Représentations semi-stables de torsion dans le cas $er < p - 1$

Xavier Caruso

Mai 2004

Abstract

Let K be a local field of mixed characteristic not absolutely ramified. Fontaine-Laffaille theory (see [13]) gives a description of the torsion crystalline $\mathbb{Z}_p$ representations of the absolute Galois group of K (p denotes the characteristic of the residual field). Improving the former works, Breuil introduced new modules and obtained an integer and torsion theory for the semi-stable representations (see [3]).

In this paper, we follow Breuil's works and adapt them to the case where the local field K can be absolutely ramified. However, we would have a limitation on the index of absolute ramification.

Résumé

Soit K un corps local de caractéristique mixte non absolument ramifié. La théorie de Fontaine-Laffaille (voir [13]) permet de décrire les $\mathbb{Z}_p$-représentations galoisiennes cristallines entières de torsion (p désigne la caractéristique du corps résiduel). Poursuivant les précédents travaux, Breuil a introduit de nouveaux modules et a obtenu une théorie entière et de torsion pour les représentations semi-stables (voir [3]).

Dans cet article, nous reprenons les travaux de Breuil et les adaptons dans le cas où le corps local K peut être absolument ramifié. Nous aurons toutefois une contrainte sur l'indice de ramification absolu.

Table des matières

1 Introduction

Dans toute la suite de ce papier, p désigne un nombre premier et k un corps parfait de caractéristique p. On note $\bar{k}$ une clôture algébrique de k, $\mathbb{F}_p$ le sous-corps premier de k et si $q = p^h$ est une puissance de p, $\mathbb{F}_q$ l'ensemble des solutions dans $\bar{k}$ de l'équation $x^q = x$.

On désigne par W l'anneau des vecteurs de Witt à coefficients dans k. On rappelle que comme k est parfait, cet anneau est un anneau de valuation discrète complet de caractéristique nulle dont p est une uniformisante et dont le corps résiduel s'identifie canoniquement à k. On dispose en outre d'une application $\sigma : W \to W$ appelée Frobenius qui induit par passage au quotient le Frobenius classique sur k, c'est-à-dire l'élévation à la puissance p.

On appelle K_0 le corps des fractions de W, c'est un corps local de caractéristique mixte. On prend K une extension finie totalement ramifiée de K_0. On note e le degré de l'extension K/K_0, c'est l'indice de ramification absolue de K. On appelle $\mathcal{O}_K$ l'anneau des entiers de K et on choisit π une uniformisante de cet anneau. On fixe $\bar{K}$ une clôture algébrique de K, on note $\mathcal{O}_{\bar{K}}$ l'anneau des entiers de $\bar{K}$ et $G_K = \mathrm{Gal}\left(\bar{K}/K\right)$ le groupe de Galois absolu du corps K. On note I le groupe d'inertie (c'est un sous-groupe de G_K), I_s le groupe d'inertie sauvage et $I_t = I/I_s$ le groupe d'inertie modérée. Enfin, on appelle v la valuation sur $\bar{K}$ normalisée par $v(\pi) = 1$ (et donc $v(p) = e$).

Une $\mathbb{Z}_p$-représentation (resp. $\mathbb{F}_p$-représentation, resp. $\mathbb{F}_q$-représentation, resp. $\mathbb{Q}_p$-représentation) de G_K est une action linéaire et continue de G_K sur un $\mathbb{Z}_p$-module (resp. un $\mathbb{F}_p$-espace vectoriel, resp. un $\mathbb{F}_q$-espace vectoriel, resp. un $\mathbb{Q}_p$-espace vectoriel). Afin d'étudier ces représentations, diverses catégories ont été introduites. Nous allons nous préoccuper dans ce papier des catégories $\underline{\mathcal{M}}^r$ introduites par Breuil dans [6], et nous montrerons comment il résulte de notre étude le théorème 1.0.1 ci-dessous.

Avant de l'énoncer, faisons quelques rappels (pour plus de précisions, voir le paragraphe 1 de [20]). Soient h un entier et $q = p^h$. Notons $\hat{V} = \{x \in \mathcal{O}_{\bar{K}} \,/\, x^{p^h} = \pi x\}$ et $V \subset \mathcal{O}_{\bar{K}}/p$ la réduction modulo p de $\hat{V}$. L'espace V est une $\mathbb{F}_p$-représentation de G_K. De plus V hérite naturellement d'une structure de $\mathbb{F}_q$-espace vectoriel de dimension 1 et fournit un caractère $I \to \mathbb{F}_q^\star$ qui se factorise par $\theta : I_t \to \mathbb{F}_q^\star$. On pose $\theta_i = \theta^{p^i}$, ce sont les *caractères fondamentaux de niveau h.* Toute $\mathbb{F}_p$-représentation irréductible de dimension d du groupe d'inertie modérée s'écrit comme un produit de caractères fondamentaux de niveau h (voir la proposition 5 du paragraphe 1 de [20]).

Théorème 1.0.1. *Soit X un schéma propre et lisse sur K à réduction semi-stable sur l'anneau des entiers $\mathcal{O}_K$. On fixe r un entier. Les exposants qui décrivent l'action de l'inertie modérée sur la semi-simplifiée modulo p de $H^r_{ét}(X_{\bar{K}}, \mathbb{Q}_p)^\star$ (où $X_{\bar{K}}$ est l'extension des scalaires de X à $\bar{K}$ et où « $\star$ » signifie que l'on prend le dual) sont compris entre* 0 *et er.*

Ce théorème est à rapprocher d'une conjecture formulée par Serre dans le paragraphe 1.13 de [20] qui prédit le même résultat pour la représentation $H^r_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p\mathbb{Z})^\star$. À l'heure actuelle, cette conjecture est connue dans le cas $r = 1$ bonne réduction ([19]), le cas non ramifié bonne réduction ([13], [18]), le cas non ramifié à réduction semi-stable ([5]) et le cas $r = 1$ ([8]). Le résultat donné ici ne fait aucune hypothèse ni sur e, ni sur r. Remarquons toutefois qu'il est vide pour $er \geqslant p - 1$.

Soit r un entier vérifiant $er < p - 1$. Nous présentons dans le chapitre 2, la catégorie $\underline{\mathcal{M}}^r$ et le foncteur T_{st} qui associe à tout objet de cette catégorie une $\mathbb{Z}_p$-représentation de torsion de G_K. Le chapitre 3 est consacré à l'étude de la catégorie $\underline{\mathcal{M}}^r$. En particulier, toujours dans le cas $er < p - 1$, on démontre qu'elle est abélienne et artinienne.

Nous donnons ensuite dans le chapitre 4 une description complète des objets simples de $\underline{\mathcal{M}}^r$, lorsque le corps résiduel k est supposé algébriquement clos. Plus précisément nous prouvons le théorème suivant :

Théorème 1.0.2. *Supposons k algébriquement clos et $er < p - 1$. Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$. Alors, il existe une base $(e_1, \ldots, e_h)$ de S et une suite d'entiers (n_i) compris entre* 0 *et er, périodique de période* exactement *h, le tout tel que :*

$$Fil^r \mathcal{M} = u^{n_1} e_1 + \ldots + u^{n_h} e_h + Fil^p S \cdot \mathcal{M},$$

$\phi_r(u^{n_i} e_i) = e_{i+1}$ et $N(e_i) = 0$ pour tout i (considéré modulo h).

En outre, ces objets sont tous simples et deux à deux non isomorphes.

Par la suite, nous nous intéressons véritablement au foncteur T_{st}. On commence par déterminer son image sur les objets simples précédemment calculés. On obtient le théorème :

Théorème 1.0.3. *Supposons k algébriquement clos et $er < p - 1$. Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$ comme dans le théorème 1.0.2. Alors la représentation galoisienne $T_{st}(\mathcal{M})$ est isomorphe à :*

$$\theta_1^{m_1} \theta_2^{m_2} \ldots \theta_h^{m_h}$$

où m_i est défini par $n_i + m_i = er$ et où les θ_i sont les caractères fondamentaux de niveau h.

En particulier, pour tout objet $\mathcal{M}$ de $\underline{\mathcal{M}}^r$ tué par p, les exposants qui décrivent l'action de l'inertie modérée sur la semi-simplifiée modulo p de $T_{st}(\mathcal{M})$ sont compris entre 0 *et er.*

La conclusion des chapitres 5 et 6 est une réponse affirmative à une conjecture formulée à la fin de [6], énoncé que nous rappelons ici :

Théorème 1.0.4. *Supposons $er < p-1$, alors le foncteur T_{st} de la catégorie $\underline{\mathcal{M}}^r$ dans la catégorie des représentations linéaires de G_K est exact, pleinement fidèle, d'image essentielle stable par sous-objets et quotients et indépendante du choix de l'uniformisante π.*

Le chapitre 7 étudie les conséquences de tout ce travail préliminaire. On commence par répondre à un cas particulier d'une conjecture formulée dans [9] (conjecture 2.2.6) :

Théorème 1.0.5. *Supposons $er < p-1$. Alors le foncteur T_{st} réalise une anti-équivalence de catégories entre la catégorie des modules fortement divisibles*[1] *et la catégorie des réseaux stables par Galois dans les $\mathbb{Q}_p$-représentations semi-stables de G_K à poids de Hodge Tate compris entre 0 et r.*

On donne ensuite une preuve du théorème 1.0.1.

Ce travail a été accompli dans le cadre de ma thèse de doctorat en mathématique que je prépare sous la direction de Christophe Breuil. Je tiens à le remercier vivement ici pour les conseils, les explications et les réponses qu'il a toujours su me fournir, ainsi que pour la relecture patiente des versions préliminaires de ce texte. Je tiens à remercier également Florian Herzig pour avoir relu en profondeur cet article, et pour ses commentaires toujours très appropriés.

2 Présentation des objets

Les objets introduits dans cette partie ne sont pas nouveaux et décrits plus en détail dans les articles [3] et [6]. La première de ces références n'étudie que le cas $e = 1$, et donc ne présente les objets que dans ce cas particulier.

On fixe maintenant et jusqu'à la fin de cet article un entier r positif ou nul vérifiant l'inégalité $er < p-1$. Les définitions que nous allons donner ont un sens pour tout entier $r < p-1$ mais certains théorèmes ne sont plus vérifiés lorsque $er \geqslant p-1$.

2.1 La catégorie $\underline{\mathcal{M}}^r$ et ses variantes

L'anneau S

On commence par définir un anneau que l'on va munir de structures supplémentaires. Bien que ces structures dépendent du corps K et de l'uniformisante π choisie, nous le notons simplement S par la suite.

Soit $W[u]$ l'anneau des polynômes en une indéterminée u à coefficients dans W. Soit $E(u)$ le polynôme minimal de l'élément π sur K_0, c'est un polynôme d'Eisenstein. On considère l'enveloppe aux puissances divisées de $W[u]$ par rapport à l'idéal principal engendré par $E(u)$ compatibles aux puissances divisées canoniques sur $pW[u]$. On rappelle que cela signifie que l'on ajoute formellement à l'anneau $W[u]$ les éléments $\frac{(E(u))^i}{i!}$. En tant qu'anneau, S est le complété p-adique de cette enveloppe aux puissances divisées. De façon plus terre à terre, S est la sous-W-algèbre de $K_0[\![u]\!]$ suivante :

$$S = \left\{ \sum_{i=0}^{\infty} w_i \frac{(E(u))^i}{i!},\ w_i \in W[u],\ \lim_{i\to\infty} w_i = 0 \right\}$$

[1]Voir le paragraphe 7.1 pour une définition.

ou encore :

$$S=\left\{\sum_{i=0}^{\infty} w_i \frac{u^i}{q(i)!},\ w_i \in W,\ \lim_{i\to\infty} w_i = 0\right\}$$

où $q(i)$ désigne le reste de la division euclidienne de i par e, e étant l'indice de ramification absolue de corps K, également le degré du polynôme $E(u)$.

On prolonge le Frobenius à l'anneau S en définissant l'application ϕ par :

$$\phi\left(\sum_{i=0}^{\infty} w_i \frac{u^i}{q(i)!}\right)=\sum_{i=0}^{\infty} \sigma(w_i) \frac{u^{pi}}{q(i)!}.$$

Il s'agit d'une application σ-semi-linéaire.

On munit en outre S de l'application W-linéaire N définie par :

$$N\left(\sum_{i=0}^{\infty} w_i \frac{u^i}{q(i)!}\right)=-\sum_{i=1}^{\infty} i w_i \frac{u^i}{q(i)!}.$$

Il s'agit d'une dérivation au sens classique mais pas de la dérivation classique par rapport à u, le degré du polynôme n'étant pas abaissé.

On munit finalement S d'une filtration : pour tout entier positif ou nul n, on définit $\mathrm{Fil}^n S$ comme le complété p-adique de l'idéal engendré par les éléments $\frac{(E(u))^i}{i!}$ pour $i \geqslant n$. On a donc :

$$\mathrm{Fil}^n S=\left\{\sum_{i=n}^{\infty} w_i \frac{(E(u))^i}{i!},\quad w_i \in W[u],\ \lim_{i\to\infty} w_i = 0\right\}.$$

Il est évident que $\mathrm{Fil}^0 S = S$, que $\mathrm{Fil}^n S \subset \mathrm{Fil}^{n-1} S$ et que $\bigcap_{n\in\mathbb{N}} \mathrm{Fil}^n S = 0$. On vérifie de plus certaines compatibilités avec les opérateurs définis précédemment : $N(\mathrm{Fil}^n S) \subset \mathrm{Fil}^{n-1} S$ et, pour $0 \leqslant n \leqslant p-1$, $\phi(\mathrm{Fil}^n S) \subset p^n S$. Ainsi, si $0 \leqslant n \leqslant p-1$, on pose $\phi_n = \frac{\phi}{p^n} : \mathrm{Fil}^n S \to S$. L'élément $\phi_1(E(u))$ est une unité de S, on le notera c par la suite.

Définition des catégories

On rappelle que r est un entier fixé vérifiant $er < p-1$. Un objet de la catégorie $\underline{\mathcal{M}}^r$ est la donnée :

1. d'un S-module $\mathcal{M}$ isomorphe à une somme directe (finie) de $S/p^n S$ pour des entiers n convenables ;
2. d'un sous-module $\mathrm{Fil}^r \mathcal{M}$ de $\mathcal{M}$ contenant $\mathrm{Fil}^r S \cdot \mathcal{M}$;
3. d'une flèche ϕ-semi-linéaire $\phi_r : \mathrm{Fil}^r \mathcal{M} \to \mathcal{M}$ vérifiant la condition :

   $$\phi_r(sx) = \frac{1}{c^r} \phi_r(s)\, \phi_r\left((E(u))^r x\right)$$

   pour tout élément $s \in \mathrm{Fil}^r S$ et tout élément $x \in \mathcal{M}$ et telle que $\mathrm{im}\, \phi_r$ engendre $\mathcal{M}$ en tant que S-module ;
4. d'une application W-linéaire $N : \mathcal{M} \to \mathcal{M}$ telle que :
   - pour tout $s \in S$ et tout $x \in \mathcal{M}$, $N(sx) = N(s)\,x + sN(x)$
   - $E(u)\, N(\mathrm{Fil}^r \mathcal{M}) \subset \mathrm{Fil}^r \mathcal{M}$

– le diagramme suivant commute :

$$\begin{tikzcd} \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "E(u)N"'] & \mathcal{M} \arrow[d, "cN"] \\ \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M} \end{tikzcd}$$

Une flèche entre deux objets $\mathcal{M}$ et $\mathcal{M}'$ de cette catégorie est un morphisme S-linéaire de $\mathcal{M}$ dans $\mathcal{M}'$ respectant la filtration et commutant aux applications ϕ_r et N.

On peut définir également la catégorie $\underline{\mathcal{M}}_0^r$. Il s'agit de la même chose sauf que l'on ne fait pas cas de l'application N, les objets sont donc la donnée des trois premiers points exposés précédemment.

2.2 Le foncteur vers les représentations galoisiennes

L'anneau A_{cris}

Soit R l'anneau limite projective du diagramme :

$$\mathcal{O}_{\bar{K}}/p\mathcal{O}_{\bar{K}} \leftarrow \mathcal{O}_{\bar{K}}/p\mathcal{O}_{\bar{K}} \leftarrow \ldots \leftarrow \mathcal{O}_{\bar{K}}/p\mathcal{O}_{\bar{K}} \leftarrow \ldots \leftarrow$$

les applications de transition étant à chaque fois l'élévation à la puissance p. Un élément de R est une suite $\left(u^{(k)}\right)_{k\geqslant 1}$ d'éléments de $\mathcal{O}_{\bar{K}}/p\mathcal{O}_{\bar{K}}$ telle que pour tout entier k, $\left(u^{(k+1)}\right)^p = u^{(k)}$.

On considère $W(R)$ l'anneau des vecteurs de Witt à coefficients dans R et l'application suivante :

$$\begin{array}{rccc} \hat{\theta}: & W(R) & \to & \mathcal{O}_{\mathbb{C}_p} \\ & (a_0, a_1, \ldots, a_n, \ldots) & \mapsto & \sum_{n\geqslant 0} p^n \hat{x}_n^{(n)} \end{array}$$

où $\mathbb{C}_p$ désigne le complété p-adique de $\bar{K}$ et où $\hat{x}_n^{(n)}$ est la limite quand m tend vers l'infini d'une suite $(\hat{a}_n^{(n+m)})^{p^m}$, $\hat{a}_i^{(j)} \in \mathcal{O}_{\bar{K}}$ désignant un relevé quelconque de $a_i^{(j)}$.

On montre[2] que le noyau de $\hat{\theta}$ est l'idéal principal de $W(R)$ engendré par l'élément $\xi = [\underline{p}] - p$, où $[\underline{p}]$ est le représentant de Teichmüller de $\underline{p} \in R$ défini par $\underline{p} = (p_1, \ldots, p_n, \ldots)$, les p_n formant un système compatible de racines p^n-ièmes de p. L'anneau A_{cris} s'obtient en introduisant des puissances divisées en ξ, et en complètant p-adiquement :

$$A_{\mathrm{cris}} = \left\{ \sum_{i\geqslant 0} a_i \frac{\xi^i}{i!}\,,\ a_i \in W(R)\,,\ a_i \longrightarrow 0 \right\}.$$

L'anneau A_{cris} hérite d'un Frobenius ϕ et d'une action du groupe de Galois G_K définis *via* leur action sur $W(R)$. On munit également A_{cris} d'une filtration décroissante définie de la façon suivante :

$$\mathrm{Fil}^n A_{\mathrm{cris}} = \left\{ \sum_{i\geqslant n} a_i \frac{\xi^i}{i!}\,,\ a_i \in W(R)\,,\ a_i \longrightarrow 0 \right\} \subset A_{\mathrm{cris}}.$$

[2]Pour une preuve simple, voir le paragraphe II.2.2 de [2]

L'anneau $\hat{A}_{\mathrm{st}}$

L'anneau $\hat{A}_{\mathrm{st}}$ s'obtient en complétant p-adiquement la PD-algèbre polynomiale $A_{\mathrm{cris}}\langle X\rangle$:

$$\hat{A}_{\mathrm{st}} = \left\{ \sum_{i\geqslant 0} a_i \frac{X^i}{i!}\ ,\ a_i \in A_{\mathrm{cris}},\ a_i \longrightarrow 0 \right\}.$$

On étend le Frobenius et l'action de Galois à $\hat{A}_{\mathrm{st}}$ de la façon suivante. On pose $\phi(X) = (1+X)^p - 1$. Soit $(\pi_1, \pi_2, \ldots, \pi_n, \ldots)$ un système compatible de racines p^n-ièmes de l'uniformisante[3] π et soit $g \in G_K$. Pour tout entier n, il existe $\varepsilon_n(g)$ une racine p^n-ième de l'unité telle que $g(\pi_n) = \varepsilon_n(g)\pi_n$. La suite $[\varepsilon_n(g)]$ définit un élément $[\underline{\varepsilon}(g)] \in A_{\mathrm{cris}}$. L'élément g agit sur X par $g(X) = [\underline{\varepsilon}(g)]X + [\underline{\varepsilon}(g)] - 1$. La filtration sur $\hat{A}_{\mathrm{st}}$ est obtenue en faisant le produit de convolution de la filtration de A_{cris} par la filtration naturelle donnée par les puissances divisées en X :

$$\mathrm{Fil}^n \hat{A}_{\mathrm{st}} = \left\{ \sum_{i\geqslant 0} a_i \frac{X^i}{i!}\ ,\ a_i \in \mathrm{Fil}^{n-i} A_{\mathrm{cris}},\ a_i \longrightarrow 0 \right\} \subset \hat{A}_{\mathrm{st}}$$

avec la convention $\mathrm{Fil}^k A_{\mathrm{cris}} = A_{\mathrm{cris}}$ si $k < 0$. Pour $n \leqslant p-1$, on a $\phi(\mathrm{Fil}^n \hat{A}_{\mathrm{st}}) \subset p^n \hat{A}_{\mathrm{st}}$ et on pose $\phi_n = \frac{\phi}{p^n}{}_{|\mathrm{Fil}^n \hat{A}_{\mathrm{st}}}$.

On munit finalement $\hat{A}_{\mathrm{st}}$ d'un opérateur de monodromie N défini comme l'unique dérivation continue A_{cris}-linéaire telle que $N(X) = 1 + X$.

L'anneau $\hat{A}_{\mathrm{st}}$ n'est pas sans lien avec S : dans [4], Breuil prouve que le morphisme de W-algèbres $S \to \hat{A}_{\mathrm{st}}$, $u \mapsto \frac{[\underline{\pi}]}{1+X}$ ($[\underline{\pi}]$ désigne le représentation de Teichmüller de $\underline{\pi} = (\bar{\pi}_1, \ldots, \bar{\pi}_n, \ldots) \in R$, $\bar{\pi}_i$ étant la réduction modulo p de π_i) identifie S avec l'ensemble $\hat{A}_{\mathrm{st}}^{G_K}$ des invariants de $\hat{A}_{\mathrm{st}}$ sous l'action du groupe de Galois. En outre, ce morphisme fait de $\hat{A}_{\mathrm{st}}$ un S-module. Toutefois, $\hat{A}_{\mathrm{st}}$ ne vérifie pas les propriétés nécessaires pour être un objet de la catégorie $\underline{\mathcal{M}}^r$.

Le foncteur T_{st}

On pose $\hat{A}_{\mathrm{st},\infty} = \hat{A}_{\mathrm{st}} \otimes_W K_0/W$. L'action du groupe de Galois, le Frobenius, la filtration et la monodromie s'étendent à $\hat{A}_{\mathrm{st},\infty}$ car $\mathrm{Fil}^n \hat{A}_{\mathrm{st}} \cap p^r \hat{A}_{\mathrm{st}} = p^r \mathrm{Fil}^n \hat{A}_{\mathrm{st}}$. En outre, pour la même raison, si $r < p-1$, l'objet $\hat{A}_{\mathrm{st},\infty}$ hérite de ϕ_r. Ce n'est toutefois pas un objet de la catégorie $\underline{\mathcal{M}}^r$: il n'est pas de longueur finie en tant que S-module, et l'image de ϕ_r n'engendre pas tout l'espace. Il est quand même légitime de considérer l'ensemble des morphismes d'un objet $\mathcal{M}$ de $\underline{\mathcal{M}}^r$ dans $\hat{A}_{\mathrm{st},\infty}$ et on définit :

$$T_{\mathrm{st}}(\mathcal{M}) = \mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st},\infty})$$

le Hom précédent signifiant que l'on prend les morphismes compatibles au Fil^r, au Frobenius et à l'opération de monodromie. Cet ensemble est naturellement une $\mathbb{Z}_p$-représentation galoisienne de torsion, tuée par la puissance de p qui annule $\mathcal{M}$.

Notre but est principalement d'étudier le foncteur T_{st}, et pour ce faire, nous allons quasiment toujours procéder par dévissage en regardant dans un premier temps les objets tués par p, que nous étudions dans le paragraphe suivant.

---

[3] Ainsi l'anneau $\hat{A}_{\mathrm{st}}$ dépend *a priori* du choix de ce système compatible de racines. Cependant, on prouve que ce n'est pas le cas.

2.3 Les objets tués par p

Les catégories $\widetilde{\underline{\mathcal{M}}}^r$

L'anneau important ici est $k[u]/u^{ep}$ qui est relié à S/pS grâce à l'application de projection $\sigma : S/pS \to k[u]/u^{ep}$ définie par $\sigma(u) = u$ et $\sigma(\frac{u^{ei}}{i!}) = 0$ pour $i \geqslant p$. Sur cet anneau, on définit une filtration par $\mathrm{Fil}^n k[u]/u^{ep} = u^{en} k[u]/u^{ep}$, un Frobenius ϕ par $\phi(\sum w_i u^i) = \sum w_i^p u^{ip}$ (pour $w_i \in k$) et un opérateur de monodromie N comme l'unique dérivation k-linéaire vérifiant $N(u) = -u$

On définit ensuite la catégorie $\widetilde{\underline{\mathcal{M}}}^r$: les objets sont les données des quatre points qui suivent :

1. un $k[u]/u^{ep}$-module $\mathcal{M}$ libre de rang fini ;
2. un sous-module $\mathrm{Fil}^r\mathcal{M}$ de $\mathcal{M}$ contenant $\mathrm{Fil}^r k[u]/u^{ep} \cdot \mathcal{M} = u^{er}\mathcal{M}$;
3. une flèche ϕ-semi-linéaire $\phi_r : \mathrm{Fil}^r\mathcal{M} \to \mathcal{M}$ telle que l'image de ϕ_r engendre $\mathcal{M}$ en tant que $k[u]/u^{ep}$-module ;
4. une application k-linéaire $N : \mathcal{M} \to \mathcal{M}$ telle que :
   - pour tout $\lambda \in k[u]/u^{ep}$ et tout $x \in \mathcal{M}$, $N(\lambda x) = N(\lambda)x + \lambda N(x)$
   - $u^e N(\mathrm{Fil}^r\mathcal{M}) \subset \mathrm{Fil}^r\mathcal{M}$
   - le diagramme suivant commute :

$$\begin{tikzcd} \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "u^e N"'] & \mathcal{M} \arrow[d, "c_\pi N"] \\ \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M} \end{tikzcd}$$

   où c_π est la réduction de c dans $k[u]/u^{ep}$.

On introduit également la catégorie $\widetilde{\underline{\mathcal{M}}}_0^r$ définie comme $\widetilde{\underline{\mathcal{M}}}^r$ sauf que l'on oublie la donnée de l'opérateur N.

On peut comparer les objets de $\underline{\mathcal{M}}^r$ tués par p et ceux de $\widetilde{\underline{\mathcal{M}}}^r$. Si $\mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r$ tué par p, c'est naturellement un S/pS-module (même libre de rang fini), et on peut donc considérer le produit tensoriel $T(\mathcal{M}) = \mathcal{M} \otimes_{(\sigma)} k[u]/u^{ep}$ qui hérite d'une filtration, d'un Frobenius et d'une monodromie et dont on vérifie qu'il est dans $\widetilde{\underline{\mathcal{M}}}^r$. Cette construction définit un foncteur T allant de la sous-catégorie pleine de $\underline{\mathcal{M}}^r$ formée des objets tués par p dans la catégorie $\widetilde{\underline{\mathcal{M}}}^r$.

Proposition 2.3.1. *Le foncteur T défini précédemment est une équivalence de catégories.*

Démonstration. Elle est en tout point similaire à celle donnée pour la proposition 2.2.2.1 de [3]. □

On obtient ainsi une description plus simple des objets de $\underline{\mathcal{M}}^r$ tués par p, les objets de $\widetilde{\underline{\mathcal{M}}}^r$ pouvant être vus comme des k-espaces vectoriels de dimension finie.

Description du quotient $\hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}}$

Soit $\mathcal{M}$ un objet de $\underline{\mathcal{M}}^r$ tel que $p\mathcal{M} = 0$. Alors $T_{\mathrm{st}}(\mathcal{M}) = \mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st}}/p)$. Nous allons dans un premier temps décrire explicitement le quotient $\hat{A}_{\mathrm{st}}/p$.

On rappelle que l'on a défini deux éléments de R qui sont $\underline{p}$ et $\underline{\pi}$. On a le résultat suivant (voir paragraphe 3.7 de [15]) :

Lemme 2.3.2. *Avec les notations précédentes, A_{cris}/pA_{cris} s'identifie à l'enveloppe aux puissances divisées R^{PD} de R par rapport à l'idéal principal engendré par $\underline{p}$. En outre, on peut également identifier cet anneau à $R[X_i]/\left(\underline{p}^p, X_i^p\right)_{i\geqslant 1}$, l'isomorphisme envoyant X_i sur la p^i-ième puissance divisée $\frac{[\underline{p}]^{p^i}}{(p^i)!} \in A_{cris}/pA_{cris}$.*

La première projection $R \to \mathcal{O}_{\bar{K}}/p$ induit un isomorphisme $R/\underline{p}^p R \simeq \mathcal{O}_{\bar{K}}/p$. On déduit du lemme précédent que $A_{\mathrm{cris}}/pA_{\mathrm{cris}}$ s'identifie canoniquement à $\mathcal{O}_{\bar{K}}/p\,[X_i]/X_i^p$, i décrivant l'ensemble des entiers strictement positifs. Finalement on voit que $\hat{A}_{\mathrm{st}}/p$ s'identifie à l'anneau suivant :

$$\left(\mathcal{O}_{\bar{K}}[X_i]\langle X\rangle\right)/\left(p, X_i^p\right)_{i\geqslant 1}.$$

On rappelle que p_1 est une racine p-ième de p. *Via* les identifications précédentes, et pour $n < p$, $\mathrm{Fil}^n(\hat{A}_{\mathrm{st}}/p)$ est le sous-$\mathcal{O}_{\bar{K}}/p$-module de $\hat{A}_{\mathrm{st}}/p$ engendré par les $p_1^{n-i}\frac{X^i}{i!}$ (pour $i \leqslant n$), les $\frac{X^i}{i!}$ (pour $i > n$) et les X_i (pour $i \geqslant 1$). On a $\phi_r(X_i) = 0$ et $\phi_1(X) = \frac{(1+X)^p-1}{p} = Y$. La monodromie est l'unique dérivation $(A_{\mathrm{cris}}/pA_{\mathrm{cris}})$-linéaire et continue N qui envoie $\frac{X^i}{i!}$ sur $(1+X)\frac{X^{i-1}}{(i-1)!}$.

Description du foncteur T_{st}

Nous cherchons à faire le transport *via* le foncteur T pour voir comment le foncteur T_{st} se réalise à travers la catégorie $\widetilde{\underline{\mathcal{M}}}^r$. L'objet à calculer est le produit tensoriel $\hat{A}_{\mathrm{st}}/p \otimes_{S/pS} k[u]/u^{ep}$. Pour cela, on définit $\hat{A} = (O_{\bar{K}}/p)\langle X\rangle$. On a un morphisme de $\mathcal{O}_{\bar{K}}/p$-modules :

$$\mathrm{pr} : \hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}} \to \hat{A}$$

donné, *via* la description précédente, par $\mathrm{pr}(X) = X$ et $\mathrm{pr}(X_i) = 0$ pour tout i. On vérifie que pr est S/pS-linéaire. On définit également $\mathrm{Fil}^r\hat{A} = \mathrm{pr}(\mathrm{Fil}^r\hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}})$ et on vérifie que l'on peut définir une unique application $\phi_r : \mathrm{Fil}^r\hat{A} \to \hat{A}$ (resp. $N : \hat{A} \to \hat{A}$) vérifiant $\phi_r \circ \mathrm{pr} = \mathrm{pr} \circ \phi_r$ (resp. $N \circ \mathrm{pr} = \mathrm{pr} \circ N$). Notons qu'il faut faire attention lorsque l'on veut effectuer des calculs avec ϕ_r : avant d'élever à la puissance p, il faut toujours relever l'élément dans $\mathrm{Fil}^r\hat{A}_{\mathrm{st}}$. Par exemple, dans $A_{\mathrm{cris}}/pA_{\mathrm{cris}}$, on a $\phi_1(p_1) = X_1 - 1$ et donc si $x \in \mathcal{O}_{\bar{K}}/p$ est un multiple de π_1^{er}, on obtient $\phi_r(x) = (-1)^r\frac{x^p}{p^r}$, avec un signe *a priori* inattendu.

De plus, on a une inclusion S/pS-linéaire :

$$i : k[u]/u^{ep} \to \hat{A}$$

définie par $i(1) = 1$. On peut former le produit :

$$\mathrm{pr}\cdot i : \hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}} \otimes_{S/pS} k[u]/u^{ep} \to \hat{A}.$$

Lemme 2.3.3. *L'application précédente est un isomorphisme qui respecte les structures.*

Démonstration. La surjectivité et le respect des structures sont immédiats. Comme $\sigma : S/pS \to k[u]/u^{ep}$ est surjectif, tout élément de $\hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}} \otimes_{S/pS} k[u]/u^{ep}$ s'écrit $x \otimes 1$ avec $x \in \hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}}$. Pour vérifier l'injectivité, il suffit donc de voir que $(\ker \mathrm{pr}) \otimes_{S/pS} k[u]/u^{ep} = 0$ mais ceci résulte directement de :

$$X_i \otimes 1 = \frac{\pi_1^{ep^i}}{(p^i)!} \otimes 1 = \frac{u^{ep^i}}{(p^i)!} \otimes 1 = 1 \otimes \sigma\left(\frac{u^{ep^i}}{(p^i)!}\right) = 0.$$

□

On construit une application :

$$\mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st},\infty}) \to \mathrm{Hom}(T(\mathcal{M}), \hat{A})$$

déduite de la tensorisation par $k[u]/u^{ep}$ au-dessus de S/pS (et où tous les morphismes doivent commuter aux structures supplémentaires).

Lemme 2.3.4. *L'application précédente est un isomorphisme de $\mathbb{Z}_p$-modules galoisiens.*

Démonstration. Commençons par l'injectivité. Soit $\psi \in \mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st},\infty})$ induisant par tensorisation l'application nulle $T(\mathcal{M}) \to \hat{A}$. Le diagramme suivant est commutatif :

$$\begin{tikzcd} \mathcal{M} \arrow[r, "\psi"] \arrow[d, "x \mapsto 1\otimes x"'] & \hat{A}_{\mathrm{st}}/p\hat{A}_{\mathrm{st}} \arrow[d, "\mathrm{pr}"] \\ T(\mathcal{M}) \arrow[r, "0"] & \hat{A} \end{tikzcd}$$

d'où $\mathrm{im}\,\psi \subset \ker \mathrm{pr}$. On vérifie facilement que $\phi_r(\ker \mathrm{pr}) = 0$. Comme ψ commute à ϕ_r et $\phi(\mathrm{Fil}^r\mathcal{M})$ engendre $\mathcal{M}$, on en déduit $\psi = 0$. L'application $\mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st},\infty}) \to \mathrm{Hom}(T(\mathcal{M}), \hat{A})$ est injective.

Pour la surjectivité, notons $T(\mathcal{M})_0$ l'image de ϕ_r sur $T(\mathcal{M})$. La preuve de la proposition 2.2.2.1 de [3] fournit l'isomorphisme :

$$\mathcal{M} \simeq T(\mathcal{M})_0 \otimes_{k[u^p]/u^{ep}} S/pS.$$

Soit $\bar{\psi} : T(\mathcal{M}) \to \hat{A}$. D'après l'isomorphisme précédent, elle induit une application S/pS-linéaire $\mathcal{M} \to \hat{A} \otimes_{k[u^p]/u^{ep}} S/pS$, et ce dernier module s'envoie de façon naturelle dans $\hat{A}_{\mathrm{st},\infty}$. On vérifie finalement que l'application composée commute à Fil^r, ϕ_r et N et relève $\bar{\psi}$. □

Description de l'anneau $\hat{A}$

Lemme 2.3.5. *Soit R un anneau dans lequel tous les entiers premiers à p sont inversibles. Alors on a un isomorphisme :*

$$(R[X']\langle Y\rangle)/(X'^p - 1, p) \longrightarrow (R\langle X\rangle)/p$$

envoyant X' sur $X+1$ et $\frac{Y^i}{i!}$ sur $\frac{1}{i!}\left(\frac{(X+1)^p-1}{p}\right)^i$.

Démonstration. D'abord, l'application précédente, disons ψ, est bien définie : on a $(1+X)^p \equiv 1 + X^p \equiv 1 \pmod{p}$.

Pour prouver que ψ est un isomorphisme, on remarque que chacun des objets intervenant est un R/p-module libre et que ψ est R/p-linéaire. Une base du module source est donnée par la famille $\left(X'^i \cdot \frac{Y^j}{j!}\right)_{0\leqslant i\leqslant p-1,\, j\geqslant 0}$. Le module but admet pour base la famille $\left(\frac{X^n}{n!}\right)_{n\geqslant 0}$. L'image par ψ de l'élément $X'^i \cdot \frac{Y^j}{j!}$ est :

$$\psi\left(X'^i \cdot \frac{Y^j}{j!}\right) = (1+X)^i \cdot \frac{\left(\frac{(1+X)^p-1}{p}\right)^j}{j!}.$$

Le terme dominant de cette dernière expression est $\frac{X^{pj+i}}{p^j j!}$ et si on note v_p la valuation p-adique normalisée par $v_p(p) = 1$, on a :

$$v_p((pj+i)!) = j + v_p(j!) = v_p\left(p^j j!\right)$$

puisque $i < p$. Comme les entiers premiers à p sont par hypothèse inversibles dans R, l'égalité précédente assure qu'il existe un élément inversible $\alpha \in R/p$ tel que $p^j j! = \alpha (pj+i)!$. Ainsi la « matrice » représentant l'application ψ dans les bases données ci-dessus est triangulaire et les termes diagonaux sont tous inversibles. Cela prouve que ψ est bijective. $\square$

L'anneau $\mathcal{O}_{\bar{K}}$ vérifie les hypothèses du lemme que l'on vient de prouver ; on obtient donc le corollaire suivant qui donne une nouvelle description relativement explicite de l'anneau $\hat{A}$:

Corollaire 2.3.6. *On a un isomorphisme :*

$$\hat{A} \to \left(\mathcal{O}_{\bar{K}}[X'] \langle Y \rangle\right) / \left(X'^p - 1, p\right)$$

En outre l'opérateur de monodromie s'exprime simplement sur cette description : on a $N(X') = X'$ *et* $N\left(\frac{Y^i}{i!}\right) = \frac{Y^{i-1}}{(i-1)!}$.

Action de Galois sur l'anneau $\hat{A}$.

On va déterminer l'action de Galois sur les éléments X' et Y. Pour X' c'est facile puisque par définition on a $g(X') = \varepsilon(g) X'$ pour tout $g \in G_K$.

Pour Y, on pourrait être tenté d'écrire :

$$g(Y) = \frac{\varepsilon(g)^p (1+X)^p - 1}{p} = Y$$

mais on n'a pas le droit de faire ce calcul à cause de la division par p. Ce qu'il faut, c'est choisir un relevé de Y dans $\hat{A}_{\text{st}}$, calculer l'action de Galois sur ce relevé et voir quel élément correspond dans $\hat{A}$.

Comme relevé, on pourrait choisir $\frac{(1+X)^p-1}{p}$ mais on choisit d'abord :

$$\log(1+X) = X - \frac{X^2}{2} + \frac{X^3}{3} + \ldots + (-1)^{i-1} \frac{X^i}{i} + \ldots \in \hat{A}_{\text{st}}$$

Soit $g \in G_K$. On a $g\log(1+X) = \log(g(1+X)) = \log([\underline{\varepsilon}(g)](1+X)) = g(Y) = Y + \hat{t}(g)$ où :

$$\hat{t}(g) = \log([\underline{\varepsilon}(g)]) = [\underline{\varepsilon}(g)] - \frac{[\underline{\varepsilon}(g)]^2}{2} + \frac{[\underline{\varepsilon}(g)]^3}{3} + \ldots + (-1)^{i-1} \frac{[\underline{\varepsilon}(g)]^i}{i} + \ldots \in A_{\text{cris}}.$$

Nous allons déterminer l'image $t(g)$ de $\hat{t}(g)$ dans $\hat{A}$. Remarquons que comme $\hat{t}(g) \in A_{\text{cris}}$, on a simplement $t(g) \in \mathcal{O}_{\bar{K}}/p$. Nous allons prouver qu'il s'agit d'une racine $(p-1)$-ième de $(-p)$.

Lemme 2.3.7. *Avec les notations précédentes,* $t(g)$ *est l'image dans* $\mathcal{O}_{\bar{K}}/p$ *de :*

$$-\frac{(\varepsilon(g)-1)^p}{p}$$

où $\varepsilon(g) \in \mathcal{O}_{\bar{K}}$ *est la racine* p*-ième de l'unité telle que* $g(\pi_1) = \varepsilon(g)\pi_1$.

Démonstration. Il est plus pratique ici d'écrire les choses sous la forme suivante :

$$Y - \frac{X^p}{p} = \frac{X'^p - 1 - (X' - 1)^p}{p}$$

et de développer :

$$Y - \frac{X^p}{p} = a_1 X' + a_2 X'^2 + \ldots + a_{p-1} X'^{p-1}$$

avec $a_i = \frac{(-1)^i \binom{p}{i}}{p}$. En appliquant g, on obtient :

$$gY - g\left(\frac{X^p}{p}\right) = a_1 [\varepsilon(g)] X' + a_2 [\varepsilon(g)]^2 X'^2 + \ldots + a_{p-1} [\varepsilon(g)]^{p-1} X'^{p-1}$$

d'où dans $\hat{A}$:

$$t(g) \equiv g\left(\frac{X^p}{p}\right) - \frac{(\varepsilon(g) - 1)^p}{p} \pmod X$$

Comme on sait que $t(g) \in \mathcal{O}_{\bar{K}}/p$, il suffit pour conclure de prouver que $g\left(\frac{X^p}{p}\right)$ est nul modulo X. Mais dans $\hat{A}_{\mathrm{st}}$, on a $g\left(\frac{X^p}{p}\right) = \frac{([\varepsilon(g)](1+X)-1)^p}{p}$ et donc modulo X, on obtient :

$$g\left(\frac{X^p}{p}\right) \equiv \frac{([\underline{\varepsilon}(g)] - 1)^p}{p} \pmod X$$

On conclut en remarquant que $[\underline{\varepsilon}(g)] - 1 \in \ker \hat{\theta}$. □

Lemme 2.3.8. *L'élément $t(g)$ est soit nul soit égal dans $\mathcal{O}_{\bar{K}}/p$ à la réduction modulo p d'une racine $(p-1)$-ième de $(-p)$ dans $\mathcal{O}_{\bar{K}}$.*

Démonstration. Supposons $t(g) \neq 0$. Prouvons d'abord que $t(g)^{p-1} \equiv -p \pmod{p^2}$. D'après le lemme 2.3.7, cela revient à montrer que :

$$(\varepsilon(g) - 1)^{p(p-1)} \equiv -p^p \pmod{p^{p+1}}.$$

Modulo $1 + X + \ldots + X^{p-1}$, le polynôme $(X-1)^{p-1}$ s'écrit $a_0 + a_1 X + \ldots + a_{p-2} X^{p-2}$ avec $a_i = (-1)^i \binom{p-1}{i} - 1$. On vérifie que a_i est un multiple de p et on pose $b_i = \frac{a_i}{p}$. En élevant à la puissance p, on obtient :

$$(X-1)^{p(p-1)} \equiv p^p \left(b_0 + b_1 X + \ldots + b_{p-2} X^{p-2}\right)^p \pmod{1 + X + \ldots + X^{p-1}}$$

d'où

$$(X-1)^{p(p-1)} \equiv p^p (b_0 + b_1 + \ldots + b_{p-2}) \pmod{1 + X + \ldots + X^{p-1}, p^{p+1}}.$$

Il ne reste plus qu'à vérifier que $b_0 + b_1 + \ldots + b_{p-2} = -1$ pour conclure.

Notons $\eta_1, \ldots, \eta_{p-1} \in \mathcal{O}_{\bar{K}}$ les racines $(p-1)$-ièmes de $(-p)$. On a :

$$(t(g) - \eta_1) \ldots (t(g) - \eta_{p-1}) = 0 \pmod{p^2}$$

ou encore $v(t(g) - \eta_1) + \ldots + v(t(g) - \eta_{p-1}) \geqslant 2e$. Il existe donc i tel que $v(t(g) - \eta_i) \geqslant \frac{2e}{p-1}$. De plus pour tout i, $v(\eta_i) = \frac{e}{p-1}$ et pour $i \neq j$, $v(\eta_i - \eta_j) = \frac{e}{p-1}$ car deux racines $(p-1)$-ièmes de l'unité sont encore distinctes dans le corps résiduel. Il vient, si $j \neq i$, $v(t(g) - \eta_j) = v((t(g) - \eta_i) + (\eta_i - \eta_j)) = \frac{e}{p-1}$, puis $v(t(g) - \eta_i) \geqslant \left(2 - \frac{p-2}{p-1}\right) e \geqslant e$. Cela conclut. □

3 Généralités sur les catégories $\underline{\mathcal{M}}^r$ et $\widetilde{\underline{\mathcal{M}}}^r$

Outre de nombreuses explicitations, cette partie a pour but de démontrer les deux résultats suivants. D'une part les catégories $\underline{\mathcal{M}}^r$ définies précédemment ne dépendent pas du choix d'une uniformisante π. D'autre part, ces catégories sont abéliennes et même artiniennes.

3.1 Indépendance du choix de l'uniformisante

Considérons π et π' deux uniformisantes de K. Notons respectivement $E(u)$ et $E'(u)$ les polynômes minimaux de π et π'.

Soit $P(u)$ un polynôme à coefficients dans W tel que $P(\pi) = \pi'$ et $P(0) = 0$. On définit une application $\nu : S \to S$ en posant $\nu(s) = s \circ P$. C'est un morphisme d'anneaux, bijectif. Il n'est par contre compatible ni au Frobenius, ni à l'opérateur de monodromie, et nous allons dans un premier temps voir comment ν se comporte vis-à-vis de ces opérateurs.

Plongeons S dans $T = K_0 [\![u]\!]$ et prolongeons les opétateurs ϕ et N à T. Ils vérifient la relation $N\phi = p\phi N$. De même la bijection ν s'étend en une bijection de T. Notons finalement $\mathfrak{m}$ l'idéal maximal de S, c'est l'idéal engendré par p, u et $\frac{u^{ei}}{i!}$ pour $i \geqslant 1$.

Lemme 3.1.1. *Soit $t \in \mathfrak{m}$. L'application de T dans T définie par :*

$$x \mapsto \sum_{i=0}^{\infty} \frac{t^i}{i!} N^i(x)$$

est l'unique morphisme d'anneaux qui envoie u sur $u \exp(-t)$.

Démonstration. Puisque $t \in \mathfrak{m}$, on n'a aucun souci de convergence dans T. En outre, comme $N(u) = -u$, il vient $N^i(u) = (-1)^i u$ et donc u est bien envoyé sur $u \exp(-t)$.

Il reste à vérifier que l'on a bien affaire à un morphisme d'anneaux. La stabilité par addition est immédiate. Soient x et y dans T, calculons :

$$\begin{aligned}
\sum_{i=0}^{\infty} \frac{t^i}{i!} N^i(xy) &= \sum_{i=0}^{\infty} \frac{t^i}{i!} \sum_{k+l=i} \binom{i}{k} N^k(x) N^l(y) \\
&= \sum_{k,l \geqslant 0} \frac{t^i}{k!l!} N^k(x) N^l(y) \\
&= \left(\sum_{k=0}^{\infty} \frac{t^k}{k!} N^k(x) \right) \cdot \left(\sum_{l=0}^{\infty} \frac{t^l}{l!} N^l(y) \right)
\end{aligned}$$

ce qui conclut la preuve. □

Lemme 3.1.2. *Il existe un (unique) élément $t \in \mathfrak{m}$ tel que l'application $\nu^{-1} \circ \phi \circ \nu : S \to S$ soit donnée par la formule :*

$$x \mapsto \sum_{i=0}^{\infty} \frac{t^i}{i!} N^i \circ \phi(x).$$

Démonstration. Faisons les calculs dans T après avoir vérifié que si une suite d'éléments de S admet une limite dans S, alors elle converge aussi dans T, et vers la même limite.

Regardons d'abord le cas où P s'écrit $uH(u)$ avec $H \in 1 + \mathfrak{m}$. Dans ces conditions on est capable de définir $\log H \in T$. D'autre part, notons $uS(u)$ l'image réciproque de u par ν.

Notons $H^{(\phi)}$ le polynôme déduit de H en appliquant ϕ à chacun de ses coefficients : on a $\phi(H)(u) = H^{(\phi)}(u^p)$.

Dans l'anneau T, on a alors les égalités suivantes :

$$\nu(x) = \sum_{i=0}^{\infty} \frac{(-\log H(u))^i}{i!} N^i(x) \quad \text{et} \quad \nu^{-1}(x) = \sum_{i=0}^{\infty} \frac{(-\log S(u))^i}{i!} N^i(x).$$

Un calcul donne :

$$\nu^{-1} \circ \phi \circ \nu(x) = \sum_{i=0}^{\infty} \frac{\left[-\log\left(H^{(\phi)}(u^p S(u)^p)\right)\right]^i}{p^i i!} \nu^{-1} \circ N^i(\phi(x)).$$

On a d'autre part :

$$\nu^{-1} \circ N^i(\phi(x)) = \sum_{j=0}^{\infty} \frac{(-\log S(u))^j}{j!} N^{i+j}(\phi(x))$$

et donc en regroupant :

$$\nu^{-1} \circ \phi \circ \nu(x) = \sum_{i,j \geqslant 0} \frac{\left[-\log\left(H^{(\phi)}(u^p S(u)^p)\right)\right]}{p^i i!} \frac{(-\log S(u))^j}{j!} N^{i+j}(\phi(x))$$

ce que l'on réduit, grâce à la formule du binôme, en :

$$\nu^{-1} \circ \phi \circ \nu(x) = \sum_{i=0}^{\infty} \frac{1}{i!} \left[\frac{-\log H^{(\phi)}(u^p S(u)^p)}{p} - \log S(u)\right]^i N^i(\phi(x)).$$

On voit sur cette dernière écriture que l'on a trouvé un candidat pour t. Il se réécrit sous la forme plus sympatique suivante :

$$t = -\frac{1}{p} \log\left[S(u)^p H^{(\phi)}(u^p S(u)^p)\right]$$

Mais par définition de S et de H, on a $S(u) H(uS(u)) = 1$ et donc en appliquant ϕ et en regardant modulo p, on trouve $S(u)^p H^{(\phi)}(u^p S(u)^p) \equiv 1 \pmod p$. On en déduit que $t \in S$ et vérifie les conditions du lemme.

Si P n'est pas de la forme précédente, on peut toujours décomposer $\nu : S \to S \to S$ où la première flèche ν_0 est de la forme précédente et la seconde un morphisme d'anneaux envoyant u sur $[\lambda] u$, où $[\lambda]$ est le représentant de Teichmüller d'un $\lambda \in k$. On vérifie que l'on a le diagramme commutatif suivant :

$$\begin{tikzcd} S \arrow[r, "\nu_0"'] \arrow[rr, bend left, "\nu"] \arrow[d, "\nu^{-1}\phi\nu = \nu_0^{-1}\phi\nu_0"'] & S \arrow[r] \arrow[d, "\phi"] & S \arrow[d, "\phi"] \\ S \arrow[r, "\nu_0"'] & S \arrow[r] & S \end{tikzcd}$$

On est donc ramené au même problème avec ν_0, déjà traité. □

Lemme 3.1.3. *Il existe un (unique) élément $n \in S$ tel que l'application $\nu^{-1} \circ N \circ \nu : S \to S$ soit donnée par la formule :*

$$x \mapsto nN(x)$$

Démonstration. Rappelons que l'application ν était donnée par $x \mapsto x \circ P$, et que l'on peut décrire N *via* la formule $N(s) = -us'$ où s' désigne la dérivée usuelle de s (par rapport à u).

On peut alors calculer :

$$\nu^{-1} \circ N \circ \nu(x) = \nu^{-1}[N(x \circ P)] = \nu^{-1}[-uP' \cdot (x' \circ P)]$$

D'autre part, on a :

$$\nu(N(x)) = \nu(-ux') = -P \cdot (x' \circ P)$$

d'où :

$$\nu^{-1} \circ N \circ \nu(x) = \nu^{-1}\left(\frac{-uP'(u)}{P(u)}\right) N(x)$$

et on a ainsi un candidat pour n. Or $\nu^{-1}(P(u)) = u$ par définition et par ν^{-1}, u s'envoie sur un multiple de u : $n = \nu^{-1}\left(\frac{-uP'(u)}{P(u)}\right) \in S$ et convient. $\square$

Construction du foncteur

Notons $\underline{\mathcal{M}}^r_\pi$ (resp. $\underline{\mathcal{M}}^r_{\pi'}$) la catégorie obtenue en choisissant π (resp. π') comme uniformisante de K. On souhaite construire un foncteur (qui va s'avérer être une équivalence de catégories) entre les catégories $\underline{\mathcal{M}}^r_\pi$ et $\underline{\mathcal{M}}^r_{\pi'}$. Notons que si $r = 0$, les catégories $\underline{\mathcal{M}}^0_\pi$ et $\underline{\mathcal{M}}^0_{\pi'}$ sont identiques. On peut supposer $r > 0$ et donc $p > 2$ (puisque $er < p - 1$).

Soit $\mathcal{M}$ un objet de $\underline{\mathcal{M}}^r$. L'application ν définie précédemment fait de S une S-algèbre et on remarque que si l'on munit les anneaux des filtrations correspondant respectivement au choix des uniformisantes π et π', l'application ν est compatible aux filtrations.

Considérons les constantes t et n fournies par les lemmes 3.1.2 et 3.1.3 et définissons :

$$\begin{aligned}
M' &= S_{(\nu)}\otimes M \\
\mathrm{Fil}^r M' &= S_{(\nu)}\otimes \mathrm{Fil}^r M \\
\phi'_r(s \otimes x) &= \phi(s) \otimes \left(\sum_{i=0}^{\infty} \frac{t^i}{i!} N^i \circ \phi_r(x)\right) \\
N'(s \otimes x) &= N(s) \otimes x + s \otimes nN(x)
\end{aligned}$$

les deux dernières égalités étant définies pour tout $s \in S$ et respectivement tout $x \in \mathrm{Fil}^r \mathcal{M}$ et tout $x \in \mathcal{M}$.

Lemme 3.1.4. *Pour tout entier $i \geqslant 1$, le diagramme suivant est commutatif :*

$$\begin{tikzcd}
Fil^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "E(u)^i N^i"'] & \mathcal{M} \arrow[d, "c^i N^i"] \\
Fil^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M}
\end{tikzcd}$$

Démonstration. On prouve la propriété par récurrence. Pour $i = 1$, elle est vraie par hypothèse. Pour l'hérédité, juxtaposons les deux diagrammes :

$$\begin{tikzcd}
\mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "E(u)^i N^i"'] & \mathcal{M} \arrow[d, "c^i N^i"] \\
\mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "E(u)N"'] & \mathcal{M} \arrow[d, "cN"] \\
\mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M}
\end{tikzcd}$$

Le grand rectangle est commutatif puisque les deux carrés le sont. Soient $x \in \mathcal{M}$ et $s \in S$. On a :

$$\begin{aligned}(sN) \circ \left(s^i N^i\right)(x) &= s\left[N\left(s^i\right) N^i(x) + s^i N^{i+1}(x)\right] \\ &= is^i N(s) N^i(x) + s^{i+1} N^{i+1}(x).\end{aligned}$$

En appliquant le calcul précédent deux fois et en utilisant la commutativité du diagramme, on obtient, pour tout $x \in \operatorname{Fil}^r \mathcal{M}$:

$$\begin{aligned}& ic^i N(c) N^i(\phi_r(x)) + c^{i+1} N^{i+1}(\phi_r(x)) \\ &\quad = \phi_r\left[iE(u)^i N(E(u)) N^i(x) + E(u)^{i+1} N^{i+1}(x)\right] \\ &\quad = i\phi(N(E(u)))\phi_r\left(E(u)^i N^i(x)\right) + \phi_r\left(E(u)^{i+1} N^{i+1}(x)\right).\end{aligned}$$

On sait que $\phi(N(E(u))) = N(c)$, ce qui permet de conclure en utilisant une dernière fois l'hypothèse de récurrence. $\square$

Lemme 3.1.5. *L'application ϕ'_r est bien définie et est ϕ-semi linéaire.*

Démonstration. Dans un premier temps, si $x \in \operatorname{Fil}^r \mathcal{M}$, d'après le lemme 3.1.4 l'élément $\frac{1}{i!} N^i \circ \phi_r(x)$ est bien défini puisqu'égal à $\phi_r\left(\frac{E(u)^i}{i!} N^i(x)\right)$. Remarquons que $\frac{E(u)^i}{i!} N^i(x)$ est toujours élément de $\operatorname{Fil}^r \mathcal{M}$: si $i < r < p$, c'est vrai car $i!$ est inversible et si $i \geqslant r$, c'est vrai par hypothèse.

D'autre part, pour $i \gg 0$, on a :

$$\phi_r\left(\frac{E(u)^i}{i!} N^i(x)\right) = \frac{1}{c^r}\phi_r\left(\frac{E(u)^i}{i!}\right)\phi_r\left(E(u)^r N^i(x)\right)$$

et le facteur $\phi_r\left(\frac{E(u)^i}{i!}\right)$ est multiple de $\frac{p^{i-r}}{i!}$. Comme on a supposé $p > 2$, la valuation p-adique de ce dernier tend vers l'infini. Cela prouve que la suite des $\frac{1}{i!} N^i \circ \phi_r(x)$ converge vers 0 et donc que la somme de la série est bien définie.

Reste à voir que si $s \in S$ et $x \in \operatorname{Fil}^r \mathcal{M}$, on a $\phi'_r(1 \otimes sx) = \phi'_r(\nu(s) \otimes x)$. Comme dans le lemme 3.1.1, on prouve :

$$\sum_{i=0}^{\infty} \frac{t^i}{i!} N^i(\phi_r(sx)) = \left(\sum_{i=0}^{\infty} \frac{t^i}{i!} N^i(\phi(s))\right) \cdot \left(\sum_{i=0}^{\infty} \frac{t^i}{i!} N^i(\phi_r(x))\right).$$

Le premier facteur vaut $\nu^{-1} \circ \phi \circ \nu(s)$ d'après le lemme 3.1.2. Cela conclut, le fait que ϕ'_r est ϕ-semi-linéaire étant évident. $\square$

Lemme 3.1.6. *L'application N' est bien définie et vérifie la condition de Leibniz.*

Démonstration. Comme précédemment, il s'agit de vérifier que pour $s \in S$ et $x \in \mathcal{M}$, on a $N'(1 \otimes sx) = N'(\nu(s) \otimes x)$. Calculons :

$$N'(1 \otimes sx) = 1 \otimes nN(sx) = 1 \otimes nN(s)x + 1 \otimes nsN(x).$$

Or d'après le lemme 3.1.3, on a $nN(s) = \nu^{-1} \circ N \circ \nu(s)$ et donc $1 \otimes nN(s)x = N \circ \nu(s) \otimes x$. D'autre part, on a $1 \otimes nsN(x) = \nu(s) \otimes nN(x)$. On en déduit que :

$$N'(1 \otimes sx) = N \circ \nu(s) \otimes x + \nu(s) \otimes nN(x)$$

comme on voulait. $\square$

Proposition 3.1.7. *L'objet $\mathcal{M}'$ muni de $Fil^r\mathcal{M}'$, de ϕ'_r et de N' est un objet de la catégorie $\underline{\mathcal{M}}^r_{\pi'}$.*

Démonstration. La seule vérification qui pose problème est la commutativité du diagramme reliant ϕ'_r à N'. Par un simple calcul, on prouve dans un premier temps qu'il existe une constante c' faisant commuter le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Fil}^r\mathcal{M}' \arrow[r, "\phi'_r"] \arrow[d, "\nu(E(u))N'"'] & \mathcal{M}' \arrow[d, "c'N'"] \\
\mathrm{Fil}^r\mathcal{M}' \arrow[r, "\phi'_r"] & \mathcal{M}'
\end{tikzcd}$$

Comme $\nu\left(E\left(u\right)\right)$ s'obtient à partir de $E'\left(u\right)$ simplement par la multiplication par une unité de S, un diagramme équivalent, dans lequel on a remplacé $\nu\left(E\left(u\right)\right)$ par $E'\left(u\right)$ et dans lequel la constante c' a été modifié, commute. D'autre part le calcul prouve que la constante c' obtenue ne dépend pas de $\mathcal{M}$.

Soient n un entier et $\mathcal{M} = S/p^nS \cdot e_1$ muni de $\mathrm{Fil}^r\mathcal{M} = \mathcal{M}$, $\phi_r\left(e_1\right) = e_1$ et $N\left(e_1\right) = 0$. On a $\left(c'N'\right) \circ \phi'_r\left(u \otimes e_1\right) = \phi'_r \circ \left(E'\left(u\right)N\right)\left(u \otimes e_1\right)$, ce qui donne après calcul :

$$\left[c'pu^p - u^p\phi\left(E'\left(u\right)\right)\right] \otimes e_1 = 0.$$

Ainsi p^n divise $c'pu^p - u^p\phi\left(E'\left(u\right)\right)$ pour tout n et finalement $c' = \phi_1\left(E'\left(u\right)\right)$. □

On a ainsi défini un foncteur (la définition sur les flèches est évidente) $\underline{\mathcal{M}}^r_\pi \to \underline{\mathcal{M}}^r_{\pi'}$.

Canonicité et compatibilité

Proposition 3.1.8. *Le foncteur défini précédemment ne dépend pas du choix de l'élément $P \in S$.*

Démonstration. Avec les notations précédentes, il suffit de prouver que si $P = uH$ est tel que $P\left(\pi\right) = \pi$, alors $\mathcal{M}$ et $\mathcal{M}'$ sont canoniquement isomorphes. Notons $\nu : S \to S$ le morphismes d'anneau tel que $\nu\left(u\right) = P\left(u\right)$. La condition implique $H\left(u\right) - 1 \in \mathrm{Fil}^1 S$ et donc l'élément $\log\left(H\left(u\right)\right)$ est bien défini dans S.

Si $\mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r_\pi$, on peut définir l'application :

$$\begin{array}{ccc}
S_{(\nu)} \otimes \mathcal{M} & \to & S \\
s \otimes x & \mapsto & s\displaystyle\sum_{i=0}^{\infty} \frac{\left(-\log H\left(u\right)\right)^i}{i!} N^i\left(x\right)
\end{array}$$

Comme $\log\left(H\left(u\right)\right) \in \mathrm{Fil}^1 S$, l'élément $\frac{\left(-\log H(u)\right)^i}{i!}$ est bien défini. En outre le fait que dans T, $\exp\left(\log H\left(u\right)\right) = H\left(u\right) \in S$ prouve que la suite $\frac{\left(\log H(u)\right)^i}{i!}$ converge vers 0 et finalement que l'application est bien définie.

Il ne reste plus qu'à voir que c'est un isomorphisme S-linéaire et compatible à toutes les structures ; c'est donc une flèche dans $\underline{\mathcal{M}}^r_\pi$. □

Corollaire 3.1.9. *Le foncteur défini précédemment est une équivalence de catégorie.*

Si, comme précédemment, π et π' sont deux uniformisantes de K, on peut définir $\hat{A}_{\mathrm{st}\pi}$ et $\hat{A}_{\mathrm{st}\pi'}$. Pour cela, rappelons que l'on avait besoin de choisir $(\pi_1, \ldots, \pi_n, \ldots)$ (resp. $(\pi'_1, \ldots, \pi'_n, \ldots)$) un système compatible de racines p^n-ièmes de π (resp. de π'). On définit ω_n en imposant $\pi_n = \omega_n \pi'_n$, obtenant ainsi $(\bar{\omega}_1, \ldots, \bar{\omega}_n, \ldots) \in R$ puis $[\underline{\omega}] \in A_{\mathrm{cris}}$ (notez que A_{cris} ne dépend pas du choix d'une uniformisante).

L'unique morphisme de A_{cris}-algèbre $\hat{A}_{\mathrm{st}\pi} \to \hat{A}_{\mathrm{st}\pi'}$ envoyant $(1+X)$ sur $[\underline{\omega}](1+X)$ est un isomorphisme compatible à ϕ_r, à N et à l'action du groupe de Galois G_K.

Proposition 3.1.10. *Le diagramme suivant est commutatif :*

$$\begin{tikzcd}
\underline{\mathcal{M}}^r_\pi \arrow[rr] \arrow[dr, "T_{st\pi}"'] & & \underline{\mathcal{M}}^r_{\pi'} \arrow[dl, "T_{st\pi'}"] \\
& Rep_{\mathbb{Z}_p}(G_K) &
\end{tikzcd}$$

où la flèche horizontale est le foncteur défini précédemment.

Démonstration. L'anneau S s'identifie à la fois aux points fixes sous l'action de Galois de $\hat{A}_{\mathrm{st}\pi}$ et de $\hat{A}_{\mathrm{st}\pi'}$. Notons $\rho : S \to \hat{A}_{\mathrm{st}\pi}$ et $\rho' : S \to \hat{A}_{\mathrm{st}\pi'}$ les inclusions correspondantes. Il existe un unique morphisme de A_{cris}-algèbre, $\nu : \hat{A}_{\mathrm{st}\pi} \to \hat{A}_{\mathrm{st}\pi'}$ faisant commuter le diagramme suivant :

$$\begin{tikzcd}
S \arrow[r, "\nu"] \arrow[d, "\rho"'] & S \arrow[d, "\rho'"] \\
\hat{A}_{\mathrm{st}\pi} \arrow[r, dotted, "\nu"] & \hat{A}_{\mathrm{st}\pi'}
\end{tikzcd}$$

En effet, le diagramme impose la valeur de $\nu\left(\frac{X^i}{i!}\right)$ et on vérifie que l'application ainsi définie convient. En outre, elle est G_K-équivariante et induit une flèche $\nu : \hat{A}_{\mathrm{st},\infty\pi} \to \hat{A}_{\mathrm{st},\infty\pi'}$ encore G_K-équivariante.

Soit $\mathcal{M}$ un objet de $\underline{\mathcal{M}}^r_\pi$ et $\mathcal{M}'$ l'objet de $\underline{\mathcal{M}}^r_{\pi'}$ qui lui est associé par le foncteur précédent. On rappelle qu'en tant que module, on a $\mathcal{M}' = S_{(\nu)} \otimes \mathcal{M}$. Soit $f \in T_{\mathrm{st}}(\mathcal{M})$. On lui associe l'application suivante :

$$\begin{array}{rcl} \mathcal{M}' & \to & \hat{A}_{\mathrm{st},\infty\pi'} \\ s \otimes x & \mapsto & \rho'(s) \cdot \nu \circ f(x) \end{array}$$

On vérifie qu'elle est S-linéaire et compatible aux structures définissant ainsi un élément de $T_{\mathrm{st}}(\mathcal{M}')$.

On définit ainsi une application $T_{\mathrm{st}}(\mathcal{M}) \to T_{\mathrm{st}}(\mathcal{M}')$. Elle est $\mathbb{Z}_p$-linéaire et bijective puisque l'on peut construire l'application réciproque de façon analogue. On vérifie qu'elle est compatible à l'action de Galois et donc qu'il s'agit d'un isomorphisme dans la catégorie des $\mathbb{Z}_p$-représentations galoisiennes. $\square$

3.2 Description des objets de $\widetilde{\underline{\mathcal{M}}}^r$

On considère dans ce paragraphe un objet $\mathcal{M}$ de $\widetilde{\underline{\mathcal{M}}}^r$. Il s'agit d'un $k[u]/u^{ep}$-module libre de rang fini d muni d'une filtration, d'une application ϕ_r et d'une application N, le tout vérifiant les propriétés données précédemment.

Bases adaptées

On a dans un premier temps un résultat bien utile (et classique) qui est le suivant :

Proposition 3.2.1. *Il existe une base* $(e_1, \ldots, e_d)$ *de* $\mathcal{M}$ *et des entiers* $n_1, \ldots, n_d$ *tels que :*

$$Fil^r \mathcal{M} = \bigoplus_{i=1}^{d} u^{n_i} k\,[u] \,/ u^{ep} \cdot e_i.$$

Une telle base est par définition une base adaptée *de* $\mathcal{M}$.

Démonstration. Comme $\mathcal{M}$ est supposé libre, il existe un $k\,[u]$-module libre $\mathcal{M}'$ tel que $\mathcal{M}'/u^{ep}\mathcal{M}' = \mathcal{M}$. Autrement dit, il existe une flèche $f : \mathcal{M}' \to \mathcal{M}$ dont le noyau est exactement $u^{ep}\mathcal{M}'$. Définissons $\mathrm{Fil}^r\mathcal{M}' = f^{-1}(\mathrm{Fil}^r\mathcal{M})$. C'est un sous-$k\,[u]$-module de $\mathcal{M}'$.

Puisque $k\,[u]$ est un anneau principal, d'après le théorème de structure, il existe une suite de polynômes $P_1, \ldots, P_d$ tels que P_i divise P_{i+1} pour tout i et une base $(\hat{e}_1, \ldots, \hat{e}_d)$ de $\mathcal{M}'$ telle que $(P_1\hat{e}_1, \ldots, P_d\hat{e}_d)$ soit une base de $\mathrm{Fil}^r\mathcal{M}'$. D'autre part, $u^{er}\mathcal{M}' \subset \mathrm{Fil}^r\mathcal{M}'$ et donc tous les polynômes P_i sont des diviseurs de u^{er} ; ils sont donc de la forme $P_i = u^{n_i}$ pour certains entiers n_i.

En posant $e_i = f(\hat{e}_i)$, on a bien le résultat annoncé. □

Remarque. Les entiers n_i ne dépendent pas à permutation près de la base considérée. En effet, la dimension en tant que k-espace vectoriel du quotient $\mathrm{Fil}^r\mathcal{M}/\left(u^k\mathcal{M} \cap \mathrm{Fil}^r\mathcal{M}\right)$ est donnée par la somme des $k - n_i$, somme étendue à tous les i pour lesquels $n_i \leqslant k$. On voit facilement que la connaissance de toutes ces sommes permet de déterminer les n_i à permutation près.

Fixons à présent $(e_1, \ldots, e_d)$ une base adaptée de $\mathcal{M}$. Nous allons essayer de décrire un peu mieux la fonction ϕ_r et pour cela nous introduisons la définition suivante.

Définition 3.2.2. *Soit* $x \in \mathcal{M} \backslash u\mathcal{M}$, *et soit* n *le plus petit entier tel que* $u^n x \in Fil^r\mathcal{M}$. *On pose* $\varphi_r(x) = \phi_r(u^n x)$.

Soit $x_i = \varphi_r(e_i)$ pour $1 \leqslant i \leqslant d$. On rappelle que la famille des e_i est la base adaptée que l'on s'est fixée précédemment.

Proposition 3.2.3. *Avec les notations précédentes,* $(x_1, \ldots, x_d)$ *est une base de* $\mathcal{M}$.
D'autre part, si $x \in \mathcal{M} \backslash u\mathcal{M}$, *alors* $\varphi_r(x) \in \mathcal{M} \backslash u\mathcal{M}$.

Démonstration. Pour le premier énoncé, il suffit de voir que si $x \in \mathrm{Fil}^r\mathcal{M}$, alors $\phi_r(x)$ s'écrit comme une combinaison linéaire (à coefficients dans $k\,[u^p] \,/ u^{ep}$) des x_i. Comme $\mathrm{im}\,\phi_r$ engendre $\mathcal{M}$ comme $k\,[u] \,/ u^{ep}$-module, il en est de même de la famille $(x_1, \ldots, x_d)$. Comme elle est de bon cardinal, elle en est une base.

Soit $x \in \mathcal{M} \backslash u\mathcal{M}$. On voit en décomposant x sur la base des e_i, que $\varphi_r(x)$ s'écrit forcément sous la forme :

$$\varphi_r(x) = Q_1(u^p)x_1 + \ldots + Q_d(u^p)x_d$$

où au moins l'un des polynômes Q_i est de valuation nulle. Dans ce cas, on a directement $\varphi_r(x) \in \mathcal{M} \backslash u\mathcal{M}$. □

Remarque. La deuxième partie de la proposition précédente permet de définir correctement les itérés de φ_r.

L'opérateur de monodromie

Nous allons à présent étudier l'opérateur de monodromie. Pour cela, nous notons $\mathcal{M}_0 = \operatorname{im}\phi_r$. Par ce qui précède, $\mathcal{M}_0$ s'identifie au $k[u^p]/u^{ep}$-module engendré par les x_i. Nous avons alors :

Proposition 3.2.4. *Pour tout i, l'opérateur $c_\pi^i N^i$ induit une application $k[u^p]/u^{ep}$-linéaire de $\mathcal{M}_0$ sur lui-même. Cette application est nulle si $i \geqslant p$.*

Démonstration. Le lemme 3.1.4 assure que le diagramme suivant :

$$\begin{tikzcd}
\operatorname{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "u^{ei}N^i"'] & \mathcal{M} \arrow[d, "c_\pi^i N^i"] \\
\operatorname{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M}
\end{tikzcd}$$

commute. Ainsi si x est dans l'image de ϕ_r, alors il en est de même de $c_\pi^i N^i(x)$, et donc que $c_\pi^i N^i$ induit une application de $\mathcal{M}_0$ dans lui-même. D'autre part, $N(u^p x) = N(u^p)x + u^p N(x) = -pu^p x + u^p N(x) = u^p N(x)$, ce qui prouve bien la linéarité annoncée.

Pour $i \geqslant p$, l'application $u^{ei}N^i$ est nulle et donc il en est de même de $c_\pi^i N^i$. $\square$

Corollaire 3.2.5. *Il existe un élément $x \in \mathcal{M}_0$ non divisible par u tel que $N(x) = 0$.*

Démonstration. Du fait que $c_\pi^p N^p = 0$, il existe $x' \in \mathcal{M}_0$, $x' \neq 0$, tel que $N(x') = 0$. Écrivons $x' = u^{pk}x''$ où x'' est un élément de $\mathcal{M}_0$ non divisible par u et où $k < e$. On a alors $N\left(u^{pk}x''\right) = u^{pk}N(x'') = 0$ et donc $N(x'')$ est un multiple de u^p. Notons n le plus petit entier tel que $u^n x'' \in \operatorname{Fil}^r\mathcal{M}$ de telle sorte que l'on ait $\varphi_r(x'') = \phi_r(u^n x'') = x$. On a :

$$\phi_r\left(u^e N(u^n x'')\right) = c_\pi N\left(\phi_r(u^n x'')\right) = c_\pi N(x).$$

Mais $N(u^n x'') = -nu^n x'' + u^n N(x'')$. Le premier terme de cette somme est dans $\operatorname{Fil}^r\mathcal{M}$ puisque $u^n x''$ y est. Le second y est également puisque $N(x'')$ est un multiple de u^p. On en déduit que $N(u^n x'') \in \operatorname{Fil}^r\mathcal{M}$ et donc que $\phi_r\left(u^e N(u^n x'')\right) = 0$. Ainsi $N(x) = 0$. D'autre part, on a $x = \varphi_r(x'')$ et donc d'après la proposition 3.2.3, x n'est pas divisible par u. Ceci conclut la preuve du corollaire. $\square$

Description matricielle

Le but de ce paragraphe est d'écrire sous forme matricielle les applications ϕ_r et N, explicitations que nous utiliserons dans la suite. On fixe $\mathcal{M}$ un objet de $\underline{\widetilde{\mathcal{M}}}^r$ et $(e_1, \dots, e_d)$ une base adaptée de $\mathcal{M}$, les entiers correspondants étant $n_1, \dots, n_d$.

On note Δ la matrice diagonale suivante :

$$\Delta = \begin{pmatrix} u^{n_1} & & \\ & \ddots & \\ & & u^{n_d} \end{pmatrix}$$

Définition 3.2.6. *La* matrice *de ϕ_r dans la base adaptée $(e_1, \dots, e_d)$ est la matrice G définie par l'égalité suivante :*

$$\begin{pmatrix} \phi_r(u^{n_1}e_1) \\ \vdots \\ \phi_r(u^{n_d}e_d) \end{pmatrix} = \phi_r\left(\Delta \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix}\right) = {}^t G \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix}$$

Remarque. Cette définition n'a un sens que si la base $(e_1, \dots, e_d)$ est adaptée. De plus, la présence de la transposée sert à rester fidèle à la définition classique de la matrice d'une application linéaire.

En gardant les notations du paragraphe précédent, on voit que G est simplement la matrice de passage de la base $(e_1, \dots, e_d)$ à la base $(x_1, \dots, x_d)$. En tant que telle, il s'agit d'une matrice inversible.

Définition 3.2.7. *Soit $(a_1, \dots, a_d)$ une base de $\mathcal{M}$. La* matrice *de N dans la base $(a_1, \dots, a_d)$ est la matrice H définie par l'égalité suivante :*

$$\begin{pmatrix} N(a_1) \\ \vdots \\ N(a_d) \end{pmatrix} = N \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = {}^{\mathrm{t}}H \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$$

On a une formule de changement de base :

Proposition 3.2.8. *Soient $\mathcal{A} = (a_1, \dots, a_d)$ et $\mathcal{B} = (b_1, \dots, b_d)$ deux bases de $\mathcal{M}$, et soit P la matrice de passage de $\mathcal{A}$ à $\mathcal{B}$. On note $H_{\mathcal{A}}$ (resp. $H_{\mathcal{B}}$) la matrice de N dans la base $\mathcal{A}$ (resp. dans la base $\mathcal{B}$). On a alors la relation :*

$$H_{\mathcal{B}} = P^{-1} H_{\mathcal{A}} P + P^{-1} N(P)$$

Démonstration. Il s'agit d'un simple calcul. On écrit :

$$\begin{aligned}
\begin{pmatrix} N(b_1) \\ \vdots \\ N(b_d) \end{pmatrix} &= N \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} = N \left({}^{\mathrm{t}}P \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \right) \\
&= N\left({}^{\mathrm{t}}P\right) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} + {}^{\mathrm{t}}P \cdot N \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \\
&= N\left({}^{\mathrm{t}}P\right) {}^{\mathrm{t}}P^{-1} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} + {}^{\mathrm{t}}P H_{\mathcal{A}} {}^{\mathrm{t}}P^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}
\end{aligned}$$

ce qui donne ${}^{\mathrm{t}}H_{\mathcal{B}} = N({}^{\mathrm{t}}P)\, {}^{\mathrm{t}}P^{-1} + {}^{\mathrm{t}}P H_{\mathcal{A}} {}^{\mathrm{t}}P^{-1}$ puis le résultat annoncé en prenant la transposée. □

Remarque. Un simple calcul prouve que si A et B sont des matrices à coefficients dans $k[u]/u^{ep}$, alors $N(AB) = N(A)B + AN(B)$. Ceci a pour conséquence l'égalité $P^{-1}N(P) = -N(P^{-1})P$ et prouve la cohérence de la formule lorsque l'on passe d'une base $\mathcal{A}$ à une base $\mathcal{B}$ puis que l'on revient à $\mathcal{A}$.

Proposition 3.2.9. *Si les n_i sont rangés par ordre croissant, la matrice de $c_\pi N$ dans la base $(x_1, \dots, x_d)$ (où on rappelle que $x_i = \phi_r(u^{n_i} e_i)$) est à coefficients dans $k[u^p]/u^{ep}$ et triangulaire inférieure avec des 0 sur la diagonale.*

Démonstration. La preuve résulte du diagramme commutatif suivant :

$$\begin{tikzcd} \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "u^e N"'] & \mathcal{M} \arrow[d, "c_\pi N"] \\ \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M} \end{tikzcd}$$

En effet, fixons un entier i et partons de l'élément $u^{n_i}e_i$. Par ϕ_r, il s'envoie sur x_i par définition. Puis par $c_\pi N$, il s'envoie sur $c_\pi N(x_i)$. Par l'autre chemin, on a d'abord :

$$u^e N(u^{n_i}e_i) = -n_i u^{e+n_i}e_i + u^{e+n_i}N(e_i)$$

Comme $u^{n_i}e_i \in \mathrm{Fil}^r\mathcal{M}$, le premier terme de la somme précédente s'envoie sur 0 par ϕ_r et $u^{e+n_i}N(e_i) \in \mathrm{Fil}^r\mathcal{M}$. Pour le second terme, décomposons $N(e_i) = \sum_{j=1}^d a_j e_j$ où $a_j \in k[u]/u^{ep}$ est tel que $u^{e+n_i}N(e_i) \in \mathrm{Fil}^r\mathcal{M}$ (*i.e.* $u^{e+n_i}a_j \in u^{n_j}k[u]/u^{ep}$). On a alors :

$$\phi_r(u^e N(u^{n_i}e_i)) = \sum_{j=1}^{d} \phi\left(u^{e+n_i-n_j}a_j\right)x_j$$

et les $\phi(u^{e+n_i-n_j}a_j)$ sont les coefficients de la j-ième colonne de la matrice de $c_\pi N$. Ils sont donc déjà tous bien dans $k[u^p]/u^{ep}$.

De plus, si $j \leqslant i$, on a par hypothèse $n_j \leqslant n_i$ et donc $e+n_i-n_j \geqslant e$. Ainsi $\phi(u^{e+n_i-n_j}a_j) = 0$ et on a bien démontré le résultat annoncé. □

Remarque. Cette dernière proposition redémontre en particulier, en donnant un résultat plus précis, la proposition 3.2.4 et le corollaire qui s'ensuit.

3.3 La catégorie $\underline{\widetilde{\mathrm{MF}}}^r$

Dans cette partie, nous introduisons des sous-catégories pleines $\underline{\widetilde{\mathrm{MF}}}^r$ de $\underline{\widetilde{\mathcal{M}}}^r$ qui correspondent aux catégories de Fontaine-Laffaille (voir [13]) tuées par p pour $e = 1$.

Commençons par donner une proposition qui caractérise les objets de cette sous-catégorie. Soit $\mathcal{M}$ un objet de $\underline{\widetilde{\mathcal{M}}}_0^r$. Notons $\mathcal{M}_0 = \mathrm{im}\,\phi_r$ et plus généralement $\mathcal{M}_i = u^i\mathcal{M}_0$ pour un entier i compris entre 0 et $p-1$. Les $\mathcal{M}_i$ sont des $k[u^p]/u^{ep}$-modules libres et :

$$\mathcal{M} = \bigoplus_{i=0}^{p-1}\mathcal{M}_i.$$

Proposition 3.3.1. *Avec les notations précédentes, les propriétés suivantes sont équivalentes :*

i) $\mathit{Fil}^r\mathcal{M} = \bigoplus_{i=0}^{p-1}\mathit{Fil}^r\mathcal{M}\cap\mathcal{M}_i$ *;*

ii) il existe une base adaptée de $\mathcal{M}$ formée d'éléments de $\mathcal{M}_0$;

iii) On peut munir $\mathcal{M}$ d'un opérateur de monodromie nul sur $\mathcal{M}_0$ et faisant de $\mathcal{M}$ un objet de $\underline{\widetilde{\mathcal{M}}}^r$.

Démonstration. La propriété ii) implique de façon presque immédiate les deux autres. Nous allons montrer que iii) implique i) puis que i) implique ii).

Supposons iii). Prouvons dans un premier temps que cela implique que $N(\mathrm{Fil}^r\mathcal{M}) \subset \mathrm{Fil}^r\mathcal{M}$. Soit $x \in \mathrm{Fil}^r\mathcal{M}$. D'après le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "u^e N"'] & \mathcal{M} \arrow[d, "c_\pi N"] \\
\mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M}
\end{tikzcd}$$

on a $\phi_r(u^e N(x)) = 0$. La proposition 3.2.3 implique facilement que $\ker \phi_r = u^e \mathrm{Fil}^r\mathcal{M}$ et donc il existe $y \in \mathrm{Fil}^r\mathcal{M}$ tel que $u^e N(x) = u^e y$. La différence $N(x) - y$ est tuée par u^e. Elle s'écrit $u^{e(p-1)}z$ pour un certain $z \in \mathcal{M}$. Comme $e(p-1) \geqslant er$, $u^{e(p-1)}z \in \mathrm{Fil}^r\mathcal{M}$ d'où $N(x) \in \mathrm{Fil}^r\mathcal{M}$. Ceci prouve la propriété annoncée.

Soit $y \in \mathrm{Fil}^r\mathcal{M}$. On cherche à construire des $y_i \in \mathrm{Fil}^r\mathcal{M} \cap \mathcal{M}_i$ tels que $y = y_0 + \ldots + y_{p-1}$. On peut déjà écrire une égalité de ce type avec $y_i \in \mathcal{M}_i$. Appliquons l'opérateur N à cette égalité en remarquant que puisque N est supposé nul sur $\mathcal{M}_0$, on a $N(y_i) = -iy_i$. On obtient successivement :

$$\begin{aligned}
y &= x_0 + y_1 + \ldots + y_{p-1} \\
N(y) &= -y_1 + \ldots - (p-1)\, y_{p-1} \\
N^2(y) &= y_1 + \ldots + (p-1)^2\, y_{p-1} \\
&\vdots \\
N^{p-1}(y) &= y_1 + \ldots + (p-1)^{p-1}\, y_{p-1}.
\end{aligned}$$

Les coefficients qui apparaissent forment une matrice de Vandermonde inversible. Ainsi on peut exprimer les y_i comme combinaisons linéaires à coefficients dans $\mathbb{F}_p$ des $N^j(y)$. Par ce qui précède, cela entraîne $y_i \in \mathrm{Fil}^r\mathcal{M}$ et donc bien la propriété voulue.

Supposons i). Fixons $(e_1, \ldots, e_d)$ une base de $\mathcal{M}_0$ comme $k[u^p]/u^{ep}$-module, et notons $\mathcal{M}'_0$ le sous-k-espace vectoriel de $\mathcal{M}_0$ engendré par les e_i. Notons également $\mathcal{M}'_i = u^i\mathcal{M}'_0$. Pour tout entier i, on a un isomorphisme $f_i : \mathcal{M}'_0 \to \mathcal{M}'_i$ qui est la multiplication par u^i. Notons $F'_i = f_i^{-1}(\mathrm{Fil}^r\mathcal{M} \cap \mathcal{M}'_i)$. On obtient une filtration croissante par des sous-k-espaces vectoriels. Il suffit alors pour répondre à la question de considérer une base $(x_1, \ldots, x_d)$ de $\mathcal{M}'_0$ compatible à cette filtration. $\square$

Définition 3.3.2. *On note $\widetilde{\underline{MF}}_0^r$ la sous-catégorie pleine de $\widetilde{\underline{\mathcal{M}}}_0^r$ formée des objets satisfaisant les propriétés de la proposition précédente. On note $\widetilde{\underline{MF}}^r$ la sous-catégorie pleine de $\widetilde{\underline{\mathcal{M}}}^r$ formée des objets dont l'image dans $\widetilde{\underline{\mathcal{M}}}_0^r$ par le foncteur d'oubli satisfait les propriétés de la proposition précédente.*

Les lettres MF font référence à « modules filtrés » car l'on peut donner une nouvelle interprétation de ces objets *via* des modules filtrés. Avant cela, faisons quelques remarques générales :

Proposition 3.3.3. *La catégorie $\widetilde{\underline{MF}}^r$ est une sous-catégorie abélienne de $\widetilde{\underline{\mathcal{M}}}^r$ stable par sous-objets et par quotients. De plus, elle est égale à $\widetilde{\underline{\mathcal{M}}}^r$ si et seulement si $e = r = 1$.*

Démonstration. Nous ne savons pas encore à ce stade que $\widetilde{\underline{\mathcal{M}}}^r$ est une catégorie abélienne. Nous allons l'admettre momentanément pour prouver la première partie de la proposition. Il suffit de prouver la stabilité par sommes directes, sous-objets et quotients, un noyau étant un sous-objet et un conoyau un quotient. Tout cela est immédiat avec la caractérisation iii).

Traitons le cas $e = r = 1$. Soit $\mathcal{M}$ un objet de $\widetilde{\underline{\mathcal{M}}}_0^r$ et soit $x \in \mathrm{Fil}^r\mathcal{M}$. On peut écrire $x = x_0 + \ldots + x_{p-1}$ avec $x_i \in \mathcal{M}_i$. Par hypothèse $u\mathcal{M} \subset \mathrm{Fil}^r\mathcal{M}$, et donc $x_i \in \mathrm{Fil}^r\mathcal{M}$ pour $i \geqslant 1$, puis $x_0 \in \mathrm{Fil}^r\mathcal{M}$. On a ainsi vérifié la propriété i). Réciproquement, considérons $\mathcal{M} = k[u]/u^{ep}e_1 \oplus k[u]/u^{ep}e_2$, $\mathrm{Fil}^r\mathcal{M} = (e_1, u^2e_2)$, $\phi_r(e_1) = e_2$, $\phi_r(u^2e_2) = e_1 + ue_2$. D'après la proposition 3.2.9, un opérateur de monodromie sur $\mathcal{M}$ doit vérifier $N(e_1 + ue_2) = 0$ et $N(e_2) = a(e_1 + ue_2)$ pour un certain $a \in k[u^p]/u^{ep}$. On doit avoir $cN \circ \phi_r(e_1) = \phi_r(u^e N(e_1))$, ce qui donne après calcul $a = -u^{p(e-1)}$. Il existe donc un unique N valable, et il n'est pas nul sur $\mathrm{im}\,\phi_r$. Cela conclut. □

Proposition 3.3.4. *Tout objet non nul de $\widetilde{\underline{\mathcal{M}}}_0^r$ (resp. de $\widetilde{\underline{\mathcal{M}}}^r$) admet un sous-objet non nul dans $\widetilde{\underline{MF}}_0^r$ (resp. dans $\widetilde{\underline{MF}}^r$ pour lequel N est nul sur $\mathrm{im}\,\phi_r$).*

Démonstration. La preuve de cette propriété est donnée dans le paragraphe 4.1 lors de l'étude des objets simples. □

Les objets de $\widetilde{\underline{\mathrm{MF}}}^r$ comme modules filtrés

Il est possible de décrire la catégorie $\widetilde{\underline{\mathrm{MF}}}^r$ avec des objets plus proches des objets de Fontaine-Laffaille du cas $e = 1$. Soit $\mathcal{M}$ un objet de $\widetilde{\underline{\mathrm{MF}}}^r$. Posons $\mathcal{M}_0 = \mathrm{im}\,\phi_r$ et $\mathcal{M}_i = u^i\mathcal{M}_0$, pour $0 \leqslant i \leqslant p-1$. On a un isomorphisme $f_i : \mathcal{M}_0 \to \mathcal{M}_i$ qui est la multiplication par u^i. Définissons $F_{i/e} = f_{er-i}^{-1}(\mathrm{Fil}^r\mathcal{M} \cap \mathcal{M}_{er-i})$. On obtient une suite décroissante de sous-$k[u^p]/u^{ep}$-modules de $\mathcal{M}_0$ contenant $u^p\mathcal{M}_0$ telle que $F_0 = \mathcal{M}_0$ par hypothèse.

L'application ϕ_r induit des applications $\phi_i : F_i \to \mathcal{M}_0$ faisant commuter les diagrammes :

$$\begin{tikzcd} F_{i+\frac{1}{e}} \arrow[r] \arrow[d, "\phi_{i+\frac{1}{e}}"'] & F_i \arrow[d, "\phi_i"] \\ \mathcal{M}_0 \arrow[r, "u^p"] & \mathcal{M}_0 \end{tikzcd}$$

La monodromie, quant à elle, définit une application $c_\pi N : \mathcal{M}_0 \to \mathcal{M}_0$ qui vérifie $\phi(c_\pi)\,[(c_\pi N) \circ \phi_i] = \phi_{i-1} \circ (c_\pi N)$.

Si on remarque pour finir que $k[u^p]/u^{ep}$ est isomorphe en tant qu'anneau à $\mathcal{O}_K/p$ (en envoyant u^p sur π), on obtient la proposition suivante qui énonce précisément le pont entre les catégories $\underline{\mathcal{M}}^r$ et celles de Fontaine-Laffaille, du moins dans le cas modulo p :

Proposition 3.3.5. *La catégorie $\widetilde{\underline{MF}}^r$ est équivalente à la catégorie dont les objets sont les données suivantes :*

1. *un $\mathcal{O}_K/p$-module libre de rang fini $\mathcal{M}$;*
2. *une filtration décroissante (F_i) de sous-modules de $\mathcal{M}$ contenant $\pi\mathcal{M}$ indexée par les rationnels de dénominateur e compris entre 0 et r telle que $F_0 = \mathcal{M}$;*
3. *des applications ϕ-semi-linéaires $\phi_i : F_i \to \mathcal{M}$ vérifiant $\phi_{i|F_{i+\frac{1}{e}}} = \pi\phi_{i+\frac{1}{e}}$, $\phi_{i+\frac{j}{e}}(\pi x) = \pi^{p-j}\phi_i(x)$ pour tout $x \in F_i$ et $0 \leqslant j \leqslant p$, et telles que $\mathcal{M}_0 = \sum_i \mathrm{im}\,\phi_i$;*
4. *d'une application linéaire $N : \mathcal{M} \to \mathcal{M}$ telle que $\phi(c_\pi) \cdot N \circ \phi_i = \phi_{i-1} \circ N$ pour tout i*

et où les flèches sont les morphismes $\mathcal{O}_K/p$-linéaires compatibles à toutes les structures.

Remarque. Dans le cas non ramifié (*i.e.* $e = 1$ et $c_\pi = 1$), on retrouve exactement la description des catégories de Fontaine-Laffaille modulo p (voir [13]). On peut étendre cette remarque à toute une sous-catégorie de $\underline{\mathcal{M}}^r$ comme expliqué dans le paragraphe 2.4.1 de [3].

On peut résumer tout ce qui précède par le diagramme suivant :

$$\begin{tikzcd} \widetilde{\underline{\mathrm{MF}}}^r_0 \arrow[r, hook] \arrow[d, bend right] & \widetilde{\underline{\mathcal{M}}}^r_0 \\ \widetilde{\underline{\mathrm{MF}}}^r \arrow[r, hook] \arrow[u] & \widetilde{\underline{\mathcal{M}}}^r \arrow[u] \end{tikzcd}$$

Les flèches qui montent correspondent aux foncteurs d'oubli évidents. La flèche courbe est un foncteur « N canonique » qui munit un objet de $\widetilde{\underline{\mathrm{MF}}}^r_0$ du N (nécessairement unique) donné par le iii) de la proposition 3.3.1. On pourrait se demander s'il est possible de prolonger ce foncteur à tout $\widetilde{\underline{\mathcal{M}}}^r_0$. La réponse est oui dans le cas $r = 1$ (voir le lemme 5.1.2. de [1]), et non dans le cas général puisqu'il n'est déjà pas vrai que le foncteur d'oubli $\widetilde{\underline{\mathcal{M}}}^r \to \widetilde{\underline{\mathcal{M}}}^r_0$ est toujours essentiellement surjectif (reprendre l'exemple donné dans la démonstration de la proposition 3.3.3)

3.4 Un mot sur le cas $r = 1$

Ce cas est amplement discuté dans [8]. Plus exactement, Breuil construit là un foncteur contravariant entre la catégorie $\widetilde{\underline{\mathcal{M}}}^1_0$ et la catégorie des schémas en groupes finis et plats sur $\mathcal{O}_K$ tués par p. Il prouve ensuite, en exhibant en quasi-inverse, que ce foncteur est une anti-équivalence de catégories.

Il étend par la suite ce foncteur à toute la catégorie $\underline{\mathcal{M}}^1_0$ et atteint tous les schémas en groupes sur $\mathcal{O}_K$ tués par une puissance de p. De cette façon, Breuil retrouve la classification des schémas en groupes sur $\mathcal{O}_K$ débutée par Raynaud ([19]) et poursuivie par Fontaine ([14]) et Conrad ([10]), et étend même cette classification sans restriction sur la ramification.

3.5 Des catégories abéliennes et artiniennes

Nous montrons dans ce paragraphe que les catégories $\widetilde{\underline{\mathcal{M}}}^r$ et $\underline{\mathcal{M}}^r$ sont abéliennes. Nous rappelons dans un premier temps que ce résultat est prouvé dans [3] lorsque $e = 1$.

La catégorie $\widetilde{\underline{\mathcal{M}}}^r$

Notons $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$ la catégorie $\underline{\mathcal{M}}^r$ obtenue en considérant des $k[u]/u^p$-modules libres à la place de $k[u]/u^{ep}$-modules libres. Un raisonnement rigoureusement identique à celui établi pour prouver le corollaire 2.2.3.2 de [3] donne :

Théorème 3.5.1. *La catégorie $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$ est abélienne et artinienne. Plus précisément soit $f : \mathcal{X} \to \mathcal{Y}$ un morphisme dans $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$, alors :*

i) $f(Fil^r \mathcal{X}) = Fil^r \mathcal{Y} \cap f(\mathcal{X})$;

ii) Soit $\mathcal{K}$ le noyau de l'application $k[u]/u^p$-linéaire sous-jacente, $Fil^r \mathcal{K} = Fil^r \mathcal{X} \cap \mathcal{K}$, $\phi_r : Fil^r \mathcal{K} \to \mathcal{K}$ la restriction de $\phi_r : Fil^r \mathcal{X} \to \mathcal{X}$ et $N : \mathcal{K} \to \mathcal{K}$ la restriction de $N : \mathcal{X} \to \mathcal{X}$. Avec ces structures, $\mathcal{K}$ est un objet de $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$ et donne le noyau de f dans $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$;

iii) Soit $\mathcal{C}$ le conoyau de l'application $k[u]/u^p$-linéaire sous-jacente, $Fil^r \mathcal{C}$ l'image de $Fil^r \mathcal{Y}$ dans $\mathcal{C}$, $\phi_r : Fil^r \mathcal{C} \to \mathcal{C}$ l'application qu'induit $\phi_r : Fil^r \mathcal{Y} \to \mathcal{Y}$ et $N : \mathcal{C} \to \mathcal{C}$ le quotient de $N : \mathcal{Y} \to \mathcal{Y}$. Avec ces structures, $\mathcal{C}$ est un objet de $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$ et donne le conoyau de f dans $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$.

Nous allons à présent montrer les propriétés analogues pour la catégorie $\widetilde{\underline{\mathcal{M}}}^r$.

Soit $f : \mathcal{X} \to \mathcal{Y}$ un morphisme de la catégorie $\widetilde{\underline{\mathcal{M}}}^r$. Notons $\bar{\mathcal{X}}$ (resp. $\bar{\mathcal{Y}}$) la réduction de $\mathcal{X}$ (resp. de $\mathcal{Y}$) modulo u^p, et $p_{\mathcal{X}} : \mathcal{X} \to \bar{\mathcal{X}}$ (resp. $p_{\mathcal{Y}} : \mathcal{Y} \to \bar{\mathcal{Y}}$) la projection correspondante. On munit $\bar{\mathcal{X}}$ et $\bar{\mathcal{Y}}$ de Fil^r, Frobenius et opérateurs de monodromie en regardant les structures quotients. On obtient des objets de la catégorie $\widetilde{\underline{\mathcal{M}}}^r_{(1)}$ et la flèche f induit un morphisme $\bar{f} : \bar{\mathcal{X}} \to \bar{\mathcal{Y}}$ dans cette catégorie. Finalement, puisque $er < p-1$, on a :

$$\mathrm{Fil}^r\mathcal{X} = p_{\mathcal{X}}^{-1}\left(\mathrm{Fil}^r\bar{\mathcal{X}}\right) \quad \text{et} \quad \mathrm{Fil}^r\mathcal{Y} = p_{\mathcal{Y}}^{-1}\left(\mathrm{Fil}^r\bar{\mathcal{Y}}\right)$$

Lemme 3.5.2. *L'image (au sens classique) de f est un $k[u]/u^{ep}$-module libre.*

Démonstration. Comme f commute à ϕ_r, elle induit une application $f : \phi_r(\mathrm{Fil}^r\mathcal{X}) \to \phi_r(\mathrm{Fil}^r\mathcal{Y})$ qui est $k[u^p]/u^{ep}$-linéaire. En recopiant l'argument de la preuve de la proposition 3.2.1, on prouve qu'il existe des éléments $e_1, \ldots, e_d, e'_1, \ldots, e'_{d'}$ et des entiers $n_1, \ldots, n_d, n'_1, \ldots, n'_{d'}$ tels que $n'_{i'} > 0$ et :

$$\begin{aligned} \mathrm{im}\, f &= k[u]/u^{ep}e_1 \oplus \ldots \oplus k[u]/u^{ep}e_d \oplus u^{pn'_1}k[u]/u^{ep}e'_1 \oplus \ldots \oplus u^{pn'_{d'}}k[u]/u^{ep}e'_{d'} \\ \mathrm{Fil}^r\mathcal{Y} \cap \mathrm{im}\, f &= u^{n_1}k[u]/u^{ep}e_1 \oplus \ldots \oplus u^{n_d}k[u]/u^{ep}e_d \oplus u^{pn'_1}k[u]/u^{ep}e'_1 \oplus \ldots \oplus u^{pn'_{d'}}k[u]/u^{ep}e'_{d'} \end{aligned}$$

De plus, comme $\phi_r(\mathrm{Fil}^r\mathcal{X})$ doit engendrer $\mathcal{X}$ et que $f(\mathrm{Fil}^r\mathcal{X}) \subset \mathrm{Fil}^r\mathcal{Y}$, on en déduit que $\phi_r(\mathrm{Fil}^r\mathcal{Y} \cap \mathrm{im}\, f)$ doit au moins engendrer $\mathrm{im}\, f$. Mais, puisque $er < p-1$, on a forcément $\phi_r(u^p\mathcal{Y}) \subset u^{2p}\mathcal{Y}$ et par un argument de dimension, le seul moyen de tout concilier est d'avoir $d' = 0$, ce qui achève la démonstration. ☐

Lemme 3.5.3. *Le noyau et le conoyau de f sont des $k[u]/u^{ep}$-modules libres.*

Démonstration. En tant que $k[u]/u^{ep}$-module, l'image de f s'identifie au quotient $\mathcal{X}/\ker f$ et le conoyau au quotient $\mathcal{Y}/\mathrm{im}\, f$. Le lemme résulte du fait que si $N \subset M$ sont des $k[u]/u^{ep}$-modules de type fini et si deux modules parmi M, N et M/N sont libres sur $k[u]/u^{ep}$, alors il en est de même du troisième. ☐

Notons $\mathcal{K}$ le noyau de f, $\mathcal{C}$ le conoyau de f, $\bar{\mathcal{K}}$ le noyau de $\bar{f}$ et $\bar{\mathcal{C}}$ le conoyau de $\bar{f}$ et considérons le diagramme suivant :

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{K} \arrow[r] \arrow[d, "p_{\mathcal{K}}"'] & \mathcal{X} \arrow[r, "f"] \arrow[d, "p_{\mathcal{X}}"'] & \mathcal{Y} \arrow[r] \arrow[d, "p_{\mathcal{Y}}"'] & \mathcal{C} \arrow[r] \arrow[d, "p_{\mathcal{C}}"'] & 0 \\ 0 \arrow[r] & \bar{\mathcal{K}} \arrow[r] & \bar{\mathcal{X}} \arrow[r, "\bar{f}"] & \bar{\mathcal{Y}} \arrow[r] & \bar{\mathcal{C}} \arrow[r] & 0 \end{tikzcd}$$

Lemme 3.5.4. *La flèche $p_{\mathcal{K}}$ (resp. $p_{\mathcal{C}}$) définie par le diagramme précédent est surjective et de noyau $u^p\mathcal{K}$ (resp. $u^p\mathcal{C}$). Autrement dit $\bar{\mathcal{K}}$ s'identifie à $\mathcal{K}/u^p\mathcal{K}$ et $\bar{\mathcal{C}}$ à $\mathcal{C}/u^p\mathcal{C}$.*

Démonstration. Commençons par le noyau et la surjectivité. Soit $\bar{x} \in \bar{\mathcal{K}}$. Il se relève en $x \in \mathcal{X}$ tel que $f(x) = 0 \pmod{u^p}$. Il existe donc $y \in \mathcal{Y}$ tel que $f(x) = u^p y$. On a $u^p y \in \mathrm{im}\, f$ et, puisque $\mathrm{im}\, f$ est libre sur $k[u]/u^{ep}$, il existe $y' \in \mathrm{im}\, f$ tel que $u^p y = u^p y'$ et donc $u^p y = f(u^p x')$ pour un certain $x' \in \mathcal{X}$. Mais alors $x - u^p x' \in \mathcal{K}$ s'envoie sur $\bar{x}$ par $p_{\mathcal{K}}$. Ceci prouve la surjectivité.

Soit maintenant $x \in \mathcal{K}$ tel que $p_{\mathcal{K}}(x) = 0$. On a $p_{\mathcal{X}}(x) = 0$ et donc x est un multiple de u^p dans $\mathcal{X}$. Il l'est aussi dans $\mathcal{K}$ puisque $\mathcal{K}$ est un $k[u]/u^{ep}$-module libre. Finalement $\ker p_{\mathcal{K}} = u^p\mathcal{K}$.

On utilise des arguments analogues pour le conoyau. ☐

Lemme 3.5.5. *On a $f(\mathrm{Fil}^r\mathcal{X}) = \mathrm{Fil}^r\mathcal{Y} \cap f(\mathcal{X})$.*

Démonstration. On a évidemment toujours l'inclusion $f(\mathrm{Fil}^r\mathcal{X}) \subset \mathrm{Fil}^r\mathcal{Y} \cap f(\mathcal{X})$.

Soit $y \in \mathrm{Fil}^r\mathcal{Y} \cap f(\mathcal{X})$. La réduction $\bar{y}$ de y modulo u^p est un élément de $\mathrm{Fil}^r\bar{\mathcal{Y}} \cap \bar{f}(\bar{\mathcal{X}})$ (en gardant les notations précédentes) et d'après le théorème 3.5.1, $\bar{y} \in \bar{f}(\mathrm{Fil}^r\bar{\mathcal{X}})$. Il existe $\bar{x} \in \mathrm{Fil}^r\bar{\mathcal{X}}$ tel que $\bar{y} = \bar{f}(\bar{x})$. Notons x un relevé de $\bar{x}$ dans $\mathrm{Fil}^r\mathcal{X}$. Il existe un élément $y' \in \mathcal{Y}$ tel que $y = f(x) + u^p y'$. Les éléments y et $f(x)$ sont dans $\mathrm{im}\, f$, il en est donc de même de $u^p y'$ et puisque $\mathrm{im}\, f$ est libre sur $k[u]/u^{ep}$, il existe $y'' \in \mathrm{im}\, f$ tel que $u^p y' = u^p y''$. On écrit $y'' = f(x'')$ pour un certain $x'' \in \mathcal{X}$, et il vient $y = f(x + u^p x'')$. Comme $u^{er}\mathcal{X} \subset \mathrm{Fil}^r\mathcal{X}$ et $er < p-1$, on a $u^p x'' \in \mathrm{Fil}^r\mathcal{X}$ et donc $x + u^p x'' \in \mathrm{Fil}^r\mathcal{X}$. Finalement $y \in f(\mathrm{Fil}^r\mathcal{X})$. □

On définit $\mathrm{Fil}^r\mathcal{K} = \mathcal{K} \cap \mathrm{Fil}^r\mathcal{X}$, un Frobenius $\phi_r : \mathrm{Fil}^r\mathcal{K} \to \mathcal{K}$ et un opérateur de monodromie $N : \mathcal{K} \to \mathcal{K}$ déduits des opérateurs sur $\mathcal{X}$. De même, on définit $\mathrm{Fil}^r\mathcal{C}$ comme l'image de $\mathrm{Fil}^r\mathcal{Y}$ par la projection $\mathcal{Y} \to \mathcal{C}$, un Frobenius et un opérateur de monodromie sur $\mathcal{C}$, les opérateurs sur $\mathcal{Y}$ passant au quotient.

Lemme 3.5.6. *Munis des structures précédentes, les objets $\mathcal{K}$ et $\mathcal{C}$ sont des objets de la catégorie $\widetilde{\underline{\mathcal{M}}}^r$ et respectivement un noyau et un conoyau de l'application f.*

Démonstration. Les conditions de compatibilité et le fait que si les objets sont dans la catégorie, ils sont noyau ou conoyau est évident. Le seul point délicat est la « surjectivité » des ϕ_r.

Modulo u^p, les objets $\mathcal{K}$ et $\mathcal{C}$ avec toutes leurs structures se réduisent d'après le lemme 3.5.4 sur $\bar{\mathcal{K}}$ et $\bar{\mathcal{C}}$ et on sait alors que les ϕ_r définis sur ces objets sont « surjectifs ». Notons $(e_1, \ldots, e_d)$ une base adaptée de $\mathcal{K}$ (qui existe bien) et G la matrice de ϕ_r dans cette base. Cette matrice est inversible modulo u^p et donc son déterminant est inversible modulo u^p puis modulo u^{ep}. La matrice G est donc inversible et $\mathrm{im}\,\phi_r$ engendre bien tout $\mathcal{K}$. On raisonne de même pour $\mathcal{C}$. □

En rassemblant tous les résultats précédents, on obtient :

Corollaire 3.5.7. *La catégorie $\widetilde{\underline{\mathcal{M}}}^r$ est abélienne et artinienne. Plus précisément soit $f : \mathcal{X} \to \mathcal{Y}$ un morphisme dans $\widetilde{\underline{\mathcal{M}}}^r$, alors :*

i) $f(\mathrm{Fil}^r\mathcal{X}) = \mathrm{Fil}^r\mathcal{Y} \cap f(\mathcal{X})$;

ii) Soit $\mathcal{K}$ le noyau de l'application $k[u]/u^{ep}$-linéaire sous-jacente, $\mathrm{Fil}^r\mathcal{K} = \mathrm{Fil}^r\mathcal{X} \cap \mathcal{K}$, $\phi_r : \mathrm{Fil}^r\mathcal{K} \to \mathcal{K}$ la restriction de $\phi_r : \mathrm{Fil}^r\mathcal{X} \to \mathcal{X}$ et $N : \mathcal{K} \to \mathcal{K}$ la restriction de $N : \mathcal{X} \to \mathcal{X}$. Avec ces structures, $\mathcal{K}$ est un objet de $\widetilde{\underline{\mathcal{M}}}^r$ et donne le noyau de f dans $\widetilde{\underline{\mathcal{M}}}^r$;

iii) Soit $\mathcal{C}$ le conoyau de l'application $k[u]/u^{ep}$-linéaire sous-jacente, $\mathrm{Fil}^r\mathcal{C}$ l'image de $\mathrm{Fil}^r\mathcal{Y}$ dans $\mathcal{C}$, $\phi_r : \mathrm{Fil}^r\mathcal{C} \to \mathcal{C}$ l'application qu'induit $\phi_r : \mathrm{Fil}^r\mathcal{Y} \to \mathcal{Y}$ et $N : \mathcal{C} \to \mathcal{C}$ le quotient de $N : \mathcal{Y} \to \mathcal{Y}$. Avec ces structures, $\mathcal{C}$ est un objet de $\widetilde{\underline{\mathcal{M}}}^r$ et donne le conoyau de f dans $\widetilde{\underline{\mathcal{M}}}^r$.

La catégorie $\underline{\mathcal{M}}^r$

On procède par dévissage. La preuve est en tout point analogue à celle déjà connue dans le cas $e = 1$ et présentée dans le paragraphe 2.3 de [3]. Les lemmes et les propositions successives gardent un sens dans ce contexte plus général, et sont également vrais, les preuves étant encore textuellement les mêmes. Nous n'insisterons donc pas davantage et laissons le lecteur se reporter à cette référence.

Remarque. De même, on prouve que les catégories $\widetilde{\underline{\mathcal{M}}}_0^r$ et $\underline{\mathcal{M}}_0^r$ sont abéliennes et artiniennes.

4 Classification des objets simples

Nous allons donner une classification complète des objets simples de la catégorie $\underline{\mathcal{M}}^r$ lorsque le corps résiduel k est algébriquement clos. Nous essaierons également d'expliquer ce qui se passe lorsque ce n'est pas le cas. Pour l'instant, on ne fait aucune hypothèse supplémentaire sur k.

On considère $\mathcal{M}$ un objet simple (donc non nul) de $\underline{\mathcal{M}}^r$. Il est obligatoirement tué par p. En effet, si ce n'était pas le cas, le noyau de la multiplication par p dans $\mathcal{M}$ fournirait un sous-objet strict de $\mathcal{M}$ (noter que la multiplication par p ne peut pas être injective car elle est nilpotente : $\mathcal{M}$ est supposé être tué par une puissance de p). L'objet simple $\mathcal{M}$ peut être vu dans la catégorie $\widetilde{\underline{\mathcal{M}}}^r$ (du moins si $r > 0$, mais dans le cas contraire, le résultat est immédiat et laissé au lecteur) : c'est un $k[u]/u^{ep}$-module muni d'un Fil^r, d'un ϕ_r et d'un opérateur de monodromie vérifiant les bonnes propriétés.

4.1 La monodromie

Si l'on note $\mathcal{M}_0 = \operatorname{im} \phi_r$, l'application de monodromie N induit une application linéaire $c_\pi N : \mathcal{M}_0 \to \mathcal{M}_0$ (voir proposition 3.2.4) et il existe $x_1 \in \mathcal{M}_0 \backslash u\mathcal{M}_0$ tel que $N(x_1) = 0$ (voir corollaire 3.2.5). Notons $x_2 = \varphi_r(x_1)$ (voir définition 3.2.2) puis par récurrence $x_{i+1} = \varphi_r(x_i)$, ce qui est possible d'après la deuxième partie de la proposition 3.2.3. On a $N(x_i) = 0$ pour tout entier i.

Notons $\bar{x}_i$ la réduction modulo u^p de x_i. Les $\bar{x}_i$ sont des éléments non nuls de $\mathcal{M}_0/u^p\mathcal{M}_0$ qui est un k-espace vectoriel de dimension finie. Notons $n \geqslant 1$ le plus petit indice tel que $\bar{x}_{n+1}$ puisse s'écrire comme combinaison linéaire des $\bar{x}_i$ pour i variant de 1 à n. Il existe donc $\lambda_i \in k$ tels que :

$$\bar{x}_{n+1} = \lambda_1 \bar{x}_1 + \ldots + \lambda_n \bar{x}_n$$

et on peut supposer $\lambda_1 \neq 0$ quitte à remplacer x_1 par le plus petit indice i tel que $\lambda_i \neq 0$. Comme $\bar{x}_{n+1} \neq 0$, les λ_i ne peuvent être tous simultanément nuls.

Nous allons à présent corriger les x_i pour que cette relation ne soit plus vraie seulement modulo u^p. On procède par approximations successives et on construit une suite indexée par j d'éléments $x_i^{(j)}$ qui sont tels que $x_i^{(j)} \equiv x_i \pmod{u^p}$, $x_{i+1}^{(j)} = \varphi_r(x_i^{(j)})$, $N(x_{i+1}^{(j)}) = 0$ et finalement :

$$x_{n+1}^{(j)} \equiv \lambda_1 x_1^{(j)} + \ldots + \lambda_n x_n^{(j)} \pmod{u^{jp}}$$

les λ_i restant inchangés. On a une solution pour $j = 1$. Supposons qu'on l'ait pour j et construisons-en une pour $j+1$. On cherche un élément $r \in \mathcal{M}_0$ tel que l'on puisse poser $x_1^{(j+1)} = x_1^{(j)} + u^{jp} r$. On définirait alors les $x_i^{(j+1)}$ *via* la formule de récurrence $x_{i+1}^{(j+1)} = \varphi_r(x_i^{(j+1)})$ et il est facile de vérifier que pour tout $i \geqslant 2$, on aurait $x_i^{(j+1)} \equiv x_i^{(j)} \pmod{u^{(j+1)p}}$. Au final, il suffit de trouver r tel que :

$$x_{n+1}^{(j)} \equiv \lambda_1 \left(x_1^{(j)} + u^{jp} r \right) + \lambda_2 x_2^{(j)} + \ldots + \lambda_n x_n^{(j)} \pmod{u^{(j+1)p}}$$

mais comme par hypothèse, on a $x_{n+1}^{(j)} \equiv \lambda_1 x_1^{(j)} + \ldots + \lambda_n x_n^{(j)} \pmod{u^{jp}}$, on a bien l'existence d'un tel r : il suffit de le prendre tel que $u^{jp} \lambda_1 r = x_{n+1}^{(j)} - \lambda_1 x_1^{(j)} - \ldots - \lambda_n x_n^{(j)}$. De plus, en appliquant N à cette dernière égalité, on voit que $N(u^{jp}\lambda_1 r) = \lambda_1 u^{jp} N(r) = 0$ et donc que $N(x_1^{(j+1)}) = 0$ puisque λ_1 est supposé non nul. Ceci implique la nullité de tous les $N(x_i^{(j+1)})$.

Pour $j = e$, l'égalité a lieu modulo u^{ep} et donc dans $\mathcal{M}$. Soit $\mathcal{K}$ le sous-$k[u]/u^{ep}$-module engendré par les $x_i^{(e)}$, pour $1 \leqslant i \leqslant n$. La liberté sur k des $\bar{x}_i$ assure que $\mathcal{K}$ est un module libre de rang n. Notons $\mathcal{M}_i$ le sous-module de $\mathcal{M}$ engendré par $x_i^{(e)}$, $\mathrm{Fil}^r\mathcal{M}_i = \mathrm{Fil}^r\mathcal{M} \cap \mathcal{M}_i$ et finalement $\mathrm{Fil}^r\mathcal{K} = \sum_{i=1}^n \mathrm{Fil}^r\mathcal{M}_i \cap \mathcal{K}$. Par construction, N stabilise $\mathcal{K}$ et ϕ_r envoie $\mathrm{Fil}^r\mathcal{K}$ sur $\mathcal{K}$. En outre, encore par construction l'image de la restriction de ϕ_r à $\mathrm{Fil}^r\mathcal{K}$ engendre $\mathcal{K}$: on voit que l'objet $\mathcal{K}$ est dans la catégorie $\widetilde{\underline{\mathrm{MF}}}^r$. Comme $\mathcal{M}$ est simple, ce sous-objet est tout $\mathcal{M}$. Ainsi on a prouvé la proposition suivante :

Proposition 4.1.1. *Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$. Alors $\mathcal{M}$ est dans la catégorie $\widetilde{\underline{MF}}^r$ et l'opérateur de monodromie N est nul sur $\mathrm{im}\,\phi_r$. De plus $\mathcal{M}$ admet une base adaptée de la forme $(x_1, \ldots, x_d)$ telle que $N(x_i) = 0$, $x_{i+1} = \varphi_r(x_i)$ (voir définition 3.2.2) et :*

$$\varphi_r(x_d) = \lambda_1 x_1 + \ldots + \lambda_d x_d$$

où les λ_i sont des éléments de k tels que $\lambda_1 \neq 0$.

qui admet pour corollaire immédiat la proposition 3.3.4 que l'on vient donc de démontrer.

4.2 Une base adaptée simple

Nous allons dans ce paragraphe préciser un peu plus l'énoncé de la proposition 4.1.1 dans le cas où le corps résiduel k est algébriquement clos.

Lemme 4.2.1. *Supposons k algébriquement clos. Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$. Alors $\mathcal{M}$ est dans $\widetilde{\underline{\mathcal{M}}}^r$ et il existe $(e_1, \ldots, e_d)$ une base adaptée de $\mathcal{M}$ telle que $N(e_i) = 0$, $e_{i+1} = \varphi_r(e_i)$, les indices i étant considérés dans $\mathbb{Z}/d\mathbb{Z}$.*

Démonstration. On sait d'après la proposition précédente qu'il existe une base adaptée $(x_1, \ldots, x_d)$ telle que $\varphi_r(x_i) = x_{i+1}$ pour i compris entre 1 et $d-1$ et $\varphi_r(x_d) = \lambda_1 x_1 + \ldots + \lambda_d x_d$ où $\lambda_i \in k$ et $\lambda_1 \neq 0$.

Parmi toutes les bases adaptées qui vérifient ces conditions, choisissons-en une pour laquelle le nombre de λ_i non nuls est minimal. On écrit alors plutôt :

$$x_{d+1} = \varphi_r(x_d) = \lambda_1 x_{i_1} + \ldots + \lambda_k x_{i_k}$$

où tous les λ_i sont non nuls et les indices i_k sont compris entre 1 et d. De plus, on a $i_1 = 1$. Notons pour tout i, n_i le plus petit entier tel que $u^{n_i} x_i \in \mathrm{Fil}^r\mathcal{M}$. Si tous les n_{i_j} n'étaient pas égaux, $\varphi_r(x_{d+1})$ s'écrirait comme une combinaison linéaire de $x_2, \ldots, x_{d+1}$ faisant intervenir strictement moins de k termes et la famille $(x_2, \ldots, x_{d+1})$ fournirait une base adaptée de $\mathcal{M}$ (en reprenant l'étude faite de le paragraphe précédent). Mais ceci est en contradiction avec la minimalité considérée.

Ainsi tous les n_{i_j} sont égaux et donc égaux à n_{d+1}. Par récurrence, on prouve que pour tout entier fixé a, tous les n_{i_j+a} sont égaux, les indices $i_j + a$ étant considérés modulo d.

Notons t le plus grand commun diviseur de d et de toutes les différences $i_j - i_{j'}$. D'après ce qui précède la suite des n_i est périodique de période (divisant) t. On considère alors le sous-k-espace vectoriel de $\mathcal{M}$ engendré par les x_{tn} où n parcourt $\mathbb{Z}/d\mathbb{Z}$. L'application φ_r^t stabilise ce sous-espace et y est ϕ^t-semi-linéaire. En particulier, puisque k est algébriquement clos, il existe un élément e_1 de ce sous-espace tel que $\varphi_r^t(e_1) = \lambda e_1$ pour un certain $\lambda \in k^\star$. Quitte à multiplier e_1 par un élément de k, on peut supposer $\lambda = 1$.

On définit $e_{i+1} = \varphi_r(e_i)$. La famille $(e_1, \ldots, e_t)$ engendre un espace stable par N et par ϕ_r qui est par construction un sous-objet non nul de $\mathcal{M}$. C'est donc tout $\mathcal{M}$. De plus, d'après la proposition 4.1.1, $N(e_i) = 0$ pour tout i. Finalement $(e_1, \ldots, e_t)$ est une base adaptée vérifiant les conditions du lemme. Cela conclut. □

4.3 Classification proprement dite

Définition 4.3.1. *Soit (n_i) une suite périodique*[4] *d'entiers compris entre* 0 *et* er. *On note* h *la période de cette suite. On définit l'objet* $\mathcal{M}(n_i) \in \widetilde{\underline{\mathcal{M}}}^r$ *de la façon suivante :*

1. $\mathcal{M}(n_i) = \bigoplus_{i \in \mathbb{Z}/h\mathbb{Z}} k[u]/u^{ep}e_i$;
2. $Fil^r \mathcal{M}(n_i) = \bigoplus_{i \in \mathbb{Z}/h\mathbb{Z}} u^{n_i} k[u]/u^{ep}e_i$;
3. $\phi_r(u^{n_i}e_i) = e_{i+1}$ *pour tout indice* i ;
4. $N(e_i) = 0$ *pour tout indice* i.

Il est facile de vérifier que tous ces objets sont bien dans la catégorie $\widetilde{\underline{\mathcal{M}}}^r$ et on a le théorème suivant :

Théorème 4.3.2. *Supposons* k *algébriquement clos. Les objets* $\mathcal{M}(n_i)$ *sont des objets simples de la catégorie* $\widetilde{\underline{\mathcal{M}}}^r$. *De plus, si* $\mathcal{M}$ *est un objet simple de la catégorie* $\widetilde{\underline{\mathcal{M}}}^r$, *alors il est isomorphe à un certain* $\mathcal{M}(n_i)$.

Démonstration. Voyons d'abord la simplicité de $\mathcal{M}(n_i)$. Soit $\mathcal{M}$ un sous-objet non nul de $\mathcal{M}(n_i)$. L'image de la restriction de ϕ_r à $\mathcal{M} \cap \mathrm{Fil}^r \mathcal{M}(n_i)$ est supposée engendrer tout $\mathcal{M}$; en particulier elle n'est pas réduite à 0 et comprend un élément non divisible par u^p, disons x. On écrit $x = \lambda_1 e_1 + \ldots + \lambda_h e_h$ où les λ_i sont des polynômes à coefficients dans $k[u^p]/u^{ep}$. On peut supposer $\lambda_i \in k$ quitte à remplacer x par $\varphi_r \circ \varphi_r \circ \varphi_r(x)$.

Considérons un x pour lequel le nombre de λ_i non nuls est minimal et écrivons :

$$x = \lambda_1 e_{i_1} + \ldots + \lambda_k e_{i_k}$$

avec ici tous les λ_i non nuls. En appliquant φ_r éventuellement plusieurs fois, on voit que tous les n_{i_j} doivent être égaux car sinon, on obtient un nouvel x qui serait combinaison d'un nombre plus petit de e_i. On applique alors φ_r à l'égalité précédente et comme précédemment, on prouve que tous les n_{i_j+1} sont égaux. Par récurrence, on voit que pour a fixé tous les n_{i_j+a} sont égaux. Ainsi, pour que la suite (n_i) soit périodique de période exactement h, il faut que $k = 1$, c'est-à-dire que x soit multiple de l'un des e_i. Mais alors le sous-objet engendré par x est tout $\mathcal{M}(n_i)$ et finalement $\mathcal{M} = \mathcal{M}(n_i)$. Ce qui assure la simplicité.

Voyons la réciproque. On applique le lemme 4.2.1 qui donne une description explicite de l'objet $\mathcal{M}$. Il reste juste à démontrer que la suite (n_i) ne peut-être périodique de période divisant strictement h. Mais supposons que ce soit le cas et notons t cette période. On considère le sous-objet engendré par l'élément $x = e_t + e_{2t} + \ldots + e_h$ et on vérifie immédiatement qu'il est non nul et strictement inclus dans $\mathcal{M}$. C'est une contradiction. □

Remarque. En utilisant la correspondance de [8], on retrouve exactement la classification donnée par Raynaud dans [19].

[4]Par « périodique », on entend dans ce papier « périodique dès le début » et pas « périodique à partir d'un certain rang ».

Étude des endomorphismes

On suppose toujours le corps k algébriquement clos. Soit $\mathcal{M}$ un objet simple de $\widetilde{\underline{\mathcal{M}}}^r$. Soit $(e_1, \ldots, e_h)$ une base adaptée de $\mathcal{M}$ vérifiant les conditions du théorème 4.3.2. Nous allons en fait voir que les e_i sont presque uniquement déterminés. Plus précisément, on a :

Théorème 4.3.3. *Supposons k algébriquement clos. Si $\lambda \in k$ vérifie $\lambda^{p^h} = \lambda$, alors l'application $\psi : \mathcal{M} \to \mathcal{M}$ définie par $\psi(e_i) = \lambda^{p^i} e_i$ est un endomorphisme de $\mathcal{M}$. Ce sont les seuls.*

Démonstration. Déjà il est facile de vérifier que les applications définies dans l'énoncé du théorème sont bien compatibles au Fil^r, au Frobenius et à l'opérateur de monodromie.

Pour la réciproque, nous allons anticiper sur des résultats ultérieurs donnant une application non nulle $\mathrm{End}(\mathcal{M}) \to \mathrm{End}(T_{\mathrm{st}}(\mathcal{M}))$ (la non-nullité se déduit de la fidélité du foncteur T_{st}, voir corollaire 5.3.4). D'autre part $\mathrm{End}(\mathcal{M})$ est un corps *a priori* non commutatif et $\mathrm{End}(T_{\mathrm{st}}(\mathcal{M}))$ est un corps fini à p^h éléments (cela se déduit de théorème 5.2.2). On en déduit facilement que la flèche $\mathrm{End}(\mathcal{M}) \to \mathrm{End}(T_{\mathrm{st}}(\mathcal{M}))$ est bijective, ce qui prouve le théorème. $\square$

Corollaire 4.3.4. *Les objets simples $\mathcal{M}(n_i)$ et $\mathcal{M}(m_i)$ sont isomorphes si et seulement si la suite (m_i) se déduit de la suite (n_i) par translation.*

Démonstration. Si deux objets $\mathcal{M}(n_i)$ et $\mathcal{M}(m_i)$ sont isomorphes, on peut transporter une base adaptée de $\mathcal{M}(n_i)$ à $\mathcal{M}(m_i)$ et le théorème précédent entraîne la conclusion voulue. $\square$

Un autre point de vue

Donnons finalement un point de vue différent sur cette classification, peut-être plus agréable à retenir.

Soit $(n_i)_{i \in \mathbb{N}}$ une suite quelconque d'entiers compris entre 0 et $p-1$ et soit t le rationnel dont le développement « décimal » en base p est :

$$t = 0\,,\, n_1\, n_2\, n_3\, n_4\ \ldots$$

On a une propriété classique :

Propriété 4.3.5. *Avec les notations précédentes, les suites périodiques sont exactement celles qui correspondent aux rationnels de $\mathbb{Z}_{(p)} \cap [0,1]$ où $\mathbb{Z}_{(p)}$ désigne le localisé de $\mathbb{Z}$ en p.*

On peut alors poser la définition suivante :

Définition 4.3.6. *Soit $\mathcal{R}$ l'ensemble des classes d'équivalence d'éléments de $\mathbb{Z}_{(p)}$ pour la relation d'équivalence suivante : $a \sim b$ si et seulement s'il existe un entier n tel que $a \equiv p^n b \pmod{\mathbb{Z}}$.*

La dernière relation d'équivalence n'est pas mystérieuse : elle correspond simplement à un décalage des décimales du nombre. En particulier, à cause de la périodicité, les classes d'équivalence sont toutes finies.

Dans ces conditions, $\mathcal{R}$ classifie exactement les objets simples de la catégorie $\underline{\mathcal{M}}^r$ (*via* la correspondance que l'on a décrite précédemment).

Nous verrons par la suite que le « *rationnel classifiant* » va réapparaître de façon naturelle.

5 Étude du foncteur T_{st}

5.1 Un système préliminaire

Ce paragraphe présente une version légèrement différente de résultats classiques et par exemple déjà discutés dans [22] ou dans le paragraphe 3.3.2 de [3]. On suppose dans ce paragraphe que le corps résiduel k est algébriquement clos.

On considère un entier h strictement postitif. On fixe $\eta^{(h)}$ une racine (p^h-1)-ième de l'uniformisante π de K et on appelle $K^{(h)}$ l'extension de K engendrée par cette racine. On rappelle que $K^{(h)}/K$ est totalement et modérément ramifiée de degré p^h-1. On rappelle également que la limite inductive de toutes ces extensions est l'extension maximale modérément ramifiée de K. Par la suite, lorsqu'il n'y aura pas de risque d'ambiguité, on notera η à la place de $\eta^{(h)}$. On rappelle enfin que π_1 désigne une racine p-ième de π.

On s'intéresse au système d'équations suivant :

$$(S) : \left\{ \begin{array}{rcl} \frac{\left(\pi_1^{n_1}\hat{x}_1+\hat{c}_1\right)^p}{\pi^{er}} & = & \varpi\hat{x}_2+\hat{r}_1 \\ \frac{\left(\pi_1^{n_2}\hat{x}_2+\hat{c}_2\right)^p}{\pi^{er}} & = & \varpi\hat{x}_3+\hat{r}_2 \\ & \vdots & \\ \frac{\left(\pi_1^{n_h}\hat{x}_h+\hat{c}_h\right)^p}{\pi^{er}} & = & \varpi\hat{x}_1+\hat{r}_h \end{array} \right.$$

où $\varpi \in \{-1,1\}$ est un signe, les n_i sont des entiers fixés tous compris entre 0 et er, et où les $\hat{r}_i$ et les $\hat{c}_i$ sont des éléments de $\mathcal{O}_{\bar{K}}$. Les inconnues sont les $\hat{x}_i$ que l'on cherche également dans $\mathcal{O}_{\bar{K}}$. On pose dans la suite $m_i = er - n_i$.

Sans coefficient constant

On s'intéresse tout d'abord au cas où toutes les constantes $\hat{r}_i$ et $\hat{c}_i$ sont nulles. Il est alors possible de résoudre directement le système dans $\mathcal{O}_{\bar{K}}$. En effet, le système se réécrit simplement :

$$\hat{x}_i^p = \varpi\pi^{m_i}\hat{x}_{i+1}.$$

Par des manipulations simples, on voit que $\hat{x}_1$ doit être solution de l'équation :

$$\hat{x}_1^{p^h} = \varpi^h\pi^{s_1}\hat{x}_1$$

où s_1 est défini par la formule :

$$s_1 = m_1p^{h-1} + m_2p^{h-2} + \ldots + m_{h-1}p + m_h.$$

Cette équation admet p^h solutions qui sont 0 et toutes les racines (p^h-1)-ièmes de $\varpi^h\pi^{s_1}$. À partir de $\hat{x}_1$, on reconstruit les autres $\hat{x}_i$ et on vérifie qu'ils forment bien une solution du système.

On peut présenter les choses de façon plus homogène en procédant comme suit. On pose pour tout $i \in \mathbb{Z}/h\mathbb{Z}$:

$$s_i = m_ip^{h-1} + m_{i+1}p^{h-2} + \ldots + m_{i+h-2}p + m_{i+h-1}.$$

Si ε est une racine (p^h-1)-ième de ϖ^h (qui est déjà dans K), la famille des $\hat{x}_i = \varpi^i\varepsilon^{p^i}\eta^{s_i}$ est une solution de (S). Toutes les solutions s'obtiennent ainsi à l'exception de la solution nulle $\hat{x}_1 = \ldots = \hat{x}_h = 0$.

Un lemme à la Hensel

On ne suppose plus que les constantes sont nulles et on cherche un lien entre les solutions de (S) modulo p et les solutions de (S) dans $\mathcal{O}_{\bar{K}}$:

Lemme 5.1.1. *Avec les notations précédentes, si le système (S) admet une solution $(x_1, \ldots, x_h)$ modulo p, alors cette solution se relève dans $\mathcal{O}_{\bar{K}}$ en une solution $(\hat{x}_1, \ldots, \hat{x}_h)$.*

Démonstration. On construit cette solution par approximations successives. Fixons tout d'abord une extension finie L de $K^{(h)}$ suffisamment grande pour contenir tous les $\hat{r}_i$, les $\hat{c}_i$ et pour que tous les x_i puissent s'y relever. L'extension $L/K^{(h)}$ est totalement ramifiée (puisque k est supposé algébriquement clos), disons de degré d. Notons $\mathcal{O}_L$ l'anneau des entiers de L.

On va construire une suite de $(x_1^{(n)}, x_2^{(n)}, \ldots, x_h^{(n)})$ de solutions compatibles du système (S) modulo η^n dans $\mathcal{O}_L$. Il suffira par la suite de prendre la limite de cette suite pour avoir une solution du système dans $\mathcal{O}_L$ et donc dans $\mathcal{O}_{\bar{K}}$.

On a déjà, par hypothèse, un h-uplet pour $n = e\left(p^h - 1\right)$. Les suivants se construisent par récurrence. On part d'un entier $n \geqslant e\left(p^h - 1\right)$ et d'éléments $x_1^{(n)}, \ldots, x_h^{(n)}$ vérifiant :

$$\frac{\left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i\right)^p}{\pi^{er}} \equiv \varpi x_{i+1}^{(n)} + \hat{r}_i \pmod{\eta^n}$$

pour tout indice i pris dans $\mathbb{Z}/h\mathbb{Z}$ et on cherche à construire $y_1, \ldots, y_h$, tels que :

$$\frac{\left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i + \pi_1^{n_i}\eta^n y_i\right)^p}{\pi^{er}} \equiv \varpi\left(x_{i+1}^{(n)} + \eta^n y_{i+1}\right) + \hat{r}_i \pmod{\eta^{n+1}}$$

Un calcul donne :

$$\frac{\left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i + \pi_1^{n_i}\eta^n y_i\right)^p}{\pi^{er}} = \frac{\left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i\right)^p}{\pi^{er}} + \sum_{k=1}^{p} \binom{p}{k} \frac{\pi_1^{kn_i}\eta^{kn}}{\pi^{er}} y_i^k \left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i\right)^{p-k}$$

Soit un entier $k \geqslant 1$. On a $v\left(\frac{\pi_1^{kn_i}\eta^{kn}}{\pi^{er}}\right) = \frac{kn_i}{p} + \frac{kn}{p^h-1} - er$. D'autre part, $\frac{(\pi_1^{n_i}x_i^{(n)}+\hat{c}_i)^p}{\pi^{er}}$ est un entier, donc de valuation positive et on en déduit que $v(\pi_1^{n_i}x_i^{(n)} + \hat{c}_i) \geqslant \frac{er}{p}$. On obtient :

$$\begin{aligned} v_k = v\left(\frac{\pi_1^{kn_i}\eta^{kn}}{\pi^{er}} \left(\pi_1^{n_i} x_i^{(n)} + \hat{c}_i\right)^{p-k}\right) &\geqslant \frac{kn}{p^h-1} + \frac{kn_i}{p} - er + (p-k)\frac{er}{p} \\ &= \frac{n}{p^h-1} + (k-1)\frac{n}{p^h-1} - \frac{km_i}{p} \end{aligned}$$

Comme par hypothèse $n \geqslant e\left(p^h - 1\right)$ et $m_i \leqslant er$, il vient :

$$v_k \geqslant \frac{n}{p^h-1} + e(k-1) - \frac{ker}{p} = \frac{n}{p^h-1} - e + ek\left(1 - \frac{r}{p}\right)$$

Maintenant si $k < p$, le coefficient binomial $\binom{p}{k}$ est multiple de p et donc :

$$v\left(\binom{p}{k}\frac{\pi_1^{kn_i}\eta^{nk}}{\pi^{er}}\left(\pi_1^{n_i}x_i^{(n)} + \hat{c}_i\right)^{p-k}\right) \geqslant e + v_k \geqslant \frac{n}{p^h-1} + ek\left(1 - \frac{r}{p}\right) \geqslant \frac{n+1}{p^h-1}$$

la dernière inégalité résultant du fait que $r \leqslant er \leqslant p-2$.

On en déduit que tous les termes de la somme pour k compris strictement entre 0 et p sont nuls modulo η^{n+1}. En fait, c'est aussi le cas pour $k=p$. En reprenant les égalités précédentes, on voit que :

$$v_p \geqslant \frac{n}{p^h-1} + e\,(p-1-r)$$

mais $p-1-r \geqslant 1$ et donc on a également $v_p \geqslant \frac{n+1}{p^h-1}$. Finalement le système que l'on a à résoudre se réduit à :

$$\frac{\left(\pi_1^{m_i} x_i^{(n)} + \hat{c}_i\right)^p}{\pi^{er}} \equiv \varpi \left(x_{i+1}^{(n)} + \eta^n y_i\right) + \hat{r}_i \pmod{\eta^{n+1}}$$

mais on sait que la différence $\frac{(\pi_1^{m_i} x_i^{(n)} + \hat{c}_i)^p}{\pi^{er}} - \varpi x_{i+1}^{(n)} - \hat{r}_i$ est un multiple de η^n, et donc s'écrit $\eta^n q_i$. Il suffit ensuite de choisir $y_i = \varpi q_i$ pour avoir la solution que l'on cherchait. $\square$

Résolution du système

Une première conséquence du lemme que l'on vient de prouver est la résolution du système (S) modulo p lorsque les constantes $\hat{r}_i$ et $\hat{c}_i$ sont toutes nulles :

Lemme 5.1.2. *Supposons que les constantes $\hat{r}_i$ et $\hat{c}_i$ soient nulles. Mise à part la solution nulle, les solutions de (S) dans $\mathcal{O}_{\bar{K}}/p$ s'écrivent $x_i = \varpi^i \varepsilon^{p^i} \bar{\eta}^{s_i}$ où $\varepsilon \in \mathcal{O}_K$ est une racine $\left(p^h-1\right)$-ième de ϖ^h, $\bar{\eta}$ est la réduction de η dans $\mathcal{O}_{\bar{K}}/p$ et :*

$$s_i = m_i p^{h-1} + m_{i+1} p^{h-2} + \ldots + m_{i+h-2} p + m_{i+h-1}.$$

Démonstration. Si ε est une racine $\left(p^h-1\right)$-ième de ϖ^h et si x_i désigne la réduction modulo p de $\varpi^i \varepsilon^{p^i} \eta^{s_i}$, le uplet $(x_1, \ldots, x_h)$ est solution du système dans $\mathcal{O}_{\bar{K}}/p$. De plus, si ε et ε' sont deux racines $\left(p^h-1\right)$-ièmes de ϖ^h distinctes, on a pour tout entier i, $\varepsilon^{p^i} \neq \varepsilon'^{p^i}$ dans le corps résiduel et donc $\varepsilon^{p^i} - \varepsilon'^{p^i}$ est de valuation nulle. On en déduit, puisque $v(\eta^{s_i}) = \frac{s_i}{p^h-1} < 1$, que $x_i = \varpi^i \varepsilon^{p^i} \eta^{s_i}$ et $x'_i = \varpi^i \varepsilon'^{p^i} \eta^{s_i}$ sont distincts dans $\mathcal{O}_{\bar{K}}/p$.

On a ainsi trouvé p^h solutions à (S) modulo p. Le lemme 5.1.1 assure qu'il y en a au moins autant dans $\mathcal{O}_{\bar{K}}$. Mais on a vu qu'il y en a exactement p^h dans $\mathcal{O}_{\bar{K}}$, on les a donc toutes. $\square$

Passons au cas général. On reprend le système (S) mais on ne suppose plus la nullité de $\hat{r}_i$ et de $\hat{c}_i$.

Théorème 5.1.3. *Supposons que le système (S) admette une solution dans $\mathcal{O}_{\bar{K}}$, alors il admet toujours p^h solutions dans $\mathcal{O}_{\bar{K}}$ et p^h solutions dans $\mathcal{O}_{\bar{K}}/p$. De plus l'application de réduction modulo p définit une bijection entre ces ensembles de solutions.*

En outre si $(x_1, \ldots, x_h)$ et $(y_1, \ldots, y_h)$ sont deux solutions distinctes dans $\mathcal{O}_{\bar{K}}/p$, alors il existe ε une racine $\left(p^h-1\right)$-ième de ϖ^h telle que $y_i = x_i + \varpi^i \varepsilon^{p^i} \eta^{s_i}$ pour tout indice $i \in \mathbb{Z}/h\mathbb{Z}$ où s_i est défini par la formule :

$$s_i = m_i p^{h-1} + m_{i+1} p^{h-2} + \ldots + m_{i+h-2} p + m_{i+h-1}$$

Démonstration. Soit $(\hat{x}_1, \ldots, \hat{x}_h)$ une solution de (S) dans $\mathcal{O}_{\bar{K}}$. Si l'on note $x_i \in \mathcal{O}_{\bar{K}}/p$ la réduction modulo p de $\hat{x}_i$, le uplet $(x_1, \ldots, x_h)$ est solution de (S) modulo p. Prenons ε une racine $\left(p^h-1\right)$-ième de ϖ^h et posons $y_i = x_i + \varpi^i \varepsilon^{p^i} \eta^{s_i}$. Un calcul donne :

$$\left(\pi_1^{n_i} \hat{x}_i + \pi_1^{n_i} \varpi^i \varepsilon^{p^i} \eta^{s_i} + \hat{c}_i\right)^p = (\pi_1^{n_i} \hat{x}_i + \hat{c}_i)^p + \pi^{n_i} \varpi^i \varepsilon^{p^{i+1}} \eta^{p s_i} + \sum_{k=1}^{p-1} \binom{p}{k} \pi_1^{k n_i} \varpi^{k i} \varepsilon^{k p^i} \eta^{k s_i} \left(\pi_1^{n_i} \hat{x}_i + \hat{c}_i\right)^{p-k}$$

Or les $\hat{x}_i$ forment une solution de (S) et donc on a $v(\pi_1^{n_i}\hat{x}_i + \hat{c}_i) \geqslant \frac{er}{p}$. Également, on a $v\left(\eta^{s_i}\right) = \frac{s_i}{p^h-1} \geqslant \frac{m_i}{p}$. Finalement, on obtient :

$$v\left(\pi_1^{kn_i}\varpi^{ki}\varepsilon^{kp^i}\eta^{ks_i}\left(\pi_1^{n_i}\hat{x}_i + \hat{c}_i\right)^{p-k}\right) \geqslant k\frac{n_i}{p} + k\frac{m_i}{p} + (p-k)\frac{er}{p} = er$$

Ainsi tous les termes de la somme sont des multiples de $p\pi^{er}$. Modulo p, il reste :

$$\begin{aligned} \frac{1}{\pi^{er}}\left(\pi_1^{n_i}\hat{x}_i + \pi_1^{n_i}\varpi^i\varepsilon^{p^i}\eta^{s_i} + \hat{c}_i\right)^p &\equiv \frac{\left(\pi_1^{n_i}\hat{x}_i + \hat{c}_i\right)^p}{\pi^{er}} + \frac{\pi^{n_i}\varpi^i\varepsilon^{p^{i+1}}\eta^{ps_i}}{\pi^{er}} \pmod p \\ &\equiv \varpi\hat{x}_{i+1} + \hat{r}_i + \varpi\frac{\varpi^{i+1}\varepsilon^{p^{i+1}}\eta^{ps_i}}{\pi^{m_i}} \pmod p \end{aligned}$$

On remarque que $ps_i = s_{i+1} + m_i\left(p^h - 1\right)$, puis que $(y_1, \ldots, y_h)$ est solution de (S). On conclut en reprenant la démonstration du lemme 5.1.2. $\square$

Voici un dernier corollaire qui nous sera utile par la suite :

Corollaire 5.1.4. *Soit g un élément du groupe de Galois G_K qui fixe tous les $\hat{r}_i$, tous les $\hat{c}_i$ et π_1. Soit $(\hat{x}_1, \ldots, \hat{x}_h)$ une solution de (S) dans $\mathcal{O}_{\bar{K}}$. On note x_i la réduction modulo p de $\hat{x}_i$. Alors, pour tout $i \in \mathbb{Z}/h\mathbb{Z}$, g fixe $\hat{x}_i$ si et seulement si g fixe x_i.*

Démonstration. Il suffit de montrer que si g fixe les x_i alors $(g\hat{x}_1, \ldots, g\hat{x}_h)$ est aussi solution de (S). En effet, d'après le théorème précédent, si ces deux solutions sont distinctes dans $\mathcal{O}_{\bar{K}}$, elles le sont aussi modulo p. Le théorème 5.1.3 donne ceci : dans le cas où les deux solutions sont distinctes, dans $\mathcal{O}_{\bar{K}}$ comme dans $\mathcal{O}_{\bar{K}}/p$, toutes les « coordonnées » des h-uplets sont distinctes. Le corollaire en découle directement. $\square$

Remarque. Dans le cas où tous les $\hat{c}_i$ sont nuls, il existe toujours une solution au système dans $\mathcal{O}_{\bar{K}}$. En effet, en combinant les équations, on aboutit à une unique équation polynomiale à coefficients entiers que doit vérifier $\hat{x}_1$. Comme $\bar{K}$ est algébriquement clos, cette équation admet une solution.

5.2 Calcul sur les objets simples

Dans ce paragraphe uniquement, on suppose le corps résiduel k algébriquement clos. On suppose également que π est choisi tel que $\pi^e = p$, ce qui est toujours possible si $r > 0$ (si $r = 0$, les résultats se démontrent indépendemment et facilement). Ainsi $E(u) = u^e - p$ et $c_\pi = -1$. Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$. Le théorème 4.3.2 affirme que $\mathcal{M}$ est de la forme $\mathcal{M}(n_i)$ pour une certaine suite périodique (n_i). Notons h sa période.

L'image de $\mathcal{M}$ par le foncteur T_{st} s'identifie, comme le prouve le lemme 2.3.4, à l'ensemble $\mathrm{Hom}(\mathcal{M}, \hat{A})$. Se donner un tel morphisme revient à se donner pour tout i, un élément $x_i \in \hat{A}$, image de e_i, ces éléments x_i étant soumis à certaines relations que nous allons expliciter. On rappelle que d'après le lemme 2.3.3, l'anneau $\hat{A}$ s'identifie à $\left(\mathcal{O}_{\bar{K}}\langle X\rangle\right)/p$.

Lemme 5.2.1. *L'ensemble des $x \in \hat{A}$ tels que $N(x) = 0$ est $\mathcal{O}_{\bar{K}}/p$.*

Démonstration. Le lemme résulte directement du fait que $N(X)$ est une unité de $\hat{A}$. $\square$

De $N(e_i) = 0$, on déduit $N(x_i) = 0$ et donc d'après le lemme précédent $x_i \in \mathcal{O}_{\bar{K}}/p$. Intéressons-nous maintenant à la condition imposée par le Frobenius. Sur l'objet $\mathcal{M}$, ϕ_r est défini par $\phi_r(u^{n_i}e_i) = e_{i+1}$. Cela impose donc deux choses : l'élément $u^{n_i}x_i$ appartient à $\mathrm{Fil}^r(\mathcal{O}_{\bar{K}}\langle X\rangle)/p$ et on a l'égalité $\phi_r(u^{n_i}x_i) = x_{i+1}$.

On rappelle que l'on avait appelé p_1 (resp. π_1) une racine p-ième de p (resp. de π) et comme $\pi^e = p$, on peut supposer en outre que $\pi_1^e = p_1$. D'autre part, si $x = \sum_{i\geqslant 0} a_i \frac{X^i}{i!} \in \hat{A}$ ($a_i \in \mathcal{O}_{\bar{K}}/p$), alors $x \in \mathrm{Fil}^r\hat{A}$ si et seulement si a_i est un multiple de $\bar{p}_1^{r-i}$ pour tout entier i compris entre 0 et r. Comme, dans $\hat{A}$, $u = \frac{\pi_1}{1+X}$, on a $u^{n_i}x_i \in \mathrm{Fil}^r\hat{A}$ si et seulement si $\pi_1^{n_i}x_i \in \mathrm{Fil}^r\hat{A}$, c'est-à-dire $\pi_1^{er-n_i}$ divise x_i pour tout $i \in \mathbb{Z}/h\mathbb{Z}$.

Soit $\hat{x}_i$ un relevé de x_i dans $\mathcal{O}_{\bar{K}}$ qui est un multiple de $\pi_1^{er-n_i}$. Par définition $\phi_r(u^{n_i}x_i)$ est la réduction modulo p de :

$$\frac{1}{p^r}\cdot\phi\left(\frac{\pi_1^{n_i}}{(1+X)^{n_i}}\hat{x}_i\right) = \frac{(-1)^r}{p^r}\cdot\frac{\pi_1^{pn_i}}{(1+X)^{pn_1}}\hat{x}_i^p = (-1)^r\frac{1}{(1+X)^{pn_1}}\cdot\frac{1}{\pi^{er-n_i}}\hat{x}_i^p.$$

Or modulo p, $(1+X)^p = 1$ et finalement $\phi_r(u^{n_i}x_i) = (-1)^r\frac{x_i^p}{\pi^{er-n_i}}$.

Ces équations fournissent un système qui est exactement celui étudié dans le paragraphe 5.1 avec $\varpi = (-1)^r$ et $\hat{c}_i = \hat{r}_i = 0$. En particulier, le lemme 5.1.2 nous fournit directement les solutions.

On vient de prouver le théorème 1.0.3 dont nous rappelons l'énoncé :

Théorème 5.2.2. *Supposons k algébriquement clos et $er < p-1$. Si l'objet simple $\mathcal{M}$ s'identifie à $\mathcal{M}(n_i)$ pour une suite (n_i) périodique de période h (voir théorème 4.3.2), alors la représentation galoisienne $T_{st}(\mathcal{M})$ est isomorphe à :*

$$\theta_1^{m_1}\theta_2^{m_2}\dots\theta_h^{m_h}$$

où m_i est défini par $n_i + m_i = er$ et où les θ_i sont les caractères fondamentaux de niveau h.

En particulier, pour tout objet $\mathcal{M}$ de $\underline{\mathcal{M}}^r$ tué par p, les exposants qui décrivent l'action de l'inertie modérée sur la semi-simplifiée modulo p de $T_{st}(\mathcal{M})$ sont tous compris entre 0 et er.

5.3 Exactitude et fidélité

Exactitude

Théorème 5.3.1. *Le foncteur T_{st} de la catégorie $\underline{\mathcal{M}}^r$ dans la catégorie des $\mathbb{Z}_p$-représentations galoisiennes de torsion est exact.*

Démonstration. La preuve est en tout point semblable à celle donnée dans le paragraphe 3.2.1. de [3], et dans le paragraphe 2.3.1. de [6]. □

Fidélité

Commençons par le lemme suivant :

Lemme 5.3.2. *Supposons k algébriquement clos. L'image par le foncteur T_{st} d'un objet simple de $\underline{\mathcal{M}}^r$ est une représentation irréductible.*

Démonstration. Par le théorème 5.2.2, on connaît l'image d'un objet simple par le foncteur T_{st}. On vérifie directement que cette image est une représentation galoisienne irréductible. □

Corollaire 5.3.3. *Supposons k algébriquement clos. Si $\mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r$, on a :*

$$long\left(\mathcal{M}\right) = long\left(T_{st}\left(\mathcal{M}\right)\right)$$

Démonstration. Cela découle directement du lemme précédent et de l'exactitude. $\square$

Remarque. Ces deux derniers résultats restent vrais si k n'est pas algébriquement clos (voir théorème 6.4.4).

Corollaire 5.3.4. *Le foncteur T_{st} de la catégorie $\underline{\mathcal{M}}^r$ dans la catégorie des $\mathbb{Z}_p$-représentations galoisiennes de torsion est fidèle.*

Démonstration. Supposons dans un premier temps k algébriquement clos. Soit $f : \mathcal{X} \to \mathcal{Y}$ un morphisme dans la catégorie $\underline{\mathcal{M}}^r$ tel que $T_{\mathrm{st}}\left(f\right) = 0$. On a la suite exacte dans $\underline{\mathcal{M}}^r$:

$$0 \longrightarrow \ker f \longrightarrow \mathcal{X} \xrightarrow{\tilde{f}} \operatorname{im} f \longrightarrow 0$$

En outre l'application $\operatorname{im} f \to \mathcal{Y}$ est injective et donc la flèche déduite $T_{\mathrm{st}}\left(\mathcal{Y}\right) \to T_{\mathrm{st}}\left(\operatorname{im} f\right)$ est surjective. On en déduit que $T_{\mathrm{st}}(\tilde{f}) = 0$. En appliquant le foncteur exact T_{st} à la suite exacte écrite précédemment, on voit que $T_{\mathrm{st}}\left(\operatorname{im} f\right) = 0$. D'après le corollaire précédent, $\operatorname{im} f = 0$, puis $f = 0$.

Pour le cas général, notons K^{nr} le complété p-adique de l'extension maximale non ramifiée de K. Son corps résiduel s'identifie à une clôture algébrique $\bar{k}$ de k. Désignons par S_{nr} l'anneau S construit à partir de K^{nr} et par $\underline{\mathcal{M}}^r_{\mathrm{nr}}$ la catégorie de modules sur S_{nr}.

Si $\mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r$, alors $\mathcal{M}_{\mathrm{nr}} = S_{\mathrm{nr}} \otimes_S \mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r_{\mathrm{nr}}$ et l'application :

$$\begin{array}{rcl} T_{\mathrm{st}}\left(\mathcal{M}\right) & \to & T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}}) \\ f & \mapsto & \left[s \otimes x \mapsto sf\left(x\right)\right] \end{array}$$

est un isomorphisme commutant à l'action de $\mathrm{Gal}\left(\bar{K}/K^{\mathrm{nr}}\right)$. De plus, le morphisme $\iota_M : \mathcal{M} \to \mathcal{M}_{\mathrm{nr}}$, $x \mapsto 1 \otimes x$ est injectif.

Soit $f : \mathcal{X} \to \mathcal{Y}$ un morphisme dans la catégorie $\underline{\mathcal{M}}^r$ tel que $T_{\mathrm{st}}\left(f\right) = 0$. Il induit un morphisme $f_{\mathrm{nr}} : \mathcal{X}_{\mathrm{nr}} \to \mathcal{Y}_{\mathrm{nr}}$ de la catégorie $\underline{\mathcal{M}}^r_{\mathrm{nr}}$ et on a $T_{\mathrm{st}}(f_{\mathrm{nr}}) = 0$. Par la fidélité dans le cas algébriquement clos, il vient $f_{\mathrm{nr}} = 0$. La composée $\iota_{\mathcal{Y}} \circ f : \mathcal{X} \to \mathcal{Y}_{\mathrm{nr}}$ est nulle et comme $\iota_{\mathcal{Y}}$ est injectif, f est nulle. Ceci démontre la fidélité. $\square$

6 Pleine fidélité du foncteur T_{st}

Dans cette partie, on suppose à nouveau dans un premier temps que le corps résiduel k est algébriquement clos. La propriété de pleine fidélité reste valable sans cette hypothèse et nous verrons dans le dernier paragraphe comment le cas général se déduit simplement du cas « algébriquement clos ».

Par un argument classique (voir [13]), on se ramène à prouver le lemme suivant :

Lemme 6.0.5. *Soient $\mathcal{M}$ et $\mathcal{N}$ deux objets simples de $\underline{\mathcal{M}}^r$. Alors la flèche canonique $Ext^1\left(\mathcal{M}, \mathcal{N}\right) \to Ext^1\left(T_{st}\left(\mathcal{N}\right), T_{st}\left(\mathcal{M}\right)\right)$ est injective.*

6.1 Le module A_{ss}

Pour prouver le lemme 6.0.5, on considère $\mathcal{M}$ et $\mathcal{N}$ deux objets simples, $\mathcal{X}$ une extension dans la catégorie $\underline{\mathcal{M}}^r$ de ces deux objets telle que $T_{\text{st}}(\mathcal{X})$ soit isomorphe au produit direct $T_{\text{st}}(\mathcal{M}) \times T_{\text{st}}(\mathcal{N})$. Il nous faut montrer que $\mathcal{X}$ est isomorphe à $\mathcal{M} \times \mathcal{N}$.

Les hypothèses impliquent que $\mathcal{X}$ est tué par p. En effet, $T_{\text{st}}(\mathcal{X})$ est tué par p, ce qui signifie que la multiplication par p sur $T_{\text{st}}(\mathcal{X})$ est l'application nulle. Par fidélité, on en déduit que la multiplication par p sur $\mathcal{X}$ est également l'application nulle. Ainsi on peut travailler dans les catégories $\widetilde{\underline{\mathcal{M}}}^r$. D'autre part, si $r = 0$, il y a un unique objet simple à isomorphisme près, ce qui règle rapidement ce cas. Ainsi on peut supposer $r > 0$ et supposer à nouveau $\pi^e = p$.

Commençons par donner une caractérisation, faisant intervenir explicitement le foncteur T_{st}, des objets de $\widetilde{\underline{\mathcal{M}}}^r$ qui sont semi-simples.

On construit un sous-module A_{ss} de $\hat{A}$ (ss pour *semi-simple*). Pour cela, comme dans le paragraphe 5.1, on fixe, pour tout entier h, $\eta^{(h)}$ une racine $\left(p^h - 1\right)$-ième de l'uniformisante π. On impose en outre une condition de compatibilité : on demande que lorsque h' divise h, on ait :

$$\left(\eta^{(h')}\right)^{\frac{p^h-1}{p^{h'}-1}} = \eta^{(h)}$$

De cette façon, si $s \in \mathbb{Z}_{(p)}$ (le localisé de $\mathbb{Z}$ en p) on pourra sans ambiguité parler de π^s. En effet, comme tout nombre premier à p admet un multiple de la forme $p^h - 1$, on peut toujours écrire $s = \frac{a}{p^h-1}$, et poser :

$$\pi^s = \left(\eta^{(h)}\right)^a.$$

La condition de compatibilité dit précisément que le résultat ne dépend pas de la fraction choisie pour représenter s. En outre, on a les formules évidentes $\pi^s \times \pi^{s'} = \pi^{s+s'}$ et $\pi^{ns} = (\pi^s)^n$ si s et s' sont dans $\mathbb{Z}_{(p)}$ et si n est un entier.

Reprenons la description donnée tout à la fin du paragraphe 4.3. Choisissons un élément $t \in \mathcal{R}$ classifiant un certain objet simple $\mathcal{M}$ de la catégorie $\widetilde{\underline{\mathcal{M}}}^r$. Appelons $t_1, \ldots, t_h$ les rationnels de $\mathbb{Z}_{(p)} \cap [0,1[$ correspondant à t. Précisément si c'est la suite $(n_i)_{i \in \mathbb{Z}/h\mathbb{Z}}$ qui classifie $\mathcal{M}$, on aura :

$$t_i = 0\,,\, n_i n_{i+1} \ldots n_{i+h-1}\, \overline{n_i n_{i+1} \ldots n_{i+h-1}}\, \ldots$$

Si l'on pose $v_i = \frac{er}{p-1} - t_i$, on voit d'après le calcul fait dans le paragraphe 5.2 que tout élément de $T_{\text{st}}(\mathcal{M})$ tombe dans le sous-$k[u]/u^{ep}$-module de $\hat{A}$ engendré par les π^{v_i}. On pose, pour tout $t \in \mathcal{R}$:

$$A_{\text{ss}t} = k[u]/u^{ep} \cdot \pi^{v_1} + k[u]/u^{ep} \cdot \pi^{v_2} + \ldots + k[u]/u^{ep} \cdot \pi^{v_h}$$

où l'entier h dépend de t. La somme précédente est directe (voir lemme 6.1.2). Il faut faire attention au fait que les modules $k[u]/u^{ep} \cdot \pi^{v_i}$ ne sont pas libres, car par exemple on a toujours $u^{ep-1}\pi^{v_i} = 0$, sauf dans le cas très particulier où $h = 1$ et $n_1 = er$. En particulier $A_{\text{ss}t}$ n'est *pas* isomorphe à $\mathcal{M}$.

Définition 6.1.1. *On pose :*

$$A_{ss} = \sum_{t \in \mathcal{R}} A_{sst} \subset \hat{A}.$$

Autrement dit, A_{ss} est le sous-$k[u]/u^{ep}$-module engendré par les $\pi^{t'}$ où t' parcourt l'ensemble des rationnels de $\mathbb{Z}_{(p)} \cap [0,1[$ dont l'écriture « décimale » en base p ne comporte que des chiffres compris entre 0 et er.

Lemme 6.1.2. *Le morphisme évident :*

$$\bigoplus_{t'} k\,[u]\,/u^{ep} \cdot \pi^{t'} \to A_{ss}$$

est un isomorphisme (où la somme est à nouveau étendue aux t' rationnels compris strictement entre 0 *et* 1 *et dont l'écriture « décimale » en base p ne comporte que des chiffres compris entre* 0 *et er).*

Avant de faire la démonstration, insistons sur le fait que la notation est trompeuse : le module $k\,(u)\,/u^{ep} \cdot \pi^{t'}$ n'est pas libre, il doit être vu comme un sous-module de $\hat{A}$. Le lemme dit donc que la somme dans $\hat{A}$ de tous ces sous-modules est directe.

Démonstration. La surjectivité est une conséquence immédiate de la définition de A_{ss}. Passons à l'injectivité. Considérons une relation de la forme :

$$P_1\,(u)\,\pi^{v_1} + \ldots + P_n\,(u)\,\pi^{v_n} = 0$$

où les v_i sont deux à deux distincts et où on peut supposer que tous les polynômes $P_i \in k\,[u]\,/u^{ep}$ sont non nuls. Il faut alors montrer que tous les termes de la somme $P_i\,(u)\,\pi^{v_i}$ sont nuls, et ceci va résulter d'un simple calcul de valuation.

On écrit $u = \pi_1 X'^{p-1}$ où l'on rappelle que $X' = 1 + X$ vérifie la relation $X'^p = 1$. En identifiant les coefficients en X', on obtient pour tout j compris entre 0 et $p-1$ des égalités de la forme :

$$P_1^{(j)}\,(\pi)\,\pi^{v_1} + \ldots + P_n^{(j)}\,(\pi)\,\pi^{v_n} = 0$$

où les $P_i^{(j)}$ sont des polynômes à coefficients dans k . On rappelle que l'on dispose d'une valuation sur $\mathcal{O}_{\bar{K}}/p$ et que le fait d'être nul signifie simplement d'être de valuation supérieure à e. La valuation de $P_i^{(j)}\,(\pi)$ est un entier. Comme $v_i \in \mathbb{Z}_{(p)} \cap [0,1[$, et que tous les v_i sont deux à deux distincts, les valuations de $P_i^{(j)}\,(\pi)\,\pi^{v_i}$ sont aussi deux à deux distinctes, et on a :

$$v\left(P_1^{(j)}\,(\pi)\,\pi^{v_1} + \ldots + P_n^{(j)}\,(\pi)\,\pi^{v_n}\right) = \min_i v\left(P_i^{(j)}\,(\pi)\,\pi^{v_i}\right)$$

En particulier, la somme est nulle si et seulement si tous les termes sont nuls, ce qui est bien ce que l'on voulait prouver. □

Soit $\mathcal{X}$ un objet de la catégorie $\widetilde{\underline{\mathcal{M}}}^r$. L'injection $A_{\mathrm{ss}} \to \hat{A}$ fournit une flèche injective $\mathrm{Hom}\,(\mathcal{X}, A_{\mathrm{ss}}) \to T_{\mathrm{st}}\,(\mathcal{X})$.

Lemme 6.1.3. *L'objet $\mathcal{X}$ est semi-simple si et seulement si la flèche précédente est surjective (et donc un isomorphisme).*

Démonstration. Le sens direct est facile : si $\mathcal{X}$ est semi-simple et s'écrit donc comme la somme $\mathcal{X} = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_n$ pour certains objets simples $\mathcal{M}_i$, alors $T_{\mathrm{st}}\,(\mathcal{X})$ se décompose lui aussi comme la somme directe :

$$T_{\mathrm{st}}\,(\mathcal{X}) = T_{\mathrm{st}}\,(\mathcal{M}_1) \oplus \ldots \oplus T_{\mathrm{st}}\,(\mathcal{M}_n)$$

et on a déjà vu que $T_{\mathrm{st}}\,(\mathcal{M}_i) = \mathrm{Hom}\,(\mathcal{M}_i, A_{\mathrm{ss}})$.

Faisons la réciproque. Le lemme 2.3.1.2 de [6] affirme que le cardinal de $T_{\mathrm{st}}\,(\mathcal{X})$ est $p^{\mathrm{rg}\,\mathcal{X}}$ où $\mathrm{rg}\,\mathcal{X}$ désigne le rang de $\mathcal{X}$ en tant que $k\,[u]\,/u^{ep}$-module. On prouve par récurrence sur la longueur de l'objet $\mathcal{X}$ que $\operatorname{Card}\operatorname{Hom}(\mathcal{X}, A_{\mathrm{ss}}) \leqslant p^{\operatorname{rg}\mathcal{X}}$ et qu'il y a égalité si et seulement si $\mathcal{X}$ est semi-simple. Cela entraînera bien le résultat annoncé dans le lemme.

Le résultat est évident si $\mathcal{X}$ est simple (de longueur 1). Prenons un objet $\mathcal{X}$ de longueur $n+1$. Il existe une suite exacte courte de la forme :

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{X} \longrightarrow \mathcal{N} \longrightarrow 0$$

où $\mathcal{M}$ est un objet simple et $\mathcal{N}$ est un objet de $\underline{\widetilde{\mathcal{M}}}^r$ de longueur n. Par application du foncteur contravariant $\operatorname{Hom}(\cdot, A_{\mathrm{ss}})$, on en déduit une suite exacte à gauche :

$$0 \longrightarrow \operatorname{Hom}(\mathcal{N}, A_{\mathrm{ss}}) \longrightarrow \operatorname{Hom}(\mathcal{X}, A_{\mathrm{ss}}) \longrightarrow \operatorname{Hom}(\mathcal{M}, A_{\mathrm{ss}})$$

d'où :

$$\operatorname{Card}\operatorname{Hom}(\mathcal{X}, A_{\mathrm{ss}}) \leqslant \operatorname{Card}\operatorname{Hom}(\mathcal{N}, A_{\mathrm{ss}}) \cdot \operatorname{Card}\operatorname{Hom}(\mathcal{M}, A_{\mathrm{ss}}) \leqslant p^{\operatorname{rg}\mathcal{N}} \cdot p^{\operatorname{rg}\mathcal{M}} = p^{\operatorname{rg}\mathcal{X}}$$

Pour que les deux inégalités précédentes soient des égalités, il faut que la flèche $\operatorname{Hom}(\mathcal{X}, A_{\mathrm{ss}}) \to \operatorname{Hom}(\mathcal{M}, A_{\mathrm{ss}})$ soit surjective et que $\operatorname{Card}\operatorname{Hom}(\mathcal{N}, A_{\mathrm{ss}}) = p^{\operatorname{rg}\mathcal{N}}$. D'après l'hypothèse de récurrence, cette dernière condition implique que $\mathcal{N}$ est semi-simple.

Exploitons la première condition. Soit $\psi \in \operatorname{Hom}(\mathcal{M}, A_{\mathrm{ss}})$, $\psi \neq 0$. Si t désigne le « rationnel classifiant » de $\mathcal{M}$, ψ tombe dans un $A_{\mathrm{ss}t}$ qui est un facteur direct de A_{ss}. Par hypothèse, ψ se prolonge à tout $\mathcal{X}$. On s'intéresse à la composée $s : \mathcal{X} \to A_{\mathrm{ss}} \to A_{\mathrm{ss}t}$ où la première flèche est ψ ainsi prolongée et la seconde flèche est la projection canonique.

Notons $(e_1, \ldots, e_d)$ une base adaptée de $\mathcal{X}$ pour les entiers $n_1, \ldots, n_d$ et notons pour tout i, f_i un relevé de $s(e_i)$ dans $\mathcal{M}$, qui existe puisque tous les morphismes non nuls $\mathcal{M} \to A_{\mathrm{ss}t}$ sont surjectifs. Nous allons corriger les f_i pour que la flèche $s : \mathcal{X} \to \mathcal{M}, e_i \mapsto f_i$ définisse un scindage de :

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{X} \longrightarrow \mathcal{N} \longrightarrow 0\,.$$

Les f_i sont uniques modulo $u^e \operatorname{Fil}^r \mathcal{X}$ (on peut faire beaucoup mieux en fait, mais ce ne sera pas utile). En particulier, quelle que soit la façon de les choisir, la flèche s obtenue respecte Fil^r. D'autre part, on a :

$$\begin{pmatrix} \phi_r(u^{n_i} f_i) \\ \vdots \\ \phi_r(u^{n_d} f_d) \end{pmatrix} = {}^t G \begin{pmatrix} f_i \\ \vdots \\ f_d \end{pmatrix} + \begin{pmatrix} r_i \\ \vdots \\ r_d \end{pmatrix}$$

où G désigne la matrice de ϕ_r dans la base adaptée $(e_1, \ldots, e_d)$ et où les r_i sont des éléments de $u^e \operatorname{Fil}^r \mathcal{X}$. On voit donc que si l'on remplace le vecteur $\begin{pmatrix} f_i \\ \vdots \\ f_d \end{pmatrix}$ par le vecteur $\begin{pmatrix} f_i \\ \vdots \\ f_d \end{pmatrix} + {}^t G^{-1} \begin{pmatrix} r_i \\ \vdots \\ r_d \end{pmatrix}$, on obtient une flèche compatible à Fil^r et à ϕ_r.

Pour prouver que cette rétraction est également compatible à N, on considère le diagramme commutatif suivant :

$$\begin{tikzcd}
 & \operatorname{Fil}^r\mathcal{M} \arrow[rr, "\phi_r"] \arrow[dd, "u^eN"' near end] & & \mathcal{M} \arrow[dd, "cN"] \\
\operatorname{Fil}^r\mathcal{X} \arrow[ur, "s"] \arrow[rr, "\phi_r"' near end] \arrow[dd, "u^eN"'] & & \mathcal{X} \arrow[ur, "s"] \arrow[dd, "cN"' near end] & \\
 & \operatorname{Fil}^r\mathcal{M} \arrow[rr, "\phi_r" near end] & & \mathcal{M} \\
\operatorname{Fil}^r\mathcal{X} \arrow[ur, "s"] \arrow[rr, "\phi_r"] & & \mathcal{X} \arrow[ur, "s"] &
\end{tikzcd}$$

Les faces du cube situées devant, derrière, au-dessus et au-dessous commutent. La face de gauche commute modulo $u^e\operatorname{Fil}^r\mathcal{M}$ et donc $\phi_r \circ (u^eN) \circ s = \phi_r \circ s \circ (u^eN)$. Une chasse au diagramme permet d'obtenir $(cN) \circ s \circ \phi_r = s \circ (cN) \circ \phi_r$, ce qui permet de conclure puisque $\phi_r\,(\operatorname{Fil}^r\mathcal{X})$ engendre tout $\mathcal{X}$. $\square$

6.2 Le calcul de $\mathbf{Hom}(\mathcal{N}, \hat{A}/A_{\mathrm{ss}})$

Rappelons que notre objectif est de prouver le lemme 6.0.5. On considère donc $\mathcal{X}$, objet de $\underline{\widetilde{\mathcal{M}}}^r$ et extension de deux objets simples $\mathcal{M}$ et $\mathcal{N}$. On suppose que $T_{\mathrm{st}}\,(\mathcal{X}) \simeq T_{\mathrm{st}}\,(\mathcal{M}) \times T_{\mathrm{st}}\,(\mathcal{N})$ et on veut montrer que $\mathcal{X}$ est semi-simple. Pour cela d'après le lemme 6.1.3, il suffit de prouver que tout élément de $T_{\mathrm{st}}\,(\mathcal{X})$ définit un morphisme qui tombe dans A_{ss}. Soit $\psi \in T_{\mathrm{st}}\,(\mathcal{X})$. On peut dessiner le diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r, "f"] \arrow[ddr, "0"'] & \mathcal{X} \arrow[r] \arrow[d, "\psi"] & \mathcal{N} \arrow[r] \arrow[ddl, dotted, "\tilde{\psi}"] & 0 \\
 & & \hat{A} \arrow[d, "\mathrm{pr}"] & & \\
 & & \hat{A}/A_{\mathrm{ss}} & &
\end{tikzcd}$$

La composée $\psi \circ f$ est un morphisme de $\mathcal{M}$ dans $\hat{A}$, qui tombe dans A_{ss} par simplicité de $\mathcal{M}$ et devient nulle lorsqu'elle est composée avec la projection canonique. Il existe donc une flèche $\tilde{\psi} : \mathcal{N} \to \hat{A}/A_{\mathrm{ss}}$ faisant commuter le diagramme. L'objectif de ce paragraphe est d'étudier plus en détail cette flèche.

Notons d'abord que le quotient $\hat{A}/A_{\mathrm{ss}}$ hérite d'une filtration, d'un Frobenius et d'un opérateur de monodromie : on définit $\operatorname{Fil}^i(\hat{A}/A_{\mathrm{ss}}) = \mathrm{pr}(\operatorname{Fil}^i\hat{A})$ et on vérifie que $N\,(A_{\mathrm{ss}}) \subset A_{\mathrm{ss}}$ et que $\phi_i(A_{\mathrm{ss}} \cap \operatorname{Fil}^i\hat{A}) \subset A_{\mathrm{ss}}$. Cela suffit pour transporter les structures.

Comme $\mathcal{M}$ est un objet simple, on sait le décrire précisément : par le théorème 4.3.2, il existe un entier h, des éléments $e_1, \ldots, e_h$ qui forment une base de $\mathcal{M}$ et des entiers $n_1, \ldots, n_h$ le tout tel que $\operatorname{Fil}^r\mathcal{M}$ soit engendré par les vecteurs $u^{n_1}e_1, \ldots, u^{n_h}e_h$, $\phi_r\,(u^{n_i}e_i) = e_{i+1}$ et $N\,(e_i) = 0$, les indices étant considérés dans $\mathbb{Z}/h\mathbb{Z}$. De même, on a une description de $\mathcal{N}$: il existe un entier h', des éléments $e'_1, \ldots, e'_{h'}$ et des entiers $n'_1, \ldots, n'_{h'}$ le tout vérifiant des conditions analogues.

Dans un premier temps, comme ψ commute à N, on a $N(\tilde{\psi}\,(e'_{i'})) = 0$ pour tout indice i'. On cherche donc les éléments de $\hat{A}$ dont l'image par N tombe dans A_{ss}. C'est l'objet du lemme suivant. On rappelle que, par le lemme 2.3.5 :

$$\hat{A} \simeq (\mathcal{O}_{\bar{K}}\,[X'] \,\langle Y \rangle) \,/\, (X'^p - 1, p)$$

l'isomorphisme consistant à faire correspondre X' à $1+X$ et $\frac{Y^i}{i!}$ à $\frac{1}{i!}\left(\frac{(1+X)^p-1}{p}\right)^i$.

Lemme 6.2.1. *Avec les notations précédentes, l'ensemble des $x \in \hat{A}$ tels que $N(x) \in A_{ss}$ est $A_{ss} + \mathcal{O}_{\bar{K}}/p + (A_{ss} \cap \mathcal{O}_{\bar{K}}/p)\, Y$.*

Démonstration. Soit $x \in \hat{A}$ tel que $N(x) \in A_{\mathrm{ss}}$. Il s'écrit :

$$x = \sum_{j \geqslant 0} P_j(X') \frac{Y^j}{j!}$$

les P_j étant des polynômes de degré inférieur à $p-1$ à coefficients dans $\mathcal{O}_{\bar{K}}/p$ nuls pour $j \gg 0$. On a :

$$N(x) = \sum_{j \geqslant 0} \left(X'P_j'(X') + P_{j+1}(X')\right) \frac{Y^j}{j!}.$$

On remarque que *via* les identifications faites, A_{ss} est entièrement inclus dans $\mathcal{O}_{\bar{K}}/p\,[X']/(X'^p - 1)$ et donc il suffit de vérifier les conditions :

1. $X'P_0'(X') + P_1(X') \in A_{\mathrm{ss}}$
2. $X'P_j'(X') + P_{j+1}(X') = 0$ pour tout $j \geqslant 1$

La deuxième condition entraîne $P_1(X') = b$ pour un certain $b \in \mathcal{O}_{\bar{K}}/p$ et $P_j(X') = 0$ pour tout $j \geqslant 2$.

Exploitons maintenant la première condition. Écrivons $P_0(X') = a_0 + a_1X' + \ldots + a_{p-1}X'^{p-1}$ où $a_i \in \mathcal{O}_{\bar{K}}/p$. On obtient :

$$b + a_1X' + 2a_2X'^2 + \ldots + (p-1)\,a_{p-1}X'^{p-1} \in A_{\mathrm{ss}}.$$

Par définition de A_{ss} et en remarquant que $u \in \hat{A}_{\mathrm{st}}$ correspond à $\pi_1 X'^{p-1} \in \hat{A}$, on voit que tous les termes de la somme précédente sont éléments de A_{ss}. En particulier on a $b \in A_{\mathrm{ss}}$. D'autre part, les entiers $2, \ldots, p-1$ sont inversibles dans $\mathcal{O}_{\bar{K}}/p$ et donc tous les $a_iX'^i$, pour $i \geqslant 1$, sont aussi éléments de A_{ss}. Cela prouve finalement que $P_0(X') \in A_{\mathrm{ss}} + \mathcal{O}_{\bar{K}}/p$ puis la conclusion annoncée.

Il reste à faire la réciproque, mais elle est immédiate au vu du calcul précédent. □

6.3 Fin de la preuve

Choisissons des relevés de $e'_{i'}$ dans $\mathcal{X}$, relevés que l'on appelle encore $e'_{i'}$. D'après le lemme 6.2.1, l'application ψ a la forme suivante :

$$\begin{aligned} \psi(e_i) &= x_i \\ \psi(e'_{i'}) &= a_{i'} + a'_{i'} + b_{i'}Y \end{aligned}$$

où $a_{i'} \in \mathcal{O}_{\bar{K}}/p$, $a'_{i'} \in A_{\mathrm{ss}}$, $b_{i'} \in A_{\mathrm{ss}} \cap \mathcal{O}_{\bar{K}}/p$, et où on connaît précisément la forme des x_i d'après le calcul fait dans le paragraphe 5.2 : si $x_i \neq 0$, si l'on note comme dans le paragraphe 6.1 :

$$\begin{aligned} t_i &= 0\,, n_i n_{i+1} \ldots n_{i+h-1}\, \overline{n_i n_{i+1} \ldots n_{i+h-1}} \ldots \\ t'_{i'} &= 0\,, n'_{i'} n'_{i'+1} \ldots n'_{i'+h'-1}\, \overline{n'_{i'} n'_{i'+1} \ldots n'_{i'+h'-1}} \ldots \end{aligned}$$

et si on pose $v_i = \frac{er}{p-1} - t_i$ et $v'_{i'} = \frac{e(r-1)}{p-1} - t'_{i'}$, il existe deux racines $\left(p^h - 1\right)$-ièmes de l'unité, ε et ε', telles que $\hat{x}_i = (-1)^{ri} \varepsilon^{p^i} \pi^{v_i}$ et où x_i est la réduction modulo p de $\hat{x}_i$ (resp $\hat{b}_{i'}$).

De plus, en remarquant qu'il existe $z \in \mathcal{M}$ tel que $u^{n'_{i'}} e'_{i'} + z \in \mathrm{Fil}^r \mathcal{X}$, on obtient des relations de la forme :

$$\phi_r \left(u^{n'_{i'}} \left(a_{i'} + b_{i'} Y \right) + c_{i'} \right) = a_{i'+1} + b_{i'+1} Y + r_{i'+1} \tag{1}$$

où $c_{i'}$ et $r_{i'}$ sont des éléments de A_{ss}. Écrivons :

$$c_{i'} = c_{i'}^{(0)} + c_{i'}^{(1)} u + \ldots + c_{i'}^{(p-1)} u^{p-1}$$

avec $c_{i'}^{(j)} \in A_{\mathrm{ss}} \cap \mathcal{O}_{\bar{K}}/p$. On peut supposer $c_{i'}^{n'_{i'}} = 0$ quitte à modifier $a_{i'}$. Décomposons $u^{n'_{i'}} \left(a_{i'} + b_{i'} Y \right) + c_{i'}$ de la façon suivante :

$$\begin{aligned} u^{n'_{i'}} \left(a_{i'} + b_{i'} Y \right) + c_{i'} &\equiv \pi_1^{n'_{i'}} a_{i'} + c_{i'}^{(0)} + c_{i'}^{(1)} \pi_1 + \ldots + c_{i'}^{(p-1)} \pi_1^{p-1} \\ &\quad - \left[n'_{i'} \pi_1^{n'_{i'}} a_{i'} + c_{i'}^{(1)} \pi_1 + \ldots + (p-1)\, c_{i'}^{(p-1)} \pi_1^{p-1} + \pi_1^{n'_{i'}} b_{i'} \right] X \\ &\equiv U - VX \pmod{\frac{X^i}{i!}, i \geqslant 2} \end{aligned}$$

Cette quantité doit appartenir à $\mathrm{Fil}^r \hat{A}$. On en déduit que π_1^{er} divise U et π_1^{er-e} divise V. De plus, en identifiant les termes constants en Y dans (1), on obtient les relations :

$$\phi_r (U) = a_{i'+1} + r_{i'+1}$$

qui impliquent $r_{i'} \in A_{\mathrm{ss}} \cap \mathcal{O}_{\bar{K}}/p$. Notons $\hat{a}_{i'} \in \mathcal{O}_{\bar{K}}$ un relevé de $a_{i'}$ et $\hat{c}_{i'}^{(j)} \in \mathcal{O}_{K^{\mathrm{mr}}}$ (K^{mr} désigne l'extension maximale modérément ramifiée de K) des relevés de $c_{i'}^{(j)}$ et posons :

$$\hat{c}_{i'} = \hat{c}_{i'}^{(0)} + \hat{c}_{i'}^{(1)} \pi_1 + \ldots + \hat{c}_{i'}^{(p-1)} \pi_1^{p-1} \in K^{\mathrm{mr}} [\pi_1] .$$

Notons finalement $\hat{r}_{i'} \in \mathcal{O}_{K^{\mathrm{mr}}}$ un relevé de $r_{i'}$. Intéressons-nous au système (dont les inconnus sont les $\hat{x}_{i'}$) donné par les équations :

$$\frac{\left(\pi_1^{n'_{i'}} \hat{x}_{i'} + \hat{c}_{i'} \right)^p}{\pi^{er}} = (-1)^r \left(\hat{x}_{i'+1} + \hat{r}_{i'+1} \right) .$$

On vient de voir que les $a_{i'}$ forment une solution modulo p, qui se remonte d'après le lemme 5.1.1 en une solution dans $\mathcal{O}_{\bar{K}}$ que l'on note $\hat{a}_{i'}$. Le corollaire 5.1.4 s'applique : un élément du groupe de Galois G_K qui fixe les $\hat{c}_{i'}$, les $\hat{r}_{i'}$ et π_1, fixe $\hat{a}_{i'}$ si et seulement s'il fixe $a_{i'}$.

D'autre part, on rappelle que par hypothèse la suite :

$$0 \longrightarrow T_{\mathrm{st}} (\mathcal{N}) \longrightarrow T_{\mathrm{st}} (\mathcal{X}) \longrightarrow T_{\mathrm{st}} (\mathcal{M}) \longrightarrow 0$$

est exacte et que l'on dispose d'une section $s : T_{\mathrm{st}} (\mathcal{M}) \to T_{\mathrm{st}} (\mathcal{X})$ qui commute à l'action de Galois.

Soit $\psi \in T_{\mathrm{st}} (\mathcal{M})$ décrit comme on vient de le voir. Le morphisme $s(\psi) \in T_{\mathrm{st}} (\mathcal{X})$ prolonge ψ, on l'appellera simplement ψ par la suite. Comme s est compatible à Galois, pour tout élément σ stabilisant les x_i, on a :

$$\sigma \left(a_{i'} + a'_{i'} + b_{i'} Y \right) = \sigma a_{i'} + \sigma a'_{i'} + \sigma b_{i'} t(\sigma) + \sigma b_{i'} Y = a_{i'} + a'_{i'} + b_{i'} Y$$

où on rappelle que $\sigma(Y) = Y + t(\sigma)$. On a vu que $t(\sigma) \in \mathcal{O}_{\bar{K}}/p$ (voir lemme 2.3.7) et donc de l'égalité précédente, on déduit en particulier :

$$\sigma a_{i'} + \sigma a'_{i'} + \sigma b_{i'} t(\sigma) = a_{i'} + a'_{i'}.$$

Si $t(\sigma) = 0$ et si σ fixe $a'_{i'}$, on obtient $\sigma a_{i'} = a_{i'}$. En particulier, tout $\sigma \in \mathrm{Gal}\left(\bar{K}/K^{\mathrm{mr}}[\pi_1]\right)$ vérifie $\sigma a_{i'} = a_{i'}$. Comme de plus tout tel σ fixe $\hat{c}_{i'}$ et $\hat{r}_{i'}$, il vient $\sigma \hat{a}_{i'} = \hat{a}_{i'}$ puis $\hat{a}_{i'} \in K^{\mathrm{mr}}[\pi_1]$.

Dès lors, la relation $\phi_r(U) = a_{i'+1} + r_{i'+1}$ entraîne que $a_{i'+1} \in \mathcal{O}_{K^{\mathrm{mr}}}/p$, et ce bien sûr pout tout i. Ainsi, il existe un entier d tel que l'on puisse écrire :

$$a_{i'} = \sum_{v \in I} \lambda_v \pi^v$$

où I désigne l'ensemble des rationnels dans $[0,1[$ et ayant pour dénominateur $\left(p^d - 1\right)$ et où les λ_v sont des éléments de $\mathcal{O}_K/p$. Soit I_{ss} l'ensemble des rationnels appartenant à I dont le développement « décimal » en base p ne fait intervenir que des chiffres compris entre 0 et er. Soit $I_{\overline{\mathrm{ss}}} = I \backslash I_{\mathrm{ss}}$. On pose :

$$a_{\mathrm{ss},i'} = \sum_{v \in I_{\mathrm{ss}}} \lambda_v \pi^v \quad \text{et} \quad a_{\overline{\mathrm{ss}},i'} = \sum_{v \in I_{\overline{\mathrm{ss}}}} \lambda_v \pi^v.$$

Alors $a_{i'} = a_{\mathrm{ss},i'} + a_{\overline{\mathrm{ss}},i'}$, $a_{\mathrm{ss},i'} \in A_{\mathrm{ss}}$ et on vérifie que :

$$\phi_r\left(\pi_1^{n'_{i'}} a_{\overline{\mathrm{ss}},i'}\right) = a_{\overline{\mathrm{ss}},i'+1}.$$

On sait résoudre cette équation et ses solutions sont dans A_{ss}. Cela entraîne $a_{\overline{\mathrm{ss}},i'} = 0$ pour tout indice i'. Ainsi $a_{i'} \in A_{\mathrm{ss}}$.

Reprenons à présent l'élément $U = \pi_1^{n'_{i'}} a_{i'} + c_{i'}^{(0)} + c_{i'}^{(1)} \pi_1 + \ldots + c_{i'}^{(p-1)} \pi_1^{p-1}$. Comme on a vu que $a_{i'} \in A_{\mathrm{ss}}$, sa valuation est un élément de $\mathbb{Z}_{(p)}$. Ainsi les valuations de termes non nuls intervenant dans U sont deux à deux distinctes. Puisque π^{er} divise U, on en déduit qu'il divise chacun de ces termes. En particulier, cela implique :

$$\phi_{r-1}(V) = \phi_{r-1}\left(\pi^{n'_{i'}} b_{i'}\right)$$

et en regardant la composante sur Y, la relation (1) implique :

$$\phi_{r-1}\left(\pi^{n'_{i'}} b_{i'}\right) = b_{i'+1}$$

On a déjà résolu plusieurs fois ce système. En particulier (c'est tout ce dont on aura besoin), $b_{i'} \in A_{\mathrm{ss}}$ et si $b_{i'} \neq 0$, on a :

$$v(b_{i'}) \leqslant \frac{e(r-1)}{p}$$

Supposons par l'absurde qu'il existe un indice i' tel que $b_{i'} \neq 0$. Soit $\sigma \in \mathrm{Gal}\left(\bar{K}/K^{\mathrm{mr}}\right)$ ne fixant pas π_1. On a $\sigma b_{i'} = b_{i'}$ et $t(\sigma) \neq 0$. On a démontré dans le lemme 2.3.8 que $t(\sigma)$ était congru à une racine $(p-1)$-ième de $(-p)$. En particulier, il est de valuation $\frac{e}{p-1}$. On en déduit :

$$v(b_{i'} t(\sigma)) \leqslant \frac{e(r-1)}{p-1} + \frac{e}{p-1} = \frac{er}{p-1} < e$$

et donc $b_{i'}t(\sigma)$ est non nul dans $\mathcal{O}_{\bar{K}}/p$. Mais on a l'égalité :

$$\sigma a_{i'} + \sigma a'_{i'} + \sigma b_{i'} t(\sigma) = a_{i'} + a'_{i'}$$

qui se simplifie ici en $b_{i'}t(\sigma) = 0$. C'est une contradiction. Ainsi $b_{i'} = 0$ pour tout i.

En conclusion, l'application ψ prend la forme suivante :

$$\begin{aligned} \psi(e_i) &= x_i \\ \psi(e'_{i'}) &= a_{i'} + a'_{i'} \end{aligned}$$

avec x_i, $a_{i'}$ et $a'_{i'}$ éléments de A_{ss}. On en déduit que ψ tombe dans A_{ss}.

Maintenant, tout élément de $\mathrm{Hom}(\mathcal{X}, \hat{A})$ s'écrit comme une somme d'un élément de $\mathrm{Hom}(\mathcal{M}, \hat{A})$ et de l'image par s d'un élément de $\mathrm{Hom}(\mathcal{N}, \hat{A})$. Ainsi on a bien prouvé que $\mathrm{Hom}(\mathcal{X}, \hat{A}) = \mathrm{Hom}(\mathcal{X}, A_{\mathrm{ss}})$ et par suite que le foncteur T_{st} est pleinement fidèle, du moins dans le cas où k est algébriquement clos.

6.4 Récapitulatif et conclusion

Récapitulons tout ce que l'on vient de voir. On a prouvé sans hypothèse sur le corps résiduel k que le foncteur T_{st} est toujours exact et fidèle. On a également prouvé, pour l'instant, que si ce corps résiduel est algébriquement clos, alors le foncteur T_{st} était également plein. En procédant comme dans le paragraphe 6.2 de [13], on peut déduire le résultat pour k quelconque du résultat pour k algébriquement clos :

Théorème 6.4.1. *Le foncteur T_{st} de la catégorie $\underline{\mathcal{M}}^r$ dans la catégorie des représentations $\mathbb{Z}_p$-linéaires de torsion du groupe de Galois G_K est exact et pleinement fidèle.*

Remarque. L'image essentielle du foncteur T_{st} est incluse dans la catégore des $\mathbb{Z}_p$-représentations de longueur finie de G_K comme le montre le théorème 6.4.4 que nous prouvons par la suite.

Nous pouvons finalement répondre complètement à la conjecture A.2 formulée dans [6]. Mais avant cela, nous allons énoncer et prouver une propriété formelle :

Propriété 6.4.2. *Soient A et B deux catégories abéliennes et artiniennes. Soit $F : A \to B$ un foncteur additif, exact et pleinement fidèle qui est tel que l'image de tout objet simple de A est encore simple dans B. Alors l'image essentielle de F est stable par sous-objets et par quotients.*

Démonstration. On se ramène directement au cas où A est une sous-catégorie pleine de B. L'hypothèse dit que les objets simples de A restent simples dans B. En particulier si M est un objet de A et si :

$$0 = M_0 \subset M_1 \subset \ldots \subset M_m = M$$

est une suite de Jordan-Hölder dans A, elle restera une suite de Jordan-Hölder dans B. Il s'agit de prouver que la catégorie A est stable par sous-objets et par quotients.

Introduisons pour cela A' la sous-catégorie pleine de B formée des objets dont tous les quotients de Jordan-Hölder sont dans A. C'est une sous-catégorie abélienne de B qui est stable par sous-objets et par quotients. Évidemment A est une sous-catégorie de A', on peut donc supposer que $A' = B$ ou si l'on préfère que les objets simples de A' et ceux de B sont les mêmes.

Soit M un objet de A et N un sous-objet de M. En considérant des suites de Jordan-Hölder de N et de M/N, on voit que l'on peut écrire une suite de Jordan-Hölder de la forme suivante :

$$0 = M_0 \subset M_1 \ldots \subset M_n = N \subset M_{n+1} \subset \ldots \subset M_m = M$$

Le quotient M_m/M_{m-1} est un objet simple et donc un objet de A. Par suite le noyau de la projection $M_m \to M_m/M_{m-1}$ qui s'identifie à M_{m-1} est également objet de A. Par récurrence, on montre que tous les M_i sont objets de A et donc qu'il en est de même de N. Ceci prouve la stabilité par sous-objets, la stabilité par quotients se traite de façon totalement identique. $\square$

Remarque. Cette propriété redémontre en particulier le fait que la sous-catégorie $\widetilde{\underline{\mathrm{MF}}}^r$ de $\widetilde{\underline{\mathcal{M}}}^r$ est stable par sous-objets et par quotients, puisque l'on a vu dans la proposition 3.3.4 que tous les objets simples de $\widetilde{\underline{\mathcal{M}}}^r$ étaient dans $\widetilde{\underline{\mathrm{MF}}}^r$.

On peut désormais énoncer le théorème qui résout la conjecture mentionnée précédemment :

Théorème 6.4.3. *L'image essentielle du foncteur T_{st} est stable par sous-objets et par quotients et indépendante du choix de l'uniformisante π.*

Démonstration. L'indépendance du choix de l'uniformisante est une conséquence directe de la propriété 3.1.10.

Supposons k algébriquement clos. On sait, par le lemme 5.3.2, que l'image par le foncteur T_{st} d'un objet simple de $\underline{\mathcal{M}}^r$ est une représentation irréductible. Le foncteur T_{st} vérifie les conditions de la propriété précédente, ce qui conclut.

Pour le cas général, notons K^{nr} le complété p-adique de l'extension maximale non ramifiée de K et $\widetilde{\underline{\mathcal{M}}}^r_{\mathrm{nr}}$ la catégorie $\widetilde{\underline{\mathcal{M}}}^r$ construite à partir de K^{nr}. Soit $\mathcal{M}$ un objet simple de $\underline{\mathcal{M}}^r$. Il est tué par p et donc peut être vu comme un objet de $\widetilde{\underline{\mathcal{M}}}^r$. Il suffit de prouver que $T_{\mathrm{st}}(\mathcal{M})$ est une représentation irréductible. Notons $\mathcal{M}_{\mathrm{nr}} = \bar{k} \otimes_k \mathcal{M}$. L'application :

$$\begin{array}{rcl} T_{\mathrm{st}}(\mathcal{M}) & \to & T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}}) \\ f & \mapsto & [\lambda \otimes x \mapsto [\lambda]\, f(x)] \end{array}$$

(où $[\lambda] \in W(\bar{k}) \subset \mathcal{O}_{\bar{K}}$ est le représentant de Teichmüller de $\lambda \in \bar{k}$) est un isomorphisme commutant à l'action de $G_{K^{\mathrm{nr}}} = \mathrm{Gal}\left(\bar{K}/K^{\mathrm{nr}}\right)$.

Supposons par l'absurde qu'il existe V un sous-$\mathbb{Z}_p$-module de $T_{\mathrm{st}}(\mathcal{M})$, strict, non nul et G_K-équivariant. C'est aussi un sous-$\mathbb{Z}_p$-module de $T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}})$ $G_{K^{\mathrm{nr}}}$-équivariant et donc d'après le cas précédent, on peut écrire $V = T_{\mathrm{st}}(\mathcal{C}_{\mathrm{nr}})$ (égalité de représentations de $G_{K^{\mathrm{nr}}}$) où $\mathcal{C}_{\mathrm{nr}}$ est un quotient de $\mathcal{M}_{\mathrm{nr}}$ dans la catégorie $\underline{\mathcal{M}}^r_{\mathrm{nr}}$. Soit $\mathcal{M}'_{\mathrm{nr}}$ le noyau de la projection $\mathcal{M}_{\mathrm{nr}} \to \mathcal{C}_{\mathrm{nr}}$, c'est un sous-objet strict et non nul de $\mathcal{M}_{\mathrm{nr}}$ dans la catégorie $\widetilde{\underline{\mathcal{M}}}^r_{\mathrm{nr}}$.

Soient $\sigma \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ et $\hat{\sigma} \in G_K$ un prolongement de σ. Soient $\psi \in V \subset T_{\mathrm{st}}(\mathcal{M})$ et ψ_{nr} son image dans $T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}})$. L'élément $\hat{\sigma}$ agit sur ψ_{nr} de la façon suivante :

$$\begin{array}{rrcl} \hat{\sigma}\psi_{\mathrm{nr}} : & \mathcal{M}_{\mathrm{nr}} & \to & \hat{A} \\ & s \otimes x & \mapsto & s\,\hat{\sigma}\psi(x) \end{array}$$

De plus, σ définit une application σ-semi-linéaire $\sigma : \mathcal{M}_{\mathrm{nr}} \to \mathcal{M}_{\mathrm{nr}}$. On vérifie qu'elle commute à ϕ_r et à N (ainsi $\sigma\mathcal{M}'_{\mathrm{nr}}$ est un sous-objet de $\mathcal{M}_{\mathrm{nr}}$) et qu'elle fait commuter le diagramme suivant :

$$\begin{tikzcd} \mathcal{M}_{\mathrm{nr}} \arrow[r, "\sigma"] \arrow[d, "\hat{\sigma}^{-1}\psi_{\mathrm{nr}}"'] & \mathcal{M}_{\mathrm{nr}} \arrow[d, "\psi_{\mathrm{nr}}"] \\ \hat{A} \arrow[r, "\hat{\sigma}"'] & \hat{A} \end{tikzcd}$$

Comme $\psi \in V$, on a $\psi_{|\mathcal{M}'_{\mathrm{nr}}} = 0$ et par le diagramme précédent, $\psi_{|\sigma\mathcal{M}'_{\mathrm{nr}}} = 0$.

On obtient un diagramme de la forme :

$$\begin{tikzcd}
0 \arrow[r] & V \arrow[r] \arrow[d, equal] & T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}}) \arrow[r] \arrow[d, equal] & T_{\mathrm{st}}(\mathcal{M}'_{\mathrm{nr}}) \arrow[r] & 0 \\
0 \arrow[r] & V \arrow[r] & T_{\mathrm{st}}(\mathcal{M}_{\mathrm{nr}}) \arrow[r] & T_{\mathrm{st}}(\sigma\mathcal{M}'_{\mathrm{nr}}) \arrow[r] & 0
\end{tikzcd}$$

qui fournit un isomorphisme $T_{\mathrm{st}}(\mathcal{M}'_{\mathrm{nr}}) \to T_{\mathrm{st}}(\sigma\mathcal{M}'_{\mathrm{nr}})$, se relevant par pleine fidélité en un isomorphisme $\sigma\mathcal{M}'_{\mathrm{nr}} \to \mathcal{M}'_{\mathrm{nr}}$ faisant commuter le diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \sigma\mathcal{M}'_{\mathrm{nr}} \arrow[r] \arrow[d] & \mathcal{M}_{\mathrm{nr}} \arrow[d, equal] \\
0 \arrow[r] & \mathcal{M}'_{\mathrm{nr}} \arrow[r] & \mathcal{M}_{\mathrm{nr}}
\end{tikzcd}$$

On en déduit $\sigma\mathcal{M}'_{\mathrm{nr}} = \mathcal{M}'_{\mathrm{nr}}$ pour tout $\sigma \in \mathrm{Gal}\left(K^{\mathrm{nr}}/K\right)$.

On pose $\mathcal{M}' = \mathcal{M}'_{\mathrm{nr}} \cap \mathcal{M} = {\mathcal{M}'_{\mathrm{nr}}}^{\mathrm{Gal}(K^{\mathrm{nr}}/K)}$. On va montrer que $\mathcal{M}'$ est un sous-objet strict et non nul de $\mathcal{M}$ dans la catégorie $\widetilde{\underline{\mathcal{M}}}^r$, ce qui est une contradiction. Soit $(e_1, \ldots, e_d)$ une $k\left[u\right]/u^{ep}$-base de $\mathcal{M}$. Soit $y \in \mathcal{M}'_{\mathrm{nr}}$, $y \neq 0$. On peut écrire :

$$y = P_1\left(u\right)e_1 + \ldots + P_d\left(u\right)e_d$$

où les P_i sont des polynômes à coefficients dans $\ell\left[u\right]/u^{ep}$ pour ℓ une extension finie de k. D'autre part, si $P \in \ell\left[u\right]/u^{ep}$, on peut définir $\mathrm{Tr}_{\ell/k}\left(P\right)$ en calculant la trace de chacun des coefficients. En outre, comme ℓ/k est séparable, on peut supposer $\mathrm{Tr}_{\ell/k}\left(P_1\right) \neq 0$, quitte à multiplier y par un élément non nul de ℓ. Posons :

$$x = \mathrm{Tr}_{\ell/k}\left(P_1\left(u\right)\right)e_1 + \ldots + \mathrm{Tr}_{\ell/k}\left(P_d\left(u\right)\right)e_d.$$

C'est un élément de $\mathcal{M}$ et, puisque $\sigma\mathcal{M}'_{\mathrm{nr}} = \mathcal{M}'_{\mathrm{nr}}$ pour tout $\sigma \in \mathrm{Gal}\left(K^{\mathrm{nr}}/K\right)$, c'est aussi un élément de $\mathcal{M}'_{\mathrm{nr}}$. Comme on a supposé $\mathrm{Tr}_{\ell/k}\left(P_1\left(u\right)\right) \neq 0$, on a $x \neq 0$, puis $\mathcal{M}' \neq 0$ comme on voulait.

On pose $\mathrm{Fil}^r\mathcal{M}' = \mathcal{M}' \cap \mathrm{Fil}^r\mathcal{M}'_{\mathrm{nr}}$. L'opérateur $\phi_r : \mathrm{Fil}^r\mathcal{M}'_{\mathrm{nr}} \to \mathcal{M}'_{\mathrm{nr}}$ (resp. $N : \mathcal{M}'_{\mathrm{nr}} \to \mathcal{M}'_{\mathrm{nr}}$) induit une application $\phi_r : \mathrm{Fil}^r\mathcal{M}' \to \mathcal{M}'$ (resp. $N : \mathcal{M}' \to \mathcal{M}'$). Ces applications vérifient les bonnes conditions pour définir un objet de $\widetilde{\underline{\mathcal{M}}}^r$. Le seul point délicat est le fait que $\phi_r\left(\mathrm{Fil}^r\mathcal{M}'\right)$ engendre $\mathcal{M}'$ en tant que $k\left[u\right]/u^{ep}$-module. Soit $x \in \mathcal{M}'$. On sait qu'il existe $\lambda_i \in \bar{k}\left[u\right]/u^{ep}$ et $y_i \in \mathrm{Fil}^r\mathcal{M}'_{\mathrm{nr}}$ tels que :

$$x = \lambda_1\phi_r(y_1) + \ldots + \lambda_n\phi_r(y_n).$$

De plus, quitte à rentrer les constantes à l'intérieur des ϕ_r, on peut supposer que $\lambda_i = u^{s_i}$ pour certains entiers s_i. Soit $(e_1, \ldots, e_d)$ une $k\left[u\right]/u^{ep}$-base de $\mathcal{M}$. Écrivons :

$$y_j = P_{1,j}\left(u\right)e_1 + \ldots + P_{d,j}\left(u\right)e_d$$

où $P_{i,j} \in \bar{k}\left[u\right]/u^{ep}$. Soit ℓ une extension finie de k contenant tous les coefficients des polynômes $P_{i,j}$ définis ci-dessus. Comme précédemment, on peut définir $\mathrm{Tr}_{\ell/k}\left(P\right)$ pour $P \in \ell\left[u\right]/u^{ep}$. Soit $\alpha \in \ell$ un élément tel que $\mathrm{Tr}_{\ell/k}\left(\alpha\right) = 1$. On pose :

$$x_j = \mathrm{Tr}_{\ell/k}\left(\alpha P_{1,j}\left(u\right)\right)e_1 + \ldots + \mathrm{Tr}_{\ell/k}\left(\alpha P_{d,j}\left(u\right)\right)e_d.$$

On a alors $x_i \in \operatorname{Fil}^r \mathcal{M}'$ et :

$$x = u^{s_1}\phi_r(x_1) + \ldots + u^{s_n}\phi_r(x_n)$$

ce qui prouve bien que $\phi_r(\operatorname{Fil}^r \mathcal{M}')$ engendre $\mathcal{M}'$ en tant que S-module. □

Remarque. Comme conséquence du théorème précédent et de la pleine fidélité de T_{st}, un objet $\mathcal{M} \in \underline{\mathcal{M}}^r$ est semi-simple si et seulement si $T_{\mathrm{st}}(\mathcal{M})$ est une représentation semi-simple.

Il résulte de la démonstration précédente et de l'exactitude du foncteur T_{st} le théorème suivant :

Théorème 6.4.4. *Si $\mathcal{M}$ est un objet de $\underline{\mathcal{M}}^r$, on a :*

$$long(\mathcal{M}) = long(T_{st}(\mathcal{M}))$$

Proposition 6.4.5. *Soit $\mathcal{M}$ un objet de $\underline{\mathcal{M}}^r$ isomorphe en tant que S-module à $S/p^{n_1}S \oplus \ldots \oplus S/p^{n_d}S$ pour certains entiers n_i. Alors en tant que $\mathbb{Z}_p$-module, $T_{st}(\mathcal{M})$ est isomorphe à $\mathbb{Z}_p/p^{n_1}\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p/p^{n_d}\mathbb{Z}_p$.*

Démonstration. Le lemme 2.3.1.2 de [6] dit que si $\mathcal{M}$ est un objet de $\widetilde{\underline{\mathcal{M}}}^r$, alors $T_{\mathrm{st}}(\mathcal{M})$ est un $\mathbb{F}_p$-espace vectoriel de dimension $\operatorname{rg}\mathcal{M}$. On en déduit par exactitude du foncteur T_{st} que :

$$\operatorname{long}_S(\mathcal{M}) = \operatorname{long}_{\mathbb{Z}_p}(T_{\mathrm{st}}(\mathcal{M}))$$

où les longueurs sont calculées respectivement dans la catégorie des S-modules et dans celle des $\mathbb{Z}_p$-modules.

Soit $\mathcal{M}$ un objet de $\underline{\mathcal{M}}^r$ isomorphe en tant que S-module à $S/p^{n_1}S \oplus \ldots \oplus S/p^{n_d}S$. La représentation galoisienne $T_{\mathrm{st}}(\mathcal{M})$ est un $\mathbb{Z}_p$-module de longueur finie et donc est isomorphe en tant que $\mathbb{Z}_p$-modules à $\mathbb{Z}_p/p^{n'_1}\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p/p^{n'_d}\mathbb{Z}_p$ pour certains entiers n'_i. Soit n un entier. Le noyau de la multiplication par p^n sur $\mathcal{M}$ s'envoie par le foncteur exact T_{st} sur le conoyau de la multiplication par p^n sur $T_{\mathrm{st}}(\mathcal{M})$. On en déduit en regardant les longueurs que :

$$\sum_{i=1}^{d} \min(n_i, n) = \sum_{i=1}^{d'} \min(n'_i, n).$$

Cela permet de conclure. □

7 Conséquences

7.1 Modules filtrés et modules fortement divisibles

Définitions

On reprend dans ce paragraphe les définitions et propriétés du paragraphe 4.1.1 de [3].

On rappelle que K_0 désigne le corps des fractions de W, anneau des vecteurs de Witt à coefficients dans k. On définit $S_{K_0} = S \otimes_W K_0$. C'est l'ensemble suivant :

$$S_{K_0} = \left\{ \sum_{i=0}^{\infty} w_i \frac{(E(u))^i}{i!},\ w_i \in K_0[u],\ \lim_{i\to\infty} w_i = 0 \right\}.$$

On munit S_{K_0} d'une filtration en posant $\mathrm{Fil}^n S_{K_0} = \mathrm{Fil}^n S \otimes_W K_0$, ou encore :

$$\mathrm{Fil}^n S_{K_0} = \left\{ \sum_{i=n}^{\infty} w_i \frac{(E(u))^i}{i!},\ w_i \in K_0[u],\ \lim_{i\to\infty} w_i = 0 \right\}.$$

On prolonge de manière évidente le Frobenius et l'opérateur de monodromie définis sur S à tout S_{K_0}.

On définit un *module fortement divisible* (resp. un *module filtré sur S_{K_0}*) comme la donnée suivante :

1. un S-module (resp. un S_{K_0}-module) $\mathcal{M}$ libre de rang fini ;
2. un sous-S-module (resp. un sous-S_{K_0}-module) de $\mathcal{M}$, noté $\mathrm{Fil}^r\mathcal{M}$ contenant $\mathrm{Fil}^r S \cdot \mathcal{M}$ (resp. contenant $\mathrm{Fil}^r S_{K_0} \cdot \mathcal{M}$) et tel que $\mathcal{M}/\mathrm{Fil}^r\mathcal{M}$ soit sans p-torsion (cette dernière condition est automatique pour les modules filtrés sur S_{K_0}) ;
3. d'une flèche ϕ-semi-linéaire $\phi_r : \mathrm{Fil}^r\mathcal{M} \to \mathcal{M}$ vérifiant la condition :

$$\phi_r(sx) = \frac{1}{c^r}\phi_r(s)\,\phi_r\left((E(u))^r x\right)$$

   et ce pour tout élément $s \in \mathrm{Fil}^r S$ (resp. tout élément $s \in \mathrm{Fil}^r S_{K_0}$) et tout élément $x \in \mathcal{M}$ telle que $\mathrm{im}\,\phi_r$ engendre $\mathcal{M}$ en tant que S-module (resp. en tant que S_{K_0}-module) ;
4. une application W-linéaire (resp. une application K_0-linéaire) $N : \mathcal{M} \to \mathcal{M}$ vérifiant les trois conditions :
   - pour tout $s \in S$ (resp. pour tout $s \in S_{K_0}$) et tout $x \in \mathcal{M}$, $N(sx) = N(s)x + sN(x)$
   - $E(u)\,N(\mathrm{Fil}^r\mathcal{M}) \subset \mathrm{Fil}^r\mathcal{M}$
   - le diagramme suivant commute :

$$\begin{tikzcd} \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] \arrow[d, "E(u)N"'] & \mathcal{M} \arrow[d, "cN"] \\ \mathrm{Fil}^r\mathcal{M} \arrow[r, "\phi_r"] & \mathcal{M} \end{tikzcd}$$

Suivant toujours [3], on définit de manière évidente la catégorie des modules filtrés sur S_{K_0} et celle des modules fortement divisibles. Elles sont équipées d'un foncteur vers les représentations galoisiennes. Précisément, si $\mathcal{M}$ est un module filtré sur S_{K_0}, on pose $T_{\mathrm{st}}(\mathcal{M}) = \mathrm{Hom}(\mathcal{M}, \hat{B}^+_{\mathrm{st}})$ où par définition $\hat{B}^+_{\mathrm{st}} = \hat{A}_{\mathrm{st}} \otimes_W K_0$ muni des structures induites et où Hom est compatible à toutes les structures ; on obtient une $\mathbb{Q}_p$-représentation de G_K. De même si $\mathcal{M}$ est un module fortement divisible, on définit $T_{\mathrm{st}}(\mathcal{M}) = \mathrm{Hom}(\mathcal{M}, \hat{A}_{\mathrm{st}})$, le Hom étant encore compatible à toutes les structures. On obtient une $\mathbb{Z}_p$-représentation libre de G_K. Les rangs des représentations obtenues coïncident avec les rangs des objets $\mathcal{M}$.

Si $\mathcal{M}$ est un module fortement divisible, on vérifie immédiatement que $\mathcal{M} \otimes_W K_0$ est un module filtré sur S_{K_0} et que pour tout entier $n \geqslant 1$, $\mathcal{M}/p^n\mathcal{M}$ est un objet de la catégorie $\underline{\mathcal{M}}^r$. De plus, on montre que $\mathcal{M}$ s'identifie à la limite projective de $\mathcal{M}/p^n\mathcal{M}$, puis que $T_{\mathrm{st}}(\mathcal{M})$ s'identifie à la limite projective de $T_{\mathrm{st}}(\mathcal{M}/p^n\mathcal{M})$. On déduit de la pleine fidélité prouvée précédemment le corollaire suivant :

Théorème 7.1.1. *Le foncteur T_{st} de la catégorie des modules fortement divisibles dans la catégories des $\mathbb{Z}_p$-représentations (libres) de G_K est pleinement fidèle.*

7.2 Modules fortement divisibles et foncteur T_{st}

Nous démontrons dans ce paragraphe le théorème 1.0.5. En fait, nous démontrons la formulation équivalente mais légèrement différente suivante :

Théorème 7.2.1. *On suppose $er < p-1$. Soit $\mathcal{M}$ un module fortement divisible sur S, et soit V la représentation galoisienne associée* via *le foncteur T_{st} à $\mathcal{M}_{K_0} = \mathcal{M} \otimes_W K_0$ qui est un module filtré sur S_{K_0}. Le foncteur T_{st} réalise une anti-équivalence de catégories entre la catégorie des sous-modules fortement divisibles de $\mathcal{M}_{K_0}$ et celle des sous-$\mathbb{Z}_p$-réseaux de V stables par G_K.*

Démonstration. Nous suivons pas à pas la preuve de la proposition 3 de [7], qui n'utilise essentiellement que la pleine fidélité du foncteur T_{st} et un équivalent du théorème 6.4.3.

Dans un premier temps, la pleine fidélité du foncteur T_{st} considérée dans l'énoncé du théorème se déduit directement du théorème 7.1.1.

Reste l'essentielle surjectivité. Soit T un $\mathbb{Z}_p$-réseau de V stable par G_K. Il existe un entier n_0 tel que :

$$p^{n_0} T \subset T_{\mathrm{st}}(\mathcal{M}) \subset (1/p^{n_0})\, T$$

On en déduit que pour $n \geqslant n_0$, $p^{n_0}T/p^nT$ est un sous-objet de $T_{\mathrm{st}}(\mathcal{M})/p^nT$, ce dernier étant un quotient de $T_{\mathrm{st}}(\mathcal{M}/p^{n+n_0}\mathcal{M})$. Le théorème 6.4.3 assure alors que $p^{n_0}T/p^nT$ s'écrit $T_{\mathrm{st}}(\mathcal{M}_n)$ pour $\mathcal{M}_n$ un certain objet de $\underline{\mathcal{M}}^r$.

La pleine fidélité de T_{st} assure l'existence d'une unique flèche $\mathcal{M}_n \to \mathcal{M}_{n+1}$ relevant la projection $p^{n_0}T/p^{n+1}T \to p^{n_0}T/p^nT$, et la limite inductive de ce système s'identifie à $\mathcal{M}_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ pour un certain module fortement divisible $\mathcal{M}_\infty$ qui répond à la question. $\square$

Remarque. Noter que si $\mathcal{M}$ est un S_{K_0}-module filtré « faiblement admissible », alors il contient toujours un module fortement divisible par [6].

7.3 Variante d'une conjecture de Serre

Dans ce paragraphe, on se propose d'expliquer comment le théorème donné dans l'introduction et que nous rappelons ci-dessous est conséquence de la théorie présentée précédemment. Noter qu'ici, on ne suppose *a priori* plus rien ni sur e, ni sur r.

Théorème 7.3.1. *Soit X un schéma propre et lisse sur K et à réduction semi-stable sur l'anneau des entiers $\mathcal{O}_K$. On fixe r un entier. Les exposants qui décrivent l'action de l'inertie modérée sur la semi-simplifiée modulo p de $H^r_{ét}(X_{\bar{K}}, \mathbb{Q}_p)^\star$ (où $X_{\bar{K}}$ est l'extension des scalaires de X à $\bar{K}$ et où « $\star$ » signifie que l'on prend le dual) sont tous compris entre* 0 *et er.*

Démonstration. Dans un premier temps, il est clair que l'on peut supposer $er < p-1$, le théorème étant trivialement vérifié dans le cas contraire. On peut donc utiliser les résultats précédents.

D'après les résultats de [21] et du paragraphe 2.2 de [9], la $\mathbb{Q}_p$-représentation $V = H^r_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p)^\star$ (le dual étant cette fois-ci le $\mathbb{Q}_p$-dual) provient *via* le foncteur T_{st} d'un module filtré $\mathcal{M}_{K_0}$ sur S_{K_0}, et d'après les résultats de [6], ce module admet un sous-module fortement divisible $\mathcal{M}$.

D'autre part, la $\mathbb{Z}_p$-représentation T est un réseau de V stable par Galois, et donc d'après le théorème 7.2.1, il existe un module fortement divisible inclus dans $\mathcal{M}_{K_0}$ dont l'image par T_{st} est isomorphe à T. Appelons $\mathcal{M}$ un tel module.

La représentation quotient T/p correspond *via* le foncteur T_{st} à $\mathcal{M}/p$ qui est un objet de $\widetilde{\underline{\mathcal{M}}}^r$. La semi-simplifiée de T/p est la somme directe de ses quotients de Jordan-Hölder, et chacun de ces quotients correspond à un objet simple de $\widetilde{\underline{\mathcal{M}}}^r$. Le théorème 5.2.2 permet de conclure. $\square$

Remarque. Si l'on préfère, on peut ne pas utiliser le théorème 7.2.1, mais dire à la place que si T et T' sont deux $\mathbb{Z}_p$-réseaux de V stables par Galois, alors les semi-simplifiées des réductions modulo p de ces deux représentations sont isomorphes. On aurait donc pu garder le premier module fortement divisible $\mathcal{M}$.

Bibliographie

[1] C. Breuil, B. Conrad, F. Diamond et R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$ *: wild* 3*-adic exercices*, J. of Amer. Math. Soc. **14** (2001), 843–939

[2] L. Berger, *An introduction to the theory of p-adic representations*, à paraitre dans Geometric Aspects of Dwork's Theory

[3] C. Breuil, *Construction de représentations p-adiques semi-stables*, Ann. Scient. ENS. **31** (1997), 281–327

[4] ———, *Représentations p-adiques semi-stables et transversalité de Griffiths*, Math. Annalen **307** (1997), 191–224

[5] ———, *Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable*, Duke mathematical journal **95** (1998), 523–620

[6] ———, *Représentation semi-stables et modules fortement divisibles*, Invent. math. **136** (1999), 89–122

[7] ———, *Une remarque sur les représentations locales p-adiques et les congruences entre formes modulaires de Hilbert*, Bull. soc. math. France **127** (1999), 459–472

[8] ———, *Groupes p-divisibles, groupes finis et modules filtrés*, Annals of Mathematics **152** (2000), 489–549

[9] ———, *Integral p-adic Hodge theory*, Advanced studies in pure mathematics **36** (2002), 51–80

[10] B. Conrad, *Finite group schemes over bases with low ramification*, Compositio Math. **119** (1999), 239–320

[11] G. Faltings, *Crystalline cohomology and p-adic Galois representations*, Journal of algebraic geometry **1** (1992), 61–82

[12] ———, *Integral crystalline cohomology over very ramified valuations rings*, J. Amer. Math. Soc **12** (1999), 117–144

[13] J.M. Fontaine et G. Laffaille, *Construction de représentations p-adiques*, Ann. Scient. ENS. **15** (1982), 547–608

[14] J.M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad. Sc. Paris **280** (1975), 1423–1425

[15] ———, *Cohomologie de de Rham, cohomologie cristalline et représentations p-adique*, Lecture notes in math. **1016** (1983), 86–108, 113–184

[16] ———, *Le corps des périodes p-adiques*, Astérisque **223**, Soc. math. France (1994), 59–111

[17] ———, *Représentations p-adiques semi-stables*, Astérisque **223**, Soc. math. France (1994), 113–184

[18] K. Kato, *On p-adic vanishing cycles*, Advanced Study in Pure Math. **10** (1987), 207–251

[19] M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. math. France **102** (1974), 241–280

[20] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones math. **15** (1972), 259–331

[21] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Inventiones math. **137** (1999), 233–411

[22] N. Wach, *Représentations cristallines de torsion*, Comp. Math. **108** (1997), 185–240