Représentations galoisiennes p-adiques et (φ, τ)-modules

Xavier Caruso

Avril 2011

Résumé

Étant donné un nombre premier impair p et un corps p-adique K, on développe dans cet article, un analogue de la théorie des (φ, Γ)-modules de Fontaine en remplaçant la p-extension cyclotomique par l'extension K_∞ de K obtenue en ajoutant un système compatible de racines p^n-ièmes d'une uniformisante π fixée. Ceci nous conduit à une nouvelle classification des représentations p-adiques de $G_K = \text{Gal}(\bar{K}/K)$ *via* des (φ, τ)-modules. Nous caractérisons ensuite les (φ, τ)-modules correspondant à des représentations semi-stables. Comme corollaire, nous répondons à une question de Tong Liu en démontrant que toute représentation de $E(u)$-hauteur finie de G_K est potentiellement semi-stable. Nous obtenons en outre une nouvelle classification des réseaux dans les représentations semi-stables en termes de la récente théorie de Kisin.

Abstract

Let p be an odd prime number and K be a p-adic field. In this paper, we develop an analogue of Fontaine's theory of (φ, Γ)-modules replacing the p-cyclotomic extension by the extension K_∞ obtained by adding to K a compatible system of p^n-th roots of a fixed uniformizer π of K. As a result, we obtain a new classification of p-adic representations of $G_K = \text{Gal}(\bar{K}/K)$ by some (φ, τ)-modules. We then caracterize the (φ, τ)-modules, that correspond to semi-stable representations. As a corollary, we answer a question of Tong Liu : we prove that every representation of G_K of $E(u)$-finite height is potentially semi-stable. We finally describe a new classification of lattices is semi-stable representations in terms of recent Kisin theory.

Table des matières

Soit p un nombre premier impair. Soit K un corps de caractéristique nulle, complet pour une valuation discrète, dont le corps résiduel k est parfait de caractéristique p. On fixe $\bar{K}$ une clôture algébrique de K

et on s'intéresse aux représentations p-adiques du groupe de Galois $G_K = \text{Gal}(\bar{K}/K)$. Plusieurs théories ont déjà été développées pour étudier ces représentations, et notamment celle des (φ, Γ)-modules dûe à Fontaine [11]. Dans cette théorie, la p-extension cyclotomique de K, notée $K(\zeta_{p^\infty})$ et obtenue en ajoutant à K les racines p^n-ièmes de l'unité, joue un rôle essentiel. En effet, une première étape cruciale consiste à démontrer que les $\mathbb{Q}_p$-représentations (resp. les $\mathbb{Z}_p$-représentations libres ou de torsion) de type fini du groupe de Galois $H_K = \text{Gal}(\bar{K}/K(\zeta_{p^\infty}))$ sont classifiées par certains φ-modules [1] sur le corps $\mathcal{E}$ (resp. sur l'anneau $\mathcal{E}^{\text{int}}$) défini comme suit

$$\mathcal{E} = \Big\{ \sum_{i\in\mathbb{Z}} a_i u^i \quad \Big| \quad a_i \in W[1/p],\ (a_i) \text{ bornée},\ \lim_{i\to-\infty} a_i = 0 \Big\}$$

$$(\text{resp. } \mathcal{E}^{\text{int}} = \Big\{ \sum_{i\in\mathbb{Z}} a_i u^i \quad \Big| \quad a_i \in W,\ \lim_{i\to-\infty} a_i = 0 \Big\})$$

où $W = W(k)$ désigne l'anneau des vecteurs de Witt à coefficients dans k. À partir de là, on retrouve l'action complète de G_K en ajoutant à ce φ-module une action du quotient $\Gamma = G_K/H_K = \text{Gal}(K(\zeta_{p^\infty})/K)$, obtenant au final un objet appelé (φ, Γ)-module.

Certains travaux récents de Breuil et Kisin (voir [4] et [13]) ont montré que, plus encore que la p-extension cyclotomique considérée précédemment, l'extension K_∞ de K, obtenue en ajoutant un système compatible de racines p^n-ièmes d'une uniformisante π fixée, joue un rôle particulier pour l'étude des représentations semi-stables de G_K. Le but de cet article est de développer un analogue de la théorie des (φ, Γ)-modules à partir de l'extension K_∞. La première étape, qui consiste à classifier les représentations de $G_\infty = \text{Gal}(\bar{K}/K_\infty)$, fonctionne comme dans le cas classique : à une telle représentation est associée un φ-module sur $\mathcal{E}$ ou $\mathcal{E}^{\text{int}}$ (selon que les coefficients soient pris dans $\mathbb{Q}_p$ ou $\mathbb{Z}_p$), et celui-ci suffit à la décrire complètement. Par contre, une fois arrivé à ce niveau, il n'est plus possible de copier à la lettre la méthode de Fontaine, tout simplement parce que l'extension K_∞/K n'est pas galoisienne. Cela n'a donc aucun sens d'ajouter au φ-module précédent l'action résiduelle de $\text{Gal}(K_\infty/K)$ puisque ce dernier groupe n'est pas défini !

Suivant certains travaux de Liu (voir [18] et [19]), on peut toutefois procéder comme suit. On considère un élément $\tau \in G_K$ agissant trivialement sur $K(\zeta_{p^\infty})$ — ou même seulement sur $K(\zeta_p)$ — tel que τ et G_∞ engendrent ensemble G_K. Dans ces conditions, connaître le φ-module M et l'action de τ suffit à reconstruire l'action complète de G_K sur T. Cette action supplémetaire de τ a un pendant au niveau des φ-modules. Elle ne correspond certes pas à un simple endomorphisme de M (comme cela aurait été le cas si l'extension K_∞/K avait été galoisienne), mais à un endomorphisme semi-linéaire de $\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M$ où $\mathcal{E}_\tau^{\text{int}}$ est une certaine $\mathcal{E}^{\text{int}}$-algèbre munie d'une action de G_K. Ceci nous conduit à définir un (φ, τ)-module sur $(\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}})$ (resp. sur $(\mathcal{E}, \mathcal{E}_\tau)$ où $\mathcal{E}_\tau = \mathcal{E}_\tau^{\text{int}}[1/p]$) comme la donnée d'un φ-module de type fini M sur $\mathcal{E}^{\text{int}}$ (resp. $\mathcal{E}$) muni d'une application supplémentaire $\tau : \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M \to \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M$ vérifiant un certain nombre de conditions (voir définition 1.18 pour plus de précisions). Nous démontrons alors le théorème suivant (se reporter au §§1.2.2 et 1.3.2 pour la définition des foncteurs).

Théorème 1. *Il existe des équivalences de catégories :*

$$\left\{ \begin{array}{c} \mathbb{Q}_p\textit{-représentations de} \\ \textit{dimension finie de } G_K \end{array} \right\} \quad \xrightarrow{\sim} \quad \left\{ \ (\varphi,\tau)\textit{-modules sur } (\mathcal{E}, \mathcal{E}_\tau) \ \right\}$$

$$\left\{ \begin{array}{c} \mathbb{Z}_p\textit{-représentations} \\ \textit{libres de type fini de } G_K \end{array} \right\} \quad \xrightarrow{\sim} \quad \left\{ \begin{array}{c} (\varphi,\tau)\textit{-modules} \\ \textit{libres sur } (\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}}) \end{array} \right\}$$

et, pour tout entier n :

$$\left\{ \begin{array}{c} \mathbb{Z}_p\textit{-représentations de type} \\ \textit{fini de } G_K \textit{ annulées par } p^n \end{array} \right\} \quad \xrightarrow{\sim} \quad \left\{ \begin{array}{c} (\varphi,\tau)\textit{-modules sur} \\ (\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}}) \textit{ annulés par } p^n \end{array} \right\}.$$

Malgré les apparences, le résultat précédent n'est pas entièrement satisfaisant. La raison principale en est la complexité de l'anneau $\mathcal{E}_\tau^{\text{int}}$, qui s'exprime comme un certain complété du perfectisé de la réunion d'une suite croissante d'extensions finis étales $\mathcal{E}_m^{\text{int}}$ ($m \geqslant 1$) de $\mathcal{E}^{\text{int}}$. De façon peut-être un peu plus parlante, cela

1. Les définitions précises seront données par la suite. On pourra se contenter pour l'instant de savoir que les φ-modules sont des modules munis d'un opérateur semi-linéaire, généralement noté φ.

signifie qu'écrire de façon explicite un élément de $\mathcal{E}_\tau^{\text{int}}$ demande d'écrire une série en une infinité de variables faisant intervenir des puissances fractionnaires, le tout étant soumis à des conditions de convergence subtiles. Dans le §2, nous introduisons la notion de (φ, τ)-réseau qui fournit quelques éléments pour contourner ce désagrément. Si M est un (φ, τ)-module, un (φ, τ)-réseau de M est un sous-$W[[u]]$-module de type fini de M, qui engendre M comme $\mathcal{E}^{\text{int}}$-module, qui est stable par φ et dont l'extension des scalaires à $\mathfrak{S}_\tau$ (un certain sous-anneau de $\mathcal{E}_\tau^{\text{int}}$ qui sera défini dans le corps du texte) est stable par τ. Une notion importante liée aux réseaux est celle de hauteur : étant donné un élément $U \in \mathfrak{S}_\tau$, on dit qu'un réseau $\mathfrak{M}$ est de hauteur divisant U si le conoyau de

$$\text{id} \otimes \varphi : \mathfrak{S}_\tau \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$$

est annulé par U. Nous démontrons un thèorème (théorème 2.25) qui énonce un certain nombre de congruences permettant de contrôler l'action de τ sur un (φ, τ)-réseau en fonction de sa hauteur. Le résultat que nous obtenons est en fait particulièrement intéressant dans le cas des représentations de torsion puisqu'il implique que, quitte à procéder à quelques transformations simple du (φ, τ)-module, on peut travailler avec l'un des anneaux $\mathcal{E}_m^{\text{int}}$ (pour un entier m explicite) en lieu et place de $\mathcal{E}_\tau^{\text{int}}$. En d'autres termes, au lieu de séries en une infinité de variables à puissances fractionnaires, on est ramené à des polynômes (définis dans un anneau quotient) en une unique variable u_m (dont, malheureusement, le lien avec la variable u n'est pas encore bien compris). Le cas des représentations libres sur $\mathbb{Z}_p$ est, quant à lui, un peu plus subtil et nous n'en dirons pas davantage à son sujet dans cette introduction. Pour plus de précisions, nous renvoyons bien entendu à l'énoncé exact du théorème 2.25 ainsi qu'à la discussion qui le suit.

Signalons, par contre, dès maintenant que la démonstration du théorème 2.25 repose de façon essentielle sur l'existence de bornes pour la ramification des représentations associées à un φ-module du hauteur divisant un élément U fixé. Chemin faisant, nous sommes donc amenés à démontrer le théorème suivant, qui nous paraît intéressant en lui-même.

Théorème 2. *On note $G_\infty^{(\mu)}$ et $G_K^{(\mu)}$ les filtrations de ramification en numérotation supérieure [2] des groupes de Galois respectifs G_∞ et G_K. On fixe un nombre entier $n \geqslant 1$ et un élément $U \in \mathfrak{S}$ qui n'est pas multiple de p. On pose $h = v_R(U \bmod p)$.*

1. *Soit T une $\mathbb{Z}_p$-représentation de G_∞ qui est de type fini comme $\mathbb{Z}_p$-module et annulée par p^n. On suppose que le φ-module étale sur $\mathcal{E}^{\text{int}}$ associé à T admet un φ-réseau de hauteur divisant U. Alors pour tout $\mu > \max(1, \frac{hp^n}{p-1})$, le sous-groupe $G_\infty^{(\mu)}$ agit trivialement sur T.*

2. *Il existe une constante $c(K)$ ne dépendant que du corps K telle que l'assertion suivante soit vraie : pour toute $\mathbb{Z}_p$-représentation T de G_K de type fini comme $\mathbb{Z}_p$-module, annulée par p^n, dont la restriction à G_∞ correspond à un φ-module étale sur $\mathcal{E}^{\text{int}}$ de hauteur divisant U, et pour tout $\mu > c(K) + e \cdot \max(\frac{1}{p-1}, n + \log_p(\frac{h}{e}))$, le groupe $G_K^{(\mu)}$ agit trivialement sur T.*

La constante $c(K)$ dépend de façon assez explicite de la ramification absolue de K ; par exemple, lorsque e est premier avec p (*i.e.* lorsque K est absolument modérément ramifié), elle peut être choisie égale à $1 + e + \frac{e}{p-1}$. Signalons encore que la deuxième partie du théorème 2 s'applique en particulier, avec $U = E(u)^r$, lorsque T est un réseau dans une représentation semi-stable à poids de Hodge-Tate dans $\{0, \ldots, r\}$. Nous démontrerons toutefois au §3.4 de cet article un résultat plus précis pour ce type particulier de représentations, qui n'est autre que la conjecture 1.2.(1) de [7].

Nous nous intéressons enfin plus particulièrement aux (φ, τ)-modules qui sont de hauteur divisant $E(u)^r$ pour un certain entier r (on dit aussi : *de $E(u)$-hauteur $\leqslant r$*). L'intérêt de cette notion a été récemment mis en lumière dans un premier temps par Breuil dans [4] puis Kisin dans [13]. Ce dernier a notamment démontré que toute représentation semi-stable est de $E(u)$-hauteur finie. Dans la dernière section de cet article, nous raffinons le résultat de Kisin en caractérisant les (φ, τ)-modules donnant lieu à des représentations semi-stables. En guise de corollaire, nous obtenons le théorème suivant, qui donne une réponse positive à la question 4.3.1.(2) de [19].

Théorème 3. *Soit s le plus grand entier tel que K contienne une racine primitive p^s-ième de l'unité. Alors toute représentation de $E(u)$-hauteur finie de G_K devient semi-stable en restriction au sous-groupe (distingué)* $\text{Gal}(\bar{K}/K(\sqrt[p^s]{\pi}))$.

2. Pour le groupe G_K, il s'agit de la ramification usuelle telle que définie, par exemple, dans [11]. Sur le groupe G_∞, la ramification est définie de même *via* l'isomorphisme de corps des normes $G_\infty \simeq \text{Gal}(F_0^{\text{sep}}/F_0)$ où $F_0 = \mathcal{E}^{\text{int}}/p\mathcal{E}^{\text{int}} \simeq k((u))$. Pour plus de précisions à ce sujet, on renvoie au §2.2.1.

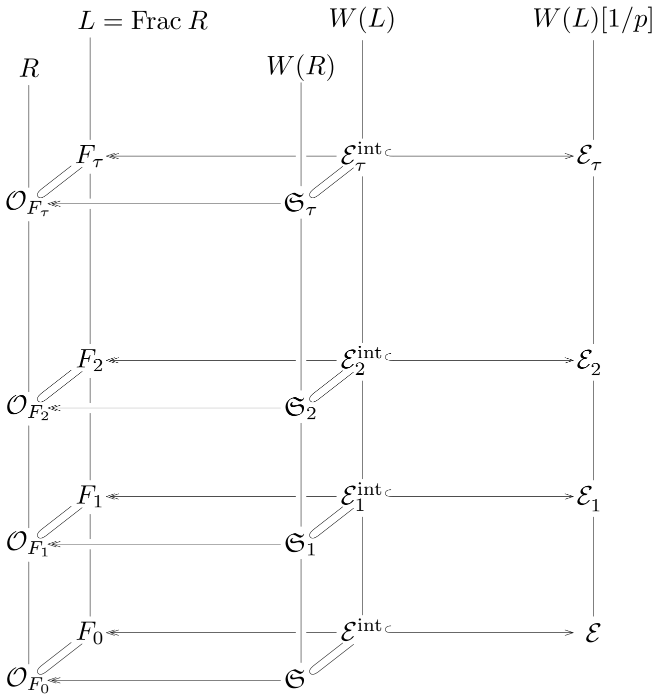


FIGURE 1 – Principaux anneaux intervenant dans la théorie des (φ, τ)-modules

La partie gauche (resp. centrale, resp. droite) du diagramme concerne la théorie sur $\mathbb{F}_p$ (resp. $\mathbb{Z}_p$, resp. $\mathbb{Q}_p$). Les anneaux qui apparaissent au second plan concernent la théorie générale des (φ, τ)-modules ; ils sont présentés et étudiés dans le §1. Au premier plan, au contraire, nous trouvons les anneaux nécessaires à l'étude des (φ, τ)-réseaux ; ceux-ci sont introduits et utilisés dans le §2.

Comme second corollaire, nous obtenons dans le §3.3 une nouvelle classification des réseaux dans les représentations semi-stables en termes de (φ, N_∇)-modules à la Kisin. Bien que proche dans l'esprit de celle proposée par Liu dans [19], elle nous paraît nettement plus simple dans sa formulation. Dans le cas général, elle fait toutefois encore intervenir des conditions délicates à manipuler, dont le nombre augmente avec les poids de Hodge-Tate de la représentation. Pour des poids de Hodge-Tate compris entre 0 et $p-1$, ces conditions disparaissent et la classification que nous obtenons s'apparente alors plutôt à celle de Breuil-Liu (voir [17]).

Ce travail puise son origine et son inspiration dans de nombreuses discussions avec Tong Liu ; à travers ces quelques lignes, l'auteur souhaite lui témoigner tous ses remerciements. Il le remercie en particulier pour lui avoir suggéré l'argument du §3.2.3 qui permet de se passer d'une hypothèse additionnelle technique dans le théorème 3. L'auteur est également reconnaissant à l'Agence Nationale de la Recherche (ANR) pour son soutien financier par l'intermédiaire du projet CETHop (Calculs Effectifs en Théorie de Hodge p-adique) référencé ANR-09-JCJC-0048-01.

1 La théorie générale des (φ, τ)-modules

L'objectif principal de cette première partie est de définir les foncteurs qui réalisent les équivalences de catégories énoncées dans le théorème 1 de l'introduction (et donc de définir, aussi, en particulier, l'anneau $\mathcal{E}_\tau^{\mathrm{int}}$), puis de démontrer ce théorème. Tout au long de cette section et de la suivante, nous allons petit à petit définir un certain nombre d'anneaux. La figure 1 présente un diagramme qui fait apparaître les plus importants d'entre eux, ainsi que les morphismes essentiels les reliant. Nous espérons que celui-ci pourra faciliter la lecture de cet article.

Comme dans l'introduction, on fixe un nombre premier impair p et un corps K muni d'une valuation discrète pour laquelle il est complet. On suppose que K est de caractéristique nulle et que son corps résiduel k est parfait de caractéristique p. On rappelle également que W désigne l'anneau des vecteurs de Witt à coefficients dans k ; son corps des fractions $W[1/p]$ s'identifie canoniquement au plus gros sous-corps de K absolument non ramifiée. L'extension $K/W[1/p]$ est totalement ramifiée et on note e son degré. On considère (ζ_{p^s}) un système compatibles de racines primitives p^s-ièmes de l'unité et on note $K(\zeta_{p^\infty}) = \bigcup_s K(\zeta_{p^s})$. L'extension $K(\zeta_{p^\infty})$ est galoisienne et son groupe de Galois Γ s'identifie *via* le caractère cyclotomique χ à un sous-groupe ouvert de $\mathbb{Z}_p^\times$.

1.1 L'extension K_∞ : définition et propriétés galoisiennes

Nous commençons par quelques préliminaires, en grande partie déja connus, concernant l'extension K_∞ de Breuil-Kisin. Soit π une uniformisante de $\mathcal{O}_K$. On choisit une fois pour toutes une système compatible (π_s) de racines p^s-ièmes de π. On pose $K_s = K(\pi_s)$ pour tout entier s et $K_\infty = \bigcup_s K_s$. Les extensions K_s/K ne sont pas galoisiennes, sauf éventuellement pour les premiers entiers s. De façon plus précise, la clôture galoisienne de K_s/K est l'extension $K_s(\zeta_{p^s})$. Ainsi K_s/K est galoisienne si, et seulement si $\zeta_{p^s} \in K_s$. L'extension K_∞/K, quant à elle, n'est *jamais* galoisienne et sa clôture galoisienne est l'extension composée $K_\infty(\zeta_{p^\infty}) = K_\infty \cdot K(\zeta_{p^\infty})$. On pose $G_\infty = \mathrm{Gal}(\bar{K}/K_\infty) \subset G_K$ et $H_\infty = \mathrm{Gal}(\bar{K}/K_\infty(\zeta_{p^\infty})) \subset G_\infty$.

1.1.1 Le cocycle c

Bien que G_∞ ne soit pas distingué dans G_K, on peut définir une application continue (qui bien sûr, n'est pas un morphisme de groupes) $c : G_K \to \mathbb{Z}_p$ dont le « noyau » (*i.e.* l'image réciproque de $0 \in \mathbb{Z}_p$) s'identifie à G_∞. Pour cela remarquons qu'étant donné un élément $g \in G_K$ et un entier s, il existe un unique élément $c_s(g) \in \mathbb{Z}/p^s\mathbb{Z}$ tel que $g(\pi_s) = \zeta_{p^s}^{c_s(g)} \pi_s$. La famille des $(c_s(g))_{s \geqslant 1}$ vérifie la congruence $c_{s+1}(g) \equiv c_s(g) \pmod{p^s}$, et définit donc un élément de $\mathbb{Z}_p$, que l'on appelle $c(g)$. On vérifie sans peine que c est continue et que le fait que $c(g)$ s'annule signifie exactement que g agit trivialement sur chacun des π_s, c'est-à-dire sur K_∞. Ainsi, comme nous le disions précédemment, on a $c^{-1}(0) = G_\infty$. L'application c n'est certes pas un morphisme de groupes mais vérifie malgré tout une relation de 1-cocycle à savoir :

$$\forall g, h \in G_\infty, \quad c(gh) = c(g) + \chi(g) c(h). \tag{1.1}$$

On en déduit que, si $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ désigne le produit semi-direct de $\mathbb{Z}_p$ par $\mathbb{Z}_p^\times$ où $\mathbb{Z}_p^\times$ agit sur $\mathbb{Z}_p$ par multiplication, l'application $\chi_\infty : G_K \to \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, $g \mapsto (c(g), \chi(g))$ est un morphisme de groupes dont le noyau est exactement H_∞. En particulier, le 1-cocycle $c : G_K \to \mathbb{Z}_p$ se factorise par G_K/H_∞, et ce dernier groupe se plonge dans $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ *via* χ_∞. Voici un diagramme qui résume les liens entre les différents groupes que l'on vient d'introduire :

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K_\infty) \arrow[r] \arrow[d] & G_K/H_\infty \arrow[r, "\chi"] \arrow[d, hook, "\chi_\infty"] & \mathbb{Z}_p^\times \arrow[d, equal] & \\
0 \arrow[r] & \mathbb{Z}_p \arrow[r] & \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times \arrow[r] & \mathbb{Z}_p^\times \arrow[r] & 0
\end{tikzcd}$$

Soulignons que les groupes qui apparaissent sur le diagramme sont tous profinis, tandis que les morphismes sont tous continus pour la topologie profinie. Par ailleurs, il résulte du diagramme que le morphisme $\mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K_\infty) \to \mathbb{Z}_p$ est injectif. Le lemme 5.1.2 de [17] (qui stipule que les extensions K_∞ et $K(\zeta_{p^\infty})$ sont linéairement disjointes sur K) montre même que c'est un isomorphisme. On déduit également du même lemme que $\chi(G_\infty) = \chi(G_K)$. On remarque encore que si $g \in G_K$ est tel que $\chi(g) \equiv 1 \pmod{p}$, alors $\chi_\infty(g)$ appartient à l'unique pro-p-Sylow de $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$; il en résulte que $\chi(g)^{p^s}$ converge vers l'élément neutre de ce groupe lorsque s tend vers l'infini, et donc que la suite des $g^{p^s} \bmod H_\infty$ converge elle aussi (vers l'élément neutre de G_K/H_∞). En particulier, si a est un entier p-adique, l'élément g^a est bien défini dans G_K/H_∞, et il en est donc de même de $c(g^a)$. Une récurrence à partir de (1.1) suivie d'un passage à la limite conduit enfin à la formule

$$\begin{aligned} c(g^a) = c(g) \cdot [a]_{\chi(g)} \quad \text{où} \quad [a]_{\chi(g)} &= a & &\text{si } \chi(g) = 1. \\ &= \frac{\chi(g)^a - 1}{\chi(g) - 1} & &\text{si } \chi(g) \neq 1. \end{aligned} \tag{1.2}$$

Dans la suite, le nombre $[a]_{\chi(g)}$ sera appelé le $\chi(g)$-*analogue* de a.

1.1.2 L'élément τ

Soit $\tau : K_\infty \to \bar{K}$ le K-plongement défini par $\tau(\pi_s) = \zeta_{p^s}\pi_s$. Les extensions K_∞ et $K(\zeta_p)$ étant linéairement disjointes sur K, on peut prolonger τ à $\bar{K}$ de façon à ce que $\chi(\tau) \equiv 1 \pmod p$. En réalité, le lemme 5.1.2 de [17] nous dit même que l'on peut imposer $\chi(\tau) = 1$. Toutefois, bien que cela complique légèrement les calculs, nous préférons continuer à travailler avec un τ plus général vérifiant seulement $\chi(\tau) \equiv 1 \pmod p$. Il suit de la définition de τ que $c(\tau) = 1$. En outre, en vertu de ce qui a été dit juste en dessous de cet alinéa, on peut définir $c(\tau^a)$ et $\chi(\tau)^a$ pour tout $a \in \mathbb{Z}_p$. La formule (1.2) s'écrit alors simplement $c(\tau^a) = [a]_{\chi(\tau)}$.

Lemme 1.1. *L'application $\mathbb{Z}_p \to \mathbb{Z}_p$, $a \mapsto [a]_{\chi(\tau)}$ est une bijection. De plus, pour tout $a \in \mathbb{Z}_p$, on a $a \equiv [a]_{\chi(\tau)} \pmod p$ et les valuations p-adiques de $a - 1$ et de $[a]_{\chi(\tau)} - 1$ sont égales.*

Démonstration. Si $\chi(\tau) = 1$, l'application est l'identité et il n'y a rien à démontrer. Dans le cas contraire, pour démontrer que $a \mapsto [a]_{\chi(\tau)}$ est bijective, il suffit de remarquer que l'inverse est donnée par $b \mapsto \frac{\log(1+(\chi(\tau)-1)b)}{\log \chi(\tau)}$, application qui est bien définie car $\chi(\tau) \equiv 1 \pmod p$ et $p > 2$. Pour la deuxième assertion, on écrit $\chi(\tau) = 1 + px$. On a alors

$$[a]_{\chi(\tau)} = a + \frac{a(a-1)}{2} \cdot px + \frac{a(a-1)(a-2)}{6} \cdot p^2x^2 + \cdots + \frac{a(a-1)\cdots(a-n+1)}{n!} \cdot p^nx^n + \cdots$$

et il est déjà clair que $a \equiv [a]_{\chi(\tau)} \pmod p$. On remarque ensuite que de $a \equiv 1 \pmod{p^s}$, il suit $[a]_{\chi(\tau)} \equiv a \pmod{p^{s+1}}$ car $\frac{p^n}{n!}$ est toujours multiple de p dans $\mathbb{Z}_p$ (on rappelle que l'on suppose $p > 2$) et $a - 1$ est lui, par définition, multiple de p^s. La conclusion en résulte. $\square$

D'après le lemme, pour tout élément $g \in G_K$, il existe un unique $a \in \mathbb{Z}_p$ tel que $[a]_{\chi(\tau)} = \chi(g)$. Notons $\chi_\tau(g)$ cet élément ; on définit de cette manière une fonction $\chi_\tau : G_K \to \mathbb{Z}_p$ qui, d'après la congruence $a \equiv [a]_{\chi(\tau)} \pmod p$, prend ses valeurs dans $\mathbb{Z}_p^\times$. On prendra garde au fait que χ_τ n'est pas un morphisme de groupes ; cependant, son « noyau » (*i.e.* l'image réciproque de $1 \in \mathbb{Z}_p^\times$) est le sous-groupe H_K. L'égalité entre valuations établie dans le lemme 1.1 assure en outre que, pour tout entier m, l'image réciproque du sous-groupe $1 + p^m\mathbb{Z}_p$ de $\mathbb{Z}_p^\times$ est le sous-groupe $\mathrm{Gal}(\bar{K}/K(\zeta_{p^m}))$ de G_K.

Lemme 1.2.
1. *Tout élément $g \in G_K/H_\infty$ s'écrit de façon unique sous la forme $\tau^a g'$ avec $a \in \mathbb{Z}_p$ et $g' \in G_\infty/H_\infty$*
2. *Pour tout $g \in G_\infty/H_\infty$, le produit $\tau^{-\chi_\tau(g)}g\tau$ calculé dans G_K/H_∞ appartient à G_∞/H_∞.*

Démonstration. Pour le premier alinéa, il s'agit de montrer que l'équation $c(\tau^{-a}g) = 0$ a une unique solution dans $\mathbb{Z}_p$. Or on a $c(\tau^{-a}g) = [-a]_{\chi(\tau)} + \chi(\tau)^{-a}c(g) = \chi(\tau)^{-a}\big(c(g) - [a]_{\chi(\tau)}\big)$, à partir de quoi le lemme 1.1 permet de conclure. Pour le deuxième alinéa, il suffit de vérifier que $c(\tau^{-\chi_\tau(g)}g\tau) = 0$, ce qui se fait comme précédemment. $\square$

Proposition 1.3. *Soit Γ un groupe topologique et $\rho : G_\infty/H_\infty \to \Gamma$ un morphisme de groupes continu. Se donner un prolongement continu $\tilde{\rho} : G_K/H_\infty \to \Gamma$ de ρ revient à se donner un élément $\tau_\Gamma \in \Gamma$ (l'image de τ) tel que pour tout $g \in G_\infty/H_\infty$ vérifiant $\chi_\tau(g) \in \mathbb{N}$, on ait :*

$$\rho(g) \cdot \tau_\Gamma = \tau_\Gamma^{\chi_\tau(g)} \cdot \rho(\tau^{-\chi_\tau(g)}g\tau). \tag{1.3}$$

Démonstration. D'après le premier point du lemme 1.2, il est clair que $\tau_\Gamma = \tilde{\rho}(\tau)$ détermine entièrement $\tilde{\rho}$. L'unicité en résulte. Pour l'existence, montrons dans un premier temps que $\lim_{s\to\infty} \tau_\Gamma^{p^s} = 1$. Étant donné que $\chi(G_\infty) = \chi(G_K)$ est ouvert dans $\mathbb{Z}_p^\times$, il existe un entier s_0 tel que $\chi(G_\infty) \supset 1 + p^{s_0}\mathbb{Z}_p$. Comme d'après le lemme 1.1, l'application $a \mapsto [a]_{\chi(\tau)}$ réalise une bijection de $1 + p^s\mathbb{Z}_p$ dans lui-même pour tout s, il existe une suite $(g_s)_{s\geqslant s_0}$ d'éléments de G_∞/H_∞ convergeant vers l'identité et telle que $\chi_\tau(g_s) = p^s + 1$. En appliquant la relation (1.3) avec g_s, il vient $\tau_\Gamma^{p^s} = \rho(g_s) \cdot \tau_\Gamma \cdot \rho(\tau^{-\chi_\tau(g_s)}g_s\tau) \cdot \tau_\Gamma^{-1}$. Un passage à la limite pour s tendant vers l'infini donne alors la conclusion annoncée. Ceci nous permet de définir τ_Γ^a pour tout élément $a \in \mathbb{Z}_p$ et en passant à la limite dans (1.3), on montre que cette dernière relation est valable pour tout $g \in G_\infty/H_\infty$. Il suffit maintenant de montrer que l'application $\tilde{\rho}$ définie par

$$\forall a \in \mathbb{Z}_p, \forall g \in G_\infty/H_\infty, \quad \tilde{\rho}(\tau^a g) = \tau_\Gamma^a \rho(g)$$

est un morphisme de groupes. Il s'agit donc de vérifier que si $g\tau^a = \tau^b h$ avec $a, b \in \mathbb{Z}_p$ et $g, h \in G_\infty/H_\infty$, alors $\rho(g)\tau_\Gamma^a = \tau_\Gamma^b \rho(h)$. Tout d'abord, en appliquant c à l'égalité $g\tau^a = \tau^b h$, on obtient $\chi(g) \cdot [a]_{\chi(\tau)} = [b]_{\chi(\tau)}$. Si $a = 1$, on voit à présent que l'égalité que l'on a à démontrer n'est autre que l'hypothèse. Pour $a \in \mathbb{N}$, l'égalité se démontre par récurrence, tandis qu'enfin, pour $a \in \mathbb{Z}_p$, on utilise un argument de passage à la limite. $\square$

Bien entendu, le cas qui nous intéressera particulièrement dans cet article est celui où le groupe Γ est le groupe des automorphismes linéaires ou semi-linéaires d'un certain espace. Dans cette situation, la proposition dit exactement ce qu'il faut ajouter à une représentation de G_∞/H_∞ pour définir une représentation de G_K/H_∞.

1.1.3 Comment se dispenser de quotienter par H_∞

Dans le lemme 1.2 et la proposition 1.3, nous avons systématiquement quotienter par H_∞. Toutefois, on peut s'affrachir de cela en prenant soin de choisir au préalable un élément $\tau \in G_K$ vérifiant $\lim_{s\to\infty} \tau^{p^s} = \mathrm{id}$. Un tel choix est toujours possible car, étant donné que l'extension K_∞/K n'admet pas de sous-extension modérément ramifiée, on peut choisir τ dans le sous-groupe d'inertie sauvage ; comme celui-ci est un pro-p-groupe, la convergence requise en résulte. Une fois ce choix fait, les démonstrations du lemme 1.2 et de la proposition 1.3 s'étendent mot pour mot en remplaçant partout G_K/H_∞ par G_K et G_∞/H_∞ par G_∞. En particulier, on voit que se donner une action de G_K revient, dans ce cas, à se donner une action de G_∞ et un automorphisme τ_Γ (correspondant à l'action de τ) vérifiant la relation de commutation (1.3). Toutefois, dans la suite, nous nous contenterons d'appliquer la proposition 1.3 au groupe quotient G_K/H_∞, et il ne nous sera donc pas nécessaire de particulariser ainsi le choix de τ.

Un fait notable, par contre, est qu'un corollaire de la généralisation que l'on vient d'évoquer permet de donner une description de G_K en termes de G_∞ à l'aide d'une construction de type « produit semi-direct ». On choisit pour cela un élément τ dans le groupe d'inertie sauvage vérifiant à la fois $c(\tau) = 1$ et $\chi(\tau) = 0$ (un tel choix est possible). On a alors les propriétés suivantes :

- tout élément de G_K s'écrit de façon unique sous la forme $\tau^a g$ avec $a \in \mathbb{Z}_p$ et $g \in G_\infty$;
- si $g \in G_\infty$ et $a \in \mathbb{Z}_p$, alors $h = \tau^{-a\chi(g)} g \tau^a \in G_\infty$ et on a bien sûr la relation $g\tau^a = \tau^{a\chi(g)} h$.

Ainsi si l'on se donne G_∞, la restriction du caractère cyclotomique $\chi : G_\infty \to \mathbb{Z}_p^\times$ et l'application $\psi : G_\infty \to G_\infty$, $g \mapsto \tau^{-\chi(g)} g \tau$, on peut reconstruire le groupe G_K tout entier en considérant l'ensemble $\mathbb{Z}_p \times G_\infty$ muni de la loi de groupe suivante :

$$(a, g) \cdot (b, h) = (a + b\chi(g), \psi^b(g)h).$$

On prendra garde néanmoins au fait que l'application ψ n'est pas un morphisme de groupes mais vérifie néanmoins une relation, à savoir $\psi(gh) = \psi^{\chi(h)}(g)\psi(h)$.

1.2 Les (φ, τ)-modules en caractéristique p

Dans ce paragraphe, nous mettons au point la théorie des (φ, τ)-modules en caractéristique p, c'est-à-dire que nous établissons la troisième équivalence de catégories du théorème 1 de l'introduction lorsque $n = 1$ (les anneaux $\mathcal{E}^{\mathrm{int}}$ et $\mathcal{E}_\tau^{\mathrm{int}}$ étant alors remplacés par des variantes plus simples). La méthode est simple et naturelle : elle consiste à mettre ensemble ce qui vient d'être fait et le théorème de Fontaine et Fontaine-Wintenberger de classification des représentations de G_∞ *via* les φ-modules étales. Nous commençons par quelques rappels à ce sujet.

1.2.1 Rappels sur la classification des représentations de G_∞

On considère l'anneau $R = \varprojlim \mathcal{O}_{\bar{K}}/p$ où les morphismes de transition sont donnés par l'élévation à la puissance p : un élément $x \in R$ est donc une suite $(x_s)_{s\geqslant 0}$ telle que $x_{s+1}^p = x_s$ pour tout s. On note $\mathrm{Frac}\, R$ le corps des fractions de R ; c'est un corps algébriquement clos. À côté de cela, il est clair que R

est muni d'une action canonique de G_K qui s'étend à $\mathrm{Frac}\, R$. Par ailleurs, si l'on note v_K la valuation sur $\bar{K}$ normalisée par $v_K(K^\star) = \mathbb{Z}$, on démontre que la formule $v_R(x) = \lim_{s\to\infty} p^s v_K(x_s)$ définit une valuation (non discrète) sur R pour laquelle il est complet. La valuation v_R s'étend naturellement à $\mathrm{Frac}\, R$ et on note encore v_R ce prolongement. Le corps résiduel k s'injecte canoniquement dans R : à un élément $\lambda \in k$, on associe la suite des λ^{1/p^s} vus comme éléments de $\mathcal{O}_{\bar{K}}/p$. Les systèmes compatibles (ζ_{p^s}) et (π_s) de racines p^s-ièmes de l'unité et de π respectivement définissent, eux aussi, des éléments de R que l'on note respectivement $\underline{\varepsilon}$ et $\underline{\pi}$. On a $v_R(\underline{\varepsilon}) = 0$ et $v_R(\underline{\pi}) = 1$. On pose $\eta = 1 - \underline{\varepsilon}$ de sorte que $v_R(\eta) = \frac{ep}{p-1}$. Par construction le groupe H_K agit trivialement sur $\underline{\varepsilon}$ et η tandis que G_∞, lui, agit trivialement sur $\underline{\pi}$. Dans la suite, on plongera systématiquement l'anneau $k[[u]]$ dans R en envoyant u sur $\underline{\pi}$. Ce morphisme s'étend aux corps des fractions et définit ainsi un plongement du corps $F_0 = k((u))$ dans $\mathrm{Frac}\, R$. On appelle F_0^{sep} la clotûre séparable de F_0 dans $\mathrm{Frac}\, R$. Étant donné que G_∞ agit trivialement sur F_0 vu dans $\mathrm{Frac}\, R$, tout élément de G_∞ stabilise F_0^{sep} et on obtient comme ceci un morphisme $G_\infty \to \mathrm{Gal}(F_0^{\mathrm{sep}}/F_0)$. La théorie du corps des normes de Fontaine et Wintenberger (voir [23]) affirme que c'est en fait un isomorphisme. Comme corollaire du théorème de Hilbert 90, Fontaine démontre alors la proposition suivante.

Proposition 1.4. *Soit T une $\mathbb{F}_p$-représentation du groupe G_∞. On suppose que T est de dimension finie d sur $\mathbb{F}_p$. Alors l'espace $\mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}})$ est de dimension d sur F_0 et, plus précisément, le morphisme naturel*

$$F_0^{\mathrm{sep}} \otimes_{F_0} \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}}) \to \mathrm{Hom}_{\mathbb{F}_p}(T, F_0^{\mathrm{sep}})$$

est un isomorphisme.

Démonstration. C'est un cas particulier [3] de la proposition A.1.2.6 et de la remarque A.1.2.7 de [11]. □

Remarque 1.5. Le vrai contenu de la proposition réside dans la surjectivité de l'application. L'injectivité, quant à elle, est un fait beaucoup plus général, qui reste valable si l'on remplace G_∞ par n'importe quel groupe topologique H, F_0^{sep} par n'importe quel corps L de caractéristique p sur lequel H agit continument, et F_0 par L^H (la démonstration étant en tout point identique).

À partir de la proposition précédente, Fontaine déduit un théorème de classification des $\mathbb{F}_p$-représentations de dimension finie de G_∞. Pour l'énoncer, on doit d'abord définir la notion de *φ-module étale sur F_0* : il s'agit de la donnée d'un espace vectoriel M de dimension finie sur F_0 muni d'une application $\varphi_M : M \to M$ semi-linéaire par rapport au Frobenius sur F_0 (défini comme l'élévation à la puissance p), et dont l'image contient une base de M. Étant donné un φ-module étale M sur F_0, il est souvent commode de considérer le linéarisé de φ_M défini comme l'application $\mathrm{id} \otimes \varphi_M : F_0 \otimes_{\varphi, F_0} M \to M$. On a alors affaire à une application F_0-linéaire, et la condition selon laquelle l'image de φ_M contient une base de M se traduit alors en disant que $\mathrm{id} \otimes \varphi_M$ est un isomorphisme. Si T est une représentation de G_∞, alors $\mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}})$ est naturellement muni d'un endomorphisme φ déduit du Frobenius usuel sur F_0^{sep}, et il est facile de vérifier que c'est en fait un φ-module étale sur F_0.

Théorème 1.6. *Les foncteurs suivants sont des équivalences de catégories quasi-inverses l'une de l'autre :*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \mathbb{F}_p\text{-représentations de} \\ \text{dimension finie de } G_\infty \end{array} \right\} & \xrightarrow{\sim} & \left\{ \varphi\text{-modules étales sur } F_0 \right\} \\ T & \mapsto & \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}}) \\ \mathrm{Hom}_{F_0,\varphi}(M, F_0^{\mathrm{sep}}) & \leftarrow & M \end{array}$$

où $\mathrm{Hom}_{F_0,\varphi}$ signifie que l'on considère les morphismes F_0-linéaires commutant à l'action de φ (celui-ci agissant par l'élévation à la puissance p sur F_0^{sep}).

Démonstration. Voir proposition A.1.2.6 et remarque A.1.2.7 de [11]. □

1.2.2 Une équivalence de catégories

On pose à partir de maintenant pour simplifier les écritures $L = \mathrm{Frac}\, R$. Le sous-corps de L, formé des éléments fixes par H_∞ contient manifestement $(F_0^{\mathrm{sep}})^{H_\infty}$ et donc en particulier F_0. On le note F_τ.

3. Dans cette référence, on travaille déjà avec des coefficients dans $\mathbb{Z}_p$, ce que, de notre côté, nous ne ferons que dans le §1.3 (voir théorème 1.6).

Définition 1.7. Un (φ, τ)-*module sur* (F_0, F_τ) est la donnée de
- un φ-module étale sur F_0, noté M ;
- un endomorphisme τ-semi-linéaire $\tau_M : F_\tau \otimes_{F_0} M \to F_\tau \otimes_{F_0} M$ qui commute à $\varphi_{F_\tau} \otimes \varphi_M$ (où φ_{F_τ} est le Frobenius usuel sur F_τ) et qui vérifie, pour tout $g \in G_\infty / H_\infty$ tel que $\chi_\tau(g) \in \mathbb{N}$, la relation suivante :
$$\forall x \in M, \quad (g \otimes \mathrm{id}) \circ \tau_M(x) = \tau_M^{\chi_\tau(g)}(x). \tag{1.4}$$

On est en droit de se demander d'où vient la différence entre la relation précédente et celle de la proposition 1.3 dans laquelle il apparaissait un terme supplémentaire dans le membre de droite. La raison en est — et nous attirons l'attention du lecteur sur ce point — que l'on ne demande à l'égalité (1.4) de n'être satisfaite que pour $x \in M$ et non pas pour tout $x \in F_\tau \otimes_{F_0} M$. La semi-linéarité de τ montre en réalité que l'identité (1.4) est équivalente à l'égalité suivante entre applications :
$$(g \otimes \mathrm{id}) \circ \tau_M = \tau_M^{\chi_\tau(g)} \circ ((\tau^{-\chi_\tau(g)} g \tau) \otimes \mathrm{id})$$
ce qui correspond bien à la formule de la proposition 1.3.

On montre comme dans la preuve de cette même proposition que pour tout (φ, τ)-module M, les applications $\tau_M^{p^s}$ forment une suite qui converge vers l'identité. On peut donc définit τ_M^a pour $a \in \mathbb{Z}_p$ et la relation (1.4) est alors satisfaite pour tout $g \in G_\infty$ sans la restriction $\chi_\tau(g) \in \mathbb{N}$. Ceci montre en particulier que τ_M^{-1} est défini, c'est-à-dire que $\tau_M : F_\tau \otimes_{F_0} M \to F_\tau \otimes_{F_0} M$ est une bijection. Dans la suite, lorsque cela ne prêtera pas à confusion, on notera simplement τ à la place de τ_M et de même, on écrira souvent φ à la place de φ_M.

Le but de ce paragraphe est de démontrer que la catégorie des $\mathbb{F}_p$-représentations de dimension finie de G_K est équivalente à la catégorie des (φ, τ)-modules sur (F_0, F_τ). À ce sujet, nous aimerions signaler au lecteur que Tavares Ribeiro s'est déjà intéressé, dans le premier chapitre de sa thèse [20], à des questions semblables. Toutefois, le point de vue que nous adoptons est un peu différent et en fait plus proche des travaux de Liu ; notamment, nous avons constamment le souci de garder explicitement la trace du φ-module M décrivant l'action du sous-groupe G_∞ alors que celui-ci n'apparaît pas du tout dans les travaux de Tavares Ribeiro.

Construction d'un foncteur On considère, dans un premier temps, une $\mathbb{F}_p$-représentation T de G_K de dimension finie d et on note $\mathcal{M}(T) = \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}})$ le φ-module associé par le théorème 1.6. On sait que $\mathcal{M}(T)$ est de dimension d sur F_0. Pour définir une structure de (φ, τ)-module sur $\mathcal{M}(T)$, il reste à construire un automorphisme τ de $F_\tau \otimes_{F_0} \mathcal{M}(T)$. On commence par un lemme qui donne une description alternative de cet espace.

Lemme 1.8. *L'application naturelle* $F_\tau \otimes_{F_0} \mathcal{M}(T) \to \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, L)$ *est un isomorphisme.*

Démonstration. Par la remarque 1.5, on sait que l'application $L \otimes_{F_\tau} \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, L) \to \mathrm{Hom}_{\mathbb{F}_p}(T, L)$ est injective, et donc que l'espace $\mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, L)$ est de dimension au plus d sur F_τ. Il suffit donc de montrer que le morphisme du lemme est injectif. Or, celui-ci s'écrit $\beta \circ (F_\tau \otimes_{(F_0^{\mathrm{sep}})^{H_\infty}} \alpha)$ où α et β sont les morphismes canoniques suivants :
$$\begin{aligned}
\alpha &: \quad (F_0^{\mathrm{sep}})^{H_\infty} \otimes_{F_0} \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}}) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, F_0^{\mathrm{sep}}) \\
\beta &: \quad F_\tau \otimes_{(F_0^{\mathrm{sep}})^{H_\infty}} \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, F_0^{\mathrm{sep}}) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, L).
\end{aligned}$$

Il suffit donc de montrer que α et β sont injectifs. Pour α, cela résulte du diagramme commutatif
$$\begin{tikzcd}
(F_0^{\mathrm{sep}})^{H_\infty} \otimes_{F_0} \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}}) \arrow[r, "\alpha"] \arrow[d, hook] & \mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, F_0^{\mathrm{sep}}) \arrow[d, hook] \\
F_0^{\mathrm{sep}} \otimes_{F_0} \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}}) \arrow[r] & \mathrm{Hom}_{\mathbb{F}_p}(T, F_0^{\mathrm{sep}})
\end{tikzcd}$$
et de la proposition 1.4 qui affirme que la flèche du bas est un isomorphisme. On en vient maintenant à β. Il suffit de montrer que si $f_1, \ldots, f_n$ est une famille d'éléments de $\mathrm{Hom}_{\mathbb{F}_p[H_\infty]}(T, F_0^{\mathrm{sep}})$ qui est liée sur F_τ, alors elle l'est déjà sur $(F_0^{\mathrm{sep}})^{H_\infty}$. Soit $\lambda_1 f_1 + \cdots + \lambda_n f_n = 0$ une relation de liaison avec tous les

λ_i dans F_τ. Puisque T est un ensemble fini, il existe un sous-groupe distingué d'indice fini $H \subset H_\infty$ qui agit trivialement sur T, ce qui signifie que les fonctions f_i prennent leurs valeurs dans $(F_0^{\text{sep}})^H$. Les extensions L^H/F_τ et $(F_0^{\text{sep}})^H/(F_0^{\text{sep}})^{H_\infty}$ sont alors galoisiennes de groupes de Galois isomorphes à H_∞/H. On considère une forme linéaire $\ell : L^H \to (F_0^{\text{sep}})^H$ qui envoie λ_1 sur un élément dont la trace sur $(F_0^{\text{sep}})^{H_\infty}$ ne s'annule pas, et on définit une application $\ell_{H_\infty} : L^H \to (F_0^{\text{sep}})^H$ en moyennant ℓ comme suit :

$$\ell_{H_\infty}(x) = \sum_{h \in H/H_\infty} h\,\ell(h^{-1}x).$$

On vérifie sans difficulté que ℓ_{H_∞} est encore une forme linéaire. Elle est en outre H_∞-équivariante, et donc applique F_τ sur $(F_0^{\text{sep}})^{H_\infty}$. Par ailleurs, puisque λ_1 est fixé par H_∞, son image par ℓ_{H_∞} est égale à $\text{tr}_{(F_0^{\text{sep}})^H/(F_0^{\text{sep}})^{H_\infty}}\,\ell(\lambda_1)$, et n'est donc pas nulle. Ainsi, en appliquant ℓ_{H_∞} à l'égalité $\lambda_1 f_1 + \cdots + \lambda_n f_n = 0$, on obtient une relation de liaison non triviale entre les f_i qui est à coefficients dans $(F_0^{\text{sep}})^{H_\infty}$, ce qui est bien ce que l'on cherchait. $\square$

Remarque 1.9. La preuve que l'on vient de donner montre plus généralement que le lemme précédent vaut pour un sous-groupe fermé quelconque H de G_∞ et un sous-corps L de $\text{Frac}\,R$ contenant F_0^{sep} et stable seulement par H.

Il n'est maintenant plus difficile de définir l'automorphisme τ. À cette fin, on note que pour $\sigma \in G_K$ et $f \in \text{Hom}_{\mathbb{F}_p[H_\infty]}(T, L)$, l'application $g : x \mapsto \sigma f(\sigma^{-1}x)$ est encore H_∞-équivariante ; la formule précédente définit donc une action de G_K sur $\text{Hom}_{\mathbb{F}_p[H_\infty]}(T, L) = F_\tau \otimes_{F_0} \mathcal{M}(T)$ qui est, comme on le vérifie directement, semi-linéaire par rapport à la structure de F_τ-espace vectoriel. De plus, pour cette action, le sous-groupe H_∞ agit trivialement (ce qui signifie que l'action se factorise par G_K/H_∞), tandis que le groupe G_∞, de son côté, agit trivialement sur le sous-ensemble $\mathcal{M}(T)$. On définit enfin l'application τ comme l'automorphisme de $F_\tau \otimes_{F_0} \mathcal{M}(T)$ donné par l'action de τ. Les remarques que l'on vient de faire, combinée au second point du lemme 1.2 assurent que l'on obtient bien comme ceci un (φ, τ)-module dans le sens de la définition 1.7.

Construction d'un quasi-inverse On part à présent d'un (φ, τ)-module M sur (F_0, F_τ) et on cherche à lui associer une représentation $\mathcal{T}(M)$ de G_K qui soit de dimension finie sur $\mathbb{F}_p$. Bien entendu, en tant que représentation de G_∞, $\mathcal{T}(M)$ est la représentation associé au φ-module sous-jacent, *i.e.* $\mathcal{T}(M) = \text{Hom}_{F_0,\varphi}(M, F_0^{\text{sep}})$. Il reste donc à expliquer comment étendre cette action à G_K en utilisant l'automorphisme τ. La clé est le lemme suivant.

Lemme 1.10. *L'application $\mathcal{T}(M) = \text{Hom}_{F_0,\varphi}(M, F_0^{\text{sep}}) \to \text{Hom}_{F_\tau,\varphi}(F_\tau \otimes_{F_0} M, L)$ déduite de l'extension des scalaires de F_0 à F_τ est un isomorphisme.*

Démonstration. On fixe une base $(e_1, \ldots, e_d)$ de M et on appelle G l'unique matrice pour laquelle l'égalité $(\varphi(e_1), \ldots, \varphi(e_d)) = (e_1, \ldots, e_d)G$ est vérifiée. Se donner un élément de $\text{Hom}_{F_0,\varphi}(M, F_0^{\text{sep}})$ (resp. de $\text{Hom}_{F_\tau,\varphi}(F_\tau \otimes_{F_0} M, L)$) revient à se donner les images de e_i qui sont des éléments $x_i \in F_0^{\text{sep}}$ (resp. $x_i \in L$) vérifiant le système d'équations $(x_1^p, \ldots, x_d^p) = (x_1, \ldots, x_d)G$. Or, un tel système a au plus p^d solutions dans n'importe quel corps, et on sait qu'il en a déjà ce nombre de F_0^{sep}. Toutes les solutions dans L sont donc dans F_0^{sep} et le lemme est démontré. $\square$

Étant donné les conditions satisfaites par τ, la proposition 1.3 s'applique et montre qu'il existe une unique action de G_K/H_∞ sur le produit tensoriel $F_\tau \otimes_{F_0} M$ pour laquelle les éléments $g \in G_\infty/H_\infty$ agissent par $(g \otimes \text{id})$ et l'élément τ agit *via* l'automorphisme τ. En composant par la projection canonique $G_K \to G_K/H_\infty$, on obtient une action de G_K sur $F_\tau \otimes_{F_0} M$. Par ailleurs, G_K agit également sur L et donc sur l'espace $\mathcal{T}(M) = \text{Hom}_{F_\tau,\varphi}(F_\tau \otimes_{F_0} M, L)$ *via* la formule usuelle $\sigma \cdot f : x \mapsto \sigma\, f(\sigma^{-1}x)$. La forme particulière de l'action de G_∞ sur $F_\tau \otimes_{F_0} M$ montre immédiatement que l'action qu'on vient de définir sur $\mathcal{T}(M)$ prolonge celle de G_∞.

Théorème 1.11. *Les deux foncteurs $\mathcal{M}$ et $\mathcal{T}$ précédents induisent des équivalences de catégories inverses l'une de l'autre entre la catégorie des $\mathbb{F}_p$-représentations de dimension finie de G_K et la catégorie des (φ, τ)-modules sur (F_0, F_τ).*

Démonstration. On sait déjà, par le théorème 1.6, que les morphismes canoniques $M \to \mathcal{M}(\mathcal{T}(M))$ et $T \to \mathcal{T}(\mathcal{M}(T))$ sont des isomorphismes pour tout (φ, τ)-module M sur (F_0, F_τ) et toute $\mathbb{F}_p$-représentation T de dimension finie de G_K. Il ne reste donc qu'à vérifier que le premier commute à l'action de τ tandis que le deuxième est G_K-équivariant, ce qui ne pose aucune difficulté. □

Remarque 1.12. En considérant non pas l'action de τ mais celle de τ^{p^s}, on obtient de la même façon une équivalence de catégories entre, d'une part, la catégorie des $\mathbb{F}_p$-représentations du groupe G_s et, d'autre part, la catégorie des (φ, τ^{p^s})-modules sur (F_0, F_τ) dont les objets sont la donnée de :

– un φ-module étale sur F_0, noté M ;
– un automorphisme τ^{p^s}-semi-linéaire $\tau_M^{(p^s)} : F_\tau \otimes_{F_0} M \to F_\tau \otimes_{F_0} M$ qui commute à φ et tel que, pour tout $g \in G_\infty/H_\infty$

$$\forall x \in M, \quad (g \otimes \mathrm{id}) \circ \tau_M^{(p^s)}(x) = (\tau_M^{(p^s)})^a(x)$$

où a est l'unique élément de $\mathbb{Z}_p$ tel que $\chi(g) \cdot [p^s]_{\chi(\tau)} = [a]_{\chi(\tau)}$.

1.2.3 Quelques mots sur le corps F_τ

Le corps F_τ est important car c'est celui qui sert de base à l'action de τ sur un (φ, τ)-module. Il semble donc crucial de bien le comprendre. Or, malheureusement, comme nous allons le voir dans ce paragraphe, sa structure est loin d'être simple.

Proposition 1.13. *Soit H un sous-groupe fermé de G_∞. Alors L^H est l'adhérence (dans L) du perfectisé de $(F_0^{\text{sep}})^H$.*

De plus, si on note $\mathfrak{m}_R$ l'idéal maximal de R, la projection canonique induit, pour tout $x \in R$, un morphisme surjectif $R^H \to (R/x\mathfrak{m}_R)^H$.

Démonstration. La première partie de la proposition s'obtient en mettant ensemble les deux ingrédients suivants : le corps F_0^{sep} est dense dans L (ce qui est contenu dans la théorie du corps des normes) et le théorème principal de [1] qui décrit les points fixes, sous l'action du groupe de Galois, du complété de la clôture algébrique d'un corps local. La seconde assertion se démontre de manière analogue en utilisant, à la place du théorème principal de [1], la proposition 2 de ce même article (p. 424), qui est un peu plus précise. □

La proposition précédente s'applique en particulier avec le groupe H_∞ et montre donc que F_τ s'identifie à l'adhérence du perfectisé du corps $F_\infty = (F_0^{\text{sep}})^{H_\infty}$. L'élément (important) $\eta = 1 - \underline{\varepsilon} \in R$, qui est clairement stable par l'action de H_∞, doit donc s'écrire comme une série faisant intervenir certains éléments du perfectisé de F_∞. Cependant, obtenir une telle écriture de façon explicite ne semble pas du tout facile. Voici une autre façon d'appréhender F_τ (qui montre encore que décrire les éléments de ce corps est une question délicate). Pour tout entier m, on note $H_m = \mathrm{Gal}(\bar{K}/K_\infty(\zeta^{p^m}))$ et $F_m = (F_0^{\text{sep}})^{H_m}$. Comme H_m est d'indice fini dans G_∞, l'extension F_m/F_0 est finie. La réunion de ces extensions, que l'on note F_{alg}, définit donc un sous-corps de F_τ qui est algébrique sur F_0. Par ailleurs, on peut considérer le morphisme $\iota : k[[X, Y]] \to F_\tau$ obtenu en envoyant X sur u et Y sur η. La proposition 1.14 ci-après montre que le corps des fractions de l'image de ι, noté $k((u, \eta))$, définit un sous-corps de F_τ qui est isomorphe à un corps de séries formelles en deux variables. C'est donc en particulier une extension purement transcendante de F_0. Les sous-corps F_{alg} et $k((u, \eta))$ apparaissent donc, d'un point de vue algébrique, comme deux constituants « orthogonaux » de F_τ. D'un point de vue topologique, par contre, ces corps semblent s'entremêler de façon subtile.

Proposition 1.14. *Le morphisme $\iota : k[[X, Y]] \to R$, $X \mapsto u$, $Y \mapsto \eta$ est injectif.*

Démonstration. Soit une série formelle $F \in k[[X, Y]]$ telle que $F(u, \eta) = 0$ dans R. En faisant agir le groupe de Galois G_K, on obtient l'annulation de $F(u(1 + \eta)^{c(g)}, (1 + \eta)^{\chi(g)} - 1)$ pour tout $g \in G_K$. Il en résulte les égalités :

$$F(u + u\eta^{p^n}, \eta) = 0 \quad \text{et} \quad F(u, \eta + \eta^{p^n} + \eta^{p^n+1}) = 0$$

pour tout entier n suffisamment grand. Pour tout entier i, soit $\partial_X^{[i]}$ l'application $\frac{1}{i!} \frac{\partial^i}{\partial X^i}$ agissant sur $k[[X, Y]]$ (qui est bien définie). On dispose de la formule de Taylor suivante :

$$F(u + u\eta^{p^n}, \eta) = F(u, \eta) + u\eta^{p^n} \partial_X^{[1]} F(u, \eta) + \cdots + u^i \eta^{ip^n} \partial_X^{[i]} F(u, \eta) + \cdots \tag{1.5}$$

grâce à laquelle on déduit, à partir des annulations précédemment citées, que $v_R(\partial_X^{[1]} F(u,\eta)) \geqslant \frac{ep^{n+1}}{p-1}$. Comme ceci est vrai pour tout n, il vient $\partial_X^{[1]} F(u,\eta) = 0$. Sachant cela, l'égalité (1.5) implique maintenant que $v_R(\partial_X^{[2]} F(u,\eta)) \geqslant \frac{ep^{n+1}}{p-1}$, et donc que $\partial_X^{[2]} F(u,\eta)$ s'annule lui aussi. Par récurrence, on démontre de la même manière que $\partial_X^{[i]} F(u,\eta) = 0$ pour tout i. Un raisonnement analogue à partir de $F(u, \eta + \eta^{p^n} + \eta^{p^n+1}) = 0$ montre que $\partial_Y^{[j]} F(u,\eta) = 0$ (avec des notations évidentes) pour tout j. En appliquant cela non pas à la série F mais à $\partial_X^{[i]} F$, on obtient même $\partial_Y^{[j]} \partial_X^{[i]} F(u,\eta) = 0$ pour tous i et j. En réduisant cette dernière égalité dans $\bar{k}$, on s'aperçoit alors que le coefficient de $X^i Y^j$ dans la série formelle F s'annule lui aussi. Il en résulte que la série F est, elle-même, nulle. □

Remarque 1.15. Le théorème 1.11 reste vrai lorsque le corps L est remplacé par la clôture séparable $k((u,\eta))^{\mathrm{sep}}$ de $k((u,\eta))$ dans L. Dans ce cas, la première partie de la proposition 1.13 se simplifie même un peu lorsque H est d'indice *fini* dans G_∞ puisque l'on peut démontrer qu'alors $(k((u,\eta))^{\mathrm{sep}})^H$ s'identifie simplement à $(F_0^{\mathrm{sep}})^H$. Ce résultat simple n'est par contre pas valable pour $H = H_\infty$: l'élément η appartient manifestement à $(k((u,\eta))^{\mathrm{sep}})^{H_\infty}$, mais il n'est pourtant pas dans $(F_0^{\mathrm{sep}})^{H_\infty}$ car, comme cela a été vu, il n'est pas algébrique sur F_0. Ainsi, décrire le corps des points fixes $(k((u,\eta))^{\mathrm{sep}})^{H_\infty}$ n'est, semble-t-il, pas non plus une question facile. En outre, le corps $k((u,\eta))^{\mathrm{sep}}$ a deux inconvénients : *primo*, il n'est pas évident de le relever en caractéristique nulle et *secundo*, il n'est pas complet pour la topologie u-adique ce qui, sans toutefois être un obstacle insurmontable, complique l'exposition de certains arguments. Par exemple, la deuxième partie de la proposition 1.13, que l'on utilisera à plusieurs reprises dans la suite, ne vaut pas lorsque L est remplacé par $k((u,\eta))^{\mathrm{sep}}$.

Terminons ce paragraphe en revenant un instant sur les corps F_m. L'extension F_1/F_0 se comprend assez bien, et on sait même la décrire complètement lorsque le corps K est absolument non ramifié (*i.e.* si $e = 1$). En effet, dans ce cas, une uniformisante de $K(\zeta_p)$ est donnée par une racine $(p-1)$-ième de $-p$, que l'on note ϖ. Si λ désigne un élément de k tel que $p \equiv -\pi\lambda \pmod{p^2}$, la suite d'éléments de $\mathcal{O}_{\bar{K}}/p$ suivante :

$$\left(\frac{1}{\lambda^{1/p^n}}\right)^{1+p+\cdots+p^{n-1}} \cdot \left(\frac{\varpi}{\pi_n^{1+p+\cdots+p^{n-1}}} \bmod p\right)$$

définit un élément v de R, qui appartient manifestement à F_1. Par ailleurs, un calcul immédiat montre que $v^{p-1} = \lambda u$. Comme F_1 est de degré $p-1$ sur F_0, il s'ensuit que $F_1 = F_0[v] = F_0[\sqrt[p-1]{\lambda u}]$. Lorsque $e > 1$, l'extension F_1/F_0 est encore totalement et modérément ramifiée, et son degré est égal à celui de l'extension $K(\zeta_p)/K$. Par contre, dès que $m \geqslant 1$, il semble bien plus difficile de comprendre l'extension F_{m+1}/F_m. On sait néanmoins qu'elle est soit triviale, soit de degré p. D'après la théorie d'Artin-Schreier, dans le deuxième cas, elle s'écrit comme le corps de rupture d'un polynôme de la forme $X^p - X - a_m$ avec $a_m \in F_m$. L'étude de la ramification sauvage de F_{m+1}/F_m permet d'accéder à la valuation de a_m, mais ne permet pas de répondre à la question plus générale suivante qui nous paraît intéressante.

Question 1.16. *Est-il possible, peut-être seulement sous l'hypothèse $e = 1$, de décrire explicitement un élément $a_m \in F_m$ tel que F_{m+1} soit le corps de rupture sur F_m du polynôme $X^p - X - a_m$?*

Plus généralement étant donné deux entiers m et m' avec $1 \leqslant m < m'$, peut-on décrire l'extension $F_{m'}/F_m$ en termes d'extensions d'Artin-Schreier-Witt ?

Comme me l'a signalé Berger, la compatibilité entre corps des normes et corps de classe (démontrée dans [14], §3) semble *a priori* une bonne piste pour étudier ce problème. Les calculs restent, malgré tout, encore à faire.

1.3 Relèvement modulo p^n et en caractéristique nulle

Le théorème 1 de l'introduction se déduit enfin du théorème 1.11 pour $L = F_\infty$ à l'aide d'arguments classiques de dévissage. Ce sont ces arguments que nous nous proposons de présenter dans cette partie. Afin surtout de mettre en place les notations, nous commençons par rappeler brièvement comment ceux-ci fonctionnent dans le cas classique des φ-modules et des représentations de G_∞.

1.3.1 La théorie de Fontaine modulo p^n et en caractéristique nulle

L'idée de base consiste à remplacer l'anneau R par l'anneau des vecteurs de Witt $W(\text{Frac}\, R)$; c'est naturellement une W-algèbre munie d'une action de G_K. L'anneau $\mathcal{E}^{\text{int}}$ défini dans l'introduction par, rappelons-le :

$$\mathcal{E}^{\text{int}} = \Big\{ \sum_{i \in \mathbb{Z}} a_i u^i \quad \Big| \quad a_i \in W, \ \lim_{i \to -\infty} a_i = 0 \Big\}$$

se plonge dans $W(\text{Frac}\, R)$ en envoyant u sur le représentant de Teichmüller $[\underline{\pi}]$. Muni de la valuation p-adique, $v_{\mathcal{E}}(\sum_{i \in \mathbb{Z}} a_i u^i) = \min_{i \in \mathbb{Z}} v_p(a_i)$, $\mathcal{E}^{\text{int}}$ est un anneau de valuation discrète qui admet F_0 pour corps résiduel. On note $\mathcal{E}^{\text{int,ur}}$ l'unique sous-algèbre étale (infinie) de $W(\text{Frac}\, R)$ ayant pour corps résiduel $F_0^{\text{sep}} \subset R$. Si l'on pose $\mathcal{E} = \text{Frac}\, \mathcal{E}^{\text{int}}$ et $\mathcal{E}^{\text{ur}} = \text{Frac}\, \mathcal{E}^{\text{int,ur}}$, le groupe de Galois de l'extension $\mathcal{E}^{\text{ur}}/\mathcal{E}$ s'identifie à celui de l'extension résiduelle F_0^{sep}/F_0 et donc finalement à G_∞. L'anneau $W(\text{Frac}\, R)[1/p]$ est naturellement muni d'un opérateur de Frobenius et celui-ci définit par restriction des endomorphismes de $\mathcal{E}^{\text{int}}$, $\mathcal{E}^{\text{int,ur}}$, $\mathcal{E}$ et $\mathcal{E}^{\text{ur}}$. Sur $\mathcal{E}^{\text{int}}$, par exemple, on voit aisément qu'il agit en appliquant le Frobenius traditionnel aux coefficients et en envoyant u sur u^p. On définit un *φ-module étale* sur $\mathcal{E}^{\text{int}}$ (resp. sur $\mathcal{E}$) comme la donnée d'un $\mathcal{E}^{\text{int}}$-module de type fini (resp. d'un $\mathcal{E}$-espace vectoriel de dimension finie) M munie d'une application $\varphi : M \to M$ semi-linéaire par rapport au Frobenius et dont l'image engendre M.

Théorème 1.17. *Les foncteurs suivants sont des équivalences de catégories quasi-inverses l'une de l'autre :*

$$\begin{array}{rcl} \left\{ \begin{array}{l} \mathbb{Q}_p\text{-représentations de} \\ \text{dimension finie de } G_\infty \end{array} \right\} & \xrightarrow{\sim} & \{ \ \varphi\text{-modules étales sur } \mathcal{E} \ \} \\ T & \mapsto & \text{Hom}_{\mathbb{Q}_p[G_\infty]}(T, \mathcal{E}^{\text{ur}}) \\ \text{Hom}_{\mathcal{E},\varphi}(M, \mathcal{E}^{\text{ur}}) & \leftarrow\!\shortmid & M \end{array}$$

On dispose d'énoncés analogues pour les $\mathbb{Z}_p$-représentations libres d'une part, et annulées par p^n d'autre part, que nous laissons au lecteur le soin d'écrire. On fait remarquer quand même qu'afin d'obtenir ces énoncés, il convient de remplacer l'anneau de périodes $\mathcal{E}^{\text{ur}}$ par $\mathcal{E}^{\text{int,ur}}$ et $\mathcal{E}^{\text{int,ur}}/p^n\mathcal{E}^{\text{int,ur}}$ respectivement. On peut également écrire une équivalence de catégories mettant en jeu à gauche la catégorie de toutes les $\mathbb{Z}_p$-représentations annulées par une puissance de p (non précisée) ; dans le cas, l'anneau de périodes $\mathcal{E}^{\text{ur}}$ doit être remplacé par le produit tensoriel $\mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathcal{E}^{\text{int,ur}}$ (qui n'est pas un anneau, mais seulement un $\mathcal{E}^{\text{int,ur}}$-module) ou, ce qui revient au même, par le quotient $\mathcal{E}^{\text{ur}}/\mathcal{E}^{\text{int,ur}}$.

1.3.2 Définition générale des (φ, τ)-modules

On pose $\mathcal{E}_\tau^{\text{int}} = W(F_\tau)$ et $\mathcal{E}_\tau = \text{Frac}\, \mathcal{E}_\tau^{\text{int}}$. Le corps F_τ étant parfait, la valuation p-adique fait de $\mathcal{E}_\tau^{\text{int}}$ un anneau de valuation discrète, complet, dont le corps résiduel s'identifie à F_τ. En outre, $\mathcal{E}_\tau$ s'obtient à partir de $\mathcal{E}_\tau^{\text{int}}$ simplement en inversant p. Tous les anneaux que l'on vient de définir sont munis d'un endomorphisme de Frobenius que l'on note φ ou φ_A (A étant l'anneau sur lequel le Frobenius afit) dans les cas où il sera important de le préciser. La définition des (φ, τ)-modules est désormais la même qu'en caractéristique p (voir définition 1.7) à part que les anneaux de base sont ceux que l'on vient de définir. On la redonne ci-dessous pour plus de clarté.

Définition 1.18. Un (φ, τ)-*module sur* $(\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}})$ (resp. $(\mathcal{E}, \mathcal{E}_\tau)$) est la donnée de

- un φ-module étale sur $\mathcal{E}^{\text{int}}$ (resp. sur $\mathcal{E}$), noté M ;
- un endomorphisme τ-semi-linéaire $\tau_M : \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M \to \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M$ qui commute à $\varphi_{\mathcal{E}_\tau^{\text{int}}} \otimes \varphi_M$ et vérifie, pour tout $g \in G_\infty/H_\infty$ tel que $\chi_\tau(g) \in \mathbb{N}$, la relation suivante :

$$\forall x \in M, \quad (g \otimes \text{id}) \circ \tau_M(x) = \tau_M^{\chi_\tau(g)}(x). \tag{1.6}$$

On souhaite à présent démontrer le théorème 1 de l'introduction, c'est-à-dire que les catégories de (φ, τ)-modules sont équivalentes aux catégories correspondantes de représentations galoisiennes. L'étape essentielle pour cela consiste à étendre les lemmes 1.8 et 1.10 (qui constituaient la clé de la démonstration dans le cas de caractéristique p) à la nouvelle situation relevée. À partir de maintenant, on supposera toujours implicitement que les $\mathbb{Q}_p$-représentations (resp. $\mathbb{Z}_p$-représentations) considérées sont de dimension finie sur $\mathbb{Q}_p$ (resp. de type fini comme $\mathbb{Z}_p$-module). Si T est une telle représentation du groupe G_∞, on note $\mathcal{M}(T)$ le φ-module étale sur $\mathcal{E}^{\text{int}}$ ou sur $\mathcal{E}$ qui lui est associé par la théorie de Fontaine. De même, si M est un φ-module étale défini sur $\mathcal{E}^{\text{int}}$ ou sur $\mathcal{E}$, on note $\mathcal{T}(M)$ la représentation p-adique qui lui correspond.

Lemme 1.19. *Pour toute $\mathbb{Z}_p$-représentation de torsion (resp. $\mathbb{Z}_p$-représentation libre, resp. $\mathbb{Q}_p$-représentation) T de G_∞, l'application naturelle*

$$\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(T) \to \mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(T, \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} W(L))$$
$$\textit{(resp. } \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(T) \to \mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(T, W(L)),$$
$$\textit{resp. } \mathcal{E}_\tau \otimes_{\mathcal{E}} \mathcal{M}(T) \to \mathrm{Hom}_{\mathbb{Q}_p[H_\infty]}(T, W(L)[1/p])\textit{)}$$

est un isomorphisme.

Pour tout φ-module étale M défini sur $\mathcal{O}_\mathcal{E}$ et de torsion (resp. défini sur $\mathcal{O}_\mathcal{E}$ et libre, resp. défini sur $\mathcal{E}$), l'application naturelle

$$\mathcal{T}(M) \to \mathrm{Hom}_{\mathcal{E}_\tau^{\text{int}},\varphi}(\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M, \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} W(L))$$
$$\textit{(resp. } \mathcal{T}(M) \to \mathrm{Hom}_{\mathcal{E}_\tau^{\text{int}},\varphi}(\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M, W(L)),$$
$$\textit{resp. } \mathcal{T}(M) \to \mathrm{Hom}_{\mathcal{E}_\tau,\varphi}(\mathcal{E}_\tau \otimes_{\mathcal{E}} M, W(L)[1/p])\textit{)}$$

est un isomorphisme.

Démonstration. On ne démontre que la première partie du lemme, la seconde étant totalement analogue. On prouve tout d'abord le résultat lorsque T est une $\mathbb{Z}_p$-représentation annulée par p^n. On raisonne par récurrence sur n. Pour $n = 1$, le résultat à démontrer est exactement l'assertion du lemme 1.8 ; il n'y a donc plus rien à faire. Pour passer de n à $n+1$, on considère T une représentation annulée par p^{n+1}. Elle s'insère dans la suite exacte $0 \to pT \to T \to T/pT \to 0$ qui donne naissance au diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(T/pT) \arrow[r] \arrow[d] & \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(T) \arrow[r] \arrow[d] & \mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(pT) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(T/pT, W(L)) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(T, CW(L)) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(pT, CW(L)) &
\end{tikzcd}$$

où $CW(L) = \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} W(L)$. La ligne du haut est exacte car, d'une part, le foncteur $\mathcal{M}$ l'est et, d'autre part, $\mathcal{E}_\tau^{\text{int}}$ est plat sur $\mathcal{E}^{\text{int}}$. Les flèches horizontales de gauche et de droite sont des isomorphismes par hypothèse de récurrence, et finalement la ligne du bas est exacte par exactitude à gauche du foncteur Hom. Une chasse au diagramme montre alors que la flèche verticale centrale est aussi un isomorphisme.

Le cas où T est une $\mathbb{Z}_p$-représentation quelconque (toujours supposée de type fini comme $\mathbb{Z}_p$-module) s'obtient alors par passage à la limite, tandis que celui où T est une $\mathbb{Q}_p$-représentation s'en déduit en inversant p. $\square$

Il nous reste à définir des foncteurs dans les deux sens entre la catégorie des $\mathbb{Z}_p$-représentations (resp. $\mathbb{Q}_p$-représentations) de G_K et celle des (φ, τ)-modules sur $(\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}})$ (resp. sur $(\mathcal{E}, \mathcal{E}_\tau)$) puis à montrer que ceux-ci réalisent des équivalences de catégories inverses l'une de l'autre. Pour cela, à la lumière du lemme précédent, il suffit de reprendre presque *verbatim* les constructions du §1.2.2, ce que nous laissons en exercice au lecteur. On réécrit toutefois explicitement les deux propriétés essentielles qui façonnent la construction de ces foncteurs : *primo*, le φ-module sous-jacent au (φ, τ)-module associé à une représentation T est $\mathcal{M}(T)$ et *secundo*, dans le cas où T est définie sur $\mathbb{Z}_p$ par exemple, l'action de τ sur $\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} \mathcal{M}(T)$ provient *via* le lemme de son action naturelle sur l'espace $\mathrm{Hom}_{\mathbb{Z}_p[H_\infty]}(T, W(L))$.

1.3.3 Deux exemples

Le premier exemple que nous aimerions présenter est celui d'une représentation T (définie au choix sur $\mathbb{F}_p$, $\mathbb{Z}_p$ ou $\mathbb{Q}_p$) dont la restriction au sous-groupe G_∞ est triviale, c'est-à-dire dont le φ-module correspondant est trivial. Cette hypothèse est en réalité très restrictive car, si l'action du sous-groupe G_∞ est triviale, il en est nécessairement de même de tous ses conjugués. Or, si s désigne le plus grand entier pour lequel le corps K admet une racine primitive p^s-ième de l'unité, les conjugués de G_∞ engendrent ensemble le sous-groupe (distingué) d'indice fini G_s. En particulier, si K ne contient pas de racine primitive p-ième de l'unité (par exemple si son indice de ramification absolu e est strictement plus petit que $p - 1$), une représentation de G_K, dont la restriction à G_∞ est triviale, est, elle même, triviale. Dans le cas général, l'action se factorise par le quotient G_K/G_s qui est un groupe cyclique de cardinal p^s engendré par l'image de τ.

Autrement dit, se donner une représentation T dont la restriction à G_∞ est triviale, revient à se donner un automorphisme τ de T d'ordre p^s. Le (φ, τ)-module M associé à T se décrit alors comme suit (la vérification est immédiate et laissée au lecteur) : on a $M = \mathcal{E}^{\text{int}} \otimes_{\mathbb{Z}_p} T$ et l'automorphisme τ_M sur $\mathcal{E}_\tau^{\text{int}} \otimes_{\mathcal{E}^{\text{int}}} M = \mathcal{E}_\tau^{\text{int}} \otimes_{\mathbb{Z}_p} T$ est $\tau \otimes \tau$.

Venons-en maintenant à notre second exemple, qui est celui du caractère cyclotomique, ou plus généralement d'une de ses puissances. En réalité, cet exemple a été traité par Liu dans son article [19] (voir exemple 3.2.3) au cours de son étude des réseaux dans les représentations semi-stables. Comme le calcul n'est pas évident et demande de connaître un peu de théorie de Hodge p-adique, nous préférons nous contenter ici de donner le résultat en renvoyant à *loc. cit.* pour la preuve.

Soit $\mathfrak{t} \in W(R)$ un élément non divisible par p vérifiant $\varphi(\mathfrak{t}) = c^{-1}E(u)\mathfrak{t}$ où $c = \frac{E(0)}{p}$ est un élément inversible dans $\mathbb{Z}_p$ (on rappelle, à toutes fins utiles, que $E(u)$ désigne le polynôme minimal sur $W[1/p]$ de l'uniformisante π choisie, et que c'est donc un polynôme d'Eisenstein). L'existence d'un tel élément $\mathfrak{t}$ découle du calcul de *loc. cit.* mais peut aussi se voir comme la conséquence du lemme 2.7 qui sera démontré dans la suite [4]. Avec ces notations, le (φ, τ)-module associé à la représentation $\mathbb{Z}_p(n)$ (avec $n \in \mathbb{Z}$), c'est-à-dire la représentation $T = \mathbb{Z}_p w$ où l'action de Galois est donnée par $gw = \chi(g)^n w$, est engendré par la fonction $f : T \to \mathcal{E}^{\text{int,ur}}$, $w \mapsto \mathfrak{t}^n$. Concrètement, il est décrit par les formules suivantes :

$$M = \mathcal{E}^{\text{int}} \cdot f \quad ; \quad \varphi(f) = c^{-n} E(u)^n \cdot f \quad \text{et} \quad \tau(f) = \left(\frac{\tau(\mathfrak{t})}{\mathfrak{t}}\right)^n \cdot f.$$

Les éléments $\mathfrak{t}$, $\tau(\mathfrak{t})$ et $E(u)$ sont inversibles dans $\mathcal{E}^{\text{int}}$, de sorte que les égalités précédentes ont bien un sens, même lorsque n est négatif. Les (φ, τ)-modules correspondant à $\mathbb{F}_p(n)$ et $\mathbb{Q}_p(n)$ sont donnés par des formules analogues.

2 Réseaux dans les (φ, τ)-modules

Nous avons démontré dans la section précédente que la catégorie des $\mathbb{Z}_p$-représentations galoisiennes de G_K est équivalente à celle des (φ, τ)-modules sur $(\mathcal{E}^{\text{int}}, \mathcal{E}_\tau^{\text{int}})$. Ce résultat peut paraître satisfaisant, mais il se heurte néanmoins à un problème pratique important lié au fait que l'anneau $\mathcal{E}_\tau^{\text{int}}$ est difficile à manipuler concrètement. On peut certes écrire ses éléments comme des séries, mais celles-ci requièrent une infinité de variables et des conditions de convergence subtiles.

Dans cette partie, nous aimerions montrer en quoi l'introduction de réseaux à l'intérieur des (φ, τ)-modules permet d'apporter des éléments de réponse au problème précédent. Nous commençons par introduire la notion de réseau dans les φ-modules étales dans le §2.1, puis montrons dans le §2.2 comment celle-ci peut être utilisée pour établir des bornes explicites portant sur la ramification des représentations galoisiennes. Forts de ces résultats préliminaires, nous en arrivons ensuite, dans le §2.3, au cœur de notre problème en introduisant la notion de (φ, τ)-réseau puis en démontrant le théorème 2.25 qui donne des contraintes fortes sur la forme des éléments de $\mathcal{E}_\tau^{\text{int}}$ — et notamment de leur représentation sous forme de séries — qui interviennent dans l'expression de l'automorphisme τ (par exemple sous forme matricielle dans le cas d'un module libre).

2.1 Réseaux dans les φ-modules étales

2.1.1 Définitions et rappels

Comme dans [13], on pose $\mathfrak{S} = W[[u]]$. Cet anneau se plonge naturellement dans $\mathcal{E}^{\text{int}}$ et dans $W(R)$ en envoyant comme d'habitude u sur le représentant de Teichmüller de $\underline{\pi}$. En particulier, $\mathfrak{S}$ apparaît comme un sous-anneau de l'intersection $\mathcal{E}^{\text{int}} \cap W(R)$, et on démontre en fait facilement qu'il s'identifie à cette intersection. Il est clair par ailleurs que le Frobenius (agissant sur $W(L)$ par exemple) stabilise $\mathfrak{S}$, et que ce dernier anneau est également stable par l'action de G_∞.

Définition 2.1. Soit M un φ-module étale défini sur $\mathcal{E}^{\text{int}}$. Un *φ-réseau* dans M est la donnée d'un sous-$\mathfrak{S}$-module de type fini $\mathfrak{M}$ de M qui est stable par φ et qui est tel que $\mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M} = M$.

4. Le même lemme assure également que la condition $\varphi(\mathfrak{t}) = c^{-1}E(u)\mathfrak{t}$ détermine $\mathfrak{t}$ à multiplication près par un élément inversible de $\mathbb{Z}_p$.

Remarque 2.2. Dans le cas où M est un module libre sur $\mathcal{E}^{\text{int}}$, on se restreindra souvent aux φ-réseaux qui sont eux-même libres (de type fini et même rang) sur $\mathfrak{S}$. Ce n'est en fait pas une véritable restriction car il suit du théorème de structure des modules sur $\mathfrak{S}$ (voir, par exemple, théorème 3.1, chap. 5 de [15] pour un énoncé de ce théorème) que si $\mathfrak{M}$ est un φ-réseau quelconque dans M, alors $(\mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}) \cap \mathfrak{M}[1/p]$ est un φ-réseau libre.

Voici une autre définition importante qui est essentiellement dûe à Fontaine et qui, en un certain sens, mesure la complexité d'un réseau.

Définition 2.3. Soit $\mathfrak{M}$ un φ-réseau à l'intérieur d'un φ-module étale sur $\mathcal{E}^{\text{int}}$. Soit encore U un élément de $W(R)$ et h un nombre entier positif ou nul.

On dit que $\mathfrak{M}$ est de *hauteur* divisant U (resp. de U-hauteur $\leqslant h$ pour un certain entier h) si le conoyau de l'application $\text{id} \otimes \varphi : W(R) \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to W(R) \otimes_{\mathfrak{S}} \mathfrak{M}$ est annulé par U (resp. U^h) [5].

Finalement, on dit que $\mathfrak{M}$ est de U-hauteur finie s'il est de U-hauteur $\leqslant h$ pour un certain entier h.

Remarque 2.4. La définition précédente de la hauteur a, en réalité, surtout un intérêt lorsque $U \in \mathfrak{S}$, auquel cas on peut se contenter de vérifier que le conoyau de $\text{id} \otimes \varphi : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$ est annulé par U (sans aller jusqu'à étendre les scalaires à $W(R)$). Toutefois, lorsque, dans la suite, nous manipulerons les (φ, τ)-réseaux, nous aurons besoin à plusieurs reprises de considérer des $U \notin \mathfrak{S}$, et c'est pourquoi nous avons préféré donner directement la définition générale précédente.

Dans le cas des φ-modules de p-torsion, on a le lemme suivant qui dénote un comportement exemplaire des réseaux.

Lemme 2.5. *Tout φ-module étale sur $\mathcal{E}^{\text{int}}$ annulé par une puissance de p admet un φ-réseau.*

Tout φ-réseau dans un φ-module étale sur $\mathcal{E}^{\text{int}}$ qui est annulé par une puissance de p est de u-hauteur finie.

Démonstration. La première assertion résulte de la remarque suivante qui suit directement de la définition de $\mathcal{E}^{\text{int}}$: si $\mathfrak{M}$ est un réseau quelconque dans un φ-module étale sur $\mathcal{E}^{\text{int}}$ annulé par une puissance de p, alors il existe un entier n tel que $u^n \mathfrak{M}$ soit stable par φ.

La seconde assertion, quant à elle, peut se voir comme une conséquence du théorème de classification des modules sur $\mathfrak{S} = W[[u]]$. En effet, étant donné un (φ, τ)-réseau $\mathfrak{M}$ comme dans la définition, le théorème en question assure que le conoyau de $\text{id} \otimes \varphi : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$ est de longueur finie comme $\mathfrak{S}$-module. Il suffit alors pour conclure de remarquer que u n'est pas inversible dans $\mathfrak{S}$. $\square$

Les résultats du lemme précédent ne s'étendent pas au cas des φ-modules libres sur $\mathcal{E}^{\text{int}}$. Dans le §2.1.2 ci-après, nous examinerons l'équivalent de la première partie du lemme. En ce qui concerne la deuxième partie du lemme, nous attirons l'attention du lecteur sur le fait trivial suivant : tout φ-réseau vivant dans un φ-module étale libre est de hauteur divisant U pour un certain $U \in \mathfrak{S}$ (il suffit de prendre pour U le déterminant de φ agissant sur le réseau). Par contre, il n'est pas vrai que U peut toujours être choisi de la forme u^n pour un certain entier n.

2.1.2 Un critère pour l'existence de φ-réseaux

Soit M un φ-réseau étale libre sur $\mathcal{E}^{\text{int}}$. Soit T la $\mathbb{Z}_p$-représentation de G_∞ qui lui correspond. Les données T et M sont alors liées par la formule $M = \text{Hom}_{\mathbb{Z}_p[G_\infty]}(T, \mathcal{E}^{\text{int,ur}})$. Une structure entière naturelle à l'intérieur de M (et donc un candidat potentiel pour être un réseau) est l'espace $\mathfrak{M} = \text{Hom}_{\mathbb{Z}_p[G_\infty]}(T, \mathfrak{S}^{\text{ur}})$ où $\mathfrak{S}^{\text{ur}} = W(R) \cap \mathcal{E}^{\text{int,ur}}$.

Proposition 2.6. *En reprenant les notations précédentes, les conditions suivantes sont équivalentes :*

1. *le sous-module $\mathfrak{M}$ de M est un φ-réseau ;*
2. *le φ-module M admet un φ-réseau qui est libre sur $\mathfrak{S}$;*
3. *le φ-module M admet un φ-réseau.*

5. On notera en particulier que les locutions « de U-hauteur $\leqslant 1$ » et « de hauteur divisant U » sont synonymes.

Démonstration. Le lemme 2.1.10 de [13] montre que la première condition implique la deuxième. Comme cette dernière implique clairement la troisième, il suffit de montrer que la troisième condition implique la première. Soit $\mathfrak{M}'$ un φ-réseau dans M (qui existe, par hypothèse). La première étape consiste à démontrer que $\mathfrak{M}'$ est inclus dans $\mathfrak{M}$. On considère les éléments de $\mathfrak{M}'$ comme des morphismes $\mathbb{Z}_p$-linéaires et G_∞-équivariants de T dans $\mathcal{E}^{\text{int,ur}}$. Soit X le sous-$\mathfrak{S}$-module de $\mathcal{E}^{\text{int,ur}}$ engendré par les images des éléments de $\mathfrak{M}'$. Il est stable par φ (puisque $\mathfrak{M}'$ l'est) et de type fini sur $\mathfrak{S}$ (puisque $\mathfrak{M}'$ l'est). On en déduit qu'il est inclus dans $W(R)$, ce qui est bien ce que l'on avait annoncé. La conclusion s'obtient maintenant facilement. En effet, de l'inclusion $\mathfrak{M}' \subset \mathfrak{M}$, on déduit que $\mathcal{E}^{\text{int,ur}} \otimes_{\mathfrak{S}} \mathfrak{M}$ contient $\mathcal{E}^{\text{int,ur}} \otimes_{\mathfrak{S}} \mathfrak{M}' = M$ et, par suite, que $\mathfrak{M}$ est un φ-réseau de M. $\square$

La proposition précédente permet en particulier de montrer que certaines représentations T correspondent à des φ-modules n'admettant pas de φ-réseau. C'est par exemple le cas de la représentation $\mathbb{Z}_p(-1)$, comme nous nous proposons de le vérifier pour conclure ce numéro. Soit w un générateur de $\mathbb{Z}_p(-1)$. D'après le deuxième exemple traité dans le §1.3.3, le φ-module associé M est engendré par la fonction $f : \mathbb{Z}_p(-1) \to \mathcal{E}^{\text{int,ur}}$, $w \mapsto V^{-1}$ où V vérifie l'équation $\varphi(V) = c^{-1}E(u)V$ et où, dans cette dernière égalité, $E(u)$ désigne le polynôme minimal de l'uniformisante π et $c = \frac{E(0)}{p} \in \mathbb{Z}_p^\times$. D'après la proposition 2.6, pour montrer que M n'admet pas de φ-réseau, il suffit de montrer qu'aucun élément non nul de M ne prend ses valeurs dans $W(R)$. Autrement dit, il suffit de montrer que $\mathcal{E}^{\text{int}} \cap VW(R)$ est réduit à 0.

On pose $\mathfrak{S}' = \mathcal{E}^{\text{int}} \cap VW(R)$. De $VW(R) \subset W(R)$, on déduit facilement que $\mathfrak{S}' \subset \mathfrak{S}$. Il est clair par ailleurs que cette inclusion induit un morphisme injectif $\mathfrak{S}'/p\mathfrak{S}' \to \mathfrak{S}/p\mathfrak{S} = k[[u]]$. On en déduit que $\mathfrak{S}'/p\mathfrak{S}'$ est un $k[[u]]$-module libre de rang $\leqslant 1$, et donc que $\mathfrak{S}'$ est un $\mathfrak{S}$-module libre de rang $\leqslant 1$. Soit a un élément de $\mathfrak{S}$, éventuellement nul, qui engendre $\mathfrak{S}'$. D'après une variante du théorème de préparation de Weierstrass (voir, par exemple, théorème 2.1, chap. 5 de [15]), on peut supposer que a est un polynôme ; on le note à partir de maintenant $A(u)$. Soit A^σ le polynôme obtenu à partir de A en appliquant le Frobenius σ à chacun de ses coefficients. On a $\varphi(A(u)) = A^\sigma(u^p)$. D'autre part, on vérifie que le quotient $\frac{\varphi(A(u))}{E(u)}$ appartient encore à $\mathfrak{S}'$. Il en résulte que $A(u)E(u)$ divise $A^\sigma(u^p)$ dans $\mathfrak{S}$. Les éléments de $\mathfrak{S}$ définissant des séries convergentes sur le disque de centre 0 et de rayon 1, la divisibilité trouvée implique que le polynôme A^σ s'annule en π^p. Par la théorie des polygones de Newton, il en résulte que A s'annule en un élément de valuation p, à partir de quoi on trouve que A^σ admet une racine de valuation p^2. Par récurrence, on démontre que A^σ admet une racine de valuation p^n pour tout entier n. Ceci n'est évidemment possible que si $A(u)$ est le polynôme nul, c'est-à-dire si $\mathfrak{S}' = 0$. On a donc finalement bien demontré ce que l'on souhaitait.

2.1.3 Calcul de la représentation galoisienne associée

On fixe un φ-module M sur $\mathcal{E}^{\text{int}}$, ainsi qu'un φ-réseau $\mathfrak{M}$ à l'intérieur de M. On suppose que l'on est dans l'alternative suivante : soit M est annulé par p^n pour un certain n, soit M est libre comme module sur $\mathcal{E}^{\text{int}}$. Dans le deuxième cas, on pose $n = \infty$, et on convient que $W_\infty(R) = W(R)$. Soit $\mathcal{T}(M)$ la représentation galoisienne associée à M. Dans ce paragraphe, nous donnons plusieurs formules permettant de calculer $\mathcal{T}(M)$ directement à partir de $\mathfrak{M}$. La plus simple consiste évidemment à commencer par retrouver M en étendant les scalaires à $\mathcal{E}^{\text{int}}$, ce qui conduit à l'expression suivante :

$$\mathcal{T}(M) = \mathrm{Hom}_{\mathcal{E}^{\text{int}},\varphi}(\mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}, \mathcal{E}^{\text{int,ur}}/p^n\mathcal{E}^{\text{int,ur}}).$$

Toutefois, on aimerait justement éviter cette solution, car l'un des intérêts d'utiliser des réseaux est bien sûr de travailler avec $\mathfrak{S}$ à la place de $\mathcal{E}^{\text{int}}$. La proposition B.1.8.3 de [11] permet de faire cela. Elle implique par exemple que :

$$\mathcal{T}(M) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R) \cap \mathcal{E}^{\text{int,ur}}/p^n\mathcal{E}^{\text{int,ur}}) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)). \tag{2.1}$$

Cette formule implique en particulier que tout morphisme de $\mathfrak{M}$ dans $W_n(R)$ qui est compatible à φ prend nécessairement ses valeurs dans $\mathcal{E}^{\text{int,ur}}/p^n\mathcal{E}^{\text{int,ur}}$ (ce que l'on peut démontrer directement sans difficulté).

En s'inspirant de [7], on peut enfin donner une troisième description de $\mathcal{T}(M)$ qui fait intervenir non pas $W_n(R)$, mais plutôt certains de ces quotients. Cette idée, qui pourrait sembler inutilement complexe à première vue, va en fait s'avérer très fructueuse tout au long de ce chapitre (comme elle l'a déjà d'ailleurs été dans [7]) : elle sera la clé pour obtenir des bornes sur la ramification dans le §2.2, mais aussi dans le §2.3.3 lorsque l'on s'évertuera à établir des congruences afin de préciser la forme de l'opérateur τ. *On se donne à partir de maintenant un élément $U \in W(R)$ qui n'est pas multiple de p et on suppose que $\mathfrak{M}$ est de hauteur divisant U.*

Lemme 2.7. *Il existe un élément $V \in W(R)$ qui n'est pas multiple de p et qui vérifie $\varphi(V) = UV$.*

Démonstration. On construit V par approximations successives : par récurrence, on construit une suite $(V_n)_{n \geqslant 1}$ d'éléments de $W(R)$ telle que $V_{n+1} \equiv V_n \pmod{p^n}$ et $\varphi(V_n) = UV_n$ pour tout n. Pour construire V_1, il suffit d'extraire une racine $(p-1)$-ième de U dans R, ce qui est possible puisque $\mathrm{Frac}\, R$ est algébriquement clos et que R est intégralement clos. Si maintenant V_n est construit, on cherche V_{n+1} sous la forme $V_n + p^n X$ avec $X \in W(R)$. La condition que doit vérifier X s'écrit :

$$\varphi(X) - UX \equiv \frac{UV_n - \varphi(V_n)}{p^n} \pmod{p}.$$

Si x et a désignent respectivement la réduction de X et $\frac{UV_n - \varphi V_n}{p^n}$ modulo p, trouver X revient à résoudre l'équation $x^p - Ux = a$ dans R. Or, par le même argument que précédemment, cette équation a bien une solution dans R, et la récurrence se termine ainsi. Enfin $V = \lim_{n \to \infty} V_n$ existe et vérifie $\varphi(V) = UV$. $\square$

Remarque 2.8. Il est évident que si V vérifie $\varphi(V) = UV$ et si $a \in \mathbb{Z}_p$, alors aV vérifie la même équation. Un examen de la preuve précédente montre que ce sont les seuls. Autrement dit, l'ensemble des solutions de l'équation $\varphi(V) = UV$ est un $\mathbb{Z}_p$-module libre de rang 1. On notera en particulier que l'idéal engendré par V est uniquement déterminé en fonction de U.

Soit $\mathfrak{m}_{W_n(R)}$ l'idéal maximal de l'anneau local $W_n(R)$: il est formé des éléments $x \in W_n(R)$ tels que $v_R(x \bmod p) > 0$. Pour tout élément $X \in W(R)$, on pose

$$\mathcal{T}_X(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)/(X \mathfrak{m}_{W_n(R)})).$$

La réduction modulo $X\mathfrak{m}_{W_n(R)}$ définit des morphismes canoniques $\rho_X : \mathcal{T}(M) \to \mathcal{T}_X(\mathfrak{M})$ et $\rho_{Y,X} : \mathcal{T}_Y(\mathfrak{M}) \to \mathcal{T}_X(\mathfrak{M})$ pour tout $Y \in W(R)$ multiple de X. En particulier, on a le diagramme suivant :

$$\begin{tikzcd} & \mathcal{T}(M) \arrow[dl, "\rho_{UV}"'] \arrow[dr, "\rho_V"] & \\ \mathcal{T}_{UV}(\mathfrak{M}) \arrow[rr, "\rho_{UV,V}"] & & \mathcal{T}_V(\mathfrak{M}) \end{tikzcd}$$

qui est manifestement commutatif.

Proposition 2.9. *Le morphisme ρ_V est injectif, et son image s'identifie dans $\mathcal{T}_V(M)$ à l'image de $\rho_{UV,V}$*

Démonstration. On démontre d'abord l'injectivité. Soient f et g deux éléments de $\mathcal{T}(M)$ tels que $f \equiv g \pmod{V\mathfrak{m}_{W_n(R)}}$. En utilisant que $\mathfrak{M}$ est de type fini et que tout élément de $\mathfrak{m}_{W_n(R)}$ s'écrit sous la forme $\sum_{n \geqslant 0} p^n [x_n]$ pour des $x_n \in \mathfrak{m}_R$, on montre qu'il existe une suite d'éléments λ_n de $\mathfrak{m}_R$ telle que la congruence $f \equiv g$ ait lieu modulo VI où I est l'idéal engendré par les éléments $p^n[\lambda_n]$. On a alors $\bigcap_{n \geqslant 0} \varphi^n(I) = 0$ et, comme $\varphi(\lambda_n)$ est multiple de λ_n dans R pour tout n, on a aussi l'inclusion $\varphi(I) \subset I$. Pour tout entier n, on pose $I_n = V\varphi^n(I)$ et on note f_n (resp. g_n) la réduction de f (resp. de g) modulo I_n. On va montrer, par récurrence, que $f_n = g_n$ pour tout entier n. Puisque $\bigcap_{n \geqslant 0} I_n = 0$, il en résultera que $f = g$, et donc l'injectivité souhaitée. L'égalité $f_0 = g_0$ ayant déjà été justifiée, il suffit de traiter l'hérédité. Soit $\psi : \mathfrak{M} \to \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$, $x \mapsto (\mathrm{id} \otimes \varphi)^{-1}(Ux)$. Le morphisme f induit alors une application linéaire :

$$\mathrm{id} \otimes f_n : \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \to \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \frac{W(R)}{I_n W(R)} = \frac{\mathfrak{S} \otimes_{\mathfrak{S},\varphi} W(R)}{\varphi(I_n) W(R)} = \frac{\mathfrak{S} \otimes_{\varphi,\mathfrak{S}} W(R)}{U I_{n+1} W(R)}.$$

Le fait que f commute à φ implique la commutativité du diagramme suivant :

$$\begin{tikzcd} \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \arrow[d, "\mathrm{id} \otimes f_n"] & \mathfrak{M} \arrow[l, "\psi"'] \arrow[r, "x \mapsto Ux"] & \mathfrak{M} \arrow[d, "f \bmod UI_{n+1}"] \\ \frac{\mathfrak{S} \otimes_{\varphi,\mathfrak{S}} W(R)}{UI_{n+1}W(R)} \arrow[rr, "\mathrm{id} \otimes \varphi"] & & \frac{W(R)}{UI_{n+1}W(R)} \end{tikzcd} \tag{2.2}$$

Comme on a bien sûr un diagramme analogue pour g, on déduit que l'égalité $f_n = g_n$ implique

$$U \cdot (f \bmod UI_{n+1}) = U \cdot (g \bmod UI_{n+1})$$

et donc finalement $f_{n+1} = g_{n+1}$.

On en vient maintenant à la preuve de la propriété concernant les images. Soit f_{UV} un élément de $\mathcal{T}_{UV}(\mathfrak{M})$. Il s'agit de démontrer que $\rho_{UV,V}(f_{UV})$ qui est une application de $\mathfrak{M}$ dans $W(R)/V\mathfrak{m}_{W(R)}$ compatible au Frobenius se relève en un morphisme $\mathfrak{M} \to W(R)$ encore compatible au Frobenius. Étant donné que $\mathfrak{M}$ est de type fini, il existe un idéal I comme précédemment tel que f_{UV} se relève en un morphisme $f_{UVI} : \mathfrak{M} \to W(R)/UVI$. On pose $f_0 = f_{UVI} \bmod I_0$. On va construire par récurrence sur n, une suite d'applications $f_n : \mathfrak{M} \to W(R)/I_n W(R)$ telle que $f_{n+1} \equiv f_n \pmod{I_n}$ pour tout n. Le diagramme (2.2) assure que, si l'on pose

$$\alpha_n = (\mathrm{id} \otimes \varphi) \circ (\mathrm{id} \otimes f_n) \circ \psi : \mathfrak{M} \to W(R)/UI_{n+1}$$

un bon candidat pour f_{n+1} est $\frac{\alpha_n}{U}$. Mais pour pouvoir le définir ainsi, il faut montrer au préalable que U divise α_n. Or, ce dernier fait est vrai et suit des deux remarques suivantes : *primo*, du fait que f_0 se rélève modulo UVI (le relève étant donné par f_{UVI}), on déduit U (et même en fait UV) divise α_0, et *secundo*, du fait que $f_n \equiv f_0 \pmod{V}$, on déduit que $\alpha_n \equiv \alpha_0 \pmod{UV}$. On peut donc bien considérer l'application $\frac{\alpha_n}{U}$ qui est défini sur $\mathfrak{M}$ mais, à cause de la division par U, prend ses valeurs dans $W(R)/I_{n+1}$ (et pas $W(R)/UI_{n+1}$ comme c'était le cas pour α_n). Enfin, de la congruence $f_{n-1} \equiv f_n \pmod{I_{n-1}}$, on déduit $\alpha_{n-1} \equiv \alpha_n \pmod{\varphi(I_{n-1})}$, puis $f_n \equiv f_{n+1} \pmod{I_n}$ étant donné que $\varphi(I_{n-1}) = UI_n$. Enfin, en passant à la limite, on obtient une application $f : \mathfrak{M} \to W(R)$ qui relève f_0 et qui commute à φ. □

Il suit de la proposition précédente que $\mathcal{T}(M)$ s'identifie à l'image de $\rho_{UV,V}$ et donc, comme nous l'avions annoncé, nous avons bien obtenu une description de cette représentation galoisienne qui ne fait pas intervenir $W_n(R)$ lui-même mais seulement deux de ces quotients.

Remarque 2.10. Une adaptation simple de la démonstration de la proposition 2.9 montre que, si $\mathfrak{M}$ et $\mathfrak{M}'$ sont deux φ-réseaux, on a l'égalité :

$$\mathrm{Hom}_\varphi(\mathfrak{M}, \mathfrak{M}') = \mathrm{image}\big(\mathrm{Hom}_\varphi(\mathfrak{M}/UV\mathfrak{M}, \mathfrak{M}'/UV\mathfrak{M}') \to \mathrm{Hom}_\varphi(\mathfrak{M}/V\mathfrak{M}, \mathfrak{M}'/V\mathfrak{M}')\big) \tag{2.3}$$

où, dans un abus de notation, on a noté $UV\mathfrak{M}$ au lieu $\mathfrak{M} \cap (UVW(R) \otimes_{\mathfrak{S}} \mathfrak{M})$ (le problème étant que UV n'appartient pas *a priori* à $\mathfrak{S}$) et de même pour $UV\mathfrak{M}'$, $V\mathfrak{M}$ et $V\mathfrak{M}'$. On en déduit que la réduction modulo V (resp. modulo UV) définit un foncteur fidèle (resp. pleinement fidèle) de la catégorie des φ-réseaux dans un φ-module étale sur $\mathcal{E}^{\mathrm{int}}$ dans la catégorie dont les objets sont les $(\mathfrak{S}/V\mathfrak{S})$-modules (resp. les $(\mathfrak{S}/UV\mathfrak{S})$-modules) de type fini munis d'un endomorphisme semi-linéaire φ et dont les morphismes sont les applications $\mathfrak{S}$-linéaires commutant à φ (resp. dont les morphismes sont donnés par la formule du membre de droite de (2.3)).

2.2 Bornes pour la ramification

Sans surprise, le but de ce numéro est de démontrer le théorème 2 de l'introduction. On commence par quelques brefs rappels au sujet des filtrations de ramification dans le §2.2.1. Les deux paragraphes suivants sont consacrés à la preuve du théorème, tandis que dans le §2.2.4, on établit une réciproque partielle.

2.2.1 Rappels sur les filtrations de ramification

Soit κ un corps complet pour une valuation discrète dont le corps résiduel est parfait de caractéristique p (dans les applications qui nous intéressent, on prendra $\kappa = K$ ou $\kappa = F_0 = k((u))$). Pour toute extension finie κ' de κ, on appelle $v_{\kappa'}$ la valuation sur κ' normalisée par $v_{\kappa'}(\kappa'^\star) = \mathbb{Z}$. Si κ' est une extension galoisienne finie de κ de groupe de Galois G, la *filtration de ramification en numérotation inférieure* de G est la filtration $(G_{(\lambda)})_{\lambda \in \mathbb{R}^+}$ définie comme suit :

$$G_{(\lambda)} = \big\{\, \sigma \in G \mid v_{\kappa'}(\sigma(x) - x) \geqslant \lambda, \, \forall x \in \mathcal{O}_{\kappa'} \,\big\}$$

où $\mathcal{O}_{\kappa'}$ est l'anneau des entiers de κ'. Les $G_{(\lambda)}$ sont des sous-groupes distingués de G, et la filtration qu'ils forment est décroissante, exhaustive et séparée. On introduit encore la fonction $\varphi_{\kappa'/\kappa} : \mathbb{R}^+ \to \mathbb{R}^+$ définie par :

$$\varphi_{\kappa'/\kappa}(\lambda) = \int_0^\lambda \frac{\mathrm{Card}\, G_{(t)}}{\mathrm{Card}\, G_{(1)}} dt.$$

C'est une fonction affine par morceaux, concave et bijective, dont on note $\psi_{\kappa'/\kappa}$ l'inverse. La *filtration de ramification en numérotation supérieure* est définie par l'égalité $G^{(\mu)} = G_{(\psi_{\kappa'/\kappa}(\mu))}$ pour tout réel $\mu \geqslant 0$. On renvoie à [21], chap. IV pour les propriétés usuelles la concernant, et en particulier le théorème d'Herbrand. La filtration de ramification en numérotation supérieure s'étend à une extension galoisienne κ'/κ non nécessairement finie en posant :

$$\mathrm{Gal}(\kappa'/\kappa)_{(\mu)} = \varprojlim_{\kappa''} \mathrm{Gal}(\kappa''/\kappa)_{(\mu)}$$

où la limite projective est prise sur toutes les extensions finies galoisiennes κ'' de κ incluses dans κ'. Dans le cas où κ'/κ est une extension algébrique séparable non galoisienne, on ne peut certes pas définir de filtration sur le groupe de Galois puisque celui-ci n'existe pas mais les fonctions $\varphi_{\kappa'/\kappa}$ et $\psi_{\kappa'/\kappa}$, elles, ont encore un sens ; on peut les définir, par exemple, grâce aux formules :

$$\psi_{\kappa'/\kappa}(\mu) = \int_0^\mu [I_\kappa : I_{\kappa'} G_\kappa^{(t)}] dt \quad \text{et} \quad \varphi_{\kappa'/\kappa} = \psi_{\kappa'/\kappa}^{-1}$$

où I_κ et $I_{\kappa'}$ sont respectivement les sous-groupes d'inertie des groupes de Galois absolus de κ et κ' (voir [23], §1.2.1). La théorie qui vient d'être rappelée brièvement s'applique en particulier aux corps $\kappa = K$ et $\kappa = F_0$. Les groupes de Galois absolus G_K et $\mathrm{Gal}(F_0^{\mathrm{sep}}/F_0) \simeq G_\infty$ héritent ainsi d'une filtration de ramification en numération supérieure.

2.2.2 Bornes pour les représentations de G_∞

On démontre dans ce paragraphe l'assertion 1 du théorème 2. Soient M un φ-module M sur $\mathcal{E}^{\mathrm{int}}$ annulé par p^n, et $\mathfrak{M}$ un φ-réseau de M de hauteur divisant U, pour un élément $U \in \mathfrak{S}$ qui n'est pas multiple de p. Comme dans l'énoncé du théorème, on note T la représentation galoisienne associée à ces données et on pose $h = v_R(U \bmod p)$. Pour tout nombre réel $v \geqslant 0$ et tout anneau A muni d'une valuation (par exemple $A \subset R$), on note encore $\mathfrak{a}_A^{>v}$ l'idéal des éléments de A de valuation strictement plus grande que v. Enfin, si F est une extension algébrique de F_0, on désigne par $\mathcal{O}_F$ son anneau des entiers. Dans le cas où F est inclus dans F_0^{sep}, on a simplement $\mathcal{O}_F = F \cap R$.

Comme cela se fait usuellement dans ce genre de situations, on va utiliser la propriété (P_m) de Fontaine (introduite dans [10], proposition 1.5). Rappelons qu'ici m est un nombre réel positif ou nul et que, par définition, une extension F de F_0 vérifie (P_m) si, et seulement si pour toute extension algébrique E de F_0, s'il existe un morphisme de $\mathcal{O}_{F_0}$-algèbres $\mathcal{O}_F \to \mathcal{O}_E/\mathfrak{a}_E^{>m}$, alors il existe un F_0-plongement de F dans E. Le lien avec la filtration de ramification en numérotation supérieure est donnée par la proposition suivante qui, dans cette formulation, est dûe à Yoshida (voir [24]).

Proposition 2.11. *Soit F une extension finie galoisienne de F_0 de groupe de Galois G. On définit :*
- *l'entier m_0 comme la borne inférieure des réels m tels que (P_m) soit satisfaite, et*
- *l'entier μ_0 comme la borne inférieure des réels μ tel que $G^{(\mu)} = \{\mathrm{id}_F\}$.*

Alors $m_0 = \mu_0$.

Notons $\rho : G_\infty \to \mathrm{GL}(T)$ le morphisme donnant l'action de G_∞ sur T, et F l'extension finie galoisienne de F_0 qui est en correspondance avec le sous-groupe distingué $\ker \rho$ de G_∞. D'après la proposition précédente, pour démontrer la première assertion du théorème 2, il suffit de prouver que l'extension F vérifie la propriété (P_m) pour $m = \frac{hp^n}{p-1}$.

Lemme 2.12. *Soit E une extension de F_0 incluse dans F_0^{sep}. Alors l'application injective naturelle*

$$\mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(\mathcal{O}_E)) \to \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)) = T$$

(déduite de l'inclusion $W_n(\mathcal{O}_E) \to W_n(R)$) est un isomorphisme si, et seulement si E contient F.

Démonstration. Il est clair que si l'application du lemme est un isomorphisme, alors le groupe de Galois absolu de E agit trivialement sur T. D'où $F \subset E$. Pour la réciproque, on remarque qu'en vertu de l'égalité (2.1), on sait que tous les morphismes $f : \mathfrak{M} \to W_n(R)$ compatibles à φ prennent leurs valeurs dans $\mathcal{E}^{\mathrm{int,ur}}$ et donc, en particulier, dans $W_n(\mathcal{O}_{F_0^{\mathrm{sep}}})$. Par ailleurs, par définition de F, son groupe de Galois absolu G_F agit trivialement sur T, ce qui implique que tous les morphismes f comme précédemment prennent leurs valeurs dans $W_n(\mathcal{O}_{F_0^{\mathrm{sep}}})^{G_F} = W_n(\mathcal{O}_F)$. Il en résulte que, si $F \subset E$, l'application du lemme est bien bijective. □

Pour tout réel $v \geqslant 0$, on introduit à présent le sous-ensemble $W_n(\mathfrak{a}_R^{\geqslant v})$ de $W_n(R)$ formé des éléments dont toutes les coordonnées sont dans $\mathfrak{a}_R^{\geqslant v}$. C'est un idéal de $W_n(R)$, et le quotient de $W_n(R)/W_n(\mathfrak{a}_R^{\geqslant v})$ s'identifie à $W_n(R/\mathfrak{a}_R^{\geqslant v})$. D'après le lemme 2.7, il existe $V \in W(R)$, non multiple de p, tel que $\varphi(V) = UV$. on fixe un tel élément V ; il vérifie $V^{p-1} = U \pmod p$, ce qui implique que $v_R(V \bmod p) = \frac{h}{p-1}$.

Lemme 2.13. *On a* $W_n(\mathfrak{a}_R^{\geqslant m}) \subset UV\mathfrak{m}_{W_n(R)}$ *pour* $m = \frac{hp^n}{p-1}$.

Démonstration. On raisonne par récurrence sur n et donc, pour éviter les confusions, on notera $m(n)$ à la place de m tout au long de la démonstration. Pour $n = 1$, on remarque que $v_R(UV \bmod p) = m(1)$ et donc que les deux idéaux considérés sont égaux. On suppose à présent que l'inclusion $W_n(\mathfrak{a}_R^{\geqslant m(n)}) \subset UV\mathfrak{m}_{W_n(R)}$ est satisfaite et on considère un élément $X = (x_1, \ldots, x_{n+1}) \in W_{n+1}(\mathfrak{a}_R^{\geqslant m(n+1)})$. On veut montrer que $X \in UV\mathfrak{m}_{W_{n+1}(R)}$. Soient $\lambda \in R$ un élément quelconque de valuation hp et $[\lambda] \in W(R)$ son représentant de Teichmüller. Un calcul immédiat sur les valuations montre que les composantes du vecteur de Witt de longueur n suivant :

$$\frac{1}{[\lambda]}(x_1, \ldots, x_n) = \Big(\frac{x_1}{\lambda}, \frac{x_2}{\lambda^p}, \ldots, \frac{x_n}{\lambda^{p^{n-1}}}\Big)$$

sont toutes dans $\mathfrak{a}_R^{\geqslant m(n)}$. L'hypothèse de récurrence s'applique donc et assure qu'il existe $Y \in \mathfrak{m}_{W_n(R)}$ tel que $\frac{1}{[\lambda]}(x_1, \ldots, x_n) = UVY$. On note encore Y un élément de $\mathfrak{m}_{W_{n+1}(R)}$ qui relève Y et on pose

$$\Delta = (x_1, \ldots, x_n, x_{n+1}) - [\lambda]UVY.$$

Les n premières coordonnées de Δ sont nulles, tandis que, si on pose $[\lambda]UVY = (z_1, \ldots, z_{n+1})$, la dernière coordonnée de Δ s'exprime comme un polynôme homogène de degré p^n en les $x_1, \ldots, x_{n+1}, z_1, \ldots, z_{n+1}$, à condition de donner le poids p^{i-1} aux variables x_i et z_i. Comme, en outre, z_i est divisible par λ^{p^i}, on en déduit que la dernière coordonnée de Δ est de valuation strictement supérieure à $m(n+1)$. Ainsi, Δ appartient à $p^n UV\mathfrak{m}_{W_{n+1}(R)}$ et donc *a fortiori* de $UV \cdot \mathfrak{m}_{W_{n+1}(R)}$. Il s'ensuit enfin que $X \in UV \cdot \mathfrak{m}_{W_{n+1}(R)}$ comme voulu. ☐

Nous sommes prêts à vérifier la propriété (P_m) pour le corps F et le nombre $m = \max(1, \frac{hp^n}{p-1})$. Soit E une extension algébrique de F_0 incluse dans F_0^{sep}. Soit également $f : \mathcal{O}_F \to \mathcal{O}_E/\mathfrak{a}_E^{\geqslant m}$ un morphisme de $\mathcal{O}_{F_0}$-algèbres. On considère la composée suivante :

$$\begin{aligned}\Psi_V :\quad T = \mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_F)) &\to \mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_F/\mathfrak{a}_F^{\geqslant m})) \to \mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_E/\mathfrak{a}_E^{\geqslant m}))\\ &\to \mathrm{Hom}\Big(\mathfrak{M}, \frac{W_n(\mathcal{O}_E)}{UV\mathfrak{m}_{W_n(R)} \cap W_n(\mathcal{O}_E)}\Big) \to \mathrm{Hom}\Big(\mathfrak{M}, \frac{W_n(\mathcal{O}_E)}{V\mathfrak{m}_{W_n(R)} \cap W_n(\mathcal{O}_E)}\Big)\end{aligned}$$

où la deuxième flèche est induite par f et l'existence de la troisième résulte du lemme 2.13. Une adaptation de la proposition 2.9 assure que, pour tout $\psi_F \in T$, il existe une unique application $\psi_E \in \mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_E))$ telle que $\Psi_V(\psi_F)$ s'identifie à $\psi_E \bmod V\mathfrak{m}_{W(R)} \cap W_n(\mathcal{O}_E)$. Ceci permet de construire un morphisme $\Psi : T \to \mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_E))$ relevant Ψ_V.

Lemme 2.14. *Le morphisme* Ψ *précédent est injectif.*

Démonstration. On raisonne par récurrence sur n. Pour $n = 1$, on considère u_F une uniformisante de F. Son polynôme minimal sur F_0 est un polynôme d'Eisenstein que l'on note P. L'élement $x = f(u_F) \in \mathcal{O}_E/\mathfrak{a}_E^{\geqslant m}$ est alors une racine de P. Comme $m \geqslant 1$, le coefficient constant de P ne s'annule pas dans $\mathcal{O}_E/\mathfrak{a}_E^{\geqslant m}$. On en déduit que x a la même valuation que u_F puis que f induit une application injective $f_{h/(p-1)} : \mathcal{O}_F/\mathfrak{a}_E^{>h/(p-1)} \to \mathcal{O}_E/\mathfrak{a}_E^{>h/(p-1)}$. Ainsi le morphisme

$$\mathrm{Hom}\big(\mathfrak{M}, \tfrac{\mathcal{O}_E}{V\mathfrak{m}_R \cap \mathcal{O}_E}\big) = \mathrm{Hom}(\mathfrak{M}, \mathcal{O}_E/\mathfrak{a}_E^{>h/(p-1)}) \to \mathrm{Hom}(\mathfrak{M}, \mathcal{O}_F/\mathfrak{a}_F^{>h/(p-1)}) = \mathrm{Hom}\big(\mathfrak{M}, \tfrac{\mathcal{O}_F}{V\mathfrak{m}_R \cap \mathcal{O}_F}\big)$$

est, lui aussi, injectif, ce qui permet de conclure.

Pour l'hérédité, on suppose que $\mathfrak{M}$ est annulé par p^{n+1} et on considère la suite exacte $0 \to p\mathfrak{M} \to \mathfrak{M} \to \mathfrak{M}/p\mathfrak{M} \to 0$. Les modules $p\mathfrak{M}$ et $\mathfrak{M}/p\mathfrak{M}$ sont encore des φ-réseaux à l'intérieur, respectivement de pM et M/pM. En outre, ils sont tous les deux de hauteur divisible par U. En effet, c'est évident pour $\mathfrak{M}/p\mathfrak{M}$ et, pour $p\mathfrak{M}$, on raisonne comme suit. On note tout d'abord que l'application $\mathrm{id} \otimes \varphi : W(R) \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}/p\mathfrak{M} \to W(R) \otimes_{\mathfrak{S}} \mathfrak{M}/p\mathfrak{M}$ est injective, ce qui implique que le morphisme suivant induit par l'inclusion naturelle de $p\mathfrak{M}$ dans $\mathfrak{M}$:

$$\mathrm{coker}\big(\mathrm{id} \otimes \varphi : W(R) \otimes_{\varphi,\mathfrak{S}} (p\mathfrak{M}) \to W(R) \otimes_{\mathfrak{S}} (p\mathfrak{M})\big) \longrightarrow \mathrm{coker}\big(W(R) \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \to W(R) \otimes_{\mathfrak{S}} \mathfrak{M}\big)$$

est, lui aussi, injectif. Comme l'espace d'arrivée est annulé par U, on en déduit qu'il en est de même de l'espace de départ, ce qui veut bien dire que $p\mathfrak{M}$ est de hauteur divisant U. On considère maintenant le diagramme suivant :

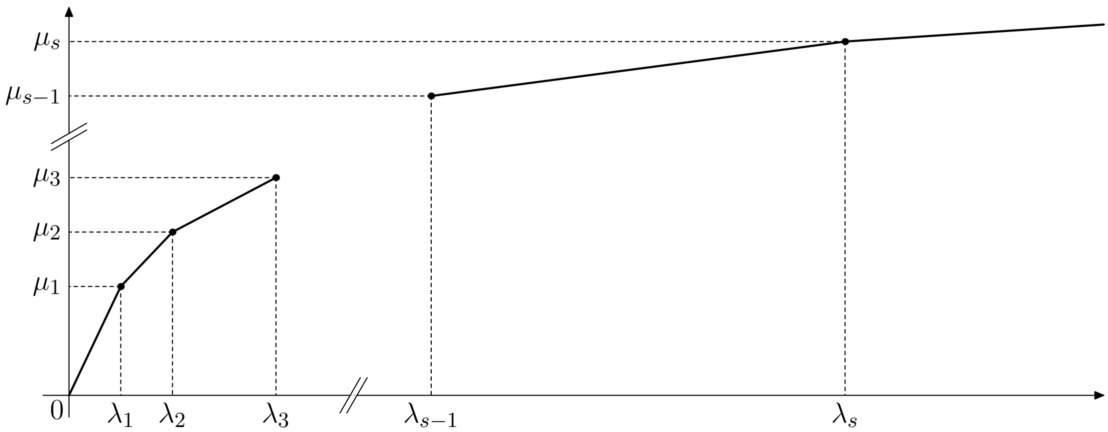
$$\begin{tikzcd}
0 \arrow[r] & \mathcal{T}(\mathfrak{M}/p\mathfrak{M}) \arrow[r] \arrow[d] & \mathcal{T}(\mathfrak{M}) \arrow[r] \arrow[d] & \mathcal{T}(p\mathfrak{M}) \arrow[r] \arrow[d] & 0 \\
 & \mathrm{Hom}(\mathfrak{M}/p\mathfrak{M}, \mathcal{O}_E) \arrow[d, hook] & \mathrm{Hom}(\mathfrak{M}, W_{n+1}(\mathcal{O}_E)) \arrow[d, hook] & \mathrm{Hom}(p\mathfrak{M}, W_n(\mathcal{O}_E)) \arrow[d, hook] & \\
0 \arrow[r] & \mathcal{T}(\mathfrak{M}/p\mathfrak{M}) \arrow[r] & \mathcal{T}(\mathfrak{M}) \arrow[r] & \mathcal{T}(p\mathfrak{M}) \arrow[r] & 0
\end{tikzcd}$$

où les flèches verticales du haut sont les morphismes Ψ correspondant respectivement à $\mathfrak{M}/p\mathfrak{M}$, $\mathfrak{M}$ et $p\mathfrak{M}$, et les flèches verticales du bas sont les inclusions canoniques. Par hypothèse de récurrence, on sait que les flèches verticales en haut à gauche et en haut à droite sont injectives. Un chasse au diagramme termine alors la récurrence. $\square$

Il est maintenant aisé de conclure. Du lemme 2.14, il découle que l'ensemble $\mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_E))$ a au moins autant d'éléments que T. L'inclusion naturelle $\mathrm{Hom}(\mathfrak{M}, W_n(\mathcal{O}_E)) \to T$ est donc nécessairement une bijection. Le lemme 2.12 assure que E contient F, ce qui est exactement ce qu'il fallait vérifier pour établir la propriété (P_m).

2.2.3 Bornes pour les représentations de G_K

Expliquons à présent comment la deuxième partie du théorème 2 se déduit de la première. on rappelle tout d'abord que la théorie du corps des normes ne se contente pas de fournir un isomorphisme canonique entre les groupes G_∞ et $G_{F_0} = \mathrm{Gal}(F_0^{\mathrm{sep}}/F_0)$, mais qu'elle compare aussi les filtrations de ramification en numérotation supérieure. Précisément, le corollaire 3.3.6 de [23] affirme que pour tout réel $\mu \geqslant 0$, les groupes $G_{F_0}^{(\mu)}$ et $G_\infty \cap G_K^{(\varphi_{K_\infty/K}(\mu))}$ se correspondent *via* l'isomorphisme du corps des normes. De surcroît, la fonction $\varphi_{K_\infty/K}$ a été calculée dans [7], §4.3. Voici sa représentation graphique :



où $\lambda_s = 1 + \frac{ep^s}{p-1}$ et $\mu_s = 1 + e(s + \frac{1}{p-1})$. Si l'on souhaite une formule explicite, on peut écrire pour tout $\lambda \geqslant \lambda_1$:

$$\varphi_{K_\infty/K}(\lambda) = 1 + es + e \cdot \left(\frac{p^{\{s\}}}{p-1} - \{s\} \right) \tag{2.4}$$

où $s = \log_p(\frac{(p-1)(\lambda-1)}{e}) \geqslant 1$ et où $\{s\}$ désigne sa partie décimale. On voit en particulier que pour sur l'intervalle $[\lambda_1, +\infty[$, la fonction $\varphi_{K_\infty/K}$ s'écrit comme la somme de la fonction $\lambda \mapsto e \cdot \log_p \lambda$ et d'une fonction bornée.

Rappelons qu'au début de l'introduction, nous avions défini l'extension $K(\zeta_{p^\infty})/K$ obtenue en ajoutant toutes les racines primitives p^n-ième de l'unité et que nous avions posé $\Gamma = \mathrm{Gal}(K(\zeta_{p^\infty})/K)$. Le caractère cyclotomique χ identifie Γ à un sous-groupe d'indice fini de $\mathbb{Z}_p^\times$. Ce groupe est, par ailleurs, muni de la filtration de ramification en numérotation supérieure, notée $(\Gamma^{(s)})_{s\geqslant 0}$ dans la suite.

Lemme 2.15. *Il existe une constante $c_0(K) \geqslant 0$ ne dépendant que de K telle que pour tout $\gamma \in \Gamma$, on ait $\gamma \in \Gamma^{(1+es-c_0(K))}$ où s est la valuation p-adique de $\chi(\gamma) - 1$.*

Démonstration. Le lemme est une conséquence directe d'un théorème très général de Sen (voir [22]). Nous donnons toutefois ci-dessous une autre démonstration, plus élémentaire. Si le corps K n'est pas absolument ramifiée, le lemme résulte d'un calcul classique que l'on peut trouver par exemple dans [21], chap. IV, §4 ; on peut alors même choisir $c_0(K) = 0$ (attention au décalage d'indice dans la numérotation des groupes de ramification entre notre convention et celle de *loc. cit.*).

Pour le cas général, on pose $K' = W[1/p]$ (c'est la sous-extension maximale non absolument ramifiée de K) et $\Gamma' = \mathrm{Gal}(K'(\zeta_{p^\infty})/K') \simeq \mathbb{Z}_p^\times$. Le groupe Γ apparaît naturellement comme un sous-groupe de Γ' et d'après le théorème d'Herbrand, on a l'égalité :

$$\Gamma^{(\mu)} = \Gamma \cap (\Gamma')^{(\varphi_{K'/K}(\mu))}.$$

Ainsi, en utilisant le cas déjà traité d'un corps de base non absolument ramifié, on obtient $\gamma \in \Gamma^{(\psi_{K'/K}(1+s))}$. Or à partir d'un certain moment, la fonction $\psi_{K'/K}$ est affine de pente e. On en déduit qu'il existe une constante $c_0(K) \geqslant 0$ telle que $\psi_{K'/K}(1 + s) \geqslant 1 + es - c_0(K)$. Le lemme s'ensuit. $\square$

Remarque 2.16. Dans le cas où l'extension K/K' est modérément ramifiée — c'est-à-dire dans le cas où e est premier avec p —, la fonction $\psi_{K'/K}$ vaut l'identité sur $[0, 1]$, et est tout de suite après affine de pente e. On en déduit que, dans ce cas, on peut prendre $c_0(K) = 0$, c'est-à-dire que $\gamma \in \Gamma^{(1+es)}$.

Étant donné que l'image de $\chi : \Gamma \to \mathbb{Z}_p^\times$ est d'indice finie dans $\mathbb{Z}_p^\times$, il existe un entier $s_0(K)$ — ne dépendant bien sûr que de K — tel que $1 + p^{s_0}\mathbb{Z}_p \subset \chi(\Gamma)$. Soit s un nombre entier vérifiant :

$$s \geqslant s_0(K) \quad \text{et} \quad s > \frac{c_0(K)}{e} + \max\left(\tfrac{1}{p-1}, n + \log_p(\tfrac{h}{e})\right). \tag{2.5}$$

D'après la première inégalité, il existe un élément $\gamma \in \Gamma$ tel que $v_p(\chi(\gamma) - 1) = s$. La deuxième inégalité, quant à elle, implique, grâce au lemme précédent, que $\gamma \in \Gamma^{(\mu_0)}$ avec $\mu_0 = 1 + e \cdot \max(\frac{1}{p-1}, n + \log_p(\frac{h}{e}))$. Par ailleurs, étant donné que les extensions K_∞/K et $K(\zeta_{p^\infty})/K$ sont linéairement disjointes, le groupe de Galois $\mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K_\infty)$ s'identifie canoniquement à Γ. *Via* cette identification, on a en outre l'égalité :

$$\mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K_\infty) \cap G_K^{(\mu)} = \Gamma^{(\mu)}$$

pour tout réel $\mu \geqslant 0$. On en déduit que $\gamma \in \Gamma$ se relève en un élement de G_K qui appartient à $G_\infty \cap G_K^{(\mu_0)} = G_\infty^{\psi_{K_\infty/K}(\mu_0)}$. Or, un calcul facile basée sur la formule (2.4) montre que $\psi_{K_\infty/K}(\mu_0) > \max(1, \frac{hp^n}{p-1})$. L'assertion 1 du théorème 2 implique alors que γ agit trivialement sur T. Si l'on choisit en outre τ dans $\mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K_\infty)$ (*i.e.* tel que $\chi(\tau) = 1$), on a l'égalité $\gamma\tau = \tau^{\chi(\gamma)}\gamma = \tau^{p^s+1}\gamma$, qui implique que τ^{p^s} agit, lui aussi, trivialement sur T.

Considérons maintenant un nombre réel $\mu > 1 + e(s + \frac{1}{p-1})$. On a $\mu > \mu_0$ et donc à nouveau $\psi_{K_\infty/K}(\mu) > \frac{hp^n}{p-1}$. En particulier $G_\infty \cap G_K^{(\mu)}$ agit trivialement sur T. Soit g un élément de $G_K^{(\mu)}$. En vertu de l'inégalité $\mu > 1 + e(s + \frac{1}{p-1})$ et de ce que l'on sait à propos de la ramification de l'extension K_∞/K, on a $g \in G_s$. D'après le lemme 1.2 et la discussion menée au §1.1.3, quitte à modifier encore un peu τ, on peut écrire g sous la forme $g = \tau^a g'$ pour un certain $g' \in G_\infty$. Du fait que g stabilise K_s, on déduit qu'il en est de même pour τ^a, et donc que p^s divise a. En particulier, on a $\tau^a \in G_K^{(\mu)}$, et donc $g' \in G_\infty \cap G_K^{(\mu)}$. Il s'ensuit que ce dernier élément agit trivialement sur T. Comme c'est aussi le cas de

τ^a, on en déduit finalement que g agit aussi trivialement sur T. Comme ceci est valable pour tout $g \in G_K^{(\mu)}$, tout $\mu > 1 + e(s + \frac{1}{p-1})$ et tout s vérifiant les inégalités (2.5), on a finalement démontré qu'en posant [6]

$$c(K) = 1 + \frac{e}{p-1} + e \cdot s_0(K) + c_0(K),$$

le sous-groupe $G_K^{(\mu)}$ agit trivialement sur T pour tout $\mu > c(K) + e \cdot \max(\frac{1}{p-1}, n + \log_p(\frac{h}{e}))$. Le théorème 2 est démontré.

Lorsque K est absolument modérément ramifiée, on a déjà vu, dans la remarque 2.16, que l'on pouvait prendre $c_0(K) = 0$. Par ailleurs, il est facile de voir que l'entier $s_0(K)$ peut être, dans ce cas, choisi égal à 1. La formule qui a été obtenue précédemment donne alors la valeur $1 + e + \frac{e}{p-1}$ pour $c(K)$. En réalité, un examen de la preuve précédente montre que, dès que $h \geqslant e$, on peut même prendre $c(K) = 1 + \frac{e}{p-1}$.

2.2.4 Une réciproque partielle au théorème 2

Le théorème 2 que nous venons de démontrer permet de contrôler la ramification d'une représentation de torsion de G_∞ ou G_K en fonction de la hauteur du φ-module associé. Dans le cas des objets annulées par p, il se trouve qu'être de hauteur divisant U (pour un élément $U \in \mathfrak{S}$) équivaut à être de u-hauteur $\leqslant h = v_R(U \bmod p)$. Ainsi, la ramification d'une $\mathbb{F}_p$-représentation est contrôlée par la u-hauteur du φ-module associé, qui est simplement un nombre entier : dans le cas des représentations de G_∞ par exemple, si cette u-hauteur est $\leqslant h$, alors le sous-groupe $G_\infty^{(\mu)}$ agit trivialement pour tout $\mu > \frac{hp}{p-1}$.

On peut alors se demander si, réciproquement, la ramification de la représentation contrôle la u-hauteur du φ-module associé. La proposition suivante apporte une réponse affirmative à cette question.

Proposition 2.17. *Soit T une $\mathbb{F}_p$-représentation de dimension finie de G_∞, et soit h un entier tel que $G_\infty^{(\mu)}$ agisse trivialement sur T pour tout $\mu > \frac{hp}{p-1}$. Alors le φ-module étale associé à T admet un φ-réseau de u-hauteur $\leqslant hp$.*

Soit T une $\mathbb{F}_p$-représentation de dimension finie de G_K, et soit h un entier strictement positif tel que $G_K^{(\mu)}$ agisse trivialement sur T pour tout $\mu > 1 + \frac{e}{p-1} + e \cdot (1 + \log_p(\frac{h}{e}))$. Alors le (φ, τ)-module associé à T admet un (φ, τ)-réseau de u-hauteur $\leqslant hp$.

Remarque 2.18. On prendra garde d'une part à ce que la borne portant sur μ ne fait pas intervenir la constante $c(K)$ comme c'était le cas dans le théorème 2 et d'autre part à ce que la borne que l'on obtient au final pour la u-hauteur est bien hp, et non pas h.

Démonstration. La deuxième partie de la proposition se déduit facilement de la première en utilisant les liens rappelés précédemment entre les filtrations de ramification sur G_∞ et G_K. Nous laissons cet exercice au lecteur et nous concentrons à partir de maintenant sur la preuve de la première affirmation.

Le φ-module étale associé à la représentation T est $M = \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, F_0^{\mathrm{sep}})$ et admet un φ-réseau canonique donné par $\mathfrak{M} = \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, \mathcal{O}_{F_0^{\mathrm{sep}}})$. Montrons que $\mathfrak{M}$ est de u-hauteur $\leqslant hp$. Étant donné notre hypothèse, il existe une extension galoisienne finie F sur F_0 telle que, d'une part, $\mathfrak{M} = \mathrm{Hom}_{\mathbb{F}_p[G_\infty]}(T, \mathcal{O}_F)$ et, d'autre part, le sous-groupe de ramification $\mathrm{Gal}(F/F_0)^{(\mu)}$ soit trivial pour tout $\mu > \frac{hp}{p-1}$. Le corps F est à l'évidence un F_0-espace vectoriel de dimension finie muni d'un opérateur de Frobenius, qui est tout simplement l'élévation à la puissance p : c'est donc un φ-module. Son anneau des entiers $\mathcal{O}_F$ définit en outre un φ-réseau à l'intérieur de F. Le lemme 3.2 de [16] implique que ce φ-réseau est de u-hauteur $\leqslant \lceil (p-1) v_R(\mathfrak{d}_{F/F_0}) \rceil$ où $\mathfrak{d}_{F/F_0}$ est la différente de l'extension F/F_0 et où $\lceil x \rceil$ désigne la partie entière supérieure du nombre réel x. De la proposition 1.3 de [10] et de la borne sur la ramification de F, il suit $v_R(\mathfrak{d}(F/F_0)) \leqslant \frac{hp}{p-1}$, d'où on déduit que le φ-réseau $\mathcal{O}_F$ est de u-hauteur $\leqslant hp$.

Reste à montrer comment cela implique que $\mathfrak{M}$ est, lui-même, de u-hauteur $\leqslant hp$. Soit f un élément de $\mathfrak{M}$; c'est un morphisme de T dans $\mathcal{O}_F$ compatible à l'action de Galois. On veut montrer que $u^{hp} f$ est dans l'image de $\mathrm{id} \otimes \varphi_{\mathfrak{M}} : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$. Or, l'application $u^{hp} f$ prend manifestement ses valeurs dans le sous-ensemble $u^{hp} \mathcal{O}_F$ qui est inclus dans l'image de $\mathrm{id} \otimes \varphi_{\mathcal{O}_F} : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathcal{O}_F \to \mathcal{O}_F$ puisque $\mathcal{O}_F$ est de u-hauteur $\leqslant hp$. Par ailleurs, on vérifie facilement que cette dernière application est injective. Il existe par suite un morphisme $g : T \to \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathcal{O}_F$ qui est compatible à l'action de Galois, et permet de factoriser

6. La constante peut être encore légèrement améliorée, mais la forme que nous donnons nous a semblé un peu plus agréable.

$u^{hp} f$ comme suit : $u^{hp} f = (\mathrm{id} \otimes \varphi_{\mathcal{O}_F}) \circ g$. Ce morphisme g définit un élément de $\mathfrak{S} \otimes_{\mathfrak{S},\varphi} \mathfrak{M}$ qui s'envoie sur f par $\mathrm{id} \otimes \varphi_{\mathfrak{M}}$. Ceci montre bien que $u^{hp} f$ est dans l'image de $\mathrm{id} \otimes \varphi_{\mathfrak{M}}$. ☐

En utilisant qu'une extension de deux φ-réseaux de hauteur divisant U_1 et U_2 respectivement est de hauteur divisant $U_1 U_2$, il est possible d'étendre la proposition 2.17 aux représentations annulées par une puissance de p. Le résultat obtenu peut se formuler comme suit.

Corollaire 2.19. *Soit T une $\mathbb{Z}_p$-représentation de longueur finie de G_∞ (resp. de G_K), soit n un entier tel que $p^n T = 0$, et soit h un entier tel que $G_\infty^{(\mu)}$ (resp. $G_K^{(mu)}$) agisse trivialement sur T pour tout $\mu > \frac{hp}{p-1}$ (resp pour tout $\mu > 1 + \frac{e}{p-1} + e \cdot (1 + \log_p(\frac{h}{e}))$). Alors, pour tout élément $U \in W(R)$ tel que $v_R(U \bmod p) \geqslant h$, le φ-module étale (resp. le (φ, τ)-module) associé à T admet un φ-réseau (resp. un (φ, τ)-réseau) de U-hauteur $\leqslant n$.*

Démonstration. C'est un dévissage immédiat à partir de la proposition 2.17. ☐

On remarquera que, si pour $n = 1$, l'écart entre les bornes appraissant dans le théorème 2 d'une part et la proposition 2.17 ne différaient que par la constante $c(K)$ dans la borne sur μ et par un facteur p dans celle sur la u-hauteur, ce même écart se creuse de façon drastique lorsque n augmente : dans le corollaire 2.19, la présence de n n'apparaît plus dans la borne sur μ mais dans celle sur la hauteur !

2.3 Les (φ, τ)-réseaux

Avant de pouvoir définir des réseaux dans les (φ, τ)-modules sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$, il est nécessaire introduire des sous-anneaux de $\mathcal{E}^{\mathrm{int}}$ et $\mathcal{E}_\tau^{\mathrm{int}}$ sur lesquels ces réseaux seront définis. Le sous-anneau de $\mathcal{E}^{\mathrm{int}}$ que l'on va considérer est bien entendu $\mathfrak{S}$, qui est déjà l'anneau qui intervenait dans la définition de φ-réseaux. L'égalité $\mathfrak{S} = \mathcal{E}^{\mathrm{int}} \cap W(R)$ nous conduit à choisir comme sous-anneau de $\mathcal{E}_\tau^{\mathrm{int}}$, l'intersection $\mathcal{E}_\tau^{\mathrm{int}} \cap W(R)$ que l'on note $\mathfrak{S}_\tau$. Celle-ci est stable par le Frobenius et l'action de G_K.

Définition 2.20. Soit M un (φ, τ)-module sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$. Un (φ, τ)-*réseau* dans M est la donnée d'un φ-réseau $\mathfrak{M}$ dans M tel que le sous-module $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ de $\mathcal{E}_\tau^{\mathrm{int}} \otimes_{\mathcal{E}^{\mathrm{int}}} \mathfrak{M}$ soit stable par l'opérateur τ.

Pour $U \in W(R)$ et $h \in \mathbb{N}$, on dit que $\mathfrak{M}$ est de hauteur divisant U (resp. de U-hauteur $\leqslant h$) s'il l'est en tant que φ-module.

Remarque 2.21. Comme -1 est la limite dans $\mathbb{Z}_p$ d'une suite d'entiers positifs, la définition ci-dessus implique que tout (φ, τ)-réseau $\mathfrak{M}$ de M est tel que $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ est stable par τ^{-1}.

2.3.1 Un théorème d'existence dans le cas de torsion

Le but de ce paragraphe est de démontrer la proposition suivante.

Proposition 2.22. *Tout (φ, τ)-module sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$ qui est annulé par une puissance de p admet un (φ, τ)-réseau.*

Pour cela, on fixe M un (φ, τ)-module sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$ annulé par une puissance de p et on considère l'ensemble $\mathcal{F}_\varphi(M)$ (resp. $\mathcal{F}_{\varphi,\tau}(M)$) des φ-réseaux (resp. (φ, τ)-réseaux à l'intérieur de M. On veut démontrer que $\mathcal{F}_{\varphi,\tau}(M)$ est non vide. On sait déjà (voir lemme 2.5) que $\mathcal{F}_\varphi(M)$ n'est pas vide. Pour tout entier h, soit $\mathcal{F}_\varphi^{\leqslant h}(M)$ le sous-ensemble de $\mathcal{F}_\varphi(M)$ formé des φ-réseaux de u-hauteur $\leqslant h$. Étant donné que M est annulé par une puissance de p, on sait par la deuxième partie du lemme 2.5 que $\mathcal{F}_\varphi(M)$ est la réunion des $\mathcal{F}_\varphi^{\leqslant h}(M)$. On en déduit qu'il existe un entier h tel que $\mathcal{F}_\varphi^{\leqslant h}(M)$, lui-même, est non vide. Par ailleurs, la relation d'inclusion fait de $\mathcal{F}_\varphi^{\leqslant h}(M)$ un ensemble partiellement ordonné dont les propriétés essentielles sont dégagées dans [6], §3.2. En particulier, le corollaire 3.2.6 nous apprend que $\mathcal{F}_\varphi^{\leqslant h}(M)$ admet un plus petit et un plus grand élément. La proposition 2.22 que nous voulons démontrer résulte ainsi directement du lemme suivant.

Lemme 2.23. *Le plus petit élément de $\mathcal{F}_\varphi^{\leqslant h}(M)$ appartient à $\mathcal{F}_{\varphi,\tau}^{\leqslant h}(M)$.*

Démonstration. Soit $\mathfrak{M}$ ce plus petit élément. C'est en particulier un φ-réseau dans M de u-hauteur $\leqslant h$. On veut montrer que $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ est stable par τ et, pour cela, on pose

$$\mathfrak{M}' = M \cap \tau^{-1}(\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}).$$

Du fait que φ et τ commutent, on déduit facilement que $\mathfrak{M}'$ est un φ-réseau dans M. Pour conclure, il suffit de montrer qu'il est de u-hauteur $\leqslant h$. En effet, par minimalité de $\mathfrak{M}$, on aura alors $\mathfrak{M} \subset \mathfrak{M}'$ d'où, en appliquant τ, on trouvera $\tau(\mathfrak{M}) \subset \tau(\mathfrak{M}') \subset \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$. Reste donc à montrer que $\mathfrak{M}'$ est de u-hauteur $\leqslant h$, c'est-à-dire que $(\mathrm{id} \otimes \varphi)^{-1}(u^h \mathfrak{M}') \subset W(R) \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}'$. Comme l'image inverse commute à l'intersection et que φ commute à τ, il suffit de justifier que

$$(\mathrm{id} \otimes \varphi)^{-1}(\tau(u^h) \cdot W(R) \otimes_{\mathfrak{S}} \mathfrak{M}) \subset W(R) \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}.$$

Or, puisque $\frac{\tau(u^h)}{u^h} = [\underline{\varepsilon}]^h$ est inversible dans $W(R)$ (car sa réduction modulo p est de valuation nulle), il revient au même de remplacer $\tau(u^h)$ par u^h dans l'inclusion précédente, et celle-ci résulte alors du fait que $\mathfrak{M}$ est de u-hauteur $\leqslant h$. $\square$

2.3.2 Réduction modulo UV des (φ, τ)-réseaux

Nous avons vu dans la remarque 2.10 qu'un φ-réseau de hauteur divisant U (où U est un élément de $W(R)$ non divisible par p) dans un φ-module étale sur $\mathcal{E}^{\mathrm{int}}$ est entièrement déterminé par sa réduction modulo V où V est un élément de $W(R)$ non divisible par p tel que $\varphi(V) = UV$. Nous établissons ici un résultat analogue pour les (φ, τ)-réseaux.

On fixe un élément U comme précédemment, et on se donne pour l'instant simplement un φ-réseau $\mathfrak{M}$ de hauteur divisant U dans un φ-module étale sur $\mathcal{E}^{\mathrm{int}}$. On se donne également un élément $V \in W(R)$ non divisible par p tel que $\varphi(V) = UV$; un tel élément existe toujours par le lemme 2.7. On note $\mathfrak{m}_{\mathfrak{S}_\tau}$ l'idéal maximal de l'anneau local $\mathfrak{S}_\tau$ et si X est un élément de $W(R)$, on s'autorise à écrire, dans un léger abus de notations, $X\mathfrak{m}_{\mathfrak{S}_\tau}$ à la place de $\mathfrak{S}_\tau \cap X\mathfrak{m}_{W(R)}$. Étant donné un entier p-adique a, ainsi qu'un élément $X \in W(R)$, on définit $\mathcal{A}_X(\mathfrak{M})$ comme l'ensemble des automorphismes τ^a-semi-linéaires

$$\tau_X^{(a)} : (\mathfrak{S}_\tau / X\mathfrak{m}_{\mathfrak{S}_\tau}) \otimes_{\mathfrak{S}} \mathfrak{M} \to (\mathfrak{S}_\tau / X\mathfrak{m}_{\mathfrak{S}_\tau}) \otimes_{\mathfrak{S}} \mathfrak{M}$$

commutant à φ et tels que pour tout $g \in G_\infty / H_\infty$, on ait

$$(g \otimes \mathrm{id}) \circ \tau_X^{(a)} = (\tau_X^{(a)})^b \circ ((\tau^{ab} g \tau) \otimes \mathrm{id}). \tag{2.6}$$

où b est l'unique élément de $\mathbb{Z}_p$ tel que $\chi(g) \cdot [b]_{\chi(\tau)} = [a]_{\chi(\tau)}$. Si X divise Y, la réduction modulo $X\mathfrak{m}_{\mathfrak{S}_\tau}$ définit une application canonique $\rho_{Y,X} : \mathcal{A}_Y(\mathfrak{M}) \to \mathcal{A}_X(\mathfrak{M})$. Par ailleurs, $\mathcal{A}_0(\mathfrak{M})$ est exactement l'ensemble des τ qui font de $\mathfrak{M}$ un (φ, τ)-réseau. La proposition suivante, qui est très semblable à la proposition 2.9, montre que $\mathcal{A}_0(\mathfrak{M})$ se retrouve entièrement à partir du morphisme $\rho_{UV,V} : \mathcal{A}_{UV}(\mathfrak{M}) \to \mathcal{A}_V(\mathfrak{M})$.

Proposition 2.24. *Comme précédemment, on se donne $\mathfrak{M}$ un φ-réseau de hauteur divisant U. L'application $\rho_{0,V} : \mathcal{A}_0(\mathfrak{M}) \to \mathcal{A}_V(\mathfrak{M})$ est injective et son image s'identifie à celle de $\rho_{UV,V} : \mathcal{A}_{UV}(\mathfrak{M}) \to \mathcal{A}_V(\mathfrak{M})$.*

Démonstration. En utilisant la commutation de τ^{-a} et φ, on démontre tout de suite que $\mathfrak{M}$ est de hauteur divisant $\tau^{-a}(U)$ pour tout $a \in \mathbb{Z}_p$. En reprenant la preuve de la proposition 2.9, on démontre alors qu'étant donné un élément $\tau_{UV}^{(a)} \in \mathcal{A}_{UV}(\mathfrak{M})$, il existe une unique application τ^a-semi-linéaire $\tau^{(a)} : \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M} \to \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ qui commute à φ et est congrue à $\tau_{UV}^{(a)}$ modulo $V\mathfrak{m}_{\mathfrak{S}_\tau}$. L'injectivité de $\rho_{0,V}$ résulte de cela, tandis pour établir l'égalité annoncée entre les images, il suffit de prouver que l'application $\tau^{(a)}$ construite vérifie la relation (2.6).

Pour cela, le plus rapide est sans doute de remarquer qu'étant donné un élément $b \in \mathbb{Z}_p$, on peut appliquer ce qui précède avec ab à la place de a. On obtient comme cela en particulier l'existence d'une unique application τ^{ab}-semi-linéaire $\tau^{(ab)} : \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M} \to \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ qui est congrue à $(\tau_0^{(a)})^b$ modulo $V\mathfrak{m}_{\mathfrak{S}_\tau}$ et qui commute à φ. Or, pour $g \in G_\infty / H_\infty$ et b tel que $\chi(g) \cdot [b]_{\chi(\tau)} = [a]_{\chi(\tau)}$, les deux applications τ^b et $(g \otimes \mathrm{id}) \circ \tau \circ ((\tau^{-b} g \tau)^{-1} \otimes \mathrm{id})$ sont τ^{ab}-semi-linéaires, congrues à $(\tau_0^{(a)})^b$ modulo I_0 et commutent à φ ; on en déduit donc bien qu'elles coïncident. $\square$

Comme annoncé, le résultat que l'on vient de démontrer permet de faire suite à la remarque 2.10. En effet, étant donné $\mathfrak{M}$ et $\mathfrak{M}'$ deux (φ, τ)-réseaux, il implique l'égalité

$$\mathrm{Hom}_{\varphi,\tau}(\mathfrak{M}, \mathfrak{M}') = \mathrm{image}\big(\mathrm{Hom}_{\varphi,\tau}(\mathfrak{M}/UV\mathfrak{M}, \mathfrak{M}'/UV\mathfrak{M}') \to \mathrm{Hom}_{\varphi,\tau}(\mathfrak{M}/V\mathfrak{M}, \mathfrak{M}'/V\mathfrak{M}')\big)$$

à partir de quoi on déduit que la réduction modulo UV définit un foncteur pleinement fidèle de la catégorie des (φ, τ)-réseaux dans une catégorie de (φ, τ)-modules sur $(\mathfrak{S}/UV\mathfrak{S}, \mathfrak{S}_\tau/UV\mathfrak{S}_\tau)$ dont les morphismes sont twistés (et dont on laisse au lecteur le soin d'écrire la définition exacte).

2.3.3 L'action de τ sur un (φ, τ)-réseau

L'objectif de ce numéro est de montrer qu'il est possible, dans une certaine mesure, de contrôler l'action de τ agissant sur un (φ, τ)-réseau en fonction de la hauteur de celui-ci. Le résultat précis que nous allons démontrer à ce sujet est le théorème 2.25 ci-après, mais avant de l'énoncer, il nous faut définir une suite croissante $(\mathfrak{S}_m)_{m \geqslant 1}$ de sous-anneaux de $\mathfrak{S}_\tau$. On rappelle, pour cela, qu'on a introduit dans le §1.2.3 les corps F_m définis par $F_m = (F_0^{\mathrm{sep}})^{H_m}$ avec $H_m = \mathrm{Gal}(\bar{K}/K_\infty(\zeta_{p^m})) \subset G_\infty$. Ces corps définissent une suite croissante d'extensions finies séparables de F_0 incluses dans F_τ. Par ailleurs, pour tout m, il correspond à F_m une unique extension non ramifiée de $\mathcal{E}$: c'est celle qui admet F_m pour corps résiduel. On la note $\mathcal{E}_m$, on définit $\mathcal{E}_m^{\mathrm{int}}$ comme son anneau des entiers et on pose enfin $\mathfrak{S}_m = \mathcal{E}_m^{\mathrm{int}} \cap W(R)$. On vérifie aisément que pour tous entiers n et m, on a $p^n\mathfrak{S}_m = p^n\mathcal{E}_m^{\mathrm{int}} \cap W(R)$ et $\mathfrak{S}_m/p^n\mathfrak{S}_m = (\mathcal{E}_m^{\mathrm{int}}/p^n\mathcal{E}_m^{\mathrm{int}}) \cap W_n(R)$.

Théorème 2.25. *Il existe une constante $c'(K)$ ne dépendant que de K telle que pour toute donnée de*
- *deux éléments U et V de $W(R)$ non multiples de p tels que $\varphi(V) = UV$, et*
- *un (φ, τ)-réseau $\mathfrak{M}$ de hauteur divisant U à l'intérieur d'un (φ, τ)-module M,*

on ait, en notant s_0 le plus petit entier $\geqslant \log_p(v_R(U \bmod p)) + c'(K)$, l'inclusion suivante :

$$(\tau^{p^s} - \mathrm{id})(\mathfrak{M}) \subset \left(V\mathfrak{m}_{\mathfrak{S}_\tau} + \sum_{\substack{n \geqslant 0 \\ n > s - s_0}} p^n \mathfrak{S}_{s_0 - s + n} \right) \otimes_{\mathfrak{S}} \mathfrak{M} \tag{2.7}$$

pour tout entier $s \geqslant 0$.

Faisons tout de suite trois remarques. *Primo*, on sait par le lemme 2.7 que, dès que l'on se donne un élément $U \in W(R)$, il existe V vérifiant la condition requise. En outre, d'après la remarque 2.8, l'idéal engendré par V — et donc en particulier l'inclusion (2.7) — ne dépend que de U. Ainsi, l'élément V ne joue pas véritablement de rôle dans le théorème précédent, hormis le fait qu'il permet de l'énoncer relativement simplement. *Secundo*, le théorème 2.25 implique l'inclusion (2.8) ci-après moins précise mais également moins technique :

$$(\tau^{p^s} - \mathrm{id})(\mathfrak{M}) \subset \big(V\mathfrak{m}_{W(R)} + p^{\max(0, s - s_0 + 1)} W(R)\big) \otimes_{\mathfrak{S}} \mathfrak{M}. \tag{2.8}$$

Tertio, il est intéressant de combiner le résultat du théorème précédent avec celui du §2.3.2. En effet, on a démontré là que la connaissance de τ^{p^s} modulo $V\mathfrak{m}_{\mathfrak{S}_\tau}$ suffit à retrouver complètement τ^{p^s}. En outre, il suit de la preuve (voir aussi la démonstration de la proposition 2.9) que τ^{p^s} s'obtient à partir de $\tau^{p^s} \bmod V\mathfrak{m}_{\mathfrak{S}_\tau}$ grâce à un processus itératif simple. En appliquant ce processus itératif à l'inclusion (2.7), on obtient des renseignements encore plus précis sur la forme de l'opérateur τ^{p^s}.

Ceci étant dit, venons-en à la démonstration du théorème qui va maintenant nous occuper jusqu'à la fin de ce numéro. On se donne des éléments $U, V \in W(R)$ tels que U ne soit pas multiple de p et $\varphi(V) = UV$. On fixe un (φ, τ)-module M sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$ ainsi qu'un (φ, τ)-réseau $\mathfrak{M}$ de M de hauteur divisant U. Comme d'habitude, on désigne par la lettre T la représentation de G_K associée à M. On suppose en outre pour commencer que $\mathfrak{M}$ est annulé par p^n pour un certain entier n, et on considère un nombre entier t vérifiant les deux conditions suivantes :
- on a $\tau^{p^t}(u) \equiv u \pmod{p^n, UV\mathfrak{m}_{\mathfrak{S}_\tau}}$;
- il existe un élément $\gamma_t \in G_\infty$ agissant trivialement sur T et tel que $v_p(\chi(\gamma_t) - 1) = t$ (où v_p est la valuation p-adique normalisée par $v_p(p) = 1$).

On expliquera, dans la suite de la démonstration, comment déterminer un tel t, mais pour l'instant on se contente de supposer qu'il est donné. Afin de minimiser les confusions, on notera tout au long de la preuve $\tau_{\mathfrak{M}}$ l'automorphisme τ agissant sur $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$. De $\tau^{p^t}(u) \equiv u \pmod{p^n, UV\mathfrak{m}_{\mathfrak{S}_\tau}}$, on déduit que l'application τ^{p^t}-semi-linéaire

$$\tau_{\mathfrak{M},\mathrm{triv}}^{(p^t)} = \tau^{p^t} \otimes \mathrm{id} : \frac{\mathfrak{S}_\tau}{UV\mathfrak{m}_{\mathfrak{S}_\tau}} \otimes_{\mathfrak{S}} \mathfrak{M} \to \frac{\mathfrak{S}_\tau}{UV\mathfrak{m}_{\mathfrak{S}_\tau}} \otimes_{\mathfrak{S}} \mathfrak{M}$$

est bien définie. La proposition 2.24 s'applique et montre qu'il existe une application $\tilde{\tau}_{\mathfrak{M},\mathrm{triv}}^{(p^t)} : \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M} \to \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ qui commute avec φ, vérifie la relation (2.6) et est congrue à $\tau_{\mathfrak{M},\mathrm{triv}}^{p^t}$ modulo $V\mathfrak{m}_{\mathfrak{S}_\tau}$. L'automorphisme $\tilde{\tau}_{\mathfrak{M},\mathrm{triv}}^{(p^t)}$ prolongé à $\mathcal{E}_\tau^{\mathrm{int}} \otimes_{\mathcal{E}^{\mathrm{int}}} M$ définit une structure de (φ, τ^{p^t})-module sur $\mathfrak{M}$ à laquelle il correspond une représentation T_{triv} du sous-groupe G_t. Puisque les représentations T et T_{triv} sont liées au même φ-module, leurs restrictions à G_∞ coïncident.

On rappelle que l'on a supposé l'existence d'un élément $\gamma_t \in G_\infty$ qui agit trivialement sur T et qui est tel que $v_p(\chi(\gamma_t) - 1) = t$. L'élément $\tau^{\chi_\tau(\gamma_t)-1}$ est égal au produit $\gamma_t \tau \gamma_t^{-1} \tau^{-1}$, et donc agit également trivialement sur T. Comme, par le lemme 1.1, la valuation p-adique de $\chi_\tau(\gamma_t) - 1$ est égale à t, on en déduit enfin que τ^{p^t}, aussi, agit trivialement sur T. Puisque γ_t appartient à G_∞, il agit également trivialement sur T_{triv} et, en reprenant le raisonnement précédement, on obtient enfin que τ^{p^t} agit aussi trivialement sur T_{triv}. Il s'ensuit que tout le sous-groupe G_t agit de la même manière sur T et T_{triv}. Autrement dit, T_{triv} n'est rien d'autre que la représentation T restreinte au sous-groupe G_t. Au niveau des (φ, τ)-modules, cela nous donne l'égalité $\tau_{\mathfrak{M}}^{p^t} = \tilde{\tau}_{\mathfrak{M},\mathrm{triv}}^{(p^t)}$, d'où il résulte notamment que $\tau_{\mathfrak{M}}^{p^t} \equiv \tau^{p^t} \otimes \mathrm{id} \pmod{V\mathfrak{m}_{\mathfrak{S}_\tau}}$. Pour $x \in \mathfrak{M}$, on obtient en particulier $\tau_{\mathfrak{M}}^{p^t}(x) \equiv x \pmod{V\mathfrak{m}_{\mathfrak{S}_\tau}}$. Cette congruence reste clairement vraie si t est remplacée par un entier $s \geqslant t$. Autrement dit, on a l'inclusion $(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset V\mathfrak{m}_{\mathfrak{S}_\tau} \otimes_{\mathfrak{S}} \mathfrak{M}$ pour tout $s \geqslant t$. Celle-ci se généralise à un entier $s < t$ sous la forme suivante :

$$(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset (\mathfrak{S}_{t-s} + V\mathfrak{m}_{\mathfrak{S}_\tau}) \otimes_{\mathfrak{S}} \mathfrak{M}. \tag{2.9}$$

Pour démontrer cela, on fixe un entier $s < t$, et on considère un élément $\gamma \in G_\infty$ tel que $v_p(\chi(\gamma)-1) \geqslant t-s$. Le commutateur $\gamma \tau^{p^s} \gamma^{-1} \tau^{-p^s}$ est alors égal à $\tau^{p^s(\chi_\tau(\gamma)-1)}$ et appartient donc à G_t. Ainsi, par ce qui a été fait avant, on sait que cet élément agit trivialement sur $\mathfrak{M}$ modulo $V\mathfrak{m}_{\mathfrak{S}_\tau}$. Il en résulte que pour $x \in \mathfrak{M}$, on a $(\gamma \otimes \mathrm{id}) \circ \tau^{p^s}(x) \equiv \tau^{p^s}(x) \pmod{V\mathfrak{m}_{\mathfrak{S}_\tau}}$. Comme ceci est vrai pour tout γ tel que $v_p(\chi(\gamma) - 1) \geqslant t - s$, on en déduit en utilisant la deuxième partie de la proposition 1.13 que

$$(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset W_n(\mathcal{O}_{F_{t-s}}^{\mathrm{perf}}) \otimes_{\mathfrak{S}/p^n\mathfrak{S}} \mathfrak{M} + V\mathfrak{m}_{\mathfrak{S}_\tau} \otimes_{\mathfrak{S}} \mathfrak{M}$$

où, pour un entier m donné, on a noté $\mathcal{O}_{F_m}^{\mathrm{perf}}$ l'anneau des entier du perfectisé de $(F_0^{\mathrm{sep}})^{H_m}$ avec $H_m = \mathrm{Gal}(\bar{K}/K_\infty(\zeta_{p^m}))$. Étant donné que $\mathfrak{M}$ est de type fini, il existe un entier ν_0 tel que l'on puisse remplacer dans l'inclusion précédent $\mathcal{O}_{F_{t-s}}^{\mathrm{perf}}$ par l'anneau plus petit $\varphi^{-\nu_0}(\mathcal{O}_{F_{t-s}})$. En écrivant que φ et τ^{p^s} commutent, on démontre par récurrence sur ν, de même que dans la première partie de la preuve de la proposition 2.9, que l'on a :

$$(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset \big((\mathfrak{S}/p^n\mathfrak{S}) \cdot W_n(\varphi^{\nu-\nu_0}(\mathcal{O}_{F_{t-s}}))\big) \otimes_{\mathfrak{S}/p^n\mathfrak{S}} \mathfrak{M} + UV\mathfrak{m}_{\mathfrak{S}_\tau} \otimes_{\mathfrak{S}} \mathfrak{M}$$

pour tout entier $\nu \geqslant 0$. L'inclusion (2.9) résulte alors du lemme suivant.

Lemme 2.26. *Avec les notations précédentes, on a* $W_n(\varphi^{N_n}(\mathcal{O}_{F_{t-s}})) \subset \mathfrak{S}_{t-s}/p^n\mathfrak{S}_{t-s}$ *avec* $N_n = \frac{n(n-1)}{2}$.

Démonstration. On pose $m = t - s$ et on raisonne par récurrence sur n. Pour $n = 1$, le quotient $\mathfrak{S}_m/p\mathfrak{S}_m$ est égal à $\mathcal{O}_{F_m}$, et il n'y a donc rien à démontrer. Par ailleurs, si le résultat est vrai pour n et si $x \in W_{n+1}(F_{t-s})$, on peut écrire $\varphi^{N_n}(x) = y + z$ avec $y \in \mathfrak{S}_{t-s}/p^{n+1}\mathfrak{S}_{t-s} \subset W_{n+1}(\mathcal{O}_{F_{t-s}})$ et $z \in W_{n+1}(\mathcal{O}_{F_{t-s}})$ multiple de p^n. L'élement $\frac{z}{p^n}$ est alors bien défini dans $\mathcal{O}_{F_{t-s}}^{\mathrm{perf}}$ et il appartient à $\varphi^{-n}(\mathcal{O}_{F_{t-s}})$. Il s'ensuit que $p^n\varphi^n(z)$ appartient à $\mathfrak{S}_{t-s}/p^{n+1}\mathfrak{S}_{t-s}$ et par suite qu'il en est de même de $\varphi^{N_n+n}(x) = \varphi^{N_{n+1}}(x)$. □

Il nous reste à présent à déterminer des conditions simples sur le nombre t permettant d'assurer qu'il satisfait aux deux hypothèses faites au début de la démonstration. On a en fait déjà étudié la deuxième hypothèse au §2.2.3 (voir en particulier la formule (2.5)) : on a montré qu'elle est vérifiée dès que

$$t \geqslant s_0(K) \quad \text{et} \quad t > \frac{c_0(K)}{e} + \max\left(\tfrac{1}{p-1}, n + \log_p(\tfrac{h}{e})\right)$$

où $s_0(K)$ et $c_0(K)$ étaient des constantes ne dépendant que du corps K.

Examinons maintenant la première condition. Elle stipule que $\tau^{p^t}(u) \equiv u \pmod{p^n, UV\mathfrak{m}_{\mathfrak{S}_\tau}}$, c'est-à-dire que la réduction modulo p^n de $\tau^{p^t}(u) - u$ est dans l'idéal $UV\mathfrak{m}_{W_n(R)}$. Or la différence $\tau^{p^t}(u) - u$ se calcule facilement ; elle vaut $u([\underline{\varepsilon}]^{p^t} - 1) \in W(R)$ où on rappelle que $\underline{\varepsilon}$ est l'élément de R défini par le système compatible (ζ_{p^s}) de racines primitives p^s-ièmes de l'unité, qui avait été fixé au début de l'article. En particulier, étant donné que $v_R(\underline{\varepsilon}) = \frac{p}{p-1}$, on voit clairement sur cette écriture que $\tau^{p^t}(u) - u \in W(\mathfrak{a}_R^{>p^{t+1}/(p-1)})$. Par le lemme 2.13, on en déduit que la réduction modulo p^n de $\tau^{p^t}(u) - u$ est dans l'idéal $UV\mathfrak{m}_{W_n(R)}$ dès que $p^t \geqslant hp^{n-1}$, c'est-à-dire dès que $t \geqslant n - 1 + \log_p h$.

Au final, en mettant ensemble les résultats des deux alinéas précédents, on trouve qu'il existe une constante $c'(K)$ ne dépendant que du corps K telle que tout nombre entier $t \geqslant c'(K) + n - 1 + \log_p h$ vérifie les hypothèses requises. L'inclusion (2.9) est donc vraie pour de tels t. Si, comme dans l'énoncé du théorème 2.25, on note s_0 le plus petit entier supérieur ou égal à $c'(K) + \log_p h$, on obtient donc :

$$(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset (\mathfrak{S}_{s_0-s+n-1} + UV\mathfrak{m}_{\mathfrak{S}_\tau}) \otimes_{\mathfrak{S}} \mathfrak{M}.$$

Enfin, si on ne suppose plus que $\mathfrak{M}$ est annulée par p^n, on peut quand même appliquer ce que l'on vient de faire au quotient $\mathfrak{M}/p^n\mathfrak{M}$, ce qui conduit à l'inclusion :

$$(\tau_{\mathfrak{M}}^{p^s} - \mathrm{id})(\mathfrak{M}) \subset (\mathfrak{S}_{s_0-s+n-1} + UV\mathfrak{m}_{\mathfrak{S}_\tau} + p^n\mathfrak{S}_\tau) \otimes_{\mathfrak{S}} \mathfrak{M}.$$

L'inclusion du théorème 2.25 en résulte finalement en prenant l'intersection sur tous les n.

3 Le cas des représentations de $E(u)$-hauteur finie

L'élement $E(u)$ qui apparaît dans la locutation « $E(u)$-hauteur finie » est le polynôme minimal de l'uniformisante π sur $W[1/p]$. Il s'agit d'un polynôme d'Eisenstein de degré e. C'est donc en particulier un élément de $W(R)$ qui n'est pas multiple de p. Ainsi, il fait bien sens de parler de φ-modules de $E(u)$-hauteur $\leqslant r$ pour un certain entier r ou de $E(u)$-hauteur finie. Une $\mathbb{Z}_p$-représentation de G_∞ ou de G_K est dite de $E(u)$-hauteur $\leqslant r$ (resp. de $E(u)$-hauteur finie) si le φ-module qui lui est associé l'est, tandis qu'une $\mathbb{Q}_p$-représentation est ainsi qualifiée si elle admet un réseau stable par Galois satisfaisant à cette propriété.

Reprenant des idées de Breuil, Kisin a élaboré dans [13] une théorie prometteuse pour étudier les représentations semi-stables (ainsi que leurs déformations) et a, au passage, montré que celles-ci entretenaient un lien étroit avec les représentations de $E(u)$-hauteur finie. Précisément, il a démontré qu'une représentation semi-stable dont tous les poids de Hodge-Tate sont dans $\{0, 1, \dots, r\}$ est de $E(u)$-hauteur $\leqslant r$. Or, la théorie que nous avons développée dans cet article donne une description des représentations de G_K de $E(u)$-hauteur $\leqslant r$ en termes de (φ, τ)-modules. Dans ce dernier chapitre, nous étudions comment cette nouvelle description s'insère dans la théorie de Kisin. Comme corollaire, nous obtenons le théorème 3 de l'introduction, ainsi qu'une description, en termes de la théorie de Kisin, des réseaux dans les représentations semi-stables.

3.1 Les (φ, τ)-modules comme complément de la théorie de Kisin

Le polynôme $E(u)$ étant un polynôme d'Eisenstein, son coefficient constant $E(0)$ s'écrit sous la forme pc où c est un élément inversible dans $\mathbb{Z}_p$. On pose $U = \frac{E(u)}{c}$; il est alors clair qu'être de $E(u)$-hauteur $\leqslant r$ est équivalent à être de U-hauteur $\leqslant r$. Soit $\mathfrak{t}$ un élément de $W(R)$ tel que $\varphi(\mathfrak{t}) = U\mathfrak{t}$ (un tel élément existe bien d'après le lemme 2.7).

3.1.1 Un concentré de théorie de Kisin

On commence par quelques rappels très sommaires concernant l'anneau A_{cris} de Fontaine. Il est défini comme le complété p-adique de l'enveloppe à puissances divisées de $W(R)$ par rapport à l'idéal principal engendré par $E(u)$ (et compatibles avec les puissances divisées canoniques sur l'idéal (p)). La série

$$\log([\underline{\varepsilon}]) = \sum_{n \geqslant 1} \frac{(1-[\underline{\varepsilon}])^n}{n}$$

converge dans A_{cris} vers un élément t qui joue un rôle très important en théorie de Hodge p-adique. Il vérifie $\varphi(t) = pt$ et $\gamma(t) = \chi(\gamma)t$ pour tout $\gamma \in G_K$.

On en vient à présent aux rappels sur la théorie de [13]. On se borne à présenter uniquement ce qui sera utile dans la suite. Soit $\mathcal{O}$ l'anneau des séries en la variable u convergant sur le disque ouvert de centre 0 et de rayon 1. Il contient clairement $\mathfrak{S}[1/p]$ et se plonge dans A_{cris} en envoyant comme d'habitude u sur $[\underline{\pi}]$. L'élément λ défini par le produit convergeant suivant :

$$\lambda = \prod_{n=0}^{\infty} \varphi^n\Big(\frac{E(u)}{E(0)}\Big) = \prod_{n=0}^{\infty} \varphi^n\Big(\frac{U}{p}\Big) \in \mathcal{O}$$

est solution de l'équation $\frac{U}{p} \cdot \varphi(\lambda) = \lambda$. Par ailleurs, d'après l'exemple 5.3.3 de [18][7], il est possible de choisir $\mathfrak{t}$ de façon à ce que l'égalité $\varphi(\lambda\mathfrak{t}) = -t$ soit satisfaite, ce que nous supposerons dans la suite. L'élément λ permet de munir l'anneau $\mathcal{O}$ d'un opérateur de dérivation N_∇ défini par $N_\nabla = -u\lambda\frac{d}{du}$, puis de définir la catégorie $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla}$ dont un objet consiste en la donnée des points suivants :

- un $\mathcal{O}$-module $\mathcal{M}$ libre de rang fini ;
- un morphisme φ-semi-linéaire $\varphi : \mathcal{M} \to \mathcal{M}$ qui est tel que le conoyau de $\mathrm{id} \otimes \varphi : \mathcal{O} \otimes_{\varphi,\mathcal{O}} \mathcal{M} \to \mathcal{M}$ soit annulé par une puissance de $E(u)$;
- un opérateur $N_\nabla : \mathcal{M} \to \mathcal{M}$ vérifiant la loi de Leibniz (*i.e.* $N_\nabla(ax) = N_\nabla(a)x + aN_\nabla(x)$ pour tout $a \in \mathcal{O}$ et $x \in \mathcal{M}$) et la relation $N_\nabla \circ \varphi = p \cdot \frac{E(u)}{E(0)} \cdot \varphi \circ N_\nabla$.

Si l'on note $\mathrm{Rep}^{\text{st}}_{[0,+\infty[}(G_K)$ la catégorie des représentations semi-stables de G_K à poids de Hodge Tate positifs ou nuls, un résultat essentiel de [13] est la construction d'un foncteur pleinement fidèle $\mathcal{K} : \mathrm{Rep}^{\text{st}}_{[0,+\infty[}(G_K) \to \mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla}$. On note $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$ son image essentielle[8]. Kisin démontre encore deux résultats importants pour ce qui va suivre, à savoir que pour tout objet $\mathcal{M}$ de $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$,

A. le φ-module $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{M}$ (muni de l'opérateur φ déduit par extension des scalaires) est étale et correspond *via* la théorie de Fontaine à la représentation $\mathcal{K}^{-1}(\mathcal{M})$ restreinte à G_∞, et

B. pour tout réseau $T \subset \mathcal{K}^{-1}(\mathcal{M})$ stable par G_∞, il existe dans le φ-module sur $\mathcal{E}^{\text{int}}$ correspondant (qui vit à l'intérieur de $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{M}$) un unique φ-réseau libre sur $\mathfrak{S}$ qui est de $E(u)$-hauteur finie.

La propriété B précédente permet de construire un foncteur $\mathcal{R}_\varphi : \mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0} \to \mathrm{Mod}_{/\mathfrak{S}}^{\varphi} \otimes \mathbb{Q}_p$, où $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi}$ désigne la catégorie des φ-réseaux (dans un φ-module étale sur $\mathcal{E}^{\text{int}}$) *libres* sur $\mathfrak{S}$, et où $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi} \otimes \mathbb{Q}_p$ est sa catégorie à isogénie près[9]. Enfin, si l'on note $\mathcal{T}_\varphi$ le foncteur qui à un φ-réseau $\mathfrak{M}$ fait correspondre la représentation de G_∞ associée à $\mathcal{E} \otimes_{\mathfrak{S}} \mathfrak{M}$, et si l'on définit $\mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_\infty)$ comme la catégorie des représentations de G_∞ qui sont de $E(u)$-hauteur finie, la propriété A nous dit que la composée $\mathcal{T}_\varphi \circ \mathcal{R}_\varphi \circ \mathcal{K}$ n'est autre que la restriction de l'action de G_K à G_∞. Le carré commutatif suivant :

$$\begin{tikzcd}
\mathrm{Rep}^{\text{st}}_{[0,+\infty[}(G_K) \arrow[r, "\text{res}"] \arrow[d, "\mathcal{K}"', "\sim"] & \mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_\infty) \\
\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0} \arrow[r, "\mathcal{R}_\varphi"] & \mathrm{Mod}_{/\mathfrak{S}}^{\varphi} \otimes \mathbb{Q}_p \arrow[u, "\mathcal{T}_\varphi"']
\end{tikzcd} \tag{3.1}$$

dans lequel res désigne le foncteur de restriction de l'action de G_K à G_∞, résume de façon concise — et, qui plus est, commode pour notre propos — les résultats de Kisin qui viennent d'être rappelés.

7. Les notations de cette référence correspondent à celles de cet article selon l'égalité $c = \varphi(\lambda)$.

8. Kisin donne en fait une caractérisation de cette image essentielle en termes de filtrations par les pentes à la Kedlaya. Nous ne détaillons par ce point dans ces rappels car il ne nous sera pas utile dans la suite.

9. Cela signifie que les objets sont les mêmes, mais que les ensembles de morphismes sont tensorisés par $\mathbb{Q}$

3.1.2 Une démonstration directe de l'unicité dans la propriété B

La démonstration que Kisin donne dans [13] de la propriété B énoncée précédemment utilise de façon essentielle des théorèmes difficiles portant sur les φ-modules sur l'anneau $\mathcal{O}$. Dans ce paragraphe, nous nous proposons de donner une démonstration alternative de la partie « unicité », qui est plus élémentaire (et plus simple), dans le sens où elle ne fait intervenir à aucun moment ni l'anneau $\mathcal{O}$, ni la théorie de Kisin. Nous démontrons même un résultat très légèrement plus général qui s'énonce comme suit.

Proposition 3.1. *Soient $\mathfrak{M}_1$ et $\mathfrak{M}_2$ deux φ-réseaux libres sur $\mathfrak{S}$ de $E(u)$-hauteur finie. Soit également un morphisme $f : \mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}_1 \to \mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}_2$. Alors $f(\mathfrak{M}_1) \subset \mathfrak{M}_2$.*

On rappelle avant d'entamer la démonstration que si $\mathfrak{M}$ est un φ-réseau (pas nécessairement libre sur $\mathfrak{S}$) à l'intérieur d'un φ-module M libre sur $(\mathcal{E}^{\text{int}}, \mathcal{E}^{\text{int}}_\tau)$, il résulte du théorème de classification des modules sur $\mathfrak{S}$ que $\text{Libre}(\mathfrak{M}) = (\mathcal{E}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}) \cap \mathfrak{M}[1/p]$ est un φ-réseau libre sur $\mathfrak{S}$. En outre, si $\mathfrak{M}$ est de $E(u)$-hauteur finie, il en est de même de $\text{Libre}(\mathfrak{M})$ et les $E(u)$-hauteurs sont, dans ce cas, égales.

Quitte à remplacer $\mathfrak{M}_1$ par $\text{Libre}(f(\mathfrak{M}_1) + \mathfrak{M}_2)$ (qui est encore de $E(u)$-hauteur finie comme on le vérifie sans peine), on peut supposer que f est l'identité et que $\mathfrak{M}_1$ contient $\mathfrak{M}_2$. Il s'agit alors de montrer que $\mathfrak{M}_1 = \mathfrak{M}_2$. En passant aux déterminants, on peut supposer que $\mathfrak{M}_1$ et $\mathfrak{M}_2$ sont libres de rang 1 sur $\mathfrak{S}$. Si le vecteur e_1 forme une base de $\mathfrak{M}_1$, il existe un élément $a \in \mathfrak{S}$ tel que $e_2 = ae_1$ soit une base de $\mathfrak{M}_2$. D'après une variante du théorème de préparation de Weierstrass (voir par exemple théorème 2.1, chap. 5 de [15]), a s'écrit comme le produit d'un élément inversible de $\mathfrak{S}$ et d'un polynôme $A(u)$ à coefficients dans W de la forme $A(u) = u^d + p(a_{d-1}u^{d-1} + \cdots + a_0)$. On veut montrer que $A(u)$ est inversible dans $\mathfrak{S}$, c'est-à-dire concrètement que $d = 0$. Soit A^σ le polynôme obtenu en appliquant le Frobenius sur W à tous les coefficients de A. On a $\varphi(A(u)) = A^\sigma(u^p)$. Du fait que, par hypothèse, $\mathfrak{M}_2$ est un φ-module de hauteur $E(u)$-hauteur finie, on déduit l'existence d'un élément $b \in \mathfrak{S}$ qui divise une puissance de $E(u)$ dans $\mathfrak{S}$ et qui vérifie l'égalité $\varphi(e_2) = be_2$.

Lemme 3.2. *L'élement b s'écrit sous la forme $E(u)^n b'$ où n est un entier et b' est inversible dans $\mathfrak{S}$.*

Démonstration. Le fait que $\mathfrak{S}$ soit un anneau intègre et que l'idéal principal engendré par $E(u)$ soit premier (puisque le quotient s'identifie à l'anneau intègre $\mathcal{O}_K$) implique le résultat dans le cas où b est un diviseur de $E(u)$ (et non d'une puissance de $E(u)$). Pour le cas général, on raisonne de la même façon par récurrence sur la plus petite puissance de $E(u)$ que b divise. □

On utilise maintenant que $\mathfrak{M}_1$ est, lui aussi, par hypothèse, un φ-module de $E(u)$-hauteur finie. La formule $\varphi(e_1) = A^\sigma(u^p)be_2$ implique que $A(u)$ divise $A^\sigma(u^p)b$ dans $\mathfrak{S}$ (puisque $\mathfrak{M}_1$ est stable par φ) et que le quotient $\frac{A^\sigma(u^p)b}{A(u)}$ est divisible par une puissance de $E(u)$ (puisque $\mathfrak{M}_1$ est de $E(u)$-hauteur finie). En écrivant b sous la forme $E(u)^n b'$ comme dans le lemme précédent, on obtient les deux divisibilités suivantes dans $\mathfrak{S}$:

$$A(u) \text{ divise } A^\sigma(u^p)E(u)^n \quad \text{et} \quad A^\sigma(u^p) \text{ divise } A(u)E(u)^m$$

pour un certain entier m. Quitte à augmenter n et m, on peut supposer que ces deux nombres sont strictement positifs. Comme $\mathfrak{S} \subset \mathcal{O}$, on peut évaluer les séries appartenant à $\mathfrak{S}$ en tout élément de l'idéal maximal de $\mathcal{O}_{\bar{K}}$. Les divisibilités qui viennent d'être écrites assurent ainsi que toute racine du polynôme $A(u)$ (resp. $A^\sigma(u^p)$) qui appartient à l'idéal maximal de $\mathcal{O}_{\bar{K}}$ est également racine du produit $A^\sigma(u^p)E(u)^n$ (resp. $A(u)E(u)^m$). On suppose à présent, par l'absurde, que $d > 0$. La théorie des polygônes de Newton affirme que les polynômes $A(u)$ et $A^\sigma(u)$ admettent chacun d racines (comptées avec multiplicité) dans l'idéal maximal de $\mathcal{O}_{\bar{K}}$ et que les valuations de ces racines, notées $v_1, \ldots, v_d$, se correspondent deux à deux. On peut bien entendu supposer que les v_i sont triées par ordre croissant. Si x désigne une racine de $A(u)$ de valuation v_d et si $v_d < \infty$, on ne peut avoir $A^\sigma(x^p) = 0$ puisque la valuation de x^p dépasse tous les v_i. Ainsi, on a nécessairement $E(x) = 0$, ce qui signifie que x est un conjugué de π. En particulier, v_d ne peut valoir que $+\infty$ ou 1. De la même façon, si y désigne une racine p-ième d'une racine de $A^\sigma(u)$ de valuation v_1, on a $A(y) \neq 0$, et donc $E(y) = 0$. Il s'ensuit que $v_1 \in \{p, +\infty\}$. Clairement la seule façon de concilier les contraintes que l'on vient d'obtenir est d'avoir $v_i = +\infty$ pour tout i, c'est-à-dire $A(u) = u^d$. Mais, ce cas n'est pas non plus possible car $A^\sigma(u) = u^{pd}$ ne divise manifestement pas $A(u)E(u)^m = u^d E(u)^m$ si d est strictement positif. Ainsi se termine donc la démonstration de la proposition 3.1.

3.1.3 L'apport des (φ,τ)-modules

La théorie des (φ,τ)-modules, qui a été développée dans cet article, fournit des objets qui s'insèrent de façon très naturelle dans le diagramme (3.1) et permet de le compléter de façon satisfaisante. C'est ce que nous nous proposons de présenter dans ce paragraphe. Plus précisément, nous allons construire le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Rep}^{\mathrm{st}}_{[0,+\infty[}(G_K) \arrow[r, hook] \arrow[d, "\mathcal{K}"', "\sim"] & \mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_K) \arrow[r, "\mathrm{res}"] & \mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_\infty) \\
\mathrm{Mod}^{\varphi,N_\nabla,0}_{/\mathcal{O}} \arrow[r, "\mathcal{R}_{\varphi,\tau}"] \arrow[rr, bend right, "\mathcal{R}_\varphi"'] & \mathrm{Mod}^{\varphi,\tau}_{/\mathfrak{S}} \otimes \mathbb{Q}_p \arrow[u, "\sim", "\mathcal{T}_{\varphi,\tau}"'] \arrow[r, "\text{oubli de } \tau"] & \mathrm{Mod}^{\varphi}_{/\mathfrak{S}} \otimes \mathbb{Q}_p \arrow[u, "\sim", "\mathcal{T}_\varphi"']
\end{tikzcd} \tag{3.2}$$

Les notations $\mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_K)$ et $\mathrm{Mod}^{\varphi,\tau}_{/\mathfrak{S}}$ qui apparaissent dans le diagramme (3.2) font respectivement référence à la catégorie des représentations de G_K de $E(u)$-hauteur finie et à celle des (φ,τ)-réseaux libres sur $\mathfrak{S}$ de $E(u)$-hauteur finie. Le foncteur $\mathcal{T}_{\varphi,\tau}$, quant à lui, est celui qui fait correspondre à un (φ,τ)-réseau $\mathfrak{M}$ de $E(u)$-hauteur finie la représentation de G_K associée au (φ,τ)-module $\mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$. Le diagramme (3.2) indique que c'est une équivalence de catégories, ce qui est effectivement le cas :

Proposition 3.3. *Les foncteurs $\mathcal{T}_\varphi$ et $\mathcal{T}_{\varphi,\tau}$ sont des équivalences de catégorie.*

Démonstration. La pleine fidélité de deux foncteurs suit de la proposition 3.1. L'essentielle surjectivité de $\mathcal{T}_\varphi$ est vraie par définition des représentations de $E(u)$-hauteur finie. Il ne reste donc qu'à démontrer l'essentielle surjectivité de $\mathcal{T}_{\varphi,\tau}$, et il suffit pour cela de justifier que si $\mathfrak{M}$ est un φ-réseau libre sur $\mathfrak{S}$, de $E(u)$-hauteur finie, dans un (φ,τ)-module sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}^{\mathrm{int}}_\tau)$, alors $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ est automatiquement stable par τ. On adapte pour ce faire l'argumentation présentée dans la démonstration du lemme 2.23. On se donne $\mathfrak{M}$ comme précédemment, et on pose :

$$\mathfrak{M}' = (\mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}) \cap \tau^{-1}(\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$$

l'intersection étant calculée dans $W(L) \otimes_{\mathfrak{S}} \mathfrak{M}$. Soit $\mathrm{pr} : W(L) \otimes_{\mathfrak{S}} \mathfrak{M} \to L \otimes_{\mathfrak{S}} \mathfrak{M}$ le morphisme canonique déduit de la réduction modulo p. L'image de $\mathfrak{A} = (\mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M})$ sous pr s'identifie à $F_0 \otimes_{\mathfrak{S}} \mathfrak{M}$, vu de façon canonique comme un sous-espace de $L \otimes_{\mathfrak{S}} \mathfrak{M}$. De même, l'image de $\mathfrak{B} = \tau^{-1}(\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ n'est autre que $\tau^{-1}(F_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ respectivement. On a la suite exacte

$$0 \longrightarrow \mathfrak{M}' \xrightarrow{x \mapsto (x,x)} \mathfrak{A} \oplus \mathfrak{B} \xrightarrow{(x,y) \mapsto x-y} \mathfrak{A} + \mathfrak{B} \longrightarrow 0$$

dont la réduction modulo p s'insère dans la diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{M}'/p\mathfrak{M}' \arrow[r] \arrow[d, "\mathrm{pr}"] & \mathfrak{A}/p\mathfrak{A} \oplus \mathfrak{B}/p\mathfrak{B} \arrow[r] \arrow[d, "\mathrm{pr}\oplus\mathrm{pr}"] & \frac{\mathfrak{A}+\mathfrak{B}}{p(\mathfrak{A}+\mathfrak{B})} \arrow[r] \arrow[d, "\mathrm{pr}"] & 0 \\
0 \arrow[r] & L \otimes_{\mathfrak{S}} \mathfrak{M} \arrow[r, "x \mapsto (x,x)"] & (L \otimes_{\mathfrak{S}} \mathfrak{M}) \oplus (L \otimes_{\mathfrak{S}} \mathfrak{M}) \arrow[r, "(x,y) \mapsto x-y"] & L \otimes_{\mathfrak{S}} \mathfrak{M} \arrow[r] & 0
\end{tikzcd}$$

La suite du haut est exacte à droite par exactitude du produit tensoriel, et on vérifie par ailleurs directement qu'elle est exacte à gauche du fait que $p\mathfrak{M}' = p\mathfrak{A} \cap p\mathfrak{B}$ (ce qui est clair car la multiplication par p sur $W(L) \otimes_{\mathfrak{S}} \mathfrak{M}$ est injective). On obtient de même l'injectivité de la flèche centrale verticale $\mathrm{pr} \oplus \mathrm{pr}$, ce qui implique par une chasse au diagramme l'injectivité de toutes les flèches verticales. Il en résulte que l'on a l'égalité :

$$\mathfrak{M}'/p\mathfrak{M}' = (F_0 \otimes_{\mathfrak{S}} \mathfrak{M}) \cap \tau^{-1}(F_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$$

dans $L \otimes_{\mathfrak{S}} \mathfrak{M}$. Ainsi $(\mathfrak{M}'/p\mathfrak{M}')[1/u] = F_0 \otimes_{\mathfrak{S}} \mathfrak{M}' = F_0 \otimes_{\mathfrak{S}} \mathfrak{M}$, ce qui signifie que le morphisme naturel $f : \mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}' \to \mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$ induit un isomorphisme modulo p. Comme $\mathcal{E}^{\mathrm{int}}$ est complet pour la topologie p-adique, il s'ensuit que f est lui-même un isomorphisme, c'est-à-dire que $\mathfrak{M}'$ est un φ-réseau à l'intérieur de $\mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$. En outre, tout $x \in \mathcal{E}^{\mathrm{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$, qui est tel qu'il existe des entiers n et m tels que $u^n x$ et $p^m x$ soient tous les deux dans $\mathfrak{M}'$, appartient déjà à $\mathfrak{M}'$. On en déduit, grâce au théorème de structure des modules de type fini sur $\mathfrak{S}$, que $\mathfrak{M}'$ est libre sur $\mathfrak{S}$. Par ailleurs, en utilisant que les idéaux principaux engendrés respectivement par $E(u)$ et $\tau(E(u))$ sont conjugués dans $W(R)$, on démontre, de même que dans le lemme 2.23, que $\mathfrak{M}'$ est de $E(u)$-hauteur finie. La proposition 3.1 appliquée à $\mathfrak{M}$ et $\mathfrak{M}'$ entraîne alors l'égalité de ces deux réseaux. Ainsi $\tau(\mathfrak{M}) = \tau(\mathfrak{M}') \subset \mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ comme souhaité. $\square$

On en vient enfin à la construction du foncteur $\mathcal{R}_{\varphi,\tau} : \mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0} \to \mathrm{Mod}_{/\mathfrak{S}}^{\varphi,\tau} \otimes \mathbb{Q}_p$. On considère pour cela $\mathcal{M}$ un objet de $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$, et on fixe un réseau T de $\mathcal{K}^{-1}(\mathcal{M})$ stable par G_K. Soit M le (φ,τ)-module sur $(\mathcal{E}^{\mathrm{int}}, \mathcal{E}_\tau^{\mathrm{int}})$ qui lui est associé. D'après la propriété B, il existe dans M un unique φ-réseau $\mathfrak{M}$ qui est libre sur $\mathfrak{S}$ et de $E(u)$-hauteur finie, et d'après la démonstration de la proposition 3.3, le produit tensoriel $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ est stable par τ. L'objet $\mathfrak{M}$ est donc un (φ,τ)-réseau qui, à cause du choix de T, n'est défini qu'à isogénie près. Autrement dit, c'est un objet de la catégorie $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi,\tau} \otimes \mathbb{Q}_p$, et on peut donc poser $\mathcal{R}_{\varphi,\tau}(\mathcal{M}) = \mathfrak{M}$.

3.2 L'image essentielle du foncteur $\mathcal{R}_{\varphi,\tau}$

3.2.1 Énoncé des résultats

Du diagramme 3.2, il suit immédiatement que $\mathcal{R}_{\varphi,\tau}$ est pleinement fidèle. Se pose alors naturellement la question de décrire son image essentielle. Une première contrainte la concernant résulte de précédents travaux de Liu. Plus précisément, étant donné $\mathfrak{M}$ un objet de $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi,\tau} \otimes \mathbb{Q}_p$, cela a un sens de considérer le produit tensoriel $W \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$. En effet, le morphisme de projection $R \to \bar{k}$ induit par fonctioralité une application $W(R) \to W(\bar{k})$ qui envoie $\mathfrak{S}_\tau$ sur W. Il suit alors des résultats de [19] (voir notamment les formules (2.3.1) et (3.2.1)) que si $\mathfrak{M}$ est dans l'image essentielle de $\mathcal{R}_{\varphi,\tau}$, alors $\mathrm{id} \otimes \tau$ agit sur $W \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ comme l'identité. Le théorème suivant énonce la réciproque, sous une hypothèse technique supplémentaire.

Théorème 3.4. *Soit $\mathfrak{M}$ un objet de $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi,\tau} \otimes \mathbb{Q}_p$. Les trois conditions suivantes sont équivalentes :*

1. *l'objet $\mathfrak{M}$ est dans l'image essentielle de $\mathcal{R}_{\varphi,\tau}$*
2. *l'opérateur* $\mathrm{id} \otimes \tau$ *agit trivialement sur* $W \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$
3. *l'opérateur* $\mathrm{id} \otimes \tau$ *agit trivialement sur* $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$.

Ce théorème sera démontré dans le §3.2.2 sous l'hypothèse technique supplémentaire $W[1/p](\pi^p) = K$ (qui permet d'éviter d'avoir recours à la théorie de Breuil) et dans le cas général dans le §3.2.3. Donnons pour l'instant quelques unes de ses conséquences. La situation la plus favorable est celle où le corps K ne contient pas de racines primitives p-ièmes de l'unité (ce qui se produit, par exemple, dès que $e < p-1$). On a, dans ce cas, le corollaire suivant.

Corollaire 3.5. *On suppose que K ne contient pas de racines primitives p-ièmes de l'unité. Alors le foncteur $\mathcal{R}_{\tau,\varphi}$ est essentiellement surjectif.*

Démonstration. Soit $\mathfrak{M}$ un objet de $\mathrm{Mod}_{/\mathfrak{S}}^{\varphi,\tau} \otimes \mathbb{Q}_p$. L'hypothèse sur K assure qu'il existe dans G_K un élément γ tel que $\chi(\gamma)-1$ soit de valuation nulle. La relation (1.6) qui apparaît dans la définition des (φ,τ)-modules implique alors que $\tau^{\chi(\gamma)-1}$ agit trivialement sur $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$. Par ailleurs, étant donné que la suite des τ^{p^s} tend vers l'identité, il existe un exposant s tel que l'action de τ^{p^s} sur $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ soit triviale. Comme la différence $\chi(\gamma) - 1$ est un nombre premier avec p, on en déduit que τ agit aussi trivialement sur $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$. La conclusion en résulte grâce au théorème 3.4. $\square$

Le résultat du corollaire 3.5 n'est plus vrai si K contient une racine primitive p-ième de l'unité. Il n'est pas nécessaire d'aller chercher loin un contre-exemple, puisque $K = \mathbb{Q}_p(\zeta_p)$ convient déjà. En effet, l'extension K_1/K est alors galoisienne de groupe de Galois cyclique de cardinal p. Notons T la représentation régulière sur $\mathbb{Q}_p$ de $\mathrm{Gal}(K_1/K)$; c'est aussi une représentation de G_K puisque $\mathrm{Gal}(K_1/K)$ en est un quotient. En restriction à G_∞, cette représentation est triviale, ce qui indique que le φ-module qui lui est associé est, lui aussi, trivial. Ce cas relève donc du premier exemple traité dans le §1.3.3. Des résultats de ce numéro, il suit que τ agit sur $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ de la même façon qu'il agit sur T, et donc en tout cas non trivialement. En particulier, la représentation T n'est pas dans l'image de $\mathcal{R}_{\varphi,\tau}$.

Enfin, si l'on retourne un instant voir le diagramme (3.2), il apparaît clairement que les résultats précédents permettent de caractériser l'image essentielle du foncteur d'inclusion $\mathrm{Rep}^{\mathrm{st}}_{[0,+\infty[}(G_K) \to \mathrm{Rep}^{E(u)}_{[0,+\infty[}(G_K)$, c'est-à-dire de donner un critère pour reconnaître parmi les représentations de $E(u)$-hauteur finie celles qui sont semi-stables. Lorsque les hypothèses du corollaire 3.5 sont satisfaites, ce critère disparaît même et l'on obtient ainsi le théorème 3 de l'introduction pour $s = 0$. Pour les s supérieurs, il suffit de remplacer partout dans la démonstration du théorème 3.4 (voir §3.2.2 ci-après) et du corollaire 3.5 l'opérateur τ par τ^{p^s}.

3.2.2 Démonstration du théorème 3.4 lorsque $W[1/p](\pi^p) = K$

Comme le titre l'indique, on suppose dans ce numéro que l'uniformisante π est telle que π^p engendre K sur le corps $W[1/p]$. On a déjà vu que la première condition du théorème 3.4 implique la deuxième, et il est clair que la deuxième implique la troisième. Il ne reste donc plus qu'à démontrer que la troisième implique la seconde comme suit. Soit $\mathfrak{M}$ un (φ, τ)-réseau pour lequel $\mathrm{id} \otimes \tau$ agit trivialement sur $k \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$. Pour simplifier les notations, on note f l'endormorphisme W-linéaire $\mathrm{id} \otimes \tau^{p^s}$ de $W \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$. Par hypothèse, on a donc $f \equiv \mathrm{id} \pmod p$. Par ailleurs, si on considère un entier s tel qu'il existe un élément γ dans G_∞ avec $\chi(\gamma) \equiv 1 \pmod{p^s}$, les arguments de la démonstration du corollaire 3.5 impliquent que $f^{p^s} \equiv \mathrm{id} \pmod{p^n}$ pour tout entier n, c'est-à-dire que $f^{p^s} = \mathrm{id}$. Or, si l'on suppose que f n'est pas l'identité, on peut l'écrire sous la forme $\mathrm{id} + p^n g$ où n est un entier supérieur ou égal à 1 et g un endomorphisme de $W \otimes_{\mathfrak{S}_\tau} (\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M})$ non divisible par p. On a alors

$$\mathrm{id} = f^{p^s} = (\mathrm{id} + p^n g)^{p^s} \equiv \mathrm{id} + p^{ns} g^{p^s} \pmod{p^{ns+1}},$$

d'où il résulte que g est divisible par p. C'est une contradiction de laquelle on déduit que f est l'identité.

Il ne reste donc plus qu'à démontrer que la deuxième condition du théorème 3.4 implique la première. On remarque tout d'abord qu'étant donné que les éléments de G_∞ agissent trivialement sur $\mathfrak{M}$, on peut supposer, quitte à composer τ par un tel élement, que $\chi(\tau) = 1$ (on rappelle qu'un tel élément existe toujours par le lemme 5.1.2 de [17] et qu'il s'écrit sous la forme $\tau \circ g$, avec $g \in G_\infty$ par le lemme 1.2 de cet article). On fixe un (φ, τ)-réseau $\mathfrak{M}$ libre sur $\mathfrak{S}$ qui vérifie la troisième condition du théorème, et on cherche à construire un objet $\mathcal{M}$ de $\mathrm{Mod}^{\varphi, N_\nabla, 0}_{/\mathcal{O}}$ dont l'image par $\mathcal{R}_{\varphi,\tau}$ est isogène à $\mathfrak{M}$. La définition du foncteur $\mathcal{R}_{\varphi,\tau}$ conduit à poser simplement $\mathcal{M} = \mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$ pour définir sa structure de $\mathcal{O}$-module, et à munir celui-ci du Frobenius $\varphi \otimes \varphi$. Ne reste donc plus qu'à définir l'opérateur N_∇. La discussion menée dans le §5.1 de [17] montre que celui-ci doit s'obtenir *via* la formule :

$$N_\nabla = \frac{1}{p\mathfrak{t}} \cdot \log \tau = \frac{1}{p\mathfrak{t}} \cdot \sum_{i=1}^{\infty} \frac{(\mathrm{id} - \tau)^i}{i}.$$

Toutefois, il n'est pas clair que cette formule ait un sens puisque aussi bien la division par $\mathfrak{t}$ que la convergeance de la somme posent *a priori* problème. Nous allons démontrer dans la suite que ce n'est pas le cas, puis que l'opérateur N_∇ ainsi obtenu est défini sur $\mathcal{O}$. Lors de la démonstration, nous allons être amené à introduire un certain nombre de modules sur $\mathfrak{S}$; pour donner au lecteur une vision d'ensemble de la situation, nous les avons regroupé dans le diagramme de la figure (2).

Construction du logarithme de τ Justifier l'existence de $\log \tau$ revient à démontrer que la série de terme général $\frac{(\mathrm{id}-\tau)^i}{i}$ converge. En réalité, si l'on s'autorise à considérer des espaces suffisamment grands, la convergence s'obtient sans grande difficulté. En effet, étant donné que par hypothèse $\mathrm{id} \otimes \tau$ agit trivialement sur $\mathfrak{M}/u\mathfrak{M}$, il existe un élément $Z \in W(\mathfrak{m}_R)$ tel que $\tau(x) - x \in Z\, W(\mathfrak{m}_R) + p\, W(\mathfrak{m}_R)$ pour tout $x \in W(R) \otimes_{\mathfrak{S}} \mathfrak{M}$. On peut en outre supposer que Z n'est pas multiple de p. Étant donné que l'idéal $Z\, W(\mathfrak{m}_R) + p\, W(\mathfrak{m}_R)$ est stable par τ, on en déduit que

$$(\tau - \mathrm{id})^i(\mathfrak{M}) \subset \left(\sum_{j=0}^{i} p^{i-j} Z^j W(\mathfrak{m}_R) \right) \otimes_{\mathfrak{S}} \mathfrak{M}$$

puis que, pour tout $x \in \mathfrak{M}$, la série $\sum_{i \geqslant 1} \frac{(\tau - \mathrm{id})^i}{i}(x)$ converge dans l'espace $W(R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$ où, par définition, $W(R)[Z/p]^\wedge$ est le complété p-adique de l'anneau quotient $W(R)[Z']/(pZ' - Z)$. En examinant plus précisément les dénominateurs, on s'aperçoit même que $(\log \tau)(\mathfrak{M}) \subset W(\mathfrak{m}_R)^{Z\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$ où $W(\mathfrak{m}_R)^{Z\text{-dp}}$ est l'adhérence dans $W(R)[Z/p]^\wedge$ du $W(R)$-module $\sum_{m \geqslant 0} \frac{Z^{p^m}}{p^m} W(\mathfrak{m}_R)$.

$$
\begin{tikzcd}
\mathcal{O} & & & & & & \\
 & \mathcal{E}^{\mathrm{int},\nu\text{-dp}} \arrow[r, hook] & \mathcal{E}^{\mathrm{int},\varphi^{-n},\nu\text{-dp}} \arrow[r, hook] & \mathcal{E}^{\mathrm{int},\mathrm{perf},\nu\text{-dp}} \arrow[rr, hook, "\times\mathfrak{t}"] & & W(L)^{Z\text{-dp}} & \\
\mathfrak{S}^{\nu\text{-dp}} \arrow[uu, hook] \arrow[ur, hook] \arrow[rrrr, hook, "\times\mathfrak{t}"] & & & & W(\mathfrak{m}_R)^{Z\text{-dp}} \arrow[ur, hook] \arrow[rr, hook] & & W(R)[Z/p]^\wedge \\
 & \mathcal{E}^{\mathrm{int}} \arrow[uu, hook] \arrow[rrrr, hook, "\times\mathfrak{t}"] & & & & W(L) \arrow[uu, hook] & \\
\mathfrak{S} \arrow[uu, hook] \arrow[ur, hook] \arrow[rrrr, hook, "\times\mathfrak{t}"] & & & & W(\mathfrak{m}_R) \arrow[uu, hook] \arrow[ur, hook] & &
\end{tikzcd}
$$

FIGURE 2 – Divers $\mathfrak{S}$-modules intervenant dans la démonstration du théorème 3.4

La stratégie de la preuve est la suivante. Le logarithme de τ est tout d'abord construit dans l'anneau $W(R)[Z/p]^\wedge$. On montre ensuite qu'il redescend à $\mathcal{O}$ en empruntant le chemin suivant : $W(\mathfrak{m}_R)^{Z\text{-dp}}$, $W(L)^{Z\text{-dp}}$, $\mathcal{E}^{\mathrm{int},\mathrm{perf},\nu\text{-dp}}$, $\mathcal{E}^{\mathrm{int},\nu\text{-dp}}$, $\mathfrak{S}^{\nu\text{-dp}}$ et enfin $\mathcal{O}$.

Il est à noter que le module $W(\mathfrak{m}_R)^{Z\text{-dp}}$ est stable à la fois par φ et G_∞. En effet, $\varphi(Z)$ s'écrit sous la forme $aZ + pb$ avec $a, b \in W(\mathfrak{m}_R)$ et on a alors $\frac{\varphi(Z)^{p^m}}{p^m} \equiv a^{p^m} \cdot \frac{Z^{p^m}}{p^m} \pmod{pW(\mathfrak{m}_R)}$ à partir de quoi on déduit que $\frac{\varphi(Z)^{p^m}}{p^m} \in W(\mathfrak{m}_R)^{Z\text{-dp}}$, puis la stabilité de $W(\mathfrak{m}_R)^{Z\text{-dp}}$ par φ. La stabilité par G_∞, quant à elle, se démontre de manière analogue.

La suite de la démonstration consiste à borner, par étapes successives, l'image de l'application $\log\tau$ définie sur $\mathfrak{M}$ jusqu'à parvenir finalement à prouver qu'elle est incluse dans $\mathfrak{t}\mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$. Ceci nous permettra de définir N_∇ comme nous l'avons indiqué précédemment, puis de conclure.

Un argument galoisien Le premier argument utilisé pour restreindre l'image de $\log\tau$ met à profit la relation de commutation (1.6) qui apparaît dans la définition des (φ,τ)-modules. Étant donné que $\chi(\tau) = 1$, celle-ci s'écrit simplement $\tau^{\chi(g)} = (g \otimes \mathrm{id}) \circ \tau \circ (g \otimes \mathrm{id})^{-1}$ (pour $g \in G_\infty/H_\infty$), l'égalité ayant lieu dans l'espace des endomorphimes de $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$. En prenant le logarithme, on obtient, pour tout $x \in \mathfrak{M}$, la relation

$$\chi(g) \cdot (\log\tau)(x) = (g \otimes \mathrm{id}) \circ (\log\tau) \circ (g \otimes \mathrm{id})^{-1}(x) = (g \otimes \mathrm{id}) \circ (\log\tau)(x),$$

l'égalité ayant cette fois-ci lieu *a priori* dans $W(R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$. Il s'ensuit que $(\log\tau)(x)$ appartient à l'ensemble

$$\left\{\, x \in W(\mathfrak{m}_R)^{Z\text{-dp}} \quad | \quad g(x) = \chi(g)x,\ \forall g \in G_\infty \,\right\}.$$

On est ainsi amené à étudier cet ensemble précédent. Pour cela, on rappelle que l'on avait posé $L = \mathrm{Frac}\, R$. On définit le $W(R)$-module $W(L)^{Z\text{-dp}}$ comme la somme amalgamée de $W(L)$ et $W(\mathfrak{m}_R)^{Z\text{-dp}}$ au-dessus de $W(\mathfrak{m}_R)$. Il est important de noter que l'élément Z considéré jusqu'à présent est inversible dans $W(L)$, étant donné qu'il n'est pas multiple de p dans $W(R)$. Les actions de G_∞ et de φ s'étendent naturellement à $W(L)^{Z\text{-dp}}$. On pose $\nu = v_R(Z \bmod p)$; c'est un nombre rationnel strictement positif. Soient encore $|\cdot|_p$ la norme sur $W[1/p]$ normalisée par $|p|_p = \frac{1}{p}$ et $\mathcal{E}^{\mathrm{int},\mathrm{perf},\nu\text{-dp}}$ l'espace des séries formelles de la forme

$$\sum_{q \in \mathbb{Z}[1/p]} a_q u^q, \qquad a_q \in W[1/p]$$

vérifiant les conditions de convergence suivantes :

a) pour tout $q \in \mathbb{Z}[1/p]$, on a $|a_q|_p < \max(p, \frac{e+q(p-1)}{\nu(p-1)})$;
b) le coefficient a_q tend vers 0 lorsque q tend vers $-\infty$;
c) pour tout $\varepsilon > 0$, l'ensemble des $q \in \mathbb{Z}[1/p]$ tels que $|a_q|_p > \varepsilon$ est discret [10].

10. Avec la condition précédente, cela revient à dire qu'il intersecte tous les intervalles $]-\infty, A]$ selon un ensemble fini.

On peut reformuler la première condition de façon peut-être plus parlante comme suit : si $s : \mathbb{N} \to \mathbb{R} \cup \{-\infty\}$ est la fonction définie par $s(0) = -\infty$ et $s(m) = p^m \nu - \frac{e}{p-1}$ si $m \geqslant 1$, elle dit exactement que le coefficient a_q est dans $p^{-m} W$ lorsque q est dans l'intervalle $]s(m), s(m+1)]$. On en déduit la description suivante du quotient $\mathcal{E}^{\text{int,perf},\nu\text{-dp}} / \mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ donnée par le lemme suivant :

Lemme 3.6. *Soit F_0^{perf} l'adhérence dans $L = \operatorname{Frac} R$ du perfectisé de F_0 et, pour tout élément $v \in \mathbb{R} \cup \{-\infty\}$, soit $\mathfrak{a}_{F_0^{\text{perf}}}^{>v}$ l'ensemble des éléments de F_0^{perf} de valuation strictement supérieure à v. Alors on a un isomorphisme canonique :*

$$\prod_{m=0}^{\infty} \frac{\mathfrak{a}_{F_0^{\text{perf}}}^{>s(m)}}{\mathfrak{a}_{F_0^{\text{perf}}}^{>s(m+1)}} \overset{\sim}{\longrightarrow} \frac{\mathcal{E}^{\text{int,perf},\nu\text{-dp}}}{p\, \mathcal{E}^{\text{int,perf},\nu\text{-dp}}}.$$

Démonstration. La clé consiste à remarquer que F_0^{perf} s'identifie à l'ensemble des séries $\sum_{q \in \mathbb{Z}[1/p]} a_q u^q$ telles que $a_q \in W$ pour tout q et satisfaisant aux conditions b) et c) mentionnées précedemment et que, sous cette identification, $\mathfrak{a}_{F_0^{\text{perf}}}^{>v}$ correspondant aux séries pour lesquelle $a_q = 0$ pour tout $q \leqslant v$. Le morphisme qui apparaît dans l'énoncé du lemme est alors celui qui envoie une famille $(P_m)_{m \geqslant 0}$ sur la somme $\sum_{m \geqslant 0} p^{-m} P_m$ (calculée dans $\mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ avant d'être réduite modulo p bien entendu). Le fait qu'il soit bien défini et qu'il réalise un isomorphisme entre les espaces considérées est enfin une vérification immédiate. ☐

Les conditions a), b) et c) assurent par ailleurs que l'association $\sum_q a_q u^q \mapsto \mathfrak{t} \sum_q a_q [\underline{\pi}^q]$ définit un morphisme (injectif) $\mathcal{E}^{\text{int,perf},\nu\text{-dp}} \to W(L)^{Z\text{-dp}}$. Dans la suite, son image sera notée $\mathfrak{t}\mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ ou $\mathcal{E}^{\text{int,perf},\nu\text{-dp}}(1)$, tandis que l'image d'un élément $x \in \mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ sera notée simplement $\mathfrak{t}x$.

Lemme 3.7. *Les éléments de $\mathcal{E}^{\text{int,perf},\nu\text{-dp}}(1)$ sont exactement les $x \in W(L)^{Z\text{-dp}}$ tels que $g(x) = \chi(g)x$ pour tout $g \in G_\infty$.*

Démonstration. Soit X l'ensemble des $x \in W(L)^{Z\text{-dp}}$ tels que $g(x) = \chi(g)x$ pour tout $g \in G_\infty$. Étant donnéG_∞ agit trivialement sur les éléments $[\underline{\pi}^q]$ et par la formule $g(\mathfrak{t}) = \chi(g)\mathfrak{t}$ sur l'élément $\mathfrak{t}$, il est clair que si $x \in \mathcal{E}^{\text{int,perf},\nu\text{-dp}}(1)$ alors $g(x) = \chi(g)x$ pour tout $g \in G_\infty$, c'est-à-dire que $\mathcal{E}^{\text{int,perf},\nu\text{-dp}}(1) \subset X$. Comme ces deux derniers espaces sont complets pour la topologie p-adique, il suffit pour conclure de montrer que l'inclusion précédemment trouvée induit un isomorphisme modulo p. On considère la composée :

$$f : \frac{\mathcal{E}^{\text{int,perf},\nu\text{-dp}}}{p\, \mathcal{E}^{\text{int,perf},\nu\text{-dp}}} \to X/pX \to \left\{ y \in \frac{W(L)^{Z\text{-dp}}}{p\, W(L)^{Z\text{-dp}}} \;\middle|\; g(y) = \chi(g)y,\ \forall g \in G_\infty \right\}.$$

Le second morphisme étant clairement injectif, il suffit de montrer que f est bijectif. Le lemme 3.6 donne une description de l'espace de départ de f et, par un argument analogue, on obtient une description du quotient $\frac{W(L)^{Z\text{-dp}}}{p\, W(L)^{Z\text{-dp}}}$ qui s'écrit comme suit :

$$\prod_{m=0}^{\infty} \frac{\mathfrak{a}_L^{>s(m)}}{\mathfrak{a}_L^{>s(m+1)}} \overset{\sim}{\longrightarrow} \frac{W(L)^{Z\text{-dp}}}{p\, W(L)^{Z\text{-dp}}}$$

où la flèche provient, cette fois-ci, de la multiplication par $\mathfrak{t}$. *Via* ces isomorphismes, l'application f n'est autre que l'inclusion canonique

$$\prod_{m=0}^{\infty} \left(\frac{\mathfrak{a}_L^{>s(m)}}{\mathfrak{a}_L^{>s(m+1)}} \right)^{G_\infty} \longrightarrow \prod_{m=0}^{\infty} \frac{\mathfrak{a}_{F_0^{\text{perf}}}^{>s(m)}}{\mathfrak{a}_{F_0^{\text{perf}}}^{>s(m+1)}},$$

et la deuxième partie de la proposition 1.13 montre finalement qu'il s'agit bien d'une bijection. ☐

Il résulte du lemme que la formule $\frac{\log \tau}{p\mathfrak{t}}$ définit une application $N_\nabla : \mathfrak{M} \to \frac{1}{p} \cdot \mathcal{E}^{\text{int,perf},\nu\text{-dp}} \otimes \mathfrak{M}$.

Vérification de deux relations L'ensemble d'arrivée que nous venons d'obtenir pour l'opérateur N_∇ est encore largement plus grand que ce qui avait été annoncé, mais avant de continuer à le réduire, nous allons démontrer que N_∇ satisfait aux deux relations qui apparaissent dans la définition des objets de $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$, à savoir la formule de Leibniz, qui s'écrit maintenant [11] :

$$\forall a \in \mathfrak{S},\ \forall x \in \mathfrak{M}, \quad N_\nabla(ax) = N_\nabla(a) \otimes x + aN_\nabla(x) \tag{3.3}$$

et la relation de commutation avec φ, qui s'écrit maintenant :

$$\forall x \in \mathfrak{M}, \quad N_\nabla \circ \varphi(x) = p \cdot \frac{E(u)}{E(0)} \cdot (\varphi \otimes \varphi) \circ N_\nabla(x) = U \cdot (\varphi \otimes \varphi) \circ N_\nabla(x) \tag{3.4}$$

où l'opérateur φ agissant sur $\mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ envoie $\sum_q a_q u^q$ sur $\sum_q \sigma(a_q) u^{pq}$, la lettre σ désignant le Frobenius classique sur $W[1/p]$. Par linéarité et passage à la limite, il suffit de démontrer la relation de Leibniz lorsque $a = u^q$ pour un entier positif q. On écrit :

$$(\mathrm{id} - \tau)^i (u^q x) = \sum_{j=1}^{i} \binom{i}{j} (-1)^j \tau^j (u^q x) = \sum_{j=1}^{i} \binom{i}{j} (-1)^j [\underline{\varepsilon}]^{qj} u^q \tau^j(x) = u^q \cdot (\mathrm{id} - [\underline{\varepsilon}]^q \tau)^i(x),$$

d'où on déduit les égalités suivantes dans $W(\mathfrak{m}_R)^{Z\text{-dp}}$:

$$\log \tau(u^q x) = u^q \cdot \log([\underline{\varepsilon}]^q \tau)(x) = q u^q \cdot \log([\underline{\varepsilon}]) x + u^q \cdot \log \tau(x) = q u^q t \cdot x + u^q \cdot \log \tau(x).$$

La formule attendue s'ensuit finalement en divisant par $p\mathfrak{t}$ et en se rappelant que $\varphi(\mathfrak{t}\lambda) = -t = -\varphi(t/p)$, *i.e.* $\frac{t}{p\mathfrak{t}} = -\lambda$. Enfin, la relation de commutation avec φ résulte directement du fait que $\log \tau$ et φ commutent, ce qui est vrai car φ et τ commutent par hypothèse.

Élimination des puissances fractionnaires Nous revenons à notre problématique consistant à restreindre l'image de $\log \tau$. Soit $\mathcal{E}^{\text{int},\varphi^{-n},\mu\text{-dp}}$ le sous-espace de $\mathcal{E}^{\text{int,perf},\mu\text{-dp}}$ formé des séries $\sum_q a_q u^q$ pour lesquelles $a_q = 0$ dès que $p^n q$ n'est pas un entier. On note simplement $\mathcal{E}^{\text{int},\mu\text{-dp}}$ au lieu de $\mathcal{E}^{\text{int},\varphi^{-0},\mu\text{-dp}}$, et on se propose dans ce paragraphe de démontrer que $N_\nabla(\mathfrak{M})$ est inclus dans $\frac{1}{p} \cdot \mathcal{E}^{\text{int},\mu\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$. Étant donné Q et N des nombres entiers positifs, on appelle $I_{Q,N}$ le sous-$\mathfrak{S}$-module de $\mathcal{E}^{\text{int,perf},\mu\text{-dp}}$ formé des séries $\sum_q a_q u^q$ pour lesquelle $v_p(a_q) \geqslant N$ pour tout $q < Q$. On a alors le lemme suivant, qui est la clé de la preuve.

Lemme 3.8. *Soient Q et N deux entiers positifs avec $Q \geqslant N + e$. Soit $x \in \mathcal{E}^{\text{int,perf},\mu\text{-dp}}$ tel que $Ux \in I_{Q,N}$. Alors $x \in I_{Q-N-e,N}$.*

Démonstration. Par définition, l'élément U s'écrit sous la forme $\alpha u^e + pF(u)$ où α est un élément inversible de W et où F est un polynôme à coefficients dans W. On en déduit que U est inversible dans $W(L)$ et que son inverse s'écrit sous la forme $U^{-1} = \sum_{n \geqslant 0} \frac{p^n a_n}{u^{e(n+1)}}$ où les a_n sont des éléments de W. Ainsi, si on suppose que $y = Ux$ est élément de $I_{Q,N}$, on en déduit que $x = U^{-1} y$ est dans l'adhérence de $\sum_{n \geqslant 0} p^n u^{-e(n+1)} I_{Q,N}$, et donc en particulier dans $I_{Q-N-e,N}$ comme annoncé. ☐

Par hypothèse, il existe un entier h tel que le φ-réseau $\mathfrak{M}$ est de U-hauteur $\leqslant h$. Soit (Q, N) un couple d'entiers positifs tels que $(p-1)Q \geqslant (N+e)h$. De la troisième condition de convergence imposée dans la définition de $\mathcal{E}^{\text{int,perf},\mu\text{-dp}}$, on déduit que, pour tout $x \in \mathcal{E}^{\text{int,perf},\mu\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$, il existe un entier n tel que $x \in (\mathcal{E}^{\text{int},\varphi^{-n},\mu\text{-dp}} + I_{Q,N}) \otimes_{\mathfrak{S}} \mathfrak{M}$. Étant donné, d'une part, la relation de Leibniz (3.3) et, d'autre part, le fait que $\mathfrak{M}$ est un $\mathfrak{S}$-module de type fini, on obtient l'existence d'un entier $n > 0$ tel que :

$$pN_\nabla(\mathfrak{M}) \subset (\mathcal{E}^{\text{int},\varphi^{-n},\mu\text{-dp}} + I_{Q,N}) \otimes_{\mathfrak{S}} \mathfrak{M}. \tag{3.5}$$

Soit $x \in \mathfrak{M}$. Le fait que $\mathfrak{M}$ soit de U-hauteur $\leqslant h$ implique que $U^h x$ s'écrit comme une somme de $a_i \varphi(x_i)$ avec $a_i \in \mathfrak{S}$ et $x_i \in \mathfrak{M}$. En appliquant la relation (3.4) avec $x = x_i$, on obtient

$$pN_\nabla \circ \varphi(x_i) = U \cdot (\varphi \otimes \varphi) \circ N_\nabla(x_i) \in (\mathcal{E}^{\text{int},\varphi^{-n+1},\mu\text{-dp}} + I_{pQ,N}) \otimes_{\mathfrak{S}} \mathfrak{M}.$$

11. On remarquera que, quitte à modifier Z, on peut supposer que $\nu < e$ de sorte que $N_\nabla(a) \in \frac{1}{p} \cdot \mathcal{E}^{\text{int,perf},\nu\text{-dp}}$ pour tout $a \in \mathfrak{S}$.

On en déduit que $pU^h N_\nabla(x)$ est lui aussi élément de $(\mathcal{E}^{\text{int},\varphi^{-n+1},\mu\text{-dp}} + I_{pQ,N}) \otimes_{\mathfrak{S}} \mathfrak{M}$. Une application itérée du lemme 3.8 montre que $pN_\nabla(x)$ appartient à $(\mathcal{E}^{\text{int},\varphi^{-n+1},\mu\text{-dp}} + I_{pQ-(N+e)h,N}) \otimes_{\mathfrak{S}} \mathfrak{M}$ qui, d'après l'inégalité supposée sur Q et N, est inclus dans $(\mathcal{E}^{\text{int},\varphi^{-n+1},\mu\text{-dp}} + I_{Q,N}) \otimes_{\mathfrak{S}} \mathfrak{M}$. Autrement dit, on vient de démontrer que l'inclusion (3.5) est encore valable si l'on remplace n par $n-1$. En itérant l'argument, on montre qu'elle reste valable lorsque $n = 0$, c'est-à-dire que l'on a $pN_\nabla(\mathfrak{M}) \subset (\mathcal{E}^{\text{int},\mu\text{-dp}} + I_{Q,N}) \otimes_{\mathfrak{S}} \mathfrak{M}$. En prenant l'intersection sur tous les couples (Q,N) valides, on en déduit la propriété que l'on souhaitait démontrer.

Élimination des puissances négatives Soit $\mathfrak{S}^{\mu\text{-dp}}$ le sous-espace de $\mathcal{E}^{\text{int},\mu\text{-dp}}$ formé des séries $\sum_q a_q u^q$ (avec $q \in \mathbb{Z}$) pour lesquelles $a_q = 0$ dès que q est strictement négatif. Le but de ce paragraphe est de démontrer que, sous l'hypothèse $W[1/p](\pi^p) = K$ (que l'on a pour l'instant pas encore utilisée), on a $N_\nabla(\mathfrak{M}) \subset \frac{1}{p}\mathfrak{S}^{\mu\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$.

Lemme 3.9. *L'élement* $\mathfrak{t}$ *appartient à* $W(\mathfrak{m}_R)$.

Démonstration. Il s'agit de démontrer que l'image $\bar{\mathfrak{t}}$ de $\mathfrak{t}$ dans $W(\bar{k})$ est nulle. Or, en réduisant l'équation $\varphi(\mathfrak{t}) = U\mathfrak{t}$ dans $W(\bar{k})$, on trouve $\sigma(\bar{\mathfrak{t}}) = p\bar{\mathfrak{t}}$ où σ désigne le Frobenius naturel sur $W(\bar{k})$. En prenant les valuations, on obtient $v_K(\bar{\mathfrak{t}}) = v_K(\bar{\mathfrak{t}}) + 1$, ce qui n'est possible que si $\bar{\mathfrak{t}}$ est nul. $\square$

Lemme 3.10. *On suppose* $W[1/p](\pi^p) = K$. *Alors, l'ensemble des éléments* $x \in \mathcal{E}^{\text{int},\mu\text{-dp}}$ *tels que* $\mathfrak{t}x \in W(\mathfrak{m}_R)^{Z\text{-dp}}$ *est exactement* $\mathfrak{S}^{\mu\text{-dp}}$.

Démonstration. Puisque $\mathcal{E}^{\text{int},\mu\text{-dp}}/\mathfrak{S}^{\mu\text{-dp}} = \mathcal{E}^{\text{int}}/\mathfrak{S}$, il suffit de démontrer que $\mathfrak{S}$ s'identifie à l'ensemble $\mathfrak{S}'$ des éléments x de $\mathcal{E}^{\text{int}}$ tels que $\mathfrak{t}x \in W(\mathfrak{m}_R)$. La démonstration suit alors d'assez près l'argumentation qui a été donnée à la fin du §2.1.2 pour démontrer que $\mathbb{Z}_p(-1)$ n'est pas de $E(u)$-hauteur finie.

L'ensemble des $v_R(x \bmod p)$ pour x parcourant $\mathfrak{S}'$ est clairement minoré par $-\frac{e}{p-1}$; on peut donc considérer un élément $a \in \mathfrak{S}'$ tel que $v_R(a \bmod p)$ soit minimal. Le lemme 3.9 assurant que $1 \in \mathfrak{S}'$, on a de surcroît $v_R(a \bmod p) \leqslant 0$. L'élément a est tel que $a\mathfrak{S} \subset \mathfrak{S}'$, et il est facile de vérifier que cette inclusion induit un isomorphisme modulo p. On en déduit que $\mathfrak{S}' = a\mathfrak{S}$. Par ailleurs, comme $1 \in \mathfrak{S}'$, il existe un élément $b \in \mathfrak{S}$ tel que $ab = 1$. D'après une variante du théorème de préparation de Weierstrass (voir par exemple théorème 2.1, chap. 5 de [15]), b s'écrit comme le produit d'un élément inversible de $\mathfrak{S}$ et d'un polynôme $B \in W[u]$ de la forme $B(u) = u^d + p(b_{d-1}u^{d-1} + \cdots + b_0)$. Ainsi $\mathfrak{S}'$ est aussi le $\mathfrak{S}$-module engendré par $\frac{1}{B(u)}$. De $\frac{1}{B(u)} \in \mathfrak{S}'$, on déduit que $d \leqslant \frac{e}{p-1}$. Pour conclure, il suffit de montrer que $B(u)$ est inversible dans $\mathfrak{S}$, c'est-à-dire que $d = 0$. Si $e < p-1$, la démonstration est donc terminée. Dans le cas général, on procède comme suit. Soit B^σ le polynôme déduit de B en appliquant σ à chacun de ses coefficients. On a l'égalité

$$\mathfrak{t} \cdot \frac{E(u)}{B^\sigma(u^p)} = c \cdot \varphi\Big(\frac{\mathfrak{t}}{B(u)}\Big)$$

qui montre que la fraction $\frac{E(u)}{B^\sigma(u^p)}$ appartient à $\mathfrak{S}'$, et s'écrit donc sous la forme $\frac{C(u)}{B(u)}$ pour une certaine série $C(u) \in \mathfrak{S}$. On en déduit que $B^\sigma(u^p)$ divise le produit $B(u)E(u)$ dans $\mathfrak{S}$. On suppose maintenant par l'absurde que $d > 0$. Les polynômes B et B^σ ont chacun leurs d racines dans l'idéal maximal de $\mathcal{O}_{\bar{K}}$, et les valuations de celles-ci se correspondent deux à deux.

On suppose pour commencer que B admet une racine non nulle. Soient x une racine de B^σ de valuation minimale (parmi toutes les racines de B^σ) et y une racine p-ième de x ; c'est un zéro du polynôme $B^\sigma(u^p)$ qui, par la condition sur les valuations, n'annule pas B. Ainsi, il résulte de la divisibilité que l'on a démontrée précédemment, que $E(y) = 0$. Cela signifie que y et π sont conjugués sur le corps $W[1/p]$, et donc qu'il en est de même de $x = y^p$ et π^p. Comme x est, par hypothèse, annulé par le polynôme B^σ qui est à coefficients dans W et de degré $d \leqslant \frac{e}{p-1}$, on en déduit que l'extension $W[1/p](\pi^p)/W[1/p]$ est de degré au plus $\frac{e}{p-1}$, ce qui est incompatible avec l'hypothèse que nous avons faite.

Reste à traiter le cas où $B(u) = u^d$. Mais alors $B^\sigma(u^p) = u^{pd}$ et il est clair qu'il ne peut diviser $B(u)E(u) = u^d E(u)$ si d est strictement positif. $\square$

Remarque 3.11. Le lemme précédent n'est pas vrai si l'on retire l'hypothèse portant sur π^p. Voici un contre-exemple très simple. On considère le corps $K = \mathbb{Q}_p(\sqrt[p]{-p})$ muni de l'uniformisante $\pi = \sqrt[p]{-p}$. On a alors $e = p$ et le polynôme minimal de π sur $\mathbb{Q}_p$ est $E(u) = u^p + p$. L'élément U est égal à $E(u)$, tandis que $\mathfrak{t}$ vérifie l'équation $\varphi(\mathfrak{t}) = (u^p+p)\mathfrak{t}$. En appliquant φ^{-1} à cette dernière égalité, on obtient $\mathfrak{t} = (u+p)\varphi^{-1}(\mathfrak{t})$.

La fraction $x = \frac{1}{u+p} = \sum_{n=0}^{\infty} \frac{(-1)^n p^n}{u^{n+1}}$ est donc un élément de $\mathcal{E}^{\text{int}}$ tel que $\mathfrak{t}x = \varphi^{-1}(\mathfrak{t}) \in W(\mathfrak{m}_R)$. Pourtant, on n'a manifestement pas $x \in \mathfrak{S}$.

Précédemment, nous avions déjà démontré que $pN_\nabla(\mathfrak{M}) \subset \mathcal{E}^{\text{int},\mu\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$ et que $\log \tau(\mathfrak{M}) = p\mathfrak{t}N_\nabla(\mathfrak{M}) \subset W(\mathfrak{m}_R)^{Z\text{-dp}} \otimes_{\mathfrak{S}} \mathfrak{M}$. Il suit donc du lemme 3.10 que, si l'on suppose $W[1/p](\pi^p) = K$ (comme c'est le cas dans l'énoncé du théorème que l'on veut démontrer), alors $pN_\nabla(\mathfrak{M}) \subset \mathfrak{S}^{\mu\text{-dp}} \otimes \mathfrak{M}$.

La conclusion Comme $\mathfrak{S}^{\mu\text{-dp}} \subset \mathcal{O}$ et que l'anneau $\mathcal{O}$ contient $\frac{1}{p}$ (et est donc stable par division par p), on déduit de ce qui vient d'être prouvé que $N_\nabla(\mathfrak{M}) \subset \mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$. La relation de Leibniz permet de prolonger N_∇ en un endomorphisme de $\mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M} = \mathcal{M}$. De cette façon, on fait de $\mathcal{M}$ un objet de $\text{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$ (les diverses relations de commutations ont déjà été vérifiées). Pour conclure, il ne reste plus qu'à démontrer que $\mathcal{M}$ s'envoie par le foncteur $\mathcal{R}_{\varphi,\tau}$ sur l'objet $\mathfrak{M}$ de départ. Or, le corollaire 3.2.3 et le §5.1 de [17] entraînent que si l'on note τ' l'endomorphisme de $\mathcal{M}$ déduit du N_∇ qui vient d'être construit, l'égalité $\log \tau = \log \tau'$ est vérifiée. En outre, les opérateurs τ et τ' agissent trivialement modulo $W(\mathfrak{m}_R)$. On en déduit qu'il existe un élément $Z \in \mathfrak{S}_\tau$ tel que les séries

$$\exp(\log \tau) = \sum_{i \geqslant 0} \frac{(\log \tau)^i}{i!} \quad \text{et} \quad \exp(\log \tau') = \sum_{i \geqslant 0} \frac{(\log \tau')^i}{i!}$$

convergent dans $W(R)[Z/p]^\wedge$ et que leurs limites valent respectivement τ et τ'. Ainsi les opérateurs τ et τ' agissant sur $W(R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$ sont égaux, d'où on déduit qu'il sont aussi égaux lorsqu'ils s'agissent sur $\mathfrak{S}_\tau \otimes_{\mathfrak{S}} \mathfrak{M}$ puisque ce second espace se plonge dans le premier.

3.2.3 Élimination de l'hypothèse sur π

L'argument que je vais présenter ci-après m'a été suggéré par Tong Liu. En quelques mots, son idée est de ne pas se focaliser sur le (φ, N_∇)-module à la Kisin, mais de plutôt chercher à reconstruire le (φ, N)-module filtré de Fontaine en passant par la théorie de Breuil.

D'un point de vue pratique, la démonstration reste identique jusqu'au lemme 3.10. En fait, le premier argument de la démonstration de ce lemme s'applique encore et montre, en conservant les notations du §3.2.2, que l'ensemble des éléments $x \in \mathcal{E}^{\text{int},\mu\text{-dp}}$ tels que $\mathfrak{t}x \in W(\mathfrak{m}_R)^{Z\text{-dp}}$ est inclus dans $\mathfrak{S}^{\mu\text{-dp}} + \frac{1}{B(u)}\mathfrak{S}$ où $B(u)$ est un polynôme à coefficients dans W, de degré d et congru à u^d modulo p. On en déduit que

$$N_\nabla(\mathfrak{M}) \subset \left(\mathfrak{S}^{\mu\text{-dp}} + \frac{1}{B(u)}\,\mathfrak{S}\right) \otimes_{\mathfrak{S}} \mathfrak{M}. \tag{3.6}$$

Soit S le complété p-adique de l'enveloppe à puissances divisées de $W[u]$ relativement à l'idéal principal engendré par le polynôme $E(u)$. Cet anneau est muni d'un Frobenius noté encore φ et d'un opérateur $N : s \mapsto -u\frac{ds}{du}$. On considère le S-module $\mathcal{M}$ défini par le produit tensoriel $\mathcal{M} = S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$ où l'application $\varphi : \mathfrak{S} \to S$ est celle déduite du Frobenius. On pose encore $\mathcal{D} = \mathcal{M}[1/p]$. Le Frobenius sur $\mathfrak{M}$ s'étend par semi-linéarité à ces deux modules en des opérateurs que l'on note encore φ. L'inclusion (3.6) assure que si n est un entier suffisamment grand, on a $N_\nabla(x) \in S \otimes_{\mathfrak{S}} \mathfrak{M}$ pour tout $x \in \mathfrak{M}$. La formule

$$N_n(s \otimes x) = \frac{ps}{\varphi^{n+1}(\lambda)} \otimes \varphi^n N_\nabla(x) + \varphi^n N(s) \otimes \varphi^n(x) \qquad (s \in S[1/p],\, x \in \mathfrak{M}) \tag{3.7}$$

définit alors un opérateur $N_n : \mathcal{D} \to \mathcal{D}$. Un calcul montre que celui-ci vérifie $N_n \varphi = p\varphi N_n$ ainsi que la relation $N_n(sx) = \varphi^n N(s) \cdot \varphi^n(x) + \varphi^n(s) \cdot N_n(s)$ valable pour tout $s \in S[1/p]$ et tout $x \in \mathcal{D}$. Soit f_0 la projection canonique $S \to W$ qui consiste à évaluer une série en $u = 0$. Elle permet de former le produit tensoriel $D = W \otimes_S \mathcal{D}$, sur lequel le Frobenius φ agit de façon bijective. On a en outre une application surjective canonique $\mathcal{D} \to D$. La proposition 6.2.1.1 de [3] assure que celle-ci admet une unique section $s : D \to \mathcal{D}$ qui est compatible au Frobenius. L'espace D apparaît ainsi comme un sous-$W[1/p]$-espace vectoriel de $\mathcal{D}$, et l'application $S[1/p] \otimes_{W[1/p]} D \to \mathcal{D}$ qui s'en déduit est un isomorphisme compatible à φ. Dans la suite, on identifiera sans commentaire supplémentaire D à un sous-espace de $\mathcal{D}$.

Lemme 3.12. *L'opérateur N_n défini par la formule* (3.7) *stabilise D.*

Démonstration. Comme φ est bijectif sur D, il résulte de la relation de commutation $N_n\varphi = p\varphi N_n$ que N_n envoie D sur $\varphi(\mathcal{D})$. Une récurrence immédiate, utilisant le même argument, montre plus généralement que $N_n(D) \subset \varphi^m(\mathcal{D})$ pour tout entier $m \geqslant 1$. Or, il résulte de l'isomorphisme $\mathcal{D} \simeq S[1/p] \otimes_{W[1/p]} D$ compatible à φ (l'action sur le membre de droite se faisant par $\varphi \otimes \varphi$), que l'intersection des $\varphi^m(\mathcal{D})$ n'est autre que D. Le lemme est ainsi démontré. □

Le Frobenius φ étant bijectif sur D, on peut définir l'application $N : D \to D$ par $N = \varphi^{-n} \circ N_n$. Il est clair que $N\varphi = p\varphi N$ et, en déroulant les définitions, on vérifie par ailleurs que pour tout $x \in D$, on a :

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

cette relation ayant lieu dans un espace suffisamment gros, par exemple $W(\mathfrak{m}_R)^{Z\text{-dp}}$. À partir de là, on conclut par le même argument que celui expliqué dans le §7.2 de [18].

3.3 Réseaux à l'intérieur des représentations semi-stables

Un problème classique et important consiste à de décrire les réseaux à l'intérieur des représentations semi-stables. Dans ce dernier paragraphe, nous aimerions expliquer sommairement comment cela peut être réalisé à l'aide de structures entières à l'intérieur des objets de $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$.

3.3.1 Une borne plus précise pour l'action de N_∇

Le point de départ de notre analyse consiste à remarquer que la démonstration du théorème 3.4 (voir §3.2.2) donne en réalité un peu plus que ce qui a été énoncé jusqu'à présent. Précisément, en reprenant les notations du §3.2.2, elle assure que l'on n'a pas seulement $N_\nabla(\mathfrak{M}) \subset \mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$, mais aussi

$$N_\nabla(\mathfrak{M}) \subset \mathcal{R}_1^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M} \tag{3.8}$$

où $\mathcal{R}_1^{\text{int}}$ désigne le sous-$\mathfrak{S}$-module de $\mathcal{O}$ formé des séries $f = \sum_{n \geqslant 0} a_n u^n$ pour lesquelles la quantité $v_p(a_n) + \log_p(n)$ est minorée pour $n \geqslant 1$. Ce n'est pas la première fois qu'un tel espace est introduit ; il a été, par exemple, déjà considéré dans [9], §II.1, référence dans laquelle l'auteur montre en particulier qu'il s'agit d'un espace de Banach pour la valuation $v_{\mathcal{R}_1^{\text{int}}}$ définie, en reprenant les notations précédentes, par $v_{\mathcal{R}_1^{\text{int}}}(f) = \inf_{n \geqslant 1} v_p(a_n) + \ell(n)$ où $\ell(0) = 0$ et $\ell(n) = \log_p(n)$ si $n \geqslant 1$. La proposition II.3.1 de *loc. cit.* montre en outre que $\mathcal{R}_1^{\text{int}}$ s'identifie à l'espace des distributions continues sur $\mathbb{Z}_p$ d'ordre 1, c'est-à-dire définissant une forme linéaire continue sur l'espace des fonctions de classe $\mathcal{C}^1$.

Proposition 3.13. *Soient V une représentation semi-stable de G_K, et T un $\mathbb{Z}_p$-réseau de V stable par G_K. On note $\mathfrak{M}$ un*[12] *(φ,τ)-réseau de $E(u)$-hauteur finie à l'intérieur du (φ,τ)-module associé à T. Soit $\mathcal{M}$ l'objet de $\mathrm{Mod}_{/\mathcal{O}}^{\varphi,N_\nabla,0}$ associé à V. Alors*

$$N_\nabla(\mathfrak{M}) \subset \mathfrak{S}_\nabla \otimes_{\mathfrak{S}} \mathfrak{M}$$

où $\mathfrak{S}_\nabla$ est l'ensemble des séries de la forme $\sum_{n \geqslant 0} \frac{P_n(u)}{p^{n+1}} u^{e(p^n-1)/(p-1)}$ où les $P_n(u)$ sont des polynômes à coefficients dans W.

Remarque 3.14. D'après ce qui a été expliqué dans le §3.1.1, on a $\mathcal{M} = \mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$. On peut ainsi considérer $\mathfrak{M}$ comme un sous-module de $\mathcal{M}$, et cela a donc bien un sens de regarder l'image de $\mathfrak{M}$ par N_∇. De plus, comme le module $\mathfrak{S}_\nabla$ est inclus dans $\mathcal{R}_1^{\text{int}}$, la proposition apparaît comme un raffinement de l'inclusion (3.8). En lien avec cela, signalons encore que $\mathfrak{S}_\nabla$ est borné dans $\mathcal{R}_1^{\text{int}}$; de façon explicite, il est inclus dans la boule de centre 0 et de rayon $\frac{p^2}{e}$.

Démonstration. Comme préliminaire à la démonstration, il nous faut d'abord expliquer comment l'action de τ se retrouve à partir de la connaissance de N_∇. Bien entendu, on a envie d'appliquer simplement la formule $\tau = \exp(p\mathrm{t}N_\nabla) = \sum_{i \geqslant 0} \frac{(p\mathrm{t}N_\nabla)^i}{i!}$, mais cela demande quelques précautions, car les itérés successifs de $p\mathrm{t}N_\nabla$ ne sont pas clairement définis.

12. Il est en fait unique d'après la proposition 3.1.

Pour tout entier positif ou nul i, soit $\mathcal{R}_i^{\text{int}}$ l'ensemble des séries $f = \sum_{n\geqslant 0} a_n u^n$ pour lesquelles la quantité $v_p(a_n) + i \log_p(n)$ est minorée pour $n \geqslant 1$. Si i et j sont deux entiers, le produit d'une fonction de $\mathcal{R}_i^{\text{int}}$ par une fonction de $\mathcal{R}_j^{\text{int}}$ appartient à $\mathcal{R}_{i+j}^{\text{int}}$. La relation de Leibniz permet de prolonger l'opérateur N_∇ à $\mathcal{O} \otimes_{\mathfrak{S}} \mathfrak{M}$, tandis que la remarque que l'on vient de faire montre que ce prolongement, que l'on appelle encore N_∇, envoie $\mathcal{R}_i^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$ sur $\mathcal{R}_{i+1}^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$. Les formules $N_\nabla^{(0)} = \text{id}$ et

$$N_\nabla^{(i+1)} = iu \cdot \frac{d\lambda}{du} \cdot N_\nabla^{(i)} + N_\nabla \circ N_\nabla^{(i)}$$

définissent alors des applications $\mathfrak{S}$-linéaires $N_\nabla^{(i)} : \mathfrak{M} \to \mathcal{R}_i^{\text{int}} \otimes_{\mathfrak{S}} \mathfrak{M}$ qui, d'un point de vue intuitif, doivent être pensées comme les quotients $\frac{(p\mathfrak{t}N_\nabla)^i}{(p\mathfrak{t})^i}$. À partir du fait que N_∇ prend ses valeurs dans $\mathfrak{S}^{\nu\text{-dp}}$, il n'est pas difficile de démontrer que la somme infinie $\sum_{i\geqslant 0} \frac{(p\mathfrak{t})^i}{i!} \cdot N_\nabla^{(i)}$ converge vers un opérateur W-linéaire $\tau : \mathfrak{M} \to W(R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$. Une récurrence sur i montre que, pour tout $x \in \mathfrak{M}$ et tout entier i, on a la formule :

$$N_\nabla^{(i)}(ux) = u \cdot \sum_{j=0}^{i} \binom{i}{j} (-\lambda)^{i-j} N_\nabla^{(j)}(x).$$

Il en résulte par un nouveau calcul que $\tau(ux) = [\underline{\varepsilon}] \cdot \tau(x)$ pour tout $x \in \mathfrak{M}$, relation qui permet de prolonger τ par semi-linéairité à tout $W(\mathfrak{m}_R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$. Par ailleurs, on montre, à nouveau par récurrence sur i, que $N_\nabla^{(i)}$ et φ satisfont à la relation de commutation $N_\nabla^{(i)} \circ \varphi = U^i \cdot \varphi \circ N_\nabla^{(i)}$, à partir de quoi il suit que τ et φ commutent. Finalement, on laisse en exercice au lecteur le soin de vérifier que la série définissant le logarithme de τ converge vers un endormorphisme de $W(R)[Z/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$ qui coïncide avec $p\mathfrak{t}N_\nabla$ sur $\mathfrak{M}$.

On est maintenant prêt à démontrer la proposition. La construction de l'opérateur τ donnée ci-dessus montre que celui-ci envoie $\mathfrak{M}$ sur $\mathfrak{t}W(R) \otimes_{\mathfrak{S}} \mathfrak{M}$. Sachant cela, on peut reprendre l'argumentation du §3.2.2 en remplaçant $W(\mathfrak{m}_R)^{Z\text{-dp}}$ par $W(R)^{\mathfrak{t}\text{-dp}}$. La proposition en résulte. $\square$

La proposition 3.13 permet, à son tour, de contraindre l'espace d'arrivée de l'opérateur τ. Soit, en effet, pour tout entier i, $\mathfrak{S}_\nabla^{(i)}$ le sous-$\mathfrak{S}$-module de $\mathcal{O}$ engendré par les produits de i éléments de $\mathfrak{S}_\nabla$. Par convention, on pose également $\mathfrak{S}_\nabla^{(0)} = \mathfrak{S}$. Pour tout i, $\mathfrak{S}_\nabla^{(i)}$ est alors un sous-ensemble borné de $\mathcal{R}_i^{\text{int}}$ et les $p^i \mathfrak{S}_\nabla^{(i)}$ se plongent également dans $W(R)[\mathfrak{t}/p]^\wedge$ en envoyant, comme d'habitude, u sur $[\underline{\pi}]$. Il est alors immédiat de vérifier que les morphismes $N_\nabla^{(i)}$ définis précédemment prennent leurs valeurs dans $\mathfrak{S}_\nabla^{(i)} \otimes_{\mathfrak{S}} \mathfrak{M}$, et donc que :

$$\tau(\mathfrak{M}) \subset \left(\sum_{i\geqslant 0} p^i \mathfrak{S}_\nabla^{(i)} \cdot \mathfrak{t}^i \right)^\wedge \otimes_{\mathfrak{S}} \mathfrak{M} \tag{3.9}$$

où le produit $p^i \mathfrak{S}_\nabla^{(i)}$ est vu dans $W(R)[\mathfrak{t}/p]^\wedge$ et l'exposant $^\wedge$ signifie que l'on prend l'adhérence dans $W(R)[\mathfrak{t}/p]^\wedge$. L'inclusion que l'on vient d'obtenir est, bien sûr, à mettre en parallèle avec l'inclusion (2.7) donnée par le théorème 2.25, l'élément V pouvant être alors choisi égal à une certaine puissance de $\mathfrak{t}$.

3.3.2 Structures entières à l'intérieur des objets de $\text{Mod}_{/\mathcal{O}}^{\varphi, N_\nabla, 0}$

Le résultat de la proposition 3.13 conduit naturellement à la définition (sans doute provisoire) suivante.

Définition 3.15. Un (φ, N_∇)-*réseau* est la donnée d'un objet $\mathfrak{M}$ de $\text{Mod}_{/\mathfrak{S}}^{\varphi}$ muni d'un morphisme $N_\nabla : \mathfrak{M} \to \mathfrak{S}_\nabla \otimes_{\mathfrak{S}} \mathfrak{M}$ vérifiant la relation de Leibniz (3.3) et la relation de commutation (3.4).

Un morphisme entre deux (φ, N_∇)-réseaux $\mathfrak{M}$ et $\mathfrak{M}'$ est un morphisme f entre les objets de $\text{Mod}_{/\mathfrak{S}}^{\varphi}$ faisant commuter le diagramme suivant :

$$\begin{tikzcd} \mathfrak{M} \arrow[r, "N_\nabla"] \arrow[d, "f"'] & \mathfrak{S}_\nabla \otimes_{\mathfrak{S}} \mathfrak{M} \arrow[d, "\text{id}\otimes f"] \\ \mathfrak{M}' \arrow[r, "N_\nabla"] & \mathfrak{S}_\nabla \otimes_{\mathfrak{S}} \mathfrak{M}' \end{tikzcd}$$

On note $\text{Mod}_{/\mathfrak{S}}^{\varphi, N_\nabla}$ la catégorie des (φ, N_∇)-réseaux. Si, par ailleurs, $\text{Rep}_{[0,+\infty[}^{\text{int,st}}(G_K)$ désigne la catégorie des réseaux stables par G_K à l'intérieur des représentations semi-stables à poids de Hodge-Tate positifs ou nuls, on a construit précédemment un foncteur $\mathcal{K}^{\text{int}} : \text{Rep}^{\text{int,st}}_{[0,+\infty[}(G_K) \to \text{Mod}^{\varphi,N_\nabla}_{/\mathfrak{S}}$ qui s'insère dans le carré commutatif suivant :

$$\begin{tikzcd} \text{Rep}^{\text{int,st}}_{[0,+\infty[}(G_K) \arrow[r] \arrow[d, "\mathcal{K}^{\text{int}}"'] & \text{Rep}^{\text{st}}_{[0,+\infty[}(G_K) \arrow[d, "\mathcal{K}", "\sim"'] \\ \text{Mod}^{\varphi,N_\nabla}_{/\mathfrak{S}} \arrow[r] & \text{Mod}^{\varphi,N_\nabla,0}_{/\mathcal{O}} \end{tikzcd}$$

Proposition 3.16. *Le foncteur K^{int} est pleinement fidèle. De plus, un (φ, N_∇)-réseau $\mathfrak{M}$ est dans son image essentielle si, et seulement si l'endomorphisme τ de $W(R)[\mathfrak{t}/p]^\wedge \otimes_{\mathfrak{S}} \mathfrak{M}$ défini ci-dessus stabilise $W(R) \otimes_{\mathfrak{S}} \mathfrak{M}$.*

Démonstration. C'est immédiat. □

La condition qui vient d'apparaître n'est pas très commode car il ne semble *a priori* pas facile de décider si un élément de $W(R)[\mathfrak{t}/p]^\wedge$ appartient à $W(R)$. Typiquement, si l'on écrit cet élément comme une série en $\frac{\mathfrak{t}}{p}$, on obtient un nombre infini de conditions à examiner. La proposition suivante explique comment l'on peut se remener à un nombre fini de vérifications.

Proposition 3.17. *Soit $\mathfrak{M}$ un (φ, N_∇)-réseau. On suppose que le φ-réseau sous-jacent est de $E(u)$-hauteur $\leqslant r$. Alors, $\mathfrak{M}$ est dans l'image essentielle de $\mathcal{K}^{\text{int}}$ si, et seulement si, pour tout $x \in \mathfrak{M}$, la somme finie*

$$x + p\mathfrak{t} \cdot N_\nabla^{(1)}(x) + \frac{(p\mathfrak{t})^2}{2} \cdot N_\nabla^{(2)}(x) + \cdots + \frac{(p\mathfrak{t})^r}{r!} \cdot N_\nabla^{(r)}(x) \tag{3.10}$$

appartient à $\left(W(R) + \left(\frac{\mathfrak{t}}{p}\right)^r \mathfrak{m}_{W(R)} W(R)[\mathfrak{t}/p]^\wedge\right) \otimes_{\mathfrak{S}} \mathfrak{M}$.

Remarque 3.18. Bien entendu, il suffit de vérifier que la somme (3.10) est dans l'ensemble souhaité pour x parcourant une base de $\mathfrak{M}$ sur $\mathfrak{S}$.

Démonstration. Comme dans la preuve de la proposition 2.9, on démontre qu'en vertu de la relation de commutation avec φ, l'opérateur τ s'obtient par un procéde itératif à partir de sa réduction modulo $\left(\frac{\mathfrak{t}}{p}\right)^r \mathfrak{m}_{W(R)} W(R)[\mathfrak{t}/p]^\wedge$. Le corollaire résulte de cela. □

Corollaire 3.19. *Tout (φ, N_∇)-réseau de $E(u)$-hauteur $\leqslant p-1$ est dans l'image essentielle de $\mathcal{K}^{\text{int}}$.*

Remarque 3.20. En d'autres termes, le corollaire dit que le foncteur $\mathcal{K}^{\text{int}}$, une fois restreint à la catégorie des réseaux dans les représentations semi-stable à poids de Hodge-Tate dans $\{0, \ldots, p-1\}$, et corestreint à la catégorie des (φ, N_∇)-réseaux de $E(u)$-hauteur $\leqslant p-1$, est une équivalence de catégories.

Démonstration. Puisque $v_R(u^e \bmod p) > v_R(\mathfrak{t}^{p-2} \bmod p)$, on a $u^e \in pW(R) + \mathfrak{t}^{p-2}\mathfrak{m}_{W(R)}$. Il en résulte facilement que tous les modules $p^i \mathfrak{S}_\nabla^{(i)}$ sont inclus dans $W(R) + \left(\frac{\mathfrak{t}}{p}\right)^{p-2} \mathfrak{m}_{W(R)} W(R)[\mathfrak{t}/p]^\wedge$. Le corollaire est alors une conséquence de la proposition 3.17 appliquée avec $r = p-1$. □

3.4 Bornes pour la ramification sauvage des représentations semi-stables

Nous concluons cette section en expliquant sommairement comment la combinaison de plusieurs idées qui ont été développées dans les pages précédentes permettent de compléter les méthodes de [7] et de démontrer la conjecture 1.2.(1) dont voici l'énoncé.

Théorème 3.21. *Soit r un entier positif. Soit T le quotient de deux réseaux stables par G_K dans une représentation semi-stable à poids de Hodge-Tate dans $\{0, \ldots, r\}$. On se donne un entier n tel que $p^n T = 0$. Si $\frac{r}{p-1}$ s'écrit sous la forme $p^\alpha \beta$ avec $\alpha' \in \mathbb{N}$ et $\frac{1}{p} < \beta' \leqslant 1$, alors pour tout*

$$\mu > 1 + e(n+\alpha) + \max(e\beta - \frac{1}{p^{n+\alpha}}, \ \frac{e}{p-1})$$

le sous-groupe de ramfication $G_K^{(\mu)}$ agit trivialement sur T.

Démonstration. Elle est analogue à celle présentée dans [7] sauf que, comme dans le §2.2 de cet article, on remplace les quotients $W_n(R)/[\mathfrak{a}_R^{>a}]$ et $W_n(R)/[\mathfrak{a}_R^{>b}]$ (avec les notations de *loc. cit.* par $W_n(R)/(E(u)^r \mathfrak{t}^r)\mathfrak{m}_{W_n(R)}$ et $W_n(R)/\mathfrak{t}^r \mathfrak{m}_{W_n(R)}$ respectivement. La clé réside en fait dans une généralisation appropriée du lemme 3.2.1 de [7] qui stipule que, si $\mathfrak{M}$ est l'unique (φ, τ)-réseau de $E(u)$-hauteur $\leqslant r$ dans le (φ, τ)-module associé à un réseau dans une représentation semi-stable à poids de Hodge-Tate dans $\{0, \ldots, r\}$, alors pour tout $s > n - 1 + \log_p r$ et pour tout $\sigma \in G_s$, on a :

$$(\sigma - \mathrm{id})(\mathfrak{M}) \subset (\mathfrak{t}^r \mathfrak{m}_{\mathfrak{S}_\tau} + p^n \mathfrak{S}_\tau) \otimes_{\mathfrak{S}} \mathfrak{M}.$$

Il suffit bien sûr d'établir cette inclusion lorsque $g = \tau^{p^s}$. Dans ce cas, elle découle d'une expression de τ^{p^s} en fonction de l'opération N_∇ analogue à celle qui a été établie pour τ dans la démonstration de la proposition 3.13. Si l'on préfère, elle peut également s'obtenir, de même que dans [7], comme une conséquence de la théorie des $(\varphi, \hat{G})$-modules de Liu. Le reste de la démonstration est absolument similaire à [7] ; on ne le répète donc pas ici. $\square$

4 Quelques perspectives

Le cas $p = 2$

Tout au long de cet article, nous avons supposé que le nombre premier p était impair. Bien que cette hypothèse ait été utilisée à plusieurs reprises au fil des démonstrations, l'auteur est d'avis que l'ensemble des résultats obtenus devrait s'étendre (sans doute avec quelques modifications mineures) au cas $p = 2$. L'exercice reste cependant à faire.

Lien avec les (φ, Γ)-modules

Comme cela a été démontré dans cet article, la catégorie des (φ, τ)-modules est équivalente à celle des représentations galoisiennes de G_K. Ainsi elle est aussi équivalente à la catégorie des (φ, Γ)-modules de Fontaine. Expliciter cette équivalence sans passer par les représentations de G_K nous semble une question naturelle et intéressante. L'obtention d'un tel résultat devrait permettre de déduire du théorème 3.4 un critère pour reconnaître les représentations semi-stables en termes de leurs (φ, Γ)-modules. Se poserait alors la question de comparer celui-ci avec celui qui découle de la théorie de Berger (voir [2]). Le rapprochement des deux points de vue pourrait peut-être conduire à une meilleure compréhension des représentations semi-stables.

Dans le même veine, on peut chercher à rendre explicite les liens entre les différentes catégories de (φ, τ)-modules que l'on obtient en faisant varier l'uniformisante π, la famille des π_n, ou encore l'élément τ. Ceci devrait permettre une meilleure compréhension des (φ, τ)-modules. Un moyen, qui semble raisonnable, pour aborder cette question consiste à adapter les constructions du §3.1 de [5] en gardant à l'esprit que τ joue le rôle de l'opérateur $\exp(tN)$ où $t = \log[\underline{\varepsilon}] \in A_{\text{cris}}$.

Surconvergence des (φ, τ)-modules

Un résultat important de la théorie des (φ, Γ)-modules est le théorème de Cherbonnier-Colmez (voir [8]) qui affirme que tout (φ, Γ)-module étale sur $\mathcal{E}$ admet un « (φ, Γ)-réseau défini sur un anneau des séries surconvergentes, c'est-à-dire convergentes sur une coronne infinitésimale sur le bord du disque unité. Dans cet article, nous nous sommes contentés de considérer des réseaux définis sur l'anneau $\mathfrak{S}$ dont les éléments ne se contentent pas de surconverger, mais convergent dans tout le disque unité. Comme nous l'avons vu, cela suffit pour l'application aux représentations semi-stables à poids de Hodge-Tate positifs ou nuls car, d'après les résultats de Kisin, les (φ, τ)-modules qui leur sont associés admettent toujours de tels réseaux. Par contre, comme nous l'avons montré dans le §2.1.2, il n'est pas vrai que tous les (φ, τ)-modules admettent un tel réseau. Le contre-exemple que nous avons donné est celui de la représentation $\mathbb{Z}_p(-1)$, représentation que l'on a *a priori* pas envie d'écarter. Pour pouvoir continuer à travailler avec cet exemple basique (et bien d'autres), il paraît donc important de comprendre si — et, le cas échéant, comment — le théorème de Cherbonnier-Colmez s'étend aux (φ, τ)-modules.

Utilisation du logarithme dans le cas de torsion

Dans le §3, nous avons vu que, dans le cas des (φ, τ)-modules libres sur $\mathcal{E}^{\text{int}}$, la considération du logarithme de τ s'est relévé être un outil puissant pour décrire cet opérateur. C'est par exemple elle qui nous a permis d'obtenir l'inclusion (3.9). On peut donc se demander dans quelle mesure des arguments similaires s'appliquent dans le cas des (φ, τ)-modules de p-torsion. Bien entendu, la considération du logarithme devient alors bien plus délicate à cause des divisions par p qu'il faudra désormais contrôler avec plus d'attention [13]. Le théorème 2.25 pourrait avoir un rôle important à jouer dans cette histoire.

Le problème du rélèvement des représentations

Dans [7], les auteurs ont posé dans le §5 un certain nombre de questions sur la possibilité de relever en caractéristique nulle des représentations galoisiennes de torsion. Typiquement, on se donne une $\mathbb{F}_p$-représentation $\bar{T}$ de G_K, et on se demande s'il existe un réseau T dans une représentation cristalline (resp. semi-stable), dont les poids de Hodge-Tate sont éventuellement fixés, et un morphisme surjectif $T \to \bar{T}$. La théorie des (φ, τ)-modules nous semble être une approche intéressante pour aborder ce type de problèmes (au moins dans le cas des représentations semi-stables) puisqu'elle permet à la fois de décrire les représentations libres et de torsion, et de reconnaître de façon particulièrement simple les réseaux dans les représentations semi-stables.

Références

[1] J. Ax, *Zeros of polynomials over local fields. The Galois action*, J. Algebra **15** (1970), 417–428

[2] L. Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), no. 2, 219–284

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

[4] C. Breuil, *Une application de corps des normes*, Compositio Math. **117** (1999), no. 2, 189–203

[5] X. Caruso, *Représentations semi-stables de torsion dans le cas $er < p - 1$*, J. reine angew. Math. **594** (2006), 35–92

[6] X. Caruso, T. Liu, *Quasi-semi-stable representations*, Bull. Soc. Math. France **137** (2009), 185–223

[7] X. Caruso, T. Liu, *Some bounds for ramification of p^n-torsion semi-stable representations*, J. Algebra **325** (2011), 70–96

[8] F. Cherbonnier, P. Colmez, *Représentations p-adiques surconvergentes*, Invent. Math. **133** (1998), no. 3, 581–611

[9] P. Colmez, *Fonctions d'une variable p-adique*, Astérisque **330** (2010), 13–59

[10] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur $\mathbb{Z}$*, Invent. Math. **81** (1985), 515–538

[11] J. M. Fontaine, *Représentations p-adiques des corps locaux*, Grothendieck Festschrift II, (1991), 249–309

[12] J.-M. Fontaine, *Le corps des périodes p-adiques*, Astérisque **223**, Soc. math. France (1994), 59–111

[13] M. Kisin, *Crystalline representations and F-crystals*, Algebraic Geometry and Number Theory, Drinfeld 50th Birthday volume, 459–496

[14] F. Laubie, *Extensions de Lie et groupes d ?automorphismes de corps locaux*, Comp. Math. **67** (1988), 165–189

[15] S. Lang, *Cyclotomic fields*, Springer, Berlin, 1978

[16] J. Le Borgne, *Un algorithme pour la réduction des ϕ-modules sur $k((u))$*, en préparation

[17] T. Liu, *On lattices in semi-stable representations : a proof of a conjecture of Breuil*, Comp. Math. **144** (2008), No. 1, 61–88

13. Dans le cas des représentations libres, nous avons certes obtenu un contrôle précis des dénominateurs, mais celui-ci découlait justement d'arguments basés sur la considération de $\log \tau$. Je ne vois pas, du moins pour le moment, comment adapter cette approche au cas de torsion.

[18] T. Liu, *Torsion p-adic Galois representation and a conjecture of Fontaine*, Ann. Sci. École Norm. Sup. **40** (2007), No. 4, 633–674

[19] T. Liu, *A note on lattices in semi-stable representations*, Math. Ann. **346** (2010), No. 1, 117–138

[20] F. Tavares Ribeiro, (φ, Γ)-*modules et loi explicite de réciprocité*, thèse de doctorat, disponible à `http://tel.archives-ouvertes.fr/docs/00/37/97/71/PDF/these_Tavares.pdf`

[21] J.P. Serre, *Corps locaux*, third edition, Herrmann (1968)

[22] S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17** (1972), 44–50

[23] J.P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux ; applications*, Ann. Sci. École Norm. Sup. **16** (1983), no. 1, 59–89

[24] M. Yoshida, *Ramification of local fields and Fontaine's property (P_m)*, disponible à `http://arxiv.org/abs/0905.1171`