SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

JEAN-MARC DECAUWERT

Modules associés aux A-modules formels

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 8, p. 1-25

<http://www.numdam.org/item?id=STNG_1974-1975__4__A8_0>

Séminaire de Théorie des Nombres
16 et 23 janvier 1975
Grenoble

MODULES ASSOCIES AUX A-MODULES FORMELS

par Jean Marc DECAUWERT

Soit L un corps p-adique complet, K une extension finie de $\mathbb{Q}_p$ contenue dans L, B et A les anneaux d'entiers de L et K. Le but de cet exposé est l'étude des A-modules formels définis sur B. Après avoir rappelé certains résultats généraux, dus pour l'essentiel à L. Cox [1] sur ces A-modules formels et leurs logarithmes, on s'intéressera au cas où l'extension L/K est non ramifiée. Dans ce cas, on associera à tout A-module formel F défini sur B un module $M^o(F)$ sur un anneau de séries formelles non commutatives à coefficients dans B et on montrera que ces modules permettent de classer les A-modules formels définis sur le corps résiduel de B. On définira ensuite un sous-B-module $L^o(F)$ de $M^o(F)$ et on montrera que l'étude des A-modules formels définis sur B se ramène à celle des couples du type $(L^o(F), M^o(F))$, en suivant une méthode indiquée par J.M. Fontaine [3] et [4].

I - GROUPES FORMELS ET A-MODULES FORMELS.

Soit B un anneau commutatif unitaire. Si $X = (x_1, \ldots, x_n)$ est un système de n variables, on notera $B[[X]]$ l'anneau des séries formelles en les n variables $x_1, \ldots, x_n$, à coefficients dans B. Si $f(X)$ et $g(X)$ sont des séries formelles de $B[[X]]$, on dira que f est congrue à g modulo degré r et on notera $f \equiv g \ (\deg r)$ si f et g ne diffèrent que par leurs termes de degré total $\geq r$. Si $\mathfrak{M}$ est un idéal de B, on écrira $f \equiv g \ (\mathfrak{M})$ si $(f-g)$ est une série formelle à coeffi-

cients dans $\mathfrak{M}$, et $f \equiv g \ (\deg r, \mathfrak{M})$ s'il existe φ et ψ dans $B[[X]]$ telles que $f-g = \varphi+\psi$ avec $\varphi \equiv 0 \ (\deg r)$ et $\psi \equiv 0 \ (\mathfrak{M})$. On notera $B[[X]]_o$ l'ensemble des séries formelles $f \equiv 0 \ (\deg 1)$.

DEFINITION I.1. Soient X et Y des systèmes de n variables $(x_1,\ldots,x_n)$ et $(y_1,\ldots,y_n)$. Un groupe formel de dimension n défini sur B est un système de n séries formelles

$$F(X,Y) = (F_1(X,Y),\ldots,F_n(X,Y)) \in B[[X,Y]]_o^n$$

vérifiant :

(i) $F(X,Y) \equiv X+Y \ (\deg 2)$

(ii) $F(F(X,Y),Z) = F(X,F(Y,Z))$.

Si de plus F vérifie $F(X,Y) = F(Y,X)$, on dit que F est commutatif.

De (i) et (ii) on déduit que $F(X,0) = F(0,X) = X$ et qu'il existe

$$i_F(X) \in B[[X]]_0^n$$

tel que

$$F(X,i_F(X)) = F(i_F(X),X) = 0 \quad .$$

L'exemple le plus simple de groupe formel commutatif est le groupe additif $G_a(X,Y) = X+Y$. Lazard a démontré que tout groupe formel de dimension un défini sur un anneau réduit est commutatif.

DEFINITION I.2. Soient F et G deux groupes formels définis sur B , de dimensions respectives n et m , et soit C un anneau contenant B . Un élément φ de $C[[X]]_0^m$ (où $X = (x_1,\ldots,x_n)$) est un homomorphisme de F dans G s'il vérifie :

$$\varphi \circ F = G \circ \varphi$$

c'est-à-dire $\varphi(F_1(X,Y),\ldots,F_n(X,Y)) = G(\varphi(X),\varphi(Y))$.

Si $m = n$ et si φ est inversible, φ^{-1} est un homomorphisme de G dans F et on dit dans ce cas que φ est un isomorphisme de F dans G ; si de plus $\varphi(X) \equiv X \ (\deg 2)$, on dit que l'isomorphisme φ

est strict.

Par la suite, nous ne nous intéresserons qu'aux groupes formels commutatifs, et "groupe formel" signifiera donc désormais "groupe formel commutatif".

On munit alors l'ensemble $\mathrm{Hom}_C(F,G)$ des C-homomorphismes de F dans G d'une structure de groupe commutatif en posant

$$(\varphi \oplus \psi)(X) = G(\varphi(X), \psi(X))$$

si φ et $\psi \in \mathrm{Hom}_C(F,G)$.

Cette addition et la composition des séries munissent en particulier $\mathrm{End}_C(F) = \mathrm{Hom}_C(F,F)$ d'une structure d'anneau, en général non commutatif.

Si B est un anneau de caractéristique nulle et L son corps des fractions, et si F est un groupe formel de dimension n défini sur B , il existe un unique L-isomorphisme strict f de F dans le groupe additif de dimension n ; on l'appelle logarithme de F .

On voit alors que si G est un groupe formel défini sur B de dimension m et de logarithme g , tout C-homomorphisme de F dans G est de la forme $\varphi = g^{-1} \circ M \circ f$ pour une matrice $M \in M_{m,n}(C)$; réciproquement si $M \in M_{m,n}(C)$, $g^{-1} \circ M \circ f \in \mathrm{Hom}_C(F,G)$ si et seulement si $g^{-1} \circ M \circ f$ est à coefficients dans C . L'application qui à φ associe M définit un isomorphisme de $\mathrm{Hom}_C(F,G)$ dans $M_{m,n}(C)$ et en particulier si F = G un isomorphisme d'anneaux de $\mathrm{End}_C(F)$ dans $M_n(C)$. On appellera M la matrice jacobienne de φ .

Si F est un groupe formel de dimension n défini sur B , on définit par récurrence des systèmes $[r]_F$ de n séries formelles $([r]_{F,1}, \ldots, [r]_{F,n})$ de $B[[X]]_0^n$ pour tout entier r en posant

$$[1]_F(X) = X$$
$$[r]_F(X) = F([r-1]_F(X), X) .$$

Nous nous intéresserons désormais au cas où B est l'anneau des entiers d'un corps p-adique complet L ; τ désignera une uniformisante de B et ℓ le corps résiduel $B/\tau B$. Si F et G sont deux groupes formels définis sur B et φ un B-homomorphisme de F dans G , la réduction $\tilde{\varphi}$ de φ à $\ell[[X]]_0^m$ définit un ℓ-homomorphisme de $\tilde{F}$ dans $\tilde{G}$.

DEFINITION I.3. Un groupe formel F de dimension n défini sur ℓ est dit de hauteur finie si $\ell[[x_1,\ldots,x_n]]$ est un module de type fini sur le sous-anneau $\ell[[[p]_{F,1},\ldots,[p]_{F,n}]]$; s'il en est ainsi $\ell[[x_1,\ldots,x_n]]$ est un module libre sur $\ell[[[p]_{F,1},\ldots,[p]_{F,n}]]$ dont le rang est une puissance p^H de p ; H est la hauteur du groupe formel F .

La hauteur d'un groupe formel défini sur B est par définition la hauteur de sa réduction à ℓ .

A-MODULES FORMELS.

DEFINITION I.4. Soient A et B deux anneaux et $i : A \to B$ un homomorphisme. Un groupe formel F défini sur B est un A-module formel si pour tout $a \in A$, il existe un B-endomorphisme $[a]_F$ de F de matrice jacobienne $i(a)I_n$ et tel que l'application ainsi définie de A dans $\mathrm{End}_B(F)$ soit un homomorphisme d'anneaux.

Si C est un anneau contenant B , un C-homomorphisme du A-module formel F dans le A-module formel G est un $\varphi \in \mathrm{Hom}_C(F,G)$ tel que pour tout $a \in A$

$$\varphi \circ [a]_F(X) = [a]_G \circ \varphi(X) \ .$$

On notera $\mathrm{Hom}_{C,A}(F,G)$ l'ensemble de ces homomorphismes, qui est muni d'une structure naturelle de A-module, et de même $\mathrm{Hom}_{C,A}(F,F) = \mathrm{End}_{C,A}(F)$ est une A-algèbre, non nécessairement commutative.

Nous allons d'abord appliquer cette définition au cas où K est un corps local contenu dans le corps p-adique L , d'anneau d'entiers A ,

d'indice de ramification e sur $\mathbb{Q}_p$, de degré résiduel d, on désignera par π une uniformisante de A et par k le corps résiduel $A/\pi A$, de cardinal $q = p^d$. Le degré de K sur $\mathbb{Q}_p$ est donc $m = de$, et i sera ici l'inclusion de A dans l'anneau B des entiers de L.

On voit en particulier que tout groupe formel défini sur B est un $\mathbb{Z}$-module formel et même un $\mathbb{Z}_p$-module formel.

PROPOSITION I.1. Soit F un A-module formel défini sur B de hauteur finie H en tant que groupe formel. Alors m divise H et $\ell[[X_1,\ldots,X_n]]$ est un module libre de rang q^h sur $\ell[[[\tilde{\pi}]_{F,1},\ldots,[\tilde{\pi}]_{F,n}]]$ où $h = H/m$.

Démonstration : Le module de Tate de F est un A-module libre puisque F est un A-module formel ; or on sait que ce module de Tate est un $\mathbb{Z}_p$-module libre de rang H ; on en déduit que m divise H.

De plus, π^e et p ont même valuation et comme la multiplication $[p]_F$ par p est une isogénie de degré p^H, $[\pi]_F$ est une isogénie de degré $p^{H/e} = q^h$.

DEFINITION I.5. On dit alors que h est la hauteur de F en tant que A-module formel.

Désormais, "la hauteur d'un A-module formel" désignera sa hauteur en tant que A-module formel.

Nous allons maintenant étudier quelques propriétés du logarithme d'un A-module formel défini sur B.

PROPOSITION I.2. Soit f le logarithme du A-module formel F. Alors :

(i) $f(\pi X) \equiv 0 \quad (\pi)$

(ii) $f^{-1}(\pi X) \equiv 0 \quad (\pi)$.

Démonstration :

(i) $f(\pi X) \equiv 0 \quad (\pi, \deg 2)$; supposons donc que $f(\pi X) \equiv 0 \quad (\pi, \deg r)$; alors

$$\pi^{r-1} f(X) \equiv \pi^{r-1} f^{(r)}(X) \qquad (\deg(r+1), \pi)$$

où $f^{(r)}$ désigne la composante homogène de degré r de f. Composons cette congruence avec $[\pi]_F(X) = f^{-1}\pi f(X)$; nous obtenons

$$\begin{aligned} \pi^{r-1} f([\pi]_F(X)) &\equiv \pi^{r-1} f^{(r)}([\pi]_F(X)) \\ &\equiv \pi^{r-1} f^{(r)}(\pi X) \qquad (\pi, \deg(r+1)) \\ &\equiv \pi^{2r-1} f^{(r)}(X) \end{aligned}$$

d'autre part

$$\begin{aligned} \pi^{r-1} f([\pi]_F(X)) &= \pi^{r} f(X) \\ &\equiv \pi^{r} f^{(r)}(X) \quad (\deg r+1, \pi) \end{aligned}$$

donc

$$\pi^{r} f^{(r)}(X) \equiv 0 \quad (\deg r+1, \pi) ,$$

ce qui montre par récurrence que $f(\pi X) \equiv 0 \ (\pi)$.

(ii) Posons $g = f^{-1}$. Nous pouvons de même supposer que

$$g(\pi X) \equiv 0 \quad (\pi, \deg r) .$$

Soit

$$g(\pi X) \equiv \pi^{r} g^{(r)}(X) \qquad (\deg r+1, \pi) .$$

Composons de même avec $[\pi]_F$:

$$g(\pi^2 X) \equiv \pi^{r+1} g^{(r)}(X) \quad (\deg r+1, \pi)$$

soit

$$\pi^{2r} g^{(r)}(X) \equiv \pi^{r+1} g^{(r)}(X) \quad (\pi)$$

ce qui montre que $\pi^{r} g^{(r)}$ est à coefficients entiers. Mais

$$\begin{aligned} f \circ g(\pi X) &\equiv f(\pi^{r} g^{(r)}(X)) \quad (\deg r+1, \pi) \\ &\equiv 0 \end{aligned}$$

donc $\pi^{r} g(X) \equiv 0 \quad (\deg(r+1), \pi)$, ce qui achève de montrer par récurrence que $g(\pi X) \equiv 0 \ (\pi)$.

COROLLAIRE. Soit f le logarithme du A-module formel F et α et β des systèmes de n séries formelles à coefficients dans B. Alors

$$f(\alpha+\pi\beta) \equiv f(\alpha) \quad (\pi)$$

et

$$f^{-1}(\alpha+\pi\beta) \equiv f^{-1}(\alpha) \quad (\pi) \quad .$$

En effet

$$F(\alpha+\pi\beta, i_F(\alpha)) \equiv 0 \quad (\pi)$$

donc

$$f(F(\alpha+\pi\beta, i_F(\alpha))) = f(\alpha+\pi\beta) - f(\alpha) \equiv 0 \quad (\pi) \quad .$$

Nous pouvons également préciser dans le cas d'un A-module formel un résultat de Lazard.

PROPOSITION I.3. Soient F et G deux A-modules formels de dimension n définis sur B tels que $F \equiv G$ (deg r) ; alors

$$F(X,Y) \equiv G(X,Y) + \Delta(X,Y) \quad (\deg r+1)$$

où $\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y)$ pour un système Γ de polynômes homogènes de degré r définis sur B si r n'est pas une puissance de q, et

$$\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y) + DB_{q^i}(X,Y)$$

si $r = q^i$ où $D \in M_n(L)$ est telle que $\pi D \in M_n(B)$ et où

$$B_{q^i}(X,Y) = (B_{q^i}(x_1,y_1);\ldots;B_{q^i}(x_n,y_n))$$

si $B_s(X,Y) = (X+Y)^s - X^s - Y^s$.

Démonstration : Lazard a montré dans le cas des groupes formels que

$$F(X,Y) \equiv G(X,Y) + \Delta(X,Y) \quad (\deg r+1)$$

où $\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y)$ si r n'est pas une puissance de p et $\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y) + DB_{p^i}(X,Y)$ si r est une puissance p^i de p, et D est une matrice de $M_n(L)$ telle que $pD \in M_n(B)$.

Nous n'avons donc qu'à examiner le cas où r est une puissance de p. Posons alors $D = (\alpha_{ij})$ et définissons un système de n séries formelles $s = (s_1,\ldots,s_n)$ par

$$s_i(X) = -\Gamma_i(X) - \sum_{j=1}^{n} \alpha_{ij} X_j^r \quad .$$

Alors $\Phi(X) = X + s(X)$ définit un isomorphisme modulo degré $(r+1)$ de F dans G et par conséquent pour tout $a \in A$

$$\Phi \circ [a]_F \equiv [a]_G \circ \Phi \quad (\deg\ r+1)$$

soit

$$[a]_F(X) - [a]_G(X) \equiv as(X) - s(aX) \quad (\deg\ r+1)$$

donc

$$as(X) - s(aX) \in B[[X]]_o^n \quad .$$

Soit

$$a \sum_{j=1}^{n} \alpha_{ij} X_j^r - \sum_{j=1}^{n} \alpha_{ij} a^r X_j^r \in B[[X]]_o$$

pour tout $i = 1, \ldots, n$.

Donc $\alpha_{ij} a(1-a^{r-1}) \in B$ pour tout couple (i,j) . Cette relation étant vraie pour tout $a \in A$, elle montre que $D \in M_n(B)$ si r n'est pas une puissance de q ; si r est une puissance de q , pour $a = \pi$, on trouve que $\pi D \in M_n(B)$.

II - MODULES ASSOCIES AUX A-MODULES FORMELS.

On suppose désormais l'extension L/K non ramifiée ; les valuations considérées sont normalisées par $v(\pi) = 1$ (soit $v(p) = e$) . On désigne par C le complété de la clôture algébrique $\overline{L}$ de L , par $\mathfrak{M}_C$ son idéal maximal, par $\mathfrak{g}$ le groupe de Galois de $\overline{L}$ sur L . On définit :

$$\mathfrak{M}_r = \{\alpha \in C \mid v(\alpha) \geq r\} \quad \text{si} \quad r \in \mathbb{R}$$

et en particulier

$$\mathfrak{M} = \mathfrak{M}_1 \quad .$$

On note $L\{t\}$ l'ensemble des séries formelles convergeant pour tout $\alpha \in \mathfrak{M}_C^n$ si $t = (t_1, \ldots, t_n)$ est un système de n indéterminées.

Si F est un A-module formel de dimension n défini sur B , on munit $\mathfrak{M}_C^n$ d'une structure de A-module en posant :

$$\alpha \underset{F}{+} \beta = F(\alpha,\beta) \quad \text{si} \quad \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathfrak{M}_C^n$$
$$\beta = (\beta_1,\ldots,\beta_n) \in \mathfrak{M}_C^n$$

$$a.\alpha = [a]_F(\alpha) \quad \text{si} \quad a \in A \ .$$

Comme F est défini sur B, $\mathfrak{M}_C^n$ a une structure de $A[\mathcal{G}]$-module ; on le notera $F(\mathfrak{M}_C)$. On considérera aussi les $A[\mathcal{G}]$-modules

$$W = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_p, F(\mathfrak{M}_C))$$
$$= \{\underline{\alpha} = (\alpha_0,\ldots,\alpha_k,\ldots) \mid \begin{array}{l} \alpha_k \in \mathfrak{M}_C^n \\ [p]_F(\alpha_{k+1}) = \alpha_k \text{ pour tout } k \end{array}\} \ .$$

$$T = \{\underline{\alpha} \in W \mid \alpha_0 = 0\} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_p/\mathbb{Z}_p, F(\mathfrak{M}_C)) \ .$$

On a alors la suite exacte de $A[\mathcal{G}]$-modules :

$$0 \to T \to W \to F(\mathfrak{M}_C) \to 0 \ .$$

Soit η un $A[\mathcal{G}]$-homomorphisme de W dans C ; l'image de T par η est contenue dans un $\mathfrak{M}_r$, et on peut donc factoriser η en $\underline{\eta}$: $F(\mathfrak{M}_C) \to C/\mathfrak{M}_r$.

DEFINITION II.1. Un $A[\mathcal{G}]$-homomorphisme η de W dans C est dit analytique s'il existe une série formelle $\varphi(t) \in L\{t\}$ $(= L\{t_1,\ldots,t_n\})$ et un réel r tels que :

$$\eta(\underline{\alpha}) \equiv \varphi(\alpha_0) \quad (\mathfrak{M}_r)$$

pour tout $\underline{\alpha} = (\alpha_0,\ldots) \in W$.

On note $\mathrm{Hom}_a(W,C)$ le L-espace vectoriel des $A[\mathcal{G}]$-homomorphismes analytiques de W dans C .

On appelle $M(F)$ l'ensemble des $\eta \in \mathrm{Hom}_a(W,C)$ tels qu'il existe $\varphi \in L\{t\}$ telle que $\eta(\underline{\alpha})$ soit congru à $\varphi(\alpha_0)$ modulo $\mathfrak{M}$ pour tout $\underline{\alpha} = (\alpha_0,\ldots) \in W$; $M(F)$ est un sous-B-module de $\mathrm{Hom}_a(W,C)$ et il est clair que $\mathrm{Hom}_a(W,C) = M(F) \otimes_B L$.

Soit $S(F)$ l'ensemble des séries formelles $\varphi \in L\{t_1,\ldots,t_n\}$ telles

que $\varphi(F(X,Y)) \equiv \varphi(X) + \varphi(Y)$ $(\mathfrak{M})$ et $\varphi([a]_F(X)) \equiv a\varphi(X)$ $(\mathfrak{M})$ pour tout $a \in A$.

Nous nous proposons de construire un homomorphisme surjectif de $S(F)$ sur $M(F)$. Remarquons d'abord que si $\eta \in M(F)$, il existe une série $\varphi(t) \in L\{t\}$ telle que $\eta(\underline{\alpha}) \equiv \varphi(\alpha_o)$ $(\mathfrak{M})$ pour tout $\underline{\alpha} = (\alpha_o, \ldots) \in W$. Du fait que η soit un A-homomorphisme, on déduit que :

$$\varphi(F(\alpha,\beta)) \equiv \varphi(\alpha) + \varphi(\beta) \quad (\mathfrak{M}) \quad \text{pour tout } \alpha \text{ et tout } \beta \in \mathfrak{M}_c^n$$

$$\varphi([a]_F(\alpha)) \equiv a\varphi(\alpha) \quad (\mathfrak{M}) \quad \text{pour tout } \alpha \in \mathfrak{M}_c^n$$

et il est alors facile de voir que $\varphi \in S(F)$. La suite $p^n\varphi(\alpha_n)$ est alors convergente pour $\underline{\alpha} \in W$ et $\eta(\underline{\alpha})$ en est la limite.

Soit donc $\varphi \in S(F)$ et $\underline{\alpha} = (\alpha_o, \ldots) \in W$; la suite $p^n\varphi(\alpha_n)$ converge dans C , car

$$\varphi(\alpha_n) = \varphi([p]_F(\alpha_{n+1}))$$

$$\equiv p\varphi(\alpha_{n+1}) \quad (\mathfrak{M})$$

donc

$$p^n\varphi(\alpha_n) \equiv p^{n+1}\varphi(\alpha_{n+1}) \quad (\mathfrak{M}^{1+ne}) \ .$$

On peut donc poser $\eta(\underline{\alpha}) = \lim_{n\to\infty} p^n\varphi(\alpha_n)$ et on vérifie alors que η est un $A[g]$-homomorphisme analytique de W dans C .

Nous avons ainsi défini un homomorphisme de $S(F)$ dans $M(F)$ et d'après la remarque précédente, cet homomorphisme est surjectif. Son noyau contient évidemment $\pi B[[t_1, \ldots, t_n]]$ et on voit facilement que c'est exactement $\pi B[[t_1, \ldots, t_n]]$. Nous avons donc établi un isomorphisme entre $S(F)/\pi B[[t]]$ et $M(F)$.

On note S_r l'ensemble des séries formelles à r variables à coefficients dans $L/\pi B$; il s'identifie à

$$L[[t_1, \ldots, t_r]]/\pi B[[t_1, \ldots, t_r]]$$

et a une structure naturelle de $B[[t_1, \ldots, t_r]]$-module.

On notera S_r^o le sous $B[[t_1, \ldots, t_r]]$-module de S_r constitué des

séries φ telles que $\frac{\partial\varphi}{\partial t_i} \in \ell[[t_1,\ldots,t_r]]$ pour $1 \leq i \leq r$. $M(F)$ est un sous-B-module de S_n et nous en étudierons le sous-B-module $M^o(F) = M(F) \cap S_n^o$.

Comme l'extension L/K est non ramifiée, il existe un automorphisme de Frobenius σ , qui est l'unique K-automorphisme de L tel que $\sigma(b) \equiv b^q \ (\pi)$ pour tout $b \in B$.

On désigne par $E = B_\sigma[[T]]$ l'anneau des séries formelles non commutatives à une variable à coefficients dans B où $Tb = \sigma(b)T$ pour $b \in B$. On munit alors $L[[X]]_o^m$ d'une structure de E-module à gauche en posant

$$[T * (\varphi_1,\ldots,\varphi_m)](x_1,\ldots,x_r) = (\varphi_1^\sigma(x_1^q,\ldots,x_r^q),\ldots,\varphi_m^\sigma(x_1^q,\ldots,x_r^q))$$

où φ^σ désigne la série formelle obtenue en appliquant σ aux coefficients de φ . Cette structure induit une structure de E-module à gauche sur S_r^m et $(S_r^o)^m$ en est un sous E-module.

De même, si $X = (x_1,\ldots,x_n)$ est un système de n variables, si $f \in L[[X]]_o^m$ et $u(T) \in M_{\ell,m}(E)$, on peut définir

$$u(T) * f \in L[[X]]_o^\ell$$

et on voit que si $v(T) \in M_{k,\ell}(E)$

$$(v(T)u(T)) * f = v(T) * (u(T)*f) .$$

Nous allons établir quelques lemmes en vue d'étudier la structure de $M^o(F)$:

LEMME II.1. Soit $\varphi \in M(F)$. Alors $\varphi \in M^o(F)$ si et seulement si $\frac{\partial\varphi}{\partial X_i}(0) \in \ell$ pour tout $i = 1,\ldots,n$.

Démonstration : En dérivant par rapport à Y la relation dans S_n

$$\varphi(F(X,Y)) = \varphi(X) + \varphi(Y)$$

et en y faisant $Y = 0$, on obtient la relation :

$$(\frac{\partial\varphi}{\partial x_1}(X),\ldots,\frac{\partial\varphi}{\partial x_n}(X))(\frac{\partial F_i}{\partial Y_j}(X,0)) = (\frac{\partial\varphi}{\partial Y_1}(0),\ldots,\frac{\partial\varphi}{\partial Y_n}(0))$$

Or :

$$\left(\frac{\partial F_i}{\partial Y_j}(X,0)\right) \in M_n(B[[X]]_o)$$

et

$$\left(\frac{\partial F_i}{\partial Y_j}(0,0)\right) = I_n$$

par conséquent $\left(\frac{\partial F_i}{\partial Y_j}(X,0)\right)$ est inversible et donc

$$\left(\frac{\partial \varphi}{\partial x_1}(X),\ldots,\frac{\partial \varphi}{\partial x_n}(X)\right) = \left(\frac{\partial \varphi}{\partial x_1}(0),\ldots,\frac{\partial \varphi}{\partial x_n}(0)\right)\left(\frac{\partial F_i}{\partial Y_j}(X,0)\right)^{-1}$$

On en déduit le lemme, et le corollaire :

COROLLAIRE. $M(F) \otimes_B L = M^o(F) \otimes_B L = \mathrm{Hom}_a(W,C)$.

LEMME II.2. Soit $\varphi_r(X)$ un polynôme homogène de degré r en les n variables $(x_1,\ldots,x_n)$ à coefficients dans L , vérifiant

$$\varphi_r(X+Y) \equiv \varphi_r(X) + \varphi_r(Y) \quad (\pi) .$$

Alors, si r n'est pas une puissance de p , $\varphi_r(X) \equiv 0$ (π) et si r est une puissance de p , il existe $c_1,\ldots,c_n \in \pi^{1-e}B$ tels que

$$\varphi_r(X) \equiv \sum_{i=1}^{n} c_i x_i^r \quad (\pi) .$$

Démonstration : voir Honda [7, lemme 3.2]. Nous pouvons maintenant donner la structure de $M^o(F)$:

PROPOSITION II.1. $M^o(F)$ est un sous-E-module de S_n^o , engendré sur E par les réductions $\bar{f}_1,\ldots,\bar{f}_n$ à S_n^o des composantes du logarithme de F ; de plus il ne dépend que de la structure de A-module formel de la réduction $\tilde{F}$ de F à ℓ .

En tant que B-module, il est libre de rang h . On a $\pi M^o(F) \subset T_* M^o(F)$, et le quotient $M^o(F)/T_* M^o(F)$ est un espace vectoriel de dimension n sur ℓ .

Démonstration : Il est d'abord clair que $\overline{f}_1,\ldots,\overline{f}_n$ appartiennent à $M^o(F)$. De plus :

$$\begin{aligned}(T^\nu{}_*f_i)(F(X,Y)) &= f_i^{\sigma^\nu}((F(X,Y))^{q^\nu}) \\ &\equiv f_i^{\sigma^\nu}(F^{\sigma^\nu}(X^{q^\nu},Y^{q^\nu})) \quad (\pi) \quad \text{(d'après la proposition I.2)} \\ &\equiv f_i^{\sigma^\nu}(X^{q^\nu}) + f_i^{\sigma^\nu}(Y^{q^\nu}) \quad (\pi) \\ &= (T^\nu{}_*f_i)(X) + (T^\nu{}_*f_i) \quad (Y)\end{aligned}$$

ce qui montre que $T^\nu{}_*\overline{f}_i \in M^o(F)$ pour tout entier ν et $i = 1,\ldots,n$.

Soit $\varphi \in M^o(F)$ et r le plus petit entier tel que φ ne soit pas congru à zéro modulo degré $(r+1)$; en désignant par φ_r la composante homogène de degré r de φ , on voit que

$$\varphi_r(X+Y) = \varphi_r(X) + \varphi_r(Y)$$

et le lemme II.2 montre alors que r doit être une puissance de p ; mais φ_r doit aussi vérifier :

$$\varphi_r([a]_F(X)) \equiv a\varphi_r(X) \quad (\deg\ r+1)$$

soit $(a^r-a)\varphi_r(X) = 0$ pour tout $a \in A$. Cette dernière relation implique que r est une puissance q^ν de q , et on voit que $\varphi_r(X) \in \ell[X]$. Il existe donc $c_1,\ldots,c_n \in \ell$ tels que

$$\varphi(X) - \sum_{i=1}^{n} c_i x_i^{q^\nu} \equiv 0 \quad (\deg\ (r+1))$$

soit

$$\varphi - \sum_{i=1}^{n} c_i T^\nu{}_*\overline{f}_i \equiv 0 \quad (\deg\ r+1) \quad .$$

On peut donc construire de proche en proche des séries $v_1(T),\ldots,v_n(T) \in E$ telles que :

$$\varphi = \sum_{i=1}^{n} v_i(T) * \overline{f}_i \quad .$$

On en déduit que $M^o(F)$ est un E-module engendré par $(\overline{f}_i)$ $(i=1,\ldots,n)$; de plus ce module ne dépend que de la réduction $\tilde{F}$ de F ; on sait en effet que $f(\alpha+_\pi\beta) \equiv f(\alpha)$ pour toutes séries α et β dans $B[[X]]_o^n$; par conséquent tout $\varphi \in M^o(F)$ vérifie également $\varphi(\alpha+_\pi\beta) = \varphi(\alpha)$. En consi-

dérant la relation

$$\pi\varphi(X) = \varphi([\pi]_F(X))$$

vraie pour tout $\varphi \in M^o(F)$, et en se souvenant que $[\pi]_F$ est une isogénie de degré q^h , on voit que $M^o(F)$ est un B-module libre de rang h .

Les dernières assertions de la proposition sont claires. En particulier, les éléments $\pi\overline{f}_i$ de $M^o(F)$ s'écrivent :

$$\pi\overline{f}_i = -\sum_{j=1}^{n} v_{i,j}(T) * \overline{f}_j$$

pour des séries $u_{i,j}(T) \in E$, sans terme constant c'est-à-dire que :

$$\sum_{j=1}^{n} (\pi\,\delta_{i,j} + v_{i,j}(T)) * \overline{f}_j = 0 \quad \text{pour} \quad i = 1,\ldots,n .$$

Il existe donc une matrice $u(T) = (\pi\delta_{i,j}+v_{i,j}(T)) \in M_n(E)$ telle que

$$u(T)*f \equiv 0 \quad (\pi)$$

et

$$u(T) \equiv \pi I_n \quad (\deg\ 1) .$$

Une matrice $u(T)$ telle que $u(T) \equiv \pi I_n$ (deg 1) sera dite <u>spéciale</u> et on dira que $\varphi \in L[[X]]_o^n$ est de type u si

$$u*f \equiv 0 \quad (\pi) .$$

Nous venons donc de montrer que pour tout A-module formel F de dimension n défini sur B , il existe une matrice spéciale $u(T) \in M_n(E)$ telle que le logarithme de F soit de type u . La réciproque est vraie :

PROPOSITION II.2. <u>Soit</u> $u(T)$ <u>un élément spécial de</u> $M_n(E)$, <u>et</u> $f \in L[[X]]_o^n$ <u>de type</u> u ; <u>alors</u> $F(X,Y) = f^{-1}(f(X)+f(Y))$ <u>est un</u> A-<u>module formel défini sur</u> B .

La démonstration est fondée sur le lemme suivant (voir Honda [7, lemme 2.3]).

LEMME II.3. *Soit* $f \in L[[X]]_o^n$ *de type* u ; $v \in M_{m,n}(E)$, *et* $\psi \in L[[X']]_o^n$ *où* X' *désigne un ensemble fini de variables. Si les coefficients des termes de degré* $\leq r-1$ *des composantes de* ψ *appartiennent à* B

$$v_*(f \circ \psi) \equiv (v_* f) \circ \psi \quad (\deg r+1, \pi) .$$

A l'aide de ce lemme, Honda montre que F est un groupe formel défini sur B dont f est le logarithme. Il est facile de voir que c'est aussi un A-module formel ; on considère pour cela

$$h(X) = (u^{-1}\pi)_* i \quad \text{où} \quad i(X) = X$$

et le groupe formel $H(X,Y) = h^{-1}(h(X)+h(Y))$. On suppose que les coefficients des termes de degré $\leq r-1$ des $[a]_H(X) = h^{-1}ah(X)$ sont entiers pour tout $a \in A$; alors :

$$\begin{aligned} \pi\,[a]_H(X) &= (u_* h)(h^{-1}ah)(X) \\ &\equiv u * (hh^{-1}ah)(X) \quad (\pi, \deg r+1) \\ &= u * (ah)(X) \\ &= a(u*h)(X) \quad \text{car} \quad a \in A \\ &\equiv 0 \quad (\pi) \end{aligned}$$

ce qui montre par récurrence que $[a]_H(X)$ est à coefficients entiers. On en déduit que $[a]_F$, qui s'écrit

$$[a]_F = \varphi^{-1} \circ [a]_H \circ \varphi \quad \text{pour un} \quad \varphi \in B[[X]]_o^n$$

est aussi à coefficients entiers pour tout $a \in A$, c'est-à-dire que F est un A-module formel défini sur B .

Nous allons maintenant utiliser ces résultats pour classer, d'abord les A-modules formels définis sur le corps résiduel ℓ , puis les A-modules formels définis sur B .

III - CLASSIFICATION DES A-MODULES FORMELS DEFINIS SUR ℓ .

Nous avons vu que le module $M^O(F)$ ne dépend que de la structure de A-module formel de la réduction de F à ℓ . Nous nous proposons de démontrer que ces modules permettent de classifier les A-modules formels définis sur ℓ .

Plus précisément, soit $\mathcal{M}$ la catégorie des E-modules à gauche M vérifiant les propriétés

(i) M est B-libre de rang fini

(ii) $\pi M \subset T*M$

(iii) $M/T*M$ est un espace vectoriel de dimension finie sur ℓ .

Les morphismes de $\mathcal{M}$ sont par définition les morphismes E-linéaires.

PROPOSITION III.1. *Le foncteur* $\tilde{F} \longmapsto M^O(\tilde{F})$ *définit une anti-équivalence de la catégorie des A-modules formels de hauteur finie définis sur* ℓ *sur la catégorie* $\mathcal{M}$. *A un A-module formel de hauteur* h *et de dimension* n , *il fait correspondre un module* M *de rang* h *sur* B , *tel que* $M/T*M$ *soit de dimension* n *sur* ℓ .

Nous allons d'abord montrer que tout A-module formel de dimension n défini sur ℓ provient par réduction d'un A-module formel de dimension n défini sur B .

LEMME III.1. *Soient* F_o *et* G_o *deux A-modules formels de dimension* n *définis sur* ℓ *tels que*

$$F_o(X,Y) \equiv G_o(X,Y) \quad (\deg\ r)$$

et

$$[a]_{F_o}(X) \equiv [a]_{G_o}(X) \quad (\deg\ r)$$

pour tout $a \in A$.

Alors

$$F_o(X,Y) \equiv G_o(X,Y) + \Delta(X,Y) \quad (\deg\ r+1)$$

$$[a]_{F_o}(X) \equiv [a]_{G_o}(X) + \Gamma_a(X) \quad (\deg\ r+1)$$

où $\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y)$ pour un système Γ de polynômes homogènes de degré r si r n'est pas une puissance de q, ou si r est une puissance de q et $e > 1$;

$$\Delta(X,Y) = \Gamma(X+Y) - \Gamma(X) - \Gamma(Y) + DC_{q^i}(X,Y) \quad \text{si} \quad e = 1$$

et $r = q^i$, pour une matrice $D \in M_n(\ell)$. (On rappelle que $C_{q^i}(X,Y) = \frac{1}{p} B_{q^i}(X,Y)$).

Γ_a est un système de polynômes homogènes de degré r qui vérifient les relations

$$\Gamma_{ab}(X) = \tilde{a}\Gamma_b(X) + \tilde{b}^r\Gamma_a(X) \quad \text{pour tous} \quad a \text{ et } b \in A .$$

Démonstration : Les premières relations se démontrent par des méthodes analogues à celles de la proposition I.3. La dernière relation provient de ce que les plongements de A dans $\mathrm{End}_\ell(F_o)$ et $\mathrm{End}_\ell(G_o)$ sont des homomorphismes d'anneaux ; en effet :

$$\begin{aligned}
[a]_{F_o} \circ [b]_{F_o}(X) &\equiv [a]_{G_o} \circ [b]_{G_o}(X) + \Gamma_a(\tilde{b}X) + \hat{a}\Gamma_b(X) \quad (\deg r+1) \\
&\equiv [ab]_{G_o}(X) + \Gamma_a(\tilde{b}X) + \tilde{a}\Gamma_b(X) \quad (\deg r+1) \\
&\equiv [ab]_{F_o}(X) - \Gamma_{ab}(X) + \tilde{a}\Gamma_b(X) + \tilde{b}^r\Gamma_a(X) \quad (\deg r+1)
\end{aligned}$$

d'où

$$\Gamma_{ab}(X) = \tilde{a}\Gamma_b(X) + \tilde{b}^r\Gamma_a(X) .$$

En particulier, si r est une puissance de q cette relation devient :

$$\Gamma_{ab}(X) = \tilde{a}\Gamma_b(X) + \tilde{b}\Gamma_a(X)$$

et on en déduit que $\Gamma_{a^p}(X) = pa^{p-1}\Gamma_a(X) = 0$, et donc que $\Gamma_a = 0$ si $a \in A^{*p}$; de même

$$\Gamma_{a\pi} = \tilde{a}\Gamma_\pi .$$

On montre d'autre part que

$$\Gamma_a(X+Y) - \Gamma_a(X) - \Gamma_a(Y) = (\tilde{a}^r - \tilde{a})(\Gamma(X+Y) - \Gamma(X) - \Gamma(Y))$$

et

$$(\tilde{a}^r - \tilde{a})\Gamma_b = (\tilde{b}^r - \tilde{b})\Gamma_a \quad \text{pour tous } a \text{ et } b \in A .$$

Ces diverses relations permettent de relever tout A-module formel F_o défini

sur ℓ par récurrence. Supposons en effet trouvés $\varphi_r(X) \in B[[X]]_o^n$ avec $\varphi_r(X) \equiv X$ (deg 2) et $u_r(T) \in M_n(E)$ avec $u_r(T) \equiv \pi I_n$ (deg 1) tels que si l'on pose

$$(\pi u_r^{-1}(T) * i) \circ \varphi_r = g_r$$

et

$$G_r(X,Y) = g_r^{-1}(g_r(X) + g_r(Y))$$

on ait :

$$\tilde{G}_r(X,Y) \equiv F_o(X,Y) \quad (\deg r)$$
$$[\tilde{a}]_{G_r}(X) \equiv [a]_{F_o}(X) \quad (\deg r) \text{ pour tout } a \in A .$$

Alors :

- Si r n'est pas une puissance de q

$$\tilde{G}_r(X,Y) \equiv F_o(X,Y) + \Gamma(X+Y) - \Gamma(X) - \Gamma(Y) \quad (\deg r+1)$$
$$[\tilde{a}]_{G_r}(X) \equiv [a]_{F_o}(X) + \Gamma_a(X) \quad (\deg r+1)$$

on construit alors

$$\varphi_{r+1}(X) = \varphi_r(X) - \Gamma^a(X)$$

(où $\Gamma^a(X)$ désigne un relèvement de $\dfrac{\Gamma_a(X)}{\tilde{a}^r - \tilde{a}}$; ce dernier terme ne dépend pas de $a \in A$ pourvu que $\tilde{a}^r \neq \tilde{a}$ et il est possible de trouver un tel $a \in A$ puisque r n'est pas une puissance de q). On vérifie alors que si $g_{r+1} = (\pi u_r^{-1}(T) * i) \circ \varphi_{r+1}$ le A-module formel

$$G_{r+1}(X,Y) = g_{r+1}^{-1}(g_{r+1}(X) + g_{r+1}(Y))$$

satisfait

$$\tilde{G}_{r+1}(X,Y) \equiv F_o(X,Y) \quad (\deg r+1)$$

et

$$[\tilde{a}]_{G_{r+1}}(X) \equiv [a]_{F_o}(X) \quad (\deg r+1) \text{ pour tout } a \in A .$$

- Si r est une puissance q^ν de q et si $e > 1$

$$\tilde{G}_r(X,Y) \equiv F_o(X,Y) + \Gamma(X+Y) - \Gamma(X) - \Gamma(Y) \quad (\deg r+1)$$
$$[\tilde{a}]_{G_r}(X) \equiv [a]_{F_o}(X) + \Gamma_a(X) \quad (\deg r+1)$$

où $\Gamma_a = 0$ si $a \in A^{*p}$ et $\Gamma_a(X+Y) = \Gamma_a(X) + \Gamma_a(Y)$ pour tout $a \in A$; de cette dernière relation on déduit que $\Gamma_a(X)$ est de la forme $M_a(X^{q^\nu})$

pour une matrice $M_a \in M_n(\ell)$ (voir lemme II.2) ; on construit alors

$$u_{r+1}(T) = u_r(T) + M^{\pi}T^{\nu}$$

où M^{π} est un relèvement de $\frac{M_{\pi}}{\pi}$.

$$\varphi_{r+1}(X) = \varphi_r(X) + \Gamma'(X) \quad (\Gamma' \text{ relèvement de } \Gamma)$$

$$g_{r+1}(X) = (\pi u_{r+1}^{-1}(T) * i) \circ \varphi_{r+1}(X)$$

et le A-module formel $G_{r+1}(X,Y) = g_{r+1}^{-1}(g_{r+1}(X) + g_{r+1}(Y))$ satisfait

$$\tilde{G}_{r+1}(X,Y) \equiv F_o(X,Y) \qquad (\deg\ r+1)$$

$$[\tilde{a}]_{G_{r+1}}(X) \equiv [a]_{F_o}(X) \qquad (\deg\ r+1) \quad \text{pour tout } a \in A .$$

- Si r est une puissance q^{ν} de q et si $e = 1$

$$\tilde{G}_r(X,Y) \equiv F_o(X,Y) + \Gamma_o(X+Y) - \Gamma_o(X) - \Gamma_o(Y) + D_o C_{q^i}(X,Y)$$

et on prend

$$u_{r+1}(T) = u_r(T) - DT^{\nu}$$

$$\varphi_{r+1}(X) = \varphi_r(X) + \Gamma(X)$$

pour un relèvement D de D_o et un relèvement Γ de Γ_o .

Nous avons donc montré que tout A-module formel F_o défini sur ℓ provient par réduction d'un A-module formel défini sur B . Or si F est un A-module formel défini sur B , $M^o(\tilde{F})$ est un objet de $\mathcal{M}$, et l'application qui à $\tilde{F}$ associe $M^o(\tilde{F})$ est fonctorielle contravariante ; en effet soient F et G deux A-modules formels définis sur B et ψ un ℓ-homomorphisme de $\tilde{F}$ dans $\tilde{G}$; alors si $\varphi \in M^o(G)$

$$\varphi \circ \psi(F(X,Y)) = \varphi(G(\psi(X), \psi(Y))$$

$$= \varphi \circ \psi(X) + \varphi \circ \psi(Y)$$

et

$$\varphi \circ \psi([a]_F(X)) = \varphi([a]_G \circ \psi(X))$$

$$= a\varphi \circ \psi(X)$$

ce qui montre que $\varphi \circ \psi \in M^o(F)$.

Nous définirons donc :

$$M^{O}(\psi)\ (\varphi) = \varphi \circ \psi \quad .$$

Il reste à montrer que tout objet de $\mathcal{M}$ est isomorphe à un $M^{O}(\tilde{F})$ et que M^{O} est un foncteur pleinement fidèle.

Soit donc M un objet de $\mathcal{M}$ et soient $\lambda_1, \ldots, \lambda_n \in M$ dont les images dans $M/T*M$ engendrent $M/T*M$; on sait que $\pi\lambda_i \in T*M$ (d'après (iii)) et on peut donc construire une matrice $u(T) \in M_n(E)$ telle que $u(T)*\lambda = 0$ où $\lambda = {}^{t}(\lambda_1, \ldots, \lambda_n)$ et $u(T) \equiv \pi I_n$ (deg 1) . Par conséquent, si $f \in L[[X]]^{n}_{o}$ est de type u , et si on forme $F(X,Y) = f^{-1}(f(X)+f(Y))$, $\tilde{F}$ est un A-module formel défini sur ℓ , de dimension n et de hauteur h , et le module associé $M^{O}(\tilde{F})$ est isomorphe à M .

Montrons que M^{O} définit une bijection de $\mathrm{Hom}_{\ell,A}(\tilde{F},\tilde{G})$ sur $\mathrm{Hom}_{E}(M^{O}(\tilde{G}), M^{O}(\tilde{F}))$; soient ψ et $\psi' \in \mathrm{Hom}_{\ell,A}(\tilde{F},\tilde{G})$ tels que $\varphi \circ \psi = \varphi \circ \psi'$ pour tout $\varphi \in M^{O}(G)$; cette relation est en particulier vraie pour les réductions $\bar{g}_i$ des composantes du logarithme g de G et donc $\bar{g} \circ \psi = \bar{g} \circ \psi'$, mais la proposition I.2 permet alors de conclure que $\psi = \psi'$.

Soit maintenant θ un E-homomorphisme de $M^{O}(G)$ dans $M^{O}(F)$; considérons $\psi = g^{-1} \circ h$, où h désigne un relèvement quelconque à B de $\theta(\bar{g})$; la proposition I.2 montre que $\tilde{\psi}$ ne dépend pas du relèvement choisi, et comme $M^{O}(G)$ est engendré sur E par $\bar{g}_1, \ldots, \bar{g}_n$, θ est en fait égal à $M^{O}(\psi)$, ce qui montre que l'application de $\mathrm{Hom}_{\ell,A}(\tilde{F},\tilde{G})$ dans $\mathrm{Hom}_{E}(M^{O}(\tilde{G}) , M^{O}(\tilde{F}))$ est surjective, et achève la démonstration de la proposition III.1.

IV - CLASSIFICATION DES A-MODULES FORMELS DEFINIS SUR B .

A un A-module formel F défini sur B , nous avons associé un E-module $M^{O}(F)$. Nous pouvons aussi considérer le "module des loga-

rithmes" de F , c'est-à-dire l'ensemble des $\varphi \in L[[X]]_o$ vérifiant

$$\varphi(F(X,Y)) = \varphi(X) + \varphi(Y)$$

et

$$\frac{\partial \varphi}{\partial X_i}(X) \in B[[X]] \quad \text{pour} \quad i = 1,\ldots,n \ ;$$

on notera $L^o(F)$ son image dans S^o_n ; $L^o(F)$ est un sous-B-module de $M^o(F)$. En fait $L^o(F)$ est le sous-B-module de $M^o(F)$ engendré par les réductions $\overline{f}_1,\ldots,\overline{f}_n$ des composantes du logarithme de F , et on a les relations :

$$L^o(F) \cap T_* M^o(F) = \pi L^o(F)$$

$$L^o(F)/\pi L^o(F) = M^o(F)/T_* M^o(F) \ .$$

Nous sommes ainsi amenés à considérer la catégorie $\mathcal{H}$ dont les objets sont les couples (L,M) où M est un objet de $\mathcal{M}$ et L un sous-B-module de M vérifiant

(iv) $L \cap T_* M = \pi L$

(v) $L/\pi L = M/T_* M$

les morphismes de (L,M) dans (L',M') étant les applications E-linéaires de M dans M' envoyant L dans L' .

On définit alors le foncteur contravariant LM de la catégorie des A-modules formels définis sur B dans la catégorie $\mathcal{H}$ comme étant le foncteur qui à F associe le couple $LM(F) = (L^o(F), M^o(F))$

PROPOSITION IV.1. *Soient F et G deux A-modules formels définis sur B ;*

(i) *l'homomorphisme de $\mathrm{Hom}_B(F,G)$ dans $\mathrm{Hom}_{\mathcal{H}}(LM(G),LM(F))$ est surjectif.*

(ii) *étant donné un objet (L,M) de $\mathcal{H}$,*

il existe un A-module formel F défini sur B , unique à isomorphisme près, tel que $LM(F)$ soit isomorphe à (L,M) .

Démonstration : (i) Soit θ un morphisme de $LM(G)$ dans $LM(F)$. Alors $\theta(\overline{g}_i) \in L^o(F)$ pour toute composante g_i du logarithme g de G ; soit donc $h_i \in B[[X]]_o$ un relèvement de $\theta(\overline{g}_i)$ tel que

$$h_i(F(X,Y)) = h_i(X) + h_i(Y)$$

et h la famille $(h_1,\ldots,h_m)$ (m est la dimension de G). Alors $\varphi = g^{-1} \circ h$ est un B-homomorphisme de F dans G et θ est l'image de φ dans $\mathrm{Hom}_{\mathfrak{H}}(LM(G),LM(F))$.

(ii) Soient $(\lambda_1,\ldots,\lambda_n)$ des générateurs de $L/\pi L$; on construit une matrice $u(T) \in M_n(E)$ telle que

$$u(T) * \lambda = 0 \quad \text{où} \quad \lambda = {}^t(\lambda_1,\ldots,\lambda_n)$$

et

$$u(T) \equiv \pi I_n \ (\deg 1) .$$

Alors si $f \in L[[X]]_o^n$ est de type u et si on forme

$$F(X,Y) = f^{-1}(f(X)+f(Y)) ,$$

F est un A-module formel défini sur B, de dimension n et de hauteur h, dont le système associé est isomorphe à (L,M). L'unicité est immédiate.

Remarque : Nous avons ainsi classifié les A-modules formels définis sur B à isomorphisme près ; pour obtenir une classification à isomorphisme strict près, il faudrait rajouter à la donnée du couple $(L^o(F),M^o(F))$ celle d'un système de générateurs de $L^o(F)$ sur B. Ce dernier résultat n'est en fait que la transcription d'un résultat de Honda.

PROPOSITION. *Les classes à isomorphisme strict près de A-modules formels de dimension n définis sur B sont en bijection avec les classes de conjugaison à gauche d'éléments spéciaux de $M_n(E)$.*

En particulier, si F est de dimension un, il existe un théorème de préparation de Weierstrass dans E :

PROPOSITION. *Soit $u(T) = \pi + \sum_{i=1}^{\infty} c_i T^i \in E$ et soit h le plus petit entier tel que $c_h \in B^*$; il existe alors une unité $t(T)$ de E telle que*

$$t(T)u(T) = \pi + \sum_{i=1}^{h} b_i T^i \quad \text{où} \quad b_1,\ldots,b_{h-1} \in \pi B \quad \text{et} \quad b_h \in B^* \ .$$

Par conséquent, en dimension un, l'ensemble des classes d'isomorphisme strict de A-modules formels définis sur B est en bijection avec les éléments de E de la forme :

$$u(T) = \pi + b_1 T + \ldots + b_h T^h$$

où $b_1,\ldots,b_{h-1} \in \pi B$ et $b_h \in B^*$.

APPLICATION : Equation caractéristique de l'endomorphisme de Frobenius.

Soit F un A-module formel de dimension n défini sur A . Il existe une matrice spéciale $u(T) \in M_n(E)$ telle que le logarithme f de F soit de type u . Remarquons que $E = A[[T]]$ est ici un anneau commutatif. Soit $w \in M_n(E)$ telle que

$$uw = wu = (\text{dét } u) I_n \ .$$

Alors

$$\begin{aligned} (\text{dét } u)f &= (wu)_* f \\ &= w_*(u_* f) \\ &\equiv 0 \qquad (\pi) \ . \end{aligned}$$

Soit $$\text{dét } u = \pi^n + \sum_{\nu=1}^{\infty} c_\nu T^\nu \qquad (c_\nu \in A) \ .$$

Alors

$$\begin{aligned} (\text{dét } u)_* f(X) &= \pi^n f(X) + \sum_{\nu=1}^{\infty} c_\nu f(X^{q^\nu}) \\ &= f([\pi^n]_F(X)) + \sum_{\nu=1}^{\infty} f([c_\nu]_F(X^{q^\nu})) \\ &= f([\pi^n]_F(X) \underset{F}{+} \sum_{\nu=1}^{\infty}{}^{F} \ [c_\nu]_F(X^{q^\nu})) \end{aligned}$$

(où $\underset{F}{+}$ et $\sum^F$ désignent les sommes pour la loi de groupe formel F) ; d'après la proposition I.2, on en déduit que

$$[\pi^n]_F(X) \underset{F}{+} \sum_{\nu=1}^{\infty}{}^{F} \ [c_\nu]_F(X^{q^\nu}) \equiv 0 \quad (\pi)$$

ce qui signifie que l'endomorphisme de Frobenius ξ du A-module formel $\tilde{F}$ vérifie l'équation

$$\pi^n + \sum_{\nu=1}^{\infty} c_\nu \xi^\nu = 0$$

(on a ici identifié A à son image dans $\mathrm{End}_A(F)$) .

En particulier, si F est de dimension un, le Frobenius ξ vérifie l'équation

$$\pi + \sum_{i=1}^{h} b_i \xi^i = 0$$

où $u(T) = \pi + \sum_{i=1}^{h} b_i T^i$ est l'annulateur du logarithme de F dans $M^o(F)$, et on voit donc que le A-module formel F est déterminé à isomorphisme strict près par le polynôme caractéristique du Frobenius de $\tilde{F}$ (ce résultat avait été démontré par Hill [6] pour $A = \mathbb{Z}_p$ et généralisé par Cox [1]). Soit K_o le corps des fractions de l'anneau $W(k)$ des vecteurs de Witt sur k et $\Gamma = \mathrm{Gal}(K/K_o)$; on peut considérer

$$v(T) = \overline{\prod_{\gamma \in \Gamma}} u^\gamma(T) .$$

Comme $A[T]$ est commutatif, $v(T)$ est un polynôme d'Eisenstein de degré he de $W(k)[T]$. On peut donc lui associer une classe de $W(k)$-modules formels définis sur $W(k)$; en interprétant $u(T)$ et $v(T)$ comme polynômes caractéristiques d'endomorphismes de Frobenius, on voit que si G est un $W(k)$-module formel défini sur $W(k)$ associé à $v(T)$, $\tilde{G}$ et $\tilde{F}$ sont isomorphes sur k .

-:-:-:-

BIBLIOGRAPHIE

[1] - COX L. - "Formal A-modules". Bull. Amer. Math. Soc. 79, 1973.

[2] - COX L. - "Formal A-modules over p-adic integer rings". A paraître.

[3] - FONTAINE J.M. - "Sur la construction du module de Dieudonné d'un groupe formel". C.R. Acad. Sc. Paris t. 280 1975, pp. 1273-1276.

[4] - FONTAINE J.M. - "Groupes p-divisibles sur les vecteurs de Witt". C.R. Acad. Sc. Paris t. 280 , 1975, pp.1353-1356.

[5] - FROHLICH A. - "Formal groups". Lecture Notes in Math. 74. Springer Verlag, New-York, 1968.

[6] - HILL W. - "Formal groups and Zeta functions of Elliptic Curves". Inv. Math. 12, 1971, pp. 321-336.

[7] - HONDA T. - "On the theory of Commutative Formal Groups". Jour. Math. Soc. Japan 22, 1970, pp. 213-246.

[8] - LUBIN J. - "Formal A-modules defined over A ". Instituto Nazionale di Alta Matematica, Symposia Matematica 3, 1970, pp. 241-245.

-:-:-:-