SCHEMAS EN GROUPES ET CORPS DES NORMES
Article non publié daté de 1998

Christophe Breuil
C.N.R.S.
Université Paris-Sud

1. Introduction

Dans cette note, on désigne par k un corps parfait de caractéristique $p > 0$, $W = W(k)$ l'anneau des vecteurs de Witt, K une extension finie totalement ramifiée de degré e de $Frac(W)$, $\mathcal{O}_K$ son anneau d'entiers et π une uniformisante fixée de $\mathcal{O}_K$. On note π_n ($n \in \mathbf{N}^*$) des éléments d'une clôture algébrique de K tels que $\pi_1^p = \pi$ et $\pi_n^p = \pi_{n-1}$ si $n \geq 2$, $K_n = K(\pi_n)$, $\mathcal{O}_{K_n}$ les entiers de K_n et $\mathcal{O}_{K_\infty} = \cup_{n\in\mathbf{N}}\mathcal{O}_{K_n}$.

On sait classer tous les p-groupes finis et plats (et les groupes p-divisibles) sur $\mathcal{O}_K$ lorsque $p \geq 3$ ([Fo1], [Con] pour $e \leq p-2$, [Br1] pour tout e). Lorsque $p = 2$, on ne dispose que d'une classification partielle et dans le cas $e = 1$ seulement ([FL],9). A l'origine du présent travail est la volonté d'essayer de combler le "trou" $p = 2$ en recherchant une autre classification, au moins conjecturale, valable pour tout p et tout e (et nécessairement nouvelle même pour $p \geq 3$). Dans ce qui suit, nous proposons des conjectures précises (section 2) et donnons quelques éléments très partiels en leur faveur (section 3). L'idée principale est de chercher une classification en termes de modules sur un anneau de Cohen de l'anneau des normes de $\mathcal{O}_{K_\infty}$ (c.f. [Wi], [Br2]), plutôt qu'en termes de modules filtrés à puissances divisées comme dans [Br1]. Ces nouveaux modules sont en quelque sorte en amont des anciens: ils sont plus simples, plus concrets (en particulier il n'y a plus de puissances divisées) mais aussi, semble-t-il, plus "difficiles" à obtenir. Dans un contexte un peu différent, l'idée de considérer des modules de même type, mais pour classifier des représentations p-adiques, a été introduite et utilisée pour la première fois par Fontaine ([Fo2], voir aussi [Wa1], [Wa2], [Col], [He]).

2. Les conjectures

On énonce les conjectures, puis un lien avec les modules étudiés dans [Br1]. Ce lien devrait, bien sûr, commuter aux foncteurs "schéma en groupes". On ne fait pas d'hypothèses sur p. Il est explicitement signalé lorsqu'un résultat est valable pour $p \geq 3$ seulement.

2.1. On désigne par $\underline{\pi}$ une indéterminée, $\mathfrak{S} = W[[\underline{\pi}]]$ l'anneau des séries formelles et $\mathfrak{S}_n = W_n[[\underline{\pi}]]$ ($n \in \mathbf{N}^*$). On munit $\mathfrak{S}$ et $\mathfrak{S}_n$ d'un Frobenius W-semi-linéaire en posant $\phi(\underline{\pi}^i) = \underline{\pi}^{pi}$. On note $E(\underline{\pi}) \in \mathfrak{S}$ le polynôme d'Eisenstein de π. On définit trois catégories de $\mathfrak{S}$-modules avec Frobenius:

- $(ModLi/\mathfrak{S})$ ("Li" pour "Libre") est la catégorie des $\mathfrak{S}$-modules libres de type fini $\mathfrak{M}$ munis d'une application $\mathfrak{S}$-semi-linéaire injective $\phi : \mathfrak{M} \to \mathfrak{M}$ telle que, si $\mathfrak{M}^\phi = \mathfrak{S} \otimes_{(\phi),\mathfrak{S}} \mathfrak{M}$, $\mathfrak{M}/(Id \otimes \phi)(\mathfrak{M}^\phi)$ est annulé par $E(\underline{\pi})$.
- $(ModFI/\mathfrak{S})$ ("FI" pour "Facteurs Invariants") est la catégorie des $\mathfrak{S}$-modules $\mathfrak{M}$ de la forme $\oplus_{i\in I}\mathfrak{S}_i$ (I ensemble fini d'entiers) munis d'une application $\mathfrak{S}$-semi-linéaire injective $\phi : \mathfrak{M} \to \mathfrak{M}$ telle que, si $\mathfrak{M}^\phi = \mathfrak{S} \otimes_{(\phi),\mathfrak{S}} \mathfrak{M}$, $\mathfrak{M}/(Id \otimes \phi)(\mathfrak{M}^\phi)$ est annulé par $E(\underline{\pi})$.
- $(Mod/\mathfrak{S}_1)$ est la sous-catégorie pleine de $(ModFI/\mathfrak{S})$ formée des objets tué par p. Il s'agit donc des $\mathfrak{S}_1$-modules libres de type fini $\mathfrak{M}$ tels que $\mathfrak{M}/(Id \otimes \phi)(\mathfrak{M}^\phi)$ est annulé par $\underline{\pi}^e =$ l'image de $E(\underline{\pi})$.

Les flèches des catégories sont les applications $\mathfrak{S}$-linéaires qui commutent à ϕ. On dit qu'un diagramme $0 \to \mathfrak{M}' \to \mathfrak{M} \to \mathfrak{M}'' \to 0$ dans $(ModFI/\mathfrak{S})$ est une suite exacte courte si c'est une suite exacte courte de $\mathfrak{S}$-modules.

Conjecture 2.1.1. *Pour tout p, la catégorie $(ModFI/\mathfrak{S})$ est naturellement anti-équivalente à la catégorie des schémas en groupes finis et plats G sur $\mathcal{O}_K$ annulés par une puissance de p tels que $Ker(p^n_G)$ est encore plat (sur $\mathcal{O}_K$) pour tout n. Cette équivalence préserve (en les renversant) les suites exactes courtes.*

Conjecture 2.1.2. *Pour tout p, la catégorie $(ModLi/\mathfrak{S})$ est naturellement anti-équivalente à la catégorie des groupes p-divisibles sur $\mathcal{O}_K$.*

De (2.1.1), on devrait donc aussi déduire:

Conjecture 2.1.3. *Pour tout p, la catégorie $(Mod/\mathfrak{S}_1)$ est naturellement anti-équivalente à la catégorie des schémas en groupes finis et plats sur $\mathcal{O}_K$ annulés par p. Cette équivalence préserve les suites exactes courtes.*

Remarque 2.1.4. On peut peut-être proposer une conjecture pour *tous* les p-groupes finis et plats, dans le style de ([Br1],4.2.1.6). Par souci de simplicité, nous avons préféré nous limiter aux cas précédents, suffisants pour beaucoup d'applications.

Exemple 2.1.5. Soit $pc_0 \in W$ le coefficient constant de $E(\underline{\pi})$, le module $\mathfrak{S}_n e_1$ avec $\phi(e_1) = c_0^{-1}E(\underline{\pi})e_1$ doit correspondre à μ_{p^n}. Lorsque $n = 1$, $e = p-1$ et $\mathcal{O}_K \simeq W[[\underline{\pi}]]/(\underline{\pi}^e + p)$ (par exemple $e = 1,\ p = 2$), on remarque qu'on a bien une flèche non nulle dans $(Mod/\mathfrak{S}_1)$:

$$(\mathfrak{S}_1 e_1,\ \phi(e_1) = \underline{\pi}^e e_1) \longrightarrow (\mathfrak{S}_1 e_2,\ \phi(e_2) = e_2),\ e_1 \mapsto \underline{\pi} e_2$$

qui doit correspondre à une flèche non nulle $\mathbf{Z}/p\mathbf{Z} \to \mu_p$.

2.2. On désigne par u une indéterminée, S la complétion p-adique de $W[u, \frac{u^{ie}}{i!}]_{i\in\mathbf{N}}$, $Fil^1 S$ la complétion p-adique de l'idéal engendré par $(\frac{E(u)^i}{i!})_{i\geq 1}$ et, pour $n \in \mathbf{N}^*$, $S_n = S/p^n S$ et $Fil^1 S_n = Fil^1 S/p^n Fil^1 S$. On munit S et S_n de l'unique opérateur ϕ semi-linéaire par rapport au Frobenius sur W et continu pour la topologie p-adique tel que $\phi(u) = u^p$ et $\phi(u^{ie}/i!) = u^{pie}/i!$. On a $\phi(Fil^1 S) \subset pS$ et on pose $\phi_1 = (\phi/p)|_{Fil^1 S}$. Soit $'(Mod/S)$ la catégorie des S-modules $\mathcal{M}$ munis d'un sous-S-module $Fil^1\mathcal{M}$ contenant $Fil^1 S \cdot \mathcal{M}$ et d'une flèche S-semi-linéaire $\phi_1 : Fil^1\mathcal{M} \to \mathcal{M}$ telle que pour tout $s \in Fil^1 S$ et $x \in \mathcal{M}$, $\phi_1(sx) = \frac{\phi_1(s)}{\phi_1(E(u))}\phi_1(E(u)x)$ (les flèches sont les morphismes S-linéaires qui préservent $Fil^1\mathcal{M}$ et commutent à ϕ_1). On définit les catégories suivantes de S-modules filtrés avec Frobenius (c.f. [Br1] pour $p \geq 3$):

- $(ModLi/S)$ ("Li" pour "Libre") est la sous-catégorie pleine de $'(Mod/S)$ formée des objets $\mathcal{M}$ qui sont des S-modules libres de type fini tels que $\mathcal{M}/Fil^1\mathcal{M}$ est sans p-torsion et $\phi_1(Fil^1\mathcal{M})$ engendre $\mathcal{M}$ sur S. On appelle aussi ces objets des S-modules fortement divisibles.
- $(ModFI/S)$ ("FI" pour "Facteurs Invariants") est la sous-catégorie pleine de $'(Mod/S)$ formée des objets $\mathcal{M}$ dont le S-module est de la forme $\oplus_{i\in I} S_i$ (I ensemble fini d'entiers) et tels que $\phi_1(Fil^1\mathcal{M})$ engendre $\mathcal{M}$ sur S.
- (Mod/S_1) est la sous-catégorie pleine de $(ModFI/S)$ formée des objets tués par p. Il s'agit donc des S_1-modules libres de type fini $\mathcal{M}$ tels que $\phi_1(Fil^1\mathcal{M})$ engendre $\mathcal{M}$ sur S_1.

On dit qu'un diagramme $0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$ dans $'(Mod/S)$ est une suite exacte courte si les deux suites de S-modules $0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$ et $0 \to Fil^1\mathcal{M}' \to Fil^1\mathcal{M} \to$

$Fil^1\mathcal{M}'' \to 0$ sont exactes.

On va définir des foncteurs $(ModLi/\mathfrak{S}) \to (ModLi/S)$ et $(ModFI/\mathfrak{S}) \to (ModFI/S)$. La construction est similaire à celle de ([Br2],4).

Soit $s : \mathfrak{S} \to S$ défini par $s(\sum x_i\underline{\pi}^i) = \sum x_i u^i$ $(x_i \in W)$. A $\mathfrak{M}$, objet de $(ModFI/\mathfrak{S})$ ou $(ModLi/\mathfrak{S})$, on associe un objet $\mathcal{M}$ de $(ModFI/S)$ ou $(ModLi/S)$ de la façon suivante:

- en tant que S-module, $\mathcal{M} = S \otimes_{(\phi\circ s),\mathfrak{S}} \mathfrak{M}$. On a un "Frobenius relatif": $Id \otimes \phi : S \otimes_{(\phi\circ s),\mathfrak{S}} \mathfrak{M} \longrightarrow S \otimes_{(s),\mathfrak{S}} \mathfrak{M}$
- on pose $Fil^1\mathcal{M} = \{y \in S \otimes_{(\phi\circ s),\mathfrak{S}} \mathfrak{M} \ / \ (Id \otimes \phi)(y) \in Fil^1S \otimes_{(s),\mathfrak{S}} \mathfrak{M} \subset S \otimes_{(s),\mathfrak{S}} \mathfrak{M}\}$
- on définit $\phi_1 : Fil^1\mathcal{M} \to \mathcal{M}$ comme la composée:

$$Fil^1\mathcal{M} \stackrel{Id\otimes\phi}{\longrightarrow} Fil^1S \otimes_{(s),\mathfrak{S}} \mathfrak{M} \stackrel{\phi_1\otimes Id}{\longrightarrow} S \otimes_{(\phi\circ s),\mathfrak{S}} \mathfrak{M} \simeq \mathcal{M}.$$

Tout élément x de $\mathfrak{M}$ est tel que $E(\underline{\pi})x = \sum \sigma_i\phi(x_i)$ où $\sigma_i \in \mathfrak{S}$ et $x_i \in \mathfrak{M}$, d'où on déduit que $\sum s(\sigma_i) \otimes x_i \in Fil^1\mathcal{M}$ et $\phi_1(\sum s(\sigma_i) \otimes x_i) = (\phi_1 \otimes Id)(E(u) \otimes x) = \phi_1(E(u)) \otimes x$ ce qui montre bien que $\phi_1(Fil^1\mathcal{M})$ engendre $\mathcal{M}$ sur S puisque $\phi_1(E(u)) \in S^*$. Les autres conditions se vérifient facilement, de même que la fonctorialité.

Lemme 2.2.1. *Le foncteur $(ModFI/\mathfrak{S}) \to (ModFI/S)$ est exact.*

Preuve. — Soient $\mathfrak{M}, \mathfrak{M}'$ deux $\mathfrak{S}$-modules de la forme $\oplus\mathfrak{S}_i$ et $0 \to \mathfrak{M}' \to \mathfrak{M} \to \mathfrak{M}'' \to 0$ une suite exacte de $\mathfrak{S}$-modules, alors les suites: $0 \to S \otimes_{(\phi\circ s)} \mathfrak{M}' \to S \otimes_{(\phi\circ s)} \mathfrak{M} \to S \otimes_{(\phi\circ s)} \mathfrak{M}'' \to 0$ et $0 \to Fil^1S \otimes_{(s)} \mathfrak{M}' \to Fil^1S \otimes_{(s)} \mathfrak{M} \to Fil^1S \otimes_{(s)} \mathfrak{M}'' \to 0$ sont exactes. Cela découle du cas $p\mathfrak{M} = p\mathfrak{M}'' = 0$ et d'un dévissage à partir du diagramme commutatif:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{M}' \cap p\mathfrak{M} & \to & p\mathfrak{M} & \to & p\mathfrak{M}'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{M}' & \to & \mathfrak{M} & \to & \mathfrak{M}'' & \to & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{M}'/(\mathfrak{M}' \cap p\mathfrak{M}) & \to & \mathfrak{M}/p\mathfrak{M} & \to & \mathfrak{M}''/p\mathfrak{M}'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Soit maintenant $0 \to \mathfrak{M}' \to \mathfrak{M} \to \mathfrak{M}'' \to 0$ une suite exacte dans $(ModFI/\mathfrak{S})$, il reste à voir l'exactitude de $0 \to Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M}') \to Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M}) \to Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M}'') \to 0$. L'injectivité est triviale et l'exactitude au milieu découle de la suite exacte $0 \to Fil^1S \otimes_{(s)} \mathfrak{M}' \to Fil^1S \otimes_{(s)} \mathfrak{M} \to Fil^1S \otimes_{(s)} \mathfrak{M}'' \to 0$. Soit $x \in Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M}'')$, qu'on peut supposer de la forme $x = \sum_{i=1}^{d''} s_i \otimes e_i$ avec $s_i \in \oplus_{i=0}^{e-1} Wu^i$ et où $\mathfrak{M}'' \simeq \oplus_{i=1}^{d''} \mathfrak{S}_{n_i} e_i$ $(n_i \in \mathbf{N}^*)$. Alors, $(Id \otimes \phi)(x) = E(u) \otimes x'$ pour un $x' \in \mathfrak{M}'$. Soit $\hat{x}'$ un relevé de x' dans $\mathfrak{M}$, comme $E(\underline{\pi})(\mathfrak{M}/(Id \otimes \phi)(\mathfrak{M}^{\phi})) = 0$, il existe $\hat{x} \in Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M})$ tel que $(Id \circ \phi)(\hat{x}) = E(u) \otimes \hat{x}'$. Soit y l'image de $\hat{x}$ dans $S \otimes_{(\phi\circ s)} \mathfrak{M}''$ et $z = x - y$, on a $(Id \otimes \phi)(z) = 0$, d'où on déduit facilement, en utilisant $E(\underline{\pi})(\mathfrak{M}''/(Id \otimes \phi)(\mathfrak{M}''^{\phi})) = 0$, $E(u)z = 0$ dans $S \otimes_{(\phi\circ s)} \mathfrak{M}''$. Mais si $s \in S_n$ est tel que $E(u)s = 0$, on a forcément $s \in E(u)^{p-1}S_n \subset Fil^1S_n$, d'où $z \in Fil^1S \otimes_{(\phi\circ s)} \mathfrak{M}''$. Soit $\hat{z}$ un relevé de z dans $Fil^1S \otimes_{(\phi\circ s)} \mathfrak{M}$, alors $\hat{x} + \hat{z}$ est un relevé de x dans $Fil^1(S \otimes_{(\phi\circ s)} \mathfrak{M})$, et la flèche de droite est bien surjective. □

Compte tenu de ce qui précède et des résultats de [Br1] pour $p \geq 3$, on devrait donc avoir:

Conjecture 2.2.2. *Supposons $p \geq 3$, alors le foncteur ci-dessus induit des équivalences de catégories* $(ModLi/\mathfrak{S}) \xrightarrow{\sim} (ModLi/S)$ *et* $(ModFI/\mathfrak{S}) \xrightarrow{\sim} (ModFI/S)$.

Exemple 2.2.3. Donnons l'exemple du groupe p-divisible $(\mu_{p^n})_{n\in\mathbf{N}^*}$: on sait que l'objet correspondant de $(ModLi/S)$ est donné pour tout choix de π par $(\mathcal{M} = Se_1, Fil^1\mathcal{M} = Se_1, \phi_1(e_1) = e_1)$. Soit $\mathfrak{M} = \mathfrak{S}e_1$ avec $\phi(e_1) = c_0^{-1}E(\underline{\pi})e_1$ où $pc_0 \in W$ est le coefficient constant de $E(\underline{\pi})$. L'objet associé à $\mathfrak{M}$ par le foncteur précédent est $S\cdot 1\otimes e_1$ avec $1\otimes e_1 \in Fil^1$ et $\phi_1(1\otimes e_1) = \phi_1(c_0^{-1}E(u))\cdot 1\otimes e_1$. Mais $\phi_1(c_0^{-1}E(u)) = 1 + u^p(*) + u^{ep}/p$, donc $c = \prod_{i\in\mathbf{N}}\phi^i(\phi_1(c_0^{-1}E(u)))$ converge dans S^* et, si on note $e'_1 = c\otimes e_1$, on vérifie que $\phi_1(e'_1) = e'_1$.

Partant d'un objet $\mathcal{M}$, il ne semble pas trivial en général d'expliciter un objet $\mathfrak{M}$ dont il pourrait provenir. Le problème est de généraliser le changement de base $1\otimes e_1 \to c\otimes e_1$ de l'exemple ci-dessus.

3. Quelques résultats en faveur des conjectures

3.1.

Théorème 3.1.1. *Supposons $p \geq 3$, alors le foncteur $(Mod/\mathfrak{S}_1) \to (Mod/S_1)$ est une équivalence de catégories.*

Preuve. — A partir de ([Br1],2.2.2.1) et ([Br1],2.2.2.2), la preuve est similaire à celle de ([Br2],4.1.1). □

Par (2.2.1), on en déduit la conjecture (2.1.3) pour $p \geq 3$:

Corollaire 3.1.2. *Pour $p \geq 3$, la catégorie $(Mod/\mathfrak{S}_1)$ est naturellement anti-équivalente à la catégorie des schémas en groupes finis et plats sur $\mathcal{O}_K$ annulés par p. Cette équivalence préserve les suites exactes courtes.*

et, à tout le moins:

Corollaire 3.1.3. *Supposons $p \geq 3$, alors le foncteur $(ModFI/\mathfrak{S}) \to (ModFI/S)$ est exact et pleinement fidèle. En particulier, pour $p \geq 3$, $(ModFI/\mathfrak{S})$ est une sous-catégorie pleine de la catégorie des p-groupes sur $\mathcal{O}_K$.*

Preuve. — Tout objet de $(ModFI/\mathfrak{S})$ admet une filtration par des objets dont les gradués sont dans $(Mod/\mathfrak{S}_1)$ (prendre les puissances $p^{\text{ièmes}}$). C'est aussi vrai pour les objets de $(ModFI/S)$ ([Br1],2.2.1.3). On conclut alors par (3.1.1) et les dévissages habituels. □

3.2. Dans cette section, on explore un cas particulier de (2.1.3) où p peut être 2. On suppose $e = 1$ et, pour simplifier, $\pi = p$. On note $(p, ..., p)/W$ la catégorie des schémas en groupes finis et plats sur W annulés par p. Nous allons construire **pour tout p** un foncteur exact de $(Mod/\mathfrak{S}_1)$ dans $(p, ..., p)/W$ qui, pour $p \geq 3$, coïncidera avec le foncteur composé: $(Mod/\mathfrak{S}_1) \xrightarrow{\sim} (Mod/S_1) \xrightarrow{\sim} (p, ..., p)/W$. Le résultat est énoncé en (3.2.4.1). Bien que nous n'ayons pas réussi à le montrer, nul doute que ce foncteur est aussi une équivalence de catégories pour $p = 2$.

3.2.1. Nous donnons d'abord quelques lemmes d'algèbre linéaire.

Lemme 3.2.1.1. *Soit $\mathfrak{M}$ un objet de $(Mod/\mathfrak{S}_1)$ de rang d, il existe $d' \leq d$, une base $(e_1, ..., e_d)$ de $\mathfrak{M}$ et $\mathcal{G} \in GL_d(\mathfrak{S}_1)$ tels que:*

$$\begin{pmatrix} \phi(e_1) \\ \vdots \\ \phi(e_d) \end{pmatrix} = diag(\underbrace{\underline{\pi}, ..., \underline{\pi}}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G} \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix}.$$

Preuve. — Soit $F^1\mathfrak{M} = \{x \in \mathfrak{M} \text{ tq } \phi(x) \in \underline{\pi}\mathfrak{M}\}$, $d' = dim_k(F^1\mathfrak{M}/\underline{\pi}\mathfrak{M})$, V un supplémentaire de $F^1\mathfrak{M}/\underline{\pi}\mathfrak{M}$ dans $\mathfrak{M}/\underline{\pi}\mathfrak{M}$, $(e_1, ..., e_{d'})$ des relevés d'une base de $F^1\mathfrak{M}/\underline{\pi}\mathfrak{M}$ et $(e_{d'+1}, ..., e_d)$ des relevés d'une base de V. Soit $x \in \mathfrak{M}$, on a $\underline{\pi}x = \sum s_i\phi(e_i)$ pour des $s_i \in \mathfrak{S}_1$, donc $\sum_{i>d'} s_i\phi(e_i) \in \underline{\pi}\mathfrak{M}$ donc $s_i \in \underline{\pi}\mathfrak{S}_1$ pour $i > d'$. On en déduit $x = \sum_{i\leq d'} s_i(\phi(e_i)/\underline{\pi}) + \sum_{i>d'}(s_i/\underline{\pi})\phi(e_i)$ donc $(\frac{\phi(e_1)}{\underline{\pi}}, ..., \frac{\phi(e_{d'})}{\underline{\pi}}, \phi(e_{d'+1}), ..., \phi(e_d))$ est une base de $\mathfrak{M}$, d'où le résultat. $\square$

Définition 3.2.1.2. *On dit qu'un objet $\mathfrak{M}$ de $(Mod/\mathfrak{S}_1)$ est multiplicatif si $\phi(\mathfrak{M}) \subset \underline{\pi}\mathfrak{M}$ et qu'il est unipotent s'il n'a pas de quotient multiplicatif (dans $(Mod/\mathfrak{S}_1)$).*

Lemme 3.2.1.3. *Soit $\mathfrak{M}$ un objet de $(Mod/\mathfrak{S}_1)$, il existe une unique suite exacte $0 \to \mathfrak{M}^u \to \mathfrak{M} \to \mathfrak{M}^m \to 0$ dans $(Mod/\mathfrak{S}_1)$ telle que $\mathfrak{M}^u$ est unipotent et $\mathfrak{M}^m$ multiplicatif.*

Preuve. — Soit $\mathfrak{S}_1(1) = (\mathfrak{S}_1e_1, \phi(e_1) = -\underline{\pi}e_1)$ (c.f. 2.1.5). Pour $\mathfrak{M}$ dans $(Mod/\mathfrak{S}_1)$, on pose $\mathfrak{M}^* = Hom_{\mathfrak{S}_1}(\mathfrak{M}, \mathfrak{S}_1(1))$ et, si $f \in \mathfrak{M}^*$, on définit $\phi(f) \in \mathfrak{M}^*$ comme l'unique application $\mathfrak{S}_1$-linéaire telle que $\phi(f)(\phi(x)) = \phi(f(x))$, $\forall\, x \in \mathfrak{M}$. Cela fait de $\mathfrak{M}^*$ un objet de $(Mod/\mathfrak{S}_1)$ et on vérifie que $\mathfrak{M} \mapsto \mathfrak{M}^*$ est une dualité, i.e. $\mathfrak{M} \xrightarrow{\sim} \mathfrak{M}^{**}$. Disons qu'un objet $\mathfrak{M}$ est étale si $\phi(\mathfrak{M})$ engendre $\mathfrak{M}$ sur $\mathfrak{S}_1$. Par dualité, on voit qu'il suffit de montrer qu'il existe une unique suite exacte $0 \to \mathfrak{M}^{ét} \to \mathfrak{M} \to \mathfrak{M}^c \to 0$ dans $(Mod/\mathfrak{S}_1)$ avec $\mathfrak{M}^{ét}$ étale et $\mathfrak{M}^c$ sans sous-objet étale. Cela découle du fait que la réunion de deux sous-objets étales est encore un sous-objet étale (exercice). $\square$

Lemme 3.2.1.4. *Soit $0 \to \mathfrak{M}' \to \mathfrak{M} \to \mathfrak{M}'' \to 0$ une suite exacte dans $(Mod/\mathfrak{S}_1)$, alors elle induit des suites exactes dans $(Mod/\mathfrak{S}_1)$: $0 \to \mathfrak{M}'^u \to \mathfrak{M}^u \to \mathfrak{M}''^u \to 0$ et $0 \to \mathfrak{M}'^m \to \mathfrak{M}^m \to \mathfrak{M}''^m \to 0$.*

Preuve. — Par dualité, il suffit de montrer qu'on a une suite exacte $0 \to \mathfrak{M}'^{ét} \to \mathfrak{M}^{ét} \to \mathfrak{M}''^{ét} \to 0$ et une chasse au diagramme montre qu'il reste à voir la surjectivité de droite. Or, si $\overline{\mathfrak{M}}^{ét} = \mathfrak{M}^{ét}/\underline{\pi}\mathfrak{M}^{ét}$, un argument classique d'itération du Frobenius fournit une section k-linéaire $\overline{\mathfrak{M}}^{ét} \hookrightarrow \mathfrak{M}^{ét}$ et un isomorphisme $\mathfrak{S}_1 \otimes_k \overline{\mathfrak{M}}^{ét} \xrightarrow{\sim} \mathfrak{M}^{ét}$ (resp. avec $\mathfrak{M}''^{ét}$). Il suffit donc de montrer la surjectivité de $\overline{\mathfrak{M}}^{ét} \to \overline{\mathfrak{M}}''^{ét}$. Mais $\overline{\mathfrak{M}}^{ét} = \cap_{n\in\mathbf{N}}\phi^n(\overline{\mathfrak{M}}) = \phi^n(\overline{\mathfrak{M}})$ pour $n >> 0$ où $\overline{\mathfrak{M}} = \mathfrak{M}/\underline{\pi}\mathfrak{M}$ (resp. avec $\overline{\mathfrak{M}}''^{ét}$), d'où le résultat. $\square$

Lemme 3.2.1.5. *Soient $\mathfrak{M}$ un objet unipotent de $(Mod/\mathfrak{S}_1)$ de rang d, $(e_1, ..., e_d)$, d' et $\mathcal{G}$ comme en (3.2.1.1). On écrit $\mathcal{G}^{-1} = (a'_{ij})_{1\leq i,j\leq d} \in GL_d(\mathfrak{S}_1)$. Alors la sous-matrice $(a'_{ij})_{1\leq i,j\leq d'}$ est topologiquement nilpotente (pour la topologie $\underline{\pi}$-adique).*

Preuve. — Il suffit de montrer que si $(a'_{ij})_{1\leq i,j\leq d'}$ n'est pas topologiquement nilpotente, i.e. si son image dans $M_{d'}(k)$ n'est pas nilpotente, alors on peut fabriquer un quotient multiplicatif de $\mathfrak{M}$. La preuve est une variante de ([Wa1],2.3.1.2.2) (avec notations matricielles transposées). Quitte à faire un changement de base à coefficients dans k dans $\oplus_{i=1}^{d'}\mathfrak{S}_1e_i$, on peut supposer $\mathcal{G}^{-1} = (a'_{ij}) = \begin{pmatrix} A & B \\ \underline{\pi}C & D \end{pmatrix}$ avec $A \in GL_{d''}(\mathfrak{S}_1)$ et $1 \leq d'' \leq d$. On pose alors $\mathfrak{M}^m = \oplus_{i=1}^{d''}\mathfrak{S}_1\overline{e}_i$ avec $\overline{e}_i = \sum_{j=1}^{d''} a'_{ij}\frac{\phi}{\underline{\pi}}(\overline{e}_j)$ et on définit $\tilde{f} : \mathfrak{M} \to \mathfrak{M}^m$

par $\tilde{f}(e_i) = \overline{e}_i$ si $1 \leq i \leq d''$ et $\tilde{f}(e_i) = \sum_{j=1}^{d''} a'_{ij}\frac{\phi}{\underline{\pi}}(\overline{e}_j)$ si $d''+1 \leq i \leq d$. Un calcul analogue à ([Wa1],2.3.1.2.2) montre que $\tilde{f}(\phi(e_i)) = \phi(\tilde{f}(e_i)) + \underline{\pi}^2\epsilon_i$ si $1 \leq i \leq d'$ et $\tilde{f}(\phi(e_i)) = \phi(\tilde{f}(e_i)) + \underline{\pi}\epsilon_i$ si $d'+1 \leq i \leq d$ pour des $\epsilon_i \in \mathfrak{M}^m$. On cherche alors $\underline{\pi}\delta_i \in \underline{\pi}\mathfrak{M}^m$ tels que, en posant $f(e_i) = \tilde{f}(e_i) + \underline{\pi}\delta_i$, on ait $f \circ \phi = \phi \circ f$. On tombe sur des équations du type: $\delta_i = c_i + \underline{\pi}^{p-1}\sum_{j=1}^{d'} a'_{ij}\frac{\phi}{\underline{\pi}}(\delta_j) + \underline{\pi}^{p-1}\sum_{j=d'+1}^{d} a'_{ij}\phi(\delta_j)$ ($i \in \{1,...,d\}$, $c_i \in \mathfrak{M}^m$), qui se résolvent bien dans $\mathfrak{M}^m$ par approximations successives. $\square$

Lemme 3.2.1.6. *Supposons $p \geq 3$ ou $\mathfrak{M}$ unipotent, alors on peut prendre $\mathcal{G} \in GL_d(k)$ dans (3.2.1.1).*

Preuve. — On écrit $\mathcal{G} = \mathcal{G}_0(Id + \underline{\pi}\mathcal{H}_0)$ avec $\mathcal{G}_0 \in GL_d(k)$ et $\mathcal{H}_0 \in M_d(\mathfrak{S}_1)$. Posons par récurrence:

$$\mathcal{H}_n = \mathcal{G}_0^{-1} diag(\underbrace{\underline{\pi}^{p-2},...,\underline{\pi}^{p-2}}_{d' \text{ fois}}, \underline{\pi}^{p-1},...,\underline{\pi}^{p-1})\phi(\mathcal{H}_{n-1}) diag(\underbrace{\underline{\pi},...,\underline{\pi}}_{d' \text{ fois}}, 1,...,1)\mathcal{G}_0,$$

on voit que $\mathcal{H}_n$ tend $\underline{\pi}$-adiquement vers 0 quand $n \to +\infty$ (pour $p \geq 3$, c'est évident et pour $p = 2$, utiliser (3.2.1.5) sur $\mathcal{G}_0^{-1}$). Soit $\mathcal{B}_\infty = \lim_{n\to+\infty}(Id+\underline{\pi}\mathcal{H}_n)(Id+\underline{\pi}\mathcal{H}_{n-1})...(Id+\underline{\pi}\mathcal{H}_0)$, on vérifie que la base $\mathcal{B}_\infty \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix}$ convient. $\square$

Remarque 3.2.1.7. Pour tout p, la sous-catégorie pleine $(Mod/\mathfrak{S}_1)^u$ de $(Mod/\mathfrak{S}_1)$ formée des objets unipotents est équivalente à la catégorie des groupes unipotents sur W tués par p. On peut le voir en montrant, de façon similaire à ([Br2],4.1.1) à partir de (3.2.1.5), que le foncteur $(Mod/\mathfrak{S}_1) \to (Mod/S_1)$ induit une équivalence entre $(Mod/\mathfrak{S}_1)^u$ et la catégorie $\underline{MF}_k^{f,2'}$ de ([FL],9), vue comme sous-catégorie pleine de (Mod/S_1).

3.2.2. Nous continuons avec de l'algèbre commutative. On fixe A une W-algèbre noethérienne plate p-adiquement complète et on pose $A_0 = A$, $A_i = \mathcal{O}_{K_i}\otimes_W A$ ($i \geq 1$), $A_\infty = \mathcal{O}_{K_\infty}\otimes_W A$. On note $N_{i/i-1} : A_i \to A_{i-1}$ la norme, i.e. l'application qui à $x \in A_i$ associe le déterminant de la multiplication par x sur le A_{i-1}-module libre de rang p A_i.

Lemme 3.2.2.1. *Soit $x = x_0 + \pi_i x_1 + ... + \pi_i^{p-1}x_{p-1} \in A_i$ ($x_j \in A_{i-1}$) et ζ une racine $p^{\text{ième}}$ de 1 ($\zeta \neq 1$), on a:*

$$N_{i/i-1}(x) = \prod_{l=0}^{p-1}\Big(\sum_{j=0}^{p-1}(\pi_i\zeta^l)^j x_j\Big).$$

En particulier, $N_{i/i-1}(x) - x^p \in pA_i$.

Preuve. — Soient:

$$\Delta_1 = N_{i/i-1}(x) = \begin{vmatrix} x_0 & \pi_{i-1}x_{p-1} & \cdots & \cdots & \pi_{i-1}x_1 \\ x_1 & x_0 & \ddots & \ddots & \pi_{i-1}x_2 \\ \vdots & x_1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \pi_{i-1}x_{p-1} \\ x_{p-1} & x_{p-2} & \cdots & x_1 & x_0 \end{vmatrix},$$

$$\Delta_2 = \begin{vmatrix} x_0 & \pi_i^{p-1}x_{p-1} & \dots & \pi_i^2 x_2 & \pi_i x_1 \\ \pi_i x_1 & x_0 & \ddots & \ddots & \pi_i^2 x_2 \\ \pi_i^2 x_2 & \pi_i x_1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \pi_i^{p-1}x_{p-1} \\ \pi_i^{p-1}x_{p-1} & \pi_i^{p-2}x_{p-2} & \dots & \pi_i x_1 & x_0 \end{vmatrix},$$

σ_p les permutations de $\{0,...,p-1\}$ et $\tau \in \sigma_p$ tel que $\tau(i) = i-1$ si $i \geq 1$ et $\tau(0) = p-1$. Un calcul donne $\Delta_1 = \sum_{\sigma\in\sigma_p} sgn(\sigma)\pi_{i-1}^{h(\sigma)} \prod_{j=0}^{p-1} x_{\tau^j(\sigma(j))}$ où $h(\sigma) = \#\{j \in \{0,...,p-1\}$ tq $\sigma(j) \leq j-1\}$ et $\Delta_2 = \sum_{\sigma\in\sigma_p} sgn(\sigma)\pi_i^{g(\sigma)} \prod_{j=0}^{p-1} x_{\tau^j(\sigma(j))}$ où $g(\sigma) = \sum_{j=0}^{p-1} \tau^j(\sigma(j))$. Or $\tau^j(\sigma(j)) = \sigma(j) - j$ si $\sigma(j) \geq j$ et $\tau^j(\sigma(j)) = \sigma(j) - j + p$ si $\sigma(j) \leq j-1$, donc $g(\sigma) = \sum_{j=0}^{p-1}(\sigma(j) - j) + p\#\{j \in \{0,...,p-1\}$ tq $\sigma(j) \leq j-1\} = ph(\sigma)$ d'où clairement $\Delta_1 = \Delta_2$. Il est par ailleurs bien connu que Δ_2, déterminant d'une matrice circulante, se calcule par la formule du lemme. Notons $\Delta_2(X_0,...,X_{p-1}) = \prod_{l=0}^{p-1}\left(\sum_{j=0}^{p-1}\zeta^{lj}X_j\right) \in \mathbf{Z}[X_0,...,X_{p-1}]$, on a $\Delta_2(X_0,...,X_{p-1}) = \sum_{j=0}^{p-1} X_j^p + P(X_0,...,X_{p-1})$ avec $P \in \mathbf{Z}[X_0,...,X_{p-1}]$. Mais $\Delta_2(X_0,...,X_{p-1})^p = \prod_{l=0}^{p-1}\left(\sum_{j=0}^{p-1} X_j^p\right) + pQ = \left(\sum_{j=0}^{p-1} X_j^p\right)^p + pQ$ avec $Q \in \mathbf{Z}[X_j]$, donc $P^p \in p\mathbf{Z}[X_j]$ d'où $P \in p\mathbf{Z}[X_j]$. On en déduit facilement la dernière assertion. $\square$

Pour $r \geq 1$, on pose:

$$I_r = \{x \in A_\infty \ / \ x^p \in pA_\infty, x^{p^2} \in p^{p+1}A_\infty, ..., x^{p^r} \in p^{p^{r-1}+p^{r-2}+...+1}A_\infty\}.$$

On vérifie que les I_r sont des idéaux de A_∞.

Lemme 3.2.2.2. *Pour* $1 \leq r \leq i$, *on a:*

$$I_r \cap A_i = \{x \in A_i \ / \ N_{i/i-1}(x) \in pA_{i-1}, N_{i/i-2}(x) \in p^{p+1}A_{i-2}, ...$$
$$..., N_{i/i-r}(x) \in p^{p^{r-1}+p^{i-2}+...+1}A_{i-r}\}.$$

Preuve. — Par récurrence sur r. Pour $r = 1$ et $i \geq 1$, cela découle de la dernière assertion de (3.2.2.1). Supposons le résultat au cran $r-1 \geq 1$ pour tout $i \geq r-1$ et soit $x \in I_r \cap A_i$, par récurrence, on a donc $N_{i/i-1}(x) \in pA_{i-1}, ..., N_{i/i-r+1}(x) \in p^{p^{r-2}+...+1}A_{i-r+1}$ et $N_{i/i-1}(\frac{x^p}{p}) \in pA_{i-1}, ..., N_{i/i-r+1}(\frac{x^p}{p}) \in p^{p^{r-2}+...+1}A_{i-r+1}$. Mais:

$$\begin{aligned} N_{i/i-r+1}\Big(\frac{x^p}{p}\Big) \in p^{p^{r-2}+...+1}A_{i-r+1} \quad &\Longleftrightarrow \quad \Big(\frac{N_{i/i-r+1}(x)}{p^{p^{r-2}+...+1}}\Big)^p \in pA_{i-r+1} \\ &\overset{(\text{cas } r=1)}{\Longleftrightarrow} \quad N_{i-r+1/i-r}\Big(\frac{N_{i/i-r+1}(x)}{p^{p^{r-2}+...+1}}\Big) \in pA_{i-r} \\ &\Longleftrightarrow \quad N_{i/i-r}(x) \in p^{p^{r-1}+p^{i-2}+...+1}A_{i-r}. \end{aligned}$$

Soit $x \in A_i$ tel que $N_{i/i-1}(x) \in pA_{i-1}, ..., N_{i/i-r}(x) \in p^{p^{r-1}+...+1}A_{i-r}$, par récurrence, $x \in I_{r-1} \cap A_i$ et $\frac{N_{i/i-1}(x)}{p} \in I_{r-1} \cap A_{i-1}$. Donc $\left(\frac{N_{i/i-1}(x)}{p}\right)^{p^{r-1}} \in p^{p^{r-2}+...+1}A_{i-1}$ c'est-à-dire $N_{i/i-1}\left(\frac{x^{p^{r-1}}}{p^{p^{r-2}+...+1}}\right) \in pA_{i-1}$ d'où, par le cas $r = 1$, $x^{p^r} \in p^{p^{r-1}+...+1}A_i$. $\square$

Lemme 3.2.2.3. *Soit* $x = x_0 + \pi_i x_1 + ... + \pi_i^{p-1}x_{p-1} \in A_i$ $(x_j \in A_{i-1})$, *alors:*
(a) si $1 \leq r \leq i-1$, $x \in I_r \Longleftrightarrow x_j \in I_r, \forall\ j \in \{0,...,p-1\}$,
(b) $x \in I_i \Longleftrightarrow \pi_i^j x_j \in I_i, \forall\ j \in \{0,...,p-1\} \Longleftrightarrow x_0 \in I_i$ *et* $x_j \in I_{i-1}$, $\forall\ j \geq 1$.

Preuve. — Les sens $\Leftarrow$ sont triviaux (pour $r = i$, remarquer que $x_j \in I_{i-1} \Leftrightarrow \pi_i x_j \in I_i$). Montrons $\Rightarrow$ pour (a) par récurrence sur $r \leq i-1$. Si $r = 1$ (et $i \geq 2$), soit x comme dans l'énoncé, on remarque que $x_j^p \in A_{i-2} + pA_{i-1}$, d'où:

$$x^p \in pA_i \Longleftrightarrow \sum_{j=0}^{p-1} x_j^p \pi_{i-1}^j \in pA_{i-1} \Longleftrightarrow x_j^p \in pA_{i-2} + pA_{i-1} \subset pA_{i-1} \Longleftrightarrow x_j \in I_1.$$

Si $x \in I_r$ ($2 \leq r \leq i-1$), $x^p \in pI_{r-1}$ et (récurrence) $x_j \in I_{r-1}$ pour tout j, donc $\sum_{j=0}^{p-1} x_j^p \pi_{i-1}^j \in pI_{r-1}$. Par récurrence appliquée à $x_j \in I_{r-1}$, on a facilement $x_j^p - y_j \in pI_{r-1}$ pour des $y_j \in A_{i-2}$. Donc $\sum_{j=0}^{p-1} y_j \pi_{i-1}^j \in pI_{r-1}$ d'où $y_j \in pA_{i-2}$ et (récurrence) $y_j/p \in I_{r-1}$. Finalement $x_j \in pI_{r-1}$ i.e. $x_j \in I_r$. Le cas (b) s'en déduit car $x \in I_i \Rightarrow x_j \in I_{i-1}, \forall\, j \Rightarrow \pi_i^j x_j \in I_i$ si $j \geq 1 \Rightarrow x_0 \in I_i$. $\square$

3.2.3. On garde les notations de la section précédente. Par (3.2.2.2), la norme $K_i \otimes_W A \to K_{i-1} \otimes_W A$ induit une application notée encore $N_{i/i-1} : \frac{I_i \cap A_i}{\pi_1 \pi_2 \ldots \pi_i} \to \frac{I_{i-1} \cap A_{i-1}}{\pi_1 \pi_2 \ldots \pi_{i-1}}$ et on note:

$$\mathfrak{M}_1^{nor}(A) = \varprojlim_{N_{i/i-1}} \frac{I_i \cap A_i}{\pi_1 \pi_2 \ldots \pi_i} \subset \varprojlim_{N_{i/i-1}} K_i \otimes_W A.$$

On pose dans la suite $\mathfrak{M}_i(A) = \frac{I_i \cap A_i}{\pi_1 \pi_2 \ldots \pi_i}$: c'est un $\mathcal{O}_{K_i}$-module de type fini p-adiquement complet.

Lemme 3.2.3.1. *Soient $x_i, y_i \in (I_i \cap A_i)^n$, alors:*

$$N_{i/i-1}(x_i + y_i) - N_{i/i-1}(x_i) - N_{i/i-1}(y_i) \in p((I_i \cap A_i)^{pn} \cap A_{i-1}).$$

Preuve. — Cela découle de (3.2.2.1) et (3.2.2.3). $\square$

Lemme 3.2.3.2. *Pour $n \in \mathbf{N}$, $(I_i \cap A_i)^n \cap A_{i-1} \subset (I_{i-1} \cap A_{i-1})^n$ ($n \in \mathbf{N}$).*

Preuve. — Un élément de $(I_i \cap A_i)^n$ est une somme de $x_1 \ldots x_n$ où $x_l = \sum_{j=0}^{p-1} x_{l,j} \pi_i^j \in I_i$ ($x_{l,j} \in A_{i-1}$). Par (3.2.2.3), $x_{l,j} \in I_{i-1}$ d'où le résultat en développant. $\square$

Corollaire 3.2.3.3. *Soient $x = (x_i)_{i \geq 1}$ et $y = (y_i)_{i \geq 1}$ dans $\mathfrak{M}_1^{nor}(A)$, alors $N_{i+r/i}(x_{i+r} + y_{i+r})$ converge dans $\mathfrak{M}_i(A)$ quand $r \to +\infty$.*

Preuve. — En écrivant $N_{i+r/i} = N_{i+1/i} \circ \ldots \circ N_{i+r/i+r-1}$ et en utilisant les deux lemmes ci-dessus, il suffit de voir que $N_{i+r/i}\Big(\frac{(I_{i+r} \cap A_{i+r})^p}{\pi_1 \pi_2 \ldots \pi_{i+r}}\Big)$ tend vers 0 quand $r \to +\infty$. Une deuxième utilisation de (3.2.3.1) et (3.2.3.2) montre que:

$$N_{j/j-1}\Big(\frac{(I_j \cap A_j)^n}{\pi_1 \pi_2 \ldots \pi_j}\Big) \subset p^{n-1} \frac{(I_{j-1} \cap A_{j-1})^n}{\pi_1 \pi_2 \ldots \pi_{j-1}} + \frac{(I_{j-1} \cap A_{j-1})^{pn}}{\pi_1 \pi_2 \ldots \pi_{j-1}} \subset \frac{(I_{j-1} \cap A_{j-1})^{2n-1}}{\pi_1 \pi_2 \ldots \pi_{j-1}}.$$

On en déduit facilement le résultat puisque A est noethérien. $\square$

On pose $x + y = (z_i)_{i \geq 1}$ avec $z_i = \lim_{r \to +\infty} N_{i+r/i}(x_{i+r} + y_{i+r})$. On vérifie que cette loi fait de $\mathfrak{M}_1^{nor}(A)$ un groupe abélien annulé par p. Pour $a \in k$, $n \in \mathbf{N}$ et $x = (x_i)_{i \geq 1} \in \mathfrak{M}_1^{nor}(A)$, on définit $a\underline{\pi}^n \cdot x = ([a^{p^{-i}}]\pi_i^n x_i)_{i \geq 1} \in \mathfrak{M}_1^{nor}(A)$ où $[\cdot] \in W$ est le représentant de Teichmüller. En étendant l'action par linéarité, cela fait de $\mathfrak{M}_1^{nor}(A)$ un $\mathfrak{S}_1$-module. On définit $\phi : \mathfrak{M}_1^{nor}(A) \to \mathfrak{M}_1^{nor}(A)$ par $\phi((x_i)_{i \geq 1}) = (x_i^p)_{i \geq 1}$. Pour toute W-algèbre A noethérienne, plate et p-adiquement complète, $\mathfrak{M}_1^{nor}(A)$ est un $\mathfrak{S}_1$-module sans $\underline{\pi}$-torsion muni d'un Frobenius ϕ injectif semi-linéaire.

Remarque 3.2.3.4. Notons $\overline{\mathfrak{M}}_i(A) = \mathfrak{M}_i(A)/\left(\frac{I^p_{i+1}\cap A_i}{\pi_1\pi_2\ldots\pi_i}\right)$, on peut déduire de ce qui précède que la norme induit une application $\overline{N}_{i/i-1} : \overline{\mathfrak{M}}_i(A) \to \overline{\mathfrak{M}}_{i-1}(A)$ et que l'application naturelle $\mathfrak{M}^{nor}_1(A) = \varprojlim \mathfrak{M}_i(A) \to \varprojlim \overline{\mathfrak{M}}_i(A)$ est un isomorphisme de $\mathfrak{S}_1$-modules.

3.2.4. Soit $Spf(W)_{fppf}$ la catégorie des schémas formels p-adiques plats localement de type fini sur W munie de la topologie de Grothendieck engendrée par les familles surjectives de morphismes fppf. Le préfaisceau $\mathfrak{M}_i$ qui à X associe $\mathfrak{M}_i(\Gamma(X, \mathcal{O}_X))$ est un faisceau sur $Spf(W)_{fppf}$, sous-faisceau de $(X \mapsto K_i \otimes_W \Gamma(X, \mathcal{O}_X))$. De même, $(X \mapsto \mathfrak{M}^{nor}_1(\Gamma(X, \mathcal{O}_X))$ est un faisceau de $\mathfrak{S}_1$-modules sur $Spf(W)_{fppf}$. Soit $\mathfrak{M}$ un objet de $(Mod/\mathfrak{S}_1)$, on lui associe un faisceau $Gr(\mathfrak{M})$ sur $Spf(W)_{fppf}$ en posant:

$$Gr(\mathfrak{M})(X) = Hom_{\phi,\mathfrak{S}_1}\Big(\mathfrak{M}, \mathfrak{M}^{nor}_1(\Gamma(X, \mathcal{O}_X)) \otimes_{k,(\phi)} k\Big)$$

(applications $\mathfrak{S}_1$-linéaires commutant à ϕ). La torsion par le Frobenius sur k n'est là que pour une question de compatibilité avec le foncteur défini en ([Br1],3.1) lorsque $p \geq 3$. Le but de cette section est de montrer:

Théorème 3.2.4.1. *Pour tout p et tout $\mathfrak{M}$, le foncteur $Gr(\mathfrak{M})$ est représentable dans $Spf(W)_{fppf}$ par un schéma fini sur W de rang $p^{rg_{\mathfrak{S}_1}(\mathfrak{M})}$. Le foncteur $Gr : (Mod/\mathfrak{S}_1) \to (p, .., p)/W$ ainsi obtenu préserve les suites exactes courtes et coïncide, lorsque $p \geq 3$, avec le foncteur composé $(Mod/\mathfrak{S}_1) \xrightarrow{2.2} (Mod/S_1) \xrightarrow{[Br1]} (p, ..., p)/W$.*

Soit $\mathfrak{M}$ dans $(Mod/\mathfrak{S}_1)$. On fixe une base $(e_1, ..., e_d)$ et une matrice $\mathcal{G} = (a_{ij})_{1\leq i,j\leq d}$ comme en (3.2.1.1), en prenant $\mathcal{G}$ dans $GL_d(k)$ si $p \geq 3$ ou $\mathfrak{M}$ unipotent (3.2.1.6). On a une surjection $\mathfrak{S}_1 = k[[\underline{\pi}]] \to \mathcal{O}_{K_1}/p$, $a\underline{\pi}^n \mapsto a^{p^{-2}}\pi_1^n$ et on note $\mathcal{G}_1 = (a^1_{ij})_{1\leq i,j\leq d}$ un relevé dans $GL_d(\mathcal{O}_{K_1})$ de l'image de $\mathcal{G}$ dans $GL_d(\mathcal{O}_{K_1}/p)$ et $\mathcal{G}_0 = (a^0_{ij})_{1\leq i,j\leq d}$ un relevé dans $GL_d(W)$ de $\phi^{-1}(\mathcal{G}) = (a^{p^{-1}}_{ij})$ si $p \geq 3$ ou $\mathfrak{M}$ unipotent. On pose:

$$R_{1,\mathfrak{M}} = \frac{\mathcal{O}_{K_1}[X_1, ..., X_d]}{X_1^p - \pi_1^{p+\delta_1-1}(\sum_{j=1}^d a^1_{1j}X_j), ..., X_d^p - \pi_1^{p+\delta_d-1}(\sum_{j=1}^d a^1_{dj}X_j)}$$

et, si $p \geq 3$ ou $\mathfrak{M}$ unipotent:

$$R_{\mathfrak{M}} = \frac{W[X_1, ..., X_d]}{X_1^p - p^{\delta_1}(\sum_{j=1}^d a^0_{1j}X_j), ..., X_d^p - p^{\delta_d}(\sum_{j=1}^d a^0_{dj}X_j)}$$

avec $\delta_i = 1$ si $1 \leq i \leq d'$ et 0 sinon. Pour alléger le texte, on note dans la suite les d-uplets en caractère gras (ex: $\mathbf{x} = (x_1, ..., x_d)$, $\mathbf{x}^p = (x_1^p, ..., x_d^p)$, etc...).

Lemme 3.2.4.2. *Soit $\mathbf{x} \in A_1^d$ tel que $\mathbf{x}^p = diag(\underbrace{p, ..., p}_{d' \text{ fois}}, \pi_1^{p-1}, ..., \pi_1^{p-1})\mathcal{G}_1\mathbf{x}$, alors $\mathbf{x} \in (I_1 \cap A_1)^d$.*

Preuve. — En écrivant chaque composante $x_i = \sum_{j=0}^{p-1} x_{i,j}\pi_1^j$ $(x_{i,j} \in A)$, il suffit de montrer $x_{i,0} \in I_1 \cap A$ i.e. $x^p_{i,0} \in pA$, ce qui est facile en développant les équations. $\square$

Lemme 3.2.4.3. *Soit $\delta \in I^p_r \cap A_j$ avec $r \geq 2$ et $j \geq 1$ et définissons par récurrence $\delta_1 = \delta^p/p$ et $\delta_n = \delta^p_{n-1}/p$ si $n \geq 2$, alors $\delta_n \in A_j$ et $\delta_n \to 0$ dans A_j quand $n \to +\infty$.*

Preuve. — Comme $\delta_n \in K_j \otimes_W A$, il suffit de montrer $\delta_n \in A_\infty$ et $\delta_n \to 0$ quand $n \to +\infty$. En utilisant $I_r^n \cap A_i \to 0$ quand $n \to +\infty$, on voit qu'il suffit de considérer le cas $\delta = x_1 x_2 ... x_p$ avec $x_i \in I_2 \subset I_r$. On a $\delta^p/p \in p^{p-1} I_1^p$ et $\delta_2 = \delta^{p^2}/p^{p+1} \in p^{p(p-1)-1+p} A_\infty = p^{p^2-1} A_\infty$. D'où $\delta_n \in p^{p^n - p^{n-2} - ... - 1} A_\infty$, $\forall\ n \geq 2$. Mais, pour *tout* p, $p^n - p^{n-2} - ... - 1 \to 0$ quand $n \to +\infty$. $\square$

Proposition 3.2.4.4. *Pour toute W-algèbre noethérienne plate et p-adiquement complète A, on a des morphismes canoniques et fonctoriels:*
(a) $Hom_{\phi, \mathcal{G}_1}\left(\mathfrak{M}, \mathfrak{M}_1^{nor}(A) \otimes_{k,(\phi)} k\right) \to Hom_{\mathcal{O}_{K_1}}(R_{1,\mathfrak{M}}, A_1)$ *pour tout p et tout $\mathfrak{M}$,*
(b) $Hom_{\phi, \mathcal{G}_1}\left(\mathfrak{M}, \mathfrak{M}_1^{nor}(A) \otimes_{k,(\phi)} k\right) \to Hom_W(R_{\mathfrak{M}}, A)$ *pour $p \geq 3$ ou $\mathfrak{M}$ unipotent.*

Preuve. — Commençons par (a). Soient $f \in Hom_{\phi, \mathcal{G}_1}\left(\mathfrak{M}, \mathfrak{M}_1^{nor}(A) \otimes_{k,(\phi)} k\right)$, $f(e_i)$ l'image de e_i "rentrée" dans $\mathfrak{M}_1^{nor}(A)$, $x_i = \pi_1 f(e_i)_1 \in I_1 \cap A_1$ et $\mathbf{x} = (x_1, ..., x_d)$. D'après (3.2.3.1), on a des équations:

$$(1) \qquad \left(\frac{\mathbf{x}}{\pi_1}\right)^p = diag(\underbrace{\pi_1, ..., \pi_1}_{d' \text{ fois}}, 1, ..., 1)\left[\mathcal{G}_1 \frac{\mathbf{x}}{\pi_1} + \frac{\mathbf{c}'}{\pi_1}\right]$$

où $\mathbf{c}' \in (I_2^p \cap A_1)^d$. Cherchons $\mathbf{v} \in (I_2^p \cap A_1)^d$ tel qu'en posant $\mathbf{y} = \mathbf{x} + \mathbf{v}$, on ait:

$$(2) \qquad \left(\frac{\mathbf{y}}{\pi_1}\right)^p = diag(\underbrace{\pi_1, ..., \pi_1}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_1 \frac{\mathbf{y}}{\pi_1}.$$

Un calcul donne une équation du type:

$$(3) \qquad \mathbf{v} = \mathbf{c} + \mathcal{H}_1 \mathbf{v}^2 + \cdots + \mathcal{H}_{p-1}\mathbf{v}^{p-1} + \mathcal{H}_p \frac{\mathbf{v}^p}{p}$$

pour un $\mathbf{c} \in (I_2^p \cap A_1)^d$ et où $\mathcal{H}_i \in M_d(A_1)$. En reportant l'expression de $\mathbf{v}$ dans les termes en $\mathbf{v}^2$, $\mathbf{v}^3$, ..., $\mathbf{v}^p/p$ plusieurs fois de suite et en utilisant (3.2.4.3), on voit qu'il y a une et une seule solution à (3) dans $(I_2^p \cap A_1)^d$, donc une et une seule solution à (2) congrue à $\mathbf{x}$ modulo $I_2^p \cap A_1$. Par (3.2.4.2), une solution de (2) est équivalente à un morphisme dans $Hom_{\mathcal{O}_{K_1}}(R_{1,\mathfrak{M}}, A_1)$.
Pour (b), le même raisonnement au cran d'après (i.e. dans $A_0 = A$ au lieu de A_1) fournit des équations:

$$(4) \qquad \mathbf{x}^p = diag(\underbrace{p, ..., p}_{d' \text{ fois}}, 1, ..., 1)\left[\mathcal{G}_0 \mathbf{x} + \mathbf{c}'\right]$$

pour un $\mathbf{c}' \in (I_1^p \cap A)^d$. Notons $Fil^i A = (I_1 \cap A)^i$, on remarque que $I_1^p \cap A = Fil^p A + pA$ (utiliser 3.2.2.3). Sous les conditions de (b), c'est un résultat classique qu'il existe une unique façon de corriger $\mathbf{x}$ par un $\mathbf{v} \in Fil^p A + pA$ de telle sorte que $\mathbf{y} = \mathbf{x} + \mathbf{v}$ vérifie:

$$(5) \qquad \mathbf{y}^p = diag(\underbrace{p, ..., p}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_0 \mathbf{y}$$

(voir par exemple ([Wa1],2.3.3.1) pour $A = \mathcal{O}_{\bar{K}}$ ou [Fo3]). $\square$

Proposition 3.2.4.5. *Les morphismes en (3.2.4.4) sont des bijections.*

Preuve. — Nous allons construire dans chaque cas une flèche dans l'autre sens. On fixe des matrices $\mathcal{G}_r \in GL_d(\mathcal{O}_{K_r})$ obtenues à partir de $\mathcal{G}_1$ de la façon suivante: si $a_{ij}^1 = \sum_{j=0}^{p-1} a_j \pi_1^j$ avec $a_j \in W$, on pose $a_{ij}^r = \sum_{j=0}^{p-1} \phi^{-r}(a_j)\pi_r^j$ et $\mathcal{G}_r = (a_{ij}^r)_{1 \leq i,j \leq d}$. Soit $f \in Hom_{\mathcal{O}_{K_1}}(R_{1,\mathfrak{M}}, A_1)$, par (3.2.4.2), f correspond à $\frac{\mathbf{x}^{(1)}}{\pi_1} \in (\mathfrak{M}_1(A))^d$ solution de (2). Si $\mathbf{x}^{(1)} = (x_1^{(1)}, ..., x_d^{(1)})$, on remarque que $x_i^{(1)} \in I_2 \cap A_1$ si $1 \leq i \leq d'$ (car $x_i^{(1)p} \in pI_1$) et $\pi_2 x_i^{(1)} \in I_2 \cap A_1$ pour tout i. Posons $\frac{\tilde{\mathbf{x}}^{(2)}}{\pi_1\pi_2} = \mathcal{G}_2^{-1} diag(\underbrace{\frac{1}{\pi_2}, ..., \frac{1}{\pi_2}}_{d' \text{ fois}}, 1, ..., 1)\frac{\mathbf{x}^{(1)}}{\pi_1} \in (\mathfrak{M}_2(A))^d$, un calcul donne:

$$\left(\frac{\tilde{\mathbf{x}}^{(2)}}{\pi_1\pi_2}\right)^p - diag(\underbrace{\pi_2, ..., \pi_2}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_2 \frac{\tilde{\mathbf{x}}^{(2)}}{\pi_1\pi_2} \in \left(\frac{I_2^p \cap A_2}{\pi_1}\right)^d. \tag{6}$$

Cherchons $\mathbf{v} \in (I_2^p \cap A_2)^d$ tel que:

$$\left(\frac{\tilde{\mathbf{x}}^{(2)} + \mathbf{v}}{\pi_1\pi_2}\right)^p = diag(\underbrace{\pi_2, ..., \pi_2}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_2 \frac{\tilde{\mathbf{x}}^{(2)} + \mathbf{v}}{\pi_1\pi_2}, \tag{7}$$

en développant, on obtient:

$$\mathbf{v} = \mathbf{c} + \mathcal{H}_1 \mathbf{v}^2 + \cdots + \mathcal{H}_{p-1}\mathbf{v}^{p-1} + \mathcal{H}_p \frac{\mathbf{v}^p}{p} \tag{8}$$

avec $\mathbf{c} \in (I_2^p \cap A_2)^d$ et $\mathcal{H}_i \in M_d(A_2)$. En procédant comme en (3.2.4.4) grâce à (3.2.4.3), on voit que cette équation a une solution et une seule dans $(I_2^p \cap A_2)^d$. Posons $\mathbf{x}^{(2)} = \tilde{\mathbf{x}}^{(2)} + \mathbf{v}$ et, de même, $\frac{\tilde{\mathbf{x}}^{(3)}}{\pi_1\pi_2\pi_3} = \mathcal{G}_3^{-1} diag(\underbrace{\frac{1}{\pi_3}, ..., \frac{1}{\pi_3}}_{d' \text{ fois}}, 1, ..., 1)\frac{\mathbf{x}^{(2)}}{\pi_1\pi_2} \in (\mathfrak{M}_3(A))^d$, un calcul analogue au précédent donne:

$$\left(\frac{\tilde{\mathbf{x}}^{(3)}}{\pi_1\pi_2\pi_3}\right)^p - diag(\underbrace{\pi_3, ..., \pi_3}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_3 \frac{\tilde{\mathbf{x}}^{(3)}}{\pi_1\pi_2\pi_3} \in \left(\frac{I_3^p \cap A_3}{\pi_1\pi_2}\right)^d \tag{9}$$

et, en utilisant (3.2.4.3), on peut de même corriger cette équation dans $I_3^p \cap A_3$. Finalement, en remarquant que $N_{j/j-1}(I_j^p \cap A_j) \subset p(I_j^p \cap A_{j-1})$ (utiliser $N_{j/j-1}(x) - x^p \in pI_j^p$ si $x \in I_j \cap A_j$ et $p^p I_{j-1}^p \subset p(\pi_j I_{j-1})^p \subset pI_j^p$), on obtient pour tout $r \geq 1$ une solution $\mathbf{x}^{(r)} \in (I_r \cap A_r)^d$ à l'équation $(\frac{\mathbf{x}^{(r)}}{\pi_1 ... \pi_r})^p = diag(\underbrace{\pi_r, ..., \pi_r}_{d' \text{ fois}}, 1, ..., 1)\mathcal{G}_r \frac{\mathbf{x}^{(r)}}{\pi_1 ... \pi_r}$ telle que, avec des notations évidentes:

$$N_{r/r-1}\left(\frac{\mathbf{x}^{(r)}}{\pi_1 ... \pi_r}\right) - \frac{\mathbf{x}^{(r-1)}}{\pi_1 ... \pi_{r-1}} \in \left(\frac{I_r^p \cap A_{r-1}}{\pi_1 ... \pi_{r-1}}\right)^d.$$

On laisse au lecteur le soin de vérifier que $\left(\lim_{r\to+\infty} N_{i+r/i}(\frac{\mathbf{x}^{(i+r)}}{\pi_1 ... \pi_{i+r}})\right)_{i\geq 1} \in (\mathfrak{M}_1^{nor}(A))^d$ permet de construire un antécédent à f. Pour le cas (a), seul le 1$^{\text{er}}$ cran est différent puisqu'on commence avec $A_0 = A$. On tombe sur une équation du type:

$$\mathbf{v} = \mathbf{c} + \mathcal{H}_1 \mathbf{v}^2 + \cdots + \mathcal{H}_{p-1}\mathbf{v}^{p-1} + (Id + \mathcal{H}_p)\mathcal{G}_1^{-1} diag(\underbrace{1, ..., 1}_{d' \text{ fois}}, \pi_1, ..., \pi_1)\frac{\mathbf{v}^p}{p} \tag{10}$$

où $\mathcal{H}_i \in M_d(I_1 \cap A_1)$ et où la sous-matrice supérieure gauche $d' \times d'$ de $\mathcal{G}_1^{-1}$ est topologiquement nilpotente. Cette équation a une et une seule solution dans $(I_1 \cap A_1)^d$ et on continue comme précédemment. $\square$

Soient $R''_{\mathfrak{M}}$ la restriction à la Weil de $\mathcal{O}_{K_1}$ à W de $R_{1,\mathfrak{M}}$, $R'_{\mathfrak{M}}$ l'adhérence schématique de $R''_{\mathfrak{M}}$ et $R_{\mathfrak{M}}$ la complétion p-adique de $R'_{\mathfrak{M}}$. Par construction, $Hom_W(R_{\mathfrak{M}}, A) \simeq Hom_{\mathcal{O}_{K_1}}(R_{1,\mathfrak{M}}, A_1)$

et les notations sont bien consistantes par (3.2.4.5) lorsque $p \geq 3$ ou $\mathfrak{M}$ unipotent (plus précisément, dans ce cas, le $R_{\mathfrak{M}}$ décrit précédemment et le $R_{\mathfrak{M}}$ obtenu par descente sont des W-algèbres isomorphes). Pour montrer que $Gr(\mathfrak{M})$ est représentable par un schéma fini et plat sur W pour tout p, il suffit de montrer la:

Proposition 3.2.4.6. *Pour tout p et tout $\mathfrak{M}$, $R_{\mathfrak{M}}$ est fini sur W de rang p^d.*

Preuve. — Seul reste le cas $p = 2$ et $\mathfrak{M}$ quelconque. Par (3.2.1.3), on écrit $0 \to \mathfrak{M}^u \to \mathfrak{M} \to \mathfrak{M}^m \to 0$ avec $\mathfrak{M}^u$ unipotent et $\mathfrak{M}^m$ multiplicatif. Soient d^u, d^m les rangs de $\mathfrak{M}^u$ et $\mathfrak{M}^m$ sur $\mathfrak{S}_1$ ($d = d^u + d^m$). Par (3.2.4.5), si $R_{\mathfrak{M}}$ est fini de rang p^d pour un choix de matrices $(\mathcal{G}, \mathcal{G}_1)$ comme précédemment, alors tous les $R_{\mathfrak{M}}$ pour tous les autres choix $(\mathcal{G}, \mathcal{G}_1)$ sont aussi finis de rang p^d (car isomorphes au précédent). C'est un exercice de voir qu'on peut trouver une base de $\mathfrak{M}$ telle que la matrice (transposée) de ϕ dans cette base soit du type:

$$diag(\underbrace{\pi_1, ..., \pi_1}_{d^{u\prime} \text{ fois}}, 1, ..., 1, \underbrace{\pi_1, ..., \pi_1}_{d^m \text{ fois}}) \begin{pmatrix} \mathcal{G}_1^u & 0 \\ A & \mathcal{G}_1^m \end{pmatrix}$$

où $\mathcal{G}_1^u \in GL_{d^u}(\mathcal{O}_{K_1})$ et $\mathcal{G}_1^m = (a_{ij}^m)_{1 \leq i,j \leq d^m} \in GL_{d^m}(\mathcal{O}_{K_1})$. On a alors:

$$R_{1,\mathfrak{M}} \simeq \frac{R_{1,\mathfrak{M}^u}[X_1, ..., X_{d^m}]}{X_1^p - p(\sum_{j=1}^{d^m} a_{1j}^m X_j + c_1), ..., X_d^p - p(\sum_{j=1}^{d^m} a_{d^m j}^m X_j + c_{d^m})}$$

pour des $c_j \in R_{1,\mathfrak{M}^u}$. Plaçons nous en $p = 2$ et notons $a_{ij}^m = a_{ij}^{m,0} + \pi_1 a_{ij}^{m,1}$ avec $a_{ij}^{m,\cdot} \in W$. Un calcul montre que $R'_{\mathfrak{M}} \simeq R'_{\mathfrak{M}^u}[X_1^0, X_1^1, ..., X_{d^m}^0, X_{d_m}^1]/I$ où I est l'idéal engendré par les équations ($1 \leq i \leq d^m$):

$$\begin{aligned} X_i^{0^2} + 2X_i^{1^2} &= 2\sum_{j=1}^{d^m} a_{ij}^{m,0} X_j^0 + 4\sum_{j=1}^{d^m} a_{ij}^{m,1} X_j^1 + 2c_i^0 \\ X_i^0 X_i^1 &= \sum_{j=1}^{d^m} a_{ij}^{m,1} X_j^0 + \sum_{j=1}^{d^m} a_{ij}^{m,0} X_j^1 + c_i^1 \end{aligned}$$

avec $c_i^0, c_i^1 \in R'_{\mathfrak{M}^u}$. Comme $(a_{ij}^{m,0}) - diag(X_i^0) \in GL_{d^m}(R_{\mathfrak{M}})$, la deuxième équation montre que les X_j^1 sont déterminés dans $R_{\mathfrak{M}}$ en fonction des X_j^0 et de $R_{\mathfrak{M}^u}$. Comme $R_{\mathfrak{M}^u}$ est fini de rang 2^{d^u} sur W par (3.2.4.5) et comme $R_{\mathfrak{M}}/(2) \simeq \frac{R_{\mathfrak{M}^u}/(2)[X_1^0, ..., X_{dm}^0]}{(X_1^{0^2}, ..., X_{dm}^{0^2})}$, $R_{\mathfrak{M}}$ est fini de rang 2^d sur W. $\square$

Proposition 3.2.4.7. *Pour tout p, le foncteur Gr est exact. Pour $p \geq 3$, il est compatible avec le foncteur composé $(Mod/\mathfrak{S}_1) \to (Mod/S_1) \to (p, ..., p)/W$.*

Preuve. — Avec les notations de la preuve précédente, on a clairement $R_{\mathfrak{M}^u} \to R_{\mathfrak{M}}$ fidèlement plat et $W \otimes_{R_{\mathfrak{M}^u}} R_{\mathfrak{M}} \xrightarrow{\sim} R_{\mathfrak{M}^m}$ où $R_{\mathfrak{M}^u} \to W$ est la section nulle, ce qui montre par des arguments standards que la suite $0 \to Gr(\mathfrak{M}^m) \to Gr(\mathfrak{M}) \to Gr(\mathfrak{M}^u) \to 0$ est une suite exacte de schémas en groupes. D'après (3.2.1.4), il suffit donc de montrer l'exactitude avec des modules unipotents ou multiplicatifs (séparément), ce qui se voit directement sur les $R_{\mathfrak{M}}$ correspondants par le même argument. Supposons maintenant $p \geq 3$. Pour toute W-algèbre plate p-adiquement complète A, posons $M(A) = \mathfrak{M}_1^{nor}(A)/(\underline{\pi})$ avec le ϕ induit, $Fil^1 M(A) = Ker(\phi)$, ϕ_1 la flèche composée:

$$\begin{array}{ccccc} Fil^1\left(\frac{\mathfrak{M}_1^{nor}(A)}{\underline{\pi}}\right) & \to & \underline{\pi}\frac{\mathfrak{M}_1^{nor}(A)}{\underline{\pi}^p} & \to & \frac{\mathfrak{M}_1^{nor}(A)}{\underline{\pi}} \\ x & \mapsto & \phi(\hat{x}) & \mapsto & -\overline{\frac{\phi(\hat{x})}{\underline{\pi}}} = \phi_1(x) \end{array}$$

où $\hat{x}$ est un relevé quelconque de x dans $\mathfrak{M}_1^{nor}(A)/(\underline{\pi}^p)$. La norme $N_{1/0} : A_1 \to A_0$ induit un morphisme semi-linéaire (c.f. 3.2.3.1 et preuve de 3.2.4.4): $M(A) \to A/(\underline{I_1^p \cap A}) = A/(Fil^pA + pA)$ compatible aux Fil^1, ϕ et ϕ_1 (ϕ_1 à droite est défini par $\phi_1(x) = -\overline{\frac{\hat{x}^p}{p}}$ si $\hat{x}$ est un relevé dans A). Soit $M = \mathfrak{M}/(\underline{\pi})$ muni du ϕ induit, de $Fil^1M = Ker(\phi)$ et de $\phi_1 : Fil^1M \to M$ défini comme précédemment en remplaçant $\mathfrak{M}_1^{nor}(A)$ par $\mathfrak{M}$. On voit que M est un objet de la catégorie $\underline{MF}_k^{f,2}$ de [FL] et que $S_1 \otimes_k M$ (muni des structures "produit tensoriel") s'identifie à l'objet de (Mod/S_1) associé à $\mathfrak{M}$ en (2.2). De plus le composé $\mathfrak{M}_1^{nor}(A) \to M(A) \to \frac{A}{Fil^pA+pA}$ induit clairement une application canonique:

$$Hom_{\phi,\mathfrak{S}_1}\Big(\mathfrak{M}, \mathfrak{M}_1^{nor}(A) \otimes_{k,(\phi)} k\Big) \longrightarrow Hom_{\phi_1,Fil^1}\Big(M, \frac{A}{Fil^pA + pA} \otimes_{k,(\phi)} k\Big)$$

où les flèches à droite sont les morphismes k-linéaires qui préservent Fil^1 et commutent à ϕ et ϕ_1. Supposons A syntomique sur W ([Br1],2). On a une flèche naturelle compatible à toutes les structures: $A/(Fil^pA + pA) \otimes_{k,(\phi)} k \to \mathcal{O}_1^{cris}(A)/\mathcal{J}_1^{[p]}(A)$ où $\mathcal{O}_1^{cris}(A) = H^0_{cris}(A/k)$ et $\mathcal{J}_1(A) = Ker(\mathcal{O}_1^{cris}(A) \to A/p)$ (c.f. [Br1]) et, d'après ([Br1],3.1.6), un isomorphisme:

$$Hom_{\phi_1,Fil^1}\Big(M, \mathcal{O}_1^{cris}(A)\Big) \xrightarrow{\sim} Hom_{\phi_1,Fil^1}\Big(M, \mathcal{O}_1^{cris}(A)/\mathcal{J}_1^{[p]}(A)\Big).$$

Finalement, on dispose d'une suite d'applications canoniques:

$$Hom\Big(\mathfrak{M},\mathfrak{M}_1^{nor}(A)\otimes_{k,(\phi)}k\Big)\to Hom\Big(M,\frac{A}{Fil^pA+pA}\otimes_{k,(\phi)}k\Big)\to Hom\Big(M,\mathcal{O}_1^{cris}(A)/\mathcal{J}_1^{[p]}(A)\Big)\xleftarrow{\sim} Hom\Big(M,\mathcal{O}_1^{cris}(A)\Big).$$

Mais les trois premiers groupes sont tous les trois isomorphes (de façon compatible) à $Hom_W(R_{\mathfrak{M}}, A)$! : par (3.2.4.5) pour le premier, [Fo3] pour le deuxième et ([Br1],3.1.2 et 3.1.8) pour le troisième. $\square$

Bibliographie

[Br1] Breuil C., *Schémas en groupes sur un anneau de valuation discrète complet très ramifié*, prépublication, Université Paris-Sud, 1998.

[Br2] Breuil C., *Une application du corps des normes*, à paraître à Compositio Math.

[Col] Colmez P., *Représentations cristallines et représentations de hauteur finie*, preprint du LMENS, 1997.

[Con] Conrad B., *Finite group schemes over bases with low ramification*, preprint.

[Fo1] Fontaine J.-M., *Groupes p-divisibles sur les corps locaux*, Astérisque 47-48, Soc. Math. de France, 1977.

[Fo2] Fontaine J.-M., *Représentations p-adiques des corps locaux*, Grothendieck Festschrift II, Birkhauser, 1991, 249-309.

[Fo3] Fontaine J.-M., Exposé à l'I.A.S., 10 octobre 1995.

[FL] Fontaine J.-M., Laffaille G., *Construction de représentations p-adiques*, Ann. Scient. E.N.S. 15, 1982, 547-608.

[He] Herr L., *Sur la cohomologie galoisienne des corps p-adiques*, à paraître au Bulletin de la S.M.F.

[Wa1] Wach N., *Représentations cristallines de torsion*, Comp. Math. 108, 1997, 185-240.

[Wa2] Wach N., *Représentations p-adiques potentiellement cristallines*, Bull. Soc. math. France 124, 1996, 375-400.

[Wi] Wintenberger J.-P., Le corps des normes de certaines extensions infinies de corps locaux; applications, Ann. Scient. E.N.S. 16, 1983, 59-89.