UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE
Laboratoire de Mathématiques Pures associé au C.N.R.S.

Jean-Marc Fontaine
INSTITUT FOURIER
MATHÉMATIQUES PURES
Boîte Postale 116
38402 SAINT-MARTIN-D'HÈRES

Téléphone (76) 87-45-61 à 64

Nouveau n° Tél. (76) 54 61 45

le 3 novembre 1977

Cher Serre,

Je pense être en mesure de donner une réponse complète (je n'ai pas tout vérifié) au problème que tu m'avais posé en juillet dernier sur la possibilité de décrire en termes de module de Dieudonné + filtration les invariants (ou "covariants") par Galois d'une opération tensorielle sur le module de Tate d'un groupe p-divisible (à ceci près que, mes constructions étant contravariantes, ce qu'on va obtenir sera le $\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Galois}]}(-,\mathbb{Z}_p)$ où le $\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Galois}]}(-,\mathbb{Z}_p(\chi$

Cette réponse est un sous-produit d'une conjecture plus générale, avec morceaux de démonstrations (qui suffisent pour ton problème), qui dit qu'il y a anti-équivalence entre une catégorie assez vaste de "représentations p-adiques" et une certaine catégorie de "modules filtrés".

Ce que j'affirme dans la suite est, en principe, démontré (mais tout n'a pas été suffisamment soigneusement vérifié ; si les démonstrations sont souvent très techniques, les idées sont simples et tout ne devrait pas se casser la gueule).

Pour simplifier, et parce que c'est le seul cas que j'ai vraiment regardé, je suppose $e = 1$ et $p \neq 2$. Il n'est pas douteux que cela se généralise à $e < p-1$, et aussi à e et p quelconques à condition de remplacer les $\mathbb{Z}_p$-modules par des vectoriels sur $\mathbb{Q}_p$.

<u>Notations</u> : Soit k un corps parfait de car. $p \neq 0,2$. Soit $A = W(k)$, $K = \mathrm{Frac}(A)$, $\overline{K}$ une clôture algébrique de K, $\mathcal{G} = \mathrm{Gal}(\overline{K}/K)$

C le complété de $\overline{K}$, A_C les entiers de C, $\underline{m}_C$ l'idéal maximal de A_C. Soit $A[F]$ l'anneau (non commutatif si $k \neq \mathbb{F}_p$) habituel (dans cette histoire, il n'y a plus de V ce qui fera plaisir aux amateurs de cristaux).

§ 1. - Les résultats. (il ft dem. à isogénie près)

Je note $\underline{Rp}_A$ la catégorie des "représentations p-adiques pas néc. de dimension finie", i.e. la catégorie des $\mathbb{Z}_p$-modules séparés et complets pour la topologie p-adique sur lesquels $\mathcal{G}$ opère linéairement et continûment, et $\underline{Rp}_A^f$ la sous-catégorie pleine formée des objets dont le $\mathbb{Z}_p$-module sous-jacent est libre de rang fini (c'est celle qui m'intéresse vraiment, rassure-toi).

Je note $\underline{MF}_A$ la catégorie dont les objets sont les suites $\mathcal{N}$

$$(\mathcal{N}) \quad N = N_0 \supset N_1 \supset \dots \supset N_i \supset N_{i+1} \supset \dots$$

où N est un $A[F]$-module à gauche, libre de rang fini sur A, et les N_i forment une suite décroissante de sous-A-modules, les N_i/N_{i+1} étant sans torsion et $N_i = 0$ pour i assez grand.

Les flèches, bien sûr, sont les applications $A[F]$-linéaires compatibles avec la filtration.

C'est une catégorie additive qui a des sommes directes, mais aussi des produits tensoriels : si $\mathcal{N}' = (N' = N'_0 \supset N'_1 \supset \dots)$ et $\mathcal{N}'' = (N'' = N''_0 \supset N''_1 \supset \dots)$, alors $\mathcal{N} = \mathcal{N}' \otimes \mathcal{N}'' = (N = N_0 \supset N_1 \supset \dots)$ avec

$N = N' \otimes_A N''$ (l'action de F est définie par $F(a \otimes b) = Fa \otimes Fb$),

$$N_i = \sum_{i'+i''=i} N'_{i'} \otimes_A N''_{i''}, \text{ pour tout } i.$$

On peut alors construire un foncteur contravariant additif $\underline{N}_A$ de $\underline{Rp}_A^f$ dans $\underline{MF}_A$ et un foncteur contravariant additif $\underline{T}_A$ de $\underline{MF}_A$ dans $\underline{Rp}_A$ (je vais les décrire au § 2) qui sont "adjoints à gauche", i.e. si T est un objet de $\underline{Rp}_A^f$ et si $\mathcal{N}$ est un objet de $\underline{MF}_A$, les deux groupes $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,\underline{T}_A(\mathcal{N}))$ et $\mathrm{Hom}_{\underline{MF}_A}(\mathcal{N},\underline{N}_A(T))$ s'identifient canoniquement et fonctoriellement en T et $\mathcal{N}$ (même si $\underline{T}_A(N)$ n'est pas de rang fini sur $\mathbb{Z}_p$).

Ces deux foncteurs ont plein de bonnes propriétés.

Proposition 1. Soit T un objet de $\underline{Rp}_A^f$ et soit $\mathcal{N} = (N = N_o \supset N_1 \supset \dots) = \underline{N}_A(T)$.

i) Il existe une application A-linéaire injective de N_o/N_1 dans $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,A_C)$;

ii) pour tout $i \geqslant 1$, il existe une application A-linéaire injective de N_i/N_{i+1} dans $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,\underline{m}_C(\chi^i))$ (où χ est le caractère fondamental).

Corollaire. - On a $rg_A N \leq rg_{\mathbb{Z}_p} T$.

Ceci grâce à Tate !

Définition : Je dis qu'un objet T de $\underline{Rp}_A^f$ est admissible si $rg_A N = rg_{\mathbb{Z}_p} T$, et je note $\underline{Rp}_A^a$ la sous-catégorie pleine de $\underline{Rp}_A^f$ formée des modules admissibles.

Compte-tenu de Tate, si T est admissible cela implique que T est du type Hodge-Tate avec, en outre, $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,C(\chi^i)) = 0$ si $i < 0$. Il n'y a aucune raison pour que cette condition soit suffisante (toutefois, si T est un objet de $\underline{Rp}_A^f$ et si i , supposé $\geqslant 0$, est le plus grand entier tel que $n_i = \mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,C(\chi^i)) \neq 0$, je sais que $rg_A N_i = n_i$).

La catégorie $\underline{Rp}_A^a$ est certainement "assez grosse" :

Proposition 2.

i) Le module de Tate d'un groupe p-divisible sur A est admissible ;

ii) si T' et T'' sont admissibles, $T' \oplus T''$ l'est et

$\underline{N}_A(T'\oplus T'')$ s'identifie à $\underline{N}_A(T')\oplus\underline{N}_A(T'')$ (c'est évident !) ;

iii) si T' et T'' sont admissibles, $T'\otimes_{\mathbb{Z}_p} T''$ l'est et $\underline{N}_A(T'\otimes T'')$ s'identifie à $\underline{N}_A(T')\otimes\underline{N}_A(T'')$;

iv) si $0 \longrightarrow T' \longrightarrow T \longrightarrow T'' \longrightarrow 0$ est une suite exacte d'objets de Mp_A^f et si T est admissible, T' et T'' le sont ;

v) la restriction de $\underline{N}_A$ à Rp_A^a est exacte.

Conjecture. - La restriction de $\underline{N}_A$ à Rp_A^a est pleinement fidèle et la restriction de $\underline{T}_A$ à son image essentielle est un quasi-inverse.

Remarque. Il est vraisemblable que l'image essentielle en question est formée des $\mathcal{N} = (N = N_0 \supset N_1 \supset \dots)$ qui ont la propriété suivante : si $N^{(i)} = \{ a \in N \mid Fa \in p^i N \}$, alors $N_i \subset N^{(i)}$ et $N_i/pN_i \simeq (N^{(i)}+pN)/pN$.

Proposition 3. - La restriction de $\underline{N}_A$ à Rp_A^d , sous-catégorie pleine de Rp_A^a dont les objets sont les modules de Tate des groupes p-divisibles sur A , est pleinement fidèle et la restriction de $\underline{T}_A$ à son image essentielle (que je sais décrire explicitement) est un quasi-inverse.

La démonstration de cette dernière proposition consiste, bien sûr, à comparer ces foncteurs avec mes constructions pour les groupes p-divisibles : il y a un petit canular technique : si je note $(L,M) = \underline{LM}_A(G)$ le couple formé du module de Dieudonné M et du sous-machin L associés au groupe p-divisible G dans ma construction, je note $M^{(-1)}$ le $A[F,V]$-module déduit de M par l'extension des scalaires σ^{-1} (où σ est le Frobenius absolu) ; si j'identifie de manière évidente, le $\mathbb{Z}_p[F,V]$-module sous-jacent à $M^{(-1)}$ à M , V définit une application $A[F,V]$-linéaire de M dans $M^{(-1)}$ et je note encore L l'image de L dans $M^{(-1)}$ par cette application

Alors, $\underline{N}_A(T_p(G)) = (N = N_o \supset N_1 \supset \ldots)$ avec $N = M^{(-1)}$ (en oubliant l'action de V), $N_1 = L$, $N_i = 0$ pour $i \geq 2$.

Remarque. - Le couple $(L,M^{(-1)})$ est ce que donne la construction, via les cristaux, à la Grothendieck-Messing).

Il n'y a pas de difficulté à montrer que le quasi-inverse constr dans mon "astérisque" s'identifie à la restriction de $\underline{T}_A$ à la catégorie qu'il faut.

Corollaire. - Soit T un objet de Mp_A^f et soit G un groupe p-divisible sur A . Alors $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(T,T_p(G))$ s'identifie canoniquement et fonctoriellement en T et G , à $\mathrm{Hom}_{\underline{MF}_A}(\underline{N}_A(T_p(G)),\underline{N}_A(T))$.

En effet $T_p(G)$ s'identifie à $\underline{T}_A\underline{N}_A(T_p(G))$ d'après la proposition précédente, et cela résulte alors de l'adjonction.

Cela entraîne en particulier les résultats que tu me demandais (à la variance près, ce qui n'est pas gênant grâce à la dualité). Par exemple, si $G_1,G_2,\ldots,G_n$ sont des groupes p-divisibles sur A , si $T_r = T_p(G_r)$, $M_r = M^{(-1)}(G_r)$, L_r = sous-machin habituel , alors

i) le groupe $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(\otimes G_r,\mathbb{Z}_p)$ s'identifie à celui des $\alpha \in \otimes M_r$ tels que $F\alpha = \alpha$;

ii) le groupe $\mathrm{Hom}_{\mathbb{Z}_p[\eta]}(\otimes G_r,\mathbb{Z}_p(\chi))$ s'identifie au sous-groupe de $\otimes M_r$ formé des α qui vérifient

$$\begin{cases} F\alpha = p\alpha \\ \alpha \text{ est dans l'image de } \sum M_1\otimes\ldots\otimes M_{r-1}\otimes L_r\otimes M_{r+1}\otimes\ldots\otimes M \end{cases}$$

§ 2. - Construction des foncteurs.

Elle se fait grâce à la construction d'un monstre dualisant qui est formé de bivecteurs de Witt d'un style un peu particulier (ce

n'est d'ailleurs que le week-end dernier que je me suis rendu comp
que le monstre pouvait se représenter à l'aide de bivecteurs ; ça
le rend beaucoup plus maniable (et plus facile à décrire) et ça m'a permis de démontrer la
proposition 3 qui donne à la théorie sa consistance). Je vais te l
décrire sans chercher à t'expliquer d'où il sort.

Soit, pour tout entier $n \geqslant 1$, $R_n = A_C/pA_C$ et soit $R = \varprojlim$ l'application de R_{n+1} dans R_n étant l'élévation à la puissance p-ième. On voit aussi que tout élément de R peut s'écrire sous la forme $x = (x^{(n)})_{n \in \mathbb{Z}}$, avec les $x^{(n)} \in R$ vérifiant $(x^{(n+1)})^p$ $x^{(n)}$, pour tout n. La multiplication se fait composante par composante et l'addition est définie par

$$x+y = z = (z^{(n)})_{n \in \mathbb{Z}}, \text{ avec } z^{(n)} = \lim_{m \to +\infty} (x^{(n+m)}+y^{(n+m)})^{p^m}.$$

En outre R est un anneau parfait de car. p, valué complet (dans la suite, je note v la valuation de C normalisée par $v(p) = 1$ et je note encore v la valuation de R définie par $v(x) = v(x^{(o)})$).

J'ai introduit dans mon "astérisque" (chap.V, §1), les bivecteurs de Witt $BW(R)$ à coefficients dans R :

Je te rappelle que $BW^u(R)$ (les bivecteurs "unipotents") est une limite inductive de vecteurs de Witt $W(R)$ indexée par les entiers naturels, l'application de transition est le décalage, et qu'un élément de $BW^u(R)$ s'écrit

$$a = (\ldots, a_{-n}, \ldots, a_o, \ldots, a_m, \ldots) = (a_n)_{n \in \mathbb{Z}},$$ où les $a_n \in R$ et sont presque tous nuls.

Les bivecteurs $BW^u(R)$ forment, de manière naturelle, un $A[F,V]$-module et aussi un $A[\eta]$-module. On peut munir $BW^u(R)$ d'une topologie telle que tout cela soit continu et le séparé complété pour cette topologie est $BW(R)$ et hérite des structures de $A[F,V]$-module et $A[\eta]$-module. Un élément de $BW(R)$ s'écrit sous la forme $a = (a_n)_{n \in \mathbb{Z}}$, avec les $a_n \in R$ et vérifiant

(φ) il existe $\varepsilon > 0$ et un entier n_o tel que $v(a_n) \geq \varepsilon$, pour $n < n_o$.

Du point de vue qui nous intéresse $BW(R)$ a toutes les bonnes propriétés sauf une : celle d'être un anneau (et il en a une qui est trop bonne : il y a une action de V).

Mais $BW^u(R)$ est, lui, un anneau : du fait que R est réduit, $BW^u(R)$ s'identifie à $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} W(R)$.

L'idée va consister à prendre un sous-anneau convenable de $BW^u(R)$, à le munir d'une topologie non moins convenable, et à le compléter.

Soit $BW^{u,a}(R)$ le sous-ensemble de $BW^u(R)$ formé des $a = (a_n)_{n\in\mathbb{Z}}$ qui vérifient $v(a_{-n}) > p^{-n+1}n/(p-1)$, pour $n > 0$ (les a_{-n} en question sont presque tous nuls puisque l'on est dans $BW^u(R)$).

On démontre sans difficulté que c'est un sous-$A[F]$-module de $BW^u(R)$ (mais non stable par V), un sous-$A[\varphi]$-module, et aussi un sous-anneau. On munit $BW^{u,a}(R)$ de la topologie la plus bête, i.e. la topologie du produit direct, avec la topologie définie par la valuation sur chaque composante. Il se trouve (ce n'est pas évident) que tout est continu pour cette topologie, y compris la multiplication. Je note $BW^a(R) = BW^a$ le séparé complété : c'est donc un anneau, un $A[F]$-module et un $A[\varphi]$-module ; en tant qu'ensemble,

$$BW^a = \{ (a_n)_{n\in\mathbb{Z}} \mid a_n \in R \text{ et } v(a_{-n}) > p^{-n+1}n/(p-1) \text{ si } n > 0 \}$$

(notez que la valuation des a_{-n} a le droit de tendre vers 0 lorsque $n \mapsto +\infty$, ce qui n'est pas du tout le cas dans les bivecteurs habituels).

Enfin, je définis une application $\theta_o : BW^a \longrightarrow A_C$ en posant $\theta_o((a_n)_{n\in\mathbb{Z}}) = \sum_{n\in\mathbb{Z}} p^n a_n^{(n)}$ (la convergence pour $n \to -\infty$ ne fait pas problème : si $m > 0$, $v(p^{-m}a_{-m}^{(-m)}) = -m+p^{m}v(a_{-m}^{(o)}) = -m+p^{m}v(a_{-m})$ $> -m+pm/(p-1) = m/(p-1) \longrightarrow +\infty$. On démontre que Θ_o est $A[\gamma]$-linéaire continue, surjective.

Pour tout $i \geq 0$, je note alors BW_i^a la puissance i-ème de l'idéal noyau de Θ_o . J'ai donc en particulier une suite exacte de $A[\gamma]$-modules

$$0 \longrightarrow BW_1^a \longrightarrow BW_o^a \xrightarrow{\Theta_o} A_C \longrightarrow 0$$

et je sais définir, pour tout entier $i \geq 1$, une application Θ_i qui induit une suite exacte de $A[\gamma]$-modules

$$0 \longrightarrow BW_{i+1}^a \longrightarrow BW_i^a \xrightarrow{\Theta_i} \underline{m}_C(\chi^i) \longrightarrow 0 .$$

Enfin, on a, avec des notations évidentes, $\Theta_i(x)\Theta_j(y) = \Theta_{i+j}(xy)$ si $x \in BW_i^a$, $y \in BW_j^a$.

C'est clair maintenant ce que vont être mes foncteurs :

- si T est un $\mathbb{Z}_p[\gamma]$-module , $\underline{N}_A(T) = (N = N_o \supset N_1 \supset \dots)$, avec

$$N = \mathrm{Hom}_{\mathbb{Z}_p[\gamma]}(T, BW^a) ,$$
$$N_i = \mathrm{Hom}_{\mathbb{Z}_p[\gamma]}(T, BW_i^a) .$$

- si $\mathcal{N} = (N = N_o \supset N_1 \supset \dots)$ est un module filtré,

$$\underline{T}_A(\mathcal{N}) = \{ u \in \mathrm{Hom}_{A[F]}(N, BW^a) \mid u(N_i) \subset BW_i^a , \text{ pour tout } i \} .$$

Si tu crois à l'existence de BW^a , avec les propriétés que j'ai indiquées ci-dessus, et si tu connais les résultats de Astérisque, chap.V, § 1 , les résultats annoncés dans le § 1 sont alors à peu près complètement triviaux.

+

J'envoie une copie de cette lettre aux deux Raynaud et à Berthelot qui devraient être intéressés. On pourra peut-être reparler de tout cela au moment de Bourbaki (je n'aurai sans doute guère avancé d'ici là, mais j'aimerais bien que tu m'expliques comment ce genre de choses te permet de décrire l'enveloppe algébrique de l'image de Galois). Nous n'avons pas encore de projet précis, mais cela s'oriente vers un séjour court avec Isabelle et sans les jumelles (lesquelles, ainsi d'ailleurs que la dite Isabelle, ne font que des conneries, au grand désespoir de Laurence qui a plus que marre de l'emmerdante, de l'emmerdeuse et de l'emmerderesse).

Bien à toi

[illegible]

P.S. Je n'ai pas de nouvelles du manuscrit d'Astérisque qui est parti à Paris, il y a environ une quinzaine de jours. J'y ai déjà découvert un lapsus dont la correction ne demanderait qu'un peu de snow-pake s'il est encore temps : dans l'énoncé de la proposition 1.5 du chapitre V , il faut lire " <u>tels que</u> $x_n \in \mathrm{Res}^+_{A'}(\underline{S})$ " et non "<u>tels que</u> $x_n^{(o)} \in \mathrm{Res}^+_{A'}(\underline{S})$ " .

En outre, les résultats que je viens de te raconter m'auraient permis, si j'avais encore le manuscrit sous la main, d'améliorer les remarques qui sont à la fin du § 1 du chapitre V :

- dans la remarque 1 du n°1.8 , j'aurais aimé remplacer " On devrait pouvoir montrer" par "on peut montrer" , à condition de remplacer aussi " de dimension $\leq n_o+n_1$ " (resp. " de dimension $\leq n_1$ ") par " de dimension $\leq \sum_{i=0}^{\infty} n_i$ " (resp. " de dimension $\leq \sum_{i=1}^{\infty} n_i$ ") ;
- dans la remarque 2 du même n°1.8, j'aurais pu alors supprimer les conditionnels ; autrement dit remplacer " Des considérations sur les dimensions ... obtiendrait ainsi un procédé " par

" Le résultat précédent et des considérations sur les dimensions impliquent alors que ce sont des isomorphismes. On obtient ainsi un procédé " .

Mais il sera sans doute trop tard ! De toutes façons, il y a tellement d'autres choses que j'aurais aimé changer, bien sûr ! Cela pourra au moins te servir à améliorer ton exemplaire quand tu le recevras !