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

<u>Démonstration</u> : 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 $X_0, X_1, \dots, X_n$ défini par

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

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

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

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

$$\dots$$

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

$$\dots$$

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

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

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

Les S_n et les P_n définissent un schéma en anneaux commutatifs, affine sur Spec $\mathbb{Z}$, d'algèbre affine $\mathbb{Z}[X_0, X_1, \dots, X_n, \dots ; Y_0, \dots, Y_n, \dots]$. 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

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

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

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

$$s_n = S_n(a_0, a_1, \ldots, a_n ; b_0, b_1, \ldots, b_n) ,$$

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

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

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

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

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

1.3. Pour tout anneau commutatif R, et pour tout $x \in R$, notons $[x]$ l'élément de $W(R)$ défini par $[x] = (x, 0, \ldots, 0, \ldots)$. On appelle $[x]$ le <u>représentant multiplicatif</u> ou le <u>représentant de Teichmüller</u> de x dans $W(R)$. Il résulte de la définition des polynômes P_n que l'application $x \mapsto [x]$ est multiplicative (i.e., on a $[x][y] = [xy]$, si $x, y \in R$). On voit aussi que, si $x \in R$ et si $\underline{a} = (a_0, \ldots, a_n, \ldots) \in W(R)$, on a $[x]\underline{a} = (xa_0, x^p a_1, \ldots, x^{p^n} a_n, \ldots)$.

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

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

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

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

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

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

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

Witt unipotents.

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

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

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

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

pour m suffisamment grand.

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

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

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

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

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

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

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

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

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

i) pour tout entier $n \geq 0$, la suite des $S_m(a_{-n-m}, \dots, a_{-n-1}, a_{-n} ; b_{-n-m}, \dots, b_{-n-1}, b_{-n})$ est stationnaire ;

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

Commençons par démontrer deux lemmes :

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

La démonstration se fait par récurrence sur t :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

d'où l'assertion (i).

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

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

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

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

La loi $+$ est une loi de groupe abélien sur $CW(R)$.

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

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

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

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

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

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

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

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

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

Remarque : pour tout $\mathfrak{n} \in \mathfrak{N}_R$, soit $CW(R, \mathfrak{n}) = \varinjlim_{r \in \mathbb{N}} CW(R, \mathfrak{n}, r)$. C'est le sous-groupe de $CW(R)$ formé des éléments dont les composantes sont presque toutes dans $\mathfrak{n}$. On voit que la topologie du sous-groupe $CW(R,\mathfrak{n})$ est celle du produit direct restreint (cf. par exemple [34], p. 138) $R^{\mathbb{N}}$ relativement à $\mathfrak{n}$ pour chaque composante.

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

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

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

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

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

§ 2.- Endomorphismes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROPOSITION 2.2.- *Soit* R *un k-anneau.*

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

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

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

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

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

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

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

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

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

(7) $\underline{F}\,\underline{a} = (\dots, a^p_{-n}, \dots, a^p_{-1}, a^p_0)$ et $\underline{V}\,\underline{a} = (\dots, a_{-n-1}, \dots, a_{-2}, a_{-1})$.

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

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

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

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

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

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

Remarques :

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

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

(4') si $x = (x_0, x_1, \ldots, x_n, \ldots) \in A$ et $\underline{a} = (\ldots, a_{-n}, \ldots, a_{-1}, a_0) \in CW_k(R)$, on a $\underline{x}\underline{a} = (\ldots, b_{-n}, \ldots, b_{-1}, b_0)$ avec

$$b_{-n} = \lim_{m\to+\infty} P_m(\sigma^{-n-m}(x_0), \sigma^{-n-m}(x_1), \ldots, \sigma^{-n-m}(x_m) ; a_{-n-m}, \ldots, a_{-n-1}, a_{-n})\ .$$

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

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

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

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

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

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

on en déduit que

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

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

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

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

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

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

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

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

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

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

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

on commence par considérer le A-anneau profini $R = A[[(Y_{-n})_{n \in \mathbb{N}}]]$ des série formelles en les Y_{-n} . En appliquant la formule (4") à $(\dots, 0, \dots, 0, Y_{-m}, \dots, Y_{-1}, Y_0) \in CW^u(R)$, on voit que, dans R ,
$$P_m(\sigma^{-m}(\underline{x}_0), \dots, \sigma^{-m}(\underline{x}_m) ; Y_{-m}, \dots, Y_0)$$
$$= P_{m+1}(\sigma^{-m-1}(\underline{x}_0), \dots, \sigma^{-m-1}(\underline{x}_{m+1}) ; 0, Y_{-m}, \dots, Y_0) .$$

Si l'on note encore $\mathfrak{b}_r$ l'idéal de R engendré par les Y_{-n} , avec $n \geq r$, le même raisonnement que celui fait pour prouver le lemme 2.1 montre que
$$P_m(\sigma^{-m}(\underline{x}_0), \dots, \sigma^{-m}(\underline{x}_m) ; Y_{-m}, \dots, Y_0)$$
$$\equiv P_{m+1}(\sigma^{-m-1}(\underline{x}_0), \dots, \sigma^{-m-1}(\underline{x}_{m+1}) ; Y_{-m-1}, \dots, Y_{-1}, Y_0) \pmod{\mathfrak{b}_r^s}$$

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

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

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

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

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

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

§ 3.- <u>Quelques séries formelles</u>.

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

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

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

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

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

Considérons maintenant les trois S-anneaux topologiques suivant :

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

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

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

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

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

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

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

On a un diagramme commutatif :

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

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

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

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

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

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

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

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

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

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

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

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

Remarquons maintenant que le lemme 1.3 peut se réénoncer

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

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

$$S_0 = S = S(\ldots,X_{-n},\ldots,X_{-1},X_0;\ldots,Y_{-n},\ldots,Y_{-1},Y_0),$$
$$S_{-1} = S(\ldots,X_{-n-1},\ldots,X_{-2},X_{-1};\ldots,Y_{-n-1},\ldots,Y_{-2},Y_{-1}),$$
$$\ldots$$
$$S_{-m} = S(\ldots,X_{-n-m},\ldots,X_{-m-1},X_{-m};\ldots,Y_{-n-m},\ldots,Y_{-m-1},Y_{-m})$$
$$\ldots$$

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

PROPOSITION 3.2.-

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

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

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

Démonstration : c'est clair !

Remarques :

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

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

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

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

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

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

On définit de la même manière

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

Nous allons établir le résultat suivant :

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

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

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

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

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

Démonstration : la proposition résulte trivialement du lemme suivant :

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

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

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

Démonstration : il est clair qu'il suffit de démontrer ce lemme lorsque les entiers r et s satisfont $r \geq 1$, $s \geq p$ et $s \leq p^r$. Montrons qu'alors la congruence annoncée est vérifiée dès que $m \geq r-1+(s-p)/(p-1)$:

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

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

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

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

- Si $n < r$, on a, d'après le lemme 1.3,
  $S_{m'-n}(X_{-m'}, \dots, X_{-n} ; Y_{-m'}, \dots, Y_{-n})$
  $\equiv S_{m'+1-n}(X_{-m'-1}, \dots, X_{-n} ; Y_{-m'-1}, \dots, Y_{-n}) \pmod{\overline{\mathfrak{d}_{r-n+n}^s}}$,
  pourvu que $m'-n \geq (r-n)-1+(s-p)/(p-1)$. C'est donc le cas si $m' \geq m$ et, par passage à la limite, on en déduit $T_{-n} \equiv S_{-n} \pmod{\overline{\mathfrak{d}_r^s}}$; donc, a fortiori, $T_{-n}^{p^n} \equiv S_{-n}^{p^n} \pmod{\overline{\mathfrak{d}_r^s}}$.

§4.- Le groupe formel des covecteurs.

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

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

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

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

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

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

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

Remarques :

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

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

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

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

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

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

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

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

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

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

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

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

2.- La formule précédente implique que $\widehat{CW}_k^u$ est la "composante unipotente" de $\widehat{CW}_k$ (cf. n° I. 7. 6).

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

4.4. Soit k un corps parfait de caractéristique p . Si R est un k-anneau

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

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

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

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

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

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

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

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

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

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

PROPOSITION 4.1.- Soit R un k-anneau fini ou profini.

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

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

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

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

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

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

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

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

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

ce qui achève de prouver (iii).

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

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

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

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

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

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

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

§ 5.- Relèvement des covecteurs.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ou encore

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

d'où

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

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

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

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

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

Remarque : on aurait pu aussi déduire cette proposition de la proposition 3.3.

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

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

Remarques.

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

$$(1)\quad \begin{tikzcd} CW_A(\mathcal{R}) \arrow[r, "\hat{w}_{\mathcal{R}}"] \arrow[d, "CW(\varphi)"'] & \mathcal{R}_K \arrow[d, "\varphi_K"] \\ CW_A(\mathcal{S}) \arrow[r, "\hat{w}_{\mathcal{S}}"] & \mathcal{S}_K \end{tikzcd} \qquad (1')\quad \begin{tikzcd} CW_k(\mathcal{R}_k) \arrow[r, "w_{\mathcal{R}}"] \arrow[d, "CW(\varphi_k)"'] & \mathcal{R}_K/p\mathcal{R} \arrow[d, "\tilde{\varphi}_K"] \\ CW_k(\mathcal{S}_k) \arrow[r, "w_{\mathcal{S}}"] & \mathcal{S}_K/p\mathcal{S} \end{tikzcd}$$

sont commutatifs.

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

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

topologie quotient, est un anneau p-adique.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Supposons d'abord que $\mathfrak{R}$ est un anneau local et soit $\mathfrak{m}_{\mathfrak{R}}$ son idéal maximal. Pour tout entier $s \geq 1$, soit J_s le sous-A'-module de $\mathfrak{R}_K$ défini

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

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

PROPOSITION 5.2.-

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

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

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

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

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

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

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

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

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

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

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

Soit maintenant s un entier ≥ 1 ; si $n \geq 1$, on voit que $\pi^{-n+1}m_{\mathfrak{R}}^{ns}$ est un sous-A''-module fermé de $\hat{\mathfrak{R}}_K^{I}$, topologiquement libre, admettant comme base topologique les $\pi^{ns-|\underline{i}|-n+1}\underline{X}^{\underline{i}}$, pour $0 \leq |\underline{i}| \leq ns$, et les $\pi^{-n+1}\underline{X}^{\underline{i}}$, pour $|\underline{i}| > ns$. On en déduit facilement que J_s est formé des éléments $\sum a_{\underline{i}}\underline{X}^{\underline{i}}$ de $\mathfrak{R}_K$ vérifiant

$$\begin{cases} (1_a) & \text{si } |\underline{i}| \leq s , \quad v(a_{\underline{i}}) \geq s - |\underline{i}| , \\ (1_b) & \text{si } ms \leq |\underline{i}| < (m+1)s , \quad v(a_{\underline{i}}) \geq -m+1 , \text{ pour } m \text{ entier } \geq 1 , \end{cases}$$

où l'on a noté v la valuation de K'' normalisée par $v(\pi) = 1$.

Soit $u_j = \sum a_{\underline{i},j}\underline{X}^{\underline{i}}$, pour $j \in \mathbb{N}$, une suite d'éléments de $\mathfrak{R}_K$ qui est une suite de Cauchy pour la topologie définie par les J_s . La condition (1_a) implique que, pour $\underline{i}$ fixé , la suite des $a_{\underline{i},j}$ converge dans K'' ; ceci signifie que la suite des u_j est aussi une suite de Cauchy pour la topologie définie par les $I^m + p^n\mathfrak{R}$; par conséquent, la première topologie est plus fine que la seconde, et on voit immédiatement que l'application de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^{I}$ que l'on en déduit est injective.

Soit $\overline{J}_s$ l'adhérence de J_s dans $\hat{\mathfrak{R}}_K^{I}$ (pour la topologie définie par les $I^m + p^nR$) : il est clair que $\overline{J}_s$ est formé des $\sum a_{\underline{i}}\underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^{I}$ qui vérifient les conditions (1_a) et (1_b) . Un élément $\sum a_{\underline{i}}\underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^{I}$ est dans l'image de $\hat{\mathfrak{R}}_K^{an}$ si et seulement s'il est congru, modulo chaque $\overline{J}_s$, à un élément de $\mathfrak{R}_K$.

On voit facilement que tout élément de $\hat{\mathfrak{R}}_K^{I}$ qui n'est pas dans $\mathfrak{R}_K$ peut s'écrire sous la forme $\sum_{j=0}^{\infty} \pi^{-\lambda_j}u_{n_j}$ où

- les λ_j forment une suite strictement croissante d'entiers ≥ 0 ,
- les n_j forment une suite strictement croissante d'entiers ≥ 0 ,
- pour tout j , $u_{n_j} \in I^{n_j}$, et, si $j \geq 1$, le terme homogène de degré n_j en $X_1,\dots,X_d$ de u_{n_j} n'a pas tous ses coefficients divisibles par π .

Supposons qu'un tel élément soit dans l'image de $\hat{\mathfrak{R}}_K^{an}$; on voit que, pour tout $s \geq 1$, presque tous les $\pi^{-\lambda_j}u_{n_j}$ sont dans $\overline{J}_s$. Mais, pour $j \geq 1$, $\pi^{-\lambda_j}u_{n_j} \in \overline{J}_s$ implique que $-\lambda_j \geq -m+1$ si $n_j < (m+1)s$ donc que $-\lambda_j + (n_j/s) > 2$. Par conséquent, pour tout $s \geq 1$, on a $-\lambda_j + (n_j/s) > 2$, pour presque tout j ; il est clair que ceci implique que, pour tout $\varepsilon > 0$, la suite des $-\lambda_j + n_j\varepsilon$ tend vers l'infini, et l'élément considéré est bien de la forme indiquée dans le lemme.

Réciproquement, soit $\alpha = \sum_{n=0}^{\infty} \pi^{-\nu_n}u_n$ un élément de $\hat{\mathfrak{R}}_K^{I}$ avec $u_n \in I^n$, pour tout n , et $-\nu_n + n\varepsilon$ tend vers l'infini, pour tout $\varepsilon > 0$ fixé. On a alors, pour s fixé, $-\nu_n \geq -(n/s)+1$, pour presque tout n ; ce qui, d'après (1_b) implique que $\pi^{-\nu_n}u_n \in \overline{J}_s$; on en déduit que l'élément considéré est bien dans l'image de $\hat{\mathfrak{R}}_K^{an}$ dans $\hat{\mathfrak{R}}_K^{I}$.

Compte-tenu du lemme précédent, la proposition 5.2, est essentiellement triviale lorsque les A'-anneaux spéciaux qui interviennent sont des anneaux locaux ; le cas général s'en déduit en décomposant les anneaux spéciaux qui interviennent en produits d'anneaux locaux.

5.5. Soit $\mathfrak{R}$ un A'-anneau spécial. Notons $\Omega_{A'}(\mathfrak{R})$ (resp. $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$) le A'-module des A'-différentielles continues de $\mathfrak{R}$ (resp. $\hat{\mathfrak{R}}_K^{an}$) . L'injection canonique de $\mathfrak{R}$ dans $\hat{\mathfrak{R}}_K^{an}$ induit une application A'-linéaire de $\Omega_{A'}(\mathfrak{R})$ dans $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$; on voit que celle-ci est injective, et nous l'utilisons pour identifier $\Omega_{A'}(\mathfrak{R})$ à un sous-module de $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$. Si d désigne l'application canonique de $\hat{\mathfrak{R}}_K^{an}$ dans $\Omega_{A'}(\hat{\mathfrak{R}}_K^{an})$, nous notons $P(\mathfrak{R})$ l'ensemble des éléments $\alpha \in \hat{\mathfrak{R}}_K^{an}$ tels que $d\alpha \in \Omega_{A'}(\mathfrak{R})$. Il est clair que c'est un sous-A'-module fermé de $\hat{\mathfrak{R}}_K^{an}$.

Supposons $\mathfrak{R}$ local et choisissons des coordonnées $X_1, X_2, \ldots, X_d$. Alors $\mathfrak{R}$ s'identifie à l'anneau $A''[[X_1, X_2, \ldots, X_d]]$ des séries formelles en les X_i à coefficients dans A'' , anneau des entiers d'une extension finie non ramifiée K'' de K' . Utilisons le lemme 5.3 pour identifier $\hat{\mathfrak{R}}_K^{an}$ à un sous-anneau de $K''[[X_1, X_2, \ldots, X_d]] = \hat{\mathfrak{R}}_K^{I}$.

Soit $\alpha = \sum a_{\underline{i}} \underline{X}^{\underline{i}} \in \hat{\mathfrak{R}}_K^{I}$. On voit que $\alpha \in P(\mathfrak{R})$ si et seulement si les deux conditions suivantes sont satisfaites :

$$\begin{cases} (2_a) & \text{on a } \alpha \in \hat{\mathfrak{R}}_K^{an} , \\ (2_b) & \text{pour tout } \underline{i} = (i_1, i_2, \ldots, i_d) \in \mathbb{N}^d \text{ et tout } j \in \{1, 2, \ldots, d\} \text{ , on a } i_j a_{\underline{i}} \in A'' . \end{cases}$$

Soit v_n la composante homogène de degré n en les X_j de α . La condition (2_b) implique que si r_n est le plus grand entier tel que $p^{r_n} \leq n$, alors $p^{r_n} v_n \in \mathfrak{R}$; si on pose $u_n = p^{r_n} v_n$, on voit que $\alpha = \sum_{n=0}^{\infty} p^{-r_n} u_n$, avec $u_n \in I^n$; comme il est clair que, pour tout $\varepsilon > 0$, la suite des $-r_n + n\varepsilon$ tend vers l'infini, il résulte du lemme 5.3 que la condition (2_b) implique la condition (2_a) .

Pour tout $\underline{i} = (i_1, i_2, \ldots, i_d) \in \mathbb{N}^d$, $\neq 0 = (0,0,\ldots,0)$, notons $h(\underline{i})$ le plus grand entier h tel que p^h divise tous les i_j . On voit que $P(\mathfrak{R})$ est la somme directe de K'' et d'un A''-module topologiquement libre admettant comme base topologique les $p^{-h(\underline{i})} \underline{X}^{\underline{i}}$, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$.

Si nous revenons maintenant au cas où $\mathfrak{R}$ est un A'-anneau spécial quelconque, et si $\mathfrak{R} = \prod \mathfrak{R}_m$ représente la décomposition de $\mathfrak{R}$ en le produit de

ses composantes locales, on voit que $P(\mathfrak{R}) = \prod P(\mathfrak{R}_m)$.

5.6. PROPOSITION 5.4.- Soit $\mathfrak{R}$ un A'anneau spécial. Soit $\underline{\hat{a}} = (\ldots, \hat{a}_{-n}, \ldots, \hat{a}_{-1}, \hat{a}_0) \in CW_A(\mathfrak{R})$. La série de terme général $p^{-n} \hat{a}_{-n}^{p^n}$ converge dans $\hat{\mathfrak{R}}_K^{an}$. Notons $\hat{w}_{\mathfrak{R}}(\underline{\hat{a}})$ la somme de cette série. L'application $\hat{w}_{\mathfrak{R}} : CW_A(\mathfrak{R}) \to \hat{\mathfrak{R}}_K^{an}$ ainsi définie est A-linéaire continue et son image est contenue dans $P(\mathfrak{R})$.

Remarque : la notation $\hat{w}_{\mathfrak{R}}$ ne crée pas de risque de confusion avec la notation employée pour la proposition 5.1 : si $\mathfrak{R}$ est un A'-anneau spécial qui est aussi un A-anneau-p-adique, $\mathfrak{R}$ est un produit fini d'extensions finies non ramifiées de K' , $\mathfrak{R}_K$ s'identifie à $\hat{\mathfrak{R}}_K^{an}$ et les deux définitions de $\hat{w}_{\mathfrak{R}}$ coïncident.

Démonstration : en décomposant $\mathfrak{R}$ en le produit de ses composantes locales, on se ramène au cas où l'anneau spécial est local. Supposons qu'il en est ainsi et reprenons les notations qui précèdent.

Si $\underline{\hat{a}} = (\ldots, \hat{a}_{-n}, \ldots, \hat{a}_{-1}, \hat{a}_0) \in CW_A(\mathfrak{R})$, on voit que, pour n suffisamment grand, $\hat{a}_{-n} \in \mathfrak{m}_{\mathfrak{R}}$, donc que $p^{-n} \hat{a}_{-n}^{p^n} \in p^{-n} \mathfrak{m}_{\mathfrak{R}}^{p^n} \subset p^{-n} \mathfrak{m}_{\mathfrak{R}}^{(n+1)s} \subset J_s$, si $p^n > (n+1)s$; pour s fixé, ceci est vrai pour tout n suffisamment grand ; la convergence de la série en résulte.

Si $\underline{\hat{a}}_m = (\ldots, \hat{a}_{m,-n}, \ldots, \hat{a}_{m,0})$, pour $m \in \mathbb{N}$, est une suite d'éléments de $CW_A(\mathfrak{R})$ convergent vers un élément $\underline{\hat{a}} = (\ldots, \hat{a}_{-n}, \ldots, \hat{a}_0)$, on voit que

- d'une part, il existe un entier r , indépendant de m , tel que les $\hat{a}_{m,-n}$ et $\hat{a}_{-n}$ sont dans $\mathfrak{m}_{\mathfrak{R}}$, pour $n \geq r$;
- d'autre part, pour n fixé, la suite des $\hat{a}_{m,-n}$ converge, dans $\mathfrak{R}$, vers $\hat{a}_{-n}$.

Soit s un entier ≥ 1 . La première condition montre qu'il existe un entier n_0 , indépendant de m , tel que les $p^{-n} \hat{a}_{m,-n}^{p^n}$ et $p^{-n} \hat{a}_{-n}^{p^n}$ sont dans J_s , pour $n \geq n_0$. La deuxième implique qu'il existe un entier m_0 tel que, si $m \geq m_0$, $p^{-n} \hat{a}_{m,-n}^{p^n} \equiv p^{-n} \hat{a}_{-n}^{p^n} \pmod{J_s}$, pour $n < n_0$. La continuité de l'application $\hat{w}_{\mathfrak{R}}$ s'en déduit.

On voit que $CW^u(\mathfrak{R})$ est dense dans $CW_A(\mathfrak{R})$. Le fait que la restriction de $\hat{w}_{\mathfrak{R}}$ à $CW^u(\mathfrak{R})$ est A-linéaire résulte immédiatement des définitions ; la linéarité de $\hat{w}_{\mathfrak{R}}$ s'en déduit, par continuité.

Tout élément α de $\hat{\mathfrak{R}}_K^{an}$ qui est dans l'image de $\hat{w}_{\mathfrak{R}}$ s'écrit sous la forme $\sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n}$; on a donc $d\alpha = \sum \hat{a}_{-n}^{p^n-1} d\hat{a}_{-n} \in \Omega_{A'}(\mathfrak{R})$ et $\alpha \in P(\mathfrak{R})$, d'où la proposition.

5.7. Revenons sur les vecteurs de Witt : soit $\mathfrak{R}$ un A-anneau spécial. Posons $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. C'est un k-anneau profini. L'application canonique de $\mathfrak{R}$ sur $\mathfrak{R}_k$ induit une application de $CW_A(\mathfrak{R}) = CW(\mathfrak{R})$ dans $CW(\mathfrak{R}_k) = \widehat{CW}_k(\mathfrak{R}_k)$. Il est clair que c'est une application A-linéaire continue surjective et que son noyau $CW_A(p\mathfrak{R})$ est formé des covecteurs dont toutes les composantes sont dans l'idéal $p\mathfrak{R}$.

Si $a \in \mathfrak{R}$, pour tout entier $n \geq 0$, $p^{-n}(pa)^{p^n} \in p^{p^n-n}\mathfrak{R} \subset p\mathfrak{R}$; on en déduit que l'image de $CW_A(p\mathfrak{R})$ par $\hat{w}_{\mathfrak{R}}$ est contenue dans $p\mathfrak{R}$. L'application $\hat{w}_{\mathfrak{R}}$ définit donc, par passage aux quotients, une application A-linéaire continue $w_{\mathfrak{R}}$ de $CW_k(\mathfrak{R}_k)$ dans $P(\mathfrak{R})/p\mathfrak{R}$.

PROPOSITION 5.5.- <u>Soit</u> $\mathfrak{R}$ <u>un A-anneau spécial. L'application A-linéaire continue</u> $w_{\mathfrak{R}} : CW_k(\mathfrak{R}_k) \to P(\mathfrak{R})/p\mathfrak{R}$ <u>définie ci-dessus est un isomorphisme</u>.

<u>Démonstration</u> : en décomposant $\mathfrak{R}$ en le produit de ses composantes locales, on se ramène au cas où $\mathfrak{R}$ est local. En reprenant les notations du n° 5.5, on voit que, si l'on choisit des coordonnées, $\mathfrak{R}$ s'identifie à $A''[[X_1,X_2,\ldots,X_d]]$ où A'' est l'anneau des entiers d'une extension non ramifiée K'' de K .

On sait (cf. n° 5.5) qu'une fois les coordonnées choisies, $P(\mathfrak{R})$ est la somme directe de K'' et d'un A''-module topologiquement libre $P^c(\mathfrak{R})$ admettant comme base topologique les $p^{-h(\underline{i})}\underline{X}^{\underline{i}}$, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$. En particulier $P(\mathfrak{R})$ est un A''-module pro-artinien, et il en est de même de $P(\mathfrak{R})/p\mathfrak{R}$ qui est la somme directe de K''/pA'' et de $P^c(\mathfrak{R})/(p\mathfrak{R}) \cap P^c(\mathfrak{R})$.

Si k'' désigne le corps résiduel de A'' , on voit que $\mathfrak{R}_k$ s'identifie à $k''[[X_1,X_2,\ldots,X_d]]$; on a donc $\widehat{CW}_k(\mathfrak{R}_k) = \widehat{CW}_{k''}(\mathfrak{R}_k)$ et c'est aussi un A''-module pro-artinien (cf. prop. 4.1). On voit que $\widehat{CW}_k^{et}(\mathfrak{R}_k) = \widehat{CW}_k(k'')$ s'identifie par $w_{\mathfrak{R}}$ à K''/pA'' (cf. n° 2.3) ; d'autre part, pour $\underline{i} \in \mathbb{N}^d$, $\underline{i} \neq 0$, posons $\underline{i}' = p^{-h(\underline{i})}\underline{i}$; on voit que l'image par $w_{\mathfrak{R}}$ du covecteur $(\ldots,0,\ldots,0,\underline{X}^{\underline{i}'},0,\ldots,0)$ (où la seule composante non nulle est celle d'indice

$-h(\underline{i})$) est l'image dans $P(\mathfrak{R})/p\mathfrak{R}$ de $p^{-h(\underline{i})}\underline{X}^{\underline{i}}$. On en déduit que l'image de $w_{\mathfrak{R}}$ est dense dans $P(\mathfrak{R})/p\mathfrak{R}$, donc que $w_{\mathfrak{R}}$ est surjective puisque c'est une application A''-linéaire continue d'un A''-module pro-artinien dans un autre.

Montrons l'injectivité. Pour cela, si $a = \sum_{\underline{i}} a_{\underline{i}}\underline{X}^{\underline{i}} \in \mathfrak{R}_k$ (avec les $a_{\underline{i}} \in k''$), notons $\hat{a}$ le relèvement de a dans $\mathfrak{R}$ défini par $\hat{a} = \sum_{\underline{i}} [a_{\underline{i}}]\underline{X}^{\underline{i}}$ (où $[a_{\underline{i}}]$ désigne le représentant multiplicatif de $a_{\underline{i}}$ dans $A'' = W(k'')$). Si l'on note v la valuation $\underline{X}$-adique dans $\mathfrak{R}_k$ et $\hat{v}$ la valuation $\underline{X}$-adique dans $\mathfrak{R}$ et dans $K''[[X_1,\ldots,X_d]]$, on a donc, pour tout $a \in \mathfrak{R}_k$, $\hat{v}(\hat{a}) = v(a)$.

On a déjà dit que $w_{\mathfrak{R}}$ induit un isomorphisme de $\widehat{CW}_k^{et}(\mathfrak{R}_k)$ sur K''/pA'' ; on a $\widehat{CW}_k(\mathfrak{R}_k) = \widehat{CW}_k^{et}(\mathfrak{R}_k) \oplus \widehat{CW}_k^{c}(\mathfrak{R}_k)$ et l'on voit que $\widehat{CW}_k^{c}(\mathfrak{R}_k)$ est formé des covecteurs $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ vérifiant $v(a_{-n}) \geq 1$, pour tout n ; pour un tel covecteur, on voit que $\alpha = \sum_{n=0}^{\infty} p^{-n}\hat{a}_{-n}^{p^n} \in P^c(\mathfrak{R})$; pour achever la démonstration de l'injectivité, il suffit donc de montrer que si $\underline{a} \neq 0$, alors $\alpha \notin p\mathfrak{R}$. Pour cela, commençons par établir un lemme :

LEMME 5.6.- <u>Avec les hypothèses et les notations qui précèdent, si</u> $\alpha \in p\mathfrak{R}$, <u>pour tout</u> $m \in \mathbb{N}$ <u>tel que</u> $a_{-m} \neq 0$, <u>il existe</u> $m' \in \mathbb{N}$ <u>tel que</u> $v(a_{-m'}) \leq p^{-1}v(a_{-m})$.

<u>Démonstration du lemme</u> : il est clair que $\alpha \equiv \sum_{n=m}^{\infty} p^{-n}\hat{a}_{-n}^{p^n}$ (mod $p^{-m+1}\mathfrak{R}$). On a $\hat{v}\left(\hat{a}_{-m}^{p^m}\right) = p^m\hat{v}(\hat{a}_{-m}) = p^m v(a_{-m})$ et $p^{-m}\hat{a}_{-m}^{p^m}$ "commence" par un polynôme homogène en les X_j , de degré $p^m v(a_{-m})$, à coefficients dans K'' , dont les coefficients ne sont pas tous dans $p^{-m+1}A''$. Il doit donc exister un entier $m' > m$ tel que $\hat{v}\left(p^{-m'}\hat{a}_{-m'}^{p^{m'}}\right) \leq p^m\hat{v}(a_{-m})$, i.e. tel que $p^{m'}v(a_{-m'}) \leq p^m v(a_{-m})$; comme $m' \geq m+1$, on a donc $v(a_{-m'}) \leq p^{-1}v(a_{-m})$.

<u>Fin de la démonstration de la proposition</u> : si, avec les notations qui précèdent, il existait $\underline{a} \in \widehat{CW}_k^{c}(\mathfrak{R}_k)$, $\underline{a} \neq 0$, tel que $\alpha \in p\mathfrak{R}$, l'hypothèse $\underline{a} \neq 0$ impliquerait l'existence d'un entier m_0 tel que $a_{-m_0} \neq 0$; on pourrait alors construire par récurrence, en utilisant le lemme, une suite d'entiers $m_0,m_1,\ldots,m_i,\ldots$ telle que $v\left(a_{-m_{i+1}}\right) \leq p^{-1}v\left(a_{-m_i}\right)$, pour tout i , ce qui contredit le fait que $v(a_{-n}) \geq 1$, pour tout n .

<u>Remarque</u> : soit σ le Frobenius absolu sur k et sur $A = W(k)$ et soit $\tau = \sigma^{-1}$. Pour tout k-anneau fini ou profini R , notons $\widehat{CW}_k^{\tau}(R)$ le A-module déduit de $\widehat{CW}_k(R)$ par l'extension des scalaires $\tau : A \to A$ (autrement dit $\widehat{CW}_k^{\tau}(R)$ s'identifie à $\widehat{CW}_k(R)$ comme groupe abélien et, si $\lambda \in A$ et

$\underline{a} \in \widehat{CW}_k(R)$, multiplier λ par $\underline{a}$ dans $\widehat{CW}_k^{\tau}(R)$ revient à multiplier $\tau(\lambda)$ par $\underline{a}$ dans $\widehat{CW}_k(R)$). On voit que l'on peut aussi décrire $\widehat{CW}_k^{\tau}(R)$ comme étant l'ensemble des covecteurs $(\ldots,a_{-n},\ldots,a_{-1})$ où les a_{-n} (indexés par les entiers strictement négatifs) vérifient les mêmes conditions que celles demandées pour $\widehat{CW}_k(R)$, l'addition et la multiplication par un scalaire étant données par les mêmes formules. On voit aussi que, avec ces conventions, l'application

$$(\ldots,a_{-n},\ldots,a_{-1},a_0) \longmapsto (\ldots,a_{-n},\ldots,a_{-1})$$

permet d'identifier le A-module $\widehat{CW}_k^{\tau}(R)$ au quotient de $\widehat{CW}_k(R)$ par le sous-module formé des covecteurs de la forme $(\ldots,0,\ldots,0,a_0)$, i.e. le noyau de $\underline{V}$.

Si R est réduit (en particulier si $R = \mathfrak{R}_k$ où $\mathfrak{R}$ est un A'-anneau spécial), on voit que le noyau de $\underline{V}$ est aussi le noyau de p .

Dans le cas où $R = \mathfrak{R}_k$, avec $\mathfrak{R}$ un A-anneau spécial, on voit donc que l'application $w_{\mathfrak{R}}$ induit un isomorphisme $w_{\mathfrak{R}}^{\tau}$ de $\widehat{CW}_k^{\tau}(R_k)$ sur $P(\mathfrak{R})/\mathfrak{R}$.

§ 6. - Groupe de Cartier et exponentielle d'Artin-Hasse.

6.1. Pour tout anneau commutatif R , nous notons $\Lambda(R) = R[[T]]$ l'anneau des séries formelles en une variable T , à coefficients dans R , et $C(R)$ le groupe multiplicatif des éléments de $\Lambda(R)$ congrus à 1 modulo l'idéal engendré par T .

On voit que C est, de manière naturelle, un $\mathbb{Z}$-foncteur en groupes ; il est clair que c'est un $\mathbb{Z}$-groupe affine lisse.

Soit $\mu : \mathbb{N}^* \to \{0,-1,+1\}$ la fonction de Möbius :

$$\mu(n) = \begin{cases} 1 \text{ si } n=1 , \\ (-1)^r \text{ si } n \text{ est le produit de } r \text{ nombres premiers distincts,} \\ 0 \text{ dans les autres cas.} \end{cases}$$

Soit $\mathbb{Z}_{(p)}$ le localisé en p de l'anneau $\mathbb{Z}$. Nous notons $F(T)$ l'élément de l'anneau $\Lambda(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}[[T]]$ défini par

$$F(T) = \prod_{\substack{n\geq 1\\(n,p)=1}} (1-T^n)^{n^{-1}\mu(n)} .$$

Soit R un $\mathbb{Z}_{(p)}$-anneau. Pour tout $\underline{a} = (a_0,a_1,\ldots,a_n,\ldots) \in W(R)$, notons $E_R(\underline{a})$ l'élément de $C(R)$ défini par

$$E_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_n T^{p^n}) .$$

On sait (cf. par exemple, [15], chap. III, § 1) que E_R est un homomorphisme injectif du groupe $W(R)$ dans le groupe $C(R)$ et il est clair que E_R est fonctoriel en R . Autrement dit les E_R , pour R décrivant les $\mathbb{Z}_{(p)}$-anneaux, définissent un monomorphisme

$$E : W_{\mathbb{Z}_{(p)}} \longrightarrow C_{\mathbb{Z}_{(p)}}$$

de $\mathbb{Z}_{(p)}$-groupes affines.

6.2. Soit m un entier ≥ 1 . Notons $C^{(m)}(R)$ le sous-groupe de $C(R)$ formé des séries formelles congrues à 1 modulo l'idéal engendré par T^{p^m} . Il est clair que $C^{(m)}$ est un sous-$\mathbb{Z}$-groupe affine de C et que le quotient $C_m = C/C^{(m)}$ est encore un $\mathbb{Z}$-groupe affine lisse.

Si R est un $\mathbb{Z}_{(p)}$-anneau et si $\underline{a} = (a_0,\ldots,a_n,\ldots) \in W(R)$ est tel que $a_0 = a_1 = \ldots = a_{m-1} = 0$, on voit que $E_R(\underline{a}) \in C^{(m)}(R)$. Par passage au quotient, on déduit donc de E un morphisme de $\mathbb{Z}_{(p)}$-groupes affines

$$E_m : (W_m)_{\mathbb{Z}_{(p)}} \longrightarrow (C_m)_{\mathbb{Z}_{(p)}} .$$

Pour tout anneau commutatif R et tout entier $m \geq 1$, notons $\Lambda_m(R)$ l'anneau quotient $\Lambda(R)/T^{p^m}\Lambda(R)$ et T_{-m+1} l'image de T dans $\Lambda_m(R)$. On voit que $C_m(R)$ s'identifie au groupe multiplicatif des éléments de l'anneau $\Lambda_m(R)$ qui sont congrus à 1 modulo l'idéal engendré par T_{-m+1} .

Si on identifie T_{-m+1} à T_{-m}^p , $\Lambda_m(R)$ s'identifie à un sous-anneau de $\Lambda_{m+1}(R)$; on en déduit un monomorphisme de C_m dans C_{m+1} ; nous notons CC^u le $\mathbb{Z}$-foncteur en groupes $\varinjlim C_m$. On voit que, pour tout anneau commutatif R , $CC^u(R)$ s'identifie au groupe multiplicatif des éléments de l'anneau $C\Lambda^u(R) = \varinjlim \Lambda_m(R)$ qui sont congrus à 1 modulo l'idéal engendré par les T_{-m} .

Il est clair que, pour tout m , le diagramme

$$\begin{array}{ccc} (W_m)_{\mathbb{Z}_{(p)}} & \xrightarrow{E_m} & (C_m)_{\mathbb{Z}_{(p)}} \\ {\scriptstyle V_m}\downarrow & & \downarrow \\ (W_{m+1})_{\mathbb{Z}_{(p)}} & \xrightarrow{E_{m+1}} & (C_{m+1})_{\mathbb{Z}_{(p)}} \end{array}$$

est commutatif. Par passage à la limite, on en déduit un morphisme de $\mathbb{Z}_{(p)}$-foncteurs en groupes

$$CE^u : CW^u_{\mathbb{Z}_{(p)}} \longrightarrow CC^u_{\mathbb{Z}_{(p)}} .$$

Si R est un $\mathbb{Z}_{(p)}$-anneau et si $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW^u(R)$, on voit que

$$CE^u_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_{-n}T_{-n})$$

expression qui a un sens car, pour n assez grand, $a_{-n} = 0$, donc $F(a_{-n}T_{-n}) = 1$.

6.3. Soit $S = \mathbb{N}[1/p]$ l'ensemble des nombres rationnels ≥ 0 dont le dénominateur est une puissance de p. Soit R un anneau commutatif. Tout élément du R-module R^S s'écrit, avec des notations évidentes, d'une manière et d'une seule, sous la forme

$$\sum_{s\in S} a_s\theta_s , \text{ avec les } a_s \in R .$$

Notons $B\Lambda(R)$ le sous-R-module de R^S formé des éléments $\sum a_s\theta_s$ qui satisfont la propriété suivante :

$$(\Phi) \quad \begin{cases} \underline{\text{pour tout nombre réel}}\ r > 0 ,\ \underline{\text{il existe}}\ \varepsilon > 0\ \underline{\text{tel que}}\ a_s = 0 , \\ \underline{\text{si}}\ r - \varepsilon \leq s < r . \end{cases}$$

Soit $\alpha = \sum a_s\theta_s$ et $\beta = \sum b_s\theta_s$ deux éléments de $B\Lambda(R)$; on voit facilement que (Φ) implique, d'une part, que, pour tout $s \in S$, les $a_{s'}b_{s''}$ avec $s' + s'' = s$ sont presque tous nuls et, d'autre part, que, pour tout $r > 0$ il existe $\varepsilon > 0$ tel que $a_{s'}b_{s''} = 0$ si $r - \varepsilon \leq s' + s'' < r$; on peut donc définir un produit dans $B\Lambda(R)$ en posant

$$\alpha\beta = \sum_{s',s''\in S} a_{s'}b_{s''}\theta_{s'+s''} .$$

On voit que l'on a ainsi muni $B\Lambda(R)$ d'une structure de R-anneau

Soit $C\Lambda(R)$ le quotient de l'anneau $B\Lambda(R)$ par l'idéal engendré par θ_p. Si l'on note $\overline{\theta}_s$ l'image de θ_s dans $C\Lambda(R)$, tout élément de $C\Lambda(R)$ s'écrit d'une manière et d'une seule sous la forme $\sum_{s\in S, s<p} a_s\overline{\theta}_s$, où les a_s sont dans R et vérifient (Φ).

Nous notons $CC(R)$ le groupe multiplicatif des éléments de $C\Lambda(R)$ congrus à 1 modulo l'idéal engendré par les $\overline{\theta}_s$, pour $s > 0$. On voit que CC est de manière naturelle un $\mathbb{Z}$-foncteur en groupes.

Si l'on identifie T_{-n} et $\overline{\theta}_{1/p^n}$, on voit que $C\Lambda^u(R)$ s'identifie au sous-anneau de $C\Lambda(R)$ formé des $\sum a_s\overline{\theta}_s$ tels que les a_s sont presque tous nuls. En particulier CC^u s'identifie à un sous-$\mathbb{Z}$-foncteur en groupes de CC.

PROPOSITION 6.1.- Soit R un $\mathbb{Z}_{(p)}$-anneau commutatif.

i) Pour tout $\underline{a} = (\ldots, a_{-n}, \ldots, a_0) \in CW(R)$, le produit infini $\prod_{n=0}^{\infty} F(a_{-n}T_{-n})$ converge "ponctuellement" dans $CC(R)$ (i.e. si $\prod_{n=0}^{m} F(a_{-n}T_{-n}) = \sum b_{m,s}\overline{\theta}_s$, la suite des $b_{m,s}$, pour s fixé est stationnaire).

ii) Pour tout $\underline{a} \in CW(R)$, posons $CE_R(\underline{a}) = \prod_{n=0}^{\infty} F(a_{-n}T_{-n})$. L'application CE_R est un homomorphisme injectif du groupe $CW(R)$ dans $CC(R)$.

Pour tout $\underline{i} = (i_n)_{n\in\mathbb{Z}} \in \mathbb{N}^{(\mathbb{Z})}$, posons $|\underline{i}| = \sum i_n$; pour tout $s \in S$, soit $h(s)$ la somme des chiffres de s écrit "en base p". Commençons par établir quelques lemmes élémentaires :

LEMME 6.2.- Soit m un entier > 0 et soit $s \in S$. Il n'y a qu'un nombre fini de $\underline{i} \in \mathbb{N}^{(\mathbb{Z})}$ tels que $\sum p^{-n}i_n = s$ et $|\underline{i}| < m$.

Démonstration : quitte à multiplier s par une puissance de p, on peut supposer que $s \in \mathbb{N}$. Soit r un entier tel que $s < p^{r+1}$; on a nécessairement $i_n = 0$ pour $n < -r$. Soit t le plus grand entier tel que $i_t \neq 0$. Si $t > 0$, $p^{-t}i_t + \ldots + p^{-2}i_2 + p^{-1}i_1 \in \mathbb{N}$, donc $i_t + \ldots + p^{t-2}i_2 + p^{t-1}i_1$ est divisible par p^t et, d'après le lemme 1.2, $i_t + \ldots + i_2 + i_1 \geq (t-1)(p-1) + p$; on en déduit que $t < (m-1)/(p-1)$. On a donc nécessairement $i_n = 0$ si $n < -r$ ou si $n \geq (m-1)/(p-1)$. Le lemme est alors évident.

LEMME 6.3.- Soit $\underline{i} \in \mathbb{N}^{(\mathbb{Z})}$ et soit $s = \sum p^{-n}i_n$. Alors $|\underline{i}| \geq h(s)$.

Démonstration : soit $s = \sum p^{-n}j_n$, avec $0 \leq j_n < p$, l'écriture de s en base p. Il faut montrer que $\sum i_n \geq \sum j_n$. Quitte à multiplier par une puissance de p, on peut supposer que $i_n = j_n = 0$, pour $n > 0$. Procédons par récurrence sur le plus grand entier r tel que $j_{-r} \neq 0$:

- si $r = 0$, c'est clair ;
- dans le cas général, on voit que $i_0 = j_0 + pu$, avec $u \in \mathbb{N}$; on a donc

$j_{-1} + pj_{-2} + \ldots + p^{r-1}j_{-r} = (u+i_{-1}) + pi_{-2} + \ldots + p^{m-1}i_{-m} + \ldots$ et l'hypothèse de récurrence implique que $(u+i_{-1}) + i_{-2} + \ldots + i_{-m} + \ldots \geq j_{-1} + j_{-2} + \ldots + j_{-r}$; l'inégalité $i_0 + i_{-1} + \ldots + i_{-m} + \ldots \geq j_0 + j_{-1} + \ldots + j_{-r}$ s'en déduit immédiatement.

LEMME 6.4.- Soit $s,t \in S$. On a $h(s+t) \leq h(s) + h(t)$.

C'est une conséquence triviale du lemme précédent.

LEMME 6.5.- Soit m un entier > 0 et soit S_m l'ensemble des $s \in S$ vérifiant $h(s) < m$. Pour tout nombre réel $r > 0$, il existe $\varepsilon > 0$ tel que, si $s \in S_m$ vérifie $s < r$, alors $s \leq r - \varepsilon$.

Démonstration : il est clair qu'il suffit de montrer que, si

$s_1 < s_2 < \ldots < s_n < \ldots$

est une suite strictement croissante d'éléments de S tendant vers r , alors les $h(s_n)$ ne sont pas bornés.

Considérons l'écriture en base p de chacun des s_n :

$s_n = \sum_{t\in\mathbb{Z}} p^{-t}c_{n,t}$, avec les $c_{n,t}$ entiers presque tous nuls vérifiant $0 \leq c_{n,t} < p$.

On voit facilement que, pour t fixé, la suite des $c_{n,t}$ est stationnaire et que, si on note c_t sa limite, le nombre réel $r = \sum_{t\geq-\infty} p^{-t}c_t$ est égal à la limite des s_n . Comme la suite des s_n est strictement croissante, il y a une infinité de t tels que $c_t \neq 0$. La série de terme général c_t est donc divergente et les $h(s_n)$ ne sont pas bornés.

Démonstration de la proposition 6.1. : pour tout $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in CW(R)$, notons $r_{\underline{a}} = r$ le plus petit entier tel que l'idéal de R engendré par les a_{-n} , avec $n \geq r$, est nilpotent ; notons $\mathfrak{b}_{\underline{a}} = \mathfrak{b}$ cet idéal et $m_{\underline{a}} = m$ le plus petit entier ≥ 1 tel que $\mathfrak{b}^m = 0$.

Supposons d'abord que $r_{\underline{a}} = 0$. On voit que $F(a_{-n}T_{-n})$ est un polynôme de degré $< m$ en T_{-n} et que le coefficient de T^i_{-n} appartient à $\mathfrak{b}^i$. On en déduit que les monômes non nuls intervenant dans le développement du produit infini sont de la forme

$a_{\underline{i}} \cdot \prod_{n\in\mathbb{N}} T_{-n}^{i_n}$, avec $|\underline{i}| = \sum i_n < m$ et $a_{\underline{i}} \in \mathfrak{b}_{\underline{a}}^{|\underline{i}|}$.

On a $\prod T_{-n}^{i_n} = \overline{\theta}_s$, si $s = \sum p^{-n} i_n$. Pour s fixé, le coefficient de

$\overline{\theta}_s$ dans le produit infini est donc la somme $a'_s = \sum a_{\underline{i}}$, la sommation étant étendue aux $\underline{i}$ tel que $\sum p^{-n} i_n = s$ et $|\underline{i}| < m$; c'est une somme finie, d'après le lemme 6.2, d'où la convergence ponctuelle dans $R^{\overline{S}}$ (si $\overline{S} = \{s \in S \mid s < p\}$) ; de plus $a_{\underline{i}} \in \mathfrak{b}_{\underline{a}}^{|\underline{i}|} \subset \mathfrak{b}_{\underline{a}}^{h(s)}$, d'après le lemme 6.3, et on peut donc écrire

$$CE_R(\underline{a}) = \sum_{s\in S_m} a'_s \overline{\theta}_s \ , \text{ avec } a'_s \in \mathfrak{b}_{\underline{a}}^{h(s)} ,$$

et c'est un élément de $CC(R)$, d'après le lemme 6.5.

Soit maintenant $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ un élément quelconque de $CW(R)$ et soit $r = r_{\underline{a}}$, $m = m_{\underline{a}}$. En appliquant ce qui précède au covecteur $\underline{b} = (\ldots,a_{-n},\ldots,a_{-r},0,0,\ldots,0)$ on voit que le produit infini $\prod_{n=r}^{\infty} F(a_{-n}T_{-n})$ converge dans $CC(R)$ vers un élément de la forme $\sum_{s\in S_m} b'_s \overline{\theta}_s$, avec les b'_s dans R .

D'autre part, on voit que $\prod_{n=0}^{r-1} F(a_{-n}T_{-n})$ est un polynôme de degré $< p^r$ en T_{-r+1} (car $T_{-r+1}^{p^r} = 0$) ; pour tout entier j vérifiant $0 \leq j < p^r$, on a $T^j_{-r+1} = \overline{\theta}_{j/p^{r-1}}$ et $h(j/p^{r-1}) \leq (p-1)r$; on en déduit que $\prod_{n=0}^{r-1} F(a_{-n}T_{-n})$ s'écrit comme une somme finie de la forme $\sum_{\substack{s\in S \\ h(s)\leq(p-1)r}} c'_s \overline{\theta}_s$, avec les c'_s dans R .

La finitude de cette dernière somme implique que le produit infini

$$\prod_{n=0}^{\infty} F(a_{-n}T_{-n}) = \left(\prod_{n=0}^{r-1} F(a_{-n}T_{-n})\right).\left(\prod_{n=r}^{\infty} F(a_{-n}T_{-n})\right) = (\sum c'_s \overline{\theta}_s).(\sum b'_t \overline{\theta}_t)$$

converge dans $CC(R)$, ce qui achève de prouver l'assertion (i). On voit en outre que l'inégalité $h(s+t) \leq h(s) + h(t)$ (lemme 6.4) implique que l'on peut écrire, en posant $m' = m + (p-1)r$,

$$CE_R(a) = \sum_{s\in S_{m'}} a'_s \overline{\theta}_s \ , \text{ avec les } a'_s \in R .$$

Montrons que si $\underline{a}$ et $\underline{b} \in CW(R)$, alors $CE_R(\underline{a}+\underline{b}) = CE_R(\underline{a}).CE_R(\underline{b})$.

a) Si $\underline{a}$ et $\underline{b}$ sont dans $CW^u(R)$, cela résulte du n° 6.2.

b) Dans le cas général, il suffit de montrer que pour chaque $u \in S$ fixé, les coefficients de $\overline{\theta}_u$ dans $CE_R(\underline{a}+\underline{b})$ et dans $CE_R(\underline{a}).CE_R(\underline{b})$ sont égaux. Compte-tenu de (a) il suffit de montrer que pour un u donné, on peut trouver un entier t tel que si l'on remplace

$\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ par $(\ldots,0,\ldots,0,a_{-t},a_{-t+1},\ldots,a_0)$ et

$\underline{b} = (\ldots,b_{-n},\ldots,b_0)$ par $(\ldots,0,\ldots,0,b_{-t},b_{-t+1},\ldots,b_0)$,

cela ne change le coefficient de $\overline{\theta}_u$ ni dans $CE_R(\underline{a}+\underline{b})$ ni dans $CE_R(\underline{a}).CE_R(\underline{b})$. Or, il existe des entiers m_1 et m_2 tels que $CE_R(\underline{a})$ et $CE_R(\underline{b})$ peuvent s'écrire

$$CE_R(\underline{a}) = \sum_{s\in S_{m_1}} a'_s\overline{\theta}_s \quad \text{et} \quad CE_R(\underline{b}) = \sum_{s\in S_{m_2}} b'_s\overline{\theta}_s .$$

Il résulte facilement du lemme 6.5 qu'il n'existe qu'un nombre fini de couples $(s,s') \in S_{m_1} \times S_{m_2}$ tels que $s+s' = u$. L'assertion résulte alors de ce que, si $\underline{d}$ est un élément quelconque de $CW(R)$, le calcul du coefficient d'un $\overline{\theta}_s$ donné dans $CE_R(\underline{d})$ ne dépend que d'un nombre fini des composantes d_{-n} du covecteur $\underline{d}$.

Il reste à démontrer l'injectivité. Soit $\underline{a}$ un élément non nul de $CW(R)$. Si $\underline{a} \in CW^u(R)$, il existe un entier t tel que $a_{-t} \neq 0$ et $a_{-n} = 0$, pour $n > t$; le coefficient de T_{-t} dans $CE_R(\underline{a})$ est a_{-t} et $CE_R(\underline{a}) \neq 0$. Supposons donc que $\underline{a} \notin CW^u(R)$ et soit i le plus grand entier tel que $a_{-n} \in \mathfrak{b}^i_{\underline{a}}$, pour tout $n \geq r_{\underline{a}}$; on a $1 \leq i < m_{\underline{a}}$. Soit t un entier tel que $a_{-t} \notin \mathfrak{b}^{i+1}_{\underline{a}}$. On voit que le coefficient de T_{-t} dans $CE_R(\underline{a})$ est congru à $-a_{-t}$ modulo $\mathfrak{b}^{i+1}_{\underline{a}}$ et est donc $\neq 0$; par conséquent $CE_R(\underline{a}) \neq 0$.

6.4. Il est clair que l'application CE_R qui vient d'être construite est fonctorielle en R .

Soit k un $\mathbb{Z}_{(p)}$-anneau. Par restriction aux k-anneaux, CC définit un k-foncteur en groupes que nous notons CC_k . La famille des CE_R , pour tout k-anneau R , définit un monomorphisme de k-foncteurs en groupes que nous notons $CE_{(k)}$ ou simplement $CE : CW_k \to CC_k$.

<u>Remarque</u> : si k a de plus une structure d'anneau pseudo-compact, notons $\widehat{CC}_k$ le complété formel de CC_k (on a donc $\widehat{CC}_k(R) = CC_k(R)$, pour tout k-anneau fini R). On vérifie facilement que $\widehat{CC}_k$ est un k-groupe formel : soit $\overline{S} = \{s\in S \mid s<p\}$ et soit $\mathfrak{S}$ l'ensemble des parties S' de $\overline{S}$ qui vérifient :

(Φ') <u>pour tout</u> $r > 0$, <u>il existe</u> $\varepsilon > 0$ <u>tel que</u> $[r-\varepsilon,r[\cap \overline{S} \subset S'$.

Soit $\mathcal{C} = k[(X_s)_{s\in\overline{S}}]$ l'anneau des polynômes en les X_s à coefficients dans k ; pour tout $S' \in \mathfrak{S}$, notons $I_{S'}$ l'idéal de $\mathcal{C}$ engendré par les X_s ,

pour $s \in S'$. On voit que, pour tout k-anneau fini R , $\widehat{CC}_k(R)$ s'identifie à l'ensemble des homomorphismes continus du k-anneau $\mathcal{C}$ dans R , pour la topologie de $\mathcal{C}$ définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux de la forme $\mathfrak{a}\mathcal{C} + I_{S'}$, pour $\mathfrak{a}$ idéal ouvert de k et $S' \in \mathfrak{S}$. L'algèbre affine de $\widehat{CC}_k$ s'identifie donc à la complétion profinie de $\mathcal{C}$ pour cette topologie (cf. n° 4.8).

6.5. Supposons maintenant que k est un corps parfait de caractéristique p . Nous allons caractériser l'image de CE_R dans $CC(R)$ lorsque R est un k-anneau.

Soit $\overline{k}$ une clôture algébrique de k . Si $a \in \overline{k}$ et si s est un élément de S de la forme $p^{-r}t$, avec r et t entiers, nous notons a^s l'unique élément b de $\overline{k}$ tel que $b^{p^r} = a^t$ (autrement di $b = \sigma^{-r}(a^t)$).

Soit ℓ un nombre premier $\neq p$. Notons μ_ℓ le groupe des racines ℓ-ièmes de l'unité dans $\overline{k}$; posons $k_\ell = k(\mu_\ell)$ et, pour tout k-anneau R , $R_\ell = R \otimes_k k_\ell$. Si $\alpha = \sum a_s\overline{\theta}_s \in CC(R)$, pour tout $\eta \in \mu_\ell$,

$$\sum a_s\eta^s\overline{\theta}_s \in CC(R_\ell)$$

et $\prod_{\eta\in\mu_\ell} (\sum a_s\eta^s\overline{\theta}_s)$ est invariant par l'action de $Gal(k_\ell/k)$ et appartient donc à $CC(R)$. On a donc ainsi défini, pour tout k-anneau R , un endomorphisme U_ℓ du groupe $CC(R)$:

$$U_\ell(\sum a_s\overline{\theta}_s) = \prod_{\eta\in\mu_\ell} (\sum a_s\eta^s\overline{\theta}_s) .$$

Soit, pour tout k-anneau R ,

$$CCT(R) = \{\alpha\in CC(R) \mid U_\ell\alpha = 1 \text{ , pour tout } \ell \neq p\} .$$

Pour tout k-anneau R , notons $CC'(R)$ l'ensemble des éléments $\sum a_s\overline{\theta}_s$ de $CC(R)$ vérifiant :

(Ψ') <u>il existe</u> $\varepsilon > 0$ <u>tel que l'idéal de</u> R <u>engendré par les</u> a_s , <u>avec</u> $s < \varepsilon$, <u>est nilpotent</u>.

Il est clair que $CC'(R)$ est un sous-groupe de $CC(R)$. Si $\alpha = \sum a_s\overline{\theta}_s \in CC(R)$, on a, pour r entier ≥ 1 ,

$$\alpha^{p^r} = \sum a_s^{p^r}\overline{\theta}_s^{p^r} = \sum_{0\leq s<p^{-r+1}} a_s^{p^r}\overline{\theta}_{sp^r} .$$

On en déduit que $CC'(R)$ est contenu dans le sous-groupe $CC_{p^\infty}(R)$ de $CC(R)$ formé des éléments d'ordre une puissance de p.

Remarque 1 : si R est un k-anneau fini, le radical r_R de R est nilpotent, et la condition (Ψ') est équivalente à la suivante

(Ψ'') *il existe* $\varepsilon > 0$ *tel que* $a_s \in r_R$, *pour* $s < \varepsilon$.

En particulier, on voit que $CC'(R) = CC_{p^\infty}(R)$.

Enfin, nous posons $CCT'(R) = CCT(R) \cap CC'(R)$.

PROPOSITION 6.6.- *Soit* R *un k-anneau. L'application* CE_R *est un isomorphisme du groupe* $CW_k(R)$ *sur* $CCT'(R)$.

Pour montrer que l'image est contenue dans $CCT'(R)$, nous aurons besoin du lemme suivant :

LEMME 6.7.- *Soit* $F(T) = \prod_{(n,p)=1} (1-T^n)^{\mu(n)/n} \in \mathbb{Z}[[T]]$ *et soit* ℓ *un nombre premier* $\neq p$. *Dans* $\mathbb{Z}(\sqrt[\ell]{1})[[T]]$, *on a*

$$\prod_{\eta\in\mu_\ell} F(\eta T) = 1 .$$

Démonstration du lemme : comme $\mu(n) = 0$ si ℓ^2 divise n , on peut écrire

$$F(T) = \Big(\prod_{(n,p\ell)=1} (1-T^n)^{\mu(n)/n}\Big)\cdot\Big(\prod_{(n,p\ell)=1} (1-T^{n\ell})^{\mu(n\ell)/n\ell}\Big)$$

$$= \prod_{(n,p\ell)=1} \left(\frac{(1-T^n)^\ell}{(1-T^{n\ell})}\right)^{\mu(n)/n\ell}$$

puisque $\mu(n\ell) = -\mu(n)$ si $(n,\ell) = 1$. On a donc

$$\prod_{\eta\in\mu_\ell} F(\eta T) = \prod_{(n,p\ell)=1}\left(\prod_{\eta\in\mu_\ell} \frac{(1-\eta^nT^n)^\ell}{(1-\eta^{n\ell}T^{n\ell})}\right)^{\mu(n)/n\ell}$$

$$= \prod_{(n,p\ell)=1}\left(\frac{\prod_{\eta\in\mu_\ell}(1-\eta^nT^n)}{(1-T^{n\ell})}\right)^{\mu(n)/n} = 1$$

puisque $\prod_{\eta\in\mu_\ell}(1-\eta^nT^n) = 1 - T^{n\ell}$ si $(n,\ell) = 1$.

Démonstration de $\mathrm{Im}\, CE_R \subset CCT'(R)$: soit $\underline{a} = (\dots,a_{-n},\dots,a_0) \in CW_k(R)$. On a $CE_R(\underline{a}) = \prod F(a_{-n}T_{-n})$.

Soit ℓ un nombre premier $\neq p$. Il est clair que

$$U_\ell(CE_R(\underline{a})) = \prod_{n=0}^{\infty} U_\ell(F(a_{-n}T_{-n})) = \prod_{n=0}^{\infty}\Big(\prod_{\eta\in\mu_\ell} F(a_{-n}\eta^{p^{-n}}T_{-n})\Big) .$$

Comme $(\ell,p) = 1$, on a $\prod_{\eta\in\mu_\ell} F(a_{-n}\eta^{p^{-n}}T_{-n}) = \prod_{\eta\in\mu_\ell} F(\eta a_{-n}T_{-n}) = 1$, d'après le lemme 6.7. Par conséquent, $CE_R(\underline{a}) \in CCT(R)$.

Le fait que les composantes de $\underline{a}$ vérifient la condition (Ψ) (cf. n° 1.5) implique trivialement que les coefficients de $CE_R(\underline{a})$ vérifient (Ψ') donc que $CE_R(\underline{a}) \in CC'(R)$. Finalement, pour tout $\underline{a} \in CW_k(R)$,

$CE_R(\underline{a}) \in CCT(R) \cap CC'(R) = CCT'(R)$.

Si $\mathfrak{b}$ est un idéal de R et si ℓ est un nombre premier $\neq p$, nous notons $\mathfrak{b}_\ell$ l'idéal $\mathfrak{b}\otimes_k k_\ell$ de $R_\ell = R\otimes_k k_\ell$. Etant donnés deux éléments α et β de $CC(R_\ell)$ et un $\varepsilon > 0$,

- on pose $\alpha \equiv \beta \mod(\mathfrak{b},\varepsilon)$ si le coefficient de $\overline{\theta}_s$ dans $\alpha - \beta$ appartient à $\mathfrak{b}_\ell$, pour $0 < s < \varepsilon$;
- on pose $\alpha \equiv \beta \mod \varepsilon$ si $\alpha \equiv \beta \mod(0,\varepsilon)$.

LEMME 6.8.- *Soit* $\overline{S} = \{s\in S \mid s<p\}$ *et soit* $\delta = \sum_{s\in\overline{S}} d_s\overline{\theta}_s$ *un élément de* $CCT'(R)$.

i) *Soit* $\mathfrak{b}$ *un idéal de* R *et soit* ε *un nombre réel* > 0 *tels que* $\delta \equiv 1 \mod(\mathfrak{b},\varepsilon)$. *On a* $d_s \in \mathfrak{b}^2$, *pour tout* $s \in \overline{S}$ *vérifiant* $0 < s < \varepsilon$ *qui n'est pas de la forme* $s = p^{-n}$, *avec* n *entier*.

ii) *Soit* ε' *un nombre réel* > 0 *tel que* $\delta \equiv 1 \mod \varepsilon'$. *On a* $d_s = 0$ *pour tout* $s \in \overline{S}$ *vérifiant* $0 < s < 2\varepsilon'$ *qui n'est pas de la forme* $s = p^{-n}$, *avec* n *entier*.

Démonstration du lemme : commençons par prouver (i). Il est clair que si α et β sont deux éléments de $CC(R_\ell)$ vérifiant $\alpha \equiv \beta \equiv 1 \mod(\mathfrak{b},\varepsilon)$, on a $\alpha\beta \equiv \alpha + \beta - 1 \mod(\mathfrak{b}^2,\varepsilon)$. Par conséquent, si $\delta \equiv 1 \mod(\mathfrak{b},\varepsilon)$, on a

$$U_\ell\delta = \prod_{\eta\in\mu_\ell}(\sum d_s\eta^s\overline{\theta}_s) \equiv 1 + \sum_{\eta\in\mu_\ell}\sum_{0<s<\varepsilon} \eta^s d_s\overline{\theta}_s$$

$$\equiv 1 + \sum_{0<s<\varepsilon}\Big(\sum_{\eta\in\mu_\ell}\eta^s\Big)d_s\overline{\theta}_s \mod(\mathfrak{b}^2,\varepsilon) .$$

Soit $s \in S$ vérifiant $0 < s < \varepsilon$ et $s \neq p^{-n}$ pour tout n . Il existe un $\ell \neq p$ tel que $\eta^s = 1$ pour tout $\eta \in \mu_\ell$. Le coefficient de $\overline{\theta}_s$ dans

$U_\ell \delta$ est donc $\equiv \ell d_s \mod \mathfrak{d}^2$. Comme ℓ est premier à p, si $U_\ell \delta = 1$, on a $d_s \in \mathfrak{d}^2$.

La preuve de (ii) est analogue à celle de (i) si l'on remarque que, α et β étant deux éléments de $CC(R_\ell)$ vérifiant $\alpha \equiv \beta \equiv 1 \mod \varepsilon'$, on a $\alpha\beta \equiv \alpha + \beta - 1 \mod 2\varepsilon'$.

Fin de la démonstration de la proposition 6.6 : soit $\alpha \in CCT'(R)$. Comme $\alpha \in CC'(R)$, il existe un $\varepsilon > 0$ et un idéal nilpotent $\mathfrak{d}$ de R tel que $\alpha \equiv 1 \mod(\mathfrak{d}, \varepsilon)$.

Montrons, par récurrence sur i, que pour tout entier $i \geq 0$, il existe un $\beta_i \in \mathrm{Im}\, CE_R$ tel que $\alpha \equiv \beta_i \mod(\mathfrak{d}^{2^i}, \varepsilon)$:

- pour $i = 0$, on peut prendre $\beta_0 = 1$;
- si $\alpha \equiv \beta_i \mod(\mathfrak{d}^{2^i}, \varepsilon)$, on a $\alpha\beta_i^{-1} \equiv 1 \mod(\mathfrak{d}^{2^i}, \varepsilon)$; si $\alpha\beta_i^{-1} = \sum c_s \bar{\theta}_s$ et si $\mathfrak{d}^{2^i} = \mathfrak{d}'$, on a $c_s \in \mathfrak{d}'$ pour $0 < s < \varepsilon$ et, en particulier, $c_{p^{-n}} \in \mathfrak{d}'$ si $p^{-n} < \varepsilon$; donc $\underline{c} = (\ldots, c_{p^{-n}}, \ldots, c_{p^{-1}}, c_1) \in CW_k(R)$. On voit que $\gamma = CE_R(\underline{c}) \equiv 1 - \sum c_{p^{-n}} T_{-n} \mod(\mathfrak{d}'^2, \varepsilon)$. Posons $\delta = \alpha\beta_i^{-1}\gamma$; il est clair que le coefficient de $T_{-n} = \bar{\theta}_{p^{-n}}$ dans δ appartient à $\mathfrak{d}'^2$ et que $\delta \equiv 1 \mod(\mathfrak{d}', \varepsilon)$; il résulte de l'assertion (i) du lemme 6.8 que $\delta \equiv 1 \mod(\mathfrak{d}'^2, \varepsilon)$ ou encore que $\alpha \equiv \beta_i \gamma^{-1} \mod(\mathfrak{d}^{2^{i+1}}, \varepsilon)$ et la récurrence est établie.

En appliquant ceci à un entier i tel que $\mathfrak{d}^{2^i} = 0$, on se ramène à montrer que, si $\alpha \in CCT'(R)$ vérifie $\alpha \equiv 1 \mod \varepsilon$ (pour un ε donné > 0), alors $\alpha \in \mathrm{Im}\, CE_R$. En prodédant par récurrence sur ε', on voit qu'il suffit de montrer que, pour tout nombre réel $\varepsilon' > 0$, si $\alpha \in CCT'(R)$ vérifie $\alpha \equiv 1 \mod \varepsilon'$, il existe $\beta \in \mathrm{Im}\, CE_R$ tel que $\alpha \equiv \beta \mod 2\varepsilon'$:

- s'il n'existe pas d'entier n tel que $\varepsilon' \leq p^{-n} < 2\varepsilon'$, il résulte de l'assertion (ii) du lemme 6.8 que $\alpha \equiv 1 \mod 2\varepsilon'$ et on peut prendre $\beta = 1$;
- s'il existe un entier n tel que $\varepsilon' \leq p^{-n} < 2\varepsilon'$, il résulte de l'assertion (ii) du lemme 6.8 que $\alpha \equiv 1 - aT_{-n} \mod 2\varepsilon'$, pour un $a \in k$ convenable; on voit qu'il suffit alors de prendre $\beta = F(aT_{-n})$.

Remarque 2 : soit R un k-anneau. Par transport de structure, l'isomorphisme CE_R munit $CCT'(R)$ d'une structure de D_k-module à gauche. Si $\alpha = \sum a_s \bar{\theta}_s \in CCT'(R)$, on voit que

$$\underline{F}\alpha = \sum a_s^p \bar{\theta}_s ,$$
$$\underline{V}\alpha = \sum a_s \bar{\theta}_{sp} ,$$
$$[x]\alpha = \sum a_s x^s \bar{\theta}_s ,$$ pour tout $x \in k$ (on a noté $[x]$ le représentant multiplicatif de x dans $A = W(k)$).

Remarque 3 : pour tout k-anneau R, soit $BC(R)$ le groupe multiplicatif des éléments de $B\Lambda(R)$ congrus à 1 modulo l'idéal engendré par les θ_s, pour $s > 0$. Pour tout nombre premier ℓ, notons $B\Lambda(R)_\ell$ l'anneau $B\Lambda(R)[X]/(X^\ell - \theta_1)$. On voit que c'est un $B\Lambda(R)$-module libre de rang ℓ et que, si l'on note τ l'image de X, pour tout $s \in S$, il existe un élément $\theta_{s/\ell}$ de $B\Lambda(R)_\ell$ et un seul, de la forme $\tau^i \theta_t$, tel que $(\theta_{s/\ell})^\ell = \theta_s$. Pour tout $\alpha = \sum a_s \theta_s \in BC(R)$, posons

$$F_\ell(\alpha) = \prod_{\eta \in \mu_\ell} \left(\sum a_s \eta^s \theta_{s/\ell}\right)$$
$$V_\ell(\alpha) = \sum a_s \theta_{s\ell} .$$

On voit que F_ℓ et V_ℓ définissent des endomorphismes du groupe $BC(R)$ et que $F_\ell V_\ell(\alpha) = \alpha^\ell$.

On voit aussi que le sous-groupe $C(R)$ de $BC(R)$, formé des éléments de la forme $\sum_{s \in \mathbb{N}} a_s \theta_s$ (autrement dit le groupe multiplicatif des séries formelles, de terme constant égal à 1, en la variable $\theta_1 = T_0$), est stable par V_ℓ et F_ℓ. Par restriction V_ℓ et F_ℓ définissent des endomorphismes de $C(R)$; ce sont les opérateurs du même nom introduits par Cartier ([6], §2).

Le noyau de la projection canonique de $BC(R)$ sur $CC(R)$ n'est pas stable par V_ℓ, mais l'est par $V_\ell F_\ell$; par conséquent $V_\ell F_\ell$ opère sur $CC(R)$; on voit que, dans $CC(R)$, $V_\ell F_\ell = U_\ell$.

6.6. Supposons encore que k est un corps parfait de caractéristique p. Nous posons $A = W(k)$ et nous notons K le corps des fractions de A. Comme au numéro précédent, nous posons $S = \mathbb{N}[1/p]$ et $\bar{S} = \{s \in S \mid 0 \leq s < p\}$. Nous allons, pour terminer ce paragraphe, utiliser ce qui a été fait au §5 pour donner une interprétation du module des covecteurs de Witt à coefficients dans $C\Lambda(k)$.

Pour tout anneau commutatif R, muni de la topologie discrète, munissons l'anneau $B\Lambda(R)$ de la topologie définie en prenant comme système fondamental de voisinages ouverts de 0 les idéaux (θ_{p^m}), pour $m \in \mathbb{N}$. Il est clair que $B\Lambda(R)$ est un R-anneau linéairement topologisé, séparé et complet pour cette topologie.

Soit $\mathcal{B}_A = \varprojlim B\Lambda(A/p^n)$. Il est clair que, si A est muni de la topologie p-adique, $\mathcal{B}_A$ est un A-anneau linéairement topologisé, séparé et complet. On voit que $\mathcal{B}_A$ s'identifie au sous-A-module de A^S formé des éléments $\sum_{s\in S} a_s\theta_s$, avec les a_s dans A vérifiant

(Φ_1) $\left\{\right.$ *pour tout entier* $n \ge 0$ *et tout nombre réel* $r > 0$, *il existe* $\varepsilon > 0$ *tel que* $a_s \in p^nA$, *si* $r-\varepsilon \le s < r$.

Les idéaux (θ_{p^m}, p^n), pour m, $n \in \mathbb{N}$, forment un système fondamental de voisinages ouverts de 0 dans $\mathcal{B}_A$. On en déduit, avec la terminologie du n° 5.3, que $\mathcal{B}_A$ est un A-anneau pro-p-adique et que l'ensemble $\mathfrak{J}$ des idéaux de $\mathcal{B}_A$ de la forme (θ_{p^m}), pour m entier, est une famille d'idéaux co-p-adiques de $\mathcal{B}_A$ qui détermine sa topologie.

Posons $\mathcal{B}_K = (\mathcal{B}_A)_K = \mathcal{B}_A \otimes_A K$ et $\hat{\mathcal{B}}_K = \hat{\mathcal{B}}_K^{\mathfrak{J}}$. Il est clair que $\hat{\mathcal{B}}_K$ s'identifie, en tant que K-anneau topologique à la limite projective des $\mathcal{B}_K/\theta_{p^m}\mathcal{B}_K$, chaque quotient étant muni de la topologie p-adique.

On vérifie facilement que tout élément de $\hat{\mathcal{B}}_K$ s'écrit d'une manière et d'une seule sous la forme $\sum a_s\theta_s$, avec les $a_s \in K$ vérifiant (Φ_1) et

(Φ_2) $\left\{\right.$ *pour tout* $r > 0$, *il existe un entier* m *tel que* $p^m a_s \in A$, *si* $s < r$.

Enfin, nous notons $\mathcal{B}'_K$ le sous-espace vectoriel de $\hat{\mathcal{B}}_K$ formé des $\sum a_s\theta_s$ qui vérifient

(Φ_3) $\left\{\right.$ *pour tout* $r > 0$, *il existe* $c > 0$ *tel que* $|a_s|_p \le cs$, *si* $s \ge r$ *(en notant* $|\ |_p$ *la valeur absolue p-adique sur* K*)*.

On voit enfin que le k-anneau linéairement topologisé $\mathcal{B}_k = \mathcal{B}_A \otimes_A k = \mathcal{B}_A/p\mathcal{B}_A$ s'identifie canoniquement à $B\Lambda(k)$.

On a défini au n° 5.3 une application A-linéaire continue $w^{\mathfrak{J}}_{\mathcal{B}_A}$ de $CW_k(\mathcal{B}_k)$ dans $\hat{\mathcal{B}}_K/p\mathcal{B}_A$. En composant avec la multiplication par $1/p$ on en déduit une application A-linéaire continue $\varpi_k = p^{-1}w^{\mathfrak{J}}_{\mathcal{B}_A} : CW_k(\mathcal{B}_k) \to \hat{\mathcal{B}}_K/\mathcal{B}_A$.

Si $\underline{a} = (\ldots, a_{-n},\ldots,a_0) \in CW_k(\mathcal{B}_k)$ et si $\hat{a}_{-n}$ désigne un relèvement de a_{-n} dans $\mathcal{B}_A$, on voit que $\varpi_k(\underline{a})$ est l'image, dans $\hat{\mathcal{B}}_K/\mathcal{B}_A$ de la somme de la série de terme général $p^{-n-1}\hat{a}^{p^n}_{-n}$.

PROPOSITION 6.9.- *L'application A-linéaire continue* $\varpi_k : CW_k(\mathcal{B}_k) \to \hat{\mathcal{B}}_K/\mathcal{B}_A$ *est injective. Son image est* $\mathcal{B}'_K/\mathcal{B}_A$.

Démonstration : on voit que $CW_k(\mathcal{B}_k)$ est formé des $\underline{a} = (\ldots,a_{-n},\ldots,a_{-1},a_0)$, avec les $a_{-n} \in \mathcal{B}_k$ vérifiant

(Ψ'') $\left\{\right.$ *il existe des entiers* m *et* n_0 *tels que* $a_{-n} \in \theta_{p^{-m}}\mathcal{B}_k$, *si* $n \ge n_0$.

En procédant comme pour démontrer l'injectivité de $w_{\mathcal{R}}$ dans la proposition 5.5, on voit facilement que si $\underline{a} = (\ldots,a_{-n},\ldots,a_0)$ était un élément non nul de $CW_k(\mathcal{B}_k)$ tel que $\varpi_k(\underline{a}) = 0$, il existerait un entier m et une suite infinie $n_1, n_2, \ldots, n_i, \ldots$ telle que $a_{-n_i} \notin \theta_{p^{m-n_i}}\mathcal{B}_k$, ce qui contredirait (Ψ''). L'application ϖ_k est donc injective.

Soit $\underline{a} = (\ldots,a_{-n},\ldots,a_0) \in CW_k(\mathcal{B}_k)$ et soit m et n_0 des entiers tels que $a_{-n} \in \theta_{p^{-m}}\mathcal{B}_k$, si $n \ge n_0$. On peut choisir les relèvements $\hat{a}_{-n}$ des a_{-n} dans $\mathcal{B}_A$ pour que $\hat{a}_{-n} \in \theta_{p^{-m}}\mathcal{B}_A$, si $n \ge n_0$. Si on pose

$$\alpha = \sum_{n=0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n} \in \hat{\mathcal{B}}_K,$$

on a alors

$$\alpha = \sum_{n=0}^{n_0-1} p^{-n}\hat{a}^{p^n}_{-n} + \sum_{n=n_0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n} = p^{-n_0+1}\beta + \gamma,$$

avec $\beta \in \mathcal{B}_A$ et $\gamma = \sum_{n=n_0}^{\infty} p^{-n}\hat{a}^{p^n}_{-n}$.

On voit que, pour tout $s \in S$, le coefficient c_s de θ_s dans γ vérifie $|c_s|_p \le p^n$ si $s < p^{-m+n+1}$; donc, si $p^{-m+n} \le s < p^{-m+n+1}$, on a $s^{-1}|c_s|_p \le p^m$.

Pour tout $s \in S$, le coefficient b_s de θ_s dans $p^{-n_0+1}\beta$ vérifie $|b_s|_p \le p^{n_0-1}$; si r est un nombre réel > 0, on a donc

$$s^{-1}|b_s|_p \le r^{-1}p^{n_0-1} \quad \text{si } s \ge r.$$

On en déduit que pour tout $r > 0$, le coefficient a_s de θ_s dans α vérifie $|a_s|_p \le c(r)s$, pour tout $s \ge r$, si l'on pose $c(r) = \max(p^m, r^{-1}p^{n_0-1})$.

Par conséquent α, donc $p^{-1}\alpha$, vérifie (Φ_3) et appartient à $\mathcal{B}'_K$. On a donc montré que l'image de ϖ_k est contenue dans $\mathcal{B}'_K/\mathcal{B}_A$.

Si $\alpha = \sum a_s\theta_s$ est un élément quelconque de $\mathcal{B}_A$, nous posons, pour tout entier $n \geq 0$, $\alpha^{(n)} = \sum \sigma^{-n}(a_s)\theta_{sp^{-n}}$ (rappelons que σ est le Frobenius absolu). On voit que

$$(\alpha^{(n)})^{p^n} \equiv \alpha \pmod{p\mathcal{B}_A} \qquad \text{ou encore que}$$

$$p^{-n-1}(\alpha^{(n)})^{p^n} \equiv p^{-n-1}\alpha \pmod{p^{-n}\mathcal{B}_A} .$$

On en déduit facilement que l'image par ϖ_k de $CW^u(\mathcal{B}_k)$ (sous-groupe de $CW_k(\mathcal{B}_k)$ formé des covecteurs dont presque toutes les composantes sont nulles) est $\mathcal{B}_K/\mathcal{B}_A$.

Soit maintenant $\alpha = \sum a_s\theta_s$ un élément de $\mathcal{B}'_K$. Nous allons chercher un élément $\underline{a}$ de $CW_k(\mathcal{B}_k)$ tel que $\varpi_k(\underline{a})$ soit égal à l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$. La condition (Φ_2) montre que $\sum\limits_{0\leq s<1} a_s\theta_s \in \mathcal{B}_K$. Comme $\mathcal{B}_K/\mathcal{B}_A$ est contenu dans l'image de ϖ_k, on voit que l'on peut supposer $a_s = 0$ pour $s < 1$. D'après (Φ_3) il existe donc un $c > 0$ tel que $|a_s|_p \leq cs$, pour tout $s \in S$.

Pour $s < c^{-1}p$, on a $|a_s|_p < p$, donc $|a_s|_p \leq 1$ et $a_s \in A$; pour tout entier $n \geq 0$ et pour $c^{-1}p^{n+1} \leq s < c^{-1}p^{n+2}$, on a $|a_s|_p < p^{n+2}$, donc $|a_s|_p \leq p^{n+1}$. On a donc

$$\alpha \equiv \sum_{n=0}^{\infty}\Bigg(\sum_{c^{-1}p^{n+1}\leq s<c^{-1}p^{n+2}} a_s\theta_s\Bigg) \pmod{\mathcal{B}_A} ,$$

avec $p^{n+1}a_s \in A$ si $c^{-1}p^{n+1} \leq s < c^{-1}p^{n+2}$. Soit $m \in \mathbb{Z}$ tel que $p^m \leq c^{-1}p$. On voit que l'on peut réécrire α sous la forme

$$\alpha \equiv \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n \pmod{\mathcal{B}_A} ,$$

les β_n étant des éléments de $\mathcal{B}_A$.

Pour achever la démonstration de la proposition il suffit donc d'établir le lemme suivant :

LEMME 6.10.- Soit $m \in \mathbb{Z}$ et soit $\beta_0,\beta_1,\dots,\beta_n,\dots$ des éléments de $\mathcal{B}_A$. Il existe $\underline{a} \in CW_k(\mathcal{B}_k)$ tel que $\varpi_k(\underline{a})$ soit égal à l'image dans $\mathcal{B}'_K/\mathcal{B}_A$ de $\sum\limits_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n$.

Démonstration : soit $m' \in \mathbb{Z}$ et soit $\gamma_0,\gamma_1,\dots,\gamma_n,\dots$ des éléments de $\mathcal{B}_A$. Pour tout $n \geq 0$, on a $\left(\gamma_n^{(n)}\right)^{p^n} \equiv \gamma_n \pmod{p\mathcal{B}_A}$; par conséquent

$$\gamma'_n = p^{-1}\left(\gamma_{n+1} - \left(\gamma_{n+1}^{(n+1)}\right)^{p^{n+1}}\right) \in \mathcal{B}_A , \text{ pour tout } n \geq 0$$

et

$$\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m'+n}}\gamma_n = \sum_{n=0}^{\infty} p^{-n-1}\left(\theta_{p^{m'}}\gamma_n^{(n)}\right)^{p^n} + \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m'+1)+n}}\gamma'_n .$$

On voit donc que l'image de $\sum\limits_{n=0}^{\infty} p^{-n-1}\theta_{p^{m'+n}}\gamma_n$ dans $\mathcal{B}'_K/\mathcal{B}_A$ est égale à la somme de l'image de $\sum\limits_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m'+1)+n}}\gamma'_n$ et de $\varpi_k(\underline{b})$ où $\underline{b} = (\dots,b_{-n},\dots,b_0)$ est un élément de $CW_k(\mathcal{B}_k)$ tel que $b_{-n} \in \theta_{p^m}\mathcal{B}_k$, pour tout n.

En appliquant ceci successivement à $m' = m, m+1,\dots,m+t,\dots$, on voit que l'on peut construire des éléments $\underline{b}_m,\underline{b}_{m+1},\dots,\underline{b}_{m+t},\dots$ de $CW(\mathcal{B}_k)$ vérifiant, pour tout $t \geq 0$,

- les coefficients de $\underline{b}_{m+t}$ appartiennent à $\theta_{p^{m+t}}\mathcal{B}_k$,
- si α_t est un relèvement dans $\mathcal{B}'_K$ de $\varpi_k(\underline{b}_m+\underline{b}_{m+1}+\dots+\underline{b}_{m+t})$, on a

$$\alpha = \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{m+n}}\beta_n \equiv \alpha_t + \sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{(m+t)+n}}\delta_{n,t} \pmod{\mathcal{B}_A} ,$$ où les $\delta_{n,t}$ sont dans $\mathcal{B}_A$.

On voit donc que la suite des α_t converge vers l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$; le fait que les coefficients de $\underline{b}_{m+t}$ sont dans $\theta_{p^{m+t}}\mathcal{B}_k$ implique que la série de terme général $\underline{b}_{m+t}$ converge, dans $CW_k(\mathcal{B}_k)$, vers un élément $\underline{a}$; la continuité de ϖ_k implique que $\varpi_k(\underline{a})$ est égal à l'image de α dans $\mathcal{B}'_K/\mathcal{B}_A$

6.7. On conserve les hypothèses et les notations du numéro précédent. Posons $\mathcal{C}_k = C\Lambda(k)$; rappelons que c'est le quotient de l'anneau $\mathcal{B}_k = B\Lambda(k)$ par l'idéal engendré par θ_p. Notons $CW_k(\theta_p\mathcal{B}_k)$ le sous-A-module fermé de $CW_k(\mathcal{B}_k)$ formé des covecteurs dont toutes les composantes sont dans $\theta_p\mathcal{B}_k$. Il est clair que l'on a une suite exacte de A-modules topologiques

$$0 \longrightarrow CW_k(\theta_p\mathcal{B}_k) \longrightarrow CW_k(\mathcal{B}_k) \longrightarrow CW_k(\mathcal{C}_k) \longrightarrow 0 .$$

Soit $$\mathcal{B}''_K = \left\{ \sum a_s\theta_s \in \hat{\mathcal{B}}_K \;\middle|\; \begin{array}{l} a_s = 0 \quad \text{si} \quad s < p \\ |a_s|_p \leq s \quad \text{pour tout} \quad s \in S \end{array} \right\} .$$

On voit que $\mathcal{B}''_K \subset \mathcal{B}'_K$ et qu'un élément α de $\hat{\mathcal{B}}_K$ de la forme $\sum_{s\geq p} a_s\theta_s$ est dans $\mathcal{B}''_K$ si et seulement si $p^n a_s \in A$, si $p^n \leq s < p^{n+1}$. Il est clair que $\mathcal{B}''_K$ est aussi l'ensemble des éléments de $\hat{\mathcal{B}}_K$ qui peuvent s'écrire sous la forme

$$\sum_{n=0}^{\infty} p^{-n-1}\theta_{p^{n+1}}\beta_n \text{ , avec des } \beta_n \in \mathcal{B}_A .$$

On voit facilement (cf. la démonstration du lemme 6.10) que l'image par ϖ_k de $CW_k(\theta_p\mathcal{B}_k)$ est formé des éléments de $\mathcal{B}'_K/\mathcal{B}_A$ que l'on peut relever, dans $\mathcal{B}'_K$, en un élément de $\mathcal{B}''_K$. Par passage au quotient, on en déduit un isomorphisme

$$\overline{\varpi}_k : CW_k(\mathcal{C}_k) \longrightarrow \mathcal{B}'_K/(\mathcal{B}''_K + \mathcal{B}_A) .$$

On peut énoncer ce résultat sous la forme suivante :

PROPOSITION 6.11.- *Notons* Θ_k *le A-module formé des éléments* $\sum a_s\theta_s$, *avec*

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

vérifiant les conditions (Φ_1), (Φ_2) *et* (Φ_3). *L'application* ϖ_k *définit, par passage au quotient, un isomorphisme* $\overline{\varpi}_k$ *du A-module* $CW_k(\mathcal{C}_k)$ *sur* Θ_k.

Remarque : en particulier, la structure de D_k-module à gauche sur $CW_k(\mathcal{C}_k)$ se transporte sur Θ_k. On voit que l'action de $\underline{F}$ et de $\underline{V}$ sont définies par

$$\underline{F}(\sum a_s\theta_s) = \sum \sigma(a_s)\theta_{sp} \quad \text{et} \quad \underline{V}(\sum a_s\theta_s) = \sum p\sigma^{-1}(a_s)\theta_{s/p} .$$

CHAPITRE III

MODULE DE DIEUDONNÉ

Dans tout ce chapitre et dans les suivants, on note k un corps parfait de caractéristique p, on note $A = W(k)$ l'anneau des vecteurs de Witt à coefficients dans k et $D_k = A[\underline{F},\underline{V}]$ l'anneau de Dieudonné de k. Si τ est un automorphisme de k, on note encore τ son relèvement à A ainsi que le prolongement de ce relèvement à D_k (avec $\tau(\underline{F}) = \underline{F}$, $\tau(\underline{V}) = \underline{V}$). Nous appliquerons ceci en particulier au Frobenius absolu σ (on a $\sigma(x) = x^p$, pour tout x dans k).

§ 1.- Classification des p-groupes formels.

1.1. Nous disons qu'un groupe formel (commutatif) G sur k est un *p-groupe formel* s'il s'identifie à la limite inductive, pour $n \to \infty$, des noyaux de la multiplication par p^n.

Les assertions suivantes sont évidentes :

- tout k-groupe formel connexe est un p-groupe formel ;
- si $G = G^c \times G^{et}$, avec G^c connexe et G^{et} étale, est un k-groupe formel, G est un p-groupe formel si et seulement si G^{et} l'est ;
- un k-groupe formel G est un p-groupe formel si et seulement si $G(k')$ est un groupe de p-torsion, pour toute extension finie k' du corps k ;
- un k-groupe formel G est un p-groupe formel si et seulement si $G(R)$ est un groupe de p-torsion, pour tout k-anneau fini R ;
- la catégorie des p-groupes formels sur k est une sous-catégorie épaisse de la catégorie des k-groupes formels ;
- le groupe $\widehat{CW}_k$ est un p-groupe formel.

1.2. Soit G un k-groupe formel et soit B_G son algèbre affine. L'ensemble des morphismes de k-schémas formels de G dans $\widehat{CW}_k$ s'identifie, par le