CHAPITRE I

THÉORIE ÉLÉMENTAIRE DES SCHÉMAS EN GROUPES AFFINES COMMUTATIFS

§ 1.- Schémas affines.

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

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

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

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

$$\begin{tikzcd} X(R) \arrow[r, "\varphi_R"] \arrow[d, "X(\xi)"'] & Y(R) \arrow[d, "Y(\xi)"] \\ X(S) \arrow[r, "\varphi_S"] & Y(S) \end{tikzcd}$$

est commutatif).

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

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

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

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

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

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

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

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

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

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

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

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

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

est commutatif.

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

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

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

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

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

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

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

§ 2.- <u>Groupes affines</u>.

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

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

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

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

soit commutatif.

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

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

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

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

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

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

(B_1) (<u>associativité</u>) le diagramme

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

est commutatif ;

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

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

est commutatif ;

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

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

est commutatif.

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

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

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

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

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

$$\begin{tikzcd} B \arrow[r, "\Delta_B"] \arrow[d, "\eta"'] & B \otimes_k B \arrow[d, "\eta \otimes \eta"] \\ C \arrow[r, "\Delta_C"] & C \otimes_k C \end{tikzcd}$$

est commutatif.

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

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

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

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

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

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

- la catégorie des k-foncteurs en groupes a un objet nul : le groupe e_k défini par $e_k(R) = \{1\}$, pour tout k-anneau R ; c'est un k-groupe affine dont l'algèbre affine s'identifie à k ;
- si G et G' sont deux k-foncteurs en groupes, le k-foncteur en groupes $G \times G'$ est défini par $(G \times G')(R) = G(R) \times G'(R)$, pour tout k-anneau R ; si G et G' sont affines d'algèbres affines B et B' , $G \times G'$ est affine, d'algèbre affine $B \otimes_k B'$; on voit que le coproduit $\Delta_{B \otimes B'} : B \otimes B' \to B \otimes B' \otimes B \otimes B'$ est le composé
$$B \otimes B' \xrightarrow{\Delta_B \otimes \Delta_{B'}} B \otimes B \otimes B' \otimes B' \xrightarrow{id_B \otimes t \otimes id_{B'}} B \otimes B' \otimes B \otimes B'$$
où $t : B \otimes B' \to B' \otimes B$ est définie par $t(f \otimes f') = f' \otimes f$;
- plus généralement, si G , G' et H sont trois k-foncteurs en groupes et si $\varphi : G \to H$ et $\psi : G' \to H$ sont des morphismes de k-foncteurs en groupes, le produit fibré $G \times_H G'$ est le k-foncteur en groupes défini par $(G \times_H G')(R) = G(R) \times_{H(R)} G'(R)$, pour tout k-anneau R ; si G , G' et H sont affines, il en est de même de $G \times_H G'$ et son algèbre affine s'identifie à $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G')$.

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

(B_4) (commutativité) le diagramme

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

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

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

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

§ 3.- Anneaux et modules profinis.

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

Dans ce paragraphe, tous les anneaux sont supposés commutatifs.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On a le résultat suivant :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 4.- Schémas formels.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

est commutatif.

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

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

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

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

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

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

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

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

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

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

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

et on vérifie facilement que f est un isomorphisme.

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

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

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

4.9. La catégorie des k-foncteurs formels a des limites inductives. Une limite inductive de k-schémas formels est encore un k-schéma formel et son

algèbre affine s'identifie à la limite projective des algèbres affines.

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

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

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

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

§5.- <u>Groupes formels et dualité de Cartier</u>.

5.1. Soit k un anneau commutatif pseudo-compact.

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

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

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

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

(B_1^f) le diagramme

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

est commutatif ;

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

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

est commutatif ;

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

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

est commutatif ;

(B_4^f) le diagramme

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

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

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

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

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

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

5.4. Soit maintenant k un anneau commutatif artinien.

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

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

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

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

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

5.5. Soit maintenant k un anneau commutatif nœthérien.

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

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

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

Soit G un k-groupe fini et plat et soit B son algèbre affine. Soit B' la bigèbre duale. Pour tout k-anneau R l'ensemble sous-jacent à $\mathbb{D}(G)(R)$ est formé des homomorphismes du k-anneau B' dans R et c'est un sous-ensemble du k-module des applications k-linéaires de B' dans R. Comme

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

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

§ 6.- <u>Noyaux et conoyaux</u>.

6.1. Soit k un anneau commutatif.

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

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

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

Dans toute la suite de ce paragraphe, *on suppose que* k *est un corps*.

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

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

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

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

une sous-k-bigèbre formelle de C. On voit donc que $\psi \circ \varphi = 0$ si et seulement si $\psi^*(C') \subset b_C(k \oplus \mathfrak{a})$. On en déduit que φ admet un conoyau J et que l'algèbre affine de J s'identifie à $b_C(k \oplus \mathfrak{a})$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Commençons par établir un lemme :

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

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

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

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

correspond un diagramme commutatif

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

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

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

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

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

<u>Remarques</u> :

1.- Comme on sait que la catégorie des k-groupes affines (resp. formels) admet des noyaux et conoyaux, il suffit, pour montrer que cette catégorie est

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

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

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

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

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

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

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

§ 7.- <u>Groupes étales et connexes</u>.

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

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

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

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

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

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

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

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

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

l'élément neutre").

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

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

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

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

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

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

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

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

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

On déduit immédiatement de l'exactitude la suite

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

celle de la suite

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

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

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

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

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

Plus généralement, pour tout entier $n \geq 0$, on voit que F_B^n peut être

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

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

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

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

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

Notons $TS^p B$ le sous-k-espace vectoriel fermé des tenseurs symétriques de $\hat{\otimes}^p B$. Soit s l'application k-linéaire continue de $\hat{\otimes}^p B$ dans $TS^p B$ qui, à $b_1 \hat{\otimes} b_2 \hat{\otimes} \dots \hat{\otimes} b_p$ associe $\sum_{g \in \mathfrak{S}_p} b_{g(1)} \hat{\otimes} b_{g(2)} \hat{\otimes} \dots \hat{\otimes} b_{g(p)}$ et soit $TS_{\mathfrak{S}}^p B$ l'image de s . On voit facilement que tout élément de $TS^p B$ s'écrit d'une manière et d'une seule sous la forme $w = (b(w))^{\hat{\otimes} p} + w_0$, avec $b(w) \in B$ et $w_0 \in TS_0^p B$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Montrons que, si

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

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

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

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

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

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

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

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

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

est exacte ;

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

§ 8.- Espaces tangent et cotangent.

Dans ce paragraphe, k est un anneau commutatif.

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

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

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

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

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

PROPOSITION 8.1.- <u>Le</u> k-<u>module</u> $\omega_{G/k}$ <u>est canoniquement isomorphe à</u> $t_G^*(k)$ <u>et l'homomorphisme canonique de</u> $B \otimes_k \omega_{G/k}$ <u>dans</u> $\Omega_k(B)$ <u>est un isomorphisme</u>.

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

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

On voit que le diagramme

$$\begin{tikzcd} G \arrow[r, "id"] \arrow[d, "\delta"'] & G \arrow[d, "\nu"] \\ G \times G \arrow[r, "\eta"] & G \times G \end{tikzcd}$$

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

$$\begin{tikzcd} B & B \arrow[l, "id"'] \\ B \otimes_k B \arrow[u, "prod."] & B \otimes_k B \arrow[l, "\eta^*"'] \arrow[u, "id_B \otimes \varepsilon_B"'] \end{tikzcd}$$

où les flèches horizontales sont des isomorphismes et les flèches verticales sont surjectives ; les noyaux de ces dernières, i.e. I et $B \otimes_k B^+$ (car B^+ est facteur direct de B en tant que k-module) s'identifient donc canoniquement. On en déduit que I/I^2 s'identifie à $B \otimes_k (B^+/B_2^+)$, donc à $B \otimes_k t_G^*(k)$.

Enfin, on vérifie facilement que, dans cette identification, $\omega_{G/k}$ s'identifie à $t_G^*(k)$.

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

Il résulte de la propriété universelle du module des différentielles que $\mathrm{Der}_k(B,R)$ s'identifie canoniquement au R-module des applications B-linéaires de $\Omega_k(B)$ dans R . Comme $\Omega_k(B)$ est canoniquement isomorphe à $B \otimes_k (B^+/B_2^+)$, $\mathrm{Der}_k(B,R)$ s'identifie au R-module des applications k-linéaires de B^+/B_2^+ dans R , i.e. à $t_G(R)$.

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

8.4. Pour tout k-anneau R , notons $R(t) = R \otimes_k k(t)$ l'<u>algèbre des nombres duaux</u> à valeurs dans R , i.e. l'algèbre $R[T]/T^2$ (on a noté t l'image de T). Pour tout k-groupe affine G , on note $\mathrm{Lie}\,G(R)$ le noyau de l'homomorphisme canonique de $G(R(t))$ dans $G(R)$ (provenant de l'application R-linéaire de $R(t)$ dans R qui envoie t sur 0). Dire qu'un élément $u \in G(R(t))$ est dans $\mathrm{Lie}\,G(R)$ revient à dire que $u(B^+) \subset tR(t)$. Comme $t^2 = 0$, le noyau de u contient alors B_2^+ et u induit une application k-linéaire $\tilde{u} : B^+/B_2^+ \to R$; on vérifie immédiatement que l'application $u \mapsto \tilde{u}$ définit un isomorphisme du groupe $\mathrm{Lie}\,G(R)$ sur $t_G(R)$.

8.5. Tout ce qui précède se transpose, de manière évidente, au cas des groupes formels. Supposons maintenant que k est un anneau commutatif pseudo-compact. Soit G un k-groupe formel, d'algèbre affine B , soit B^+ l'idéal d'augmentation et soit B_2^+ l'adhérence de $(B^+)^2$ dans B . Pour tout k-anneau fini ou profini R , l'espace cotangent de G à valeurs dans R est le R-module topologique $t_G^*(R) = (B^+/B_2^+) \hat{\otimes}_k R$ et l'espace tangent est le R-module $t_G(R)$ des applications k-linéaires continues de B^+/B_2^+ dans R . Le B-module $\Omega_k(B)$ des k-différentielles continues de l'anneau B s'identifie à $B \hat{\otimes}_k t_G^*(k)$, le k-module des différentielles invariantes $\omega_{G/k}$ s'identifiant à $t_G^*(k)$; le B-module des k-dérivations continues de B à valeurs dans B s'identifie encore à $t_G(B)$ et celui des k-dérivations invariantes à $t_G(k)$. Enfin, pour tout k-anneau fini ou profini R , $t_G(R)$ s'identifie à $\mathrm{Lie}\,G(R)$.

<u>Remarque</u> : supposons k local et soit G un k-groupe formel topologiquement plat. Si G est étale, on a évidemment $B_2^+ = B^+$ et $t_G(R) = t_G^*(R) = 0$, pour tout k-anneau fini ou profini R ; dans le cas général, on voit que $t_G(R)$ (resp. $t_G^*(R)$) s'identifie canoniquement à $t_{G^c}(R)$ (resp. $t^*_{G^c}(R)$) .

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

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

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

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

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

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

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

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

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

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

En particulier, si G est un k-groupe formel, on a deux structures naturelles de $k[F]$-module topologique sur $t_{\mathbb{D}(G)}(k)$: celle provenant de l'isomorphisme canonique entre $\mathrm{Hom}(G,\hat{G}_a)$ et $t_{\mathbb{D}(G)}(k)$ et celle obtenue par dualité, à partir de la structure de $k[V]$-module sur $t_{\mathbb{D}(G)}^*(k)$; on vérifie immédiatement que ces deux structures coïncident.

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

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

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

Dans tout ce paragraphe, k est un corps parfait.

9.1. Commençons par introduire la définition suivante :

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

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

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

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

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

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

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

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

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

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

9.4. Passons maintenant au cas général. Pour tout entier $r \geq 0$, soit $V_r = \{a \in A \mid a^{p^r} \in \mathfrak{a}\}$. Il est clair que les V_r forment une suite croissante d'idéaux fermés de A. Pour chaque r, le quotient $\tilde{V}_r = V_r/(V_r \cap I_2)$ est un

sous-k-espace vectoriel fermé de I/I_2, lui-même canoniquement isomorphe à $B^+/B_2^+ = t_G^*(k)$:

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

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

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

$$\nu(j) = \nu^{\underline{X}}(j) = \begin{cases} +\infty & \text{si } X_j \not\in \bigcup_{r \geq 0} V_r , \\ r & \text{si } X_j \in V_r - V_{r-1} . \end{cases}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

9.5. Remarques :

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

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

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

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

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

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

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

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

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

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

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

est exacte.

§10.- Cohomologie de Hochschild.

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

10.1. Pour tout entier $r \geq 2$, soit $B_r(X,Y) = (X+Y)^r - X^r - Y^r \in \mathbb{Z}[X,Y]$, soit η_r le pgcd des coefficients de $B_r(X,Y)$ et soit $C_r(X,Y) = \eta_r^{-1} B_r(X,Y)$; c'est

donc un polynôme à deux variables, homogène de degré r, dont les coefficients sont des entiers premiers entre eux.

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

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

On en déduit facilement le résultat suivant :

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

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

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

- si k est de caractéristique 0, ou si r n'est pas une puissance de p, il existe un $c \in k$ et un seul tel que $P(X,Y) = c((X+Y)^r - X^r - Y^r)$;
- si k est de caractéristique p et si $r = p^s$ (avec s entier ≥ 1), il existe un $c \in k$ et un seul tel que $P(X,Y) = c\Lambda(X^{p^{s-1}}, Y^{p^{s-1}})$.

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

L'assertion (i) est alors triviale.

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

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

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

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

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

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

On vérifie immédiatement que $\partial^n \circ \partial^{n-1} = 0$, pour $n \geq 1$; on note $C^{\cdot}(G,J)$ le complexe $(C^n(G,J), \partial^n)_{n \in \mathbb{N}}$; on note $Z^n(G,J)$ le noyau de ∂^n et $B^n(G,J)$ l'image de ∂^{n-1}, pour $n \geq 1$, $B^0(G,J) = 0$; on note $H^n_0(G,J)$ le groupe quotient $Z^n(G,J)/B^n(G,J)$ et on l'appelle le n-<u>ième groupe de Hochschild de</u> G <u>à valeurs dans</u> J. Enfin, nous écrirons ∂ au lieu de ∂^n lorsqu'il n'y aura pas de confusions possible sur l'entier n.

On voit, en particulier, que $H^0_0(G,J)$ s'identifie à $J(k)$ et que $H^1_0(G,J)$ s'identifie au groupe $\mathrm{Hom}(G,J)$ des morphismes de G dans J, dans la catégorie des k-groupes formels.

Nous notons $C^2_s(G,J)$ le groupe des 2-cocycles symétriques, i.e. le sous-groupe de $C^2(G,J)$ formé des f tels que $f_R(u,v) = f_R(v,u)$, pour tout k-anneau fini R et pour $u,v \in G(R)$. On pose $Z^2_s(G,J) = C^2_s(G,J) \cap Z^2(G,J)$. Il est clair que $B^2(G,J) \subset Z^2_s(G,J)$ et on note $H^2_s(G,J)$ le sous-groupe $Z^2_s(G,J)/B^2(G,J)$ de $H^2_0(G,J)$.

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

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

est exacte).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On voit que cette graduation est compatible avec l'opérateur bord et induit donc une graduation sur la cohomologie. Avec des notations évidentes, on a $H^n_0(G,\hat{G}_a) = \prod_{r=0}^{\infty} H^{n,r}_0(G,\hat{G}_a)$ et $H^2_s(G,\hat{G}_a) = \prod_{r=0}^{\infty} H^{2,r}_s(G,\hat{G}_a)$.

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

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

i) <u>Si</u> k <u>est de caractéristique</u> 0 <u>ou si</u> r <u>n'est pas une puissance de</u> p, <u>on a</u> $H^{1,r}_0(G,\hat{G}_a) = 0$ <u>et</u> $H^{2,r}_s(G,\hat{G}_a) = 0$.

ii) <u>Si</u> k <u>est de caractéristique</u> p <u>et si</u> $r = p^t$, <u>avec</u> $t \geq 1$, <u>on a</u> $H^{1,r}_0(G,\hat{G}_a) \simeq k^I$, <u>les</u> X^r_i, <u>pour</u> $i \in I$, <u>forment une base topologique de</u> $H^{1,r}_0(G,\hat{G}_a) = Z^{1,r}(G,\hat{G}_a)$ <u>sur</u> k ;

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

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

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

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

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

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

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

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

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

i) *si* k *est de caractéristique* 0 *ou si* r *n'est pas une puissance de* p , *on a* $H_r^1(G,\hat{G}_a) = 0$ *et* $H_{s,r}^2(G,\hat{G}_a) = 0$;

ii) *si* k *est de caractéristique* p *et si* $r = p^t$, *avec* t *entier* ≥ 1 ,

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

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

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

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

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

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

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

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

CHAPITRE II

COVECTEURS DE WITT

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

§ 1.- Vecteurs et covecteurs de Witt.

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

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

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

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

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

$$\ldots$$

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

$$\ldots$$

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

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

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

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

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

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