ <u>vérifiant, pour tout</u> $\varphi \in \underline{M}'(G)$,

$[\varepsilon]\varphi = \nu_\varepsilon \circ \varphi$, <u>si</u> $[\varepsilon]$ <u>désigne le représentant multiplicatif dans</u> $A = W(k)$ <u>d'un élément quelconque</u> ε <u>de</u> k ,

$\underline{F}\varphi = F_p \cdot \varphi$ <u>et</u> $\underline{V}\varphi = V_p \cdot \varphi$.

ii) Le D_k-module à gauche $\underline{M}'(G)$ est un D_k-module fini. Alors $\underline{M}'$ est (de manière évidente) un foncteur covariant additif de la catégorie des p-groupes finis sur k dans celle des D_k-modules finis ; ce foncteur induit une équivalence entre ces deux catégories.

iii) Notons $\mathbb{D}$ le foncteur contravariant additif de la catégorie des p-groupes finis sur k dans elle-même qui à G associe son dual de Cartier. Il existe une équivalence naturelle entre les foncteurs $\underline{M}'$ et $\underline{M}\cdot\mathbb{D}$.

Démonstration : soit B_G l'algèbre affine du p-groupe fini G . Soit $R = B'_G$ l'algèbre affine du dual de Cartier $\mathbb{D}(G)$ de G . Comme $\mathbb{D}(\mathbb{D}(G))$ s'identifie à G , on sait (cf. n°I.5.5) que, pour tout k-anneau S , le groupe G(S) s'identifie canoniquement au groupe multiplicatif de l'anneau $R \otimes_k S$ formé des éléments α vérifiant $\Delta\alpha = \alpha\otimes\alpha$ et $\epsilon\alpha = 1$.

Comme R est un k-anneau fini, on voit que l'anneau $C\Lambda(R)$ défini au n°II.6.3 s'identifie canoniquement à l'anneau $R \otimes_k C\Lambda(k) = R \otimes_k \mathcal{C}_k$; on peut donc identifier le groupe $G(\mathcal{C}_k)$ au groupe multiplicatif $C(G)$ formé des éléments α de $C\Lambda(R)$ vérifiant $\Delta\alpha = \alpha \otimes \alpha$ et $\epsilon\alpha = 1$.

On vérifie immédiatement que, dans cette identification, pour tout nombre premier $\ell \neq p$, l'application u_ℓ qui vient d'être définie correspond à l'endomorphisme U_ℓ de l'anneau $C\Lambda(R)$, défini en II.6.5. Par conséquent le groupe $\underline{M}'(G)$ s'identifie canoniquement au groupe multiplicatif

$$CT(G) = \{\alpha \in C\Lambda(R) \mid \Delta\alpha = \alpha\otimes\alpha \ , \ \epsilon\alpha = 1 \ , \ U_\ell\alpha = 1 \ , \text{ pour tout } \ell \neq p\} \ .$$

Comme $\epsilon\alpha = 1$ implique que α appartient au groupe noté $CC(R)$ en II.6.3 et comme le groupe $CCT(R)$ a été défini comme le sous-groupe de $CC(R)$ formé des α vérifiant $U_\ell\alpha = 1$, pour tout $\ell \neq p$, on a

$$CT(G) = \{\alpha \in CCT(R) \mid \Delta\alpha = \alpha\otimes\alpha \ , \ \epsilon\alpha = 1\} \ .$$

Considérons alors l'isomorphisme $CE_R : CW_k(R) \to CCT'(R)$ (prop.II.6.6). Le module de Dieudonné $\underline{M}(\mathbb{D}(G))$ du groupe $\mathbb{D}(G)$ s'identifie à l'ensemble des $\underline{a} \in CW_k(R)$ vérifiant $\Delta\underline{a} = \underline{a}\otimes 1 + 1\otimes\underline{a}$ (avec des notations évidentes). On voit donc que CE_R définit un isomorphisme du groupe $\underline{M}(\mathbb{D}(G))$ sur le groupe

$$CT_1(G) = \{\alpha \in CCT'(R) \mid \Delta\alpha = \alpha\otimes\alpha\} \ .$$

Montrons que $CT(G) = CT_1(G)$:

- comme G est un p-groupe fini tout élément de $G(\mathbb{C}_k)$ est d'ordre une puissance de p ; comme $CT(G)$ est isomorphe à un sous-groupe de $G(\mathbb{C}_k)$, tout élément de $CT(G)$ est d'ordre une puissance de p et appartient donc à $CCT'(R)$ qui, comme R est un k-anneau fini, est le sous-groupe des éléments de $CCT(R)$ d'ordre une puissance de p ; d'où $CT(G) \subset CT_1(G)$;
- soit $\alpha \in CT_1(G)$; alors $\alpha = CE_R(\underline{a})$ avec $\underline{a} = (\dots, a_{-n}, \dots, a_0) \in \underline{M}(\mathbb{D}(G))$; on sait (cf. n°3.1) que les a_{-n} sont tous dans l'idéal d'augmentation de R ; on a donc $\epsilon_{\mathbb{D}(G)}(a_{-n}) = 0$ pour tout n ; comme $\alpha = \prod F(a_{-n}T_{-n})$, on en déduit que $\epsilon(\alpha) = 1$ et $\alpha \in CT(G)$.

On a donc construit un isomorphisme ρ_G du groupe $\underline{M}(\mathbb{D}(G))$ sur le groupe $\underline{M}'(G)$: soit $\underline{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0) \in \underline{M}(\mathbb{D}(G))$ et soit $\varphi = \rho_G(\underline{a})$; si l'on pose $\alpha = CE_R(\underline{a}) = \prod F(a_{-n}T_{-n})$ et si l'on réécrit α sous la forme $\alpha = \sum b_s\bar{\theta}_s$, on voit que φ est défini par

$$\varphi(x) = \sum x(b_s)\bar{\theta}_s \ , \text{ pour tout } x \in B_G = R' .$$

Par transport de structure $\underline{M}'(G)$ devient alors un D_k-module à gauche ; montrons que cette structure satisfait l'assertion (i) de la proposition :

- soit $\epsilon \in k$; on a $[\epsilon]\underline{a} = (\dots, \epsilon^{p^{-n}}a_{-n}, \dots, \epsilon a_o)$ et $[\epsilon]\alpha = \prod F(\epsilon^{p^{-n}}a_{-n}T_{-n}) = \sum \epsilon^s b_s\bar{\theta}_s$; donc, si $x \in B_G$, $([\epsilon]\varphi)(x) = \sum x(\epsilon^s b_s\bar{\theta}_s) = \sum \epsilon^s x(b_s)\bar{\theta}_s$ et $[\epsilon]\varphi = \nu_\epsilon \circ \varphi$;
- on a $\underline{F}\underline{a} = (\dots, a^p_{-n}, \dots, a^p_0)$ et $\underline{F}\alpha = \prod F(a^p_{-n}T_{-n}) = \sum b^p_s\bar{\theta}_s$; donc, si $x \in B_G$, $(\underline{F}\varphi)(x) = \sum x(b^p_s)\bar{\theta}_s$; mais, pour tout $b \in R$, on a $x(b^p) = (\Delta_p x)(b^{\otimes p})$ (en appelant Δ_p le p-ième itéré du co-produit dans B_G) et $\Delta_p x = V_{B_G}(x) + y$, où y est un tenseur obtenu par "symétrisation" d'un certain tenseur z ; on voit donc que $x(b^p) = ((V_{B_G}x)(b))^p = \sigma((V_{B_G}x)(b))$; d'où $(\underline{F}\varphi)(x) = \sum \sigma((V_{B_G}x)(b_s))\bar{\theta}_s$, donc $\underline{F}\varphi = \langle\sigma\rangle \circ \varphi \circ V_{B_G}$;
- on a $\underline{V}\underline{a} = (\dots, a_{-n-1}, \dots, a_{-1})$ et $\underline{V}\alpha = \prod F(a_{-n-1}T_{-n}) = \sum b_{s/p}\bar{\theta}_s$; donc, si $x \in B_G$, $(\underline{V}\varphi)(x) = \sum x(b_{s/p})\bar{\theta}_s$; en utilisant le fait que $V_R a_{-n} = a_{-n-1}$, on voit que $b_{s/p} = V_R b_s$; en raisonnant comme précédemment, on voit que $\sigma(x(V_R b_s)) = x^p(b_s)$; donc $(\underline{V}\varphi)(x) = \sum \sigma^{-1}(x^p(b_s))\bar{\theta}_s$ et $\underline{V} = \langle\sigma^{-1}\rangle \circ \varphi \circ F_{B_G}$.

Il est clair que l'isomorphisme ρ_G est fonctoriel en G. La proposition résulte alors du théorème 1 du § 1 .

Remarques :

1.- Notons v l'endomorphisme du k-anneau $\bar{\Lambda}_k$ défini par $v(\sum a_s\bar{\theta}_s) = \sum a_s\bar{\theta}_{sp}$. On voit que pour tout $\varphi \in \underline{M}'(G)$, on a aussi $\underline{V}\varphi = v\circ\varphi$.

2.- Lorsque le p-groupe fini G est connexe, on peut, dans la construction qui précède, remplacer, avec les notations du n°II.6.2, l'anneau $\mathcal{C}_k = C\Lambda(k)$ par l'anneau $C\Lambda^u(k) = \varinjlim \Lambda_m(k)$ (qui est le sous-anneau de $\mathcal{C}_k$ formé des $\sum_{s\in\bar{S}} a_s\bar{\theta}_s$, avec les a_s presque tous nuls). Si, en effet, m est un entier tel que $F_G^m = 0$, on voit que $G(\mathcal{C}_k) = G(\Lambda_m(k))$.

5.2. Nous allons construire de deux manières différentes le dual d'un D_k-module fini. Il sera commode de la considérer comme un D_k-module à droite. Pour cela, observons que tout D_k-module à gauche M peut être considéré comme un D_k-module à droite, et vice versa, si l'on pose, pour tout $x \in M$,

$$\begin{cases} ax = xa , \text{ pour tout } a\in A , \\ \underline{F}x = x\underline{V} \text{ et } \underline{V}x = x\underline{F} . \end{cases}$$

En particulier, ceci permet de considérer tout D_k-module fini aussi bien comme un D_k-module à gauche que comme un D_k-module à droite, ce que nous ferons désormais.

Si M est un D_k-module fini, nous notons $M' = \mathrm{Hom}_A(M,K/A)$ le A-module des applications A-linéaires de M dans K/A. On peut le munir d'une structure de D_k-module fini en posant, pour tout $u \in M'$, tout $x \in M$:

$$\begin{cases} (au)(x) = (ua)(x) = au(x) , \text{ pour tout } a\in A , \\ (\underline{F}u)(x) = (u\underline{V})(x) = \sigma(u(\underline{V}x)) , \\ (\underline{V}u)(x) = (u\underline{F})(x) = \sigma^{-1}(u(\underline{F}x)) . \end{cases}$$

Il est clair que $M \mapsto M'$ est un foncteur contravariant additif de la catégorie des D_k-modules finis dans elle-même, induisant une dualité sur cette catégorie.

Pour $n \in \mathbb{Z}$, posons $A_n = K/A$ si $n<0$ et $A_n = K/p^{-n}A$ si $n\geq 0$, et considérons le A-module $\Theta T_k = \prod_{n\in\mathbb{Z}} A_n$. Avec des notations évidentes, tout élément de ΘT_k s'écrit d'une manière et d'une seule sous la forme $\sum_{n\in\mathbb{Z}} a_nT_n$, avec

$$a_n \in \begin{cases} K/A & \text{si } n<0 , \\ K/p^{-n}A & \text{si } n\geq 0 . \end{cases}$$

On munit ΘT_k d'une structure de D_k-bimodule en posant :

$$\begin{cases} a(\sum a_n T_n) = \sum a a_n T_n , \\ \underline{F}(\sum a_n T_n) = \sum \sigma(a_n) T_{n+1} , \\ \underline{V}(\sum a_n T_n) = \sum p\sigma^{-1}(a_n) T_{n-1} , \end{cases} \quad \text{et} \quad \begin{cases} (\sum a_n T_n) a = \sum \sigma^n(a) a_n T_n , \\ (\sum a_n T_n)\underline{F} = \sum a_n T_{n+1} , \\ (\sum a_n T_n)\underline{V} = \sum p a_n T_{n-1} \end{cases}$$

(on prendra garde qu'ici la structure de D_k-module à droite n'est pas la structure à droite induite par la structure de D_k-module à gauche).

Si M est un D_k-module fini, nous notons $M^* = \mathrm{Hom}_{D_k}(M, \Theta T_k)$ le D_k-module à droite des applications D_k-linéaires à gauche de M dans ΘT_k. Il est clair que $M \mapsto M^*$ peut être considéré comme un foncteur contravariant additif de la catégorie des D_k-modules finis dans celle des D_k-modules à droite.

PROPOSITION 5.2.- Pour tout D_k-module fini M, M^* est un D_k-module fini. Les foncteurs $M \mapsto M'$ et $M \mapsto M^*$ de la catégorie des D_k-modules finis dans elle-même sont naturellement équivalents.

Démonstration : pour tout $\varphi \in M^*$ et tout $x \in M$, posons $\varphi(x) = \sum\limits_{m\in\mathbb{Z}} (x,\varphi)_m T_m$.

Pour tout entier $n \geq 0$, on a

$$\varphi(\underline{F}^n x) = \sum_m (\underline{F}^n x,\varphi)_m T_m = \underline{F}^n \varphi(x) = \sum_m \sigma^n((x,\varphi)_m) T_{m+n} ;$$

en particulier $\sigma^n((x,\varphi)_{-n}) = (\underline{F}^n x,\varphi)_0$ ou

(1) $\quad (x,\varphi)_{-n} = \sigma^{-n}((\underline{F}^n x,\varphi)_0)$, pour tout $n \geq 0$.

De même, on a $\varphi(\underline{V}^n x) = \sum\limits_m (\underline{V}^n x,\varphi)_m T_m = \underline{V}^n \varphi(x) = \sum\limits_m p^n \sigma^{-n}((x,\varphi)_m) T_{m-n}$; en particulier $p^n \sigma^{-n}((x,\varphi)_n) = (\underline{V}^n x,\varphi)_0$ ou encore

(1') $\quad (x,\varphi)_n = p^{-n}\sigma^n((\underline{V}^n x,\varphi)_0)$, pour tout $n \geq 0$.

Pour tout $\varphi \in M^*$, soit $\eta_M(\varphi)$ l'application de M dans K/A définie par $\eta_M(\varphi)(x) = (x,\varphi)_0$, pour tout $x \in M$.

Il est clair que $\eta_M(\varphi) \in M'$ et que l'application $\eta_M : M^* \to M'$ est

A-linéaire. Si l'on pose $u = \eta_M(\varphi)$, on voit que

$$(u\underline{F})(x) = \sigma^{-1}(u(\underline{F}x)) = \sigma^{-1}((\underline{F}x,\varphi)_0) ;$$

d'autre part $\eta_M(\varphi\underline{F})(x) = (x,\varphi\underline{F})_0$; mais $(\varphi\underline{F})(x) = \varphi(x)\underline{F} = \sum (x,\varphi)_m T_{m+1}$, donc $\eta_M(\varphi\underline{F})(x) = (x,\varphi)_{-1} = \sigma^{-1}((\underline{F}x,\varphi)_0)$, d'après (1) , et $\eta_M(\varphi\underline{F}) = \eta_M(\varphi)\underline{F}$.

De même, on a $(u\underline{V})(x) = \sigma(u(\underline{V}x)) = \sigma((\underline{V}x,\varphi)_0)$; d'autre part $\eta_M(\varphi\underline{V})(x) = (x,\varphi\underline{V})_0$; mais $(\varphi\underline{V})(x) = \varphi(x)\underline{V} = \sum p(x,\varphi)_m T_{m-1}$, donc $\eta_M(\varphi\underline{V})(x) = p(x,\varphi)_1 = \sigma((Vx,\varphi)_0)$, d'après (1') ; et $\eta_M(\varphi\underline{V}) = \eta_M(\varphi)\underline{V}$. L'application η_M est donc D_k-linéaire à droite.

Pour tout $u \in M'$, soit $\eta'_M(u)$ l'application de M dans Θ_k définie par

$$\eta'_M(u)(x) = \sum_{n=1}^{\infty} \sigma^{-n}(u(\underline{F}^n x))T_{-n} + \sum_{n=0}^{\infty} p^{-n}\sigma^n(u(\underline{V}^n x))T_n .$$

On vérifie immédiatement que $\eta'_M(u) \in M^*$ et on déduit des formules (1) et (1') que η_M et η'_M sont des applications réciproques l'une de l'autre, donc que η_M est un isomorphisme de M^* sur M' . En particulier, M^* est un D_k-module fini.

Enfin, il est clair que l'isomorphisme η_M est fonctoriel en M , ce qui achève la démonstration.

5.3. Nous allons montrer maintenant que, si G est un p-groupe fini sur k , le D_k-module fini $\underline{M}'(G)$ s'identifie au dual de $\underline{M}(G)$.

Pour cela nous utiliserons de façon essentielle l'isomorphisme $\bar{\varpi}_k$ de $CW_k(C_k)$ sur Θ_k défini en II.6.7.

Rappelons (cf. prop. **II**.6.11) que le D_k-module à gauche Θ_k est formé des éléments $\sum_{s\in\mathbb{N}[1/p]} b_s\theta_s$, avec $b_s \in K/A$ si $s<p$, $b_s \in K/p^{-n}A$ si $p^n \leq s < p^{n+1}$ et $n \geq 1$, assujettis à vérifier des conditions notées (Φ_1), (Φ_2) et (Φ_3) .

Notons $\Theta T'_k$ l'ensemble des $\sum b_s\theta_s \in \Theta_k$ vérifiant $b_s = 0$ si s n'est pas une puissance entière (positive ou négative) de p . Il est clair que c'est un sous-D_k-module à gauche de Θ_k . Si, pour tout $n \in \mathbb{Z}$, on pose $T_n = \theta_{p^n}$, on voit que les éléments de $\Theta T'_k$ peuvent s'écrire sous la forme $\sum a_n T_n$, avec $a_n \in K/A$ si $n \leq 0$, $a_n \in K/p^{-n}A$ si $n > 0$. Ceci permet d'identifier

$\Theta T'_k$ à une partie du D_k-bimodule ΘT_k défini au n° précédent. On constate facilement que $\Theta T'_k$ est en fait un sous-D_k-module à gauche de ΘT_k ; si l'on explicite les conditions (Φ_1) , (Φ_2) et (Φ_3) pour les éléments de la forme $\sum a_n T_n$, on vérifie immédiatement que $\Theta T'_k$ s'identifie à la partie de torsion de ΘT_k , autrement dit au sous-D_k-module à gauche de ΘT_k formé des éléments dont l'ordre est une puissance de p . En particulier $\Theta T'_k$ est stable pour l'action de D_k à droite et peut donc également être considéré comme un D_k-bimodule. On voit que, pour tout D_k-module fini M , $M^* = \mathrm{Hom}_{D_k}(M, \Theta T_k) = \mathrm{Hom}_{D_k}(M, \Theta T'_k)$.

Soit maintenant G un p-groupe fini sur k et soit B_G son algèbre affine. Il résulte de la proposition 1.2 que l'application qui à $\varphi : B_G \to \mathcal{C}_k$ associe la restriction de $CW_k(\varphi) : CW_k(B_G) \to CW_k(\mathcal{C}_k)$ à $\underline{M}(G)$ est un isomorphisme du groupe $G(\mathcal{C}_k)$ sur $\mathrm{Hom}_{D_k}(\underline{M}(G), CW_k(\mathcal{C}_k))$. En composant avec l'isomorphisme $\bar{\varpi}_k : CW_k(\mathcal{C}) \to \Theta_k$,on obtient un isomorphisme

$$\lambda_G : G(\mathcal{C}_k) \longrightarrow \mathrm{Hom}_{D_k}(\underline{M}(G), \Theta_k)$$

qui est visiblement fonctoriel en G .

PROPOSITION 5.3.- <u>Soit</u> G <u>un</u> p-<u>groupe fini sur</u> k . <u>L'application</u> λ_G <u>induit, par restriction à</u> $\underline{M}'(G)$, <u>un isomorphisme du</u> D_k-<u>module</u> $\underline{M}'(G)$ <u>sur</u> $\underline{M}(G)^* = \mathrm{Hom}_{D_k}(\underline{M}(G), \Theta T'_k)$ <u>(autrement dit, si</u> $\varphi \in G(\mathcal{C}_k)$, $\lambda_G(\varphi) \in \underline{M}(G)^*$ <u>si et seulement si</u> $\varphi \in \underline{M}'(G)$ <u>et l'isomorphisme de la structure de groupes de</u> $\underline{M}'(G)$ <u>sur</u> $\underline{M}(G)^*$ <u>induit par</u> λ_G <u>est</u> D_k-<u>linéaire</u>).

<u>Démonstration</u> : soit $\bar{k}$ une clôture algébrique de k et soit $\varepsilon \in \bar{k}$. L'application $\nu_\varepsilon : \mathcal{C}_k \to \mathcal{C}_{k(\varepsilon)}$, définie au n°5.1, induit une application $CW_k(\nu_\varepsilon) : CW_k(\mathcal{C}_k) \to CW_k(\mathcal{C}_{k(\varepsilon)})$. Comme les applications $\bar{\varpi}_k$ et $\bar{\varpi}_{k(\varepsilon)}$ sont des isomorphismes, il existe une application $\hat{\nu}_\varepsilon : \Theta_k \to \Theta_{k(\varepsilon)}$ et une seule qui rend le diagramme

$$\begin{tikzcd}
CW_k(\mathcal{C}_k) \arrow[r, "CW_k(\nu_\varepsilon)"] \arrow[d, "\bar{\varpi}_k"'] & CW_k(\mathcal{C}_{k(\varepsilon)}) \arrow[d, "\bar{\varpi}_{k(\varepsilon)}"] \\
\Theta_k \arrow[r, "\hat{\nu}_\varepsilon"] & \Theta_{k(\varepsilon)}
\end{tikzcd}$$

commutatif. On voit facilement que $\hat{\nu}_\varepsilon(\sum a_s \theta_s) = \sum [\varepsilon]^s a_s \theta_s$, pour tout

$\sum a_s\theta_s \in \Theta_k$ (on a noté $[\varepsilon]$ le représentant multiplicatif de ε dans A).

Notons encore λ_G l'application de $G(\mathcal{C}_{k(\varepsilon)})$ dans $\mathrm{Hom}_{D_k}(\underline{M}(G), \Theta_{k(\varepsilon)})$ qui à $\psi : B_G \to \mathcal{C}_{k(\varepsilon)}$ associe $\bar{\varpi}_{k(\varepsilon)} \circ CW_k(\psi)|_{\underline{M}(G)}$. Il est clair que, si $\varphi \in G(\mathcal{C}_k)$, $\lambda_G(\nu_\varepsilon \circ \varphi) = \hat{\nu}_\varepsilon \circ \lambda_G(\varphi)$.

En particulier, pour tout nombre premier $\ell \neq p$, comme $u_\ell(\varphi) = \sum_{\varepsilon \in \mu_\ell} \nu_\varepsilon \circ \varphi$ (cf. n°5.1), on a $\lambda_G(u_\ell(\varphi)) = \sum_{\varepsilon\in\mu_\ell} \hat{\nu}_\varepsilon \circ \lambda_G(\varphi)$. On a donc, pour tout $\underline{a} \in \underline{M}(G)$, si $\lambda_G(\varphi)(\underline{a}) = \sum a_s\theta_s$, $\lambda_G(u_\ell(\varphi))(\underline{a}) = \sum_{\varepsilon\in\mu_\ell}(\sum_{s\in S} \xi^s a_s\theta_s) = \sum_{s\in S}(\sum_{\varepsilon\in\mu_\ell}\varepsilon^s)a_s\theta_s = \ell(\sum_{s\in S_\ell} a_s\theta_s)$, où S_ℓ désigne l'ensemble des éléments de $S = \mathbb{N}[1/p]$ divisibles par ℓ.

Par définition, φ est dans $\underline{M}'(G)$ si et seulement si $u_\ell(\varphi) = 0$, pour tout ℓ ; ou encore si et seulement si $\lambda_G(u_\ell(\varphi)) = 0$, pour tout ℓ. Cela revient à dire que, pour tout $\underline{a} \in M(G)$, si $\lambda_G(\varphi)(\underline{a}) = \sum a_s\theta_s$, on a $a_s = 0$, pour tout $s \in S$ divisible par un nombre premier différent de p ; ou encore que $a_s = 0$ si s n'est pas une puissance entière de p. On en déduit bien que $\varphi \in \underline{M}'(G)$ si et seulement si $\lambda_G(\varphi) \in \underline{M}(G)^*$.

La restriction de λ_G à $\underline{M}'(G)$ est donc bien un isomorphisme de la structure de groupe de $\underline{M}'(G)$ sur $\underline{M}(G)^*$ et, pour achever la démonstration de la proposition, on voit qu'il suffit de vérifier que, pour tout $\varphi \in \underline{M}'(G)$,

$$\lambda_G(\varphi[\varepsilon]) = \lambda_G(\varphi)[\varepsilon] \text{ , pour tout } \varepsilon \in k \text{ ,}$$

$$\lambda_G(\varphi\underline{F}) = \lambda_G(\varphi)\underline{F}$$

$$\lambda_G(\varphi\underline{V}) = \lambda_G(\varphi)\underline{V} \text{ .}$$

- Pour tout $\varepsilon \in k$, on a $\varphi[\varepsilon] = [\varepsilon]\varphi = \nu_\varepsilon \circ \varphi$ et $\lambda_G(\varphi[\varepsilon]) = \hat{\nu}_\varepsilon \circ \lambda_G(\varphi)$; donc, pour tout $\underline{a} \in \underline{M}(G)$, si $\lambda_G(\varphi)(\underline{a}) = \sum b_n T_n = \sum b_n \theta_{p^n}$,
$\lambda_G(\varphi[\varepsilon])(\underline{a}) = \sum b_n[\varepsilon]^{p^n}\theta_{p^n} = \sum b_n\sigma^n([\varepsilon])T_n = (\sum b_nT_n)[\varepsilon]$, d'où
$\lambda_G(\varphi[\varepsilon]) = \lambda_G(\varphi)[\varepsilon]$.

- On a $\varphi\underline{F} = \underline{V}\varphi = v\circ\varphi$, d'après la remarque 1 du n°5.1. Si $\hat{v} : \Theta_k \to \Theta_k$ est définie par $\hat{v}(\sum c_s\theta_s) = \sum c_s\theta_{sp}$, on voit que $\bar{\varpi}_k \circ CW_k(v) = \hat{v}\circ\bar{\varpi}_k$. Pour tout $\underline{a} \in \underline{M}(G)$, si $\lambda_G(\varphi)(\underline{a}) = \sum b_nT_n = \sum b_n\theta_{p^n}$, on a donc
$\lambda_G(\varphi\underline{F})(\underline{a}) = \hat{v}(\sum b_nT_n) = \sum b_nT_{n+1} = (\sum b_nT_n)\underline{F}$, d'où $\lambda_G(\varphi\underline{F}) = \lambda_G(\varphi)\underline{F}$.

■ Par définition, on a $\varphi\underline{V} = \underline{F}\varphi = \langle\sigma\rangle\circ\varphi\circ V_{B_G}$.

Il est clair que si $\langle\hat{\sigma}\rangle : \Theta_k \to \Theta_k$ est l'application définie par $\langle\hat{\sigma}\rangle(\sum c_s\theta_s) = \sum\sigma(c_s)\theta_s$, on a $\bar{\varpi}_k\circ CW_k(\langle\sigma\rangle) = \langle\hat{\sigma}\rangle\circ\bar{\varpi}_k$.

D'autre part, si $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in \underline{M}(G)$, on sait (n°3.1) que $V_{B_G}(a_{-n}) = a_{-n-1}$, pour tout n , et on en déduit que $CW_k(V_{B_G})(\underline{a}) = \underline{V}\,\underline{a}$.

On a alors, pour tout $\underline{a} \in \underline{M}(G)$,

$$\begin{aligned}\lambda_G(\varphi\underline{V})(\underline{a}) = (\bar{\varpi}_k\circ CW_k(\langle\sigma\rangle\circ\varphi\circ V_{B_G}))(\underline{a}) &= (\langle\hat{\sigma}\rangle\circ\bar{\varpi}_k\circ CW_k(\varphi))(\underline{V}\,\underline{a}) \\ &= \langle\hat{\sigma}\rangle(\underline{V}(\lambda_G(\varphi)(\underline{a}))) .\end{aligned}$$

Si $\lambda_G(\varphi)(\underline{a}) = \sum b_n T_n$, on voit que

$$\langle\hat{\sigma}\rangle(\underline{V}(\lambda_G(\varphi)(\underline{a}))) = \langle\hat{\sigma}\rangle(\sum p\sigma^{-1}(b_n)T_{n-1}) = \sum pb_n T_{n-1} = (\sum b_n T_n)\underline{V} ,$$

d'où $\lambda_G(\varphi\underline{V}) = \lambda_G(\varphi)\underline{V}$.

COROLLAIRE 1.- <u>Les foncteurs</u> $G \mapsto \underline{M}'(G)$ <u>et</u> $G \mapsto \underline{M}(G)^*$ <u>de la catégorie des</u> p-<u>groupes finis sur</u> k <u>dans celle des</u> D_k-<u>modules finis sont naturellement équivalents</u>.

C'est clair puisque l'isomorphisme canonique de $\underline{M}'(G)$ sur $\underline{M}(G)^*$ défini dans la proposition 5.3 est visiblement fonctoriel en G .

COROLLAIRE 2.- <u>Les foncteurs</u> $G \mapsto \underline{M}(\mathbb{D}(G))$ <u>et</u> $G \mapsto (\underline{M}(G))'$ <u>de la catégorie des</u> p-<u>groupes finis sur</u> k <u>dans celle des</u> D_k-<u>modules finis sont naturellement équivalents</u>.

Il suffit de composer les équivalences naturelles

$$\underline{M}(\underline{D}(G)) \longmapsto \underline{M}'(G) \longmapsto \underline{M}(G)^* \longmapsto (\underline{M}(G))'$$

définies par la proposition 5.1, le corollaire 1 à la proposition 5.3 et la proposition 5.2.

COROLLAIRE 3.- <u>Pour tout</u> p-<u>groupe fini</u> G <u>sur</u> k , <u>notons</u> $M_D(G)$ <u>le module de Dieudonné de</u> G <u>au sens de Gabriel ou Manin</u> (<u>tel qu'il est décrit par exemple dans</u> [15] , chap.III). <u>Les foncteurs</u> M <u>et</u> M_D <u>de la catégorie des</u> p-<u>groupes finis sur</u> k <u>dans celle des</u> D_k-<u>modules finis sont naturellement équivalents</u>.

Il est clair qu'il suffit de démontrer ce résultat d'une part pour les groupes unipotents, d'autre part pour les groupes de type multiplicatif.

Si G est unipotent, on vérifie que $\underline{M}_D(G)$ s'identifie à $\mathrm{Hom}(G, CW^u_k) \subset \underline{M}(G) = \mathrm{Hom}(G, CW_k)$: mais, pour n assez grand, on a $V^n_G = 0$, donc $\underline{V}^n\underline{a} = 0$, pour tout $\underline{a} \in \underline{M}(G)$ et $\underline{M}(G) = \underline{M}_D(G)$.

Si G est de type multiplicatif, on a, par définition, $\underline{M}_D(G) = (\underline{M}_D(\mathbb{D}(G)))'$; comme $\mathbb{D}(G)$ est unipotent, $\underline{M}_D(\mathbb{D}(G)) \simeq \underline{M}(\mathbb{D}(G))$ et l'assertion résulte du corollaire 2.

§ 6.- Groupes formels lisses.

6.1. Soit G un p-groupe formel sur k et soit $M = \underline{M}(G)$. On sait (n° I.9.6) que G est lisse si et seulement si F_G est un épimorphisme ; on voit que ceci revient à dire que l'action de $\underline{F}$ sur M est injective. S'il en est ainsi, $M/\underline{F}M$ s'identifie, d'après la proposition 4.3, à $t^*_G(k)$ et G est de dimension finie si et seulement si $M/\underline{F}M$ est un k-espace vectoriel de dimension finie ; ces deux dimensions sont alors égales.

Pour tout p-groupe formel G sur k , et tout $n \in \mathbb{N}$, notons G^F_n le sous-groupe de G noyau de F^n_G . Il est clair que $\underline{M}(G^F_n)$ s'identifie à $\underline{M}(G)/\underline{F}^n\underline{M}(G)$. Le groupe G est connexe si et seulement si $G = \varinjlim G^F_n$, ou encore si et seulement si $\underline{M}(G)$ s'identifie à $\varprojlim \underline{M}(G)/\underline{F}^n\underline{M}(G)$, i.e. si et seulement si l'action de $\underline{F}$ sur $\underline{M}(G)$ est topologiquement nilpotente.

Pour tout p-groupe formel G sur k , et tout $n \in \mathbb{N}$, notons G_n le noyau de la multiplication par p^n dans G . Il est clair que $\underline{M}(G_n)$ s'identifie à $\underline{M}(G)/p^n\underline{M}(G)$ et que, comme $G = \varinjlim G_n$, on a $\underline{M}(G) = \varprojlim \underline{M}(G)/p^n\underline{M}(G)$.

Rappelons que la catégorie des <u>groupes</u> p-<u>divisibles</u> (<u>ou de Barsotti-Tate</u>) sur k s'identifie à la sous-catégorie pleine de celle des p-groupes formels sur k dont les objets G ont la propriété suivante : il existe un entier h tel que, pour tout n , G_n est d'ordre p^{nh} ; l'entier h s'appelle alors <u>la hauteur de</u> G .

On voit que si G est un groupe p-divisible sur k , de hauteur h , $\underline{M}(G)/p^n\underline{M}(G)$ est un (A/p^nA)-module libre de rang h , donc que $\underline{M}(G)$ est un A-module libre de rang h . Réciproquement si G est un p-groupe formel sur k tel que $\underline{M}(G)$ est un A-module libre de rang fini, on voit que G est p-divisible. Enfin, il est clair que tout groupe p-divisible sur k est lisse de dimension finie.

Le théorème 1 implique la proposition suivante :

PROPOSITION 6.1.- Le foncteur $\underline{M}$ induit une anti-équivalence entre la catégorie des p-groupes formels lisses sur k et celle des D_k-modules $A[\underline{F}]$-profinis sur lesquels l'action de $\underline{F}$ est injective. Si G est un p-groupe formel sur k et si $M = \underline{M}(G)$

i) le groupe G est connexe si et seulement si l'action de $\underline{F}$ sur M est topologiquement nilpotente ;

ii) le groupe G est de dimension finie si et seulement si $M/\underline{F}M$ est un k-espace vectoriel de dimension finie (celle-ci est alors égale à la dimension de G) ;

iii) le groupe G est p-divisible si et seulement si M est un A-module libre de rang fini (celui-ci est alors égal à la hauteur de G).

Remarques :

1.- Soit M un $A[\underline{F}]$-module profini sur lequel l'action de $\underline{F}$ est injective. Pour qu'il existe une structure de D_k-module sur M qui prolonge la structure de $A[\underline{F}]$-module, il faut que $pM \subset \underline{F}M$; on voit que cette condition est aussi suffisante et qu'alors cette structure est unique : pour tout $\underline{a} \in M$, $\underline{V}\underline{a}$ est l'unique $\underline{b} \in M$ tel que $\underline{F}\underline{b} = p\underline{a}$. On peut donc dire que $\underline{M}$ induit une anti-équivalence entre les p-groupes formels lisses sur k et les $A[\underline{F}]$-modules profinis M sur lesquels l'action de $\underline{F}$ est injective et qui vérifient $pM \subset \underline{F}M$.

2.- Si G est un k-groupe formel lisse et connexe, de dimension finie, on a $\underline{M}(G) = \varprojlim \underline{M}(G)/\underline{F}^n\underline{M}(G)$, chaque quotient étant muni de la topologie discrète. Ceci permet de considérer $\underline{M}(G)$ comme un $A[[\underline{F}]]$-module et l'on voit que c'est un $A[[\underline{F}]]$-module de type fini. De la même manière que dans la remarque 1, on voit que l'on peut dire que $\underline{M}$ induit une anti-équivalence entre k-groupes formels lisses et connexes de dimension finie et $A[[\underline{F}]]$-modules M de type finis sur lesquels l'action de $\underline{F}$ est injective et qui vérifient $pM \subset \underline{F}M$.

Soit toujours G un k-groupe formel lisse et connexe de dimension finie et soit $M = \underline{M}(G)$. Soit R un k-anneau fini ; on sait (th.1) que $G(R)$ s'identifie canoniquement au groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R))$ des applications D_k-linéaires continues de M dans $\widehat{CW}_k(R)$; on voit qu'une telle application est toujours à valeurs dans $\widehat{CW}^c_k(R)$; comme l'action de $\underline{F}$ sur $\widehat{CW}^c_k(R)$ est nilpotente, on peut considérer $\widehat{CW}^c_k(R)$ comme un $A[[\underline{F}]]$-module. On voit que $G(R)$ s'identifie encore au groupe $\mathrm{Hom}_{A[[\underline{F}]][\underline{V}]}(M, \widehat{CW}^c_k(R))$ des applications $A[[\underline{F}]]$-linéaires de M dans $\widehat{CW}^c_k(R)$ qui commutent à l'action de $\underline{V}$ (les hypothèses de continuité sont inutiles).

3.- Le même type de considérations montre que l'on peut dire que $\underline{M}$ induit une anti-équivalence entre groupes p-divisibles sur k et $A[\underline{F}]$-modules M qui sont des A-modules libres de rang fini tels que $pM \subset \underline{F}M$.

Ou encore entre groupes p-divisibles sur k et D_k-modules qui sont des A-modules libres de rang fini (la topologie sur M qui est la topologie p-adique "ne sert plus à rien").

En particulier, soit G un groupe p-divisible sur k , soit $M = \underline{M}(G)$ et soit R un k-anneau fini. On voit que toute application A-linéaire de M dans $\widehat{CW}_k(R)$ est continue et l'on a, avec des conventions évidentes,

$$G(R) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R)) = \mathrm{Hom}_{D_k}(M, \widehat{CW}_k(R)) .$$

6.2. Soit G un p-groupe formel sur k qui est limite inductive de groupes finis (c'est le cas si G est un p-groupe formel lisse et de dimension finie, en particulier si G est un groupe p-divisible). Soit R son algèbre affine et soit $M = \underline{M}(G)$. Soit $(G_i)_{i \in I}$ l'ensemble des sous-groupes finis de G . Pour tout $i \in I$, soit R_i l'algèbre affine de G_i et soit $M_i = \underline{M}(G_i)$; on a donc $R = \varprojlim R_i$ et $M = \varprojlim M_i$.

Pour tout k-anneau S (pas nécessairement fini) notons $G(S)$ le groupe des homomorphismes continus de R dans S (muni de la topologie discrète) ; on a donc $G(S) = \varinjlim G_i(S)$.

PROPOSITION 6.2.- _Soit_ G _un_ p-_groupe formel sur_ k _qui est limite inductive de groupes finis et soit_ $M = \underline{M}(G)$. _Pour tout_ k-_anneau_ S _le groupe_ $G(S)$ _s'identifie canoniquement_ (_et fonctoriellement en_ S) _au groupe_ $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(S))$ _des applications_ D_k-_linéaires continues de_ M _dans_ $CW_k(S)$.

Démonstration : on sait (proposition 1.2) que, pour tout $i \in I$, le groupe $G_i(S)$ s'identifie à $\mathrm{Hom}_{D_k}(M_i, CW_k(S)) = \mathrm{Hom}^{cont}_{D_k}(M_i, CW_k(S))$. Comme $M = \varprojlim M_i$, on a $G(S) = \varinjlim \mathrm{Hom}^{cont}_{D_k}(M_i, CW_k(S))$ et tout revient à montrer que si $u \in \mathrm{Hom}^{cont}_{D_k}(M, CW_k(S))$, son noyau est ouvert.

Il résulte facilement de ce que M est profini qu'il existe un entier $r \geq 0$ et un idéal nilpotent $\mathfrak{n}$ de S tel que, avec les notations du n° II.1.6, $u(M) \subset CW_k(S,\mathfrak{n},r)$. Pour tout entier $t \geq 1$, notons $CW_k(\mathfrak{n}^t)$ le sous-D_k-module fermé de $CW_k(S,\mathfrak{n},r)$ formé des covecteurs dont toutes les composantes sont dans $\mathfrak{n}^t$ et M_t l'image réciproque par u de $CW_k(\mathfrak{n}^t)$. Comme $CW_k(\mathfrak{n})$ est ouvert dans $CW_k(S,\mathfrak{n},r)$, M_1 est ouvert dans M ; comme $\mathfrak{n}$ est nilpotent, M_t est égal au noyau de u dès que t est suffisamment grand et il suffit de démontrer le lemme suivant :

LEMME 6.3.- Pour tout entier $t \geq 1$, M_{t+1} est ouvert dans M_t.

Démonstration : posons $E = \mathfrak{n}^t/\mathfrak{n}^{t+1}$ et $CW_k(E) = CW_k(\mathfrak{n}^t)/CW_k(\mathfrak{n}^{t+1})$. Pour tout $a \in \mathfrak{n}^t$, notons $\tilde{a}$ son image dans E. On vérifie immédiatement que l'application, qui à $(\dots, a_{-n}, \dots, a_{-1}, a_0) \in CW_k(\mathfrak{n}^t)$ associe $(\tilde{a}_{-n})_{n\in\mathbb{N}}$, induit, par passage au quotient, un isomorphisme du groupe topologique sous-jacent à $CW_k(E)$ sur $E^{\mathbb{N}}$ (la topologie de $E^{\mathbb{N}}$ étant la topologie produit, avec la topologie discrète sur chaque composante). Si on l'utilise pour identifier $CW_k(E)$ à $E^{\mathbb{N}}$, on voit que $CW_k(E)$ est un D_k-module tué par $\underline{F}$, ce qui permet de le considérer comme un $k[\underline{V}]$-module, et que, pour tout $\underline{\tilde{a}} = (\tilde{a}_{-n})_{n\in\mathbb{N}} \in CW_k(E)$, on a

$$\begin{cases} \underline{V}\underline{\tilde{a}} = (\tilde{a}_{-n+1})_{n\in\mathbb{N}} \\ x\underline{\tilde{a}} = (\sigma^{-n}(x)\tilde{a}_{-n})_{n\in\mathbb{N}}, \text{ pour tout } x \in k . \end{cases}$$

Il est clair que M_t est un D_k-module profini et que u induit une application D_k-linéaire continue u' de M_t dans $CW_k(E)$ dont le noyau est M_{t+1} et contient $\underline{F}M_t$. Posons $\tilde{M}_t = M_t/\underline{F}M_t$; c'est un $k[\underline{V}]$-module profini et, par passage au quotient, u' induit une application $k[\underline{V}]$-linéaire continue $\tilde{u} : \tilde{M}_t \to CW_k(E)$; on voit qu'il suffit de démontrer que le noyau de $\tilde{u}$ est ouvert dans $\tilde{M}_t$.

Soit $\theta : CW_k(E) \to E$ l'application qui à $(\tilde{a}_{-n})_{n\in\mathbb{N}}$ associe $\tilde{a}_0$. Il est clair que θ est k-linéaire continue. L'application $\theta\circ\tilde{u}$ est donc k-linéaire continue et son image est un sous-k-espace vectoriel de dimension finie E' de E . En utilisant le fait que l'application $\tilde{u}$ est $\underline{V}$-linéaire, on voit facilement que l'image de $\tilde{u}$ est contenue dans le sous-$k[\underline{V}]$-module $CW_k(E')$ de $CW_k(E)$ formé des covecteurs dont toutes les composantes sont dans E' . Comme l'anneau $k \oplus E'$ (où la multiplication est définie par $(x+\tilde{a})(y+\tilde{b}) = xy + (x\tilde{b}+y\tilde{a})$, pour $x, y \in k$, $\tilde{a}, \tilde{b} \in E'$) est fini, tout $u \in \mathrm{Hom}^{\mathrm{cont}}_{k[\underline{V}]}(\tilde{M}_t, CW_k(E')) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(\tilde{M}_t, CW_k(E')) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(\tilde{M}_t, CW_k(k\oplus E'))$ a son noyau ouvert (en effet $\underline{G}(\tilde{M}_t)(k\oplus E')$ s'identifie à $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(\tilde{M}_t, CW_k(k\oplus E'))$ et, comme M_t est profini, le groupe formel $\underline{G}(\tilde{M}_t)$ est réunion de ses sous-groupes finis).

<u>Remarque</u> : si le noyau de la multiplication par p est un groupe fini (en particulier si G est un groupe p-divisible), toute application D_k-linéaire de M dans $CW_k(S)$ est continue et on a donc aussi $G(S) = \mathrm{Hom}_{D_k}(M, CW_k(S))$.

6.3. Soit G un groupe p-divisible sur k et soit, pour tout $n \in \mathbb{N}$, G_n le noyau de la multiplication par p^n . La multiplication par p définit un épimorphisme de G_{n+1} sur G_n ; on en déduit, par dualité, un monomorphisme de $\mathbb{D}(G_n)$ dans $\mathbb{D}(G_{n+1})$. On voit que $\varinjlim \mathbb{D}(G_n)$ est un groupe p-divisible sur k , de même hauteur que G ; nous le notons $\mathbb{D}_p(G)$ et l'appelons le dual de G ; il est clair que $\mathbb{D}_p$ définit de manière évidente une dualité dans la catégorie des groupes p-divisibles sur k .

Soit maintenant M un D_k-module qui est un A-module libre de rang fini ; on munit le A-module M^d des applications A-linéaires de M dans A d'une structure de D_k-module en posant, pour tout $u \in M^d$ et tout $\underline{a} \in M$:

$$(\underline{F}\,\underline{u})(\underline{a}) = \sigma(\underline{u}(\underline{V}\,\underline{a})) \quad \text{et} \quad (\underline{V}\,\underline{u})(\underline{a}) = \sigma^{-1}(\underline{u}(\underline{F}\,\underline{a})) \ .$$

La correspondance $M \to M^d$ définit, de manière évidente, une dualité dans la catégorie des D_k-modules qui sont des A-modules libres de rang fini.

PROPOSITION 6.4.- <u>Les foncteurs</u> $G \mapsto (\underline{M}(G))^d$ <u>et</u> $G \mapsto \underline{M}(\mathbb{D}_p(G))$ <u>de la catégorie des groupes</u> p-<u>divisibles sur</u> k <u>dans celle des</u> D_k-<u>modules sont naturellement équivalents</u>.

Cela résulte immédiatement du corollaire 2 à la proposition 5.3.

6.4. Pour terminer ce paragraphe, nous allons donner une interprétation élémentaire du module de Dieudonné d'un groupe formel lisse et de dimension finie.

Soit G un p-groupe formel lisse et de dimension finie sur k et soit R son algèbre affine. Appelons <u>relèvement lisse de</u> R la donnée d'un A-anneau spécial $\mathcal{R}$ (au sens du n°II.5.4) et d'un isomorphisme de $\mathcal{R}/p\mathcal{R} \simeq \mathcal{R}\otimes_A k$ sur R. Un tel relèvement existe toujours (si $R = \prod R_i$ est la décomposition de R en produit d'anneaux locaux, alors, pour chaque i, un choix de coordonnées permet d'identifier R_i à l'anneau des séries formelles $k_i[[X_1,X_2,\dots,X_d]]$ à coefficients dans une extension finie k_i de k ; on peut prendre $\mathcal{R} = \prod \mathcal{R}_i$, avec $\mathcal{R}_i = W(k_i)[[X_1,\dots,X_d]]$ et l'isomorphisme évident de $\mathcal{R}/p\mathcal{R}$ sur R) ; il est unique à isomorphisme non unique près.

Soit $\Delta : R \to R\hat{\otimes}_k R$ le coproduit et soit $\hat{\Delta} : \mathcal{R} \to \mathcal{R}\hat{\otimes}_A \mathcal{R}$ un homomorphisme continu de A-anneaux qui relève Δ (un tel homomorphisme existe toujours -on ne demande pas qu'il munisse $\mathcal{R}$ d'une structure de bigèbre formelle). Il est clair que $\hat{\Delta}$ se prolonge, de manière unique, en un homomorphisme continu de $\hat{\mathcal{R}}_K^{an}$ dans $(\widehat{\mathcal{R}\hat{\otimes}_A\mathcal{R}})_K^{an}$ que nous notons encore $\hat{\Delta}$.

Pour tout $\alpha \in \hat{\mathcal{R}}_K^{an}$, posons $\hat{\partial}\alpha = \alpha\hat{\otimes}1 - \hat{\Delta}\alpha + 1\hat{\otimes}\alpha$ et

$$\mathcal{MH}_{\mathcal{R}}(G) = \{\alpha \in P(\mathcal{R}) \mid \hat{\partial}\alpha \in p\mathcal{R}\hat{\otimes}_A\mathcal{R}\} ;$$

c'est un sous-A-module de $P(\mathcal{R})$ contenant $p\mathcal{R}$; on voit que $\mathcal{MH}_{\mathcal{R}}(G)$ ne dépend pas du choix du relèvement $\hat{\Delta}$ de Δ (si $\hat{\Delta}_1$ est un autre relèvement de Δ, on a $\hat{\Delta}_1\beta \equiv \hat{\Delta}\beta \pmod{p\mathcal{R}}$, pour tout $\beta \in \mathcal{R}$; tout élément de $P(\mathcal{R})$ s'écrit comme une somme infinie d'éléments de la forme $p^{-n}\beta^{p^n}$, avec $\beta \in \mathcal{R}$ et $n \in \mathbb{N}$, et l'on a $\hat{\Delta}_1\beta^{p^n} \equiv \hat{\Delta}\beta^{p^n} \pmod{p^{n+1}\mathcal{R}}$ donc $\hat{\Delta}_1(p^{-n}\beta^{p^n}) \equiv \hat{\Delta}(p^{-n}\beta^{p^n})$ $\pmod{p\mathcal{R}}$).

Posons $MH_{\mathcal{R}}(G) = \mathcal{MH}_{\mathcal{R}}(G)/p\mathcal{R}$. On peut considérer $MH_{\mathcal{R}}(G)$ comme un sous-A-module de $P(\mathcal{R})/p\mathcal{R}$. D'après la proposition 5.5 du chapitre II, l'application $w_{\mathcal{R}}$ définit un isomorphisme de $CW_k(R)$ sur $P(\mathcal{R})/p\mathcal{R}$; en particulier, $P(\mathcal{R})/p\mathcal{R}$ devient, par transport de structure, un D_k-module. On sait que $\underline{M}(G)$ est le sous-D_k-module de $CW_k(R)$ formé des covecteurs $\underline{a}$ tels que $\underline{a}\hat{\otimes}1 - \Delta\underline{a} + 1\hat{\otimes}\underline{a} = 0$; on en déduit le résultat suivant :

PROPOSITION 6.5.- <u>Soit</u> G <u>un</u> p-<u>groupe formel lisse et de dimension finie</u> <u>sur</u> k <u>et soit</u> $\mathcal{R}$ <u>un relèvement lisse de l'algèbre affine de</u> G. <u>Le module</u> $MH_{\mathcal{R}}(G)$ <u>est un sous</u>-D_k-<u>module de</u> $P(\mathcal{R})/p\mathcal{R}$ <u>et l'application</u> $w_{\mathcal{R}}$ <u>induit un isomorphisme de</u> $\underline{M}(G)$ <u>sur</u> $MH_{\mathcal{R}}(G)$.

CHAPITRE IV

GROUPES FORMELS LISSES SUR UN ANNEAU DE VALUATION DISCRÈTE

§ 1.- Le cas $e = 1$.

1.1. Soit G un p-groupe formel lisse de dimension finie sur $A = W(k)$ et soit $\mathfrak{R}$ son algèbre affine. Soit $G_k = G \otimes_A k$ la réduction de G modulo p ; c'est un groupe formel lisse de dimension finie sur k dont l'algèbre affine s'identifie à $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. On voit, avec les conventions de II.5.4 et III.6.4, que $\mathfrak{R}$ est un A-anneau spécial qui est un relèvement lisse de $\mathfrak{R}_k$. Notons $\Delta : \mathfrak{R} \to \mathfrak{R} \hat{\otimes}_A \mathfrak{R}$ (resp. $\Delta_k : \mathfrak{R}_k \to \mathfrak{R}_k \hat{\otimes}_k \mathfrak{R}_k$) le coproduit relatif à G (resp. à G_k) ; il est clair que Δ relève Δ_k . Notons encore Δ le prolongement de Δ à $\hat{\mathfrak{R}}_K^{an}$ et, pour tout $\alpha \in \hat{\mathfrak{R}}_K^{an}$, posons $\partial\alpha = \alpha \hat{\otimes} 1 - \Delta\alpha + 1 \hat{\otimes} \alpha$. Notons $\mathcal{MH}(G)$ le sous-A-module de $\hat{\mathfrak{R}}_K^{an}$ formé des $\alpha \in P(\mathfrak{R})$ tels que $\partial\alpha \in p\mathfrak{R} \hat{\otimes}_A \mathfrak{R}$ et $MH(G)$ le quotient de $\mathcal{MH}(G)$ par $p\mathfrak{R}$. Avec les notations du n° III.6.4, on a $\mathcal{MH}(G) = \mathcal{MH}_{\mathfrak{R}}(G_k)$ et $MH(G) = \mathbf{MH}_{\mathfrak{R}}(G_k)$. Il résulte donc de la proposition 6.5 du chapitre III que $MH(G)$ s'identifie canoniquement au module de Dieudonné $\underline{M}(G_k)$ de G_k .

Notons $\mathcal{L}(G)$ l'ensemble des éléments α de $P(\mathfrak{R})$ tels que $\partial\alpha = 0$. Il est clair que $\mathcal{L}(G)$ est un sous-A-module de $\mathcal{MH}(G)$. Nous notons $\rho(G)$ l'application A-linéaire

$$\mathcal{L}(G) \xrightarrow{\text{inclusion}} \mathcal{MH}(G) \xrightarrow{\text{proj. can.}} MH(G) \xrightarrow{\text{iso. can.}} \underline{M}(G_k) .$$

L'image par $\rho(G)$ de $p\mathcal{L}(G)$ est contenue dans $p\underline{M}(G_k) \subset \underline{F}\underline{M}(G_k)$; on en déduit, par passage aux quotients, une application k-linéaire $\tilde{\rho}(G)$ de $\mathcal{L}(G)/p\mathcal{L}(G)$ dans $\underline{M}(G_k)/\underline{F}\underline{M}(G_k)$.

PROPOSITION 1.1.- <u>Soit</u> G <u>un p-groupe formel lisse de dimension finie sur</u> A. <u>Posons</u> $M = \underline{M}(G_k)$, $\mathcal{L} = \mathcal{L}(G)$ <u>et</u> $\tilde{\rho} = \tilde{\rho}(G)$. <u>Alors</u>

i) <u>l'application</u> $\tilde{\rho} : \mathcal{L}/p\mathcal{L} \to M/\underline{F}M$ <u>est un isomorphisme de k-espaces vectoriels</u> ;

ii) <u>le A-module</u> $\mathcal{L}$ <u>est libre de rang fini</u>.

Démonstration :

i) posons $\rho = \rho(G)$. Soit $\alpha \in \mathfrak{L}$; si $\rho(\alpha) = \underline{a}$, $\underline{a}$ s'écrit comme un covecteur $(\dots, a_{-n}, \dots, a_0)$ à coefficients dans $\mathfrak{R}_k$ et, quel que soit le choix des relèvements $\hat{a}_{-n}$ des a_{-n} dans $\mathfrak{R}$, $\alpha - \sum p^{-n}\hat{a}_{-n}^{p^n} \in p\mathfrak{R}$.

Si $\alpha \in \mathfrak{L}$ est tel que $\rho(\alpha) = \underline{a} \in \underline{F}M$, il existe $\underline{b} = (\dots, b_{-n}, \dots, b_0) \in M$ tel que $\underline{a} = \underline{F}\,\underline{b} = (\dots, b_{-n}^p, \dots, b_0^p)$. Si, pour tout n , $\hat{b}_{-n}$ est un relèvement de b_{-n} dans $\mathfrak{R}$, on a donc $\alpha - \sum p^{-n}(\hat{b}_{-n}^p)^{p^n} = \alpha - \sum p^{-n}\hat{b}_{-n}^{p^{n+1}} \in p\mathfrak{R}$. Il existe donc un élément $\hat{b}_1 \in \mathfrak{R}$ tel que $\alpha = \sum_{n=-1}^{\infty} p^{-n}\hat{b}_{-n}^{p^{n+1}} = p\left(\sum_{n=0}^{\infty} p^{-n}\hat{b}_{-n+1}^{p^n}\right)$; on voit donc que $\beta = p^{-1}\alpha$ vérifie $\partial\beta = 0$ et $\beta \in P(\mathfrak{R})$. Donc $\alpha \in p\mathfrak{L}$, ce qui montre que l'application $\tilde{\rho}$ est injective.

Pour montrer que $\tilde{\rho}$ est surjective, commençons par établir un lemme :

LEMME 1.2.- <u>Soit</u> r <u>un entier</u> ≥ 1 <u>et soit</u> $\alpha \in P(\mathfrak{R})$ <u>tel que</u> $\partial\alpha \in p^r\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}$. <u>Il existe un élément</u> $\gamma \in \mathcal{M}\mathcal{H}(G)$ <u>tel que</u> $\rho(\gamma) \in \underline{F}M$ <u>et</u> $\partial(\alpha - p^{r-1}\gamma) \in p^{r+1}\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}$ <u>(on a encore noté</u> ρ <u>la projection canonique de</u> $\mathcal{M}\mathcal{H}(G)$ <u>sur</u> $\underline{M}(G_k) = M$).

Démonstration du lemme : si $\hat{G}_{aA}$ est le complété formel du groupe additif sur A , $\mathfrak{R}^{\hat{\otimes}n}$ s'identifie au groupe des n-cochaînes de G à valeurs dans $\hat{G}_{aA}$ et l'opérateur bord coïncide, en dimension 1 , avec ∂ .

Si l'on pose $\partial\alpha = p^r\beta$, alors $\beta \in \mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}$ et vérifie $\partial\beta = 0$ car $p^r\partial\beta = \partial(p^r\beta) = \partial(\partial\alpha) = 0$. Si b_0 désigne l'image de β dans $\mathfrak{R}_k\,\hat{\otimes}_k\,\mathfrak{R}_k$, on a donc $\partial b_0 = 0$ (où ∂ désigne maintenant l'opérateur bord pour la cohomologie de G_k à valeurs dans $\hat{G}_{ak}$). Si l'on pose

$$\underline{b} = (\dots, 0, \dots, 0, b_0) \in \widehat{CW}_k(\mathfrak{R}_k\,\hat{\otimes}_k\,\mathfrak{R}_k) = C^1(G_k, \widehat{CW}_k) ,$$

on voit que $\partial\underline{b} = 0$ (où, cette fois-ci, ∂ est l'opérateur bord pour la cohomologie de G_k à valeurs dans $\widehat{CW}_k$). Comme b_0 est un tenseur symétrique, $\underline{b}$ est un 2-cocycle symétrique. Comme $\widehat{CW}_k$ est un objet injectif de la catégorie des groupes formels sur k (théorème 2 du chapitre III), on a

$$H_s^2(G_k, \widehat{CW}_k) = \mathrm{Ext}_{ab}^1(G_k, \widehat{CW}_k) = 0 \quad ;$$

on en déduit l'existence d'un élément $\underline{c} = (\dots, c_{-n}, \dots, c_0) \in \widehat{CW}_k(\mathfrak{R}_k)$ tel que $\partial\underline{c} = \underline{b}$. Si l'on désigne par $\hat{c}_{-n}$ un relèvement de c_{-n} dans $\mathfrak{R}$, on voit donc que $\partial\left(\sum_{n=0}^{\infty} p^{-n}\hat{c}_{-n}^{p^n}\right) \equiv \beta \pmod{p\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}}$. Posons $\gamma = p\sum_{n=0}^{\infty} p^{-n}\hat{c}_{-n}^{p^n}$; on a

$\partial(p^{r-1}\gamma) \equiv p^r\beta \pmod{p^{r+1}\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}}$ donc $\partial(\alpha - p^{r-1}\gamma) \in p^{r+1}\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}$.

On voit d'autre part que γ est un relèvement dans $P(\mathfrak{R})$ de $p\underline{c} = \underline{F}\,\underline{V}\,\underline{c} = \underline{F}(\ldots,c_{-n+1},\ldots,c_{-1})$; mais l'égalité $\partial\underline{c} = \underline{b}$ montre que $\partial(\underline{V}\,\underline{c}) = \underline{V}\,\underline{b} = 0$, donc que $\underline{V}\,\underline{c} \in M$. On voit donc que $\gamma \in \mathcal{M}\mathfrak{H}(G)$ et que $\rho(\gamma) = p\underline{c} \in \underline{F}M$, d'où le lemme.

Pour montrer que $\tilde{\rho}$ est surjective, on voit qu'il suffit de vérifier que pour tout $\underline{a} \in M$, il existe $\alpha \in \mathfrak{L}$ tel que $\rho(\alpha) \equiv \underline{a} \pmod{\underline{F}M}$.

Si $\underline{a} \in M$ et si α_1 est un élément de $P(\mathfrak{R})$ tel que $\rho(\alpha_1) = \underline{a}$, on sait que $\alpha_1 \in \mathcal{M}\mathfrak{H}(G)$, donc que $\partial\alpha_1 \in p\mathfrak{R}$.

Le lemme permet donc de construire par récurrence une suite $\gamma_1,\gamma_2,\ldots,\gamma_r,\ldots$ d'éléments de $\mathcal{M}\mathfrak{H}(G)$ tels que $\rho(\gamma_r) \in \underline{F}M$ et $(\alpha_1 - \gamma_1 - \ldots - p^{r-1}\gamma_r) \in p^{r+1}\mathfrak{R}\,\hat{\otimes}_A\,\mathfrak{R}$, pour tout r .

Mais $\mathcal{M}\mathfrak{H}(G)$, extension du A-module profini $MH(G)$ $(\simeq M)$ par le A-module $p\mathfrak{R}$ qui est topologiquement libre donc profini, est un A-module profini. Il est donc séparé et complet pour la topologie p-adique. En particulier, la série de terme général $p^{r-1}\gamma_r$ converge dans $P(\mathfrak{R})$; si $\alpha = \alpha_1 - \sum_{r=1}^{\infty} p^{r-1}\gamma_r$, on voit que $\partial\alpha = 0$ et que $\rho(\alpha) = \rho(\alpha_1) - \sum_{r=1}^{\infty} p^{r-1}\rho(\gamma_r) \equiv \rho(\alpha_1) \pmod{\underline{F}M}$ et $\tilde{\rho}$ est bien surjective.

L'assertion (ii) est alors évidente : d'après (i), $\mathfrak{L}$ est un A-module de type fini ; mais c'est un sous-A-module de $P(\mathfrak{R})$ qui est sans torsion ; il est donc libre de rang fini (on voit que son rang est égal à $\dim_k(M/\underline{F}M)$, donc à la dimension de G).

1.2. Notons Λ_A^{ℓ} la catégorie dont les objets sont les triplets $(\mathfrak{L},M,\rho)$

- où M est un D_k-module profini sur lequel l'action de $\underline{F}$ est injective, tel que le quotient $M/\underline{F}M$ est un espace vectoriel de dimension finie sur k ,
- où $\mathfrak{L}$ est un A-module libre de rang fini,
- où ρ est une application A-linéaire de $\mathfrak{L}$ dans M telle que l'application $\tilde{\rho} : \mathfrak{L}/p\mathfrak{L} \to M/\underline{F}M$, induite par passage aux quotients, est un isomorphisme de k-espaces vectoriels.

Un morphisme $u : (\mathfrak{L},M,\rho) \to (\mathfrak{L}',M',\rho')$ de la catégorie Λ_A^{ℓ} est un couple $(u_{\mathfrak{L}}, u_M)$ formé d'une application A-linéaire $u_{\mathfrak{L}} : \mathfrak{L} \to \mathfrak{L}'$ et d'une application D_k-linéaire continue $u_M : M \to M'$ tel que le diagramme

$$\begin{array}{ccc} \mathfrak{L} & \xrightarrow{u_{\mathfrak{L}}} & \mathfrak{L}' \\ \rho \downarrow & & \downarrow \rho' \\ M & \xrightarrow{u_M} & M' \end{array}$$

soit commutatif.

Il est clair que Λ_A^{ℓ} est une catégorie additive.

La proposition 6.1 du chapitre III et la proposition 1.1 montrent que, si G est un p-groupe formel lisse, de dimension finie, sur A, le triplet $\mathfrak{L}M_A(G) = (\mathfrak{L}(G), \underline{M}(G_k), \rho(G))$ est un objet de Λ_A^{ℓ}.

Soit maintenant $f : G' \to G$ un morphisme de p-groupes formels lisses de dimension finie sur A. Par réduction modulo p, f induit un morphisme $f_k : G'_k \to G_k$ donc une application D_k-linéaire continue $\underline{M}(f_k) : \underline{M}(G_k) \to \underline{M}(G'_k)$. Soit, d'autre part, $\mathfrak{R}$ (resp. $\mathfrak{R}'$) l'algèbre affine de G (resp. G') ; le morphisme f induit un homomorphisme continu $f^* : \mathfrak{R} \to \mathfrak{R}'$ qui se prolonge, de manière unique, en un homomorphisme continu $f_K^* : \hat{\mathfrak{R}}_K^{an} \to (\hat{\mathfrak{R}}')_K^{an}$. Il est clair que f_K^* envoie $P(\mathfrak{R})$ dans $P(\mathfrak{R}')$ et $\mathfrak{L}(G)$ dans $\mathfrak{L}(G')$. Si l'on note $\mathfrak{L}(f)$ la restriction de f_K^* à $\mathfrak{L}(G)$, on vérifie immédiatement que le couple $(\mathfrak{L}(f), \underline{M}(f_k))$ est un morphisme de la catégorie Λ_A^{ℓ}, i.e. que le diagramme

$$\begin{array}{ccc} \mathfrak{L}(G) & \xrightarrow{\mathfrak{L}(f)} & \mathfrak{L}(G') \\ \rho(G) \downarrow & & \downarrow \rho'(G') \\ \underline{M}(G_k) & \xrightarrow{\underline{M}(f_k)} & M(G'_k) \end{array}$$

est commutatif.

Ceci permet de considérer $\mathfrak{L}M_A$ comme un foncteur contravariant de la catégorie des p-groupes formels lisses de dimension finie sur A dans Λ_A^{ℓ}. On voit facilement que ce foncteur est additif.

Rappelons (cf. n° I.7.6) que l'on dit qu'un k-groupe formel H est <u>unipotent</u> si $H = \varinjlim \operatorname{Ker} V_{H^{\sigma^n}}$. Si G est un groupe formel sur A (plus généralement sur A', anneau des entiers d'une extension finie totalement ramifiée de $K = \mathrm{Frac}(A)$), nous disons que G est <u>unipotent</u> si G_k l'est.

Notons enfin Λ_A^{c} (resp. Λ_A^{u}) la sous-catégorie pleine de Λ_A^{ℓ} dont les objets sont les triplets $(\mathcal{L}, M, \rho)$ tels que M est "connexe" (resp. "unipotent") i.e. tels que l'action de $\underline{F}$ (resp. de $\underline{V}$) sur M est topologiquement nilpotente.

Il est clair que, si G est un p-groupe formel lisse de dimension finie sur A qui est connexe, (resp. unipotent), $\mathcal{L}M_A(G)$ est un objet de Λ_A^c (resp. Λ_A^u) .

L'objet essentiel de ce paragraphe est de démontrer le résultat suivant :

THÉORÈME 1.- <u>Si</u> $p \neq 2$, <u>le foncteur</u> $\mathcal{L}M_A$ <u>induit une anti-équivalence entre la catégorie des p-groupes formels lisses et de dimension finie sur</u> A <u>et la catégorie</u> Λ_A^ℓ .

<u>Pour</u> p <u>quelconque, la restriction de</u> $\mathcal{L}M_A$ <u>aux p-groupes formels lisses et connexes (resp. et unipotents) de dimension finie sur</u> A <u>induit une anti-équivalence entre cette catégorie et</u> Λ_A^c <u>(resp.</u> Λ_A^u) .

1.3. Soit $(\mathcal{L}, M, \rho)$ un objet de Λ_A^ℓ . Nous allons lui associer un foncteur covariant de la catégorie des A-anneaux p-adiques (cf. n° II.5.1) dans celle des groupes abéliens.

Soit $\mathcal{S}$ un A-anneau p-adique :

- nous notons $N_{\mathcal{L}}(\mathcal{S})$ (resp. $N^0_{\mathcal{L}}(\mathcal{S})$) le groupe $\mathrm{Hom}_A(\mathcal{L}, \mathcal{S}_K)$ (resp. $\mathrm{Hom}_A(\mathcal{L}, \mathcal{S}_K/p\mathcal{S})$ des applications A-linéaires de $\mathcal{L}$ dans $\mathcal{S}_K = \mathcal{S} \otimes_A K$ (resp. dans $\mathcal{S}_K/p\mathcal{S}$) ;
- nous notons $G_M(\mathcal{S})$ le groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(\mathcal{S}_k))$ des applications D_k-linéaires continues de M dans $CW_k(\mathcal{S}_k)$ (où $\mathcal{S}_k = \mathcal{S} \otimes_A k$) ;
- nous notons φ_ρ l'application de $G_M(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ qui à $u \in G_M(\mathcal{S})$ associe $w_{\mathcal{S}} \circ u \circ \rho$ (où $w_{\mathcal{S}} : CW_k(\mathcal{S}_k) \to \mathcal{S}_K/p\mathcal{S}$ est l'application qui a été définie au n° II.5.2) ; il est clair que φ_ρ est un homomorphisme de groupes ;
- enfin, nous notons $G_{(\mathcal{L},M,\rho)}(\mathcal{S})$ le produit fibré $N_{\mathcal{L}}(\mathcal{S}) \times_{N^0_{\mathcal{L}}(\mathcal{S})} G_M(\mathcal{S})$, où le morphisme de $N_{\mathcal{L}}(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ est celui qui provient de la projection de $\mathcal{S}_K$ sur $\mathcal{S}_K/p\mathcal{S}$ et celui de $G_M(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ est φ_ρ .

Il est clair que toutes ces constructions sont fonctorielles en S .

Choisissons maintenant un p-groupe formel lisse G_k dont le module de Dieudonné $M_0 = \underline{M}(G_k)$ est isomorphe à M (un tel groupe existe et est unique, à isomorphisme près, d'après la proposition 6.1 du chapitre III) ainsi qu'un isomorphisme i de M sur M_0 .

Soit R l'algèbre affine de G_k et choisissons un A-anneau spécial $\mathfrak{R}$ qui relève R . Choisissons enfin un isomorphisme ι de $\mathfrak{L}$ sur un sous-A-module $\mathfrak{L}_0$ de $P(\mathfrak{R})$ tel que le diagramme

$$\begin{tikzcd} \mathfrak{L} \arrow[r, "\iota"] \arrow[d, "\rho"'] & \mathfrak{L}_0 \arrow[r, hook] & P(\mathfrak{R}) \arrow[dr] & \\ & & & P(\mathfrak{R})/p\mathfrak{R} \\ M \arrow[r, "i"] & M_0 \arrow[r, hook] & CW_k(R) \arrow[ur, "w_{\mathfrak{R}}"'] & \end{tikzcd}$$

soit commutatif (il est clair qu'un tel ι existe toujours) et notons ρ_0 l'application A-linéaire $i \circ \rho \circ \iota^{(-1)} : \mathfrak{L}_0 \to M_0$.

Pour tout A-anneau p-adique $\mathfrak{S}$, notons $X_{\mathfrak{R}}(\mathfrak{S})$ l'ensemble des homomorphismes continus du A-anneau $\mathfrak{R}$ dans $\mathfrak{S}$.

Si $x \in X_{\mathfrak{R}}(\mathfrak{S})$, x se prolonge, de manière unique, en un homomorphisme continu de $\hat{\mathfrak{R}}_K^{an}$ dans $\mathfrak{S}_K$; nous notons $x_{\mathfrak{L}_0}$ sa restriction à $\mathfrak{L}_0$ et $x_{\mathfrak{L}} : \mathfrak{L} \to \mathfrak{S}_K$ l'application A-linéaire composée $x_{\mathfrak{L}_0} \circ \iota$.

De même x induit un homomorphisme continu $x_k : R \to \mathfrak{S}_k$ donc une application D_k-linéaire $CW_k(x_k) : CW_k(R) \to CW_k(\mathfrak{S}_k)$; nous notons x_{M_0} sa restriction à M_0 et $x_M : M \to CW_k(\mathfrak{S}_k)$ l'application D_k-linéaire composée $x_{M_0} \circ i$.

LEMME 1.3.- <u>Pour tout</u> $x \in X_{\mathfrak{R}}(\mathfrak{S})$, $(x_{\mathfrak{L}}, x_M) \in G_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$. <u>L'application</u> $x \mapsto (x_{\mathfrak{L}}, x_M)$ <u>de</u> $X_{\mathfrak{R}}(\mathfrak{S})$ <u>dans</u> $G_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$ <u>est bijective si</u> $p \neq 2$ <u>ou si</u> M <u>est unipotent (i.e. si</u> G_k <u>l'est</u>).

La démonstration de ce lemme est renvoyée au n° 1.6.

1.4. Soit alors G un p-groupe formel lisse et de dimension finie sur A et soit $\mathfrak{L}M_A(G) = (\mathfrak{L}, M, \rho)$. Il est clair que le lemme précédent s'applique en prenant $G_k = G \otimes_A k$, $M_0 = M$, $i = id_M$, $\mathfrak{R}$ = l'algèbre affine de G , $\mathfrak{L}_0 = \mathfrak{L}$ et $\iota = id_{\mathfrak{L}}$.

PROPOSITION 1.4.- Soit G un p-groupe formel lisse et de dimension finie sur A, soit $\mathfrak{R}$ son algèbre affine, et soit $(\mathfrak{L}, M, \rho) = \mathfrak{L}M_A(G)$. Soit $\mathfrak{S}$ un A-anneau p-adique. Pour tout $x \in G(\mathfrak{S}) = \mathrm{Hom}_{\mathrm{cont}}(\mathfrak{R}, \mathfrak{S})$, $(x_{\mathfrak{L}}, x_M) \in G_{(\mathfrak{L}, M, \rho)}(\mathfrak{S})$ et l'application $x \mapsto (x_{\mathfrak{L}}, x_M)$ est un homomorphisme du groupe $G(\mathfrak{S})$ dans $G_{(\mathfrak{L}, M, \rho)}(\mathfrak{S})$; c'est un isomorphisme si $p \neq 2$ ou si G est unipotent.

Démonstration : compte-tenu du lemme 1.3, il suffit de montrer que l'application $x \mapsto (x_{\mathfrak{L}}, x_M)$ est un homomorphisme de groupes, ou encore que chacune des deux applications $x \mapsto x_M$ et $x \mapsto x_{\mathfrak{L}}$ est un homomorphisme de groupes.

Pour l'application $x \mapsto x_M$ c'est clair : on voit que c'est le composé de l'application canonique de $G(\mathfrak{S})$ dans $G(\mathfrak{S}_k) = G_k(\mathfrak{S}_k)$ par l'isomorphisme canonique de $G_k(\mathfrak{S}_k)$ sur $G_M(\mathfrak{S})$ résultant de la proposition 6.2 du chapitre III.

Montrons donc que l'application $x \mapsto x_{\mathfrak{L}}$ est un homomorphisme de groupes. Soit $\Delta : \mathfrak{R} \to \mathfrak{R} \hat{\otimes}_A \mathfrak{R}$ le co-produit ; il se prolonge en une application $\Delta_K : \hat{\mathfrak{R}}_K^{an} \to \hat{\mathfrak{R}}_K^{an} \hat{\otimes}_A \hat{\mathfrak{R}}_K^{an}$. Soit x et y des éléments de $G(\mathfrak{S})$ et soit $z = x + y$. Les applications x, y, z de $\mathfrak{R}$ dans $\mathfrak{S}$ se prolongent en des homomorphismes continus x_K, y_K, z_K de $\hat{\mathfrak{R}}_K^{an}$ dans $\mathfrak{S}_K$. Si $\alpha \in \hat{\mathfrak{R}}_K^{an}$, on voit que $z_K(\alpha) = (\pi_{\mathfrak{S}} \circ (x_K \hat{\otimes} y_K) \circ \Delta_K)(\alpha)$, où $\pi_{\mathfrak{S}} : \mathfrak{S}_K \hat{\otimes}_A \mathfrak{S}_K \to \mathfrak{S}_K$ est définie par la multiplication dans $\mathfrak{S}_K$. Si $\alpha \in \mathfrak{L}$, on a donc

$$\begin{aligned} z_{\mathfrak{L}}(\alpha) &= z_K(\alpha) = (\pi_{\mathfrak{S}} \circ (x_K \hat{\otimes} y_K))(\alpha \hat{\otimes} 1 + 1 \hat{\otimes} \alpha) = \pi_S(x_{\mathfrak{L}}(\alpha) \hat{\otimes} 1 + 1 \hat{\otimes} y_{\mathfrak{L}}(\alpha)) \\ &= x_L(\alpha) + y_L(\alpha) \quad ; \end{aligned}$$

d'où la proposition.

1.5. Montrons maintenant le théorème 1 pour $p \neq 2$ et pour les groupes unipotents (et p quelconque).

Il résulte du lemme de Yoneda qu'un groupe formel topologiquement plat sur A est complètement déterminé par la restriction du foncteur en groupes qu'il définit à la catégorie des A-anneaux p-adiques.

Si $p \neq 2$ et si $(\mathfrak{L}, M, \rho)$ est un objet de Λ_A^{ℓ} (resp. si p est quelconque et si $(\mathfrak{L}, M, \rho)$ est un objet de Λ_A^{u}), le lemme 1.3 implique qu'il existe un A-anneau spécial $\mathfrak{R}$ tel que, pour tout A-anneau p-adique $\mathfrak{S}$, $G_{(\mathfrak{L}, M, \rho)}(\mathfrak{S})$ s'identifie à l'ensemble des homomorphismes continus de $\mathfrak{R}$ dans

$\mathcal{S}$, et ceci fonctoriellement en $\mathcal{S}$. On voit donc que $G_{(\mathcal{L},M,\rho)}$ définit un p-groupe formel G lisse et de dimension finie sur A , dont l'algèbre affine est isomorphe à $\mathfrak{R}$. On vérifie immédiatement que $\mathcal{L}M_A(G)$ s'identifie à $(\mathcal{L},M,\rho)$ et que G est unipotent si M l'est. On en déduit que le foncteur $\mathcal{L}M_A$ est essentiellement surjectif.

Il reste donc à montrer que $\mathcal{L}M_A$ est pleinement fidèle : soit G et G' deux groupes formels lisses et de dimension finie sur A . Posons

$$\mathcal{L}M_A(G) = (\mathcal{L},M,\rho) \ , \quad \mathcal{L}M_A(G') = (\mathcal{L}',M',\rho') \ .$$

Avec des notations évidentes, il résulte de la proposition 1.4 que, pour tout A-anneau p-adique $\mathcal{S}$, $G'(\mathcal{S})$ (resp. $G(\mathcal{S})$) s'identifie canoniquement (et fonctoriellement en $\mathcal{S}$) à $N_{\mathcal{L}'}(\mathcal{S}) \times_{N^0_{\mathcal{L}'}(\mathcal{S})} G_{M'}(\mathcal{S})$ (resp. $N_{\mathcal{L}}(\mathcal{S}) \times_{N^0_{\mathcal{L}}(\mathcal{S})} G_M(\mathcal{S})$) .

Soit f un morphisme de G' dans G et soit $\mathcal{L}M_A(f) = (\mathcal{L}(f), \underline{M}(f_k))$. Pour tout A-anneau p-adique $\mathcal{S}$, et tout $x = (x_{\mathcal{L}'}, x_{M'}) \in G'(\mathcal{S})$ on a $f_{\mathcal{S}}(x) = (x_{\mathcal{L}}, x_M)$ avec $x_{\mathcal{L}} = x_{\mathcal{L}'} \circ \mathcal{L}(f)$ et $x_M = x_{M'} \circ \underline{M}(f_k)$; on voit donc que $x_{\mathcal{L}} = 0$ si $\mathcal{L}(f) = 0$ et $x_M = 0$ si $\underline{M}(f_k) = 0$; par conséquent, si $\mathcal{L}M_A(f) = 0$, on a $f_{\mathcal{S}}(x) = 0$, pour tout A-anneau p-adique $\mathcal{S}$ et tout $x \in G'(\mathcal{S})$, ce qui montre que $\mathcal{L}M_A$ est fidèle.

Si maintenant $u : (L,M,\rho) \to (L',M',\rho')$ est un morphisme de la catégorie Λ^{ℓ}_A (resp. Λ^u_A si $p=2$), il définit, de manière évidente, un morphisme $u_S : N_{\mathcal{L}'}(\mathcal{S}) \times_{N^0_{\mathcal{L}'}(\mathcal{S})} G_{M'}(\mathcal{S}) \to N_{\mathcal{L}}(\mathcal{S}) \times_{N^0_{\mathcal{L}}(\mathcal{S})} G_M(\mathcal{S})$, pour tout A-anneau p-adique $\mathcal{S}$, visiblement fonctoriel en $\mathcal{S}$. D'où une famille, fonctorielle en $\mathcal{S}$, de morphisme $f_{\mathcal{S}} : G'(\mathcal{S}) \to G(\mathcal{S})$, i.e. un morphisme $f : G' \to G$ tel que $\mathcal{L}M_A(f) = u$ et le foncteur $\mathcal{L}M_A$ est pleinement fidèle.

1.6. Nous reprenons les hypothèses et les notations du lemme 1.3 que nous nous proposons de démontrer maintenant. Nous posons $G(\mathcal{S}) = G_{(\mathcal{L},M,\rho)}(\mathcal{S})$ et nous utilisons l'application i (resp. ι) pour identifier M et M_0 (resp. $\mathcal{L}$ et $\mathcal{L}_0$).

Comme tout p-groupe formel sur k , G_k se décompose en le produit direct d'un groupe G^c_k connexe et d'un groupe G^{et}_k étale. Si R^c (resp. R^{et}) désigne l'algèbre affine de G^c_k (resp. G^{et}_k) , R^c et R^{et} s'identifient à des sous-anneaux de R et le produit définit un isomorphisme de $R^{et} \hat{\otimes}_k R^c$ sur

R . Nous notons $\mathfrak{R}^{et}$ le relèvement de R^{et} dans $\mathfrak{R}$ et nous choisissons un sous-anneau local $\mathfrak{R}^c$ de $\mathfrak{R}$ qui relève R^c ; ici encore le produit définit un isomorphisme de $\mathfrak{R}^{et} \hat{\otimes}_A \mathfrak{R}^c$ sur $\mathfrak{R}$.

Comme $G_k = G_k^c \times G_k^{et}$, on a $M = M^c \oplus M^{et}$, avec $M^c = \underline{M}(G_k^c)$ et $M^{et} = \underline{M}(G_k^{et})$; tout élément $\underline{a} \in M$ s'écrit donc d'une manière et d'une seule sous la forme $\underline{a} = \underline{a}^c + \underline{a}^{et}$, avec $\underline{a}^c \in M^c \subset CW_k(R^c)$ et $\underline{a}^{et} \in M^{et} \subset CW_k(R^{et})$.

Soit $\alpha \in \mathfrak{L}$ et soit $\underline{a} = \rho(\alpha) = \underline{a}^c + \underline{a}^{et}$; si $\underline{a}^c = (\dots, a_{-n}^c, \dots, a_{-1}^c, a_0^c)$ et $\underline{a}^{et} = (\dots, a_{-n}^{et}, \dots, a_{-1}^{et}, a_0^{et})$ et si l'on choisit des relèvements $\hat{a}_{-n}^c$ des a_{-n}^c dans $\mathfrak{R}^c$ et $\hat{a}_{-n}^{et}$ des a_{-n}^{et} dans $\mathfrak{R}^{et}$, $w_{\mathfrak{R}}(\underline{a})$ est l'image, dans $P(\mathfrak{R})/p\mathfrak{R}$ de $\sum_{n=0}^{\infty} p^{-n}(\hat{a}_{-n}^c)^{p^n} + \sum_{n=0}^{\infty} p^{-n}(\hat{a}_{-n}^{et})^{p^n}$. Comme $\underline{a} = \rho(\alpha)$, l'image de α dans $P(\mathfrak{R})/p\mathfrak{R}$ est $w_{\mathfrak{R}}(\underline{a})$ et l'on a donc $\alpha = \alpha^c + \alpha^{et} + p\beta$, avec $\alpha^c = \sum p^{-n}(\hat{a}_{-n}^c)^{p^n} \in P(\mathfrak{R}^c)$, $\alpha^{et} = \sum p^{-n}(\hat{a}_{-n}^{et})^{p^n} \in P(\mathfrak{R}^{et})$ et $\beta \in \mathfrak{R}$.

Choisissons des coordonnées $\underline{X} = (X_1, X_2, \dots, X_d)$ pour $\mathfrak{R}^c$: l'anneau $\mathfrak{R}^c$ s'identifie donc à $A[[\underline{X}]] = A[[X_1, \dots, X_d]]$ et R^c à $k[[\underline{\tilde{X}}]] = k[[\tilde{X}_1, \dots, \tilde{X}_d]]$, en notant $\tilde{X}_i$ l'image de X_i dans R .

Si maintenant $\alpha_1, \alpha_2, \dots, \alpha_d$ est une base du A-module libre $\mathfrak{L}$, chaque α_i peut s'écrire, compte-tenu de ce qui précède, sous la forme

$$\alpha_i = \alpha_i^c + \alpha_i^{et} + p\beta_i ,$$

avec $\alpha_i^c \in P(\mathfrak{R}^c)$, $\alpha_i^{et} \in P(\mathfrak{R}^{et})$, $\beta_i \in \mathfrak{R}$; en particulier, chaque α_i^c peut être considéré comme une série formelle en les X_j à coefficients dans K .

Commençons par établir un autre lemme :

LEMME 1.5.-

i) <u>La matrice des</u> $\dfrac{\partial \alpha_i^c}{\partial X_j}$ <u>est à coefficients dans</u> $\mathfrak{R}^c$ <u>et inversible dans</u> $\mathfrak{R}^c$;

ii) <u>la matrice des</u> $\dfrac{\partial^p \alpha_i^c}{\partial X_j^p}$ <u>est à coefficients dans</u> $\mathfrak{R}^c$; <u>si</u> M <u>est unipotent (i.e. si</u> G_k <u>l'est), on peut choisir les coordonnées</u> X_j <u>et la base des</u> α_i <u>pour que cette matrice soit topologiquement nilpotente</u>.

<u>Démonstration</u> :

i) Si $\rho(\alpha_i) = \underline{a}_i^c + \underline{a}_i^{et}$ et si $\underline{a}_i^c = (\dots, a_{-n,i}^c, \dots, a_{0,i}^c)$, on a

$\alpha_i^c = \sum p^{-n}(\hat{a}^c_{-n,i})^{p^n}$, pour des relèvements convenables $\hat{a}^c_{-n,i}$ des $a^c_{-n,i}$ dans $\mathfrak{R}^c$.

Notons $\mathfrak{m}$ (resp. $\hat{\mathfrak{m}}$) l'idéal maximal de R^c (resp. $\mathfrak{R}^c$) . Comme G_k^c est connexe, $M^c = \mathrm{Hom}(G_k^c, \widehat{CW}_k) = \mathrm{Hom}(G_k^c, \widehat{CW}_k^c)$ est contenu dans $CW_k^c(R^c)$, autrement dit tous les $a^c_{-n,i}$ sont dans $\mathfrak{m}$; par conséquent, tous les $\hat{a}^c_{-n,i}$ sont dans $\hat{\mathfrak{m}}$.

On a $\dfrac{\partial \alpha_i^c}{\partial X_j} = \sum\limits_{n=0}^{\infty} (\hat{a}^c_{-n,i})^{p^n-1} \dfrac{\partial \hat{a}^c_{-n,i}}{\partial X_j} \in \mathfrak{R}^c$.

De plus, comme les $\hat{a}^c_{-n,i}$ sont dans $\hat{\mathfrak{m}}$, $(\hat{a}^c_{-n,i})^{p^n-1} \in \hat{\mathfrak{m}}$, si $p^n-1 \geq 1$, i.e. si $n \neq 0$, et $\dfrac{\partial \alpha_i^c}{\partial X_j} \equiv \dfrac{\partial \hat{a}^c_{0,i}}{\partial X_j}$ (mod $\hat{\mathfrak{m}}$) .

On sait (cf. proposition 4.3 du chapitre III) que l'application qui à $\underline{a} = (\dots, a_{-n}, \dots, a_0) \in M^c$ associe l'image de a_0 dans $\mathfrak{m}/\mathfrak{m}^2$, induit, par passage au quotient, un isomorphisme de $M^c/\underline{F}M^c$ sur $\mathfrak{m}/\mathfrak{m}^2$ $\left(\simeq t^*_{G_k^c}(k)\right)$; comme ρ induit un isomorphisme $\tilde{\rho} : \mathfrak{L}/p\mathfrak{L} \to M/\underline{F}M$ et comme la projection de M sur M^c induit un isomorphisme de $M/\underline{F}M$ sur $M^c/\underline{F}M^c$, on en déduit que les images des $a^c_{0,i}$ dans $\mathfrak{m}/\mathfrak{m}^2$ forment une base du k-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$: il en résulte que la matrice des $\dfrac{\partial a^c_{0,i}}{\partial X_j}$ est inversible dans R^c ; on voit qu'il en est de même de celle des $\dfrac{\partial \hat{a}^c_{0,i}}{\partial X_j}$, donc aussi de celle des $\dfrac{\partial \alpha_i^c}{\partial X_j}$, dans $\mathfrak{R}^c$.

ii) Il est clair que $\dfrac{\partial^p \alpha_i^c}{\partial X_j^p} = \dfrac{\partial^{p-1}}{\partial X_j^{p-1}}\left(\dfrac{\partial \alpha_i}{\partial X_j}\right) \in \mathfrak{R}^c$.

Posons, pour $1 \leq i \leq d$, $\hat{a}^c_{-1,i} = pb_i + \sum\limits_{j=1}^{d} c_{i,j} X_j$ + termes de $d° \geq 2$ (avec les b_i et les $c_{i,j}$ dans A). En utilisant le fait que les $\hat{a}^c_{-n,i}$ sont tous dans $\hat{\mathfrak{m}}$, on voit que $\dfrac{\partial^p \alpha_i^c}{\partial X_j^p} \equiv p^{-1}.p!.c^p_{i,j} \equiv -c^p_{i,j}$ (mod $\hat{\mathfrak{m}}$) .

Il est clair que la matrice des $\dfrac{\partial^p \alpha_i^c}{\partial X_j^p}$ est topologiquement nilpotente si et seulement si la matrice des $-c^p_{i,j}$ l'est, ou encore si et seulement si la matrice des $\tilde{c}_{i,j}$ est nilpotente dans k (en notant $\tilde{c}_{i,j}$ l'image de $c_{i,j}$ dans k).

Dire que M est unipotent revient à dire que l'action de $\underline{V}$ sur M/pM est nilpotente ; il revient au même de dire que l'action de $\underline{V}$ sur $M/\underline{F}M$ l'est ; on en déduit que l'on peut trouver une base $(\underline{\tilde{a}}_1, \underline{\tilde{a}}_2, \dots, \underline{\tilde{a}}_d)$ de $M/\underline{F}M$ sur k telle que $\underline{V}\underline{\tilde{a}}_d = 0$ et, pour $1 \le i < d$, $\underline{V}\underline{\tilde{a}}_i =$ ou bien 0 ou bien $\underline{\tilde{a}}_{i+1}$.

Choisissons, pour $1 \le i \le d$, un élément α_i de $\mathfrak{L}$ tel que l'image de $\rho(\alpha_i)$ dans $M/\underline{F}M$ soit $\underline{\tilde{a}}_i$: le fait que ρ induise un isomorphisme de $\mathfrak{L}/p\mathfrak{L}$ sur $M/\underline{F}M$ implique que de tels α_i existent et forment une base du A-module libre $\mathfrak{L}$.

L'isomorphisme composé $\mathfrak{L}/p\mathfrak{L} \to M/\underline{F}M \to M^c/\underline{F}M^c \to \mathfrak{m}/\mathfrak{m}^2$ nous montre que, si l'on note X_i un relèvement de $\hat{a}_{0,i}$ dans $\mathfrak{R}^c$, les X_i forment un système de coordonnées pour $\mathfrak{R}^c$. L'image de $\underline{V}\underline{a}_i^c = (\dots, a^c_{-n-1,i}, \dots, a^c_{-1,i})$ dans $\mathfrak{m}/\mathfrak{m}^2$ est l'image de $a^c_{-1,i}$ dans $\mathfrak{m}/\mathfrak{m}^2$ et c'est donc aussi celle de $\sum_{j=1}^{d} c_{i,j} X_j$; mais, comme la projection de $M/\underline{F}M$ sur $M^c/\underline{F}M^c$ est un $k[\underline{V}]$-isomorphisme, on voit que l'image de $\underline{V}\underline{a}_i^c$ dans $\mathfrak{m}/\mathfrak{m}^2$ est aussi celle de $\underline{V}\underline{\tilde{a}}_i$ qui vaut ou bien 0 ou bien $\underline{\tilde{a}}_{i+1}$; on voit donc que l'image de $\underline{V}\underline{a}_i^c$ dans $\mathfrak{m}/\mathfrak{m}^2$ est 0, sauf si $\underline{V}\underline{\tilde{a}}_i = \underline{\tilde{a}}_{i+1}$, auquel cas c'est l'image de X_{i+1}. Finalement les $\tilde{c}_{i,j}$ sont nuls, sauf peut-être certains des $\tilde{c}_{i,i+1}$ pour $1 \le i < d$ et la matrice des $\tilde{c}_{i,j}$ est bien nilpotente.

Démontrons maintenant le lemme 1.3

Montrer que $(x_{\mathfrak{L}}, x_M) \in G(\mathfrak{S})$ revient à montrer que le diagramme

$$\begin{tikzcd}
\mathfrak{L} \arrow[r, "x_{\mathfrak{L}}"] \arrow[d, "\rho"'] & \mathfrak{S}_K \arrow[dr, "\text{proj.}"] & \\
M \arrow[r, "x_M"] & CW_k(\mathfrak{S}_k) \arrow[r, "w_{\mathfrak{S}}"] & \mathfrak{S}_K/p\mathfrak{S}
\end{tikzcd}$$

est commutatif. Soit $\alpha \in \mathfrak{L}$ et soit $\underline{a} = (\dots, a_{-n}, \dots, a_0) = \rho(\alpha)$. On peut choisir des relèvements $\hat{a}_{-n}$ des a_{-n} dans $\mathfrak{R}$ pour que $\alpha = \sum p^{-n} \hat{a}_{-n}^{p^n}$; on a alors $x_{\mathfrak{L}}(\alpha) = \sum p^{-n} (x(\hat{a}_{-n})^{p^n})$.

D'autre part, on a $x_M(\rho(\alpha)) = (\dots, x_k(a_{-n}), \dots, x_k(a_0))$ et $(w_{\mathfrak{S}} \circ x_M \circ \rho)(\alpha)$ est l'image dans $\mathfrak{S}_K/p\mathfrak{S}$ de $\sum p^{-n} \hat{b}_{-n}^{p^n}$, en désignant par $\hat{b}_{-n}$ un relèvement quelconque dans $\mathfrak{S}$ de $x_k(a_{-n})$; il est clair que l'on peut choisir $\hat{b}_{-n} = x(\hat{a}_{-n})$ et on en déduit que $(w_{\mathfrak{S}} \circ x_M \circ \rho)(\alpha)$ est l'image de $x_{\mathfrak{L}}(\alpha)$ dans $\mathfrak{S}_K/p\mathfrak{S}$, ce qui démontre la première partie du lemme.

Soit ξ une application A-linéaire de $\mathfrak{L}$ dans $\mathcal{S}_K$ et soit η une application D_k-linéaire continue de M dans $CW_k(\mathcal{S}_k)$ telles que $(\xi,\eta) \in G(\mathcal{S})$. Pour achever la démonstration du lemme, il faut montrer qu'il existe un homomorphisme continu $x : \mathfrak{R} \to \mathcal{S}$ et un seul tel que $x_{\mathfrak{L}} = \xi$ et $x_M = \eta$.

D'après la proposition 6.2 du chapitre III, $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M, CW_k(\mathcal{S}_k))$ s'identifie à $G_k(\mathcal{S}_k)$: plus précisément, il existe un homomorphisme continu $x_k : R \to \mathcal{S}_k$ et un seul tel que $\eta(\underline{a}) = CW_k(x_k)(\underline{a})$, pour tout $\underline{a} \in M$.

Choisissons alors des X_i et des α_j comme dans le lemme 1.5 et cherchons quels sont les homomorphismes continus $x : \mathfrak{R} \to \mathcal{S}$ tels que $x_M = \eta$, ou, ce qui revient au même, qui relèvent x_k :

Si l'on note x_k^{et} la restriction de x_k à R^{et} , on voit que x_k^{et} se relève, de manière unique, en un homomorphisme continu $x^{et} : \mathfrak{R}^{et} \to \mathcal{S}$; si de plus, on pose $\tilde{x}_i = x_k(\tilde{X}_i) \in \mathcal{S}_k$, on voit que la restriction de x à $\mathfrak{R}^c$ est déterminée par le d-uple $(x_1, x_2, \dots, x_d)$, avec $x_i = x(X_i)$, et que les x_i peuvent être des élêments quelconques de $\mathcal{S}$ relevant les $\tilde{x}_i$. Comme $\mathfrak{R}$ s'identifie à $\mathfrak{R}^{et} \hat{\otimes}_A \mathfrak{R}^c$, on a ainsi obtenu une bijection entre les $x : \mathfrak{R} \to \mathcal{S}$ tels que $x_M = \eta$ et les d-uples $(x_1, \dots, x_d)$ d'éléments de $\mathcal{S}$ relevant les $\tilde{x}_i$.

Si maintenant x est un relèvement quelconque de x_k , on voit, d'après la première partie du lemme, que $(x_{\mathfrak{L}}, x_M) = (x_{\mathfrak{L}}, \eta) \in G(\mathcal{S})$ et on en déduit que le composé de $x_{\mathfrak{L}}$ avec la projection de $\mathcal{S}_K$ sur $\mathcal{S}_K/p\mathcal{S}$ est égal au composé de x avec cette projection ; on en déduit que, pour tout $\alpha \in \mathfrak{L}$, $x_{\mathfrak{L}}(\alpha) - \xi(\alpha) \in p\mathcal{S}$.

On voit donc que, pour achever la démonstration du lemme, il suffit d'établir le résultat suivant :

<u>soit</u> r <u>un entier</u> ≥ 1 . <u>Supposons qu'il existe un d-uple</u> $(x_1^0, x_2^0, \dots, x_d^0)$ <u>d'éléments de</u> $\mathcal{S}$ <u>relevant les</u> $\tilde{x}_i$, <u>uniquement déterminé modulo</u> p^r , <u>tel que</u> $x_{\mathfrak{L}}^0(\alpha) - \xi(\alpha) \in p^r\mathcal{S}$, <u>pour tout</u> $\alpha \in \mathfrak{L}$. <u>Il existe alors un d-uple</u> $(x_1, x_2, \dots, x_d)$ <u>d'éléments de</u> $\mathcal{S}$ <u>relevant les</u> x_i , <u>uniquement déterminé modulo</u> p^{r+1} , <u>tel que</u> $x_{\mathfrak{L}}(\alpha) - \xi(\alpha) \in p^{r+1}\mathcal{S}$, <u>pour tout</u> $\alpha \in \mathfrak{L}$ (on a noté x^0 (resp. x) le relèvement de x_k associé au d-uple $(x_1^0, \dots, x_d^0)$ (resp. $(x_1, \dots, x_d)$).

Pour le montrer, posons, pour $1 \leq i \leq d$, $x_L^0(\alpha_i) = \xi(\alpha_i) + p^r\gamma_i$, avec

$\gamma_i \in \mathfrak{S}$. On voit que, avec des notations évidentes,

$$x^0_{\mathfrak{L}}(\alpha_i) = \alpha^c_i(x^0_1,\dots,x^0_d) + x^{et}_{\mathfrak{L}}(\alpha^{et}_i) + px^0(\beta_i) .$$

Pour $1 \leq i \leq d$, posons $x_i = x^0_i + p^r y_i$, où les y_i sont des éléments quelconques de $\mathfrak{S}$. On a

$$x_{\mathfrak{L}}(\alpha_i) = \alpha^c_i(x_1,\dots,x_d) + x^{et}_{\mathfrak{L}}(\alpha^{et}_i) + px(\beta_i) .$$

Comme $x(X_j) \equiv x^0(X_j) \pmod{p^r\mathfrak{S}}$, pour tout j , on voit que $x(\beta_i) \equiv x^0(\beta_i)$ $(\mathrm{mod}\ p^r\mathfrak{S})$, pour tout i . On en déduit que

$$\begin{aligned} x_{\mathfrak{L}}(\alpha_i) &\equiv \alpha^c_i(x_1,\dots,x_d) + x^{et}_{\mathfrak{L}}(\alpha^{et}_i) + px^0(\beta_i) \\ &\equiv x^0_L(\alpha_i) + \alpha^c_i(x_1,\dots,x_d) - \alpha^c_i(x^0_1,\dots,x^0_d) \\ &\equiv \xi(\alpha_i) + p^r\gamma_i + \alpha^c_i(x_1,\dots,x_d) - \alpha^c_i(x^0_1,\dots,x^0_d) \pmod{p^{r+1}\mathfrak{S}} . \end{aligned}$$

Posons $\underline{x} = (x_1,\dots,x_d)$ et $\underline{x}^0 = (x^0_1,\dots,x^0_d)$. Pour tout $\underline{n} = (n_1,\dots,n_d) \in \mathbb{N}^d$, posons $|\underline{n}| = n_1 +\dots+ n_d$, $n! = n_1!\dots n_d!$, $\dfrac{\partial^{|\underline{n}|}}{\partial \underline{X}^{\underline{n}}} = \dfrac{\partial^{|\underline{n}|}}{\partial X_1^{n_1}\dots\partial X_d^{n_d}}$ et $\underline{y}^{\underline{n}} = y_1^{n_1}\dots y_d^{n_d}$. On a $\alpha^c_i(\underline{x}) - \alpha^c_i(\underline{x}^0) = \sum\limits_{n=1}^{\infty} p^{rn} \sum\limits_{|\underline{n}|=n} u_{\underline{n}}$, avec $u_{\underline{n}} = \dfrac{1}{\underline{n}!}\cdot\dfrac{\partial^{|\underline{n}|}\alpha^c_i}{\underline{X}^{\underline{n}}}(\underline{x}^0).\underline{y}^{\underline{n}}$.

Soit $\underline{n} \in \mathbb{N}^d$, avec $n = |\underline{n}| \geq 2$ et soit s un entier tel que $n_s \geq 1$, et $\underline{m} = (n_1,\dots,n_{s-1},n_s-1,n_{s+1},\dots,n_d)$. On a

$$u_{\underline{n}} = \frac{1}{\underline{n}!}\cdot\frac{\partial^{n-1}}{\partial\underline{X}^{\underline{m}}}\left(\frac{\partial\alpha^c_i}{\partial X_s}\right)(\underline{x}^0)\cdot\underline{y}^{\underline{n}} = \frac{1}{n_s}\cdot\frac{1}{\underline{m}!}\cdot\frac{\partial^{n-1}}{\partial\underline{X}^{\underline{m}}}\left(\frac{\partial\alpha^c_i}{\partial X_s}\right)(\underline{x}^0)\cdot\underline{y}^{\underline{n}} ,$$

donc $n_s u_{\underline{n}} \in \mathfrak{S}$.

Soit v_p la valuation p-adique. Si $rn - v_p(n_s) \geq r + 1$, on voit que $p^{rn}u_{\underline{n}} \in p^{r+1}\mathfrak{S}$. Or

- si $2 \leq n < p$, n_s est premier à p et $r_n - v_p(n_s) = rn \geq 2r \geq r+1$;
- si $p^t \leq n < p^{t+1}$, avec t entier ≥ 1 , on a $n_s \leq n < p^{t+1}$, donc $v_p(n_s) \leq t$ et $rn - v_p(n_s) \geq rp^t - t \geq r+1$, sauf si on a simultanément $r = 1$, $p = 2$ et $t = 1$;
- si $r = 1$, $p = 2$ et si $n = 2$ ou 3 , on voit que $n - v_2(n_s) \geq 2$, sauf si $\underline{n}$ est de la forme $(0,\dots,0,2,0,\dots,0)$.

Finalement, on voit que

$$\alpha_i^c(\underline{x}) - \alpha_i^c(\underline{x}^0) \equiv p^r \sum_{j=1}^{d} \frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0) y_j \quad (\mathrm{mod}\ p^{r+1}\mathfrak{s}) ,$$

sauf, peut-être, si $p = 2$ et $r = 1$, auquel cas on a

$$\alpha_i^c(\underline{x}) - \alpha_i^c(\underline{x}^0) \equiv 2\left(\sum_{j=1}^{d} \frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)\right)\cdot y_j + \sum_{j=1}^{d} \frac{\partial^2 \alpha_i^c}{\partial X_j^2}(\underline{x}^0)\cdot y_j^2 \quad (\mathrm{mod}\ 4\mathfrak{s}) .$$

Supposons d'abord $p \neq 2$ ou $p = 2$ et $r \geq 2$. On a alors, pour tout i,

$$x_L(\alpha_i) \equiv \xi(\alpha_i) + p^r\left(\gamma_i + \sum \frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)\cdot y_j\right) \quad (\mathrm{mod}\ p^{r+1}\mathfrak{s}) .$$

Les y_j doivent donc être solutions du système d'équations

$$\gamma_i + \sum \frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)\cdot y_j \equiv 0 \quad (\mathrm{mod}\ p\mathfrak{s}) .$$

Comme la matrice des $\frac{\partial \alpha_i^c}{\partial X_j}$ est inversible dans $\mathfrak{R}^c$, on voit que l'image, dans $\mathfrak{s}_k = \mathfrak{s}/p\mathfrak{s}$, de celle des $\frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)$ est inversible ; le système d'équations linéaires ci-dessus admet donc une solution et une seule modulo p, d'où le résultat.

Supposons enfin $p = 2$ et $r = 1$. Le même raisonnement montre que l'on doit résoudre le système d'équations

$$\gamma_i + \sum \frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)\cdot y_j + \sum \frac{\partial^2 \alpha_i^c}{\partial X_j^2}(\underline{x}^0)\cdot y_j^2 \equiv 0 \quad (\mathrm{mod}\ 2\mathfrak{s}) .$$

On voit que l'image, dans $\mathfrak{s}_k = \mathfrak{s}/2\mathfrak{s}$, de la matrice des $\frac{\partial \alpha_i^c}{\partial X_j}(\underline{x}^0)$ (resp. des $\frac{\partial^2 \alpha_i^c}{\partial X_j^2}(\underline{x}^0)$) est inversible (resp. nilpotente) et l'on en déduit facilement l'existence et l'unicité d'une solution modulo 2.

1.7. Nous allons maintenant indiquer comment on peut modifier les constructions des numéros précédents pour obtenir un analogue de la proposition 1.4 et une démonstration du théorème 1 pour les groupes connexes (pour p quelconque, bien qu'il suffirait, évidemment, de le faire pour $p = 2$).

Soit G un p-groupe formel connexe sur k (pas nécessairement lisse) qui est réunion de ses sous-groupes finis, soit R son algèbre affine et soit $\mathfrak{r}_R$ l'idéal maximal de R. Notons $R^{\#}$ le A-anneau profini $A \oplus \mathfrak{r}_R$ (la structure de A-module topologique est claire, le produit est défini par

$(\lambda.1+a)(\mu.1+b) = \lambda\mu.1 + (\lambda b+\mu a+ab)$, si $\lambda,\mu \in A$ et $a,b \in \mathfrak{r}_R$). On voit que $R^\# \otimes_A k = R^\#/pR^\#$ s'identifie à R et il est clair qu'il existe sur $R^\#$ une structure de bigèbre formelle et une seule telle que $\mathfrak{r}_R$ soit l'idéal d'augmentation de $R^\#$ et que la structure de bigèbre formelle induite sur R , par passage au quotient, soit celle provenant de G ; nous notons $G^\#$ le A-groupe formel dont l'algèbre affine est $R^\#$.

Soit S un A-anneau (muni de la topologie discrète) et soit $\mathfrak{r}_S$ son nilradical ; supposons que $p\mathfrak{r}_S = 0$. Notons S' le k-anneau $S' = k \oplus \mathfrak{r}_S$; on voit que le nilradical de S' s'identifie à $\mathfrak{r}_S$; si $x \in G^\#(S)$, x est une application continue de R dans S et envoie $\mathfrak{r}_R$ dans $\mathfrak{r}_S$; on en déduit que le groupe $G^\#(S)$ s'identifie au groupe $G(S')$. D'après la proposition 6.2 du chapitre III, le groupe $G(S')$ s'identifie au groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(S'))$ des applications D_k-linéaires continues de $M = \underline{M}(G)$ dans $CW_k(S')$. Si l'on note $CW_k(\mathfrak{r}_S)$ le sous-D_k-module fermé de $CW_k(S')$ formé des covecteurs dont toutes les composantes sont dans $\mathfrak{r}_S$, on voit que

$$CW_k(S') = CW_k(k) \oplus CW_k(\mathfrak{r}_S) .$$

Comme G est connexe, on a

$$\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(k)) \simeq G(k) = 0 \quad \text{et}$$

$$\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(S')) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(\mathfrak{r}_S)) .$$

D'où un isomorphisme canonique $u^\#_G(S)$ de $G^\#(S)$ sur $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(\mathfrak{r}_S))$: si $x \in G^\#(S)$, $u^\#_G(S)(x)$ est l'application qui à $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in M$ associe $(\ldots, x(a_{-n}), \ldots, x(a_0)) \in CW_k(\mathfrak{r}_S)$ (le fait que $\underline{a} \in M$ implique que tous les a_{-n} sont dans $\mathfrak{r}_R$).

Soit maintenant $\mathcal{S}$ un A-anneau p-adique et soit $\mathfrak{r}_{\mathcal{S}}$ l'idéal de $\mathcal{S}$ formé des x tels que $x^n \in p\mathcal{S}$, pour n suffisamment grand. Si l'on pose $S = \mathcal{S}/p\mathfrak{r}_{\mathcal{S}}$, S est un A-anneau dont le nilradical $\mathfrak{r}_S = \mathfrak{r}_{\mathcal{S}}/p\mathfrak{r}_{\mathcal{S}}$ vérifie $p\mathfrak{r}_S = 0$, et la topologie induite sur S par la topologie p-adique sur $\mathcal{S}$ est la topologie discrète.

Posons $\mathcal{S}_K = \mathcal{S} \otimes_A K$. Soit $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW_k(\mathfrak{r}_S)$; pour tout n , soit $\hat{a}_{-n}$ un relèvement de a_{-n} dans $\mathfrak{r}_{\mathcal{S}}$; on voit que la série $\sum_{n=0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n}$ converge dans $\mathcal{S}_K$ et que son image $w^\#_{\mathcal{S}}(\underline{a})$ dans $\mathcal{S}_K/p\mathfrak{r}_{\mathcal{S}}$ ne dépend pas du choix des relèvements des a_{-n} ; on voit facilement que l'application $w^{\#}_{\mathcal{S}} : CW_k(r_{\mathcal{S}}) \to \mathcal{S}_K/pr_{\mathcal{S}}$ ainsi définie est A-linéaire.

Soit $(\mathcal{L}, M, \rho)$ un objet de Λ^c_A. Soit $\mathcal{S}$ un A-anneau p-adique et soit $r_{\mathcal{S}} = \{x \in \mathcal{S} \mid x^n \in p\mathcal{S}$, pour n assez grand$\}$:

- comme au n° 1.3, nous notons $N_{\mathcal{L}}(\mathcal{S})$ le groupe $\mathrm{Hom}_A(\mathcal{L}, \mathcal{S}_K)$ des applications A-linéaires de $\mathcal{L}$ dans $\mathcal{S}_K = \mathcal{S} \otimes_A K$, et nous notons $N^{\#}_{\mathcal{L}}(\mathcal{S})$ le quotient $\mathrm{Hom}_A(\mathcal{L}, \mathcal{S}_K/pr_{\mathcal{S}})$;
- nous notons $G^{\#}_M(S)$ le groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(r_{\mathcal{S}}/pr_{\mathcal{S}}))$ des applications D_k-linéaires continues de M dans $CW_k(r_{\mathcal{S}}/pr_{\mathcal{S}})$;
- nous notons $\varphi^{\#}_{\rho}$ l'application de $G^{\#}_M(\mathcal{S})$ dans $N^{\#}_{\mathcal{L}}(\mathcal{S})$ qui à $u \in G^{\#}_M(\mathcal{S})$ associe $w^{\#}_{\mathcal{S}} \circ u \circ \rho$; il est clair que c'est un homomorphisme de groupes ;
- enfin, nous notons $G^{\#}_{(\mathcal{L},M,\rho)}(\mathcal{S})$ le produit fibré $N_{\mathcal{L}}(\mathcal{S}) \times_{N^{\#}_{\mathcal{L}}(\mathcal{S})} G^{\#}_M(\mathcal{S})$, où le morphisme de $N_{\mathcal{L}}(\mathcal{S})$ dans $N^{\#}_{\mathcal{L}}(\mathcal{S})$ est celui qui provient de la projection canonique de $\mathcal{S}_K$ sur $\mathcal{S}_K/pr_{\mathcal{S}}$ et celui de $G^{\#}_M(\mathcal{S})$ dans $N^{\#}_{\mathcal{L}}(\mathcal{S})$ est $\varphi^{\#}_{\rho}$.

Il est clair que toutes ces constructions sont fonctorielles en $\mathcal{S}$ et nous permettent de considérer $G^{\#}_{(\mathcal{L},M,\rho)}$ comme un foncteur covariant de la catégorie des A-anneaux p-adiques dans celle des groupes abéliens.

Choisissons maintenant un p-groupe formel lisse G_k dont le module de Dieudonné $M_0 = \underline{M}(G_k)$ est isomorphe à M (un tel groupe existe, est unique à isomorphisme près et est connexe) ainsi qu'un isomorphisme i de M sur M_0.

Soit R l'algèbre affine de G_k et choisissons un A-anneau spécial $\mathcal{R}$ qui relève R, ainsi qu'une augmentation ε, i.e. un homomorphisme continu du A-anneau profini $\mathcal{R}$ sur A, et notons $\mathcal{R}^{\varepsilon}$ le noyau de ε.

Le D_k-module topologique $CW^c_k(R)$ est formé des covecteurs dont les composantes sont toutes dans l'idéal maximal r_R de R. Si $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW^c_k(R)$ et si l'on choisit des relèvements $\hat{a}_{-n}$ des a_{-n} dans $\mathcal{R}^{\varepsilon}$ (et pas seulement dans $\mathcal{R}$), on voit que l'image $w^{\varepsilon}_{\mathcal{R}}(\underline{a})$ de $\sum_{n=0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n}$ dans $P(\mathcal{R})/pr_{\mathcal{R}}$ (où $r_{\mathcal{R}}$ est l'idéal maximal de $\mathcal{R}$) ne dépend pas du choix de ces relèvements ; on vérifie encore que l'application

$$w^{\varepsilon}_{\mathcal{R}} : CW^c_k(\mathcal{R}) \longrightarrow P(\mathcal{R})/pr_{\mathcal{R}}$$

ainsi définie est A-linéaire continue.

Choisissons enfin un isomorphisme ι de $\mathcal{L}$ sur un sous-A-module $\mathcal{L}_0$ de $P(\mathfrak{R})$ tel que le diagramme

$$\begin{tikzcd}
\mathcal{L} \arrow[r, "\iota"] \arrow[d, "\rho"'] & \mathcal{L}_0 \arrow[r, hook] & P(\mathfrak{R}) \arrow[dr] & \\
 & & & P(\mathfrak{R})/p\mathbf{r}_{\mathfrak{R}} \\
M \arrow[r, "i"] & M_0 \arrow[r, hook] & CW_k^c(R) \arrow[ur, "w^{\epsilon}_{\mathfrak{R}}"'] &
\end{tikzcd}$$

soit commutatif (l'existence d'un tel ι est claire).

Pour tout A-anneau p-adique $\mathfrak{S}$ notons, comme en 1.3, $X_{\mathfrak{R}}(\mathfrak{S})$ l'ensemble des homomorphismes continus du A-anneau $\mathfrak{R}$ dans $\mathfrak{S}$. A $x \in X_{\mathfrak{R}}(\mathfrak{S})$ on associe, comme en 1.3, un élément $x_{\mathcal{L}}$ de $N_{\mathcal{L}}(\mathfrak{S})$. On lui associe aussi un élément x^{ϵ}_{M} de $G^{\#}_{M}(\mathfrak{S})$ de la manière suivante :

le A-anneau profini $\mathfrak{R}/p\mathfrak{R}^{\epsilon}$ s'identifie à $R^{\#}$; on a $x(\mathfrak{R}^{\epsilon}) \subset x(\mathbf{r}_{\mathfrak{R}}) \subset \mathbf{r}_{\mathfrak{S}}$ et x définit, par passage aux quotients, un homomorphisme continu $x^{\epsilon}_{k} : R^{\#} \to \mathfrak{S}/p\mathbf{r}_{\mathfrak{S}}$; il lui correspond donc un élément $x^{\epsilon}_{M_0} = u^{\#}_{G}(\mathfrak{S}/p\mathbf{r}_{\mathfrak{S}})(x^{\epsilon}_{k})$ de $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M_0, CW_k(\mathbf{r}_{\mathfrak{S}}/p\mathbf{r}_{\mathfrak{S}}))$ et $x^{\epsilon}_{M} = x^{\epsilon}_{M_0} \circ i$.

LEMME 1.3'.- <u>Pour tout</u> $x \in X_{\mathfrak{R}}(\mathfrak{S})$, $(x_{\mathcal{L}}, x^{\epsilon}_{M}) \in G^{\#}_{(\mathcal{L},M,\rho)}(\mathfrak{S})$. <u>L'application</u> $x \mapsto (x_{\mathcal{L}}, x^{\epsilon}_{M})$ <u>de</u> $X_{\mathfrak{R}}(\mathfrak{S})$ <u>dans</u> $G^{\#}_{(\mathcal{L},M,\rho)}(\mathfrak{S})$ <u>est bijective</u>.

La démonstration est entièrement analogue à celle du lemme 1.3. Avec les conventions employées dans la démonstration de ce lemme, on voit que le seul problème est pour $p = 2$ et $r = 1$ où l'on est ramené à résoudre un système d'équations du type

$$\gamma_i + \sum \frac{\partial \alpha^c_i}{\partial X_j}(\underline{x}^0)\cdot y_j + \sum \frac{\partial^2 \alpha^c_i}{\partial X^2_j}(\underline{x}^0)\cdot y^2_j \equiv 0 \quad (\mathrm{mod}\ 2\mathfrak{S})$$

dont on veut montrer qu'il admet une solution $(y_1, y_2, \dots, y_d)$ formée d'éléments de $\mathbf{r}_{\mathfrak{S}}$ et que cette solution est unique modulo $2\mathfrak{S}$; on sait encore que l'image, dans $\mathfrak{S}/2\mathfrak{S}$, de la matrice des $\frac{\partial \alpha^c_i}{\partial X_j}(\underline{x}^0)$ est inversible ; il n'est plus toujours vrai que l'image de celle des $\frac{\partial^2 \alpha^c_i}{\partial X^2_j}(\underline{x}^0)$ est nilpotente, mais on sait que les γ_i sont dans $\mathbf{r}_{\mathfrak{S}}$; l'existence et l'unicité s'en déduisent facilement.

Soit alors G un p-groupe formel lisse et connexe, de dimension finie sur A, et soit $\mathcal{L}M_A(G) = (\mathcal{L}, M, \rho)$. Il est clair que le lemme précédent s'applique en prenant $G_k = G \otimes_A k$, $M_0 = M$, $i = \mathrm{id}_M$, $\mathfrak{R}$ = l'algèbre affine de G , ε = l'augmentation provenant de G , $\mathfrak{L}_0 = \mathfrak{L}$ et $\iota = \mathrm{id}_{\mathfrak{L}}$.

PROPOSITION 1.4'.- Soit G un p-groupe formel lisse et connexe, de dimension finie sur A , soit $\mathfrak{R}$ son algèbre affine et soit $(\mathfrak{L}, M, \rho) = \mathfrak{L}M_A(G)$. Soit $\mathfrak{S}$ un A-anneau p-adique. Pour tout $x \in G(\mathfrak{S}) = \mathrm{Hom}_{\mathrm{cont}}(\mathfrak{R}, \mathfrak{S})$, $(x_{\mathfrak{L}}, x_M^{\varepsilon}) \in G^{\#}_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$ et l'application $x \to (x_{\mathfrak{L}}, x_M^{\varepsilon})$ est un isomorphisme du groupe $G(\mathfrak{S})$ sur $G^{\#}_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$.

La démonstration de cette proposition est entièrement analogue à celle de la proposition 1.4. Le théorème 1 dans le cas connexe se déduit du lemme 1.3' et de la proposition 1.4' de la même manière qu'il se déduit, dans le cas $p \neq 2$, du lemme 1.3 et de la proposition 1.4.

1.8. Le théorème 1 implique le résultat suivant, d'ailleurs bien connu :

COROLLAIRE.- Tout groupe formel lisse et de dimension finie sur k admet un relèvement lisse sur A .

Soit, en effet, G un tel groupe formel. Il s'écrit sous la forme $G = G^c \times G^{et}$, avec G^c connexe et G^{et} étale ; comme il est clair que G^{et} se relève, il suffit de vérifier que G^c se relève. Soit d sa dimension et soit M son module de Dieudonné ; soit $\underline{a}_1, \underline{a}_2, \dots, \underline{a}_d$ des éléments de M qui relèvent une base de $M/\underline{F}M$ sur k ; soit $e_1, e_2, \dots, e_d$ la base canonique du A-module libre A^d et soit ρ l'application A-linéaire de A^d dans M définie par $\rho(e_i) = \underline{a}_i$, pour $1 \leq i \leq d$. On voit que (A^d, M, ρ) est un objet de Λ_A^c qui définit un groupe formel lisse sur A relevant G^c .

1.9. Remarque : soit G un p-groupe formel lisse et de dimension finie sur A. Si $p = 2$, supposons G connexe ou unipotent. Soit $(\mathfrak{L}, M, \rho) = \mathfrak{L}M(G)$. On peut décrire le groupe $G(S)$ des points de G à valeurs dans n'importe quel A-anneau fini S à l'aide du triplet $(\mathfrak{L}, M, \rho)$. En effet, on vérifie facilement que l'on peut trouver un A-anneau p-adique $\mathfrak{S}$ (qui est un A-module libre de rang fini) et un homomorphisme de $\mathfrak{S}$ sur S . Soit $\mathfrak{a}$ le noyau de cet homomorphisme. Comme G est lisse, l'homomorphisme de $G(\mathfrak{S})$ dans $G(S)$ est surjectif et il suffit donc de savoir décrire son noyau. Si $\mathfrak{R}$ est l'algèbre affine de G et si $\mathfrak{R}^+$ est l'idéal d'augmentation, on voit que ce noyau est le sous-groupe $G(\mathfrak{a})$ de $G(\mathfrak{S})$ formé des $x : \mathfrak{R} \to \mathfrak{S}$ tels que $x(\mathfrak{R}^+) \subset \mathfrak{a}$. Le

A-module libre de rang fini $A \oplus \mathfrak{a}$ peut être muni d'une manière évidente d'une structure de A-anneau p-adique telle que la projection sur la première composante soit un homomorphisme d'anneaux. On voit que $G(\mathfrak{a})$ s'identifie au noyau de la projection de $G(A \oplus \mathfrak{a})$ sur $G(A)$.

1.10. Appelons <u>système de Honda lisse sur</u> A tout couple (L, M)

- où M est un D_k-module profini sur lequel l'action de $\underline{F}$ est injective, tel que le quotient $M/\underline{F}M$ est un espace vectoriel de dimension finie sur k ,
- où L est un sous-A-module de M vérifiant $\underline{F}M \cap L = pL$ et $L/pL = M/\underline{F}M$.

Les systèmes de Honda lisses sur A forment une catégorie H_A^ℓ : un morphisme $u : (L,M) \to (L',M')$ est une application D_k-linéaire continue de M dans M' telle que $u(L) \subset L'$.

Il est clair que la catégorie H_A^ℓ est additive.

Il existe un foncteur additif évident $H : \Lambda_A^\ell \to H_A^\ell$: à un triplet $(\mathfrak{L}, M, \rho)$ on associe le couple (L, M) où $L = \rho(\mathfrak{L})$. On voit que H n'est pas pleinement fidèle. Cependant, on vérifie immédiatement :

- que H est essentiellement surjectif ;
- que deux objets de Λ_A^ℓ sont isomorphes si et seulement si leurs images par H sont isomorphes dans H_A^ℓ .

Si l'on note LM_A le foncteur $H \circ \mathfrak{L}M_A$, on voit donc que tout p-groupe formel G lisse et de dimension finie sur A est déterminé, à isomorphisme près, par $LM_A(G)$.

En particulier, soit G_k un p-groupe formel, lisse et de dimension finie sur k ; si $p = 2$ supposons G_k connexe ou unipotent. On voit que déterminer les classes d'isomorphismes des relèvements lisses de G_k sur A revient à déterminer les classes d'isomorphisme des couples (L, M) de H_A^ℓ où $M = \underline{M}(G_k)$. Le groupe $\mathrm{Aut}(M)$ des automorphismes continus du D_k-module topologique M (qui est isomorphe au groupe des automorphismes de G_k) opère à gauche sur l'ensemble $\Lambda(M)$ des sous-A-modules L de M vérifiant $\underline{F}M \cap L = pL$ et $L/pL = M/\underline{F}M$; les classes d'isomorphismes des relèvements lisses de G_k correspondent alors aux classes de $\Lambda(M)$ suivant $\mathrm{Aut}(M)$.

Remarque 1 : nous verrons au § 2 du chapitre V que la classification des p-groupes formels lisses et de dimension finie sur A par leurs systèmes de Honda n'est autre, dans le cas connexe, que celle qui avait été obtenue par Honda ([32], au langage près et par des méthodes complètement différentes, la théorie de Honda ne donne pas de description de $G(\mathfrak{S})$, elle consiste à construire explicitement la loi de groupe formel). C'est pourquoi nous avons employé l'expression de "système de Honda", bien que des objets du même type aient été aussi considérés par Grothendieck ([29]).

Soit maintenant G un groupe p-divisible sur A . Il est clair qu'il revient au même de dire que G est un p-groupe formel, lisse et de dimension finie sur A , tel que G_k est un groupe p-divisible sur k . Par conséquent (cf. rem. 3 du n° III.6.1), un p-groupe formel G , lisse et de dimension finie sur A , est un groupe p-divisible si et seulement si $\underline{M}(G_k)$ est un A-module libre de rang fini.

Notons alors Λ_A^d (resp. H_A^d) la sous-catégorie pleine de Λ_A^ℓ (resp. H_A^ℓ) dont les objets sont les $(\mathcal{L}, M, \rho)$ (resp. les (L, M)) tels que M est un A-module libre de rang fini. Si $(\mathcal{L}, M, \rho)$ est un objet de Λ_A^d , on voit que $\rho : \mathcal{L} \to M$ est injective et on en déduit que la restriction du foncteur H à Λ_A^d définit une équivalence entre la catégorie Λ_A^d et H_A^d .

Si l'on note $H_A^{d,c}$ (resp. $H_A^{d,u}$) la sous-catégorie pleine de H_A^d dont les objets sont les couples (L, M) tels que M est connexe (resp. unipotent), le théorème 1 implique alors le résultat suivant :

PROPOSITION 1.6.- Si $p \neq 2$, le foncteur LM_A induit une anti-équivalence entre la catégorie des groupes p-divisibles sur A et la catégorie H_A^d .

Pour p quelconque, le foncteur LM_A induit une anti-équivalence entre la catégorie des groupes p-divisibles connexes (resp. unipotents) sur A et la catégorie $H_A^{d,c}$ (resp. $H_A^{d,u}$) .

On obtient ainsi les résultats annoncés dans [21]. Profitons-en pour signaler que le théorème 2' de [21] n'est énoncé correctement que pour $p \neq 2$. L'énoncé correct dans le cas général est la proposition 1.6 ci-dessus.

Remarque 2 : soit G un groupe p-divisible sur A et soit, pour tout entier

n , G_n le sous-groupe de G noyau de la multiplication par p^n . Soit $\mathcal{S}$ un A-anneau p-adique. Dans la proposition 1.4, nous avons noté $G(\mathcal{S})$ le groupe des homomorphismes continus de l'algèbre affine de G dans $\mathcal{S}$, i.e. le groupe des points de G , considéré comme groupe formel, à valeurs dans $\mathcal{S}$. Ce groupe ne doit pas être confondu avec le groupe des points de G , considéré comme limite inductive de groupes finis, à valeurs dans $\mathcal{S}$, autrement dit avec le groupe $\varinjlim G_n(\mathcal{S})$. Il est clair que ce dernier s'identifie au sous-groupe de torsion $G_{tor}(\mathcal{S})$ de $G(\mathcal{S})$.

Avec des notations évidentes, si $(L,M) = LM_A(G)$, le groupe $G(\mathcal{S})$ s'identifie canoniquement (en supposant G unipotent si $p = 2$) au groupe $N_L(\mathcal{S}) \times_{N_L^0(\mathcal{S})} G_M(\mathcal{S})$ (cf. prop. 1.4). Comme $N_L(\mathcal{S})$ est sans torsion et comme $G_M(\mathcal{S})$ est un groupe de torsion, on voit que $G_{tor}(\mathcal{S})$ s'identifie au sous-groupe de $G_M(\mathcal{S})$ formé des $u : M \to CW_k(S_k)$ tels que $(w_{\mathcal{S}} \circ u)(L) = 0$. On obtient une description analogue, dans le cas $p = 2$ et G connexe, en utilisant la proposition 1.4'.

Remarque 3 : soit G un groupe p-divisible sur A ; si $p = 2$, supposons G unipotent. On vient de voir que, si $\mathcal{S}$ est un A-anneau qui est un A-module libre de rang fini, le groupe $G_{tor}(\mathcal{S})$ s'identifie à un sous-groupe de $G_M(\mathcal{S}) = \mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$. On voit que la flèche $G_{tor}(\mathcal{S}) \to G_M(\mathcal{S})$ n'est autre que la composée de l'homomorphisme canonique de $G_{tor}(\mathcal{S}) \subset G(\mathcal{S})$ dans $G(\mathcal{S}/p\mathcal{S}) = G(\mathcal{S}_k) = G_k(\mathcal{S}_k)$ par l'isomorphisme canonique de $G_k(\mathcal{S}_k)$ sur $\mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$. On en déduit donc que l'homomorphisme canonique de $G_{tor}(\mathcal{S})$ dans $G_k(\mathcal{S}_k)$ est injectif. Ce résultat avait été annoncé dans [21] (th. 3) et peut d'ailleurs se démontrer directement.

§ 2.- Le foncteur $M \to M_{A'}$.

Dans ce paragraphe et dans les suivants, on note K' une extension finie totalement ramifiée de K et e son degré. On note A' l'anneau des entiers de K' , $\mathfrak{m}$ l'idéal maximal de A' et on désigne par π une uniformisante de A' .

On note $\nu(e)$ l'entier $\min_{n \in \mathbb{N}} \{p^n - ne\}$ et $s(e)$ le plus petit entier s tel que $\nu(e) = p^s - se$. On écrit ν et s au lieu de $\nu(e)$ et $s(e)$ lorsqu'il n'y a pas de confusion possible. Remarquons que, si $e \leq p-1$, on a $\nu(e) = 1$ et $s(e) = 0$.

2.1. Pour tout D_k-module M, et pour tout entier j, nous notons $M^{(j)}$ le D_k-module déduit de M par l'extension des scalaires σ^j (rappelons que σ désigne le Frobenius absolu sur k et A ; on le prolonge en un automorphisme de D_k en posant $\sigma(\underline{F}) = \underline{F}$ et $\sigma(\underline{V}) = \underline{V}$). Dans la suite, nous identifions le $\mathbb{Z}_p[\underline{F},\underline{V}]$-module sous-jacent à $M^{(j)}$ au $\mathbb{Z}_p[\underline{F},\underline{V}]$-module sous-jacent à M ; l'action d'un $\lambda \in A$ sur $M^{(j)}$ est alors la flèche $\underline{a} \mapsto \sigma^{-j}(\lambda)\underline{a}$.

Pour tout D_k-module M et pour tout entier j, on note v (resp. f) l'application D_k-linéaire de $M^{(j)}$ dans $M^{(j+1)}$ (resp. dans $M^{(j-1)}$) qui à $\underline{a} \in M^{(j)}$ (identifié à M) associe $\underline{V}\underline{a}$ (resp. $\underline{F}\underline{a}$) .

Il est clair que, si M est un D_k-module topologique, $M^{(j)}$ est, de manière naturelle, un D_k-module topologique et que les applications v et f sont continues.

Considérons le cas particulier où l'on se donne un k-anneau linéairement topologisé, séparé et complet, R et où $M = CW_k(R)$. On pose alors $CW_k^{(j)}(R) = M^{(j)}$. Il est commode de considérer les éléments de $CW_k^{(j)}(R)$ comme des covecteurs $(\ldots,a_{-n},\ldots,a_{-j-1},a_{-j})$ dont les composantes (qui sont des éléments de R vérifiant les conditions habituelles) sont indexées par les entiers $\leq -j$: avec ces conventions, les formules donnant l'addition et la multiplication par un scalaire sont les mêmes que celles qui nous ont servies à définir le D_k-module $CW_k(R)$. L'application $v : CW_k^{(j)}(R) \to CW_k^{(j+1)}(R)$ (resp. $f : CW_k^{(j)}(R) \to CW_k^{(j-1)}(R)$) associe à $(\ldots,a_{-n},\ldots,a_{-j-1},a_{-j})$ l'élément $(\ldots,a_{-n},\ldots,a_{-j-1})$ (resp. $(\ldots,a^p_{-n},\ldots,a^p_{-j-1},a^p_{-j})$) .

On voit que v est surjective et que f est injective si et seulement si R est réduit.

2.2. Nous allons associer à tout D_k-module M un A'-module $M_{A'}$:

- pour tout $(i,j) \in \mathbb{Z}\times\mathbb{Z}$, notons $M_i^{(j)}$ le A'-module $\mathfrak{m}^i \otimes_A M^{(j)}$;
- pour tout $(i,j) \in \mathbb{Z}\times\mathbb{Z}$, notons $\varphi_{i,j} : M_i^{(j)} \to M_{i-1}^{(j)}$ l'application A'-linéaire déduite, par extension des scalaires, de l'inclusion $\mathfrak{m}^i \to \mathfrak{m}^{i-1}$;

- pour tout $(i,j) \in \mathbb{Z}\times\mathbb{Z}$, notons $f_{i,j} : M_i^{(j)} \to M_i^{(j-1)}$ l'application A'-linéaire, déduite, par extension des scalaires, de l'application $f : M^{(j)} \to M^{(j-1)}$;
- enfin, pour tout $(i,j) \in \mathbb{Z}\times\mathbb{Z}$, notons $v_{i,j} : M_i^{(j)} \to M_{i-e}^{(j+1)}$ l'application A'-linéaire qui, à $\lambda \otimes \underline{a} \in \mathfrak{m}^i \otimes_A M^{(j)}$, associe $p^{-1}\lambda \otimes v(\underline{a})$.

Pour tout sous-ensemble I de $\mathbb{Z}\times\mathbb{Z}$, nous notons $\mathcal{D}_I(M)$ le diagramme (dans la catégorie des A'-modules) dont les objets sont les $M_i^{(j)}$ avec $(i,j) \in I$ et les flèches les $\varphi_{i,j}$, $f_{i,j}$ et $v_{i,j}$ dont la source et le but sont des objets de $\mathcal{D}_I(M)$. Il est clair que ce diagramme est commutatif.

Soit I_e l'ensemble des $(i,j) \in \mathbb{Z}\times\mathbb{Z}$ vérifiant $j \geq 0$ et

$$\begin{cases} i \geq 0 & \text{si } j = 0\,, \\ i \geq p^{j-1} - je & \text{si } j \geq 1\,. \end{cases}$$

On pose alors $M_{A'} = \varinjlim \mathcal{D}_{I_e}(M)$.

Lorsque M est un D_k-module topologique, les $M_i^{(j)}$ ont une structure naturelle de A'-modules topologiques et les applications $\varphi_{i,j}$, $f_{i,j}$ et $v_{i,j}$ sont continues. On peut donc considérer $M_{A'}$ comme un A'-module topologique.

On vérifie facilement que, si I'_e est l'ensemble des $(i,j) \in I_e$ tels que $i \leq 1$, on a encore $M_{A'} = \varinjlim \mathcal{D}_{I'_e}(M)$. Comme I'_e est un ensemble fini, on voit que, si M est un D_k-module A-pro-artinien (resp. A-profini), $M_{A'}$ est un A'-module pro-artinien (resp. profini).

Il est clair que la correspondance $M \mapsto M_{A'}$ est fonctorielle : si M et N sont des D_k-modules (topologiques) et si $u : M \to N$ est une application D_k-linéaire (continue), nous notons $u_{A'} : M_{A'} \to N_{A'}$ l'application A'-linéaire (continue) induite par u.

<u>Remarques</u> : soit M un D_k-module.

1.- Posons $M_0 = A' \otimes_A M = M_0^{(0)}$ et, pour $1 \leq j \leq s+1$, $M_j = p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j)} = M^{(j)}_{p^{j-1}-je}$. On voit que, étant donné un objet quelconque du diagramme $\mathcal{D}_{I_e}(M)$, il existe un chemin partant de cet objet et allant vers l'un des M_j. On en déduit que l'application canonique de $\bigoplus_{j=0}^{s+1} M_j$ dans $M_{A'}$ est surjective.

2.- Posons en outre, pour $0 \leq j \leq s$, $M'_j = p^{-j}\mathfrak{m}^{p^j} \otimes_A M^{(j)} = M^{(j)}_{p^j-je}$ et

$M''_{j+1} = p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j+1)} = M^{(j+1)}_{p^{j-1}-je}$ (avec la convention que $\mathfrak{m}^{p^{-1}} = A'$). En "éliminant toutes les flèches inutiles", on voit facilement que $M_{A'}$ s'identifie à la limite inductive du diagramme

$$\begin{tikzcd}[column sep=small]
 & M'_0 \arrow[dl, "\varphi_0"'] \arrow[dr, "v_0"] & & {} \arrow[dl] \arrow[dr] & & M'_j \arrow[dl, "\varphi_j"'] \arrow[dr, "v_j"] & & {} \arrow[dl] \arrow[dr] & & M'_s \arrow[dl, "\varphi_s"'] \arrow[dr, "v_s"] & \\
M_0 & & M_1 & \cdots & M_j & & M_{j+1} & \cdots & M_s & & M_{s+1} \\
 & M''_1 \arrow[ul] \arrow[ur, "\varphi'_0"'] & & {} \arrow[ul] \arrow[ur] & & M''_{j+1} \arrow[ul, "f_j"] \arrow[ur, "\varphi'_j"'] & & {} \arrow[ul] \arrow[ur] & & M''_{s+1} \arrow[ul, "f_s"] \arrow[ur, "\varphi'_s"'] &
\end{tikzcd}$$

où toutes les flèches sont évidentes.

En particulier, si $2 \leq e \leq p-1$, $M_{A'}$ est la limite inductive du diagramme

$$\begin{tikzcd}
 & M'_0 \arrow[dl, "\varphi_0"'] \arrow[dr, "v_0"] & \\
M_0 & & M_1 \\
 & M''_1 \arrow[ul, "f_0"] \arrow[ur, "\varphi'_0"'] &
\end{tikzcd} .$$

2.3. Pour tout D_k-module M , regardons comment le A'-module $M_{A'}$ est relié au K'-espace vectoriel $M_{K'} = K' \otimes_A M = K' \otimes_{A'} (A' \otimes_A M)$:

PROPOSITION 2.1.- <u>Soit M un D_k-module. Posons</u> $M_{K'} = K' \otimes_A M = K' \otimes_{A'} (A' \otimes_A M)$. <u>La flèche canonique de</u> $A' \otimes_A M = M_0^{(0)}$ <u>dans</u> $M_{A'}$ <u>induit, par extension des scalaires, un isomorphisme de</u> $M_{K'}$ <u>sur</u> $K' \otimes_{A'} M_{A'}$.

<u>Démonstration</u> : pour tout $(i,j) \in \mathbb{Z} \times \mathbb{Z}$, l'inclusion de $\mathfrak{m}^i$ dans K' et l'application $f^j : M^{(j)} \to M$ induisent, par passage au produit tensoriel, une application A'-linéaire de $M_i^{(j)} = \mathfrak{m}^i \otimes_A M^{(j)}$ dans $M_{K'}$; d'où, par extension des scalaires, une application K'-linéaire $\rho_{i,j} : K' \otimes_{A'} M_i^{(j)}$ dans $M_{K'}$. En utilisant le fait que le noyau de f^j est contenu dans le noyau de la multiplication par p^j et le fait que l'image de f^j contient p^jM , on voit que chaque $\rho_{i,j}$ est un isomorphisme. On voit que les $\rho_{i,j}$ sont compatibles avec les flèches du diagramme $\mathcal{D}_{I_e}(M)$. On peut donc passer à la limite inductive et on obtient encore un isomorphisme.

<u>Remarque</u> : soit M un D_k-module qui est un A-module libre de rang fini h .

Alors $M_{K'}$ est un espace vectoriel de dimension h sur K' et il résulte de la proposition précédente que $M_{A'}/(M_{A'})_{tor}$ s'identifie à un réseau (i.e. un sous-A'-module libre de rang h) de $M_{K'}$; il est clair que l'application $f^j : M^{(j)} \to M$ est injective et que son image est le sous-D_k-module $\underline{F}^j M$ de M . Si l'on utilise la platitude pour identifier les $\mathfrak{m}^i \otimes_A \underline{F}^j M$ à des réseaux de $M_{K'}$, on voit que l'image de $M_{A'}$ dans $M_{K'}$ est

$$(A' \otimes_A M) + \sum_{j=1}^{\infty} p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A \underline{F}^j M = (A' \otimes_A M) + \sum_{j=1}^{s+1} p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A \underline{F}^j M .$$

Si $e \leq p-1$, on montre facilement que $M_{A'}$ n'a pas de torsion et s'identifie donc au réseau $A' \otimes_A M + p^{-1}\mathfrak{m} \otimes_A \underline{F} M$. Si $e > p-1$, en revanche, $(M_{A'})_{tor}$ est un A'-module de longueur finie, non nul en général.

2.4. Pour tout entier j vérifiant $0 \leq j \leq s+1$, soit $I'_{e,j}$ l'ensemble des $(i,j') \in I'_e$ tels que $j' \geq j$. Pour tout D_k-module M , on note $M_{A'}[j]$ la limite inductive du diagramme $\mathcal{D}_{I'_{e,j}}(M)$. On a donc $M_{A'}[0] = M_{A'}$ et on voit que $M_{A'}[s+1]$ s'identifie à $M_{s+1} = p^{-s-1}\mathfrak{m}^{p^s} \otimes_A M^{(s+1)}$.

PROPOSITION 2.2.- <u>Soit</u> M <u>un</u> D_k-<u>module sans</u> F-<u>torsion. Pour tout entier</u> j <u>vérifiant</u> $0 \leq j \leq s$, <u>l'application canonique de</u> $M_{A'}[j+1]$ <u>dans</u> $M_{A'}$ <u>est injective</u>.

<u>Démonstration</u> : il est clair qu'il suffit de montrer que, pour tout j , l'application canonique de $M_{A'}[j+1]$ dans $M_{A'}[j]$ est injective. En utilisant les notations des remarques 1 et 2 du n° 2.2, on voit que $M_{A'}[j]$ est la limite inductive du diagramme

$$\begin{tikzcd} & M'_j \arrow[dl, "\varphi_j"'] \arrow[dr, "v_j"] & & \\ M_j & & M_{j+1} \arrow[r, "\text{can.}"] & M_{A'}[j+1] . \\ & M''_{j+1} \arrow[ul, "f_j"] \arrow[ur, "\varphi'_j"'] & & \end{tikzcd}$$

On voit qu'il suffit de montrer que l'application canonique de M_{j+1} dans la limite inductive du diagramme

$$\begin{tikzcd} & M'_j \arrow[dl, "\varphi_j"'] \arrow[dr, "v_j"] & \\ M_j & & M_{j+1} \\ & M''_{j+1} \arrow[ul, "f_j"] \arrow[ur, "\varphi'_j"'] & \end{tikzcd}$$

est injective.

Soit $N = p^{-j-1}\mathfrak{m}^{p^j} \otimes_A M^{(j)}$; soit $\tilde{\varphi}$ l'application de M_j dans N déduite par extension des scalaires de l'inclusion de $p^{-j}\mathfrak{m}^{p^{j-1}}$ dans $p^{-j-1}\mathfrak{m}^{p^j}$ et soit $\tilde{f}$ l'application de M_{j+1} dans N déduite par extension des scalaires de $f : M^{(j+1)} \to M^{(j)}$. Il est clair que le diagramme

$$\begin{tikzcd}
 & M'_j \arrow[dl, "\varphi_j"'] \arrow[dr, "v_j"] & \\
M_j \arrow[ddr, bend right, "\tilde{\varphi}"'] & & M_{j+1} \arrow[ddl, bend left, "\tilde{f}"] \\
 & M''_{j+1} \arrow[ul, "\varphi_j"] \arrow[ur, "\varphi'_j"'] & \\
 & N &
\end{tikzcd}$$

est commutatif. Comme M est sans $\underline{F}$-torsion, l'application f est injective. Comme $p^{-j-1}\mathfrak{m}^{p^j}$ est un A-module plat, l'application $\tilde{f}$ est encore injective et l'assertion en résulte facilement.

2.5. Conservons les notations qui précèdent. La proposition précédente permet, lorsque M est un D_k-module sans $\underline{F}$-torsion, d'identifier les $M_{A'}[j]$ à des sous-A'-modules de $M_{A'}$; on obtient ainsi une suite décroissante

$$M_{A'} = M_{A'}[0] \supset \ldots \supset M_{A'}[j] \supset M_{A'}[j+1] \supset \ldots \supset M_{A'}[s+1] = M_{s+1} .$$

PROPOSITION 2.3.- <u>Soit</u> M <u>un</u> D_k<u>-module sans</u> $\underline{F}$<u>-torsion. Pour</u> $0 \leq j \leq s$, <u>le</u> A'<u>-module</u> $M_{A'}[j]/M_{A'}[j+1]$ <u>est isomorphe, canoniquement et fonctoriellement en</u> M , <u>à</u> $(\mathfrak{m}^{p^{j-1}}/\mathfrak{m}^{p^j}) \otimes_A (M/\underline{F}M)^{(j)}$ (<u>en convenant que</u> $\mathfrak{m}^{p^{-1}} = A'$).

<u>Démonstration</u> : Comme $M_{A'}[j]$ est la limite inductive du diagramme

$$\begin{tikzcd}
 & M'_j \arrow[dl, "\varphi_j"'] \arrow[dr, "v_j"] & & \\
M_j & & M_{j+1} \arrow[r, "\text{can.}"] & M_{A'}[j+1] \\
 & M''_{j+1} \arrow[ul, "f_j"] \arrow[ur, "\varphi'_j"'] & &
\end{tikzcd} ,$$

on voit que la composée de l'application canonique de M_j dans $M_{A'}[j]$ avec la projection de $M_{A'}[j]$ sur $M_{A'}[j]/M_{A'}[j+1]$ est surjective et que son noyau est $\operatorname{Im}\varphi_j + \operatorname{Im} f_j$. D'où un isomorphisme canonique de $M_j/(\operatorname{Im}\varphi_j + \operatorname{Im} f_j)$ sur $M_{A'}[j]/M_{A'}[j+1]$. Or la multiplication par p^{-j} définit un isomorphisme canonique de $\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j)}$ sur $M_j = p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j)}$. On voit que l'image réciproque, par cet isomorphisme, de $\operatorname{Im}\varphi_j$ (resp. $\operatorname{Im} f_j$) est, avec des notations évidentes, $\mathrm{Im}\, \mathfrak{m}^{p^j} \otimes_A M^{(j)}$ (resp. $\mathrm{Im}\, \mathfrak{m}^{p^{j-1}} \otimes_A \underline{F}M^{(j)}$) . Il est clair que le noyau de la projection de $\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j)}$ sur $(\mathfrak{m}^{p^{j-1}}/\mathfrak{m}^{p^j}) \otimes_A (M^{(j)}/\underline{F}M^{(j)})$ est $\mathrm{Im}\, \mathfrak{m}^{p^j} \otimes_A M^{(j)} + \mathrm{Im}\, \mathfrak{m}^{p^{j-1}} \otimes_A \underline{F}M^{(j)}$ et que $M^{(j)}/\underline{F}M^{(j)}$ est canoniquement isomorphe à $(M/\underline{F}M)^{(j)}$. On en déduit un isomorphisme canonique η_j de $(\mathfrak{m}^{p^{j-1}}/\mathfrak{m}^{p^j}) \otimes_A (M/\underline{F}M)^{(j)}$ sur $M_{A'}[j]/M_{A'}[j+1]$.

Enfin, il est clair que cette construction est fonctorielle en M .

COROLLAIRE 1.- <u>Soit</u> M <u>un</u> D_k<u>-module sans</u> $\underline{F}$<u>-torsion. Le A'-module</u> $M_{A'}/M_{A'}[1]$ <u>est tué par</u> $\mathfrak{m}$ <u>et l'application qui à</u> $\underline{a} \in M$ <u>associe l'image de</u> $1 \otimes \underline{a} \in A' \otimes_A M$ <u>dans</u> $M_{A'}$ <u>induit, par passage aux quotients, un isomorphisme (de k-espaces vectoriels) de</u> $M/\underline{F}M$ <u>sur</u> $M_{A'}/M_{A'}[1]$.

<u>Démonstration</u> : c'est clair, cet isomorphisme n'est autre que l'application η_0 définie ci-dessus.

COROLLAIRE 2.- <u>Soit</u> M <u>un</u> D_k<u>-module sans</u> $\underline{F}$<u>-torsion et soit</u> L <u>un sous-</u>D_k<u>-module de</u> M <u>vérifiant</u> $\underline{F}M \cap L = \underline{F}L$. <u>L'application de</u> $L_{A'}$ <u>dans</u> $M_{A'}$ <u>déduite par fonctorialité de l'inclusion de</u> L <u>dans</u> M , <u>est injective</u>.

<u>Démonstration</u> : avec des notations évidentes, on voit que $\underline{F}M \cap L = \underline{F}L$ implique que l'application canonique de $L/\underline{F}L$ dans $M/\underline{F}M$ est injective ; on voit qu'il en est de même, pour $0 \le j \le s$, de $(L/\underline{F}L)^{(j)} \to (M/\underline{F}M)^{(j)}$ et de $(\mathfrak{m}^{p^{j-1}}/\mathfrak{m}^{p^j}) \otimes_A (L/\underline{F}L)^{(j)} \to (\mathfrak{m}^{p^{j-1}}/\mathfrak{m}^{p^j}) \otimes_A (M/\underline{F}M)^{(j)}$. D'après la proposition 2.3, l'application canonique de $L_{A'}[j]/L_{A'}[j+1]$ dans $M_{A'}[j]/M_{A'}[j+1]$ est donc injective. Enfin il est clair que l'application canonique de $L_{A'}[s+1] = L_{s+1}$ dans $M_{A'}[s+1] = M_{s+1}$ est injective et l'assertion en résulte.

2.6. Donnons maintenant d'autres propriétés d'exactitude du foncteur $M \mapsto M_{A'}$.

PROPOSITION 2.4.- <u>Le foncteur</u> $M \mapsto M_{A'}$ <u>est exact à droite</u>.

<u>Démonstration</u> : soit

$$L \longrightarrow M \longrightarrow N \longrightarrow 0$$

une suite exacte de D_k-modules. Comme le produit tensoriel est exact à droite, on voit que, pour tout $(i,j) \in \mathbb{Z} \times \mathbb{Z}$, la suite

$$L_i^{(j)} \longrightarrow M_i^{(j)} \longrightarrow N_i^{(j)} \longrightarrow 0$$

est exacte. L'exactitude de la suite

$$L_{A'} \longrightarrow M_{A'} \longrightarrow N_{A'} \longrightarrow 0$$

s'en déduit par passage à la limite inductive.

COROLLAIRE 1.- Soit

$$0 \longrightarrow L \xrightarrow{u} M \xrightarrow{u'} N \longrightarrow 0$$

une suite exacte de D_k-modules sans $\underline{F}$-torsion. La suite

$$0 \longrightarrow L_{A'} \xrightarrow{u_{A'}} M_{A'} \xrightarrow{u'_{A'}} N_{A'} \longrightarrow 0$$

est exacte.

Démonstration : compte-tenu de la proposition 2.4, il suffit de montrer que $u_{A'}$ est injective. Si l'on utilise u pour identifier L à un sous-D_k-module de M, on voit que le fait que N soit sans $\underline{F}$-torsion équivaut à $\underline{F}M \cap L = \underline{F}L$; il suffit alors d'appliquer le corollaire 2 à la proposition 2.3.

COROLLAIRE 2.- Soit

$$0 \longrightarrow L \xrightarrow{u} M \xrightarrow{u'} N$$

une suite exacte de D_k-modules sans $\underline{F}$-torsion. Supposons que $\underline{F}N \cap v(M) = v(\underline{F}M)$. Alors la suite

$$0 \longrightarrow L_{A'} \xrightarrow{u_{A'}} M_{A'} \xrightarrow{u'_{A'}} N_{A'}$$

est exacte.

Démonstration : soit $\overline{M}$ le conoyau de u. Comme $\overline{M}$ s'identifie à un sous-D_k-module de N, $\overline{M}$ est sans $\underline{F}$-torsion et, d'après le corollaire 1, la suite

$$0 \longrightarrow L_A' \longrightarrow M_{A'} \longrightarrow \overline{M}_{A'} \longrightarrow 0$$

est exacte. Il suffit donc de montrer que l'application de $\overline{M}_{A'}$ dans $N_{A'}$ induite par l'inclusion de $\overline{M}$ dans N est injective. Mais $\underline{F}N \cap u'(M) = u'(\underline{F}M)$ signifie $\underline{F}N \cap \overline{M} = \underline{F}\overline{M}$ et il suffit d'appliquer le corollaire 2 à la proposition 2.3.

2.7. Donnons, pour terminer ce paragraphe, une description de $M_{A'}$ lorsque l'action de $\underline{V}$ sur le D_k-module M est surjective :

PROPOSITION 2.5.- Soit M un D_k-module tel que $\underline{V}M = M$. Alors l'application canonique de $A' \otimes_A M = M_0^{(0)}$ dans $M_{A'}$ est surjective et son noyau est le sous-A'-module $\sum_{j=1}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M)$.

Remarques :

1.- Si $j \geq s+1$, on a $j-1 \geq s$ donc $p^j - je \leq p^{j-1} - (j-1)e$ et $p^j \geq p^{j-1} + e$; par conséquent,

$$\mathrm{Im}(\mathfrak{m}^{p^j} \otimes_A \mathrm{Ker}\, \underline{V}^{j+1}|_M) \subset \mathrm{Im}(p\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^{j+1}|_M) \subset \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A p.\mathrm{Ker}\, \underline{V}^{j+1}|_M)$$
$$\subset \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M) .$$

On en déduit que $\sum_{j=1}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M) = \sum_{j=1}^{s+1} \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M)$. En particulier, si M est A-pro-artinien, ce sous-A'-module est bien fermé dans $A' \otimes_A M$.

2.- Si M est un D_k-module tel que $\underline{V}M = M$ et tel que l'action de $\underline{F}$ est injective, on a alors $\mathrm{Ker}\, \underline{V}^j|_M = \mathrm{Ker}\, p^j|_M$ et $M_{A'}$ s'identifie donc au quotient de $A' \otimes_A M$ par $\sum_{j=1}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, p^j|_M)$.

Démonstration de la proposition : posons $N' = \sum_{j=1}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M)$ et $N = (A' \otimes_A M)/N'$. Pour tout $(i,j) \in I_e$, nous allons définir une application A'-linéaire $\theta_{i,j} : M_i^{(j)} \to N$:

- si $j = 0$, alors $i \geq 0$, et l'application $\theta_{i,0}$ est la composée de l'application canonique de $\mathfrak{m}^i \otimes_A M$ dans $A' \otimes_A M$ et de la projection de $A' \otimes_A M$ sur N ;
- si $j \geq 1$, alors $i \geq p^{j-1} - je$, et tout élément de $M_i^{(j)}$ est somme finie d'éléments de la forme $p^{-j}\lambda \otimes_A \underline{a}$, avec $\lambda \in \mathfrak{m}^{i+je} \subset \mathfrak{m}^{p^{j-1}}$ et $\underline{a} \in M^{(j)}$; comme $\underline{V}M = M$, on a $\underline{V}^j M^{(j)} = M^{(j)}$, ou encore l'application $v^j : M \to M^{(j)}$ est surjective ; il existe donc $\underline{b} \in M$ tel que $v^j\underline{b} = \underline{a}$; si $\underline{b}'$ est un autre élément de M tel que $v^j\underline{b}' = \underline{a}$, on a $\underline{b}' = \underline{b} + \underline{c}$, avec $\underline{c} \in \mathrm{Ker}\, v^j|_M$; on en déduit que l'élément $\lambda \otimes \underline{b} - \lambda \otimes \underline{b}'$ de $A' \otimes_A M$ appartient à $\mathfrak{m}^{p^{j-1}} \otimes_A \mathrm{Ker}\, \underline{V}^j|_M$, donc au noyau de la projection canonique de $A' \otimes_A M$ sur N . Il est alors clair qu'il existe une application A'-linéaire $\theta_{i,j} : M_i^{(j)} \to N$ et une seule telle que $\theta_{i,j}(p^{-j}\lambda \otimes \underline{a})$ soit l'image de $\lambda \otimes_A \underline{b}$ ($\in A' \otimes_A M$) dans N .

On voit tout de suite que les $\theta_{i,j}$ sont compatibles avec les flèches du diagramme $\mathcal{D}_{I_e}(M)$; on en déduit donc une application

$\theta : \varinjlim \mathcal{D}_{I_e}(M) = M_{A'} \to N$.

Comme le composé de la flèche canonique θ' de $A' \otimes_A M$ dans $M_{A'}$ avec θ n'est autre que la projection canonique de $A' \otimes_A M$ sur N , on voit que le noyau de θ' est contenu dans N' .

Pour montrer que le noyau de θ' contient N' , il suffit de vérifier que si $j \geq 1$, $\lambda \in \mathfrak{m}^{p^{j-1}}$ et $\underline{a} \in \operatorname{Ker} \underline{V}^j|_M$, alors l'élément $\lambda \otimes \underline{a}$ de $A' \otimes_A M$ appartient au noyau de θ' . Mais cet élément provient, par une flèche du diagramme $\mathcal{D}_{I_e}(M)$, de l'élément $\lambda \otimes \underline{a}$ de $\mathfrak{m}^{p^{j-1}} \otimes_A M = M^{(0)}_{p^{j-1}}$. Ce dernier s'envoie, par une flèche de $\mathcal{D}_{I_e}(M)$, sur l'élément $p^{-j}\lambda \otimes v^j(\underline{a})$ de $p^{-j}\mathfrak{m}^{p^{j-1}} \otimes_A M^{(j)} = M^{(j)}_{p^{j-1}-je}$. Comme $\underline{a} \in \operatorname{Ker} \underline{V}^j|_M$, on a $v^j(\underline{a}) = \underline{V}^j\underline{a} = 0$, d'où $N' \subset \operatorname{Ker} \theta'$.

Enfin le fait que $\underline{V}M = M$ implique que toutes les applications $v_{i,j}$ du diagramme $\mathcal{D}_{I'_e}(M)$ sont toutes surjectives et la surjectivité de θ' en résulte très facilement.

§3.- Relèvement des covecteurs (suite).

On conserve les hypothèses et les notations du paragraphe précédent. Pour tout k-anneau R linéairement topologisé, séparé et complet, on note $CW_{k,A'}(R)$ le A'-module topologique $(CW_k(R))_{A'}$.

3.1. Rappelons (cf. n° II.5.1) que l'on a appelé anneau p-adique tout anneau $\mathcal{S}$ linéairement topologisé, séparé et complet, dont la topologie est la topologie p-adique, tel que p n'est pas diviseur de 0 . On appelle A'-anneau p-adique tout A'-anneau topologique qui est un anneau p-adique. Il est clair que l'inclusion de A dans A' permet de considérer tout A'-anneau p-adique comme un A-anneau p-adique.

Pour tout A'-anneau p-adique $\mathcal{S}$, on pose $\mathcal{S}_k = \mathcal{S} \otimes_{A'} k = \mathcal{S}/\mathfrak{m}\mathcal{S}$ et $\mathcal{S}_K = \mathcal{S} \otimes_{A'} K' = \mathcal{S} \otimes_A K$; on identifie $\mathcal{S}$ à un sous-anneau de $\mathcal{S}_K$ de manière évidente. On note $P'(\mathcal{S})$ le sous-A'-module de $\mathcal{S}_K$ engendré par les éléments de la forme $p^{-n}\hat{a}^{p^n}$, avec $n \in \mathbb{N}$, $\hat{a} \in \mathfrak{m}\mathcal{S}$; pour n suffisamment grand, on a $p^{-n}\hat{a}^{p^n} \in \mathcal{S}$, pour tout $\hat{a} \in \mathfrak{m}\mathcal{S}$; on en déduit que $P'(\mathcal{S})$ est un sous-A'-module fermé de $\mathcal{S}_K$ vérifiant $\mathfrak{m}\mathcal{S} \subset P'(\mathcal{S}) \subset \mathfrak{m}^{\nu}\mathcal{S}$ (rappelons que $\nu = \min_{n\in\mathbb{N}} \{p^n - ne\}$; en particulier, $P'(\mathcal{S}) = \mathfrak{m}\mathcal{S}$ si $e \leq p-1$).

Soit $\mathcal{S}$ un A'-anneau p-adique. On a défini au n° II.5.1 une application A-linéaire continue $\hat{w}_{\mathcal{S}} : CW_A(\mathcal{S}) \to \mathcal{S}_K$. Si $\underline{\hat{a}} = (\dots,\hat{a}_{-n},\dots,\hat{a}_{-1},\hat{a}_0) \in CW_A(\mathcal{S})$, alors $\hat{w}_{\mathcal{S}}(\underline{\hat{a}}) = \sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n}$. On voit que l'homomorphisme canonique de $CW_A(\mathcal{S})$ dans $CW_A(\mathcal{S}/\mathfrak{m}\mathcal{S}) = CW_k(\mathcal{S}_k)$ est surjectif et que son noyau est le sous-A-module fermé $CW_A(\mathfrak{m}\mathcal{S})$ de $CW_A(\mathcal{S})$ formé des éléments dont toutes les composantes sont dans $\mathfrak{m}\mathcal{S}$; l'image de $CW_A(\mathfrak{m}\mathcal{S})$ par $\hat{w}_{\mathcal{S}}$ est contenue dans $P'(\mathcal{S})$ et, par passage aux quotients, on en déduit une application A-linéaire continue de $CW_k(\mathcal{S}_k)$ dans $\mathcal{S}_K/P'(\mathcal{S})$; d'où, par extension des scalaires, une application A'-linéaire continue

$$w'_{\mathcal{S}} : A' \otimes_A CW_k(\mathcal{S}_k) \to \mathcal{S}_K/P'(\mathcal{S}) .$$

LEMME 3.1.- <u>Soit</u> $M = CW_k(\mathcal{S}_k)$. <u>Le noyau de</u> $w'_{\mathcal{S}}$ <u>contient le sous-A'-module</u> $M' = \sum_{j=0}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^j} \otimes_A \mathrm{Ker}\, \underline{V}^{j+1}|_M)$ <u>de</u> $A' \otimes_A M$.

<u>Démonstration</u> : il suffit de montrer que, si j est un entier ≥ 0 , si $\lambda \in \mathfrak{m}^{p^j}$ et si $\underline{b} \in \mathrm{Ker}\,\underline{V}^{j+1}|_M$, on a $w'_{\mathcal{S}}(\lambda\otimes\underline{b}) = 0$. On voit que $\underline{b}$ s'écrit sous la forme $(\dots,0,\dots,0,b_{-j},\dots,b_{-1},b_0)$; si $\hat{b}_{-n}$ est un relèvement de b_{-n} dans $\mathcal{S}$, on voit que $w'_{\mathcal{S}}(\lambda\otimes\underline{b})$ est l'image, dans $\mathcal{S}_K/P'(\mathcal{S})$ de $\beta = \sum_{n=0}^{j} p^{-n}\lambda\hat{b}_{-n}^{p^n}$. Soit π une uniformisante de A' ; on peut écrire $\lambda = \mu\pi^{p^j}$, avec $\mu \in A'$. On a alors $\beta = \mu \sum_{n=0}^{j} p^{-n}(\pi^{p^{j-n}}\hat{b}_{-n})^{p^n} \in P'(\mathcal{S})$, d'où $w'_{\mathcal{S}}(\lambda\otimes\underline{b}) = 0$.

Le sous-A'-module M' , qui est aussi $\sum_{j=0}^{s} \mathrm{Im}(\mathfrak{m}^{p^j} \otimes_A \mathrm{Ker}\,\underline{V}^{j+1}|_M)$, est fermé dans $A' \otimes_A M$ (cf. rem. 1 du n° 2.7) et l'application $w'_{\mathcal{S}}$ induit, par passage au quotient, une application A'-linéaire continue
$w''_{\mathcal{S}} : (A' \otimes_A M)/M' \to \mathcal{S}_K/P'(\mathcal{S})$.

Il est clair que le D_k-module $M = CW_k(\mathcal{S}_k)$ vérifie $\underline{V}M = M$. Il résulte donc de la proposition 2.5 que l'application canonique de $A' \otimes_A M$ dans $M_{A'}$ induit, par passage au quotient, un isomorphisme φ de $(A' \otimes_A M)/M'$ sur $M_{A'}$. On obtient alors une <u>application A'-linéaire continue</u>
$w_{\mathcal{S}} = w''_{\mathcal{S}} \circ \varphi^{(-1)} : CW_{k,A'}(\mathcal{S}_k) \to \mathcal{S}_K/P'(\mathcal{S})$.

Il est immédiat que l'application $w_{\mathcal{S}}$ est une transformation naturelle au sens suivant : soit $\psi : \mathcal{S} \to \mathcal{S}'$ un morphisme de A'-anneaux p-adiques ; soit $\psi_k : \mathcal{S}_k \to \mathcal{S}'_k$ la flèche déduite de ψ par extension des scalaires et soit $CW_{k,A'}(\psi_k) : CW_{k,A'}(\mathcal{S}_k) \to CW_{k,A'}(\mathcal{S}'_k)$ la flèche déduite de $CW_k(\psi_k) : CW_k(\mathcal{S}_k) \to CW_k(\mathcal{S}'_k)$ par fonctorialité ; soit $\psi_K : \mathcal{S}_K \to \mathcal{S}'_K$ la flèche déduite de ψ par extension des scalaires et soit $\tilde{\psi}_K : \mathcal{S}_K/P'(\mathcal{S}) \to \mathcal{S}'_K/P'(\mathcal{S}')$ la flèche déduite de ψ_K par passage aux quotients (il est clair que $\psi_K(P'(\mathcal{S})) \subset P'(\mathcal{S}'))$; alors le diagramme

$$\begin{array}{ccc} CW_{k,A'}(\mathcal{S}_k) & \xrightarrow{w_{\mathcal{S}}} & \mathcal{S}_K/P'(\mathcal{S}) \\ {\scriptstyle CW_{k,A'}(\psi_k)}\downarrow & & \downarrow{\scriptstyle \tilde{\psi}_K} \\ CW_{k,A'}(\mathcal{S}'_k) & \xrightarrow{w_{\mathcal{S}'}} & \mathcal{S}'_K/P'(\mathcal{S}') \end{array}$$

est commutatif.

3.2. Pour tout A'-anneau spécial (cf. n° II.5.4) $\mathcal{R}$, on pose

$$\mathcal{R}_k = \mathcal{R} \otimes_{A'} k = \mathcal{R}/\mathfrak{m}\mathcal{R} .$$

On identifie $\mathcal{R}$ à un sous-anneau de $\mathcal{R}_K = \mathcal{R}\otimes_A K = \mathcal{R}\otimes_{A'} K'$ et $\mathcal{R}_K$ à un sous-anneau de $\hat{\mathcal{R}}_K^{an}$ (id.). On a défini $P(\mathcal{R})$ comme étant le sous-A'-module fermé de $\hat{\mathcal{R}}_K^{an}$ formé des α tels que $d\alpha \in \Omega_{A'}(\mathcal{R})$ (en identifiant $\Omega_{A'}(\mathcal{R})$ à un sous-module de $\Omega_{K'}(\hat{\mathcal{R}}_K^{an})$).

Soit $P'(\mathcal{R})$ le sous-A'-module de $\hat{\mathcal{R}}_K^{an}$ engendré par les éléments de la forme $p^{-n}\beta^{p^n}$, avec $n \in \mathbb{N}$ et $\beta \in \mathfrak{m}\mathcal{R}$; c'est un sous-A'-module fermé de $P(\mathcal{R})$, contenu dans $\mathcal{R}_K$ et vérifiant $\mathfrak{m}\mathcal{R} \subset P'(\mathcal{R}) \subset \mathfrak{m}^{\nu}\mathcal{R}$.

Soit $\mathcal{R}$ un A'-anneau spécial. On a défini au n° II.5.6 une application A-linéaire continue $\hat{w}_{\mathcal{R}} : CW_A(\mathcal{R}) \to P(\mathcal{R})$. Ici encore l'homomorphisme canonique de $CW_A(\mathcal{R})$ dans $CW_A(\mathcal{R}/\mathfrak{m}\mathcal{R}) = CW_k(\mathcal{R}_k)$ est surjectif et son noyau est le sous-A-module fermé $CW_A(\mathfrak{m}\mathcal{R})$ de $CW_A(\mathcal{R})$ formé des éléments dont toutes les composantes sont dans $\mathfrak{m}\mathcal{R}$; il est clair que l'image par $\hat{w}_{\mathcal{R}}$ de $CW_A(\mathfrak{m}\mathcal{R})$ est contenue dans $P'(\mathcal{R})$ et, par passage aux quoti nts, on en déduit une application A-linéaire continue de $CW_k(\mathcal{R}_k)$ dans $P(\mathcal{R})/P'(\mathcal{R})$; d'où, par extension des scalaires, une application A'-linéaire continue

$$w'_{\mathcal{R}} : A' \otimes_A CW_k(\mathcal{R}_k) \longrightarrow P(\mathcal{R})/P'(\mathcal{R}) .$$

Si $M = CW_k(\mathfrak{R}_k)$, on voit, comme dans le cas des A'-anneaux p-adiques, que le noyau de $w'_{\mathfrak{R}}$ contient le sous-A'-module fermé

$$M' = \sum_{j=0}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^j} \otimes_A \mathrm{Ker}\, \underline{V}^{j+1}|_M) \quad \text{de} \quad A' \otimes_A M \quad ;$$

d'où, par passage au quotient, une application A'-linéaire continue $w''_{\mathfrak{R}}$ de $(A' \otimes_A M)/M'$ dans $P(\mathfrak{R})/P'(\mathfrak{R})$.

Comme $\underline{V}M = M$, la proposition 2.5 implique que l'application canonique de $A' \otimes_A M$ dans $M_{A'}$ induit, par passage au quotient, un isomorphisme φ de $(A' \otimes_A M)/M'$ sur $M_{A'}$. D'où une application A'-linéaire continue

$$w_{\mathfrak{R}} = w''_{\mathfrak{R}} \circ \varphi^{(-1)} : CW_{k,A'}(\mathfrak{R}_k) \longrightarrow P(\mathfrak{R})/P'(\mathfrak{R}) .$$

PROPOSITION 3.2.- <u>Soit $\mathfrak{R}$ un A'-anneau spécial. L'application A'-linéaire continue $w_{\mathfrak{R}} : CW_{k,A'}(\mathfrak{R}_k) \to P(\mathfrak{R})/P'(\mathfrak{R})$ est un isomorphisme</u>.

<u>Démonstration</u> : choisissons un A-anneau spécial $\mathfrak{R}_0$ contenu dans $\mathfrak{R}$ qui relève $\mathfrak{R}_k$ (il est clair qu'un tel anneau existe toujours : on se ramène au cas où $\mathfrak{R}$ est local ; si l'on choisit des coordonnées, $\mathfrak{R}$ s'identifie alors à un anneau des séries formelles $A''[[X_1,X_2,\dots,X_d]]$ à coefficients dans l'anneau A" des entiers d'une extension finie non ramifiée du corps des fractions de A' ; si k" est le corps résiduel de A" , on peut prendre $\mathfrak{R}_0 = W(k'')[[X_1,X_2,\dots,X_d]]$). On voit que $A' \otimes_A \mathfrak{R}_0$ s'identifie à $\mathfrak{R}$ et $A' \otimes_A P(\mathfrak{R}_0)$ à $P(\mathfrak{R})$).

Posons $N = P(\mathfrak{R}_0)/p\mathfrak{R}_0$. L'isomorphisme

$$w_{\mathfrak{R}_0} : CW_k(\mathfrak{R}_k) = M \longrightarrow P(\mathfrak{R}_0)/p\mathfrak{R}_0 = N$$

défini au n° II.5.7 permet de munir, par transport de structure, N d'une structure de D_k-module topologique et $w_{\mathfrak{R}_0}$ induit un isomorphisme

$$w_{\mathfrak{R}_0,A'} : M_{A'} \longrightarrow N_{A'} .$$

Le D_k-module N , comme M , vérifie $\underline{V}N = N$ et $N_{A'}$ s'identifie (prop. 2.5) au quotient de $A' \otimes_A N$ par le sous-A'-module $\sum_{j=0}^{\infty} \mathrm{Im}(\mathfrak{m}^{p^j} \otimes_A \mathrm{Ker}\, \underline{V}^{j+1}|_N)$. On voit que $N_{A'}$ s'identifie aussi au quotient de $P(\mathfrak{R}) = A' \otimes_A P(\mathfrak{R}_0)$ par le sous-A'-module N' de $P(\mathfrak{R})$ engendré par $\mathrm{Im}(A' \otimes_A p\mathfrak{R}_0) = p\mathfrak{R}$ et les éléments de la forme $\pi^{p^j} . \sum_{n=0}^{j} p^{-n}\hat{b}_{-n}^{p^n}$, pour $j \in \mathbb{N}$ et les $\hat{b}_{-n}$ dans $\mathfrak{R}_0$ (et où π est une uniformisante de A').

Il est immédiat que $N' \subset P'(\mathfrak{R})$ et que $w_{\mathfrak{R}}$ est le composé de l'isomorphisme $w_{\mathfrak{R}_0, A'} : M_{A'} \to N_{A'} = P(\mathfrak{R})/N'$ et de la projection canonique de $P(\mathfrak{R})/N'$ sur $P(\mathfrak{R})/P'(\mathfrak{R})$. Tout revient donc à montrer que $P'(\mathfrak{R}) \subset N'$, ou encore à établir le lemme suivant :

LEMME 3.3.- Soit $n \in \mathbb{N}$ et soit $b \in \mathfrak{m}\mathfrak{R}$. Alors $p^{-n} b^{p^n} \in N'$.

Démonstration : Ecrivons b sous la forme $b = \sum_{i=1}^{e} \pi^i b_i$, avec les $b_i \in \mathfrak{R}_0$ (où π est une uniformisante de A'). On procède par récurrence sur n :

- c'est clair si $n = 0$, car $\pi b_i \in N'$, donc a fortiori $\pi^i b_i = \pi^{i-1} \pi b_i \in N'$;
- on vérifie facilement que
$$\Big(\sum_{i=1}^{e} \pi^i b_i\Big)^{p^n} = \sum_{r=0}^{n-1} p^{n-r} \varphi_r((\pi^i b_i)^{p^r}) + \sum_{i=1}^{e} \pi^{ip^n} b_i^{p^n} ,$$
où les φ_r sont des polynômes à coefficients dans $\mathbb{Z}$; on a donc
$$p^{-n} b^{p^n} = \sum_{r=0}^{n-1} p^{-r} \varphi_r((\pi^i b_i)^{p^r}) + \sum_{i=1}^{e} p^{-n} \pi^{ip^n} b_i^{p^n} ;$$
on déduit facilement de l'hypothèse de récurrence que la première somme est dans N' ; enfin, pour tout $i \geq 1$, $p^{-n}(\pi b_i)^{p^n} \in N'$ donc, a fortiori,
$$p^{-n} \pi^{ip^n} b_i^{p^n} = \pi^{(i-1)p^n} . p^{-n} (\pi b_i)^{p^n} .$$

3.3. L'isomorphisme $w_{\mathfrak{R}}$ que l'on vient de construire définit une transformation naturelle : si $\psi : \mathfrak{R} \to \mathfrak{R}'$ est un morphisme de A'-anneaux spéciaux, le diagramme

$$\begin{array}{ccc} CW_{k,A'}(\mathfrak{R}_k) & \xrightarrow{w_{\mathfrak{R}}} & P(\mathfrak{R})/P'(\mathfrak{R}) \\ {\scriptstyle CW_{k,A'}(\psi_k)} \downarrow & & \downarrow {\scriptstyle \tilde{\psi}_K} \\ CW_{k,A'}(\mathfrak{R}'_k) & \xrightarrow{w_{\mathfrak{R}'}} & P(\mathfrak{R}')/P'(\mathfrak{R}') \end{array}$$

(où toutes les flèches sont évidentes) est commutatif.

De même, si $\mathfrak{R}$ est un A'-anneau spécial, si $\mathfrak{S}$ est un A'-anneau p-adique et si $\varphi : \mathfrak{R} \to \mathfrak{S}$ est un homomorphisme continu de A'-anneaux, le diagramme

$$\begin{array}{ccc} CW_{k,A'}(\mathfrak{R}_k) & \xrightarrow{w_{\mathfrak{R}}} & P(\mathfrak{R})/P'(\mathfrak{R}) \\ {\scriptstyle CW_{k,A'}(\varphi_k)}\downarrow & & \downarrow{\scriptstyle \tilde{\varphi}_K} \\ CW_{k,A'}(\mathfrak{S}_k) & \xrightarrow{w_{\mathfrak{S}}} & \mathfrak{S}_K/P'(\mathfrak{S}) \end{array}$$

(où toutes les flèches sont encore évidentes) est commutatif.

Remarque : soit $\mathfrak{S}$ un A'-anneau p-adique et soit $P(\mathfrak{S})$ le sous-A'-module de $\mathfrak{S}_K$ engendré par les $p^{-n}\hat{b}^{p^n}$, avec $n \in \mathbb{N}$, $\hat{b} \in \mathfrak{S}$. Il est clair que $P(\mathfrak{S})$ contient $P'(\mathfrak{S})$ et que l'image de $w_{\mathfrak{S}}$ est contenue dans $P(\mathfrak{S})/P'(\mathfrak{S})$. Dans toute la suite de ce chapitre, on peut remplacer $\mathfrak{S}_K/P'(\mathfrak{S})$ par $P(\mathfrak{S})/P'(\mathfrak{S})$ sans changer ni les démonstrations, ni les résultats.

On sait que $P'(\mathfrak{S}) \subset \mathfrak{m}^{\vee}\mathfrak{S}$; on pourrait de même remplacer $\mathfrak{S}_K/P'(\mathfrak{S})$ par $\mathfrak{S}_K/\mathfrak{m}^{\vee}\mathfrak{S}$ et $w_{\mathfrak{S}}$ par son composé avec la projection canonique de $\mathfrak{S}_K/P'(\mathfrak{S})$ sur $\mathfrak{S}_K/\mathfrak{m}^{\vee}\mathfrak{S}$; en revanche si $\mathfrak{R}$ est un A'-anneau spécial, il sera essentiel de travailler avec $P(\mathfrak{R})/P'(\mathfrak{R})$ et non avec $P(R)/(\mathfrak{m}^{\vee}R) \cap P(R)$ (l'application composée de $w_{\mathfrak{R}}$ avec la projection canonique de $P(\mathfrak{R})/P'(\mathfrak{R})$ sur $P(\mathfrak{R})/(\mathfrak{m}^{\vee}\mathfrak{R}) \cap P(\mathfrak{R})$ n'est un isomorphisme que si $\mathfrak{m}^{\vee}\mathfrak{R} = P'(\mathfrak{R})$, ce qui se produit si et seulement si $e \leq p-1$).

§ 4.- Groupes formels lisses sur A' .

On conserve les hypothèses et les notations des deux paragraphes précédents.

4.1. Soit G un p-groupe formel lisse et de dimension finie sur A' et soit $\mathfrak{R}$ son algèbre affine. Soit $G_k = G \otimes_{A'} k$ sa fibre spéciale ; c'est un p-groupe formel lisse et de dimension finie sur k dont l'algèbre affine s'identifie à $\mathfrak{R}_k = R \otimes_{A'} k$ et $\mathfrak{R}$ est un A'-anneau spécial.

Notons $\Delta : \mathfrak{R} \to \mathfrak{R} \hat{\otimes}_{A'} \mathfrak{R}$ (resp. $\Delta_k : \mathfrak{R}_k \to \mathfrak{R}_k \hat{\otimes}_k \mathfrak{R}_k$) le coproduit relatif à G (resp. G_k) ; il est clair que Δ relève Δ_k. Nous notons encore Δ le prolongement de Δ à $\hat{\mathfrak{R}}_K^{an}$ et, pour tout $\alpha \in \hat{\mathfrak{R}}_K^{an}$, nous posons
$\partial\alpha = \alpha\hat{\otimes}1 - \Delta\alpha + 1\hat{\otimes}\alpha$.

Notons $\mathcal{M}\mathcal{H}_{A'}(G)$ le sous-A'-module de $\hat{\mathfrak{R}}_K^{an}$ formé des $\alpha \in P(\mathfrak{R})$ tels que $\partial\alpha \in P'(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$ et $MH_{A'}(G)$ le quotient de $\mathcal{MH}_{A'}(G)$ par $P'(\mathfrak{R})$ (c'est donc un sous-A'-module de $P(\mathfrak{R})/P'(\mathfrak{R})$).

Posons enfin $M_{A'}(G_k) = (\underline{M}(G_k))_{A'}$. Il est clair que $CW_k(\mathfrak{R}_k)$ est un D_k-module sans $\underline{F}$-torsion. On sait que $\underline{M}(G_k)$ s'identifie à un sous-D_k-module de $CW_k(\mathfrak{R}_k)$. En outre, si $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in \underline{M}(G_k) \cap \underline{F}CW_k(\mathfrak{R}_k)$, on voit que l'image de a_0 dans $t^*_G(k)$ est nulle et on en déduit (prop. 4.3 du chap. III) que $\underline{a} \in \underline{F}\,\underline{M}(G_k)$. On a donc $\underline{M}(G_k) \cap \underline{F}CW_k(\mathfrak{R}_k) = \underline{F}\,\underline{M}(G_k)$ et il résulte du corollaire 2 à la proposition 2.3 que l'application canonique de $M_{A'}(G_k)$ dans $CW_{k,A'}(\mathfrak{R}_k)$ est injective. Nous l'utilisons pour identifier $M_{A'}(G_k)$ à un sous-A'-module de $CW_{k,A'}(\mathfrak{R}_k)$. Comme $\underline{M}(G_k)$ est fermé dans $CW_k(\mathfrak{R}_k)$, $M_{A'}(G_k)$ est fermé dans $CW_{k,A'}(\mathfrak{R}_k)$.

PROPOSITION 4.1.- <u>Soit</u> G <u>un p-groupe formel lisse et de dimension finie sur</u> A' <u>et soit</u> $\mathfrak{R}$ <u>son algèbre affine. Soit</u> $G_k = G\otimes_{A'}k$ <u>et</u> $\mathfrak{R}_k = \mathfrak{R}\otimes_{A'}k$.

i) <u>Les A'-modules</u> $\mathcal{MH}_{A'}(G) = \{\alpha \in P(\mathfrak{R}) \mid \partial\alpha \in P'(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})\}$ <u>et</u> $MH_{A'}(G) = \mathcal{MH}_{A'}(G)/P'(\mathfrak{R})$ <u>ne dépendent que de la réduction modulo</u> $\mathfrak{m}$ <u>du coproduit relatif à</u> G .

ii) <u>La restriction de</u> $w_{\mathfrak{R}} : CW_{k,A'}(\mathfrak{R}_k) \to P(\mathfrak{R})/P'(\mathfrak{R})$ <u>à</u> $M_{A'}(G_k)$ <u>induit un isomorphisme du A'-module topologique</u> $M_{A'}(G_k)$ <u>sur</u> $MH_{A'}(G)$.

<u>Démonstration</u> : il est clair que la première assertion résulte de la seconde. Montrons (ii).

Notons ∂^1 l'application D_k-linéaire continue de $CW_k(\mathfrak{R}_k)$ dans $CW_k(\mathfrak{R}_k\hat{\otimes}_k\mathfrak{R}_k)$ qui à $(\ldots,a_{-n},\ldots,a_0)$ associe

$$(\ldots,a_{-n}\hat{\otimes}1,\ldots,a_0\hat{\otimes}1) - (\ldots,\Delta_k a_{-n},\ldots,\Delta_k a_0) + (\ldots,1\hat{\otimes}a_{-n},\ldots,1\hat{\otimes}a_0)$$

et $\tilde{\partial}$ l'application de $P(\mathfrak{R})/P'(\mathfrak{R})$ dans $P(\mathfrak{R}\hat{\otimes}_A\mathfrak{R})/P'(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$ déduite, par passage aux quotients, de l'application ∂ définie plus haut. Il est clair que le diagramme

$$\begin{array}{ccc} CW_{k,A'}(\mathfrak{R}_k) & \xrightarrow{\partial^1_{A'}} & CW_{k,A'}(\mathfrak{R}_k\hat{\otimes}_k\mathfrak{R}_k) \\ {\scriptstyle w_{\mathfrak{R}}}\downarrow\wr & & \wr\downarrow{\scriptstyle w_{\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}}} \\ P(\mathfrak{R})/P'(\mathfrak{R}) & \xrightarrow{\tilde{\partial}} & P(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})/P'(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}) \end{array}$$

est commutatif. On en déduit que $w_{\mathfrak{R}}$ induit, par restriction, un isomorphisme du noyau de $\partial^1_{A'}$ sur celui de $\tilde{\partial}$ qui n'est autre que $MH_{A'}(G_k)$.

Pour tout entier $n \geq 0$, soit $C^n = \widehat{CW}_k(\mathfrak{R}_k^{\hat{\otimes}n}) = CW_k(\mathfrak{R}_k^{\hat{\otimes}n})$. On a une suite exacte de D_k-modules sans $\underline{F}$-torsion

$$0 \longrightarrow \underline{M}(G_k) \longrightarrow C^1 \xrightarrow{\partial^1} C^2 .$$

Admettons que $\underline{F}C^2 \cap \partial^1 C^1 = \partial^1(\underline{F}C^1)$; le corollaire 2 à la proposition 2.4 implique que la suite

$$0 \longrightarrow M_{A'}(G_k) \longrightarrow C^1_{A'} \xrightarrow{\partial^1_{A'}} C^2_{A'}$$

est exacte et $M_{A'}(G_k)$ est bien le noyau de $\partial^1_{A'}$.

Montrons donc que $\underline{F}C^2 \cap \partial^1 C^1 = \partial^1(\underline{F}C^1)$. Pour cela, considérons le complexe de Hochschild de G_k à valeurs dans $\widehat{CW}_k$. On voit que le groupe des n-cochaines s'identifie à C^n et que l'opérateur bord en degré 1 coïncide avec ∂^1 . Comme $\widehat{CW}_k$ est injectif (th. 2 du § 1 du chap. III), on a $H^2_s(G_k, \widehat{CW}_k) = \mathrm{Ext}^1(G_k, \widehat{CW}_k) = 0$. Soit alors $\underline{a} \in C^1$ tel que $\partial^1 \underline{a} = \underline{F}\underline{b}$, avec $\underline{b} \in C^2$; il est clair que $\partial^1 \underline{a}$ est une 2-cochaîne symétrique, et on en déduit que $\underline{b}$ aussi ; on a $\underline{F}(\partial^2 \underline{b}) = \partial^2(\underline{F}\underline{b}) = \partial^2\partial^1 \underline{a} = 0$, donc $\partial^2 \underline{b} = 0$, puisque C^2 est sans $\underline{F}$-torsion ; il existe donc $\underline{a}' \in C^1$ tel que $\underline{b} = \partial^1 \underline{a}'$ et on voit que $\partial^1 \underline{a} = \underline{F}\underline{b} = \underline{F}(\partial^1 \underline{a}') = \partial^1(\underline{F}\underline{a}') \in \partial^1(\underline{F}C^1)$, d'où le résultat.

4.2. Conservons les hypothèses et les notations du n° précédent et posons $M = \underline{M}(G_k)$; on a donc $M_{A'} = M_{A'}(G_k)$.

Notons $\mathfrak{L}_{A'}(G)$ l'ensemble des $\alpha \in P(\mathfrak{R})$ tels que $\partial\alpha = 0$. Il est clair que c'est un sous-A'-module de $\mathcal{M}\mathfrak{H}_{A'}(G)$. Notons $\rho(G)$ l'application composée

$$\mathfrak{L}_{A'}(G) \xrightarrow{\text{inclusion}} \mathcal{M}\mathfrak{H}_{A'}(G) \xrightarrow{\text{proj. can.}} MH_{A'}(G) \xrightarrow{\text{iso. can.}} M_{A'} .$$

L'image par $\rho(G)$ de $\mathfrak{m}\mathfrak{L}_{A'}(G)$ est contenue dans $\mathfrak{m}M_{A'}$, lui-même contenu, avec les notations du n° 2.4, dans $M_{A'}[1]$ puisque (cor. 1 à la prop. 2.3) $M_{A'}/M_{A'}[1]$ est tué par $\mathfrak{m}$. Par passage aux quotients, $\rho(G)$ induit donc une application k-linéaire de $\mathfrak{L}_{A'}(G)/\mathfrak{m}\mathfrak{L}_{A'}(G)$ dans $M_{A'}/M_{A'}[1]$; en composant avec l'isomorphisme canonique de $M_{A'}/M_{A'}[1]$ sur $M/\underline{F}M$ (cor. 1 à la prop. 2.3), on obtient une application k-linéaire

$$\tilde{\rho}(G) : \mathfrak{L}_{A'}(G)/\mathfrak{m}\mathfrak{L}_{A'}(G) \longrightarrow M/\underline{F}M .$$

PROPOSITION 4.2.- Soit G un p-groupe formel lisse et de dimension finie sur A'. Posons $M = \underline{M}(G_k)$, $\mathfrak{L} = \mathfrak{L}_{A'}(G)$ et $\tilde{\rho} = \tilde{\rho}(G)$. Alors

i) l'application $\tilde{\rho} : \mathfrak{L}/\mathfrak{m}\mathfrak{L} \to M/\underline{F}M$ est un isomorphisme de k-espaces vectoriels ;

ii) le A'-module $\mathfrak{L}$ est libre de rang fini.

Démonstration : remarquons d'abord que la deuxième assertion résulte facilement de la première. Soit, en effet, $\mathfrak{R}^{et}$ "la sous-algèbre étale maximale de $\mathfrak{R}$", i.e. l'algèbre affine du quotient G^{et} de G par sa composante neutre. On vérifie aisément que $\mathfrak{L} \cap P(\mathfrak{R}^{et}) = 0$ et que $\bigcap_{n=0}^{\infty} \mathfrak{m}^n P(\mathfrak{R}) = P(\mathfrak{R}^{et})$. On en déduit que $\bigcap_{n=0}^{\infty} \mathfrak{m}^n \mathfrak{L} = 0$. D'autre part, la première assertion montre que $\mathfrak{L}/\mathfrak{m}\mathfrak{L}$ est un k-espace vectoriel de dimension finie égale à celle de $M/\underline{F}M$, i.e. à la dimension d de G. Comme $\mathfrak{L}$ est un sous-A'-module de $P(\mathfrak{R})$, il est sans torsion, et $\mathfrak{L}$ est un A'-module libre de rang d.

Posons $\rho = \rho(G)$ et $N = CW_k(\mathfrak{R}_k)$; on a donc $CW_{k,A'}(\mathfrak{R}_k) = N_{A'}$. Reprenons les notations du §2. On voit facilement que, pour tout $(i,j) \in I_e$, l'image de l'application

$$N_i^{(j)} \xrightarrow{\text{can.}} N_{A'} \xrightarrow{w_{\mathfrak{R}}} P(\mathfrak{R})/P'(\mathfrak{R})$$

est contenue dans $(\mathfrak{m}^{p^{j-1}}P(\mathfrak{R}) + P'(\mathfrak{R}))/P'(\mathfrak{R})$. On en déduit que l'image par $w_{\mathfrak{R}}$ de $N_{A'}[1]$ est contenue dans $(\mathfrak{m}P(\mathfrak{R}) + P'(\mathfrak{R}))/P'(\mathfrak{R})$, donc dans $(\mathfrak{m}P(\mathfrak{R}))/P'(\mathfrak{R})$ puisque $P'(\mathfrak{R}) \subset \mathfrak{m}P(\mathfrak{R})$.

Soit $\alpha \in \mathfrak{L}$ tel que $\rho(\alpha) \in M_{A'}[1]$. Il est clair que $M_{A'}[1] \subset N_{A'}[1]$ et on en déduit que l'image de α dans $P(\mathfrak{R})/P'(\mathfrak{R})$ est contenue dans $(\mathfrak{m}P(\mathfrak{R}))/P'(\mathfrak{R})$. Si π est une uniformisante de A', on peut donc écrire $\alpha = \pi\beta$ avec $\beta \in P(\mathfrak{R})$; on a $\pi\partial\beta = \partial(\pi\beta) = \partial\alpha = 0$, donc $\partial\beta = 0$ puisque $P(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$ est sans torsion. Donc $\beta \in \mathfrak{L}$ et $\alpha = \pi\beta \in \mathfrak{m}\mathfrak{L}$, ce qui prouve que $\tilde{\rho}$ est injective.

Posons alors $\mathfrak{S} = \mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}$ et considérons le complexe de Hochschild de G à valeurs dans le complété formel du groupe additif sur A'. Pour tout entier $n \geq 0$, le groupe des n-cochaines s'identifie à $C^n = \mathfrak{R}^{\hat{\otimes} n}$ (en particulier, $C^1 = \mathfrak{R}$, $C^2 = \mathfrak{S}$). Soit $\partial^n : C^n \to C^{n+1}$ l'opérateur bord ; il est clair que $\partial^n(\mathfrak{m}C^n) \subset \mathfrak{m}C^{n+1}$ et que l'application de $C_k^n = C^n/\mathfrak{m}C^n$ dans $C_k^{n+1} = C^{n+1}/\mathfrak{m}C^{n+1}$ induite par ∂^n, par passage aux quotients, n'est autre que l'opérateur bord en degré n de la cohomologie de Hochschild de G_k à valeurs dans le complété formel du groupe additif sur k ; nous le notons encore ∂^n .

En outre, l'application $\partial^n : C^n \to C^{n+1}$ se prolonge, de manière unique, en une application A'-linéaire continue de $P(C^n)$ dans $P(C^{n+1})$, que nous notons encore ∂^n ; on voit que $\partial^{n+1} \circ \partial^n = 0$ et que $\partial^1 : P(\mathfrak{R}) \to P(\mathfrak{S})$ n'est autre que l'application ∂ .

Enfin, nous notons encore ρ l'application

$$\mathcal{M}\mathfrak{H}_{A'}(G) \xrightarrow{\text{proj. can.}} MH_{A'}(G) \xrightarrow{\text{iso. can.}} M_{A'} \ .$$

LEMME 4.3.- <u>Soit</u> $\alpha' \in P'(\mathfrak{S})$ <u>un tenseur symétrique vérifiant</u> $\partial^2\alpha' = 0$. <u>Il existe</u> $\gamma \in \mathcal{M}\mathfrak{H}_{A'}(G)$ <u>vérifiant</u> $\rho(\gamma) \in M_{A'}[1]$ <u>tel que</u> $\partial\gamma = \alpha'$.

Commençons par montrer comment la surjectivité de $\tilde{\rho}$ se déduit du lemme : comme l'application

$$\mathcal{M}\mathfrak{H}_{A'}(G) \longrightarrow M_{A'} \xrightarrow{\text{proj.}} M_{A'}/M_{A'}[1] \xrightarrow{\text{iso. can.}} M/\underline{F}M$$

est surjective, il suffit de vérifier que si $\alpha \in \mathcal{M}\mathfrak{H}_{A'}(G)$, il existe $\gamma \in \mathcal{M}\mathfrak{H}_{A'}(G)$ vérifiant $\rho(\gamma) \in M_{A'}[1]$ tel que $\alpha - \gamma \in \mathfrak{L}$, i.e. tel que $\partial\alpha = \partial\gamma$. Il suffit d'appliquer le lemme à $\alpha' = \partial\alpha$.

Avant de démontrer le lemme, commençons par introduire quelques notations :

soit $\mathbb{I}$ l'ensemble des (s+1)-uples d'entiers rationnels $\underline{i} = (i_0, i_1, \dots, i_s)$ vérifiant

$$\begin{cases} i_0 \geq 1 \ , \\ i_{j-1} - e + p^j - p^{j-1} \leq i_j \leq i_{j-1} \ , \text{ pour } 1 \leq j \leq s \ . \end{cases}$$

Pour tout $\underline{i} \in \mathbb{I}$, soit $P^{(\underline{i})}(\mathfrak{S})$ le sous-ensemble de $\mathfrak{S}_K = \mathfrak{S} \otimes_{A'} K'$ formé des sommes finies d'éléments de la forme $\lambda\alpha^{p^j}$, avec $0 \leq j \leq s$, $\lambda \in \mathfrak{m}^{i_j}$ et $\alpha \in \mathfrak{S}$; il est clair que c'est un sous-A'-module de $\mathfrak{S}_K$. On voit en outre

- que si $\underline{i} = (i_0, \dots, i_s)$ et $\underline{i}' = (i'_0, \dots, i'_s)$ sont deux éléments de $\mathbb{I}$ vérifiant $i_j \leq i'_j$, pour tout j , alors $P^{(\underline{i}')}(\mathfrak{S}) \subset P^{(\underline{i})}(\mathfrak{S})$;
- que si $i_j = i_{j-1} - e + p^j - p^{j-1}$, pour tout $j \geq 1$, alors $i_j = (i_0 - 1) + p^j - je$, pour tout j , et, par conséquent, $P^{(\underline{i})}(\mathfrak{S}) = \mathfrak{m}^{i_0 - 1}P'(\mathfrak{S})$;
- et que de ces deux résultats on déduit que, pour tout $\underline{i} = (i_0, \dots, i_s) \in \mathbb{I}$,

on a $P^{(\underline{i})}(\mathbb{S}) \subset \mathfrak{m}^{i_0-1} P'(\mathbb{S})$; en particulier les $P^{(\underline{i})}(\mathbb{S})$ sont contenus dans $P'(\mathbb{S})$.

Le lemme 4.3 va résulter du lemme suivant :

LEMME 4.4.- Soit $\underline{i} = (i_0, \ldots, i_s) \in \mathbb{I}$.

i) Soit r le plus petit entier ≥ 0 vérifiant $i_r = i_s$ et soit $i = i_r = i_s$. Posons

$$i'_j = \begin{cases} i_j \ , \text{ pour } 0 \leq j \leq r-1 \ , \\ i + 1 + p^j - p^r - (j-r)e \ , \text{ pour } r \leq j \leq s \ . \end{cases}$$

Alors $\underline{i}' = (i'_0, i'_1, \ldots, i'_s) \in \mathbb{I}$.

ii) Soit α' un tenseur symétrique de $P^{(\underline{i})}(\mathbb{S})$ tel que $\partial^2\alpha' = 0$. Il existe $\gamma \in \mathfrak{m}^{i_0-1} \mathcal{M}\mathcal{H}_{A'}(G)$ vérifiant $\rho(\gamma) \in M_{A'}[1]$ tel que $\alpha' - \partial\gamma \in P^{(\underline{i}')}(\mathbb{S})$.

Commençons par montrer comment le lemme 4.4 implique le lemme 4.3 : munissons $\mathbb{I}$ de l'ordre induit par l'ordre lexicographique sur $\mathbb{Z}^{s+1}$.

On a $\alpha' \in P'(\mathbb{S}) = P^{(\underline{i}^0)}(\mathbb{S})$, avec $\underline{i}^0 = (1, \ldots, p^j - je, \ldots, p^s - se) \in \mathbb{I}$, et le lemme 4.4 montre que l'on peut trouver une suite strictement croissante

$$\underline{i}^0 < \underline{i}^1 < \ldots < \underline{i}^n < \underline{i}^{n+1} < \ldots$$

d'éléments de $\mathbb{I}$ et des éléments $\gamma_1, \gamma_2, \ldots, \gamma_n, \ldots$ de $\mathcal{M}\mathcal{H}_{A'}(G)$ vérifiant $\rho(\gamma_n) \in M_{A'}[1]$ et $\gamma_n \in \mathfrak{m}^{i_0^n - 1} \mathcal{M}\mathcal{H}_{A'}(G)$, tels que $\alpha' - \partial(\gamma_1 + \gamma_2 + \ldots + \gamma_n) \in P^{(\underline{i}^{n+1})}(\mathbb{S})$ (on a posé $\underline{i}^n = (i_0^n, i_1^n, \ldots, i_s^n)$).

On voit que le fait que la suite des $\underline{i}^n$ soit strictement croissante implique que la suite des i_0^n tend vers l'infini avec n . Comme les A'-modules $M_{A'}$, $MH_{A'}(G)$ et $\mathcal{M}\mathcal{H}_{A'}(G)$ sont visiblement séparés et complets pour la topologie $\mathfrak{m}$-adique, et comme toutes les applications qui interviennent sont continues, on voit que la série de terme général γ_n converge dans $\mathcal{M}\mathcal{H}_{A'}(G)$ et que $\alpha' - \partial(\sum_{n=1}^{\infty} \gamma_n) = 0$; comme $M_{A'}[1]$ est un sous-A'-module fermé de $M_{A'}$, on a $\rho(\sum \gamma_n) = \sum \rho(\gamma_n) \in M_{A'}[1]$, d'où le lemme 4.3.

Il reste à démontrer le lemme 4.4. La première assertion se vérifie sans difficulté. Prouvons la seconde :

on voit que toute somme finie de la forme $\sum \lambda_t \beta_t^{p^{r_t}}$, avec les λ_t dans

A' , les β_t dans $\mathcal{S}$ et les r_t des entiers $\geq r$, est congrue modulo $\mathfrak{m}\mathcal{S}$ à la puissance p^r-ième d'un élément de $\mathcal{S}$. On en déduit que, si π est une uniformisante de A' , on peut écrire α' sous la forme

$$\alpha' = \pi^i \beta^{p^r} + \beta_1 \ ,$$

où $\beta \in \mathcal{S}$ et où β_1 est une somme finie de termes de la forme $\pi^{i'}(\beta')^{p^j}$, avec $\beta' \in \mathcal{S}$ et ou bien $j < r$ et $i' \geq i_j$, ou bien $j = r$ et $i' > i$; en particulier on voit que $\beta_1 \in P^{(\underline{i'})}(\mathcal{S})$; en outre les i' vérifient tous $i' > i$ et $\pi^{-i}\beta_1 \in \mathfrak{m}\mathcal{S}$.

On a alors $\pi^{-i}\alpha' = \beta^{p^r} + \pi^{-i}\beta_1$ et $0 = \partial^2(\pi^{-i}\alpha') = \partial^2(\beta^{p^r}) + \partial^2(\pi^{-i}\beta_1)$. Soit $\tilde{\beta}$ l'image de β dans $\mathcal{S}_k = \mathcal{S}/\mathfrak{m}\mathcal{S} = \mathcal{C}_k^2$. Comme $\pi^{-i}\beta_1 \in \mathfrak{m}\mathcal{S} = \mathfrak{m}\mathcal{C}^2$, on a $\partial^2(\pi^{-i}\beta_1) \in \mathfrak{m}\mathcal{C}^3$ et $\partial^2(\tilde{\beta}^{p^r}) = 0$. Il est clair que $\partial^2(\tilde{\beta}^{p^r}) = (\partial^2(\tilde{\beta}))^{p^r}$ et, comme l'anneau $\mathcal{C}_k^3$ est réduit, on a $\partial^2\tilde{\beta} = 0$.

Posons $b_{-r} = \tilde{\beta}$ et soit $\underline{b}$ l'élément $(\ldots,0,\ldots,0,b_{-r})$ de $\widehat{CW}_k(\mathcal{S}_k)$. Le groupe $\widehat{CW}_k(\mathcal{S}_k)$ s'identifie au groupe des 2-cochaînes du complexe de Hochschild de G_k à valeurs dans $\widehat{CW}_k$. Si l'on note encore ∂^2 l'opérateur bord en degré 2 de ce complexe, on voit que $\partial^2 b_{-r} = 0$ implique que $\partial^2\underline{b} = 0$.

Mais α' est un tenseur symétrique et il en est de même de $\tilde{\beta}^{p^r}$ donc aussi de $b_{-r} = \tilde{\beta}$; on voit donc que $\underline{b}$ est un 2-cocycle symétrique. Comme $H_s^2(G_k,\widehat{CW}_k) = 0$, il existe un élément $\underline{c} = (\ldots,c_{-n},\ldots,c_0) \in \widehat{CW}_k(R_k)$ tel que $\partial^1\underline{c} = \underline{b}$.

Si l'on note $\underline{c}'$ le covecteur

$$\underline{c}' = (\ldots,c_{-n+r},\ldots,c_0,0,\ldots,0)$$

(où c_0 est la composante d'indice $-r$), on voit que

$$\partial^1\underline{c}' = (\ldots,0,\ldots,0,b_{-r},b_{-r+1},\ldots,b_0)$$

où les b_{-j} , pour $0 \leq j \leq r-1$, sont des éléments convenables de $\mathcal{S}_k$.

Choisissons pour tout n un relèvement $\hat{c}_{-n}$ de c_{-n} dans $\mathcal{R}$, et, pour $0 \leq j \leq r-1$, un relèvement $\hat{b}_{-j}$ de b_{-j} dans $\mathcal{S}$. Si l'on pose $\gamma' = \sum_{n=0}^{\infty} p^{-n-r}\hat{c}_{-n}^{p^{n+r}}$, on voit que γ' est un élément de $P(\mathcal{R})$ vérifiant $\partial\gamma' \equiv p^{-r}\beta^{p^r} + \sum_{j=0}^{r-1} p^{-j}\hat{b}_{-j}^{p^j} \pmod{P'(\mathcal{S})}$.

Posons $\gamma = p^r \pi^i \gamma'$; on a

$$\partial\gamma \equiv \pi^i \beta^{p^r} + \sum_{j=0}^{r-1} p^{r-j} \pi^i \hat{b}_{-j}^{p^j} \pmod{p^r \mathfrak{m}^i P'(\mathcal{S})} .$$

Finalement, on peut écrire $\alpha' - \partial\gamma = \beta_1 + \beta_2 + \beta_3$, avec $\beta_1 \in P^{(\underline{i}')}(\mathcal{S})$, $\beta_2 = \sum_{j=0}^{r-1} p^{r-j} \pi^i \hat{b}_{-j}^{p^j}$ et $\beta_3 \in p^r \mathfrak{m}^i P'(\mathcal{S})$. Montrons que β_2 et β_3 sont aussi dans $P^{(\underline{i}')}(\mathcal{S})$:

- pour β_2 , il suffit de vérifier que $i + (r-j)e \geq i'_j = i_j$, pour $0 \leq j \leq r-1$, ce qui ne présente pas de difficultés ;
- on voit que β_3 est somme finie d'éléments de la forme $\lambda(\beta')^{p^j}$, avec $\beta' \in \mathcal{S}$, $0 \leq j \leq s$ et $\lambda \in \mathfrak{m}^{i+re+p^j-je}$; il suffit donc de vérifier que, pour $0 \leq j \leq s$, on a $i + (r-j)e + p^j \geq i'_j$, ce qui ne présente pas, non plus, de difficultés.

On a donc $\alpha' - \partial\gamma \in P^{(\underline{i}')}(\mathcal{S})$. Il reste à vérifier que $\gamma \in \mathfrak{m}^{i_0 - 1} \mathcal{M}\mathcal{H}_{A'}(G)$ et que $\rho(\gamma) \in M_{A'}[1]$:

- posons $\gamma'' = \pi^{p^r} \gamma'$. On voit que $\gamma'' \in \mathfrak{m}^{p^r} P(\mathcal{R}) \subset P(\mathcal{R})$ et que
$$\partial\gamma'' \equiv p^{-r} \pi^{p^r} \beta^{p^r} + \sum_{j=0}^{r-1} p^{-j} (\pi^{p^{r-j}} \hat{b}_{-j})^{p^j} \pmod{P'(\mathcal{S})} ,$$ donc que $\gamma'' \in \mathcal{M}\mathcal{H}_{A'}(G)$; on en déduit que $\gamma = p^r \pi^{i-p^r} \gamma'' \in \mathfrak{m}^{i+re-p^r} \mathcal{M}\mathcal{H}_{A'}(G)$. Des inégalités $i_j \geq i_{j-1} - e + p^j - p^{j-1}$, on déduit que $i = i_r \geq i_0 - re + p^r - 1$, donc que $i + re - p^r \geq i_0 - 1$, et γ appartient bien à $\mathfrak{m}^{i_0 - 1} \mathcal{M}\mathcal{H}_{A'}(G)$.
- Enfin, comme $\partial \underline{c} = \underline{b} = (\ldots,0,\ldots,0,b_{-r})$, on a $\partial(\underline{V}\underline{c}) = \underline{V}(\partial\underline{c}) = \underline{V}\underline{b} = 0$ et $\underline{V}\underline{c} = (\ldots,c_{-n-1},\ldots,c_{-1}) \in \underline{M}(G_k) = M$. On a $i - e \geq p^r - (r+1)e$ et $M_{i-e}^{(r+1)}$ est un objet du diagramme $\mathcal{D}_{I_e}(M)$. Si l'on identifie M à $M^{(r+1)}$, on peut considérer $p^{-1}\pi^i \otimes \underline{V}\underline{c}$ comme un élément de $M_{i-e}^{(r+1)}$; comme $r+1 \geq 1$, l'image de $M_{i-e}^{(r+1)}$ dans $M_{A'}$ est contenue dans $M_{A'}[1]$. Il suffit alors pour terminer la démonstration de vérifier que $\rho(\gamma)$ est égal à l'image de $p^{-1}\pi^i \otimes \underline{V}\underline{c}$ dans $M_{A'}$.

4.3. Soit M un D_k-module sans $\underline{F}$-torsion, soit $\mathcal{L}$ un A'-module et soit $\rho : \mathcal{L} \to M_{A'}$ une application A'-linéaire. Comme $M_{A'}/M_{A'}[1]$ est canoniquement isomorphe à $M/\underline{F}M$ (cor. 1 à la prop. 2.3), le noyau de l'application composée

$$\mathcal{L} \xrightarrow{\rho} M_{A'} \xrightarrow{\text{proj.}} M_{A'}/M_{A'}[1] \xrightarrow{\text{iso. can.}} M/\underline{F}M$$

contient $\mathfrak{m}\mathcal{L}$ et nous notons $\tilde{\rho}$ l'application k-linéaire de $\mathcal{L}/\mathfrak{m}\mathcal{L}$ dans $M/\underline{F}M$ induite par passage au quotient.

Notons $\Lambda^{\ell}_{A'}$ la catégorie dont les objets sont les triplets $(\mathcal{L}, M, \rho)$

- où M est un D_k-module profini sans $\underline{F}$-torsion tel que le quotient $M/\underline{F}M$ est un espace vectoriel de dimension finie sur k ,
- où $\mathcal{L}$ est un A'-module libre de rang fini,
- où ρ est une application A'-linéaire de $\mathcal{L}$ dans $M_{A'}$ telle que l'application k-linéaire $\tilde{\rho} : \mathcal{L}/\mathfrak{m}\mathcal{L} \to M/\underline{F}M$ soit un isomorphisme.

Un morphisme $u : (\mathcal{L}, M, \rho) \to (\mathcal{L}', M', \rho')$ de la catégorie $\Lambda^{\ell}_{A'}$ est un couple $(u_{\mathcal{L}}, u_M)$ formé d'une application A'-linéaire $u_{\mathcal{L}} : \mathcal{L} \to \mathcal{L}'$ et d'une application D_k-linéaire continue $u_M : M \to M'$ telles que le diagramme

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{u_{\mathcal{L}}} & \mathcal{L}' \\ \rho \downarrow & & \downarrow \rho' \\ M_{A'} & \xrightarrow{u_{M,A'}} & M'_{A'} \end{array}$$

(où l'on a posé $u_{M,A'} = (u_M)_{A'}$) soit commutatif.

Il est clair que $\Lambda^{\ell}_{A'}$ est une catégorie additive.

La proposition 6.1 du chapitre III et la proposition 4.2 montrent que, si G est un p-groupe formel lisse et de dimension finie sur A' , le triplet $\mathcal{L}M_{A'}(G) = (\mathcal{L}_{A'}(G), \underline{M}(G_k), \rho(G))$ est un objet de $\Lambda^{\ell}_{A'}$.

Soit maintenant $f : G' \to G$ un morphisme de p-groupes formels lisses et de dimension finie sur A' . Par extension des scalaires, f induit un morphisme $f_k : G'_k \to G_k$ des fibres spéciales, donc une application D_k-linéaire continue $\underline{M}(f_k) : \underline{M}(G_k) \to \underline{M}(G'_k)$. Soit, d'autre part, $\mathfrak{R}$ (resp. $\mathfrak{R}'$) l'algèbre affine de G (resp. G') ; le morphisme f induit un homomorphisme continu $f^* : \mathfrak{R} \to \mathfrak{R}'$ qui se prolonge, de manière unique, en un homomorphisme continu $f^*_K : \hat{\mathfrak{R}}^{an}_K \to (\widehat{\mathfrak{R}'})^{an}_K$. Il est clair que f^*_K envoie $P(\mathfrak{R})$ dans $P(\mathfrak{R}')$ et $\mathcal{L}(G)$ dans $\mathcal{L}(G')$. Si l'on note $\mathcal{L}(f)$ la restriction de f^*_K à $\mathcal{L}(G)$, on vérifie sans difficultés que le couple $(\mathcal{L}(f), \underline{M}(f_k))$ est un morphisme de la catégorie $\Lambda^{\ell}_{A'}$, i.e. que le diagramme

$$\begin{array}{ccc} \mathcal{L}(G) & \xrightarrow{\mathcal{L}(f)} & \mathcal{L}(G') \\ {\scriptstyle \rho(G)}\downarrow & & \downarrow{\scriptstyle \rho(G')} \\ \underline{M}(G_k) & \xrightarrow{(\underline{M}(f_k))_{A'}} & M(G'_k) \end{array}$$

est commutatif.

Ceci permet de considérer $\mathcal{L}M_{A'}$ comme un foncteur contravariant de la catégorie des p-groupes formels lisses et de dimension finie sur A' dans $\Lambda^{\ell}_{A'}$. On voit facilement que ce foncteur est additif.

4.4. Nous allons maintenant associer à tout objet $(\mathcal{L}, M, \rho)$ de $\Lambda^{\ell}_{A'}$ un foncteur covariant $G_{(\mathcal{L},M,\rho)}$ de la catégorie des A'-anneaux p-adiques dans celle des groupes abéliens , en généralisant la construction faite au n° 1.3 dans le cas $e = 1$.

Soit $\mathcal{S}$ un tel anneau (nous renvoyons au § 3 pour la définition de $\mathcal{S}_K$, $P'(\mathcal{S})$, $\mathcal{S}_k$ et de l'application $w_{\mathcal{S}} : CW_{k,A'}(\mathcal{S}_k) \to \mathcal{S}_K/P'(\mathcal{S}))$:

- nous notons $N_{\mathcal{L}}(\mathcal{S})$ (resp. $N^0_{\mathcal{L}}(\mathcal{S})$) le groupe $\mathrm{Hom}_{A'}(\mathcal{L}, \mathcal{S}_K)$ (resp. $\mathrm{Hom}_{A'}(\mathcal{L}, \mathcal{S}_K/P'(\mathcal{S}))$ des applications A'-linéaires de $\mathcal{L}$ dans $\mathcal{S}_K$ (resp. dans $\mathcal{S}_K/P'(\mathcal{S})$;
- nous notons $G_M(\mathcal{S})$ le groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(\mathcal{S}_k))$ des applications D_k-linéaires continues de M dans $CW_k(\mathcal{S}_k)$;
- nous notons φ_ρ l'application de $G_M(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ qui à $u \in G_M(\mathcal{S})$ associe $w_{\mathcal{S}} \circ u_{A'} \circ \rho$; il est clair que φ_ρ est un homomorphismes de groupes ;
- enfin nous notons $G_{(\mathcal{L},M,\rho)}(\mathcal{S})$ le produit fibré $N_{\mathcal{L}}(\mathcal{S}) \times_{N^0_{\mathcal{L}}(\mathcal{S})} G_M(\mathcal{S})$, où le morphisme de $N_{\mathcal{L}}(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ est celui qui provient de la projection canonique de $\mathcal{S}_K$ sur $\mathcal{S}_K/P'(\mathcal{S})$ et celui de $G_M(\mathcal{S})$ dans $N^0_{\mathcal{L}}(\mathcal{S})$ est φ_ρ . Autrement dit un élément de $G_{(\mathcal{L},M,\rho)}(\mathcal{S})$ est un couple $(u_{\mathcal{L}}, u_M)$ où $u_{\mathcal{L}} : \mathcal{L} \to \mathcal{S}_K$ est une application A'-linéaire, $u_M : M \to CW_k(\mathcal{S}_k)$ est une application D_k-linéaire continue, tel que le diagramme

$$\begin{array}{ccccc} \mathcal{L} & \xrightarrow{u_{\mathcal{L}}} & \mathcal{S}_K & & \\ {\scriptstyle \rho}\downarrow & & & \searrow^{\mathrm{proj.}} & \\ & & & & \mathcal{S}_K/P'(\mathcal{S}) \\ & & & \nearrow_{w_{\mathcal{S}}} & \\ M_{A'} & \xrightarrow{u_{M,A'}} & CW_{k,A'}(\mathcal{S}_k) & & \end{array}$$

est commutatif.

Il est clair que toutes ces constructions sont fonctorielles en $\mathcal{S}$. On voit qu'elles sont aussi fonctorielles en $(\mathcal{L},M,\rho)$, i.e. que tout morphisme $u : (\mathcal{L},M,\rho) \to (\mathcal{L}',M',\rho')$ induit, de manière évidente, un morphisme de foncteurs en groupes de $G_{(\mathcal{L}',M',\rho)}$ dans $G_{(\mathcal{L},M,\rho)}$.

4.5. Dans toute la suite de ce chapitre, nous notons t le plus grand entier tel que $p^t - te \leq p^n - ne$, pour tout entier $n \geq 0$ (on a donc $t = s$ si $p^s - p^{s-1} < e < p^{s+1} - p^s$, $t = s+1$ si $e = p^{s+1} - p^s$; en particulier $t = 0$ si $1 \leq e < p-1$ et $t = 1$ si $e = p-1$).

Soit G un p-groupe formel lisse et de dimension finie sur A' . Pour tout A'-anneau p-adique $\mathcal{S}$, notons $G(\mathcal{S})$ le groupe des homomorphismes continus de $\mathcal{R}$ dans $\mathcal{S}$ et, pour tout entier $r \geq 1$, $G(\mathfrak{m}^r\mathcal{S})$ l'ensemble des $x \in G(\mathcal{S})$ tels que l'image par x de l'idéal d'augmentation de $\mathcal{R}$ est contenue dans $\mathfrak{m}^r\mathcal{S}$. Il est clair que les $G(\mathfrak{m}^r\mathcal{S})$ forment en fait une suite décroissante de sous-groupes de $G(\mathcal{S})$ et que $G(\mathcal{S})$ est séparé et complet pour la topologie définie par cette suite de sous-groupes, i.e. que $G(\mathcal{S})$ s'identifie canoniquement à $\varprojlim G(\mathcal{S})/G(\mathfrak{m}^r\mathcal{S})$.

Il est clair que $G(\mathfrak{m}\mathcal{S})$ est le noyau de l'application canonique de $G(\mathcal{S})$ dans $G(\mathcal{S}/\mathfrak{m}\mathcal{S}) = G_k(\mathcal{S}_k)$. Comme G est lisse, cette application est surjective et $G(\mathcal{S})/G(\mathfrak{m}\mathcal{S})$ s'identifie canoniquement (et fonctoriellement en $\mathcal{S}$ et en G) à $G_k(\mathcal{S}_k)$.

Si G est étale, on voit que $G(\mathfrak{m}^r\mathcal{S}) = 0$, pour tout $r \geq 1$. On en déduit que, si l'on note G^c la composante connexe de l'élément-neutre de G , on a $G(\mathfrak{m}^r\mathcal{S}) = G^c(\mathfrak{m}^r\mathcal{S})$, pour tout entier $r \geq 1$.

PROPOSITION 4.5.- <u>Soit</u> G <u>un p-groupe formel lisse et de dimension finie sur</u> A' <u>et soit</u> $\mathcal{S}$ <u>un A'-anneau p-adique. Pour tout entier</u> r <u>vérifiant</u> $0 \leq r < t$, <u>le groupe</u> $G(\mathfrak{m}^{p^r}\mathcal{S})/G(\mathfrak{m}^{p^{r+1}}\mathcal{S})$ <u>est d'exposant</u> p .

Démonstration : il est clair que l'on peut supposer G connexe. Soit d sa dimension, soit $\mathcal{R}$ son algèbre affine et soit $X_1, X_2, \dots, X_d$ des générateurs de l'idéal d'augmentation ; on a donc $\mathcal{R} = A'[[X_1, \dots, X_d]]$.

Soit $\Delta_p : \mathcal{R} \to \mathcal{R}^{\hat{\otimes} p}$, le p-ième itéré du coproduit. Il est clair que chaque

$\Delta_p(X_i)$ est une série formelle sans terme constant en les $1 \hat{\otimes} 1 \hat{\otimes} \ldots \hat{\otimes} 1 \hat{\otimes} X_j \hat{\otimes} 1 \hat{\otimes} \ldots \hat{\otimes} 1$ et que c'est aussi un tenseur symétrique. On en déduit immédiatement que l'on peut écrire $\Delta_p(X_i) = a_i + b_i$, où a_i est un tenseur obtenu par symétrisation d'un tenseur qui est une série formelle sans terme constant et où b_i ne contient pas de terme de degré $< p$ par rapport à l'ensemble des variables.

Si l'on note η l'endomorphisme de $\mathfrak{R}$ qui définit la multiplication par p, on en déduit que $\eta(X_i) = pa'_i + b'_i$, où $a'_i = a'_i(X_1,\ldots,X_d)$ et $b'_i = b'_i(X_1,\ldots,X_d)$ sont des séries formelles sans terme constant et où b'_i ne contient pas de terme de degré $< p$.

Soit $x \in G(\mathfrak{m}^{p^r}\mathcal{S})$, soit $y = px$ et soit, pour $1 \leq i \leq d$, $x_i = x(X_i)$, $y_i = y(Y_i)$. On a

$$y_i = pa'_i(x_1,\ldots,x_d) + b'_i(x_1,\ldots,x_d) .$$

On voit que

$$b'_i(x_1,\ldots,x_d) \in (\mathfrak{m}^{p^r})^p\mathcal{S} = \mathfrak{m}^{p^{r+1}}\mathcal{S}$$

et que

$$pa'_i(x_1,\ldots,x_d) \in \mathfrak{m}^{e+p^r}\mathcal{S} \subset \mathfrak{m}^{p^{r+1}}\mathcal{S} ,$$

puisque $r \leq t-1$ implique $p^{r+1} - p^r \leq e$. On a donc $y_i \in \mathfrak{m}^{p^{r+1}}\mathcal{S}$, pour tout i, d'où le résultat.

4.6. Conservons les hypothèses et les notations du numéro précédent et soit $(\mathfrak{L}, M, \rho) = \mathfrak{L}M_{A'}(G)$.

Soit $x \in G(\mathcal{S})$; c'est un homomorphisme continu de $\mathfrak{R}$ dans $\mathcal{S}$ et il se prolonge de manière unique en un homomorphisme continu de $\hat{\mathfrak{R}}_K^{an}$ dans $\mathcal{S}_K$; par restriction à $\mathfrak{L}$, on obtient une application A'-linéaire $x_{\mathfrak{L}} : \mathfrak{L} \to \mathcal{S}_K$, i.e. un élément du groupe $N_{\mathfrak{L}}(\mathcal{S})$ défini au numéro précédent.

Notons $\varphi_G^{\mathfrak{L}}(\mathcal{S}) : G(\mathcal{S}) \to N_{\mathfrak{L}}(\mathcal{S})$ l'application qui à x associe $x_{\mathfrak{L}}$. Pour tout $\alpha \in \mathfrak{L}$, $\partial\alpha = 0$, par conséquent $\Delta\alpha = \alpha \hat{\otimes} 1 + 1 \hat{\otimes} \alpha$ et on en déduit que $\varphi_G^{\mathfrak{L}}(\mathcal{S})$ est un homomorphisme de groupes. En outre il est clair que $\varphi_G^{\mathfrak{L}}(\mathcal{S})$ est fonctorielle en $\mathcal{S}$ et en G.

Enfin, nous notons $N_{\mathfrak{L}}^1(\mathcal{S})$ le groupe des applications A'-linéaires de $\mathfrak{L}$ dans $\mathfrak{m}^{p^t}\mathcal{S}$. On a $N_{\mathfrak{L}}^1(\mathcal{S}) \subset N_{\mathfrak{L}}^0(\mathcal{S}) \subset N_{\mathfrak{L}}(\mathcal{S})$. Si $t = 0$, i.e. si $e < p-1$, on a $P'(\mathcal{S}) = \mathfrak{m}\mathcal{S}$ et $N^1_{\mathfrak{L}}(\mathcal{S}) = N^0_{\mathfrak{L}}(\mathcal{S})$.

PROPOSITION 4.6.- Soit G un p-groupe formel lisse et de dimension finie sur A' et soit $\mathcal{S}$ un A'-anneau p-adique. Si $x \in G(\mathfrak{m}^{p^t}\mathcal{S})$, alors $\varphi^{\mathfrak{L}}_G(\mathcal{S})(x) = x_{\mathfrak{L}} \in N^1_{\mathfrak{L}}(\mathcal{S})$ et l'application $\varphi^{\mathfrak{L}}_G(\mathcal{S})$ induit, par restriction, un isomorphisme de $G(\mathfrak{m}^{p^t}\mathcal{S})$ sur $N^1_{\mathfrak{L}}(\mathcal{S})$.

Démonstration : il est clair que l'inclusion de G^c dans G induit un isomorphisme de $\mathfrak{L}_{A'}(G)$ sur $\mathfrak{L}_{A'}(G^c)$. Comme $G(\mathfrak{m}^{p^t}\mathcal{S}) = G^c(\mathfrak{m}^{p^t}\mathcal{S})$, on voit que l'on peut supposer G connexe.

On voit que tout élément α de $P(\mathfrak{R})$ peut s'écrire (de manière non unique) sous la forme

$$\alpha = \sum_{i=0}^{e-1} \pi^i \left(\sum_{n=0}^{\infty} p^{-n} \alpha_{-n,i}^{p^n} \right) ,$$

où π est une uniformisante de A' et où les $\alpha_{-n,i} \in \mathfrak{R}$.

Soit $\alpha_1, \alpha_2, \dots, \alpha_d$ une base de $\mathfrak{L}$ sur A' et écrivons chaque α_j sous la forme

$$\alpha_j = \sum_{i=0}^{e-1} \pi^i \left(\sum_{n=0}^{\infty} p^{-n} (\alpha_{-n,i}^{(j)})^{p^n} \right)$$

avec les $\alpha_{-n,i}^{(j)} \in \mathfrak{R}$.

Il résulte facilement du fait que $\tilde{\rho}(G) : \mathfrak{L}/\mathfrak{m}\mathfrak{L} \to M/\underline{F}M$ est un isomorphisme que, si l'on pose $X_j = \alpha_{0,0}^{(j)}$, alors $X_1, X_2, \dots, X_d$ forment un système de coordonnées pour $\mathfrak{R}$, i.e. $\mathfrak{R} = A'[[X_1, X_2, \dots, X_d]]$ et les $\alpha_{-n,i}^{(j)}$ sont des séries formelles en les X_j, à coefficients dans A' . On voit que, quitte à changer les $\alpha_{0,1}^{(j)}$, on peut supposer que les X_j sont dans l'idéal d'augmentation. On doit alors avoir $\alpha_j(0,0,\dots,0) = 0$ et on en déduit facilement que l'on peut choisir les $\alpha_{-n,i}^{(j)}$ pour que ce soit des séries formelles sans terme constant (si $a_{-n,i}^{(j)} = \alpha_{-n,i}^{(j)}(0,\dots,0)$, il suffit de remplacer chaque $\Sigma p^{-n}(\alpha_{-n,i}^{(j)})^{p^n}$, qui est l'image par $\hat{w}_{\mathfrak{R}}$ du covecteur $\alpha_i^{(j)} = (\dots, \alpha_{-n,i}^{(j)}, \dots, \alpha_{0,i}^{(j)}) \in CW(\mathfrak{R})$, par $\hat{w}_{\mathfrak{R}}(\alpha_i^{(j)} - (\dots, a_{-n,i}^{(j)}, \dots, a_{0,i}^{(j)}))$).

LEMME 4.7.- Soit r un entier $\geq p^t$ et soit $b_1, b_2, \dots, b_d$ des éléments de $\mathfrak{m}^r\mathcal{S}$. Alors, pour $1 \leq j \leq d$,

$$\alpha_j(b_1, b_2, \dots, b_d) \equiv b_j \pmod{\mathfrak{m}^{r+1}\mathcal{S}} .$$

Démonstration du lemme : fixons l'entier j et posons

$b_{-n,i} = \alpha^{(j)}_{-n,i}(b_1,b_2,\dots,b_d)$ (en particulier, on a $b_{0,0} = b_j$). Comme $\alpha^{(j)}_{-n,i}(X_1,X_2,\dots,X_d)$ est une série formelle sans terme constant, $b_{-n,i} \in \mathfrak{m}^r\mathcal{S}$; on a donc $b^{p^n}_{-n,i} \in \mathfrak{m}^{rp^n}\mathcal{S}$ et $\pi^i p^{-n} b^{p^n}_{-n,i} \in \mathfrak{m}^{i-ne+rp^n}\mathcal{S}$. On a $i - ne + rp^n = r+i+r(p^n-1) - ne \geq r+i+(p^{n+t}-p^t-ne)$. Il suffit de vérifier que $i+(p^{n+t}-p^t-ne) \geq 1$, sauf si $i = n = 0$, ce qui ne présente pas de difficulté.

<u>Fin de la démonstration de la proposition</u> : pour tout entier $r \geq 1$, l'application qui à $x \in G(\mathfrak{m}^r\mathcal{S})$ associe le d-uple $(a_1,a_2,\dots,a_d)$, avec $a_j = x(X_j)$, définit une bijection entre $G(\mathfrak{m}^r\mathcal{S})$ et $(\mathfrak{m}^r\mathcal{S})^d$, et l'on voit que $x_L(\alpha_j) = \alpha_j(a_1,a_2,\dots,a_d)$.

En appliquant le lemme pour $r = p^t$ et $b_j = a_j$, on voit que si $x \in G(\mathfrak{m}^{p^t}\mathcal{S})$, on a bien $x_L \in N^1_L(\mathcal{S})$.

Comme $G(\mathfrak{m}^{p^t}\mathcal{S}) = \varprojlim G(\mathfrak{m}^{p^t}\mathcal{S})/G(\mathfrak{m}^r\mathcal{S})$, il suffit, pour démontrer la deuxième assertion de vérifier que, étant donné un d-uple $(a_1,a_2,\dots,a_d)$ d'éléments de $\mathfrak{m}^{p^t}\mathcal{S}$, il existe, pour tout entier positif r , un élément $x_r \in G(\mathfrak{m}^{p^t}\mathcal{S})$, uniquement déterminé modulo $G(\mathfrak{m}^{r+1}\mathcal{S})$ tel que $x_r(\alpha_j) \equiv a_j \pmod{\mathfrak{m}^{r+1}\mathcal{S}}$, pour tout j .

On procède par récurrence sur r :

- c'est clair si $r < p^t$.
- Supposons $r \geq p^t$ et soit $x_{r-1} \in G(\mathfrak{m}^{p^t}\mathcal{S})$ tel que $x_{r-1}(\alpha_j) \equiv a_j \pmod{\mathfrak{m}^r\mathcal{S}}$, pour tout j . Posons $x_{r-1}(\alpha_j) = a_j - b_j$. L'élément x_r cherché doit être de la forme $x_r = x_{r-1} + y$, avec $y \in G(\mathfrak{m}^r\mathcal{S})$. Comme $(x_{r-1}+y)(\alpha_j) = x_{r-1}(\alpha_j) + y(\alpha_j)$, on doit avoir $y(\alpha_j) \equiv b_j \pmod{\mathfrak{m}^{r+1}\mathcal{S}}$. Le lemme montre que pour cela il faut et il suffit que $y(X_j) \equiv b_j \pmod{\mathfrak{m}^{r+1}\mathcal{S}}$, ce qui montre l'existence et l'unicité de y , donc aussi de x_r , modulo $G(\mathfrak{m}^{r+1}\mathcal{S})$.

COROLLAIRE.- <u>Sous les hypothèses de la proposition 4.5,</u>

i) <u>le groupe</u> $G(\mathfrak{m}^{p^t}\mathcal{S})$ <u>est sans torsion</u> ;

ii) <u>le sous-groupe de torsion</u> $G_{tor}(\mathfrak{m}\mathcal{S})$ <u>de</u> $G(\mathfrak{m}\mathcal{S})$ <u>est le noyau de la restriction de</u> $\varphi^{\mathcal{L}}_G(\mathcal{S})$ <u>à</u> $G(\mathfrak{m}\mathcal{S})$ <u>et son exposant divise</u> p^t ;

iii) <u>le sous-groupe de torsion</u> $G_{tor}(\mathcal{S})$ <u>de</u> $G(\mathcal{S})$ <u>est le noyau de</u> $\varphi^{\mathcal{L}}_G(\mathcal{S})$.

Démonstration :

L'assertion i) est claire car $G(\mathfrak{m}^{p^t}\mathcal{S}) \simeq N^1_{\mathcal{L}}(\mathcal{S})$ qui est visiblement sans torsion.

Comme $N_{\mathcal{L}}(\mathcal{S})$ est sans torsion, $G_{tor}(\mathfrak{m}\mathcal{S})$ est contenu dans le noyau de la restriction de $\varphi^{\mathcal{L}}_G(\mathcal{S})$. Réciproquement, soit $x \in G(\mathfrak{m}\mathcal{S})$ tel que $x_{\mathcal{L}} = 0$. Il résulte de la proposition 4.4 que $p^t x \in G(\mathfrak{m}^{p^t}\mathcal{S})$; comme $(p^t x)_{\mathcal{L}} = p^t x_{\mathcal{L}} = 0$, on a $p^t x = 0$, d'où l'assertion ii).

On voit de même que $G_{tor}(\mathcal{S}) \subset \ker \varphi^{\mathcal{L}}_G(\mathcal{S})$. Réciproquement, soit $x \in \ker \varphi^{\mathcal{L}}_G(\mathcal{S})$, i.e. tel que $x_{\mathcal{L}} = 0$. Comme $G(\mathcal{S})/G(\mathfrak{m}\mathcal{S})$ est isomorphe à $G_k(\mathcal{S}_k)$ qui est un groupe de p-torsion, il existe un entier i tel que $p^i x \in G(\mathfrak{m}\mathcal{S})$. Comme $(p^i x)_{\mathcal{L}} = p^i x_{\mathcal{L}} = 0$, on a $p^t(p^i x) = p^{t+i}x = 0$ et $x \in G_{tor}(\mathcal{S})$.

4.7. Soit G un p-groupe formel lisse et de dimension finie sur A . Notons G^f le foncteur en groupes sur la catégorie des A'-anneaux p-adiques qui, à tout A'-anneau p-adique $\mathcal{S}$, associe le groupe $G^f(\mathcal{S}) = G(\mathcal{S})$. La correspondance $G \mapsto G^f$ peut être considérée, de manière évidente, comme un foncteur covariant additif de la catégorie des p-groupes formels lisses et de dimension finie sur A' dans celle des foncteurs en groupes sur les A'-anneaux p-adiques. On voit facilement que ce foncteur est pleinement fidèle et nous l'utilisons pour identifier la première de ces catégories à une sous-catégorie pleine de la seconde. Autrement dit, dans la suite nous écrivons G au lieu de G^f .

Pour tout p-groupe formel lisse et de dimension finie G sur A' , si $(\mathcal{L}, M, \rho) = \mathcal{L}M_{A'}(G)$, nous posons $\overline{G} = G_{(\mathcal{L}, M, \rho)}$. Nous nous proposons de construire deux morphismes de foncteurs en groupes

$$\varphi_G : G \to \overline{G} \qquad \text{et} \qquad \psi_G : \overline{G} \to G$$

tels que $\psi_G \circ \varphi_G = p^t \cdot \mathrm{id}_G$ et $\varphi_G \circ \psi_G = p^t \cdot \mathrm{id}_{\overline{G}}$.

Soit $\mathcal{S}$ un A'-anneau p-adique. On a défini au numéro précédent un homomorphisme $\varphi^{\mathcal{L}}_G(\mathcal{S}) : G(\mathcal{S}) \to N_{\mathcal{L}}(\mathcal{S})$. Si maintenant $x \in G(\mathcal{S})$, notons x_k son image dans $G_k(\mathcal{S}_k) = G(\mathcal{S})/G(\mathfrak{m}\mathcal{S})$. On sait (prop. 6.2 du chap. III) que le groupe $G_k(\mathcal{S}_k)$ s'identifie canoniquement (et fonctoriellement en $\mathcal{S}$) au groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(\mathcal{S}_k)) = G_M(\mathcal{S})$; notons x_M l'image de x_k dans $G_M(\mathcal{S})$ (rappelons que x_M est la restriction à M de $CW_k(x_k) : CW_k(\mathcal{R}_k) \to CW_k(\mathcal{S}_k)$).

L'application $\varphi_G^M(\mathfrak{S}) : G(\mathfrak{S}) \to G_M(\mathfrak{S})$ qui à x associe x_M est un homomorphisme de groupes.

PROPOSITION 4.8.- <u>Soit</u> G <u>un p-groupe formel lisse et de dimension finie sur</u> A' <u>et soit</u> $(\mathfrak{L}, M, \rho) = \mathfrak{L}M_{A'}(G)$. <u>Soit</u> $\mathfrak{S}$ <u>un A'-anneau p-adique. Pour tout</u> $x \in G(\mathfrak{S})$ <u>l'élément</u> $\varphi_G(\mathfrak{S})(x) = (x_{\mathfrak{L}}, x_M)$ <u>de</u> $N_{\mathfrak{L}}(\mathfrak{S}) \times G_M(\mathfrak{S})$ <u>appartient à</u> $\overline{G}(\mathfrak{S})$. <u>L'application</u> $\varphi_G(\mathfrak{S}) : G(\mathfrak{S}) \to \overline{G}(\mathfrak{S})$ <u>ainsi définie est un homomorphisme de groupes, fonctoriel en</u> $\mathfrak{S}$; <u>son noyau est le sous-groupe de torsion</u> $G_{tor}(\mathfrak{m}\mathfrak{S})$ <u>de</u> $G(\mathfrak{m}\mathfrak{S})$.

<u>Démonstration</u> : dire que $(x_{\mathfrak{L}}, x_M) \in \overline{G}(\mathfrak{S})$ revient à dire que le diagramme

$$\begin{tikzcd}
\mathfrak{L} \arrow[r, "x_{\mathfrak{L}}"] \arrow[d, "\rho"'] & \mathfrak{S}_K \arrow[dr, "\text{proj.}"] & \\
M_{A'} \arrow[r, "x_{M,A'}"] & CW_{k,A'}(\mathfrak{S}_k) \arrow[r, "w_{\mathfrak{S}}"'] & \mathfrak{S}_K/P'(\mathfrak{S})
\end{tikzcd}$$

est commutatif, ce qui résulte immédiatement des définitions.

Le fait que $\varphi_G(\mathfrak{S})$ est un homomorphisme de groupes (fonctoriel en $\mathfrak{S}$) résulte de ce que les applications $\varphi_G^{\mathfrak{L}}(\mathfrak{S})$ et $\varphi_G^M(\mathfrak{S})$ sont toutes les deux des homomorphismes de groupes (fonctoriels en $\mathfrak{S}$).

Enfin, le noyau de $\varphi_G(\mathfrak{S})$ est formé des $x \in G(\mathfrak{S})$ tels que $x_{\mathfrak{L}} = 0$ et $x_M = 0$. La deuxième condition est équivalente à $x_k = 0$, donc à $x \in G(\mathfrak{m}\mathfrak{S})$. Le corollaire à la proposition 4.6 montre alors que $x_{\mathfrak{L}} = 0$ équivaut à $x \in G_{tor}(\mathfrak{m}\mathfrak{S})$.

Construisons maintenant ψ_G : soit $u = (u_{\mathfrak{L}}, u_M) \in \overline{G}(\mathfrak{S})$. Soit $u_k \in G_k(\mathfrak{S}_k)$ l'image de u_M par l'isomorphisme canonique de $G_M(\mathfrak{S})$ sur $G_k(\mathfrak{S}_k)$. Choisissons un élément x de $G(\mathfrak{S})$ qui relève u_k (un tel élément existe toujours car G est lisse). Si $\varphi_G(\mathfrak{S})(x) = (x_{\mathfrak{L}}, x_M)$, on voit que $x_M = u_M$ et que $x_{\mathfrak{L}} \equiv u_{\mathfrak{L}} \pmod{P'(\mathfrak{S})}$ (i.e. que pour tout $\alpha \in \mathfrak{L}$, $x_{\mathfrak{L}}(\alpha) \equiv u_{\mathfrak{L}}(\alpha) \pmod{P'(\mathfrak{S})}$) puisque $(x_{\mathfrak{L}}, x_M) \in \overline{G}(\mathfrak{S})$.

On a $(p^t x)_{\mathfrak{L}} = p^t x_{\mathfrak{L}}$, donc $(p^t x)_{\mathfrak{L}} \equiv p^t u_{\mathfrak{L}} \pmod{p^t P'(\mathfrak{S})}$, d'où on déduit que $(p^t x)_{\mathfrak{L}} \equiv p^t u_{\mathfrak{L}} \pmod{\mathfrak{m}^{p^t}\mathfrak{S}}$ puisque $P'(\mathfrak{S}) \subset \mathfrak{m}^{p^t - te}\mathfrak{S}$. Autrement dit $(p^t x)_{\mathfrak{L}} - p^t u_{\mathfrak{L}} \in N^1_{\mathfrak{L}}(\mathfrak{S})$ et, d'après la proposition 4.6, il existe un élément

$y \in G(\mathfrak{m}^{p^t}\mathcal{S})$ et un seul tel que $y_{\mathcal{L}} = (p^t x)_{\mathcal{L}} - p^t u_{\mathcal{L}}$. Si l'on pose $z = p^t x - y$, on voit que $z_{\mathcal{L}} = (p^t x)_{\mathcal{L}} - y_{\mathcal{L}} = p^t u_{\mathcal{L}}$.

PROPOSITION 4.9.- Avec les hypothèses et les notations qui précèdent, l'élément $z \in G(\mathcal{S})$ ne dépend pas du choix du relèvement x de u_k . L'application $\psi_G(\mathcal{S}) : \overline{G}(\mathcal{S}) \to G(\mathcal{S})$ qui à $u = (u_{\mathcal{L}}, u_M)$ associe z est un homomorphisme de groupes, fonctoriel en $\mathcal{S}$. On a $\psi_G(\mathcal{S}) \circ \varphi_G(\mathcal{S}) = p^t . \mathrm{id}_G(\mathcal{S})$ et $\varphi_G(\mathcal{S}) \circ \psi_G(\mathcal{S}) = p^t . \mathrm{id}_{\overline{G}(\mathcal{S})}$.

Démonstration : soit x' un autre relèvement de x . On a $x' \equiv x$ $(\mathrm{mod}\ G(\mathfrak{m}\mathcal{S}))$ et, d'après la proposition 4.4, $p^t x' \equiv p^t x$ $(\mathrm{mod}\ G(\mathfrak{m}^{p^t}\mathcal{S}))$. Si y' est l'unique élément de $G(\mathfrak{m}^{p^t}\mathcal{S})$ tel que $(p^t x')_{\mathcal{L}} - y'_{\mathcal{L}} = p^t u_{\mathcal{L}}$, et si $z' = p^t x' - y'$, on a donc $z' - z = (p^t x' - p^t x) - y' + y \in G(\mathfrak{m}^{p^t}\mathcal{S})$ et $(z' - z)_{\mathcal{L}} = 0$, d'où $z' - z = 0$, ce qui prouve la première assertion.

Les autres assertions sont alors évidentes.

4.8. On a le résultat suivant qui généralise le théorème 1 :

THÉORÈME 2.- Si $e < p-1$, le foncteur $\mathcal{L}M_{A'}$ induit une anti-équivalence entre la catégorie des p-groupes formels lisses et de dimension finie sur A' et la catégorie $\Lambda^{\ell}_{A'}$.

La démonstration de ce théorème est entièrement analogue à celle du théorème 1. Donnons-en les grandes lignes :

soit G et G' deux p-groupes formels lisses et de dimension finie sur A' et soit $(\mathcal{L}, M, \rho) = \mathcal{L}M_{A'}(G)$, $(\mathcal{L}', M', \rho') = \mathcal{L}M_{A'}(G')$. Tout morphisme $\eta : (\mathcal{L}, M, \rho) \to (\mathcal{L}', M', \rho')$ induit de manière évidente un morphisme $\overline{\eta}^*$ de $\overline{G}' = G_{(\mathcal{L}', M', \rho')}$ dans $\overline{G} = G_{(\mathcal{L}, M, \rho)}$. Comme $e < p-1$, on a $t = 0$, et les morphismes $\psi_G : \overline{G} \to G$ et $\varphi_{G'} : G' \to \overline{G}'$ sont des isomorphismes. Si on pose $\eta^* = \psi_G \circ \overline{\eta}^* \circ \varphi_{G'} : G' \to G$, on vérifie immédiatement que $\mathcal{L}M_{A'}(\eta^*) = \eta$ et la pleine fidélité s'en déduit.

Il reste à vérifier que $\mathcal{L}M_{A'}$ est essentiellement surjectif. Pour cela, soit $(\mathcal{L}, M, \rho)$ un objet de $\Lambda^{\ell}_{A'}$. Choisissons un p-groupe formel lisse G_k sur k dont le module de Dieudonné $M_0 = \underline{M}(G_k)$ est isomorphe à M (un tel groupe existe et est unique, à isomorphisme près, d'après la prop. 6.1 du chap. III) ainsi qu'un isomorphisme i de M sur M_0 .

Soit R l'algèbre affine de G_k et choisissons un A'-anneau spécial $\mathfrak{R}$ qui relève R . Choisissons enfin un isomorphisme ι de $\mathfrak{L}$ sur un sous-A'-module $\mathfrak{L}_0$ de $P(\mathfrak{R})$ tel que le diagramme

$$\begin{tikzcd} \mathfrak{L} \arrow[r, "\iota"] \arrow[d, "\rho"'] & \mathfrak{L}_0 \arrow[r, hook] & P(\mathfrak{R}) \arrow[dr, "\text{proj.}"] & \\ M_{A'} \arrow[r, "i_{A'}"] & (M_0)_{A'} \arrow[r, hook] & CW_{k,A'}(\mathfrak{R}) \arrow[r, "w_{\mathfrak{R}}"'] & P(\mathfrak{R})/\mathfrak{m}\mathfrak{R} \end{tikzcd}$$

soit commutatif (rappelons que, comme $e \leq p-1$, on a $P'(\mathfrak{R}) = \mathfrak{m}\mathfrak{R}$). Enfin, notons ρ_0 l'application A'-linéaire $i_{A'} \circ \rho \circ \iota^{(-1)}$ de $\mathfrak{L}_0$ dans $(M_0)_{A'}$.

Pour tout A'-anneau p-adique $\mathfrak{S}$, notons $X_{\mathfrak{R}}(\mathfrak{S})$ l'ensemble des homomorphismes continus de $\mathfrak{R}$ dans $\mathfrak{S}$.

Si $x \in X_{\mathfrak{R}}(\mathfrak{S})$, x se prolonge, de manière unique, en un homomorphisme continu de $\hat{\mathfrak{R}}_K^{an}$ dans $\mathfrak{S}_K$; nous notons $x_{\mathfrak{L}_0}$ sa restriction à $\mathfrak{L}_0$ et $x_{\mathfrak{L}} : \mathfrak{L} \to \mathfrak{S}_K$ l'application A'-linéaire composée $x_{\mathfrak{L}_0} \circ \iota$.

De même x induit un homomorphisme continu $x_k : \mathfrak{R} \to \mathfrak{S}_k$ donc une application D_k-linéaire continue $CW_k(x_k)$ de $CW_k(\mathfrak{R})$ dans $CW_k(\mathfrak{S}_k)$; nous notons x_{M_0} sa restriction à M_0 et $x_M : M \to CW_k(\mathfrak{S}_k)$ l'application D_k-linéaire composée $x_{M_0} \circ i$. Il est clair que le théorème résulte alors du lemme suivant :

LEMME 4.10.- <u>Pour tout</u> $x \in X_{\mathfrak{R}}(\mathfrak{S})$, $(x_{\mathfrak{L}}, x_M) \in G_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$. <u>L'application</u> $x \to (x_{\mathfrak{L}}, x_M)$ <u>de</u> $X_{\mathfrak{R}}(\mathfrak{S})$ <u>dans</u> $G_{(\mathfrak{L},M,\rho)}(\mathfrak{S})$ <u>est bijective</u>.

Il s'agit d'une généralisation du lemme 1.3 et la démonstration se transpose sans difficulté.

<u>Remarque</u> : notons $\Lambda_{A'}^c$ (resp. $\Lambda_{A'}^u$) la sous-catégorie pleine de $\Lambda_{A'}^{\ell}$ dont les objets sont les triplets (L,M,ρ) , avec M "connexe" (resp. "unipotent") (cf. n° 1.2). Par une généralisation sans difficultés des raffinements utilisés pour $e = 1$ et $p = 2$, on démontre que, si $e = p-1$ (et, bien sûr, aussi si $e < p-1$), la restriction de $\mathfrak{L}M_{A'}$ à la catégorie des p-groupes formels lisses et connexes (resp. unipotents) de dimension finie sur A' induit une antiéquivalence entre cette catégorie et la catégorie $\Lambda_{A'}^c$ (resp. $\Lambda_{A'}^u$) .

4.9. Lorsque $e \geq p-1$, le foncteur $\mathfrak{L}M_{A'}$ n'est plus essentiellement surjectif, ni même, en général, pleinement fidèle. Toutefois, on a le résultat suivant :

PROPOSITION 4.11.- <u>Soit</u> G <u>et</u> G' <u>deux p-groupes formels lisses et de dimension finie sur</u> A' . <u>L'homomorphisme canonique du groupe</u> $\mathrm{Hom}(G',G)$ <u>dans</u> $\mathrm{Hom}(\mathcal{L}M_{A'}(G),\mathcal{L}M_{A'}(G'))$ <u>est injectif et son image contient</u> $p^t.\mathrm{Hom}(\mathcal{L}M_{A'}(G),\mathcal{L}M_{A'}(G'))$.

<u>Démonstration</u> : soit $\mathfrak{R}$ l'algèbre affine de G . Il est clair que si $\alpha \in P(\mathfrak{R})$, alors $d\alpha \in \Omega_{A'}(\mathfrak{R})$ (on a identifié le module des A'-différentielles continues $\Omega_{A'}(\mathfrak{R})$ de $\mathfrak{R}$ à un sous-module du module des K'-différentielles continues de l'anneau $\hat{\mathfrak{R}}_K^{an}$). Il résulte immédiatement de la proposition 4.2 et de l'isomorphisme canonique entre $\omega_{G/A'}$ et $t_G^*(A')$ (cf. prop. 8.1 du chap. I) que l'application qui à α associe $d\alpha$ induit, par restriction à $\mathcal{L}_{A'}(G)$, un isomorphisme de $\mathcal{L}_{A'}(G)$ sur $\omega_{G/A'}$; il est clair que cet isomorphisme est fonctoriel par rapport à G .

Soit alors f un morphisme de G' dans G et soit $f_k : G'_k \to G_k$ le morphisme induit sur les fibres spéciales. Supposons que

$$\mathcal{L}M_{A'}(f) = (\mathcal{L}(f),\underline{M}(f_k)) = 0 .$$

- Il résulte de ce qui précède que $\mathcal{L}(f) = 0$ implique que l'application A'-linéaire de $\omega_{G/A'}$ dans $\omega_{G'/A'}$ induite par f est nulle ; on en déduit facilement que le noyau de f contient la composante neutre G'^c de G' , donc que f se factorise à travers le quotient $G'^{et} = G'/G'^c$ qui est un groupe formel étale.
- Comme le foncteur $\underline{M}$ est fidèle, $\underline{M}(f_k) = 0$ implique $f_k = 0$; on en déduit facilement que l'image de f est contenue dans la composante neutre G^c de G .

On voit donc que f se factorise à travers un morphisme d'un groupe étale dans un groupe connexe et est donc bien nul.

Soit maintenant $\eta \in \mathrm{Hom}(\mathcal{L}M_{A'}(G),\mathcal{L}M_{A'}(G'))$ et soit $\overline{\eta}^*$ le morphisme de $\overline{G}'$ dans $\overline{G}$ induit par η ; si $\eta^* = \psi_G \circ \overline{\eta}^* \circ \varphi_{G'}$, on vérifie immédiatement que $\mathcal{L}M_{A'}(\eta^*) = p^t\eta$ et la deuxième assertion de la proposition s'en déduit.

<u>Remarque</u> : on peut montrer que, si $e \leq 2(p-1)$, la restriction de $\mathcal{L}M_{A'}$ à la catégorie des p-groupes formels lisses et connexes, de dimension finie sur A' , est pleinement fidèle. Ceci n'est plus vrai, en revanche, si $e \geq 2p-1$ (même

en se restreignant aux groupes p-divisibles).

§5.- Groupes p-divisibles sur A' .

On conserve les hypothèses et les notations des trois paragraphes précédents.

5.1. Notons $H^{\ell}_{A'}$ la catégorie dont les objets sont les couples (L, M)

- où M est un D_k-module profini sur lequel l'action de $\underline{F}$ est injective, tel que le quotient $M/\underline{F}M$ est un espace vectoriel de dimension finie sur k ;
- où L est un sous-A'-module de $M_{A'}$ tel que l'application de $L/\mathfrak{m}L$ dans $M_{A'}/M_{A'}[1]$ ($\simeq M/\underline{F}M$) déduite, par passage aux quotients, de l'inclusion de L dans $M_{A'}$ est un isomorphisme.

Un morphisme $u : (L,M) \to (L',M')$ de la catégorie $H^{\ell}_{A'}$ est une application D_k-linéaire continue de M dans M' telle que $u_{A'}(L) \subset L'$ (où $u_{A'} : M_{A'} \to M'_{A'}$ est l'application déduite de u par fonctorialité).

Il est clair que la catégorie $H^{\ell}_{A'}$ est additive.

Nous notons $H^{d}_{A'}$ la sous-catégorie pleine de $H^{\ell}_{A'}$ dont les objets sont les couples (L,M) tels que M est libre de rang fini sur A et L est libre sur A' (si $e \leq p-1$, $M_{A'}$ est sans torsion et la deuxième assertion résulte de la première).

Si G est un p-groupe formel lisse et de dimension finie sur A' , nous notons $L_{A'}(G)$ l'image de $\mathcal{L}_{A'}(G)$ dans $M_{A'}(G_k)$ par l'application $\rho(G)$. Il résulte du n° 4.3 que le couple $LM_{A'}(G) = (L_{A'}(G), \underline{M}(G_k))$ est un objet de $H^{\ell}_{A'}$. On peut, en fait, de manière évidente, considérer $LM_{A'}$ comme un foncteur contravariant additif de la catégorie des p-groupes formels lisses et de dimension finie sur A' dans $H^{\ell}_{A'}$.

PROPOSITION 5.1.- Si G est un groupe p-divisible sur A' , $LM_{A'}(G)$ est un objet de $H^{d}_{A'}$. De plus

i) si $e < p-1$, la restriction de $LM_{A'}$ à la catégorie des groupes p-divisibles sur A' induit une anti-équivalence entre cette catégorie et $H^{d}_{A'}$;

ii) <u>si</u> G <u>et</u> G' <u>sont deux groupes p-divisibles sur</u> A' , <u>l'homomorphisme canonique de</u> $\mathrm{Hom}(G',G)$ <u>dans</u> $\mathrm{Hom}(LM_{A'}(G), LM_{A'}(G'))$ <u>est injectif et son image contient</u> $p^t\mathrm{Hom}(LM_{A'}(G), LM_{A'}(G'))$.

<u>Démonstration</u> : si G est un groupe p-divisible sur A' , G_k est un groupe p-divisible sur k et $\underline{M}(G_k)$ est un A-module libre de rang fini (prop. 6.1 du chap. III). On voit alors que montrer que $LM_{A'}(G)$ est un objet de $H^d_{A'}$ revient à vérifier que l'application $\rho(G)$ est injective. Si elle ne l'était pas, on voit que l'on pourrait trouver un élément non nul $\alpha \in P'(\mathfrak{R})$ tel que $\partial\alpha = \alpha \hat{\otimes} 1 + 1 \hat{\otimes} \alpha$. On voit que, quitte à multiplier α par une puissance convenable d'une uniformisante de A' , on peut supposer que $\alpha \in \mathfrak{R}$ et $\alpha \notin \mathfrak{m}\mathfrak{R}$. L'image de α dans l'algèbre affine de G_k définirait un homomorphisme non nul de G_k dans le groupe additif, ce qui n'est pas possible puisque G_k est p-divisible.

L'assertion (i) résulte alors trivialement du théorème 2 (n° 4.8) et l'assertion (ii) de la proposition 4.11.

5.2. Soit $K[\underline{F},\underline{V}]$ l'anneau (non commutatif si $k \neq \underline{F}_p$) $K\otimes_A D_k = K\otimes_A A[\underline{F},\underline{V}]$. Si M est un D_k-module, le K-espace vectoriel $M_K = K\otimes_A M$ est, de manière évidente, un $K[\underline{F},\underline{V}]$-module à gauche ; la correspondance $M \mapsto M_K$ est fonctorielle.

Notons $H^d_{K'}$ la catégorie dont les objets sont les couples $(L_{K'}, M_K)$

- où M_K est un $K[\underline{F},\underline{V}]$-module à gauche qui est un espace vectoriel de dimension finie sur le corps K ;
- où $L_{K'}$ est un sous-K'-espace vectoriel de $M_{K'} = K'\otimes_K M_K$. Un morphisme $u : (L_{K'}, M_K) \to (L'_{K'}, M'_K)$ de la catégorie $H^d_{K'}$ est une application $K[\underline{F},\underline{V}]$-linéaire de M_K dans M'_K telle que $u_{K'}(L_{K'}) \subset L'_{K'}$ (on a noté $u_{K'} : M_{K'} \to M'_{K'}$ l'application déduite de u par extension des scalaires).

Il est clair que $H^d_{K'}$ est une catégorie additive.

Enfin, on a un foncteur additif évident de la catégorie $H^d_{A'}$ dans $H^d_{K'}$: à tout objet (L,M) de $H^d_{A'}$, on associe le couple $(L_{K'}, M_K)$

- où $M_K = K\otimes_A M$;
- et où $L_{K'}$ est l'image dans $M_{K'} = K'\otimes_K M_K$ de $K'\otimes_{A'} L$ (d'après la propo-

sition 2.1, $M_{K'}$ s'identifie canoniquement à $K'\otimes_{A'} M_{A'}$).

En composant la restriction de $LM_{A'}$ à la catégorie des groupes p-divisibles sur A' avec ce foncteur, on obtient un foncteur contravariant additif $LM_{K'}$ de la catégorie des groupes p-divisibles sur A' dans $H^d_{K'}$.

PROPOSITION 5.2.- <u>Soit</u> G <u>et</u> G' <u>deux groupes p-divisibles sur</u> A' . <u>L'homomorphisme canonique de</u> $\mathrm{Hom}(G',G)$ <u>dans</u> $\mathrm{Hom}(LM_{K'}(G),LM_{K'}(G'))$ <u>est injectif et induit, par extension des scalaires, un isomorphisme de</u> $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathrm{Hom}(G',G)$ <u>dans</u> $\mathrm{Hom}(LM_{K'}(G),LM_{K'}(G'))$ (<u>autrement dit</u> $LM_{K'}$, <u>considéré comme un foncteur contravariant de la catégorie des groupes p-divisibles sur</u> A' "<u>à isogénies près" dans</u> $H^d_{K'}$, <u>est pleinement fidèle</u>).

<u>Démonstration</u> : il est immédiat que $\mathrm{Hom}(LM_{A'}(G),LM_{A'}(G'))$ est un $\mathbb{Z}_p$-module sans torsion et que $\mathrm{Hom}(LM_{K'}(G),LM_{K'}(G'))$ s'identifie canoniquement à $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathrm{Hom}(LM_{A'}(G),LM_{A'}(G'))$. La proposition résulte alors de l'assertion (ii) de la proposition 5.1.

5.3. Soit G un groupe p-divisible sur A' . Nous allons donner une interprétation de $LM_{K'}(G) = (L_{K'}(G),M_K(G))$ en terme de "fonctions analytiques".

Soit $\mathfrak{R}$ l'algèbre affine de G . Il est clair que $K\otimes_A\mathfrak{R} = K'\otimes_{A'}\mathfrak{R}$ (resp. $K\otimes_A(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}) = K'\otimes_{A'}(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$) s'identifie au sous-anneau de $\hat{\mathfrak{R}}^{an}_K$ (resp. $(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})^{an}_K$) formé des α tels que $p^n\alpha\in\mathfrak{R}$ (resp. $\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}$) pour n assez grand. On voit que l'on a aussi $K'\otimes_{A'}\mathfrak{R} = K'\otimes_{A'}P'(\mathfrak{R})$ et $K'\otimes_{A'}(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R}) = K'\otimes_{A'}P'(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$.

En reprenant les notations du n° 4.1, on voit alors que

$$\mathfrak{M}\mathfrak{H}^{an}_{K'}(G) = K'\otimes_{A'}\mathfrak{M}\mathfrak{H}_{A'}(G)$$

s'identifie au sous-K'-espace vectoriel de $\hat{\mathfrak{R}}^{an}_K$ formé des $\alpha\in K'\otimes_{A'}P(\mathfrak{R})$ tels que $\partial\alpha\in K'\otimes_{A'}(\mathfrak{R}\hat{\otimes}_{A'}\mathfrak{R})$ et que $K'\otimes_{A'}MH_{A'}(G)$ s'identifie au quotient $MH^{an}_{K'}(G)$ de $\mathfrak{M}\mathfrak{H}^{an}_{K'}(G)$ par $K'\otimes_{A'}\mathfrak{R}$. Il est clair que l'isomorphisme de $M_{A'}(G_k)$ sur $MH_{A'}(G)$ défini au n° 4.1 induit, par extension des scalaires, un isomorphisme de $M_{K'}(G) = K'\otimes_K M_K(G) = K'\otimes_{A'}M_{A'}(G_k)$ sur $MH^{an}_{K'}(G)$.

Si l'on note $\mathfrak{L}^{an}_{K'}(G)$ le K'-espace vectoriel formé des $\alpha\in K'\otimes_{A'}P(\mathfrak{R})$ tels que $\partial\alpha = 0$ et $L^{an}_{K'}(G)$ l'image de $\mathfrak{L}^{an}_{K'}(G)$ dans $MH^{an}_{K'}(G)$, on voit tout de suite que $L_{K'}^{an}(G)$ est aussi l'image de $L_{K'}(G)$ par l'isomorphisme canonique de $M_{K'}(G)$ sur $MH_{K'}^{an}(G)$.

Montrons, pour terminer, que, dans la définition de $MH_{K'}^{an}(G)$ et de $L_{K'}^{an}(G)$, on peut remplacer $K' \otimes_{A'} P(\mathfrak{R})$ par $\hat{\mathfrak{R}}_K^{an}$. Plus précisément :

PROPOSITION 5.3.- <u>Soit</u> G <u>un groupe p-divisible sur</u> A' <u>et soit</u> $\mathfrak{R}$ <u>son algèbre affine. Si</u> $\alpha \in \hat{\mathfrak{R}}_K^{an}$ <u>vérifie</u> $\partial\alpha \in K' \otimes_{A'} (\mathfrak{R} \hat{\otimes}_{A'} \mathfrak{R})$, <u>alors</u> $\alpha \in K' \otimes_{A'} P(\mathfrak{R})$.

<u>Démonstration</u> : il est clair qu'il existe un entier n tel que $\partial(p^n\alpha) \in \mathfrak{R} \hat{\otimes}_{A'} \mathfrak{R} \subset P'(\mathfrak{R} \hat{\otimes}_{A'} \mathfrak{R})$. Avec les notations du n° 4.2, on voit que $\partial(p^n\alpha)$ est un tenseur symétrique de $P'(\mathfrak{R} \hat{\otimes}_{A'} \mathfrak{R})$ vérifiant $\partial^2(\partial(p^n\alpha)) = 0$. D'après le lemme 4.3, il existe donc $\gamma \in P(\mathfrak{R})$ tel que $\partial\gamma = \partial(p^n\alpha)$. Quitte à remplacer α par $\alpha - p^{-n}\gamma$, on voit que l'on peut supposer que $\partial\alpha = 0$.

Soit alors $\varepsilon : \mathfrak{R} \to A'$ l'homomorphisme d'augmentation et soit $\varepsilon_K : \hat{\mathfrak{R}}_K^{an} \to K'$ son prolongement à $\hat{\mathfrak{R}}_K^{an}$. Soit I le noyau de ε et I_K celui de ε_K . On voit facilement que $\partial\alpha = 0$ implique que $\alpha \in I_K$ et que l'application qui à $\beta \in \mathfrak{L}_{K'}^{an}(G)$ associe son image modulo I_K^2 définit un isomorphisme de $\mathfrak{L}_{K'}^{an}(G)$ sur I_K/I_K^2 . Pour achever la démonstration, il suffit donc d'établir le lemme suivant :

LEMME 5.4.- <u>Soit</u> $\alpha \in I_K^2$. <u>Si</u> $\partial\alpha = 0$, <u>alors</u> $\alpha = 0$.

<u>Démonstration</u> : il est clair que I/I^2 est un A'-module libre de rang la dimension d de G et que I_K/I_K^2 s'identifie à $K' \otimes_{A'} (I/I^2)$. Soit $X_1, X_2, \ldots, X_d$ des éléments de $\mathfrak{R}$ qui relèvent une base de I/I^2 . On voit facilement que, pour tout entier $r \geq 1$, I_K^r/I_K^{r+1} s'identifie à l'espace vectoriel des polynômes homogènes de degré r en les X_i à coefficients dans K' et que $\Delta X_i \equiv X_i \hat{\otimes} 1 + 1 \hat{\otimes} X_i \pmod{I_K \hat{\otimes} I_K}$. Il résulte alors facilement de la proposition 10.4 du chapitre I que si $r \geq 2$ est tel que $\alpha \in I_K^r$, alors $\alpha \in I_K^{r+1}$; autrement dit $\alpha \in \bigcap_{r \in \mathbb{N}} I_K^r$.

Notons $\mathfrak{R}^0$ le facteur local de $\mathfrak{R}$ correspondant à l'élément-neutre et $(\hat{\mathfrak{R}}_K^{an})^0$ la composante de $\hat{\mathfrak{R}}_K^{an}$ correspondante. Il est clair que $\alpha \in \bigcap I_K^r$ revient à dire que la composante α^0 de α dans $(\hat{\mathfrak{R}}_K^{an})^0$ est nulle.

Soit A_C l'anneau des entiers du complété C d'une clôture algébrique de K' . Pour tout $x \in G(A_C) = \mathrm{Hom}^{cont}(\mathfrak{R}, A_C)$, notons $x_K : \hat{\mathfrak{R}}_K^{an} \to C$ l'application qui prolonge x . Il est clair que l'application qui à $x \in G(A_C)$ associe $x(\alpha)$ définit un homomorphisme de $G(A_C)$ dans le groupe additif de C. Pour tout $x \in G(A_C)$, il existe un entier n tel que $p^n x \in G^c(A_C)$, autrement dit tel que l'application $p^n x$ se factorise à travers la projection de $\mathfrak{R}$ sur $\mathfrak{R}^0$; on a alors $(p^r x)_K(\alpha) = 0$ (puisque $\alpha^0 = 0$), donc $p^r . x_K(\alpha) = 0$, d'où $x_K(\alpha) = 0$, pour tout $x \in G(A_C)$. On en déduit facilement que ceci implique que $\alpha = 0$.

<u>Remarque</u> : soit A_C l'anneau des entiers du complété C d'une clôture algébrique de K'. Soit G un groupe p-divisible sur A' et soit N l'unique sous-schéma en groupes fermé fini et plat de G tel que $N(A_C) = G_{tor}(mA_C)$. On a un diagramme commutatif

$$\begin{array}{ccccccc}
0 \to & N(A_C) & \to & G(A_C) & \to & (G/N)(A_C) & \to 0 \\
& \| & & \| & & & \\
0 \to & G_{tor}(mA_C) & \to & G(A_C) & \to & \overline{G}(A_C) &
\end{array}$$

dont les lignes sont exactes. Comme $(G/N)(A_C)$ est un groupe p-divisible (au sens élémentaire) et comme $p^t\overline{G}(A_C)$ est contenu dans l'image de $G(A_C)$, on voit que $(G/N)(A_C) = p^t\overline{G}(A_C)$. La connaissance de $LM_{A'}(G)$ détermine donc $(G/N)(A_C)$, donc aussi, d'après le théorème de pleine fidélité de Tate, le groupe p-divisible G/N.

CHAPITRE V

COMPLÉMENTS

§ 1.- Le module de Tate.

On conserve les notations des chapitres III et IV. On note B un anneau qui est soit k, soit A' (ce qui comprend le cas $B = A = W(k)$ lorsque $e = 1$). On note C le complété d'une clôture algébrique $\overline{K}'$ de K' et A_C l'anneau des entiers de C.

1.1. Soit G un groupe p-divisible sur B et soit R son algèbre affine. Pour tout B-anneau topologique S, on note $G(S)$ le groupe des homomorphismes continus du B-anneau R dans S et $G_{tor}(S)$ son sous-groupe de torsion. On voit que $G(S)$ s'identifie à $\varprojlim G(S)/p^nG(S)$, ce qui permet de considérer $G(S)$ et $G_{tor}(S)$ comme des $\mathbb{Z}_p$-modules. Nous posons

$$\begin{cases} \underline{T}(G)(S) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, G(S)) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, G_{tor}(S)) \ , \\ \underline{U}_0(G)(S) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, G_{tor}(S)) \ , \\ \underline{U}(G)(S) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, G(S)) \ . \end{cases}$$

Si, pour tout $u \in \underline{U}(G)(S)$, on pose $u(p^{-n}) = u_n$, cela permet de considérer u comme une suite $(u_0, u_1, \dots, u_n, \dots)$ d'éléments de $G(S)$ vérifiant $pu_{n+1} = u_n$. On voit que $\underline{U}_0(G)(S)$ (resp. $\underline{T}(G)(S)$) s'identifie au sous-$\mathbb{Z}_p$-module de $\underline{U}(G)(S)$ formé des u tels que $u_0 \in G_{tor}(S)$ (resp. $u_0 = 0$). On voit aussi que $\underline{U}_0(G)(S)$ s'identifie canoniquement à $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \underline{T}(G)(S)$.

L'application, qui à u associe u_0, définit un homomorphisme de $\underline{U}(G)(S)$ (resp. $\underline{U}_0(G)(S)$) dans $G(S)$ (resp. $G_{tor}(S)$) dont le noyau est $\underline{T}(G)(S)$, d'où un diagramme commutatif

$$\begin{tikzcd} 0 \arrow[r] & \underline{T}(G)(S) \arrow[r] \arrow[d, equal] & \underline{U}_0(G)(S) \arrow[r] \arrow[d, hook] & G_{tor}(S) \arrow[d, hook] \\ 0 \arrow[r] & \underline{T}(G)(S) \arrow[r] & \underline{U}(G)(S) \arrow[r] & G(S) \end{tikzcd}$$

dont les lignes sont exactes. Lorsque $G(S)$ est un groupe p-divisible (au sens élémentaire !), l'application $u \to u_o$ est surjective. C'est en particulier le cas lorsque $B = A'$ et $S = A_C$, auquel cas nous posons $T(G) = \underline{T}(G)(A_C)$, $U_0(G) = \underline{U}_0(G)(A_C)$, $U(G) = \underline{U}(G)(A_C)$; les lignes du diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(G) & \longrightarrow & U_0(G) & \longrightarrow & G_{tor}(A_C) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T(G) & \longrightarrow & U(G) & \longrightarrow & G(A_C) & \longrightarrow & 0 \end{array}$$

sont alors exactes. On sait que $T(G)$, qui est le <u>module de Tate</u> de G, est un $\mathbb{Z}_p$-module libre de rang fini égal à la hauteur h de G et que, par conséquent, $U_0(G)$ est un espace vectoriel sur $\mathbb{Q}_p$ de dimension h.

<u>Remarques</u> :

1.- Il est clair que les constructions de $\underline{T}(G)(S)$, $\underline{U}_0(G)(S)$ et $\underline{U}(G)(S)$ sont, de manière évidente, fonctorielles en G et en S.

Soit $\varphi : G \to G'$ une isogénie de groupes p-divisibles sur B et soit N son noyau. On voit facilement que, pour tout S, les applications $\underline{U}_0(G)(S) \to \underline{U}_0(G')(S)$ et $\underline{U}(G)(S) \to \underline{U}(G')(S)$ sont des isomorphismes et que la suite exacte des $\mathrm{Ext}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, -)$ donne une suite exacte

$$0 \longrightarrow \underline{T}(G)(S) \longrightarrow \underline{T}(G')(S) \longrightarrow N(S) \longrightarrow 0$$

(l'application de $\underline{T}(G')(S)$ dans $N(S)$ peut se définir ainsi : comme $G \to G'$ est une isogénie, il existe un entier r tel que $p^r G'(S) \subset \mathrm{Im}\, \varphi(S)$; on en déduit que si $u = (u_0, \dots, u_n, \dots) \in \underline{T}(G')(S)$, les u_n sont tous dans l'image de $\varphi(S)$; si $\hat{u}_n$ est un relèvement dans $G(S)$ de u_n, l'image de u dans $N(S)$ est l'image de $p^n \hat{u}_n$ pour n suffisamment grand).

2.- Soit G un groupe p-divisible sur A' et soit $G_k = G \otimes_{A'} k$ sa fibre spéciale. Soit $\mathcal{S}$ un A'-anneau p-adique et soit $\mathcal{S}_k = \mathcal{S} \otimes_{A'} k = \mathcal{S}/\mathfrak{m}\mathcal{S}$. Notons $u \to \tilde{u}$ l'application canonique de $G(\mathcal{S})$ dans $G_k(\mathcal{S}_k)$. Elle induit un homomorphisme de $\underline{U}(G)(\mathcal{S})$ dans $\underline{U}(G_k)(\mathcal{S}_k)$ qui est, en fait, un isomorphisme :

- cet homomorphisme est injectif : si $u = (u_0, \dots, u_n, \dots)$ est un élément non nul de $\underline{U}(G)(\mathcal{S})$, il existe un entier m tel que $u_m \neq 0$; si $\mathcal{R}$ est l'algèbre affine de G et $\mathcal{R}^+$ l'idéal d'augmentation, on en déduit qu'il existe un entier r tel que $u_m(\mathcal{R}^+) \not\subset \mathfrak{m}^{r+1}\mathcal{S}$; on voit facilement que cela implique que, pour $i \leq r$, $u_{m+i}(\mathcal{R}^+) \not\subset \mathfrak{m}^{r+1-i}\mathcal{S}$; on a donc $u_{m+r}(\mathcal{R}^+) \not\subset \mathfrak{m}\mathcal{S}$, d'où $\tilde{u}_{m+r} \neq 0$ et l'image de u dans $\underline{U}(G_k)(\mathcal{S}_k)$ n'est pas nulle.

- cet homomorphisme est surjectif : si $t = (t_0, \dots, t_n, \dots) \in \underline{U}(G_k)(\mathcal{S}_k)$, choisissons, pour tout n , un élément $\hat{t}_n \in G(\mathcal{S})$ qui relève t_n (c'est toujours possible car G est lisse) ; on voit que $(p\hat{t}_{n+1} - \hat{t}_n)(\mathfrak{R}^+) \subset \mathfrak{m}\mathcal{S}$ et on en déduit facilement que, pour tout entier n fixé, la suite des $p^m \hat{t}_{n+m}$ converge dans le groupe $G(\mathcal{S})$ (qui est séparé et complet pour la topologie p-adique) ; si on note u_n la limite de cette suite, on voit que $u = (u_0, \dots, u_n, \dots)$ est un élément de $\underline{U}(G)(\mathcal{S})$ qui relève t .

Ce résultat nous permettra d'identifier $\underline{U}_0(G)(\mathcal{S})$ et $\underline{T}(G)(\mathcal{S})$ à des sous-$\mathbb{Z}_p$-modules de $\underline{U}(G_k)(\mathcal{S}_k)$.

1.2. Soit G un groupe p-divisible sur k et soit S un k-anneau (quelconque, mais muni de la topologie discrète). On voit que $G(S)$ est un groupe de p-torsion et on a donc $\underline{U}(G)(S) = \underline{U}_0(G)(S)$.

Pour tout entier $n \geq 0$, soit G_n le noyau de la multiplication par p^n dans G . Il est clair que $\underline{T}(G)(S)$ s'identifie à $\varprojlim G_n(S)$, la flèche de $G_{n+1}(S)$ dans $G_n(S)$ étant la multiplication par p , et que $\underline{U}(G)(S)$ s'identifie à $\varprojlim G_{(n)}(S)$, où l'on a posé $G_{(n)}(S) = G(S)$, pour tout entier $n \geq 0$, et où la flèche de $G_{(n+1)}(S)$ dans $G_{(n)}(S)$ est la multiplication par p .

Soit $M = \underline{M}(G)$ le module de Dieudonné de G . La structure de D_k-module à gauche sur M se prolonge, de manière évidente, en une structure de D_k-module sur $K \otimes_A M$. L'identification de M à un sous-D_k-module de $K \otimes_A M$ permet d'identifier $K \otimes_A M$ à $\varinjlim p^{-n}M$, et la multiplication par p^n définit un isomorphisme de $p^{-n}M$ sur M . La proposition 6.2 du chapitre III implique donc le résultat suivant :

PROPOSITION 1.1.- <u>Soit</u> G <u>un groupe</u> p-<u>divisible sur</u> k <u>et soit</u> $M = \underline{M}(G)$. <u>Soit</u> S <u>un</u> k-<u>anneau</u>. <u>Alors</u> $\underline{U}(G)(S) = \underline{U}_0(G)(S)$ (<u>resp</u>. $\underline{T}(G)(S)$) <u>s'identifie canoniquement</u>, <u>et fonctoriellement en</u> S <u>et en</u> G , <u>au</u> $\mathbb{Q}_p$-<u>espace vectoriel</u> (<u>resp</u>. <u>au</u> $\mathbb{Z}_p$-<u>module</u>) $\mathrm{Hom}_{D_k}(K \otimes_A M, CW_k(S))$ (<u>resp</u>. $\mathrm{Hom}_{D_k}((K \otimes_A M)/M, CW_k(S))$) <u>des applications</u> D_k-<u>linéaires de</u> $K \otimes_A M$ (<u>resp</u>. $(K \otimes_A M)/M$) <u>dans</u> $CW_k(S)$.

1.3. Nous allons maintenant donner une autre description de $\underline{T}(G)(S)$ et de $\underline{U}(G)(S)$, lorsque G est un groupe p-divisible sur k et S un k-anneau, qui peut paraître plus compliquée, mais qui devrait être plus commode pour certaines applications.

Pour cela, commençons par introduire les "bivecteurs de Witt". Soit Λ un anneau commutatif quelconque. Pour tout entier $m \geq 0$, posons $CW_m(\Lambda) = CW(\Lambda)$ et $BW(\Lambda) = \varprojlim CW_m(\Lambda)$, l'application de $CW_{m+1}(\Lambda)$ dans $CW_m(\Lambda)$ étant définie par

$$(\dots, a_{-n}, \dots, a_{-1}, a_0) \longmapsto (\dots, a_{-n-1}, \dots, a_{-2}, a_{-1})$$

(autrement dit, c'est le décalage).

On voit que BW peut être considéré comme un foncteur covariant de la catégorie des anneaux commutatifs dans celle des groupes abéliens. Il résulte de la définition de $CW(\Lambda)$ que $BW(\Lambda)$ s'identifie, en tant qu'ensemble, à l'ensemble des "bivecteurs"

$$(\dots, a_{-n}, \dots, a_{-1}, a_0, a_1, \dots, a_m, \dots) = (a_n)_{n \in \mathbb{Z}}$$

où les a_n, pour $n \in \mathbb{Z}$, sont dans Λ et vérifient la condition

$$(\psi) \quad \begin{cases} \underline{\text{il existe un entier}}\ n_0\ \underline{\text{et un idéal nilpotent}}\ \mathfrak{a}\ \underline{\text{de}}\ \Lambda\ \underline{\text{tel que}} \\ a_n \in \mathfrak{a}\ \ \underline{\text{si}}\ \ n \leq n_0 . \end{cases}$$

Si maintenant Λ est un k-anneau, on voit que $BW(\Lambda)$ peut encore être considéré comme un D_k-module : si $\underline{a} = (\dots, a_{-n}, \dots, a_0, \dots, a_m, \dots) \in BW(\Lambda)$, on a

$$\underline{F\,a} = (\dots, a_{-n}^p, \dots, a_0^p, \dots, a_m^p, \dots) ,$$

$$\underline{V\,a} = (\dots, a_{-n-1}, \dots, a_{-1}, \dots, a_{m-1}, \dots) ,$$

$$[\lambda]\,\underline{a} = (\dots, \sigma^{-n}(\lambda)a_{-n}, \dots, \lambda a_0, \dots, \sigma^m(\lambda)a_m, \dots) , \text{ pour tout } \lambda \in k .$$

Enfin, si Λ est un k-anneau linéairement topologisé, séparé et complet, on pose $BW(\Lambda) = \varprojlim BW(\Lambda/\mathfrak{a})$, pour $\mathfrak{a}$ parcourant les idéaux ouverts de Λ ; les éléments de $BW(\Lambda)$ peuvent encore se représenter, de manière évidente, comme des covecteurs.

Nous allons d'autre part associer à tout anneau S de caractéristique p, un anneau parfait $\mathcal{K}(S)$, linéairement topologisé, séparé et complet, de la manière suivante :

> pour tout entier $r \in \mathbb{N}$, on pose $S_r = S$, et $\mathcal{K}(S) = \varprojlim S_r$, l'application de S_{r+1} dans S_r étant l'élévation à la puissance p-ième (la topologie de $\mathcal{K}(S)$ est la topologie de la limite projective, chaque S_r étant muni de la topologie discrète).

On voit qu'un élément x de $\mathcal{K}(S)$ peut se représenter comme une suite $x = (x_0, x_1, \ldots, x_r, \ldots)$ d'éléments de S vérifiant $x_{r+1}^p = x_r$, et que l'addition et la multiplication se font alors "composante par composante".

On voit que si S est un k-anneau, $\mathcal{K}(S)$ devient un k-anneau parfait, linéairement topologisé, séparé et complet, en posant, pour tout $\lambda \in k$ et tout $x = (x_0, x_1, \ldots, x_r, \ldots) \in \mathcal{K}(S)$,

$$\lambda x = (\lambda x_0, \sigma^{-1}(\lambda)x_1, \ldots, \sigma^{-r}(\lambda)x_r, \ldots) .$$

Si $\underline{a} = (\ldots, a_{-n}, \ldots, a_0, \ldots, a_m, \ldots) \in BW(\mathcal{K}(S))$, alors, pour tout $m \in \mathbb{Z}$, a_m peut s'écrire $a_m = (a_{m,0}, a_{m,1}, \ldots a_{m,r}, \ldots)$, avec les $a_{m,r}$ dans S et $a_{m,r+1}^p = a_{m,r}$. Nous notons η_0 l'application de $BW(\mathcal{K}(S))$ dans $CW_k(S)$ qui à $\underline{a} = (a_m)_{m\in\mathbb{Z}} \in BW(\mathcal{K}(S))$ associe $(\ldots, a_{-n,0}, \ldots, a_{-1,0}, a_{0,0})$. Il est clair que η_0 est D_k-linéaire et nous notons $BW_0(\mathcal{K}(S))$ son noyau.

PROPOSITION 1.2.- <u>Soit</u> G <u>un groupe</u> p-<u>divisible sur</u> k <u>et soit</u> $M = \underline{M}(G)$. <u>Soit</u> S <u>un</u> k-<u>anneau</u>. <u>Alors</u> $\underline{U}(G)(S)$ (<u>resp</u>. $\underline{T}(G)(S)$) <u>s'identifie canoniquement</u> (<u>et fonctoriellement en</u> S <u>et</u> G) <u>à</u> $\mathrm{Hom}_{D_k}(M, BW(\mathcal{K}(S)))$ (<u>resp</u>. $\mathrm{Hom}_{D_k}(M, BW_0(\mathcal{K}(S)))$).

<u>Démonstration</u> : pour tout $r \in \mathbb{N}$, posons $V_r(S) = CW_k(S)$ et soit $V(S) = \varprojlim V_r(S)$, l'application de $V_{r+1}(S)$ dans $V_r(S)$ étant la multiplication par p.

Soit $\eta_r : BW(\mathcal{K}(S)) \to CW_k(S) = V_r(S)$ l'application qui à $(\ldots, a_{-n}, \ldots, a_0, \ldots, a_m, \ldots)$ associe $(\ldots, a_{-n+r,r}, \ldots, a_{-1+r,r}, a_{r,r})$; on vérifie que η_r est D_k-linéaire et que le diagramme

$$\begin{tikzcd} BW(\mathcal{K}(S)) \arrow[r, "\eta_{r+1}"] \arrow[dr, "\eta_r"'] & V_{r+1}(S) \arrow[d, "p"] \\ & V_r(S) \end{tikzcd}$$

est commutatif. On obtient donc ainsi une application D_k-linéaire $\eta : BW(\mathcal{K}(S)) \to V(S)$.

On vérifie tout de suite que η est injective. Mais η est aussi surjective : soit $\underline{b} = (\underline{b}_r)_{r\in\mathbb{N}} \in V(S)$, avec $\underline{b}_r \in V_r(S) = CW_k(S)$. Si $\underline{b}_r = (\ldots, b_{-n,r}, \ldots, b_{-1,r}, b_{0,r})$, on voit que $b_{-n-1,r+1}^p = b_{-n,r}$, pour tout n

et tout r ; on en déduit que $\underline{b} = \eta(\underline{a})$, avec $\underline{a} = (\dots, a_{-n}, \dots, a_0, \dots, a_m, \dots)$ et

$$\begin{cases} a_{-n} = (b_{-n,0}, b_{-n-1,1}, \dots, b_{-n-r,r}, \dots) & \text{pour } n \geq 0 \ . \\ a_m = (b_{0,m}^{p}, b_{0,m}^{p^{m-1}}, \dots, b_{0,m}, b_{-1,m+1}, \dots, b_{m-s,s}, \dots) & \text{pour } m > 0 \ . \end{cases}$$

Par conséquent, η est un isomorphisme.

Or, si l'on pose $G_{(r)}(S) = G(S)$, on a $\underline{U}(G)(S) = \varprojlim G_{(r)}(S)$, la flèche de $G_{(r+1)}(S)$ dans $G_{(r)}(S)$ étant la multiplication par p . Comme $G_{(r)}(S) = G(S)$ s'identifie canoniquement (et fonctoriellement) à $\mathrm{Hom}_{D_k}(M, CW_k(S))$ (cf. prop. 6.2 du chap.III) $= \mathrm{Hom}_{D_k}(M, V_r(S))$, on voit que $\underline{U}(G)(S) = \varprojlim \mathrm{Hom}_{D_k}(M, V_r(S))$ est aussi $\mathrm{Hom}_{D_k}(M, \varprojlim V_r(S))$ qui s'identifie à $\mathrm{Hom}_{D_k}(M, BW(\mathcal{N}(S)))$ en utilisant l'isomorphisme η .

Un élément u de $\underline{U}(G)(S)$ est dans $\underline{T}(G)(S)$ si et seulement si son image dans $G_{(0)}(S)$ est nulle ; si on identifie $\underline{U}(G)(S)$ à $\mathrm{Hom}_{D_k}(M, BW(\mathcal{N}(S)))$, on voit que cela revient à dire que $\eta_0 \circ u = 0$, donc que $u \in \mathrm{Hom}_{D_k}(M, BW_0(\mathcal{N}(S)))$.

1.4. Soit $\mathbb{S}$ un A'-anneau p-adique. Notons $\mathrm{Res}(\mathbb{S})$ l'ensemble des familles $x = (x^{(n)})_{n\in\mathbb{Z}}$ d'éléments de $\mathbb{S}$, indexées par les entiers rationnels, vérifiant $(x^{(n+1)})^p = x^{(n)}$, pour tout $n \in \mathbb{Z}$.

Soient $x = (x^{(n)})_{n\in\mathbb{Z}}$ et $y = (y^{(n)})_{n\in\mathbb{Z}}$ deux éléments de $\mathrm{Res}(\mathbb{S})$. Il est clair que, pour tout entier n fixé, la suite des $(x^{(n+m)} + y^{(n+m)})^{p^m}$ est convergente dans $\mathbb{S}$; si l'on note $z^{(n)}$ sa limite, on voit que $z = (z^{(n)})_{n\in\mathbb{Z}}$ est un élément de $\mathrm{Res}(\mathbb{S})$.

On vérifie alors facilement que l'on munit $\mathrm{Res}(\mathbb{S})$ d'une structure de k-anneau en posant, pour $x, y \in \mathrm{Res}(\mathbb{S})$

$$\begin{cases} (x+y)^{(n)} = \lim\limits_{m\to+\infty} (x^{(n+m)} + y^{(n+m)})^{p^m} \ , \\ (xy)^{(n)} = x^{(n)} y^{(n)} \\ (\lambda x)^{(n)} = \sigma^{-n}([\lambda])x^{(n)} = [\sigma^{-n}(\lambda)]\, x^{(n)} \ , \text{ pour tout } \lambda \in k \text{ (où } [\lambda] \text{ est le} \\ \text{représentant de Teichmüller de } \lambda \text{ dans } W(k) = A \subset A') \ . \end{cases}$$

Notons $\mathrm{Res}^{+}_{A'}(\mathbb{S})$ le sous-ensemble de $\mathrm{Res}(\mathbb{S})$ formé des x tels que $x^{(0)} \in \mathfrak{m}\mathbb{S}$. On vérifie immédiatement que $\mathrm{Res}^{+}_{A'}(\mathbb{S})$ est un idéal de $\mathrm{Res}(\mathbb{S})$ et que $\mathrm{Res}(\mathbb{S})$ est séparé et complet pour la topologie $\mathrm{Res}^{+}_{A'}(\mathbb{S})$-adique.

PROPOSITION 1.3.- Soit $\mathcal{S}$ un A'-anneau p-adique et soit $\mathcal{S}_k = \mathcal{S}\otimes_{A'}k = \mathcal{S}/\mathfrak{m}\mathcal{S}$. Les k-anneaux topologiques $\mathrm{Res}(\mathcal{S})$ et $\mathcal{K}(\mathcal{S}_k)$ sont isomorphes, canoniquement et fonctoriellement en $\mathcal{S}$.

Démonstration : pour tout $s \in \mathcal{S}$, notons $\tilde{s}$ son image dans $\mathcal{S}_k$. Si $x = (x^{(n)})_{n\in\mathbb{Z}} \in \mathrm{Res}(\mathcal{S})$, on voit que $\tilde{x} = (\widetilde{x^{(0)}},\ldots,\widetilde{x^{(n)}},\ldots) \in \mathcal{K}(\mathcal{S}_k)$ et il est immédiat que l'application $x \mapsto \tilde{x}$ est un homomorphisme continu de $\mathrm{Res}(\mathcal{S})$ dans $\mathcal{K}(\mathcal{S}_k)$. Si $u = (u_0,\ldots,u_n,\ldots) \in \mathcal{K}(S_k)$, notons $\hat{u}_n$ un relèvement de u_n dans $\mathcal{S}$. On voit facilement que, pour tout entier n fixé, la suite des $\hat{u}_{n+m}^{p^m}$ converge dans $\mathcal{S}$ vers un élément $\hat{u}^{(n)}$, ne dépendant pas du choix des relèvements, et que $\hat{u} = (\hat{u}^{(n)})_{n\in\mathbb{Z}} \in \mathrm{Res}(\mathcal{S})$. On vérifie que l'application $u \to \hat{u}$ est continue et que les applications $x \to \tilde{x}$ et $u \to \hat{u}$ sont inverses l'une de l'autre.

Remarque : soit K" un sous-corps du corps des fractions K' de A' contenant le corps des fractions K de A = W(k) et soit $\mathfrak{m}_{A''}$ l'idéal maximal de A". Tout A'-anneau p-adique $\mathcal{S}$ peut être considéré comme un A"-anneau p-adique. Les k-anneaux topologiques $\mathcal{K}(\mathcal{S}/\mathfrak{m}\mathcal{S})$ et $\mathcal{K}(\mathcal{S}/\mathfrak{m}_{A''}\mathcal{S})$ sont canoniquement isomorphes puisqu'ils s'identifient tous deux à $\mathrm{Res}(\mathcal{S})$. Sur $\mathrm{Res}(\mathcal{S})$, les topologies $\mathrm{Res}^+_{A'}(\mathcal{S})$-adiques et $\mathrm{Res}^+_{A''}(\mathcal{S})$-adiques coïncident donc, mais l'inclusion $\mathrm{Res}^+_{A'}(\mathcal{S}) \subset \mathrm{Res}^+_{A''}(\mathcal{S})$ est, en général, stricte.

Compte-tenu de la remarque 2 du n°1.1 et de la proposition 1.2, la proposition 1.3 implique le résultat suivant :

COROLLAIRE. - Soit G un groupe p-divisible sur A' et soit $M = \underline{M}(G_k)$. Pour tout A'-anneau p-adique $\mathcal{S}$, $\underline{U}(G)(\mathcal{S})$ s'identifie canoniquement (et fonctoriellement en $\mathcal{S}$ et G) à $\mathrm{Hom}_{D_k}(M, BW(\mathrm{Res}(\mathcal{S})))$.

1.5. Le reste de ce paragraphe est consacré à donner une description de $U_0(G)$, et plus généralement de $\underline{U}_0(G)(\mathcal{S})$ pour tout A'-anneau p-adique $\mathcal{S}$, lorsque G est un groupe p-divisible sur A', à l'aide du couple $LM_{K'}(G) = (L_{K'}(G), M_K(G))$ défini au n°IV.5.2.

Commençons par énoncer les résultats (nous les démontrerons dans les n^{os} suivants) :

PROPOSITION 1.4.- Soit $\mathcal{S}$ un A'-anneau p-adique et soit $\mathcal{S}_K = K \otimes_A \mathcal{S} = K' \otimes_{A'} \mathcal{S}$:

i) pour tout $(x_n)_{n\in\mathbb{Z}} \in BW(\mathrm{Res}(\mathcal{S}))$, $\sum_{n\in\mathbb{Z}} p^n x_n^{(n)}$ converge dans $\mathcal{S}_K$;

ii) l'application $bw_{\mathcal{S}} : BW(\mathrm{Res}(\mathcal{S})) \to \mathcal{S}_K$, qui à $(x_n)_{n\in\mathbb{Z}}$ associe $\sum_{n\in\mathbb{Z}} p^n x_n^{(n)}$, est K-linéaire.

THÉORÈME 1.- Soit G un groupe p-divisible sur A' et soit $(L_{K'}, M_K) = LM_{K'}(G)$. Pour tout A'-anneau p-adique $\mathcal{S}$, posons $\mathcal{S}_K = K \otimes_A \mathcal{S} = K' \otimes_{A'} \mathcal{S}$ et soit $bw_{\mathcal{S},K'} : K' \otimes_K BW(\mathrm{Res}(\mathcal{S})) \to \mathcal{S}_K$ l'application K'-linéaire déduite de $bw_{\mathcal{S}}$ par extension des scalaires. Pour tout $u \in \mathrm{Hom}_{K[\underline{F},\underline{V}]}(M_K, BW(\mathrm{Res}(\mathcal{S})))$, notons $u_{K'} : K' \otimes_K M_K \to K' \otimes_K BW(\mathrm{Res}(\mathcal{S}))$ l'application K'-linéaire déduite de u par extension des scalaires. Alors $\underline{U}_0(G)(\mathcal{S})$ s'identifie canoniquement, et fonctoriellement en G et $\mathcal{S}$, au sous-$\mathbb{Q}_p$-espace vectoriel de $\mathrm{Hom}_{K[\underline{F},\underline{V}]}(M_K, BW(\mathrm{Res}(\mathcal{S})))$ formé des u tels que $u_{K'}(L_{K'}) \subset \ker bw_{\mathcal{S},K'}$.

Nous démontrerons en fait un résultat plus précis : si G est un groupe p-divisible sur A' , notons G_m le plus petit sous-schéma en groupes fermé de G tel que, pour tout A'-anneau p-adique $\mathcal{S}$, $G_m(\mathcal{S})$ est le noyau de $G_{tor}(\mathcal{S}) \to G_k(\mathcal{S}_k)$ (il revient au même de dire que c'est le plus petit sous-schéma en groupes fermé de G tel que $G_m(A_C)$ est le noyau de $G_{tor}(A_C) \to G_k(A_C/\mathfrak{m}A_C)$. On voit facilement que G_m est un schéma en groupes fini et plat sur A' et que le quotient G/G_m (dans la catégorie des faisceaux en groupes fppf sur A') est un groupe p-divisible isogène à G .

PROPOSITION 1.5.- Conservons les hypothèses et les notations du théorème précédent et soit $M = \underline{M}(G_k)$ (identifié à un sous-D_k-module de $M_K = K\otimes_A M$). Soit $BW^+_{/A'}(\mathrm{Res}(\mathcal{S}))$ le sous-D_k-module de $BW(\mathrm{Res}(\mathcal{S}))$ formé des $(x_n)_{n\in\mathbb{Z}}$ tels que $x_n^{(0)} \in \mathrm{Res}^+_{A'}(\mathcal{S})$ pour $n \leq 0$. Alors $\underline{T}(G/G_m)(S)$ s'identifie canoniquement, et fonctoriellement en G et $\mathcal{S}$, au sous-$\mathbb{Z}_p$-module de $\mathrm{Hom}_{D_k}(M, BW^+_{/A'}(\mathrm{Res}(\mathcal{S})))$ formé des u tels que $u_{K'}(L_{K'}) \subset \ker bw_{\mathcal{S},K'}$.

Remarques :

1.- Si $e < p-1$, ou si $e = p-1$ et si G est unipotent, on voit (cf. n° IV.4.8) que $G_m = 0$, donc que $\underline{T}(G/G_m)(\mathcal{S}) = \underline{T}(G)(\mathcal{S})$.

2.- On voit facilement que $BW(\mathrm{Res}(\mathcal{S}))$ s'identifie à $K\otimes_A BW^+_{/A'}(\mathrm{Res}(\mathcal{S}))$. On en déduit que $\mathrm{Hom}_{K/[\underline{F},\underline{V}]}(M_K, BW(\mathrm{Res}(\mathcal{S}))) = \mathrm{Hom}_{D_k}(M_K, BW(\mathrm{Res}(\mathcal{S})))$ s'identifie à $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{D_k}(M, BW^+{}_{/A'}\ (\mathrm{Res}(\mathcal{S})))$. Comme la projection de G sur $G/G_{\mathfrak{m}}$ est une isogénie, $\underline{U}_0(G)(\mathcal{S})$ et $\underline{U}_0(G/G_{\mathfrak{m}})(\mathcal{S})$ s'identifient et le théorème 1 résulte donc de la proposition 1.5.

1.6. Commençons par démontrer la proposition 1.4.

Rappelons que l'on a défini au n° II.5.1 une application A-linéaire continue $\hat{w}_{\mathcal{S}} : CW(\mathcal{S}) \to \mathcal{S}_K$. On voit (cf. n° IV.3.1) que l'image par $\hat{w}_{\mathcal{S}}$ de $CW(\mathfrak{m}\mathcal{S})$ est contenue dans $P'(\mathcal{S})$ et, par passage aux quotients, on en déduit une application $w^0_{\mathcal{S}} : CW(\mathcal{S}_k) \to \mathcal{S}_K/P'(\mathcal{S})$.

Reprenons les notations utilisées dans la démonstration de la proposition 1.2 et soit, pour tout entier $r \geq 0$,

$$w^r_{\mathcal{S}} : V_r(\mathcal{S}_k) = CW_k(\mathcal{S}_k) \to \mathcal{S}_K/p^r P'(\mathcal{S})$$

l'application obtenue en composant $w^0_{\mathcal{S}}$ avec l'application de $\mathcal{S}_K/P'(\mathcal{S})$ dans $\mathcal{S}_K/p^r P'(\mathcal{S})$ déduite, par passage aux quotients, de la multiplication par p^r dans $\mathcal{S}_K$. Il est clair que le diagramme

$$\begin{tikzcd}
V_{r+1}(\mathcal{S}_k) \arrow[r, "w^{r+1}_{\mathcal{S}}"] \arrow[d, "p"] & \mathcal{S}_K/p^{r+1}P'(\mathcal{S}) \arrow[d, "\text{proj.can.}"] \\
V_r(\mathcal{S}_k) \arrow[r, "w^r_{\mathcal{S}}"] & \mathcal{S}_K/p^r\mathcal{S}
\end{tikzcd}$$

est commutatif.

On sait que $BW(\mathrm{Res}(\mathcal{S})) = BW(\mathcal{K}(\mathcal{S}_k))$ s'identifie à $\varprojlim V_r(\mathcal{S}_k)$; comme il existe un entier ν tel que $P'(\mathcal{S}) \subset p^\nu \mathcal{S}$, $\varprojlim \mathcal{S}_K/p^r P'(\mathcal{S})$ s'identifie à $\mathcal{S}_K$. Par passage à la limite, les applications $w^r_{\mathcal{S}}$ définissent donc une application A-linéaire $bw^0_{\mathcal{S}}$ de $BW(\mathrm{Res}(\mathcal{S}))$ dans $\mathcal{S}_K$ et il suffit, pour démontrer la proposition 1.4, d'établir le lemme suivant :

LEMME 1.6.- <u>On a</u> $bw^0_{\mathcal{S}} = bw_{\mathcal{S}}$ (i.e., <u>pour tout</u> $\underline{x} = (x_n)_{n\in\mathbb{Z}} \in BW(\mathrm{Res}(\mathcal{S}))$, $\sum_{n\in\mathbb{Z}} p^n x_n^{(n)}$ <u>converge et</u> $bw^0_{\mathcal{S}}(x) = \sum_{n\in\mathbb{Z}} p^n x_n^{(n)}$).

<u>Démonstration</u> : si $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in V_r(\mathcal{S}_k) = CW_k(\mathcal{S}_k)$ et si $\hat{a}_{-n}$ est un relèvement de a_{-n} dans $\mathcal{S}$, on voit que $w^r_{\mathcal{S}}(\underline{a})$ est l'image, modulo $p^r P'(\mathcal{S})$, de $\sum_{n=0}^{\infty} p^{-n+r}\hat{a}_{-n}^{p^n}$.

Lorsque l'on identifie $\mathrm{Res}(\mathcal{S})$ à $\mathcal{K}(\mathcal{S}_k)$, $x_n = (x_n^{(m)})_{m\in\mathbb{Z}}$ s'identifie à $\tilde{x}_n = (\widetilde{x_n^{(0)}},\ldots,\widetilde{x_n^{(m)}},\ldots)$ (où $\widetilde{x_n^{(m)}}$ est l'image de $x_n^{(m)}$ dans $\mathcal{S}_k$).

On voit que l'image $\eta_r(\underline{x})$ de $\underline{x}$ dans $V_r(\mathcal{S}_k) = CW(\mathcal{S}_k)$ est $(\ldots,\widetilde{x_{-n+r}^{(r)}},\ldots,\widetilde{x_{-1+r}^{(r)}},\widetilde{x_r^{(r)}})$; comme $x_{-n+r}^{(r)}$ est un relèvement dans $\mathcal{S}$ de $\widetilde{x_{-n+r}^{(r)}}$, $w_{\mathcal{S}}^r(\eta_r(\underline{x}))$ est l'image, modulo $p^rP'(\mathcal{S})$, de

$$\sum_{n=0}^{\infty} p^{-n+r}(x_{-n+r}^{(r)})^{p^n} = \sum_{n=0}^{\infty} p^{-n+r}x_{-n+r}^{(r-n)} = \sum_{-\infty}^{r} p^n x_n^{(n)} \ ,$$

et, en passant à la limite, on a bien $bw_{\mathcal{S}}(\underline{x}) = \sum_{n\in\mathbb{Z}} p^n x_n^{(n)}$.

1.7. Démontrons maintenant la proposition 1.5.

Posons $(L,M) = LM_{A'}(G)$ et soit ρ l'inclusion de L dans $M_{A'}$. Soit $\overline{G} = G_{(L,M,\rho)}$ le foncteur en groupes sur la catégorie des A'-anneaux p-adiques défini au n° IV.4.7. Commençons par établir un lemme :

LEMME 1.7.- <u>Le</u> $\mathbb{Z}_p$<u>-module</u> $\underline{T}(G/G_m)(\mathcal{S})$ <u>s'identifie canoniquement</u>, <u>et fonctoriellement en</u> G <u>et en</u> $\mathcal{S}$, <u>à</u>

$$\underline{T}(\overline{G})(\mathcal{S}) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p,\overline{G}(\mathcal{S})) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p,\overline{G}_{tor}(\mathcal{S})) \ .$$

<u>Démonstration du lemme</u> : Soit $\underline{U}_0(\overline{G})(\mathcal{S}) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p,\overline{G}_{tor}(\mathcal{S}))$. Tout élément de $\underline{U}_0(\overline{G})(\mathcal{S})$ peut s'écrire sous la forme $\bar{u} = (\bar{u}_0,\bar{u}_1,\ldots,\bar{u}_n,\ldots)$, avec $\bar{u}_n \in \overline{G}_{tor}(\mathcal{S})$ et $p\bar{u}_{n+1} = \bar{u}_n$. Soit $\psi' : \underline{U}_0(\overline{G})(\mathcal{S}) \to \underline{U}_0(G)(\mathcal{S})$ l'application qui à $\bar{u}$ associe $\psi'(\bar{u}) = (\psi_G(\mathcal{S})(\bar{u}_t),\psi_G(\mathcal{S})(\bar{u}_{t+1}),\ldots,\psi_G(\mathcal{S})(\bar{u}_{t+n}),\ldots)$ (où t est l'entier défini au n° IV.4.5 et où $\psi_G : \overline{G} \to G$ est le morphisme défini au n° IV.4.7).

Comme $\psi_G(\mathcal{S})\circ\varphi_G(\mathcal{S}) = p^t\cdot\mathrm{id}_{G(\mathcal{S})}$ et $\varphi_G(\mathcal{S})\circ\psi_G(\mathcal{S}) = p^t\cdot\mathrm{id}_{\overline{G}(\mathcal{S})}$ (cf. prop. 4.9 du chap. IV) , on voit que ψ' est un isomorphisme de $\mathbb{Q}_p$-espaces vectoriels.

Pour tout $u \in G(\mathcal{S})$, notons u' son image dans $(G/G_m)(\mathcal{S})$ et soit $\varphi' : \underline{U}_0(G)(\mathcal{S}) \to \underline{U}_0(G/G_m)(\mathcal{S})$ l'application qui, à $(u_0,u_1,\ldots,u_n,\ldots) \in \underline{U}_0(G)(\mathcal{S})$, associe $(u'_0,u'_1,\ldots,u'_n,\ldots)$. Il est clair que φ' est aussi un isomorphisme de $\mathbb{Q}_p$-espaces vectoriels.

L'application $\varphi'\circ\psi'$ est donc un isomorphisme de $\underline{U}_0(\overline{G})(\mathcal{S})$ sur

$\underline{U}_0(G/G_m)(\mathcal{S})$. Pour achever la démonstration du lemme, il suffit alors de vérifier que, si $\bar{u} \in \underline{U}_0(\bar{G})(\mathcal{S})$, $\varphi'(\psi'(\bar{u})) \in \underline{T}(G/G_m)(\mathcal{S})$ si et seulement si $\bar{u} \in \underline{T}(\bar{G})(\mathcal{S})$:

Posons $\bar{u} = (\bar{u}_0, \bar{u}_1, \ldots, \bar{u}_n, \ldots)$, $\psi'(\bar{u}) = u = (u_0, u_1, \ldots, u_n, \ldots)$ et $\varphi'(u) = u' = (u'_0, u'_1, \ldots, u'_n, \ldots)$. On voit que $u' \in \underline{T}(G/G_m)(\mathcal{S})$ si et seulement si $u'_0 = 0$, ou encore si et seulement si u_0 appartient au noyau de la projection de $G(\mathcal{S})$ dans $(G/G_m)(\mathcal{S})$, qui est $G_m(\mathcal{S})$. On voit que $G_m(\mathcal{S}) = G_{tor}(m\mathcal{S})$ est le noyau de $\varphi_G(\mathcal{S})$ (prop. 4.8 du chap.IV). Donc $u' \in \underline{T}(G/G_m)(\mathcal{S})$ si et seulement si $\varphi_G(\mathcal{S})(u_0) = 0$; comme $u_0 = \psi_G(\mathcal{S})(\bar{u}_t)$, ceci est équivalent à $\psi_G(\mathcal{S}) \circ \varphi_G(\mathcal{S})(\bar{u}_t) = 0$; comme $\psi_G(\mathcal{S}) \circ \varphi_G(\mathcal{S}) = p^t . \mathrm{id}_{\bar{G}(\mathcal{S})}$, c'est encore équivalent à $p^t \bar{u}_t = 0$, i.e. à $\bar{u}_0 = 0$, ou à $\bar{u} \in \underline{T}(\bar{G})(\mathcal{S})$.

Démonstration de la proposition 1.5 : on sait (prop. 1.2) que $\underline{T}(G_k)(\mathcal{S}_k)$ s'identifie, canoniquement et fonctoriellement, à $\mathrm{Hom}_{D_k}(M, BW_0(\varkappa(\mathcal{S}_k)))$. Lorsque l'on identifie, à l'aide de la proposition 1.3, $\varkappa(\mathcal{S}_k)$ à $\mathrm{Res}(\mathcal{S})$, donc $BW(\varkappa(\mathcal{S}_k))$ à $BW(\mathrm{Res}(\mathcal{S}))$, on voit que $BW_0(\varkappa(\mathcal{S}_k))$ s'identifie à $BW^+_{/A'}(\mathrm{Res}(\mathcal{S}))$. On peut donc identifier $\underline{T}(G_k)(\mathcal{S}_k)$ à $\mathrm{Hom}_{D_k}(M, BW^+_{/A'}(\mathrm{Res}(\mathcal{S})))$.

Rappelons (cf. n° IV.4.4) que le groupe $\bar{G}(\mathcal{S})$ est formé des couples (u_L, u_M) , avec $u_L \in \mathrm{Hom}_{A'}(L, \mathcal{S}_K)$, $u_M \in \mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$ tel que le diagramme

$$\begin{tikzcd}
L \arrow[r, "u_L"] \arrow[dd, "\rho"'] & \mathcal{S}_K \arrow[dr, "\mathrm{proj.can.}"] & \\
& & \mathcal{S}_K/P'(\mathcal{S}) \\
M_{A'} \arrow[r, "u_{M,A'}"] & CW_{k,A'}(\mathcal{S}_k) \arrow[ur, "w_{\mathcal{S}}"'] &
\end{tikzcd}$$

est commutatif. Comme $\mathrm{Hom}_{A'}(L, \mathcal{S}_K)$ est sans torsion, on voit que $(u_L, u_M) \in \bar{G}_{tor}(\mathcal{S})$ si et seulement si $u_L = 0$. On en déduit que le sous-groupe $\bar{G}_{tor}(\mathcal{S})$ de $\bar{G}(\mathcal{S})$ s'identifie au sous-groupe de $\mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$ formé des u_M tels que $w_{\mathcal{S}} \circ u_{M,A'} \circ \rho = 0$.

La proposition 6.2 du chapitre III montre que $\mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$ s'identifie à $G_k(\mathcal{S}_k)$. En particulier, l'application de $\bar{G}_{tor}(\mathcal{S})$ dans $G_k(\mathcal{S}_k)$ qui en résulte est injective et $\underline{T}(\bar{G})(\mathcal{S})$ s'identifie à un sous-$\mathbb{Z}_p$-module de $\underline{T}(G_k)(\mathcal{S}_k)$.

Lorsque l'on identifie $\underline{T}(G_k)(\mathcal{S}_k)$ à $\mathrm{Hom}_{D_k}(M, BW^{+}/_{A'}(\mathrm{Res}(\mathcal{S})))$, tout élément $u \in \underline{T}(G_k)(\mathcal{S}_k)$ peut s'écrire sous la forme $u = (u_0, u_1, \dots, u_r, \dots)$ avec $u_r \in \mathrm{Hom}_{D_k}(M, V_r(\mathcal{S}_k)) = \mathrm{Hom}_{D_k}(M, CW_k(\mathcal{S}_k))$, $u_0 = 0$ et $pu_{r+1} = u_r$. On voit immédiatement qu'un tel $u \in \underline{T}(\overline{G})(\mathcal{S}_k)$ si et seulement si, pour tout entier $r \geq 0$, $w_{\mathcal{S}} \circ u_{r,A'} \circ \rho = 0$.

Pour tout entier $r \geq 0$, posons $V_{r,A'}(\mathcal{S}_k) = CW_{k,A'}(\mathcal{S}_k)$ et soit $w_{\mathcal{S},r} : V_{r,A'}(\mathcal{S}_k) \to \mathcal{S}_K/p^rP'(\mathcal{S})$ l'application obtenue en composant $w_{\mathcal{S}}$ avec l'application de $\mathcal{S}_K/P'(\mathcal{S})$ dans $\mathcal{S}_K/p^rP'(\mathcal{S})$ obtenue, par passage aux quotients, à partir de la multiplication par p^r dans $\mathcal{S}_K$. On a un diagramme commutatif

$$\begin{tikzcd}
\vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] \\
M_{A'} \arrow[r, "u_{r+1,A'}"] \arrow[d, "\mathrm{id}"'] & V_{r+1,A'}(\mathcal{S}_k) \arrow[r, "w_{\mathcal{S},r+1}"] \arrow[d, "p"] & \mathcal{S}_K/p^{r+1}P'(\mathcal{S}) \arrow[d, "\text{proj.can.}"] \\
M_{A'} \arrow[r, "u_{r,A'}"] \arrow[d] & V_{r,A'}(\mathcal{S}_k) \arrow[r, "w_{\mathcal{S},r}"] \arrow[d] & \mathcal{S}_K/p^{r}P'(\mathcal{S}) \arrow[d] \\
\vdots & \vdots & \vdots
\end{tikzcd}$$

qui, par passage à la limite, défini des applications

$$M_{A'} \xrightarrow{u_{\infty,A'}} \varprojlim V_{r,A'}(\mathcal{S}_k) \xrightarrow{w_{\mathcal{S},\infty}} \mathcal{S}_K$$

et il est clair que $u \in \underline{T}(G)(\mathcal{S})$ si et seulement si $w_{\mathcal{S},\infty} \circ u_{\infty,A'} \circ \rho = 0$.

Il résulte facilement de la proposition 2.5 du chapitre IV que l'application canonique de $A' \otimes_A CW_k(\mathcal{S}_k)$ dans $CW_{k,A'}(\mathcal{S}_k)$ est surjective et que son noyau est tué par une puissance de p (qui ne dépend que de l'indice de ramification absolu e de A'). Comme $\varprojlim V_r(\mathcal{S}_k)$ s'identifie à $BW(\mathrm{Res}(\mathcal{S}))$, on en déduit que $\varprojlim V_{r,A'}(\mathcal{S}_k)$ s'identifie à $A' \otimes_A BW(\mathrm{Res}(\mathcal{S})) = K' \otimes_K BW(\mathrm{Res}(\mathcal{S}))$. Il est immédiat que l'application $w_{\mathcal{S},\infty} : K' \otimes_K BW(\mathrm{Res}(\mathcal{S})) \to \mathcal{S}_K$ s'identifie à $bw_{\mathcal{S},K'}$ et on voit facilement que le diagramme

$$\begin{tikzcd}
L \arrow[r] \arrow[d, hook] & M_{A'} \arrow[d] \arrow[dr, "u_{\infty,A'}"] & \\
K' \otimes_A L \simeq L_{K'} \arrow[r, hook] & K' \otimes_K M \simeq K' \otimes_{A'} M_{A'} \arrow[r, "u_{K'}"'] & BW(\mathrm{Res}(\mathcal{S}))
\end{tikzcd}$$

est commutatif. On a donc $bw_{\mathcal{S},K'} \circ u_{\infty,A'}(L) = 0$ si et seulement si $u_{K'}(L_{K'}) \subset \ker bw_{\mathcal{S},K'}$, ce qui achève la démonstration.

1.8. Remarques :

1.- Soit $\mathcal{G} = \mathrm{Gal}(\overline{K}'/K')$. Le groupe $\mathcal{G}$ opère, par continuité, sur C et sur A_C , donc aussi, par fonctorialité, sur $\mathrm{Res}(A_C)$, sur $BW(\mathrm{Res}(A_C))$ et sur $BW_{K'}(\mathrm{Res}(A_C)) = K' \otimes_K BW(\mathrm{Res}(A_C))$; en outre, il est clair que l'application $bw_{A_C,K'} : BW_{K'}(\mathrm{Res}(A_C)) \to C$ est $\mathcal{G}$-linéaire.

Soit V un $\mathbb{Q}_p[\mathcal{G}]$-module à gauche, de dimension finie sur $\mathbb{Q}_p$, avec action de $\mathcal{G}$ continue. Notons $M_K^{\mathcal{G}}(V)$ le $K[\underline{F},\underline{V}]$-module à gauche $\mathrm{Hom}_{\mathbb{Q}_p[\mathcal{G}]}(V, BW(\mathrm{Res}(A_C)))$ des applications $\mathbb{Q}_p[\mathcal{G}]$-linéaires de V dans $BW(\mathrm{Res}(A_C))$. On voit que le K'-espace vectoriel $M_{K'}^{\mathcal{G}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[\mathcal{G}]}(V, BW_{K'}(\mathrm{Res}(A_C)))$ s'identifie canoniquement à $K' \otimes_K M_K^{\mathcal{G}}(V)$. Nous notons $L_{K'}^{\mathcal{G}}(V)$ le sous-K'-espace vectoriel de $M_{K'}^{\mathcal{G}}(V)$ formé des éléments dont l'image appartient au noyau de $bw_{A_C,K'}$.

On peut montrer ([24]) que si V est de Hodge-Tate de type $(n_i)_{i \in \mathbb{Z}}$, alors $M_K^{\mathcal{G}}(V)$ est un espace vectoriel sur K de dimension $\leq \sum_{i=0}^{\infty} n_i$ et $L_{K'}^{\mathcal{G}}(V)$ est un espace vectoriel sur K' de dimension $\leq \sum_{i=1}^{\infty} n_i$.

[Rappelons ce que signifie " V est de Hodge-Tate de type $(n_i)_{i \in \mathbb{Z}}$ " : soit $\chi : \mathcal{G} \to \mathbb{Z}_p^*$ le caractère qui donne l'action de $\mathcal{G}$ sur les racines de l'unité d'ordre une puissance de p (on a donc $g(\varepsilon) = \varepsilon^{\chi(g)}$, pour toute racine de l'unité ε d'ordre une puissance de p et pour tout $g \in \mathcal{G}$). On fait opérer $\mathcal{G}$ semi-linéairement sur $V_C = C \otimes_{\mathbb{Q}_p} V$ en posant $g(c \otimes v) = g(c) \otimes g(v)$, pour tout $g \in \mathcal{G}$, $c \in C$, $v \in V$. Pour tout $i \in \mathbb{Z}$, on note V_C^i le sous-K'-espace vectoriel de V_C formé des x tels que $g(x) = \chi(g)^i x$, pour tout $g \in \mathcal{G}$. L'application évidente de $\bigoplus_{i \in \mathbb{Z}} (C \otimes_K V_C^i)$ dans V_C est alors injective (cf. [42] , p.122) et on dit que V est de Hodge-Tate si c'est un isomorphisme ; si l'on appelle n_i la dimension (nécessairement finie) de V_C^i sur K' , on dit, plus précisément, que V est de Hodge-Tate de type $(n_i)_{i \in \mathbb{Z}}$.]

2. Soit alors $\mathcal{G}$ un groupe p-divisible sur A' , de dimension d et de hauteur h . On voit que T(G) est un $\mathbb{Z}_p[\mathcal{G}]$-module, libre de rang h sur $\mathbb{Z}_p$ et que, par conséquent, $U_0(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T(G)$ est un $\mathbb{Q}_p[\mathcal{G}]$-module, de dimension h sur $\mathbb{Q}_p$. On sait (cf.[44] , §4,cor.2 au th.3) qu'il est de

Hodge-Tate de type $(n_i)_{i\in\mathbb{Z}}$ avec

$$\begin{cases} n_0 = h-d \\ n_1 = d \\ n_i = 0 \quad \text{si} \quad i \neq 0,1 . \end{cases}$$

Il résulte du théorème 1 que, si $(L_{K'}, M_K) = LM_{K'}(G)$, $U_0(G) = \underline{U}_0(G)(A_C)$ s'identifie, en tant que $\mathbb{Q}_p[\mathcal{G}]$-module, au sous-module de $\mathrm{Hom}_{K[\underline{F},\underline{V}]}(M_K, BW(\mathrm{Res}(A_C))$ formé des u tels que $u_{K'}(L_{K'})$ est contenu dans le noyau de $bw_{A_C,K'}$. On en déduit, de manière évidente, des applications de M_K dans $M_K^{\mathcal{G}}(U_0(G))$ et de $L_{K'}$ dans $L_{K'}^{\mathcal{G}}(U_0(G))$ et on montre facilement qu'elles sont injectives. Le résultat précédent et des considérations sur les dimensions impliquent alors que ce sont des isomorphismes. On obtient ainsi un procédé pour construire le couple $LM_{K'}(G)$ à partir de la seule connaissance du $\mathbb{Q}_p[\mathcal{G}]$-module $U_0(G)$.

§ 2.- Travaux de Honda.

Dans ce paragraphe, on conserve les hypothèses et les notations du chapitre III et du § 1 du chapitre IV. On se propose de retrouver les résultats de Honda sur la classification des lois de groupe formel commutatif sur $A = W(k)$ et sur k en les interprétant à la lumière des résultats que nous avons obtenus.

2.1. Soit B un anneau commutatif. Rappelons que l'on appelle loi de groupe formel (sous-entendu commutatif) à d paramètres sur B , la donnée d'un d-uple de séries formelles $\Gamma(\underline{X},\underline{Y}) = (\Gamma_i(X_1,\dots,X_d,Y_1,\dots,Y_d))_{1\leq i\leq d}$, à coefficients dans B , en les $2d$ variables $X_1X_2,\dots,X_d,Y_1,\dots,Y_d$, vérifiant, avec des notations évidentes

$$\begin{cases} \Gamma(\underline{X},0) = \Gamma(0,\underline{X}) = \underline{X} , \\ \Gamma(\Gamma(\underline{X},\underline{Y}),\underline{Z}) = \Gamma(\underline{X},\Gamma(\underline{Y},\underline{Z})) \\ \Gamma(\underline{Y},\underline{X}) = \Gamma(\underline{X},\underline{Y}) . \end{cases}$$

De ces axiomes, on déduit immédiatement l'existence d'un d-uple de séries formelles sans terme constant, à coefficients dans B , unique,

$h(\underline{X}) = (h_i(X_1,\ldots,X_d))_{1\le i\le d}$ tel que $\Gamma(\underline{X},h(\underline{X})) = \Gamma(h(\underline{X}),\underline{X}) = 0$.

Lorsque B est un anneau commutatif pseudo-compact, se donner une loi de groupe formel à d paramètres sur B revient à se donner une structure de bigèbre formelle sur le B-anneau profini $R = B[[X_1,X_2,\ldots,X_d]]$: l'anneau $R\hat{\otimes}_B R$ s'identifie à $B[[X_1,\ldots,X_d,Y_1,\ldots,Y_d]]$ en posant $X_i\hat{\otimes}1 = X_i$, $1\hat{\otimes}X_i = Y_i$ et le coproduit Δ est défini par $\Delta X_i = \Gamma_i(\underline{X},\underline{Y})$, l'augmentation par $\varepsilon(X_i) = 0$. On a ainsi associé à toute loi de groupe formel Γ sur B un groupe formel lisse et connexe, de dimension finie sur B , que nous notons G_Γ .

Si, de plus, B est local, on voit que, réciproquement, étant donné un groupe formel G lisse et connexe de dimension finie d sur B , d'algèbre affine R , le choix d'un système de coordonnées (i.e. le choix d'un d-uple $X_1,X_2,\ldots,X_d$ d'éléments de R relevant une base de $t^*_G(B)$ sur B) permet d'associer à G une loi de groupe formel à d paramètres sur B .

2.2. Pour tout anneau commutatif B et tout entier $d\ge 1$, nous notons $\Lambda^d(B) = B[[X_1,X_2,\ldots,X_d]]$ l'anneau des séries formelles en les d variables $X_1,X_2,\ldots,X_d$ à coefficients dans B . Si, pour tout $\underline{i} = (i_1,i_2,\ldots,i_d)$, on pose $\underline{X}^{\underline{i}} = X_1^{i_1}X_2^{i_2}\ldots X_d^{i_d}$, tout élément de $\Lambda^d(B)$ s'écrit, d'une manière et d'une seule, sous la forme $\sum_{\underline{i}\in\mathbb{N}^d} a_{\underline{i}}\underline{X}^{\underline{i}}$, avec les $a_{\underline{i}}\in B$. Nous notons $\Lambda^d_0(B)$ l'idéal de $\Lambda^d(B)$ formé des séries formelles sans terme constant.

Lorsque B est un anneau topologique, on munit $\Lambda^d(B)$ de la topologie produit ; l'idéal $\Lambda^d_0(B)$ est alors fermé dans $\Lambda^d(B)$.

On munit $A = W(k)$ et son corps des fractions K de la topologie p-adique et on note $K[[\underline{F}]]$ (resp. $A[[\underline{F}]]$) l'anneau topologique (avec la topologie produit) des séries formelles (non commutatives si $k\ne\mathbb{F}_p$) $\sum_{i=0}^{\infty} a_i\underline{F}^i$, à coefficients dans K (resp. A), avec la règle $\underline{F}a = \sigma(a)\underline{F}$, pour tout $a\in K$ (resp. A). On voit que $A[[\underline{F}]]$ s'identifie au séparé complété du sous-anneau $A[\underline{F}]$ de $D_k = A[\underline{F},\underline{V}]$ pour la topologie $\underline{F}$-adique.

On peut munir le K-espace vectoriel topologique $\Lambda^d_0(K)$ d'une structure de $K[[\underline{F}]]$-module topologique à gauche en posant

$$\underline{F}(\sum a_{\underline{i}} \underline{X}^{\underline{i}}) = \sum \sigma(a_{\underline{i}}) \underline{X}^{p\underline{i}} .$$

Avec les conventions du n° II.5.4, on voit que $\Lambda^d(A)$ est un A-anneau spécial et que (cf. n° II.5.5) $P(\Lambda^d(A))$ s'identifie au sous-A-module fermé de $\Lambda^d(K)$ formé des $\sum a_{\underline{i}} \underline{X}^{\underline{i}}$ tels que $i_j a_{\underline{i}} \in A$, pour tout $\underline{i} = (i_1, i_2, \ldots, i_d) \in \mathbb{N}^d$ et pour $j = 1, 2, \ldots, d$.

Nous notons $P(\Lambda_0^d(A))$ l'intersection de $P(\Lambda^d(A))$ avec $\Lambda_0^d(K)$. On voit que c'est un sous-$A[[\underline{F}]]$-module fermé de $\Lambda_0^d(K)$ qui contient lui-même $p\Lambda_0^d(A)$ comme sous-$A[[\underline{F}]]$-module fermé. En particulier le quotient $P(\Lambda_0^d(A))/p\Lambda_0^d(A)$ est muni d'une structure de $A[[\underline{F}]]$-module topologique.

Si l'on pose $\mathcal{R} = \Lambda^d(A)$, on voit que l'anneau $\mathcal{R}_k = \mathcal{R} \otimes_A k = \mathcal{R}/p\mathcal{R}$ s'identifie à $\Lambda^d(k)$. On a défini au n° II.5.7 un isomorphisme de A-modules topologiques $w_{\mathcal{R}} : \widehat{CW}_k(\mathcal{R}_k) \to P(\mathcal{R})/p\mathcal{R}$, autrement dit

$$w_{\mathcal{R}} : \widehat{CW}_k(\Lambda^d(k)) \to P(\Lambda^d(A))/p\Lambda^d(A) .$$

On voit tout de suite que la restriction de $w_{\mathcal{R}}$ au sous-A-module fermé $\widehat{CW}_k(\Lambda_0^d(k))$, formé des covecteurs dont toutes les composantes sont des séries formelles sans terme constant, induit un isomorphisme

$$w^d : \widehat{CW}_k(\Lambda_0^d(k)) \to P(\Lambda_0^d(A))/p\Lambda_0^d(A) .$$

Il est clair que $\widehat{CW}_k(\Lambda_0^d(k))$ n'est autre que $\widehat{CW}_k^c(\Lambda^d(k))$ et que l'action de $\underline{F}$ sur ce module est topologiquement nilpotente. Ceci permet de considérer $\widehat{CW}_k(\Lambda_0^d(k))$ comme un $A[[\underline{F}]]$-module topologique et on vérifie facilement que w^d est, en fait, un isomorphisme de $A[[\underline{F}]]$-modules topologiques.

2.3. Soit Γ une loi de groupe formel à d paramètres sur A. Posons

$$\mathcal{MH}(\Gamma) = \{\alpha \in P(\Lambda^d(A)) \mid \alpha(\Gamma(\underline{X},\underline{Y})) - \alpha(\underline{X}) - \alpha(\underline{Y}) \in p\Lambda^{2d}(A)\} ,$$

$$\mathcal{MH}_0(\Gamma) = \{\alpha \in P(\Lambda_0^d(A)) \mid \alpha(\Gamma(\underline{X},\underline{Y})) - \alpha(\underline{X}) - \alpha(\underline{Y}) \in p\Lambda_0^{2d}(A)\} .$$

On voit que ce sont des sous-A-modules fermés de $P(\Lambda^d(A))$, que $\mathcal{MH}_0(\Gamma) = \mathcal{MH}(\Gamma) \cap P(\Lambda_0^d(A))$, que $\mathcal{MH}(\Gamma) = pA \oplus \mathcal{MH}_0(\Gamma)$ et que, avec les notations du n° IV.1.1, $\mathcal{MH}(\Gamma) = \mathcal{MH}(G_\Gamma)$.

Si l'on pose, en outre

$$\mathcal{L}(\Gamma) = \{\alpha \in P(\Lambda^d(A)) \mid \alpha(\Gamma(\underline{X},\underline{Y})) = \alpha(\underline{X}) + \alpha(\underline{Y})\} ,$$

on voit que $\mathcal{L}(\Gamma) \subset \mathcal{M}\mathcal{H}_0(\Gamma)$ et que $\mathcal{L}(\Gamma) = \mathcal{L}(G_\Gamma)$.

De plus, il est clair que le quotient $MH(\Gamma) = \mathcal{M}\mathcal{H}(\Gamma)/p\Lambda^d(A)$, qui n'est autre que $MH(G_\Gamma)$, s'identifie canoniquement à $\mathcal{M}\mathcal{H}_0(\Gamma)/p\Lambda_0^d(A)$.

Comme G_Γ est connexe, $MH(\Gamma) = MH(G_\Gamma)$ peut être considéré comme un $A[[\underline{F}]]$-module à gauche. On voit tout de suite que $\mathcal{M}\mathcal{H}_0(\Gamma)$ est un sous-$A[[\underline{F}]]$-module fermé de $P(\Lambda_0^d(A))$ et que la structure de $A[[\underline{F}]]$-module sur $MH(\Gamma)$ est la structure quotient.

Soit $\rho(\Gamma)$ l'application A-linéaire

$$\mathcal{L}(\Gamma) \xrightarrow{\text{incl.}} \mathcal{M}\mathcal{H}_0(\Gamma) \xrightarrow{\text{proj.can.}} MH(\Gamma) .$$

On sait (cf. remarque 2 du n° III.6.1) que se donner un D_k-module profini M sur lequel l'action de $\underline{F}$ est injective tel que $\dim_k M/\underline{F}M < +\infty$ revient à se donner un $A[[\underline{F}]]$-module à gauche de type fini sur lequel l'action de $\underline{F}$ est injective et qui vérifie $pM \subset \underline{F}M$. La catégorie Λ_A^c définie au n° IV.1.2 peut donc être considérée comme la catégorie dont les objets sont les triplets $(\mathcal{L}, M, \rho)$

- où M est un $A[[\underline{F}]]$-module à gauche de type fini, avec action de $\underline{F}$ injective, tel que $pM \subset \underline{F}M$,
- où $\mathcal{L}$ est un A-module libre de rang fini,
- où $\rho : \mathcal{L} \to M$ est une application A-linéaire telle que l'application $\tilde{\rho} : \mathcal{L}/p\mathcal{L} \to M/\underline{F}M$ induite par ρ , par passage aux quotients, est un isomorphisme.

En paraphrasant les résultats du § 1 du chapitre IV, on voit alors que la correspondance $\Gamma \to \mathcal{L}MH(\Gamma) = (\mathcal{L}(\Gamma), MH(\Gamma), \rho(\Gamma))$ peut être considérée, de manière évidente, comme un foncteur contravariant additif de la catégorie des lois de groupe formel sur A dans Λ_A^c , qui induit une anti-équivalence entre ces deux catégories.

On voit, en outre, que $\mathcal{M}\mathcal{H}(\Gamma)$ et $MH(\Gamma)$ ne dépendent que de la réduction Γ_k de Γ modulo p et que le foncteur, qui à Γ_k associe $MH(\Gamma_k) = MH(\Gamma)$ (où Γ est un relèvement arbitraire de Γ_k) , induit une anti-équivalence entre la catégorie des lois de groupe formel sur k et celle des $A[[\underline{F}]]$-modules à gauche, de type fini, avec action de $\underline{F}$ injective et

$pM \subset \underline{F}M$.

Ces résultats sont essentiellement, et au langage près, ceux de Honda ([32]) dans le cas particulier où la base est soit A soit k . Nous nous proposons, dans les n^{os} suivants, d'indiquer comment se construit le "dictionnaire"; cela revient, en fait, à expliquer comment on peut construire explicitement le triplet $\mathcal{L}MH(\Gamma)$ à partir de la connaissance du "logarithme" de Γ et vice-versa.

2.4. Pour tout entier $d \geq 1$, notons $\mathfrak{A}_d$ l'anneau des matrices carrées (d,d) à coefficients dans $A[[\underline{F}]]$. Avec des notations évidentes, toute matrice $u \in \mathfrak{A}_d$ peut s'écrire, d'une manière et d'une seule, sous la forme $u = \sum_{\nu=0}^{\infty} C_\nu \underline{F}^\nu$, avec les C_ν des matrices carrées (d,d) à coefficients dans A . Avec Honda, disons qu'une matrice $u = \sum_{\nu=0}^{\infty} C_\nu \underline{F}^\nu \in \mathfrak{A}_d$ est <u>spéciale</u> si $C_0 = p \cdot 1_d$ (où 1_d est la matrice unité).

Soit maintenant $(\mathcal{L}, M, \rho)$ un objet de Λ_A^c et soit $(\ell_i)_{1 \leq i \leq d}$ une base de $\mathcal{L}$ sur A . Pour tout i , posons $\tilde{\ell}_i = \rho(\ell_i)$. Comme $\tilde{\rho}$ est un isomorphisme, les $\tilde{\ell}_i$ engendrent M comme $A[[\underline{F}]]$-module. Comme $pM \subset \underline{F}M$, on voit qu'il existe des éléments $a_{ij} \in A[[\underline{F}]]$ tels que, pour $1 \leq i \leq d$,

$$p \cdot \tilde{\ell}_i = \sum_{j=1}^{d} a_{ij} \underline{F} \tilde{\ell}_j .$$

Autrement dit, si l'on note $u \in \mathfrak{A}_d$ la matrice $p \cdot 1_d - (a_{ij})\underline{F}$, on voit que u est une matrice spéciale et que l'on a

$$u \cdot \tilde{\ell} = 0 ,$$

en notant $\tilde{\ell}$ la matrice colonne des $\tilde{\ell}_i$.

Cette matrice spéciale u n'est, bien sûr, pas uniquement déterminée. Outre le fait qu'elle dépend du choix d'une base de $\mathcal{L}$, on voit qu'elle est définie à multiplication à gauche par un élément de A_d de la forme $1 + \sum_{\nu=1}^{\infty} C_\nu \underline{F}^\nu$ près.

Réciproquement, à toute matrice spéciale $u \in \mathfrak{A}_d$, on peut associer un objet $(\mathcal{L}, M, \rho)$ de Λ_A^c , muni d'une base de $\mathcal{L}$ sur A :

- on pose $\mathcal{L} = A^d$;
- si $(e_i)_{1 \leq i \leq d}$ est la base canonique du $A[[\underline{F}]]$-module à gauche $(A[[\underline{F}]])^d$,

et si u est la matrice des u_{ij} , on note M le quotient de $(A[[\underline{F}]])^d$ par le sous-$A[[\underline{F}]]$-module engendré par les $\sum_{j=1}^{d} u_{ij}e_j$, pour $1 \leq i \leq d$;

- si $(\ell_i)_{1\leq i\leq d}$ est la base canonique de $\mathfrak{L} = A^d$, l'application ρ est celle qui à ℓ_i associe l'image de e_i dans M .

2.5. Soit Γ une loi de groupe formel à d paramètres sur A et soit $(\mathfrak{L}, M, \rho) = \mathfrak{L}MH(\Gamma)$.

Il résulte facilement du n° 2.3 que, pour $i = 1,2,\dots,d$, il existe un élément $\ell_i \in \mathfrak{L}$ et un seul tel que $\ell_i \equiv X_i \pmod{(\Lambda_0^d(K))^2}$ et que le d-uple $\ell_1, \ell_2, \dots, \ell_d$ est une base de $\mathfrak{L}$ sur A ; nous le notons ℓ_Γ et l'appelons <u>la base canonique de</u> $\mathfrak{L}$ (Honda l'appelle le "<u>transformer</u>" de Γ). Il est commode de considérer ℓ_Γ comme le vecteur colonne

$$\begin{pmatrix} \ell_1 \\ \ell_2 \\ \vdots \\ \ell_d \end{pmatrix}$$

et nous notons $\tilde{\ell}_\Gamma$ le vecteur colonne des $\tilde{\ell}_i = \rho(\ell_i)$.

Soit alors $u \in \mathfrak{A}_d$ une matrice spéciale telle que $u\cdot\tilde{\ell}_\Gamma = 0$. Pour $i = 1,2,\dots,d$, la i-ème composante du vecteur colonne $u\cdot\ell_\Gamma$ appartient au noyau de la projection de $P(\Lambda_0^d(A))$ sur $P(\Lambda_0^d(A))/p\Lambda_0^d(A)$ et est donc de la forme $p\alpha_i$, avec $\alpha_i \in \Lambda_0^d(A)$. Comme $u = p1_d + v\underline{F}$, avec $v \in \mathfrak{A}_d$, on voit que

$$\alpha_i \equiv X_i \pmod{(\Lambda_0^d(A))^2} .$$

Connaissant ℓ_Γ , on peut calculer explicitement une matrice spéciale u telle que $u\cdot\tilde{\ell}_\Gamma = 0$: on cherche u sous la forme $u = \sum_{\nu=0}^{\infty} C_\nu \underline{F}^\nu$, avec les C_ν des matrices à coefficients dans A , et les C_ν se calculent de proche en proche : on a $C_0 = p\cdot 1_d$ et, si $C_0, C_1, \dots, C_{\nu-1}$ sont choisis, C_ν est le relèvement arbitraire d'une matrice à coefficients dans k qui est uniquement déterminée : soit ℓ'_i la i-ème composante du vecteur colonne $(C_0 + C_1\underline{F} + \dots + C_{\nu-1}\underline{F}^{\nu-1})\cdot\ell_\Gamma$; on voit que $\ell'_i \in p\Lambda_0^d(A) + \underline{F}^\nu\Lambda_0^d(K)$ et que, pour toute matrice $C = (c_{ij})$, à coefficients dans A , la i-ème composante ℓ''_i de $(C_0 + C_1\underline{F} + \dots + C_{\nu-1}\underline{F}^{\nu-1} + C\underline{F}^\nu)\cdot\ell_\Gamma$ vérifie

$$\ell_i'' \equiv \ell_i' + \sum_{j=1}^{d} \sigma^{\nu}(c_{ij})X_j^{p^{\nu}} \pmod{(\Lambda_0^d(K))^{p^{\nu}+1}} ;$$

il doit donc exister des $c'_{ij} \in A$ tels que

$$\ell_i' \equiv \sum_{j=1}^{d} c'_{ij}X_j^{p^{\nu}} \pmod{p\Lambda_0^d(A) + (\Lambda_0^d(K))^{p^{\nu}+1}}$$

et la matrice $C_{\nu} = (c_{ij})$ est déterminée, modulo p, par

$$c_{ij} \equiv -\sigma^{-\nu}(c'_{ij}) \pmod{pA} , \text{ pour } 1 \leq i,j \leq d .$$

2.6. Réciproquement, soit $(\mathfrak{L}, M, \rho)$ un objet de Λ_A^c. Choisissons une base $\ell_1, \ell_2, \dots, \ell_d$ de $\mathfrak{L}$ sur A et soit $u \in \mathfrak{U}_d$ une matrice spéciale telle que, avec des notations évidentes, $u \cdot \tilde{\ell} = 0$. Si l'on veut que ℓ s'identifie à la base canonique ℓ_{Γ} du A-module $\mathfrak{L}(\Gamma)$ d'une loi de groupe formel Γ définie sur A, telle que $(\mathfrak{L}, M, \rho)$ s'identifie à $\mathfrak{L}MH(\Gamma)$, il résulte de ce qui précède qu'il doit exister un d-uple $\alpha_1, \alpha_2, \dots, \alpha_d$ d'éléments de $\Lambda_0^d(A)$, vérifiant $\alpha_i \equiv X_i \pmod{(\Lambda_0^d(A))^2}$ pour tout i, tel que, si on appelle α le vecteur colonne dont la i-ème composante est α_i, on ait

$$u \cdot \ell_{\Gamma} = p\alpha .$$

On voit que, pour α fixé, cette équation a une solution et une seule dans $(\Lambda_0^d(K))^d$ (la matrice u est inversible dans l'anneau des matrices carrées (d,d) à coefficients dans $K[[\underline{F}]]$ et on a $\ell_{\Gamma} = u^{-1} \cdot p\alpha = pu^{-1} \cdot \alpha$) et que cette solution est, en fait, un vecteur colonne dont les composantes sont à coefficients dans $P(\Lambda_0^d(A))$.

Il n'est alors pas difficile de vérifier, en utilisant les résultats rappelés au n° 2.2, que, pour toute base $\ell_1, \ell_2, \dots, \ell_d$ de $\mathfrak{L}$ sur A, toute matrice spéciale $u \in \mathfrak{U}_d$ telle que $u \cdot \tilde{\ell} = 0$, tout d-uple $\alpha_1, \alpha_2, \dots, \alpha_d$ d'éléments de $\Lambda_0^d(A)$ satisfaisant $\alpha_i \equiv X_i \pmod{(\Lambda_0^d(A))^2}$, si l'on pose $\ell_{\Gamma} = pu^{-1} \cdot \alpha$, l'unique d-uple $\Gamma(\underline{X}, \underline{Y})$ de séries formelles sans terme constant, à coefficients dans K, vérifiant $\ell_{\Gamma}(\Gamma(\underline{X}, \underline{Y})) = \ell_{\Gamma}(\underline{X}) + \ell_{\Gamma}(\underline{Y})$, est une loi de groupe formel définie sur A (i.e. les coefficients de Γ sont, en fait, dans A) telle que $\mathfrak{L}MH(\Gamma)$ s'identifie à $(\mathfrak{L}, M, \rho)$. On vérifie en outre qu'en faisant varier la base $\ell_1, \ell_2, \dots, \ell_d$, la matrice u et le d-uple α, on obtient toutes les lois de groupe formel définies sur A telles que $\mathfrak{L}MH(\Gamma) \simeq (\mathfrak{L}, M, \rho)$ (en fait il suffit de faire varier la base et, la base étant choisie, soit de fixer u et faire varier α , soit de fixer α et de faire varier u) .

Tous les résultats que nous avons obtenus sur les groupes formels lisses et connexes, de dimension finie, sur A ou sur k , peuvent alors se traduire en termes de matrices spéciales : on retrouve ainsi les énoncés de Honda.

Remarque : Honda travaille, en fait, dans un cadre plus général : la base $\mathfrak{O}$ est l'anneau des entiers d'un corps de caractéristique 0 muni d'une valuation discrète, à corps résiduel k de caractéristique $p \neq 0$. Honda suppose donné, en outre, un endomorphisme τ de $\mathfrak{O}$ induisant, par réduction modulo l'idéal maximal, un endomorphisme $\tilde{\tau}$ de k qui est une puissance strictement positive du Frobenius absolu. Honda construit alors une famille de lois de groupe formel définies sur $\mathfrak{O}$; il montre que, lorsque p est une uniformisante de $\mathfrak{O}$ et $\tilde{\tau}$ est le Frobenius absolu, il obtient ainsi toutes les lois de groupes formels définies sur $\mathfrak{O}$. Lorsque $\mathfrak{O}$ est complet et k parfait, L. Cox (dans le cas de dimension 1, cf. [9] et [10]) et J.M. Decauwert (dans le cas général, cf. [11] et [12]) ont montré que les lois de groupe formel construites par Honda sont exactement celles qui, après une éventuelle extension non ramifiée des scalaires, peuvent être munies d'une structure de A-module formel, où A est un sous-anneau de $\mathfrak{O}$ tel que l'extension $\mathfrak{O}/A$ est non ramifiée. Decauwert explique en outre comment ces constructions peuvent s'interpréter en termes de modules de Dieudonné.

§ 3.- Théorie de Cartier (courbes typiques)

Dans ce paragraphe, les hypothèses et les notations sont celles du chapitre III.

3.1. Appelons D_k-module à gauche (resp. à droite) de type ℓcf tout D_k-module à gauche (resp. à droite) M séparé et complet pour la topologie $\underline{F}$-adique sur lequel l'action de $\underline{F}$ est injective et qui est tel que $M/\underline{F}M$ (resp. $M/M\underline{F}$) est de dimension finie sur k .

Les D_k-modules à gauche (resp. à droite) de type ℓcf forment une sous-catégorie pleine de la catégorie des D_k-modules topologiques à gauche (resp. à droite). On sait (prop. 6.1 du chap. III) que le foncteur $\underline{M}$ induit une anti-équivalence entre la catégorie des groupes formels lisses et connexes de dimension finie sur k et celle des D_k-modules à gauche de type ℓcf .

Nous nous proposons de construire une dualité entre D_k-modules à gauche de type ℓcf et D_k-modules à droite de type ℓcf .

3.2. Pour tout entier $n \geq 1$, posons $B_n = p^{-n}A/A$, et considérons le A-module $\Theta_k^{\ell c} = \prod_{n \geq 1} B_n$. Avec des notations évidentes, tout élément de $\Theta_k^{\ell c}$ s'écrit d'une manière et d'une seule sous la forme $\sum_{n \geq 1} b_n T'_n$, avec $b_n \in p^{-n}A/A$.

Posons en outre $T'_0 = 0$. On munit $\Theta_k^{\ell c}$ d'une structure de D_k-bimodule en posant

$$\begin{cases} \lambda(\sum b_n T'_n) = \sum \lambda b_n T'_n , & \text{pour tout } \lambda \in A , \\ \underline{F}(\sum b_n T'_n) = \sum \sigma(b_n) T'_{n+1} , \\ \underline{V}(\sum b_n T'_n) = \sum p\sigma^{-1}(b_n) T'_{n-1} , \end{cases}$$

et

$$\begin{cases} (\sum b_n T'_n)\lambda = \sum \sigma^n(\lambda) b_n T'_n , & \text{pour tout } \lambda \in A , \\ (\sum b_n T'_n)\underline{F} = \sum b_n T'_{n+1} , \\ (\sum b_n T'_n)\underline{V} = \sum p b_n T'_{n-1} . \end{cases}$$

Il est clair que $\Theta_k^{\ell c}$ est un D_k-module à gauche (resp. à droite) séparé et complet pour la topologie $\underline{F}$-adique, sur lequel l'action de $\underline{F}$ est injective.

Pour tout D_k-module à gauche M de type ℓcf , notons $M^{\vee} = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}g}(M, \Theta_k^{\ell c})$ le D_k-module à droite des applications D_k-linéaires à gauche continues de M dans $\Theta_k^{\ell c}$; on voit que $M^{\vee}$ est un D_k-module à droite, séparé et complet pour la topologie $\underline{F}$-adique, sur lequel l'action de $\underline{F}$ est injective. Il est clair que la correspondance $M \mapsto M^{\vee}$ est, de manière évidente, un foncteur contravariant additif.

On définit de la même manière un foncteur contravariant additif de la catégorie des D_k-modules à droite de type ℓcf dans celle des D_k-modules à gauche, séparés et complets pour la topologie $\underline{F}$-adique, avec action de $\underline{F}$ injective : à N on associe $N^{\wedge} = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}d}(N, \Theta_k^{\ell c})$.

PROPOSITION 3.1.-

i) <u>Si</u> M (<u>resp</u>. N) <u>est un</u> D_k-<u>module à gauche</u> (<u>resp</u>. <u>à droite</u>) <u>de type</u> ℓcf , $M^\vee$ (<u>resp</u>. $N^\wedge$) <u>est un</u> D_k-<u>module à droite</u> (<u>resp</u>. <u>à gauche</u>) <u>de type</u> ℓcf .

ii) <u>Le foncteur</u> $M \mapsto M^\vee$ <u>induit une anti-équivalence entre</u> D_k-<u>modules à gauche de type</u> ℓcf <u>et</u> D_k-<u>modules à droite de type</u> ℓcf <u>et le foncteur</u> $N \mapsto N^\wedge$ <u>est un quasi-inverse</u>.

<u>Démonstration</u> : on a défini au n° III.5.2 le D_k-bimodule ΘT_k formé des éléments de la forme $\sum\limits_{n\in\mathbb{Z}} a_n T_n$, avec

$$a_n \begin{cases} \in K/A & \text{si} \quad n < 0 \\ \in K/p^{-n}A & \text{si} \quad n \geq 0 . \end{cases}$$

Pour tout entier $r \geq 0$, soit $\Theta T_{k,r}$ le sous-D_k-bimodule de ΘT_k formé des $\sum a_n T_n$ vérifiant

$$a_n \begin{cases} = 0 & \text{si} \quad n \leq -r \\ \in p^{-n-r}A/A & \text{si} \quad -r < n \leq 0 \\ \in p^{-n-r}A/p^{-n}A & \text{si} \quad n > 0 . \end{cases}$$

Notons $\Theta T_k^{(r)}$ le D_k-bimodule qui

- en tant que D_k-module à gauche est $\Theta T_{k,r}$,
- en tant que D_k-module à droite est le module déduit de $\Theta T_{k,r}$ par l'extension des scalaires σ^r .

Autrement dit, $\Theta T_k^{(r)}$ s'identifie en tant qu'ensemble à $\Theta T_{k,r}$; l'action de D_k à gauche est la même et celle de D_k à droite est définie par, pour tout $\sum a_n T_n \in \Theta T_k^{(r)}$,

$$\begin{cases} (\sum a_n T_n)\lambda = \sum \sigma^{n-r}(\lambda) a_n T_n , \text{ pour tout } \lambda \in A , \\ (\sum a_n T_n)\underline{F} = \sum a_n T_{n+1} \\ (\sum a_n T_n)\underline{V} = \sum p a_n T_{n-1} . \end{cases}$$

On voit tout de suite que l'application $\eta_r : \Theta T_k^{(r+1)} \to \Theta T_k^{(r)}$, qui à $\sum a_n T_n$ associe $\sum a_n T_{n+1}$, est D_k-linéaire à gauche et à droite, surjective ; son noyau est formé des $a \in \Theta T_k^{(r+1)}$ tels que $\underline{F}a = 0$, ce qui équivaut à $a\underline{F} = 0$.

On voit aussi que l'application $\eta^{(r)} : \Theta_k^{\ell c} \to \Theta T_k^{(r)}$, qui à $\sum_{n=1}^{\infty} b_n T'_n$ associe $\sum_{n=1}^{\infty} b_n T_{n-r}$, est D_k-linéaire à gauche et à droite, surjective ; son noyau est $\underline{F}^r \Theta_k^{\ell c} = \Theta_k^{\ell c} \underline{F}^r$. Comme, en outre, $\eta_r \circ \eta^{(r+1)} = \eta^{(r)}$, $\Theta_k^{\ell c}$ s'identifie à $\varprojlim \Theta T_k^{(r)}$ en tant que D_k-module topologique, à gauche aussi bien qu'à droite (la topologie étant la topologie $\underline{F}$-adique sur $\Theta_k^{\ell c}$ et la topologie de la limite projective, avec topologie discrète sur les quotients, sur $\varprojlim \Theta T_k^{(r)}$). Dans cette identification, $\Theta T_k^{(r)}$ est le conoyau de $\underline{F}^r$ dans $\Theta_k^{\ell c}$ (comme module à gauche aussi bien qu'à droite).

Soit alors M un D_k-module, par exemple à gauche, de type ℓcf . On a $M^{\vee} = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}g}(M,\Theta_k^{\ell c}) = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}g}(M,\varprojlim \Theta T_k^{(r)}) = \varprojlim \mathrm{Hom}_{D_k\text{-}g}(M,\Theta T_k^{(r)}) =$
$= \varprojlim \mathrm{Hom}_{D_k\text{-}g}(M/\underline{F}^r M,\Theta T_k^{(r)})$.

Pour tout D_k-module à gauche L , notons $L^{(-r)}$ le D_k-module à gauche déduit de L par l'extension des scalaires σ^{-r} (on convient en outre d'identifier L et $L^{(-r)}$ comme $\mathbb{Z}_p[\underline{F},\underline{V}]$-modules en posant $a = 1 \otimes a$) . Soit $\nu_r : \Theta T_k^{(r)} \to \Theta T_{k,r}$ l'application qui à $\sum a_n T_n$ associe $\sum \sigma^r(a_n) T_n$. On vérifie immédiatement que, pour tout D_k-module à gauche L , l'application qui à $\varphi \in \mathrm{Hom}_{D_k\text{-}g}(L,\Theta T_k^{(r)})$ associe $\nu_r \circ \varphi$ définit un isomorphisme du D_k-module à droite $\mathrm{Hom}_{D_k\text{-}g}(L,\Theta T_k^{(r)})$ sur $\mathrm{Hom}_{D_k\text{-}g}(L^{(-r)},\Theta T_{k,r})$.

On peut donc identifier $\mathrm{Hom}_{D_k\text{-}g}(M/\underline{F}^r M,\Theta T_k^{(r)})$ à

$$\mathrm{Hom}_{D_k\text{-}g}((M/\underline{F}^r M)^{(-r)},\Theta T_{k,r}) = \mathrm{Hom}_{D_k\text{-}g}(M^{(-r)}/\underline{F}^r M^{(-r)},\Theta T_{k,r}) .$$

Comme il est clair que $\Theta T_{k,r}$ est le noyau de $\underline{F}^r$ dans ΘT_k , considéré comme D_k-module à gauche, on a aussi

$$\mathrm{Hom}_{D_k\text{-}g}(M/\underline{F}^r M,\Theta T_k^{(r)}) = \mathrm{Hom}_{D_k\text{-}g}(M^{(-r)}/\underline{F}^r M^{(-r)},\Theta T_k) .$$

Autrement dit, avec les conventions du n° III.5.2, $\mathrm{Hom}_{D_k\text{-}g}(M/\underline{F}^r M,\Theta T_k^{(r)})$ s'identifie canoniquement au dual $(M^{(-r)}/\underline{F}^r M^{(-r)})^*$ du D_k-module à gauche fini $M^{(-r)}/\underline{F}^r M^{(-r)}$. On a donc $M = \varprojlim (M^{(-r)}/\underline{F}^r M^{(-r)})^*$ et il est facile de voir quelle est l'application de transition

$$f_r^* : (M^{(-r-1)}/\underline{F}^{r+1} M^{(-r-1)})^* \longrightarrow (M^{(-r)}/\underline{F}^r M^{(-r)})^* :$$

le Frobenius $\underline{F}$ définit une application D_k-linéaire à gauche de $M^{(-r)}$ dans

$M^{(-r-1)}$ qui induit, par passage aux quotients, une application D_k-linéaire à gauche

$$f_r : M^{(-r)}/\underline{F}^r M^{(-r)} \longrightarrow M^{(-r-1)}/\underline{F}^{r+1} M^{(-r-1)} ,$$

et f_r^* est la flèche duale. En particulier, comme l'action de $\underline{F}$ sur M est injective, f_r est injective et f_r^* est surjective.

On en déduit immédiatement que $(M^{(-r)}/\underline{F}^r M^{(-r)})^*$ s'identifie à $M^\vee/M^\vee\underline{F}^r$ et la proposition résulte facilement de la dualité entre D_k-modules finis à gauche et D_k-modules finis à droite définie par le foncteur $L \mapsto L^*$ (prop. 5.2 du chap. III).

3.3. Pour tout anneau commutatif R, nous notons $\Lambda(R) = R[[T]]$ l'anneau des séries formelles en une variable à coefficients dans R.

Soit G un groupe formel lisse et connexe de dimension finie sur k. Avec Cartier ([7]), nous appelons <u>courbe de</u> G tout élément du groupe topologique $G(\Lambda(k)) = G(k[[T]]) = \varprojlim G(k[T]/T^n)$ et nous notons $C(G)$ le groupe des courbes. Comme l'a remarqué Cartier, ce groupe est muni des endomorphismes suivants :

a) pour tout $x \in k$, on note $\langle x \rangle$ l'endomorphisme de $C(G)$ induit par l'unique endomorphisme du k-anneau profini $\Lambda(k)$ qui envoie T sur xT ;

b) pour tout entier $n \geq 1$, on note V_n l'endomorphisme de $C(G)$ induit par l'endomorphisme de $\Lambda(k)$ qui envoie T sur T^n ;

c) pour tout entier $n \geq 1$, notons $T_1, T_2, \ldots, T_n$ les n racines (distinctes ou non) du polynôme $X^n - T$ dans une clôture algébrique du corps des fractions de $\Lambda(k)$ et $\Lambda^{(n)}(k)$ le k-anneau profini $\Lambda(k)[T_1, T_2, \ldots, T_n]$; pour $1 \leq i \leq n$, soit ρ_i l'homomorphisme de $C(G)$ dans $G(\Lambda^{(n)}(k))$ induit par l'homomorphisme du k-anneau profini $\Lambda(k)$ dans $\Lambda^{(n)}(k)$ qui envoie T sur T_i ; on vérifie facilement que, pour tout $\varphi \in C(G)$, $\sum_{i=1}^{n} \rho_i \varphi$ provient d'un élément de $C(G)$ et d'un seul (par l'homomorphisme induit par l'inclusion de $\Lambda(k)$ dans $\Lambda^{(n)}(k)$) ; nous notons $F_n\varphi$ cet élément.

Une courbe $\varphi \in C(G)$ est dite <u>typique</u> si $F_n\varphi = 0$, pour tout entier n

premier à p . Il est clair que l'ensemble $CT(G)$ des courbes typiques de G est un sous-groupe fermé de $C(G)$ stable par les opérateurs $\langle x \rangle$, pour $x \in k$, F_p et V_p . On voit aussi que l'on peut considérer CT , de manière évidente, comme un foncteur additif de la catégorie des groupes formels lisses et connexes, de dimension finie sur k , dans celle des groupes abéliens topologiques, munis d'endomorphismes $\langle x \rangle$, pour $x \in k$, F_p et V_p .

Remarque : on évitera de confondre les groupes $C(G)$ et $CT(G)$ définis ici lorsque G est un groupe formel lisse et connexe de dimension finie sur k avec les groupes notés de la même manière définis au n° III.5.1 lorsque G est un p-groupe fini sur k .

3.4. Pour tout D_k-module à gauche M , notons $M^{(1)}$ le D_k-module à gauche déduit de M par l'extension des scalaires σ. (cf. n° IV.3.1). Si R est un k-anneau fini ou profini, on pose $\widehat{CW}_k^{(1)}(R) = (\widehat{CW}_k(R))^{(1)}$. Rappelons (id.) que tout élément de $\widehat{CW}_k^{(1)}(R)$ peut s'écrire comme un covecteur $(\dots,a_{-n},\dots,a_{-2},a_{-1})$ dont les composantes sont des éléments de R indexés par les entiers ≤ -1 . L'application v_R qui à $\underline{a} = (\dots,a_{-n},\dots,a_{-1},a_0) \in CW_k(R)$ associe $(\dots,a_{-n},\dots,a_{-2},a_{-1}) \in \widehat{CW}_k^{(1)}(R)$ est une application D_k-linéaire surjective de $\widehat{CW}_k(R)$ sur $\widehat{CW}_k^{(1)}(R)$ dont le noyau est le noyau de $\underline{V}$ dans $\widehat{CW}_k(R)$.

Soit $A = W(k)$ et soit $\mathcal{S} = \Lambda(A) = A[[T]]$; on a donc

$$\mathcal{S}_k = \mathcal{S}/p\mathcal{S} = \mathcal{S} \otimes_A k = k[[T]] = \Lambda(k) .$$

On a défini (cf. prop. 5.5 du chap.II) un isomorphisme $w_{\mathcal{S}} : \widehat{CW}_k(\mathcal{S}_k) \to P(\mathcal{S})/p\mathcal{S}$. On voit que l'image par $w_{\mathcal{S}}$ du noyau de $\underline{V}$ dans $\widehat{CW}_k(\mathcal{S}_k)$ est $\mathcal{S}/p\mathcal{S}$. On déduit donc de $w_{\mathcal{S}}$, par passage aux quotients, un isomorphisme

$$w_{\mathcal{S}}^{(1)} : \widehat{CW}_k^{(1)}(\mathcal{S}_k) \longrightarrow P(\mathcal{S})/\mathcal{S} .$$

Soit maintenant G un groupe formel lisse et connexe de dimension finie sur k , et soit $M = \underline{M}(G)$. On sait (cf. th.1 du chap. III) que, pour tout k-anneau fini R , le groupe $G(R)$ s'identifie, canoniquement et fonctoriellement, au groupe $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M,\widehat{CW}_k(R))$; il est clair que ce dernier groupe est canoniquement isomorphe au groupe $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M^{(1)},\widehat{CW}_k^{(1)}(R))$. Par passage à la limite, on voit que $C(G) = G(k[[T]])$ s'identifie à $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M^{(1)},\widehat{CW}_k^{(1)}(k[[T]]))$.

Finalement, l'application $w_{\mathfrak{S}}^{(1)}$ permet d'identifier le groupe $C(G)$ au groupe $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M^{(1)}, P(\mathfrak{S})/\mathfrak{S})$ (en munissant le A-module topologique $P(\mathfrak{S})/\mathfrak{S}$ de la structure de D_k-module topologique déduite de celle de $\widehat{CW}_k^{(1)}(k[[T]])$ par transport de structure).

On voit (cf. n° II.5.5) que $P(\mathfrak{S})$ est formé des séries formelles $\sum_{i=0}^{\infty} a_i T^i$, avec les $a_i \in K$ vérifiant $ia_i \in A$, pour tout i. Avec des notations évidentes, $P(\mathfrak{S})/\mathfrak{S}$ est le A-module formé des éléments de la forme $\sum_{i=0}^{\infty} a_i \tilde{T}^i$, avec $a_0 \in K/A$ et $a_i \in i^{-1}A/A$, pour $i \geq 1$. On voit facilement que l'action de $\underline{F}$ et $\underline{V}$ sur $P(\mathfrak{S})/\mathfrak{S}$ est définie par

$$\begin{cases} \underline{F}(\sum a_i \tilde{T}^i) = \sum \sigma(a_i)\tilde{T}^{ip} \\ \underline{V}(\sum a_i \tilde{T}^i) = \sum p\sigma^{-1}(a_{ip})\tilde{T}^i \ . \end{cases}$$

Considérons les endomorphismes suivants du A-module $P(\mathfrak{S})/\mathfrak{S}$:

a) pour tout $x \in k$, soit $\nu_x(\sum a_i \tilde{T}^i) = \sum [x]^i a_i \tilde{T}^i$ (où $[x]$ est le représentant multiplicatif de x dans $A = W(k)$) ;

b) pour tout entier $n \geq 1$, soit $v_n(\sum a_i \tilde{T}^i) = \sum a_i \tilde{T}^{ni}$;

c) pour tout entier $n \geq 1$, soit $f_n(\sum a_i \tilde{T}^i) = \sum n a_{in} \tilde{T}^i$.

On vérifie facilement que, lorsque l'on identifie $C(G)$ à $\mathrm{Hom}_{D_k}^{\mathrm{cont}}(M^{(1)}, P(\mathfrak{S})/\mathfrak{S})$, on a, pour tout $u \in C(G)$,

$$(1) \quad \begin{cases} \langle x \rangle u = \nu_x \circ u \ , & \text{pour tout } x \in k \ , \\ V_n u = v_n \circ u \ , & \text{pour tout entier } n \geq 1 \ , \\ F_n u = f_n \circ u \ , & \text{pour tout entier } n \geq 1 \ . \end{cases}$$

D'autre part, il est immédiat que l'application, qui à $\sum_{n=1}^{\infty} b_n T'_n \in \Theta_k^{\ell c}$ associe $\sum_{n=1}^{\infty} b_n \tilde{T}^{p^n} \in P(\mathfrak{S})/\mathfrak{S}$, est D_k-linéaire à gauche, injective. Nous l'utilisons pour identifier $\Theta_k^{\ell c}$ à un sous-D_k-module à gauche de $P(\mathfrak{S})/\mathfrak{S}$.

Les formules (1) montrent que si $u \in \mathrm{Hom}_{D_k}^{\mathrm{cont}}(M^{(1)}, P(\mathfrak{S})/\mathfrak{S})$ et si $n \geq 1$, on a $F_n u = 0$ si et seulement si l'image de u est contenue dans le sous-A-module de $P(\mathfrak{S})/\mathfrak{S}$ formé des $\sum a_i \tilde{T}^i$ tels que $a_{in} = 0$, pour tout $i \geq 0$. Si l'on veut que cette condition soit satisfaite pour tout entier n premier à p, on doit avoir $a_i = 0$ si i n'est pas une puissance de p et on en déduit qu'un élément $u \in \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M^{(1)}, P(\mathbb{S})/\mathbb{S})$ est une courbe typique si et seulement si l'image par u de $M^{(1)}$ est contenue dans $\Theta_k^{\ell c}$. On a donc démontré la proposition suivante :

PROPOSITION 3.2.- <u>Soit</u> G <u>un groupe formel lisse et connexe de dimension finie sur</u> k . <u>Le groupe</u> C(G) (resp. CT(G)) <u>s'identifie</u>, <u>canoniquement et fonctoriellement en</u> G , <u>au groupe</u> $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(\underline{M}^{(1)}(G), P(\mathbb{S})/\mathbb{S})$ (resp. $(\underline{M}^{(1)}(G))^{\vee} = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}g}(\underline{M}^{(1)}(G), \Theta_k^{\ell c})$ <u>(on a posé</u> $\underline{M}^{(1)}(G) = (\underline{M}(G))^{(1)}$) .

3.5. Rappelons que tout D_k-module à droite L peut être muni d'une structure de D_k-module à gauche en posant, pour tout $a \in L$,

$$\begin{cases} \lambda a = a\lambda \quad , \text{ pour tout } \lambda \in A , \\ \underline{F}a = a\underline{V} \quad , \\ \underline{V}a = a\underline{F} \quad . \end{cases}$$

Nous appelons cette structure la structure de D_k-module à gauche induite par la structure de D_k-module à droite.

PROPOSITION 3.3.- <u>Soit</u> G <u>un groupe formel lisse et connexe de dimension finie sur</u> k <u>et soit</u> $M^{(1)} = \underline{M}^{(1)}(G)$.

i) <u>il existe sur le groupe topologique</u> CT(G) <u>une structure de</u> D_k-<u>module topologique à gauche et une seule telle que</u>, <u>pour tout</u> $\varphi \in CT(G)$,

$$\begin{cases} [x]\varphi = \langle x\rangle\varphi \ , \ \underline{\text{pour tout}} \ \ x \in k \ , \\ \underline{F}\varphi = F_p\varphi \ \ \underline{\text{et}} \ \ \underline{V}\varphi = V_p\varphi \ , \end{cases}$$

ii) <u>lorsque l'on identifie</u> CT(G) <u>au groupe</u> $(M^{(1)})^{\vee} = \mathrm{Hom}^{\mathrm{cont}}_{D_k\text{-}g}(M^{(1)}, \Theta_k^{\ell c})$, <u>cette structure de</u> D_k-<u>module à gauche est celle qui est induite par la structure de</u> D_k-<u>module à droite de</u> $(M^{(1)})^{\vee}$.

<u>Démonstration</u> : il est clair que, s'il existe une structure de D_k-module topologique à gauche sur CT(G) vérifiant les conditions requises en (i) , celle-ci est unique. Il suffit donc, pour démontrer la proposition, de vérifier que CT(G) , muni de la structure de D_k-module à gauche induite par la structure de D_k-module à droite de $(M^{(1)})^{\vee}$ vérifie bien ces conditions ; autrement dit que, pour tout $u : M^{(1)} \to \Theta_k^{\ell c}$ et tout $a \in M^{(1)}$, on a

$$\begin{cases} ((\langle x\rangle u)(a) = u(a).[x] , \text{ pour tout } x \in k , \\ (V_p u)(a) = u(a).\underline{F} , \\ (F_p u)(a) = u(a).\underline{V} , \end{cases}$$

ce qui se fait facilement à l'aide des formules (1) .

Cette proposition nous permet de retrouver le résultat suivant dû à Cartier ([7]) :

COROLLAIRE. - <u>Appelons</u> D_k-<u>module à gauche de type</u> "<u>dual de</u> ℓcf" <u>tout</u> D_k-<u>module à gauche</u> L , <u>séparé et complet pour la topologie</u> <u>V-adique</u>, <u>sur lequel l'action de</u> V <u>est injective</u>, <u>tel que</u> L/VL <u>est de dimension finie sur</u> k . <u>Alors</u>,

i) <u>si</u> G <u>est un groupe formel lisse et connexe de dimension finie sur</u> k , CT(G) <u>est un</u> D_k-<u>module à gauche de type</u> "<u>dual de</u> ℓcf" ;

ii) <u>le foncteur</u> $G \mapsto CT(G)$ <u>induit une équivalence entre la catégorie des groupes formels lisses et connexes de dimension finie sur</u> k <u>et celle des</u> D_k-<u>modules à gauche de type</u> "<u>dual de</u> ℓcf".

En effet, CT s'identifie au composé des foncteurs $G \mapsto \underline{M}(G)$, $M \mapsto M^{(1)}$, $N \mapsto N^{\vee}$. Le premier induit une anti-équivalence entre la catégorie des groupes formels lisses et connexes, de dimension finie sur k , et celle des D_k-modules à gauche de type ℓcf (prop. 6.1 du chap.III). Le second induit visiblement une équivalence de la catégorie des D_k-modules à gauche de type ℓcf sur elle-même. Le troisième induit une anti-équivalence entre D_k-modules à gauche de type ℓcf et D_k-modules à droite de type ℓcf . Enfin, il est clair que, si L est un D_k-module à droite, alors L , muni de la structure de D_k-module à gauche induite, est de type "dual de ℓcf" si et seulement si L est un D_k-module à droite de type ℓcf .

<u>Remarque</u> : on peut aussi déduire très facilement des constructions qui précèdent le fait (dû à Cartier) que tout élément de C(G) s'écrit d'une manière et d'une seule sous la forme $\sum_{n \in I(p)} V_n \gamma_n$, avec $\gamma_n \in CT(G)$ (et où I(p) est l'ensemble des entiers > 0 premiers à p).

3.6. Lorsque l'on se restreint aux D_k-modules à gauche de type ℓcf qui sont libres de rang fini sur A (i.e. aux modules de Dieudonné des groupes p-divisibles connexes sur k), on peut donner une description plus simple de la dualité $M \to M^{\vee}$.

Soit, en effet, M un D_k-module à gauche, libre de rang fini sur A . Rappelons (cf. n° III.6.3) que l'on peut munir le A-module M^d des applications A-linéaires de M dans A d'une structure de D_k-module à gauche, en posant, pour tout $u \in M^d$ et tout $a \in M$,

$$(\underline{F}u)(a) = \sigma(u(\underline{V}a)) \quad \text{et} \quad (\underline{V}u)(a) = \sigma^{-1}(u(\underline{F}a)) ,$$

et que la correspondance $M \mapsto M^d$ définit une dualité dans la catégorie des D_k-modules à gauche qui sont des A-modules libres de rang fini.

PROPOSITION 3.4.- <u>Les restrictions des foncteurs</u> $M \mapsto M^d$ <u>et</u> $M \mapsto M^{\vee}$ <u>à la catégorie des</u> D_k-<u>modules à gauche qui sont simultanément libres de rang fini sur</u> A <u>et de type</u> ℓcf <u>sont naturellement équivalentes</u> (<u>on a muni</u> $M^{\vee}$ <u>de sa structure de</u> D_k-<u>module à gauche induite par sa structure de</u> D_k-<u>module à droite</u>).

<u>Démonstration</u> : soit M un D_k-module à gauche de type ℓcf , libre de rang fini sur A . Pour tout $u \in M^d$, soit $\rho_M(u) : M \to \Theta_k^{\ell c}$ l'application définie par

$$\rho_M(u)(a) = \sum_{n=1}^{\infty} p^{-n}\sigma^n(u(\underline{V}^n a))T'_n .$$

On vérifie facilement que $\rho_M(u)$ est D_k-linéaire à gauche, donc que, pour tout $u \in M^d$, $\rho_M(u) \in M^{\vee}$.

On vérifie aussi que $\rho_M : M^d \to M^{\vee}$ est D_k-linéaire à gauche, i.e. qu'elle est additive et que, pour tout $u \in M^d$, tout $a \in M$,

$$\begin{cases} \rho_M(\lambda u)(a) = \rho_M(u)(a).\lambda \ , \text{ pour tout } \lambda \in A \ , \\ \rho_M(\underline{V}u)(a) = \rho_M(u)(a).\underline{F} \ , \\ \rho_M(\underline{F}u)(a) = \rho_M(u)(a).\underline{V} \ . \end{cases}$$

Il est clair que ρ_M est fonctorielle en M et il suffit donc pour démontrer la proposition de vérifier que ρ_M est bijective. Sur M la topologie $\underline{F}$-adique et la topologie p-adique coïncident et il existe donc un entier $r \geq 1$ tel que $\underline{F}^r M \subset pM$, ce qui implique $F^{rm}M \subset p^m M$, pour tout entier $m \geq 1$.

Soit $u \in \operatorname{Ker} \rho_M$. On voit que, pour tout $a \in M$, $u(\underline{V}^n a) \in p^n A$, donc que $u(\underline{V}^n M) \subset p^n A$, pour tout entier $n \geq 0$. Comme $\underline{F}^{rm} M \subset p^m M$ implique $p^{rm} M = \underline{V}^{rm}\underline{F}^{rm} M \subset p^m \underline{V}^{rm} M$, on a, pour tout entier $m \geq 0$, $p^{rm}u(M) = u(p^{rm}M) \subset p^m u(\underline{V}^{rm}M) \subset p^{m+rm}A$, donc $u(M) \subset p^m A$; comme ceci est vrai pour tout m on a $u = 0$ et ρ_M est bien injective.

Pour tout $a \in M$, notons a_m l'unique élément de M tel que $\underline{F}^{rm}a = p^m a_m$. Soit u' un élément quelconque de $M^\vee$. Pour tout a fixé dans M , on voit que l'on peut écrire

$$u'(a_m) = \sum p^{-n}\sigma^n(b_{n,m})T'_n ,$$

où $b_{n,m} \in A$ et est uniquement déterminé modulo p^n . En écrivant que $\underline{F}^{rm}a = p^m a_m$, on montre facilement que $p^{(1-r)m}b_{rm,m} \in A$. En écrivant que $\underline{F}^r a_m = pa_{m+1}$, on vérifie que

$$p^{-rm}b_{rm,m} \equiv p^{-r(m+1)+1}b_{r(m+1),m+1} \pmod{A} .$$

On en déduit que la suite des $p^{(1-r)m}b_{rm,m}$ converge vers un élément $u(a) \in A$. Il n'y a alors pas de difficulté à vérifier que l'application $a \to u(a)$ de M dans A est A-linéaire, donc que $u \in M^d$ et que $\rho_M(u) = u'$, d'où la surjectivité.

COROLLAIRE.- Soit G un groupe p-divisible connexe sur k et soit $\mathbb{D}_p(G)$ son dual. Les D_k-modules à gauche $CT(G)$ et $\underline{M}^{(1)}(\mathbb{D}_p(G))$ sont isomorphes, canoniquement et fonctoriellement en G .

En effet, $CT(G)$ est canoniquement isomorphe à $(\underline{M}^{(1)}(G))^\vee$ (prop. 4.2), $(\underline{M}^{(1)}(G))^\vee$ s'identifie à $(\underline{M}^{(1)}(G))^d$ d'après la proposition précédente, on voit tout de suite que $(\underline{M}^{(1)}(G))^d$ s'identifie à $(\underline{M}(G)^d)^{(1)}$, et $\underline{M}(G)^d$ s'identifie à $\underline{M}(\mathbb{D}_p(G))$ d'après la proposition 6.4 du chap. III, donc $(\underline{M}(G)^d)^{(1)}$ s'identifie à $\underline{M}(\mathbb{D}_p(G))^{(1)} = \underline{M}^{(1)}(\mathbb{D}_p(G))$.

3.7. Remarques :

1.- Si G est un p-groupe formel sur k , la connaissance de $\underline{M}(G)$ est équivalente à celle de $(\underline{M}(G))^{(1)} = \underline{M}^{(1)}(G)$ (et on prendra garde que, suivant les auteurs, ce qui est appelé "module de Dieudonné de G" s'identifie soit à $\underline{M}(G)$, soit à $\underline{M}^{(1)}(G)$). On peut se demander s'il est plus commode de travailler avec $\underline{M}(G)$ ou avec $\underline{M}^{(1)}(G)$. Du point de vue adopté dans ce mémoire, on voit que cela est indifférent lorsque l'on travaille sur k , mais qu'il est plus commode de travailler avec $\underline{M}(G)$ lorsque l'on étudie les relèvements de G sur $W(k)$.

On a vu que, pour interpréter les résultats de Honda c'est $\underline{M}(G)$ qui convient le mieux, alors que pour ceux de Cartier c'est $\underline{M}^{(1)}(G)$ qui est le plus naturel.

Lorsque l'on veut relier nos résultats à la cohomologie de de Rham (à la manière de Oda, [41] , ou de Mazur-Messing, [38] , chap. I, § 4, via les extensions universelles), on s'aperçoit que c'est $\underline{M}^{(1)}(G)$ le plus naturel.

2.- Lorsque l'on veut relier nos constructions à l'étude des extensions universelles des groupes p-divisibles, les résultats s'énoncent plus commodément avec $\underline{M}^{(1)}(G)$, mais, pour les obtenir, on travaille simultanément avec $\underline{M}^{(1)}(G)$ et $\underline{M}(G)$: soit B un anneau qui est soit k , soit A' (anneau des entiers d'une extension finie totalement ramifiée, de degré e , du corps des fractions K de $A = W(k)$), soit $A'/\mathfrak{m}^{\nu}$ (où $\mathfrak{m}^{\nu}$ est une puissance non nulle de l'idéal maximal $\mathfrak{m}$ de A'). Soit $\widehat{CW}_B$ le B-groupe formel défini par restriction de CW aux B-anneaux finis (cf. n° II.4.1). On déduit facilement du § 2 du chapitre II que le sous-anneau $A[\underline{V}]$ de $D_k = A[\underline{F},\underline{V}]$ s'identifie canoniquement à un sous-anneau de l'anneau des endomorphismes de $\widehat{CW}_B$.

Soit G un groupe p-divisible sur B , soit $G_k = G \otimes_B k$ sa fibre spéciale et soit E_G l'extension universelle de G (cf. par exemple, [38] , chap. I, § 1). On peut montrer que, si $B = k$ ou $W(k)$, le complété formel $\hat{E}_G$ de E_G s'identifie canoniquement, et fonctoriellement en G , au B-foncteur en groupes formels

$$E'_G(R) = \mathrm{Hom}_{A[\underline{V}]}(\underline{M}^{(1)}(G_k), \widehat{CW}_B(R)) \text{ , pour tout B-anneau fini } R .$$

Ce résultat reste-t-il vrai dans le cas général (i.e. $B = A'$, avec $e \neq 1$, ou $B = A'/\mathfrak{m}^{\nu}$) ?

Notons, d'autre part, $N(G)$ le $A[\underline{V}]$-module à gauche $\mathrm{Hom}(\hat{E}_G, \widehat{CW}_B)$. On construit facilement une application $A[\underline{V}]$-linéaire à gauche de $N(G)$ dans $\underline{M}^{(1)}(G)$. Lorsque $B = A$, on peut montrer que cette application est un isomorphisme ; ceci reste-t-il vrai lorsque $B = A'$ (avec $e \neq 1$) ? Que peut-on dire dans le cas général ?

Nous reviendrons sur ces questions dans une publication ultérieure ; ceci nous permettra en particulier d'expliciter le lien entre nos travaux et ceux de Mazur-Messing ([38]) donc aussi ceux de Grothendieck et Messing ([29], [30], [39]).

BIBLIOGRAPHIE

[1] I. BARSOTTI, Moduli canonici e gruppi analitici commutativi, Ann. Scuola Norm. Sup. Pisa, 13 (1959), 303-372.

[2] I. BARSOTTI, Analytical Methods for Abelian Varieties in Positive Characteristic, Coll. Théorie des groupes algébriques, C.B.R.M., Bruxelles, 1962.

[3] I. BARSOTTI, Metodi analitici per varietà abeliane in caratteristica positiva, Ann. Scuola Norm. Sup. Pisa, 18 (1964), 1-25 ; 19 (1965), 277-330 et 481-512 ; 20 (1966), 101-137 et 331-365.

[4] N. BOURBAKI, Eléments de mathématique : algèbre commutative, chap. I et II, Hermann, Paris, 1961.

[5] N. BOURBAKI, Eléments de mathématique : algèbre commutative, chap. III et IV, Hermann, Paris, 1961.

[6] P. CARTIER, Groupes formels associés aux anneaux de Witt généralisés, C.R. Acad. Sci. Paris, 265 (1967), 50-52.

[7] P. CARTIER, Modules associés à un groupe formel commutatif. Courbes typiques, C.R. Acad. Sci. Paris, 265 (1967), 129-132.

[8] P. CARTIER, Relèvement des groupes formels commutatifs, Sém. Bourbaki, 1968/69, exposé 359, Lecture Notes in Mathematics, n° 179, Springer, Berlin, 1971.

[9] L. COX, Formal A-modules, Bull. Amer. Math. Soc., 79 (1973), 690-694.

[10] L. COX, Formal A-modules over p-adic integer rings, Compositio Mathematica, 29 (1974), 287-308.

[11] J.-M. DECAUWERT, Classification des A-modules formels, C.R. Acad. Sci. Paris, 282 (1976), 1413-1416.

[12] J.-M. DECAUWERT, Modules formels, thèse de 3e cycle (1976), Université scientifique et médicale de Grenoble.

[13] M. DEMAZURE, A. GROTHENDIECK, Schémas en groupes I, Séminaire du Bois-Marie 1962/64 (SGA 3), Lecture Notes in Mathematics, n° 151 Springer, Berlin 1970.

[14] M. DEMAZURE, P. GABRIEL, Groupes algébriques I, Masson, Paris, 1970.

[15] M. DEMAZURE, Lectures on p-Divisible Groups, Lecture Notes in Mathematics, n° 302, Springer, Berlin, 1972.

[16] J. DIEUDONNÉ, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, I, Comm. Math. Helv., 28 (1954), 87-118 ; II, Amer. J. Math., 77 (1955), 218-244 ; III, Math. Z., 63 (1955), 53-75 ; IV, Amer. J. Math., 77 (1955), 429-452 ; V, Bull. Soc. Math. France, 84 (1956), 207-239 ; VI, Amer. J. Math., 79 (1957), 331-388 ; VII, Math. Ann., 134 (1957), 114-133.

[17] J. DIEUDONNÉ, Witt groups and hyperexponential groups, Mathematika, 2, (1955), 21-31.

[18] J. DIEUDONNÉ, Introduction to the Theory of Formal Groups, Dekker, New-York, 1973.

[19] J.-M. FONTAINE, Points d'ordre fini d'un groupe formel sur une extension non ramifiée de $\mathbb{Z}_p$, Journées arithmétiques de Grenoble 1973, Bull. Soc. Math. France, Mémoire 37 (1974), 75-79.

[20] J.-M. FONTAINE, Sur la construction du module de Dieudonné d'un groupe formel, C.R. Acad. Sci. Paris, 280 (1975), 1273-1276.

[21] J.-M. FONTAINE, Groupes p-divisibles sur les vecteurs de Witt, C.R. Acad. Sci. Paris, 280 (1975), 1353-1356.

[22] J.-M. FONTAINE, Groupes finis commutatifs sur les vecteurs de Witt, C. R. Acad. Sci. Paris, 280 (1975), 1423-1425.

[23] J.-M. FONTAINE, Groupes commutatifs finis et plats sur un anneau de valuation discrète, en préparation.

[24] J.-M. FONTAINE, Module de Dieudonné et module de Tate des groupes p-divisibles, en préparation.

[25] A. FRÖHLICH, Formal Groups, Lecture Notes in Mathematics, n° 74, Springer, Berlin, 1968.

[26] P. GABRIEL, Des catégories abéliennes, Bull. Soc. Math. France, 90 (1962), 323-348.

[27] P. GABRIEL, Sur les catégories localement nœthériennes et leurs applications aux algèbres étudiées par Dieudonné, Séminaire J.-P. Serre, 1960.

[28] A. GROTHENDIECK, J. DIEUDONNÉ, Eléments de géométrie algébrique, tome I, Springer, Berlin, 1971.

[29] A. GROTHENDIECK, Groupes de Barsotti-Tate et cristaux, Actes du Congrès Intern. des Math. 1970, tome I, 431-436, Gauthiers-Villars, Paris 1971.

[30] A. GROTHENDIECK, Groupes de Barsotti-Tate et cristaux de Dieudonné, Université de Montréal, Montréal, 1974.

[31] M. HAZEWINKEL, Constructing Formal Groups I : over $\mathbb{Z}_{(p)}$-algebras, Netherlands School of Economics, Econometric Institute, Report 7119, 1971.

[32] T. HONDA, On the theory of commutative formal groups, Journ. Math. Soc. Japan, 22 (1970), 213-246.

[33] H. KRAFT, Kommutative algebraische p-gruppen, Sonderforschungsbereich 40, Theoretische Mathematik, Universität Bonn, Bonn, 1975.

[34] S. LANG, Algebraic Number Theory, Addison-Wesley, Reading, 1970.

[35] M. LAZARD, Bemerkungen zur Theorie der bewerteten Körper und Ringe, Math. Nach., 12 (1954), 67-73.

[36] M. LAZARD, Commutative Formal Groups, Lecture Notes in Mathematics, n° 443, Springer, Berlin 1975.

[37] Y. MANIN, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys, 18 (1963), 1-83.

[38] B. MAZUR, W. MESSING, Universal Extensions and One Dimensional Crystalline Cohomology, Lecture Notes in Mathematics, n° 370, Springer, Berlin, 1974.

[39] W. MESSING, The Crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes, Lecture Notes in Mathematics, n° 264, Springer, Berlin, 1972.

[40] B. MITCHELL, Theory of Categories, Academic Press, New-York, 1965.

[41] T. ODA, The first de Rham cohomology group and Dieudonné modules, Ann. Ecole Norm. Sup., 2 (1959), 63-125.

[42] J.-P. SERRE, Sur les groupes de Galois attachés aux groupes p-divisibles, Proceedings of a Conference on Local Fields, Nuffic Summer School at Driebergen, 118-131, Springer, Berlin, 1967.

[43] J.-P. SERRE, Corps locaux, 2e éd., Hermann, Paris, 1968.

[44] J. TATE, p-Divisible Groups, Proceedings of a Conference on Local Fields, Nuffic Summer School at Driebergen, 158-183, Springer, Berlin, 1967.

SUMMARY

Let k be a perfect field of characteristic $p \neq 0$, let $A = W(k)$ the ring of Witt vectors with coefficients in k and let $D_k = A[\underline{F},\underline{V}]$ the Dieudonné-ring, i.e. the (non-commutative, if $k \neq \mathbb{F}_p$) ring generated by A and two elements $\underline{F}$ and $\underline{V}$ subject to the relations

$$\begin{cases} \underline{F}\,\underline{V} = \underline{V}\,\underline{F} = p\ , \\ \underline{F}\,a = \sigma(a)\,\underline{F}\ ,\ a\underline{V} = \underline{V}\sigma(a)\ ,\ \text{for any}\ \ a \in A \end{cases}$$

(where σ is the absolute Frobenius on A).

It is well-known that commutative finite group-schemes, of rank a power of p, can be classified by their Dieudonné-modules, which are left D_k-modules, of finite length as A-modules.

By using Witt covectors, we give a new description of the Dieudonné-module $\underline{M}(G)$ of such a group G : we construct a commutative formal group-scheme $\widehat{CW}_k$ over k, whose endomorphisms ring contains D_k, and then $\underline{M}(G)$ is defined as $\mathrm{Hom}(G,\widehat{CW}_k)$. This construction avoid the decomposition of the group into an unipotent group and a multiplicative type one. We give also a description of G, as a group-functor, in terms of $\underline{M}(G)$: if $M = \underline{M}(G)$, for any finite, commutative and associative k-algebra R, the group $G(R)$ can be identified, canonically and functorially in R and G, to $\mathrm{Hom}_{D_k}(M,\widehat{CW}_k(R))$.

Since Grothendieck and Messing, one knows that it is possible to associate to any p-divisible group H over A a couple (L,M), where M is the Dieudonné-module of the special fiber of H and L a suitable sub-A-module of M, and that the correspondence $H \mapsto (L,M)$ classifies p-divisible groups over A. A new construction of the functor $H \mapsto (L,M)$ is given (actually, not exactly the same (L,M) as in Grothendieck or Messing). We give also a description of a quasi-inverse functor, as well as a description of the Tate-module of H in terms of the couple (L,M).

Suitable generalisations of those results to p-divisible groups and commutative smooth formal group-schemes over the integers of a local field of characteristic 0 and residue field k are given.

We explain also how our constructions are related to the work of Cartier on commutative formal group-laws over k and of Honda on commutative formal group-laws over k and $W(k)$.

CONTENTS :