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>

$$a_s \in \begin{cases} K/A & \underline{\text{si}} \quad s < p , \\ K/p^{-n}A & \underline{\text{si}} \quad p^n \leq s < p^{n+1} \quad \underline{(\text{pour}} \quad n \geq 1) , \end{cases}$$

<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.- <u>Classification des</u> p-<u>groupes formels</u>.

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, $\underline{G}(M)(R) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R))$ 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 $\widehat{CW}^c_k(R)$ qui est tué par p^m, pour m suffisamment grand, et de $\widehat{CW}^{et}_k(R)$ qui est discret. Comme M est $A[\underline{F}]$-profini, on en déduit que le groupe $\mathrm{Hom}^{\mathrm{cont}}_A(M, \widehat{CW}_k(R))$ des applications A-linéaires continues de M dans $\widehat{CW}_k(R)$ est de p-torsion. Il en est a fortiori de même de $\underline{G}(M)(R) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R))$. 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 :

$$\begin{cases} \text{pour tout k-anneau fini } R,\ \underline{G}(\varphi)_R : \underline{G}(N)(R) \to \underline{G}(M)(R) \text{ est l'application} \\ \text{qui, à } \psi : N \to \widehat{CW}_k(R),\ \text{associe } \psi \circ \varphi : M \to \widehat{CW}_k(R). \end{cases}$$

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, $G(R) = \mathrm{Hom}^{cont}_{D_k}(M, \widehat{CW}_k(R)) = \mathrm{Hom}_{D_k}(M, \widehat{CW}_k(R))$ (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 $\underline{a}_1, \underline{a}_2, \dots, \underline{a}_r$ qui engendrent M en tant que A-module et posons $u(\underline{a}_i) = (\dots, a_{-n,i}, \dots, a_{0,i})$. 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 $i = 1,2,\dots,r$, 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 $i = 1,2,\dots,r$, $\underline{F}\,\underline{a}_i = \sum \lambda_{i,j}\underline{a}_j$, avec les $\lambda_{i,j} \in A$, on doit avoir

$$(\dots, a^p_{-n,i}, \dots, a^p_{0,i}) = \sum_{j=1}^{r} \lambda_{i,j}(\dots, a_{-n,j}, \dots, a_{0,j}) .$$

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 $i = 1,2,\dots,r$, $\underline{V}\,\underline{a}_i = \sum \mu_{i,j}\underline{a}_j$, on doit avoir

$$(\dots, a_{-n-1,i}, \dots, a_{-1,i}) = \sum_{j=1}^{r} \mu_{i,j}(\dots, a_{-n,j}, \dots, a_{0,j}) .$$

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

$$\underline{G}(M)(B_G) = \varinjlim \underline{G}(M)(R_i) = \varinjlim \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R_i)) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(B_G))$$

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.- <u>Soit</u> M <u>un</u> $A[\underline{F}]$-<u>module à gauche, qui est artinien en tant que A-module. Posons</u> $M^{et} = \bigcap_{n=0}^{\infty} \underline{F}^n M$ <u>et soit</u> M^c <u>l'ensemble des</u> $\underline{a} \in M$ <u>tels que</u> $\underline{F}^n \underline{a} = 0$, <u>pour</u> n <u>suffisamment grand</u>. <u>Alors</u> $M = M^{et} \oplus M^c$ <u>et</u> $\underline{F}M^{et} = M^{et}$.

<u>Démonstration</u> : 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 <u>composante étale</u> de M et M^c la <u>composante connexe</u> 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 :

<u>1ère étape</u> : 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> $\mathcal{G} = \mathrm{Gal}(k'/k)$ <u>opère continûment et semi-linéairement</u> (i.e. M <u>est un</u> $W(k)[\mathcal{G}]$-<u>module et si</u> $g \in \mathcal{G}$, $a \in W(k')$, $x \in M$, <u>on a</u> $g(ax) = g(a)\,g(x)$) . <u>Alors</u>

i) <u>l'application de</u> $W(k') \otimes_{W(k)} M^{\mathcal{G}}$ <u>dans</u> M <u>qui à</u> $a \otimes x$ <u>associe</u> ax <u>est un isomorphisme</u> ;

ii) <u>le</u> $\mathcal{G}$-<u>module</u> M <u>est cohomologiquement trivial</u>.

<u>Démonstration</u> : posons $A = W(k)$ et $A' = W(k')$.

Comme A' est un $A[\mathcal{G}]$-module libre de rang 1 , le $\mathcal{G}$-module $A' \otimes_A M^{\mathcal{G}}$ 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 $\mathcal{G}$ 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 $A' \otimes_A M^{\mathcal{G}}$ s'écrit, de manière unique, sous la forme $\sum_{j=1}^{n} e_j \otimes a_j$, avec les $a_j \in M^{\mathcal{G}}$. 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

$$0 \longrightarrow k' \longrightarrow M \longrightarrow M' \longrightarrow 0$$

à laquelle correspond une suite exacte de A-modules

$$0 \longrightarrow k \longrightarrow M^{\mathcal{G}} \longrightarrow M'^{\mathcal{G}} \longrightarrow 0$$

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

$$\begin{cases} \underline{F}(a \otimes x) = \sigma(a) \otimes \underline{F}x \\ \underline{V}(a \otimes x) = \sigma^{-1}(a) \otimes \underline{V}x \end{cases} \quad \text{si } a \in A' , \ x \in M ,$$

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.- Soit k' une extension finie de k et soit G un p-groupe formel sur k . Posons $M = \underline{M}(G)$ et $M' = \underline{M}'(G_{k'}) = \mathrm{Hom}(G_{k'}, \widehat{CW}_{k'})$.

i) L'application naturelle de $W(k') \otimes_{W(k)} M$ dans M' est un isomorphisme.

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

$$0 \to \mathrm{Hom}_{\mathbb{Z}[\mathfrak{G}]}(\Gamma'',K'/A') \to \mathrm{Hom}_{\mathbb{Z}[\mathfrak{G}]}(\Gamma,K'/A') \to \mathrm{Hom}_{\mathbb{Z}[\mathfrak{G}]}(\Gamma',K'/A') \to 0$$

est encore exacte. Et K'/A' est bien un $\mathfrak{G}$-module injectif.

Pour achever la démonstration de la proposition, il suffit alors d'établir l'assertion suivante :

PROPOSITION 2.4.- *Soit Δ un $\mathfrak{G}_k$-module discret. Pour que Δ soit injectif (dans la catégorie des $\mathfrak{G}_k$-modules discrets) il faut et il suffit que, pour tout sous-groupe ouvert invariant $\mathfrak{U}$ de $\mathfrak{G}_k$, $\Delta^{\mathfrak{U}}$ soit un $(\mathfrak{G}_k/\mathfrak{U})$-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 $\bar{M} = M/N$. Le sous-module Δ s'envoie injectivement sur son image $\bar{\Delta}$ dans $\bar{M}$. Comme Δ, donc $\bar{\Delta}$, est injectif, il existe un sous-module $\bar{N}'$ de $\bar{M}$ tel que $\bar{M} = \bar{\Delta} \oplus \bar{N}'$. On voit que l'image réciproque N' de $\bar{N}'$ dans M répond à la question.

Démonstration de la prop. 2.4 : si $\mathfrak{U}$ est un sous-groupe ouvert invariant de $\mathfrak{G}_k$, et si on pose $\mathfrak{G} = \mathfrak{G}_k/\mathfrak{U}$, tout $\mathfrak{G}$-module peut être considéré comme un $\mathfrak{G}_k$-module discret sur lequel $\mathfrak{U}$ opère trivialement. Pour un tel module M, on voit que $\mathrm{Hom}_{\mathbb{Z}[\mathfrak{G}]}(M,\Delta^{\mathfrak{U}}) = \mathrm{Hom}_{\mathbb{Z}[\mathfrak{G}_k]}(M,\Delta)$ et on en déduit que $\Delta^{\mathfrak{U}}$ est injectif si Δ l'est.

Réciproquement, soit M un $\mathfrak{G}_k$-module discret contenant Δ et soit N un sous-$\mathfrak{G}_k$-module de M tel que $N \cap \Delta = 0$ et qui est maximal pour cette propriété. Pour tout sous-groupe ouvert invariant $\mathfrak{U}$ de $\mathfrak{G}_k$, on voit que $N^{\mathfrak{U}}$ est un sous-$(\mathfrak{G}_k/\mathfrak{U})$-module de $M^{\mathfrak{U}}$ vérifiant $N^{\mathfrak{U}} \cap \Delta^{\mathfrak{U}} = 0$. Supposons $\Delta^{\mathfrak{U}}$ injectif. D'après le lemme précédent, il existe un sous-$(\mathfrak{G}_k/\mathfrak{U})$-module N' de

$M^{\mathfrak{U}}$ contenant $N^{\mathfrak{U}}$ tel que $M^{\mathfrak{U}} = \Delta^{\mathfrak{U}} \oplus N'$. Si, avec des notations évidentes, $n+n' = \delta \in (N+N') \cap \Delta$, on a, pour tout $g \in \mathfrak{U}$, $(g-1)n = (g-1)\delta = 0$, puisque $N \cap \Delta = 0$; par conséquent $\delta \in \Delta^{\mathfrak{U}}$ et $n \in N'$. On a donc $(N+N') \cap \Delta = 0$, d'où $N+N' = N$, ce qui implique $N' = N$. Si les $\Delta^{\mathfrak{U}}$ sont tous injectifs, on a donc $M^{\mathfrak{U}} = \Delta^{\mathfrak{U}} \oplus N^{\mathfrak{U}}$, pour tout $\mathfrak{U}$, d'où $M = \Delta \oplus N$, car $M = \varinjlim M^{\mathfrak{U}}$.

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) *Tout p-groupe étale G est réunion de ses sous-groupes finis et le D_k-module topologique $\underline{M}(G)$ s'identifie à $\varprojlim \underline{M}(G_f)$, pour G_f parcourant les sous-groupes finis de G.*

ii) *Tout D_k-module $A[\underline{F}]$-profini étale est D_k-profini* (i.e. *admet un système fondamental de voisinages ouverts de 0 formé de sous-D_k-modules*). *Si M est un tel module, le p-groupe formel étale $\underline{G}(M)$ s'identifie à $\varinjlim \underline{G}(M/N)$, pour N parcourant les sous-D_k-modules ouverts de M.*

Démonstration :

i) Soit Γ un $\mathfrak{G}_k$-module discret de p-torsion, soit $\mathfrak{U}$ un sous-groupe invariant ouvert de $\mathfrak{G}_k$ et soit $\mathfrak{G} = \mathfrak{G}_k/\mathfrak{U}$. Comme $\mathfrak{G}$ est un groupe fini, le $\mathfrak{G}$-module $\Gamma^{\mathfrak{U}}$ est réunion de ses sous-$\mathfrak{G}$-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 $\Gamma^{\mathfrak{U}}$, pour $\mathfrak{U}$ parcourant les sous-groupes invariants ouverts de $\mathfrak{G}_k$, on voit que Γ est la réunion de ses sous-$\mathfrak{G}$-modules qui sont des groupes finis. L'équivalence de catégorie entre p-groupes formels étales et $\mathfrak{G}_k$-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

$$a^w = (\dots, a_{-n}, \dots, a_{-1}, a_o) \text{ , avec } a_{-n} = V_B^n(a) \text{ pour } n \in \mathbb{N} ,$$

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

$$\underline{Va} = (\dots, a_{-n-1}, \dots, a_{-2}, a_{-1}) = (\dots, V_B(a_{-n}), \dots, V_B(a_{-1}), V_B(a_o)) .$$

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 $k[x_1,x_2,\ldots,x_r]/(x_1^p,x_2^p,\ldots,x_r^p)$. 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 $(\ldots,0,\ldots,0,a_o)$, 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 $k[x_1,x_2,\ldots,x_r]$ par l'idéal engendré par les $x_j^p - \sum_i a_{i,j}x_i$. Les images des $x_1^{i_1}x_2^{i_2}\ldots x_r^{i_r}$, 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 , $\underline{M}(G)$ *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

$$\begin{tikzcd}
0 \arrow[r] & G' \arrow[r] \arrow[d, "u_{G'}"] & G \arrow[r] \arrow[d, "u_G"] & G'' \arrow[r] \arrow[d, "u_{G''}"] & 0 \\
0 \arrow[r] & \underline{G}\underline{M}(G') \arrow[r] & \underline{G}\underline{M}(G) \arrow[r] & \underline{G}\underline{M}(G'') &
\end{tikzcd}$$

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

$$0 \to M' \to M \to M'' \to 0$$

de D_k-modules finis étales, correspond une suite exacte

$$0 \to \underline{G}(M'') \to \underline{G}(M) \to \underline{G}(M') .$$

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

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "v_{M'}"] & M \arrow[r] \arrow[d, "v_M"] & M'' \arrow[r] \arrow[d, "v_{M''}"] & 0 \\
 & \underline{M}\underline{G}(M') \arrow[r] & \underline{M}\underline{G}(M) \arrow[r] & \underline{M}\underline{G}(M'') \arrow[r] & 0
\end{tikzcd}$$

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) $$\partial_w(b-c) \equiv \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}}$$

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) $$\Lambda(X_1,X_2) + T_m(X_1+X_2,X_3,\dots,X_{m+1}) = T_{m+1}(X_1,X_2,\dots,X_{m+1}) .$$

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) 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') $$\partial_w(a) \equiv \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}} .$$

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) $$\Delta a \equiv ((a \hat{\otimes} 1) \oplus (1 \hat{\otimes} a)) - \sum \lambda_j \Lambda(x_j^{p^{s-1}} \hat{\otimes} 1 , 1 \hat{\otimes} x_j^{p^{s-1}}) \pmod{I_{2,r+1}} .$$

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) $$\Delta_m a \equiv \alpha_m - \beta_m \pmod{I_{m,r+1}} :$$

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 $b = (\dots, b_{-n}, \dots, b_{-1}, b_o) \in \underline{M}(G)$ 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.- *Si G est un p-groupe formel sur k tel que $F_G = 0$, on a $\underline{F}\,\underline{M}(G) = 0$ et $\underline{M}(G)$ s'identifie canoniquement à $t_G^*(k)$. En particulier, si G est un p-groupe fini d'ordre p^r tel que $F_G = 0$, $\underline{M}(G)$ est un espace vectoriel sur k de dimension r.*

C'est clair !

COROLLAIRE 2.- *Le foncteur $\underline{M}$, restreint à la catégorie des k-groupes formels connexes, est exact.*

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

$$\begin{tikzcd} \underline{M}(G) \arrow[r] \arrow[d, "\eta_G"] & \underline{M}(G') \arrow[d, "\eta_{G'}"] \\ t^*_G(k) \arrow[r] & t^*_{G'}(k) \end{tikzcd}$$

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.- Soit M un D_k-module $A[\underline{F}]$-profini et soit $G = \underline{G}(M)$.

i) Pour tout $u \in t_G(k)$, l'application $\xi_M(u) : M/\underline{F}M \to k$ définie ci-dessus est k-linéaire continue.

ii) L'application $\xi_M : t_G(k) \to \mathfrak{L}^{\mathrm{cont}}_k(M/\underline{F}M, k)$, espace des applications k-linéaires continues de $M/\underline{F}M$ dans k, ainsi définie, est un isomorphisme de k-espaces vectoriels.

Démonstration : 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 $\widehat{CW}{}^c_k(k[t]/t^2)$ 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 $\theta : M/\underline{F}M \to \widehat{CW}{}^c_k(k[t]/t^2)$ 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^n_G. 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 $M_n = M/\underline{F}^nM$. 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 $\underline{F}^r\widehat{CW}{}^c_k(R) = 0$. On a donc $\underline{G}(M)(R) =$ $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M,\widehat{CW}_k(R)) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M,\widehat{CW}{}^c_k(R))$ (car M est connexe) $=$ $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M/\underline{F}^rM,\widehat{CW}{}^c_k(R)) = \varinjlim \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M_n,\widehat{CW}{}^c_k(R))$, 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 $F^n_G = 0$ (resp. $\underline{F}^nM = 0$).

L'assertion (ii) se démontre alors par récurrence sur l'entier n tel que $F^n_G = 0$:

- 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

$$0 \longrightarrow \mathrm{Ker}\, F_G \longrightarrow G \longrightarrow \mathrm{Im}\, F_G \longrightarrow 0 .$$

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 $\mathrm{Ker}\, F_G$ et $\mathrm{Im}\, F_G$ (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 $\underline{F}^nM = 0$ 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 $\mathcal{C}_k = C\Lambda(k)$ 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) pour tout $r > 0$, il existe $\varepsilon > 0$ tel que $a_s = 0$ si $r-\varepsilon \leq s < r$.

Soit $\bar{k}$ une clôture algébrique de k. Pour tout $x \in \bar{k}$, notons ν_x l'application de C_k dans $C_{k(x)} = C\Lambda(k(x))$ 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 $G(C_k)$ sont les k-homomorphismes de l'algèbre affine B_G de G dans le k-anneau 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 $\varphi \in G(C_k)$, nous posons $u_\ell(\varphi) = \sum_{\varepsilon \in \mu_\ell} \nu_\varepsilon \circ \varphi$; on voit que, si $\varepsilon \in \mu_\ell$, $\nu_\varepsilon \circ \varphi : B_G \to C_{k_\ell}$ est un élément de $G(C_{k_\ell})$; 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 C_k, on peut considérer $u_\ell(\varphi)$ comme un élément de $G(C_k)$. Il est clair que u_ℓ est un endomorphisme du groupe $G(C_k)$.

Pour tout automorphisme τ de k notons $\langle\tau\rangle$ l'application de 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) 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 $\varphi \in G(C_k)$, 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 $G(C_k)$ et que F_p et V_p sont des endomorphismes de $G(C_k)$.

PROPOSITION 5.1.- Pour tout p-groupe fini G sur k soit $\underline{M}'(G)$ le sous-groupe de $G(C_k)$ formé des éléments φ vérifiant $u_\ell(\varphi) = 0$, pour tout nombre premier $\ell \neq p$.

i) Il existe une structure de D_k-module à gauche et une seule sur $\underline{M}'(G)$ vérifiant, pour tout $\varphi \in \underline{M}'(G)$,

$[\varepsilon]\varphi = \nu_\varepsilon \circ \varphi$, si $[\varepsilon]$ désigne le représentant multiplicatif dans $A = W(k)$ d'un élément quelconque ε de k,

$F\varphi = F_p \cdot \varphi$ et $V\varphi = V_p \cdot \varphi$.

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 $\varepsilon\alpha = 1$.

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 $R \otimes_k C\Lambda(k) = R \otimes_k C_k$; on peut donc identifier le groupe $G(C_k)$ au groupe multiplicatif $C(G)$ formé des éléments α de $C\Lambda(R)$ vérifiant $\Delta\alpha = \alpha \otimes \alpha$ et $\varepsilon\alpha = 1$.

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

$$CT(G) = \{\alpha \in C\Lambda(R) \mid \Delta\alpha = \alpha \otimes \alpha \ , \ \varepsilon\alpha = 1 \ , \ U_\ell \alpha = 1 \ , \text{ pour tout } \ell \neq p\} .$$

Comme $\varepsilon\alpha = 1$ 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

$$CT(G) = \{\alpha \in CCT(R) \mid \Delta\alpha = \alpha \otimes \alpha \ , \ \varepsilon\alpha = 1\} .$$

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 $G(\mathcal{C}_k)$ est d'ordre une puissance de p ; comme $CT(G)$ est isomorphe à un sous-groupe de $G(\mathcal{C}_k)$, 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 $\varepsilon_{\mathbb{D}(G)}(a_{-n}) = 0$ pour tout n ; comme $\alpha = \prod F(a_{-n}T_{-n})$, on en déduit que $\varepsilon(\alpha) = 1$ 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 $\varepsilon \in k$; on a $[\varepsilon]\underline{a} = (\dots, \varepsilon^{p^{-n}}a_{-n}, \dots, \varepsilon a_0)$ et $[\varepsilon]\alpha = \prod F(\varepsilon^{p^{-n}}a_{-n}T_{-n}) = \sum \varepsilon^s b_s \bar{\theta}_s$; donc, si $x \in B_G$, $([\varepsilon]\varphi)(x) = \sum x(\varepsilon^s b_s \bar{\theta}_s) = \sum \varepsilon^s x(b_s)\bar{\theta}_s$ et $[\varepsilon]\varphi = \nu_\varepsilon \circ \varphi$;
- 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 $F^m_G = 0$, 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 $x \in M$,

$$\begin{cases} ax = xa \ , \text{ pour tout } a \in A \ , \\ \underline{F}x = x\underline{V} \quad \text{et} \quad \underline{V}x = x\underline{F} \ . \end{cases}$$

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 $\sum_{n \in \mathbb{Z}} a_n T_n$, 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.- <u>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</u>.

<u>Démonstration</u> : pour tout $\varphi \in M^*$ et tout $x \in M$, posons

$$\varphi(x) = \sum_{m\in\mathbb{Z}} (x,\varphi)_m T_m\,.$$

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 $\varphi(\underline{V}^n x) = \sum_m (\underline{V}^n x,\varphi)_m T_m = \underline{V}^n \varphi(x) = \sum_m p^n \sigma^{-n}((x,\varphi)_m) T_{m-n}$; 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 $\varphi : B_G \to C_k$ associe la restriction de $CW_k(\varphi) : CW_k(B_G) \to CW_k(C_k)$ à $\underline{M}(G)$ est un isomorphisme du groupe $G(C_k)$ sur $\mathrm{Hom}_{D_k}(\underline{M}(G), CW_k(C_k))$. En composant avec l'isomorphisme $\bar{\varpi}_k : CW_k(C) \to \Theta_k$,on obtient un isomorphisme

$$\lambda_G : G(C_k) \longrightarrow \mathrm{Hom}_{D_k}(\underline{M}(G),\Theta_k)$$

qui est visiblement fonctoriel en G .

PROPOSITION 5.3.- <u>Soit</u> G <u>un p-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> $\varphi \in G(C_k)$, $\lambda_G(\varphi) \in \underline{M}(G)^*$ <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 $\nu_\varepsilon : C_k \to C_{k(\varepsilon)}$, définie au n°5.1, induit une application $CW_k(\nu_\varepsilon) : CW_k(C_k) \to CW_k(C_{k(\varepsilon)})$. 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

$$\begin{tikzcd} CW_k(C_k) \arrow[r, "CW_k(\nu_\varepsilon)"] \arrow[d, "\bar{\varpi}_k"'] & CW_k(C_{k(\varepsilon)}) \arrow[d, "\bar{\varpi}_{k(\varepsilon)}"] \\ \Theta_k \arrow[r, "\hat{\nu}_\varepsilon"] & \Theta_{k(\varepsilon)} \end{tikzcd}$$

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 $G(C_{k(\varepsilon)})$ dans $\mathrm{Hom}_{D_k}(\underline{M}(G),\Theta_{k(\varepsilon)})$ qui à $\psi : B_G \to C_{k(\varepsilon)}$ associe $\bar{\varpi}_{k(\varepsilon)} \circ CW_k(\psi)|_{\underline{M}(G)}$. Il est clair que, si $\varphi \in G(C_k)$, $\lambda_G(\nu_\varepsilon \circ \varphi) = \hat{\nu}_\varepsilon \circ \lambda_G(\varphi)$.

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 $\varphi \in \underline{M}'(G)$,

$$\lambda_G(\varphi[\varepsilon]) = \lambda_G(\varphi)[\varepsilon] \quad , \text{ pour tout } \varepsilon \in k ,$$

$$\lambda_G(\varphi\underline{F}) = \lambda_G(\varphi)\underline{F}$$

$$\lambda_G(\varphi\underline{V}) = \lambda_G(\varphi)\underline{V} .$$

- 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 $\lambda_G(\varphi)(\underline{a}) = \sum b_n T_n = \sum b_n \theta_{p^n}$, $\lambda_G(\varphi[\varepsilon])(\underline{a}) = \sum b_n [\varepsilon]^{p^n} \theta_{p^n} = \sum b_n \sigma^n([\varepsilon])T_n = (\sum b_n T_n)[\varepsilon]$, 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 $\lambda_G(\varphi)(\underline{a}) = \sum b_n T_n = \sum b_n \theta_{p^n}$, on a donc $\lambda_G(\varphi\underline{F})(\underline{a}) = \hat{v}(\sum b_n T_n) = \sum b_n T_{n+1} = (\sum b_n T_n)\underline{F}$, d'où $\lambda_G(\varphi\underline{F}) = \lambda_G(\varphi)\underline{F}$.

■ Par définition, on a $\varphi\underline{V} = \underline{F}\varphi = \langle\hat{\sigma}\rangle\circ\varphi\circ V_{B_G}$.

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 $\underline{a} = (\dots,a_{-n},\dots,a_0) \in \underline{M}(G)$, 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 $\lambda_G(\varphi)(\underline{a}) = \sum b_nT_n$, on voit que

$$\langle\hat{\sigma}\rangle(\underline{V}(\lambda_G(\varphi)(\underline{a}))) = \langle\hat{\sigma}\rangle(\sum p\sigma^{-1}(b_n)T_{n-1}) = \sum pb_nT_{n-1} = (\sum b_nT_n)\underline{V} ,$$

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> $\underline{M}_D(G)$ <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> $\underline{M}$ <u>et</u> $\underline{M}_D$ <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 $\mathrm{Hom}(G,CW_k^u) \subset \underline{M}(G) = \mathrm{Hom}(G,CW_k)$: mais, pour n assez grand, on a $V_G^n = 0$, 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.- <u>Groupes formels lisses</u>.

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_n^F le sous-groupe de G noyau de F_G^n . Il est clair que $\underline{M}(G_n^F)$ s'identifie à $\underline{M}(G)/\underline{F}^n\underline{M}(G)$. Le groupe G est connexe si et seulement si $G = \varinjlim G_n^F$, 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 $\mathrm{Hom}_{D_k}(M_i, CW_k(S)) = \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M_i, CW_k(S))$. Comme $M = \varprojlim M_i$, on a $G(S) = \varinjlim \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M_i, CW_k(S))$ et tout revient à montrer que si $u \in \mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, CW_k(S))$, 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

$$\begin{cases} \underline{V}\underline{\tilde{a}} = (\tilde{a}_{-n+1})_{n \in \mathbb{N}} \\ x\underline{\tilde{a}} = (\sigma^{-n}(x)\tilde{a}_{-n})_{n \in \mathbb{N}} \end{cases}, \text{ pour tout } x \in k .$$

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 fi-

nie 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).

Remarque : 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.- Les foncteurs $G \mapsto (\underline{M}(G))^d$ et $G \mapsto \underline{M}(\mathbb{D}_p(G))$ de la catégorie des groupes p-divisibles sur k dans celle des D_k-modules sont naturellement équivalents.

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 $\mathfrak{R}$ (au sens du n° II.5.4) et d'un isomorphisme de $\mathfrak{R}/p\mathfrak{R} \simeq \mathfrak{R}\otimes_A k$ 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 $\mathfrak{R} = \prod \mathfrak{R}_i$, avec $\mathfrak{R}_i = W(k_i)[[X_1, \dots, X_d]]$ et l'isomorphisme évident de $\mathfrak{R}/p\mathfrak{R}$ sur R) ; il est unique à isomorphisme non unique près.

Soit $\Delta : R \to R\hat{\otimes}_k R$ le coproduit et soit $\hat{\Delta} : \mathfrak{R} \to \mathfrak{R}\hat{\otimes}_A \mathfrak{R}$ un homomorphisme continu de A-anneaux qui relève Δ (un tel homomorphisme existe toujours -on ne demande pas qu'il munisse $\mathfrak{R}$ d'une structure de bigèbre formelle). Il est clair que $\hat{\Delta}$ se prolonge, de manière unique, en un homomorphisme continu de $\hat{\mathfrak{R}}_K^{an}$ dans $(\widehat{\mathfrak{R}\hat{\otimes}_A \mathfrak{R}})_K^{an}$ que nous notons encore $\hat{\Delta}$.

Pour tout $\alpha \in \hat{\mathfrak{R}}_K^{an}$, posons $\hat{\partial}\alpha = \alpha\hat{\otimes}1 - \hat{\Delta}\alpha + 1\hat{\otimes}\alpha$ et

$$\mathcal{MH}_{\mathfrak{R}}(G) = \{\alpha \in P(\mathfrak{R}) \mid \hat{\partial}\alpha \in p\mathfrak{R}\hat{\otimes}_A \mathfrak{R}\} ;$$

c'est un sous-A-module de $P(\mathfrak{R})$ contenant $p\mathfrak{R}$; on voit que $\mathcal{MH}_{\mathfrak{R}}(G)$ ne dépend pas du choix du relèvement $\hat{\Delta}$ de Δ (si $\hat{\Delta}_1$ est un autre relèvement de Δ, on a $\hat{\Delta}_1\beta \equiv \hat{\Delta}\beta \pmod{p\mathfrak{R}}$, pour tout $\beta \in \mathfrak{R}$; tout élément de $P(\mathfrak{R})$ s'écrit comme une somme infinie d'éléments de la forme $p^{-n}\beta^{p^n}$, avec $\beta \in \mathfrak{R}$ et $n \in \mathbb{N}$, et l'on a $\hat{\Delta}_1\beta^{p^n} \equiv \hat{\Delta}\beta^{p^n} \pmod{p^{n+1}\mathfrak{R}}$ donc $\hat{\Delta}_1(p^{-n}\beta^{p^n}) \equiv \hat{\Delta}(p^{-n}\beta^{p^n})$ $\pmod{p\mathfrak{R}}$).

Posons $MH_{\mathfrak{R}}(G) = \mathcal{MH}_{\mathfrak{R}}(G)/p\mathfrak{R}$. On peut considérer $MH_{\mathfrak{R}}(G)$ comme un sous-A-module de $P(\mathfrak{R})/p\mathfrak{R}$. D'après la proposition 5.5 du chapitre II, l'application $w_{\mathfrak{R}}$ définit un isomorphisme de $CW_k(R)$ sur $P(\mathfrak{R})/p\mathfrak{R}$; en particulier, $P(\mathfrak{R})/p\mathfrak{R}$ 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 p-groupe formel lisse et de dimension finie sur</u> k <u>et soit</u> $\mathfrak{R}$ <u>un relèvement lisse de l'algèbre affine de</u> G. <u>Le module</u> $MH_{\mathfrak{R}}(G)$ <u>est un sous-</u>D_k<u>-module de</u> $P(\mathfrak{R})/p\mathfrak{R}$ <u>et l'application</u> $w_{\mathfrak{R}}$ <u>induit un isomorphisme de</u> $\underline{M}(G)$ <u>sur</u> $MH_{\mathfrak{R}}(G)$.

CHAPITRE IV

GROUPES FORMELS LISSES SUR UN ANNEAU DE VALUATION DISCRÈTE

§ 1.- <u>Le cas</u> $e = 1$.

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 $MH(G) = MH_{\mathfrak{R}}(G_k)$. 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 $p\underline{M}(G_k) \subset \underline{FM}(G_k)$; on en déduit, par passage aux quotients, une application k-linéaire $\tilde{\rho}(G)$ de $\mathcal{L}(G)/p\mathcal{L}(G)$ dans $\underline{M}(G_k)/\underline{FM}(G_k)$.

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>.