Semi-simplifiée modulo p des représentations semi-stables : une approche algorithmique

Xavier Caruso David Lubicz

November 15, 2013

Abstract

The aim of this paper is to design an algorithm with polynomial complexity that computes the semi-simplified modulo p of a semi-stable $\mathbb{Q}_p$-representation of the absolute Galois group of a p-adic field (*i.e.* a finite extension of $\mathbb{Q}_p$). In order to do so, we make an intensive use of p-adic Hodge theory and, more precisely, the theory of Breuil–Kisin modules.

Résumé

Le but de cet article est de présenter un algorithme de complexité polynômiale pour calculer la semi-simplifiée modulo p d'une $\mathbb{Q}_p$-représentation semi-stable du groupe de Galois absolu d'un corps p-adique (*i.e.* une extension finie de $\mathbb{Q}_p$). Pour ce faire, nous utilisons abondamment la théorie de Hodge p-adique et, en particulier, la théorie des modules de Breuil–Kisin.

Table des matières

Soient p un nombre premier et k un corps fini de caractéristique p. Soient $\mathcal{O}_{K_0}$ l'anneau des vecteurs de Witt à coefficients dans k et K_0 son corps des fractions ; c'est une extension finie non ramifiée de $\mathbb{Q}_p$. On appelle σ l'endomorphisme de Frobenius agissant sur K_0. Soit K une extension totalement ramifiée de K_0. Les corps K_0 et K sont munis d'une valuation discrète que l'on note val et que l'on suppose normalisée par $\mathrm{val}(p) = 1$. Soient enfin $\bar{K}$ une clôture algébrique de K et $G_K = \mathrm{Gal}\,(\bar{K}/K)$ le groupe de Galois absolu de K. La valuation val s'étend de façon unique à $\bar{K}$ et on note encore val ce prolongement.

Les représentations p-adiques du groupe G_K jouent un rôle essentiel dans de nombreuses questions de théorie des nombres et de géométrie arithmétique. Avec les développements récents de

la théorie de Hodge p-adique, on dispose en outre maintenant d'outils théoriques efficaces pour étudier ces représentations. Toutefois, force est de constater que la complexité des objets mis en jeu est telle que, même sur des exemples qui semblent *a priori* de petite taille, il est rapidement impossible de mener à terme des calculs explicites. À titre d'exemple, les problèmes (liés entre eux) de la détermination explicite d'espaces de déformations de représentations galoisiennes p-adique et de calcul de la semi-simplifiée modulo p d'une telle représentation ont déjà donné lieu à une littérature fournie (voir notamment [1], [4], [5], [6], [17], [18], [19], *etc.*) pour des résultats qui, bien que tout à fait significatifs, restent cantonnés à des situations très particulières (dimension 2, petits poids de Hodge-Tate) et ne permettent pas toujours de formuler des conjectures générales.

Au vu de ce constat, il nous paraît opportun de commencer à réfléchir à introduire l'outil informatique pour la manipulation des représentations galoisiennes de G_K, dans l'espoir (peut-être lointain) de pouvoir confier à l'ordinateur les calculs longs et difficiles (mais aussi automatiques) qui apparaissent en théorie de Hodge p-adique, de même que, de nos jours, on s'appuie sur ce même ordinateur par exemple en analyse pour résoudre les équations aux dérivées partielles.

Dans cet article, nous nous intéressons au calcul de la semi-simplifiée modulo p d'une $\mathbb{Q}_p$-représentation de G_K — qui a déjà été mentionné précédemment. Rappelons brièvement qu'une représentation V comme ci-dessus admet toujours un $\mathbb{Z}_p$-réseau stable T par l'action de G_K et que la semi-simplifiée (c'est-à-dire la somme directe des constituants simples de Jordan-Hölder) du quotient T/pT ne dépend pas, à isomorphisme près, du choix de T ; c'est cette représentation semi-stable que l'on appelle la *semi-simplifiée modulo* p de V. Le résultat principal de cet article s'énonce comme suit.

Théorème 1. *Il existe un algorithme de complexité polynômiale qui calcule la semi-simplifiée modulo p d'une représentation semi-stable.*

La formulation précédente est volontairement imprécise : par exemple, elle ne stipule pas comment sont représentées les entrées et les sorties de l'algorithme, ni en quels paramètres la complexité est polynômiale. Pour des compléments, on renvoie au corps du texte et notamment au début du §2, ainsi qu'au §2.5 pour ce qui concerne la complexité.

La démonstration du théorème 1 repose de façon essentielle sur la théorie de Hodge p-adique et, plus précisément, sur la théorie des modules de Breuil–Kisin pressentie par Breuil dans [3] puis développée par Kisin dans [15]. Rappelons brièvement dans cette introduction que les modules de Breuil–Kisin sont des objets d'algèbre linéaire d'apparence simple — à savoir des modules libres sur l'anneau $\mathfrak{S} = \mathcal{O}_{K_0}[[u]]$ munis d'un opérateur ϕ satisfaisant à un certain nombre de conditions — qui classifient les réseaux (stables par un certain sous-groupe G_∞ de G_K) à l'intérieur d'une représentation semi-stable. En utilisant cette correspondance, on ramène le calcul que l'on souhaite mener (1) au calcul d'un réseau stable par l'opérateur ϕ à l'intérieur d'un certain ϕ-module libre sur $\mathfrak{S}[1/p]$ puis (2) au calcul de la semi-simplifiée de la réduction modulo p de celui-ci. Grâce aux travaux de Le Borgne [16], des algorithmes efficaces ont déjà été mis au point pour le calcul de la semi-simplifiée. Le calcul du réseau, quant à lui, est fondé sur une idée simple : on part d'un réseau quelconque et on itère l'opérateur ϕ jusqu'à obtenir un module stable.

Malheureusement, derrière ces apparences simples, se cachent un certain nombre de complications techniques dues, pour l'essentiel, au fait qu'il est impossible de représenter sur machine un élément de $\mathfrak{S}$ dans son intégralité (il y a une infinité de coefficients à donner et, pour chaque coefficient, une infinité de « chiffres ») ; à cause de cela, calculer avec des $\mathfrak{S}$-modules n'est pas anodin d'un point de vue algorithmique ! Toutefois, nous avons montré dans un travail antérieur [11], que ces problèmes peuvent être résolus (dans une certaine mesure) en introduisant de nouveaux anneaux $\mathfrak{S}_\nu$ (pour un paramètre ν variant dans $\mathbb{Q}^+$) définis ainsi :

$$\mathfrak{S}_\nu = \Big\{ \sum_{i\in\mathbb{N}} a_i u^i \quad | \quad a_i \in K_0 \text{ et } \mathrm{val}(a_i) + \nu i \geqslant 0, \, \forall i \geqslant 0 \Big\}$$

et en étendant les scalaires à un nouvel $\mathfrak{S}_\nu$ (pour un ν de plus en plus grand) après chaque opération élémentaire. Ceci nous conduit à développer une théorie de Breuil–Kisin sur les anneaux $\mathfrak{S}_\nu$ qui viennent d'être introduits. Notre résultat principal, à ce sujet, est le théorème 2 ci-après qui dit informellement que, tant que ν reste suffisamment petit, remplacer l'anneau $\mathfrak{S}$ par $\mathfrak{S}_\nu$ ne porte pas à conséquence.

Théorème 2 (Surconvergence des modules de Breuil–Kisin)**.** *On se donne $r > 0$ un entier, ainsi que ν un nombre rationnel vérifiant $0 \leqslant \nu < \frac{p-1}{per}$. Alors le foncteur*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Modules de Breuil–Kisin sur } \mathfrak{S} \\ \textit{de hauteur } \leqslant r \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} \textit{Modules de Breuil–Kisin sur } \mathfrak{S}_\nu \\ \textit{de hauteur } \leqslant r \end{array} \right\} \\ \mathfrak{M} & \mapsto & \mathfrak{S}_\nu \otimes_{\mathfrak{S}} \mathfrak{M} \end{array}$$

est une équialence de catégories.

Le théorème précédent a fait apparaître la notion de hauteur d'un module de Breuil–Kisin. Nous renvoyons le lecteur au §1.1.2 pour la définition de cette notion ; pour cette introduction, on pourra se contenter de retenir que les modules de Breuil–Kisin de hauteur $\leqslant r$ sont exactement ceux qui correspondent aux représentations semi-stables V dont les poids de Hodge-Tate sont dans $\{0, \dots, r\}$, c'est-à-dire pour lesquelles le produit tensoriel $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V$ (où $\mathbb{C}_p$ est le complété de $\bar{K}$) se décompose comme une somme directe de $\mathbb{C}_p(h_i)$ pour des entiers $h_i \in \{0, \dots, r\}$.

On déduit du théorème de surconvergence des modules de Breuil–Kisin que, si l'on est capable de contrôler la croissance du paramètre ν au fur et à mesure de l'exécution de notre algorithme, la méthode esquissée précédemment pour le calcul de la semi-simplifiée modulo p d'une représentation semi-stable fonctionne bel et bien. C'est cette voie que nous allons suivre tout au long de cet article.

La première partie de l'article est destinée à la mise au point des aspects théoriques : après quelques rappels, nous introduisons les modules de Breuil–Kisin sur les anneaux $\mathfrak{S}_\nu$ et démontrons le théorème 2. Les aspects algorithmiques, quant à eux, sont discutés dans la seconde partie de l'article, dont l'objectif est de présenter et d'étudier en détails (notamment en ce qui concerne les problèmes de précision) l'algorithme de calcul de la semi-simplifiée modulo p d'une représentation semi-stable promis par le théorème 1.

Ce travail a bénéficié du soutien de l'Agence Nationale de la Recherche (ANR) par l'intermédiaire du projet CETHop (Calculs Effectifs en Théorie de Hodge p-adique), référence ANR-09-JCJC-0048-01.

1 La théorie de Breuil–Kisin : rappels et compléments

On conserve les notations de l'introduction : la lettre p désigne un nombre premier, k est un corps parfait de caractéristique p, on pose $\mathcal{O}_{K_0} = W(k)$, $K_0 = \text{Frac}\, \mathcal{O}_{K_0} = \mathcal{O}_{K_0}[1/p]$, on note σ l'endomorphisme de Frobenius agissant sur K_0 et on considère K une extension finie totalement ramifiée de K_0 de degré e. On désigne par $\bar{K}$ une clôture algébrique de K et par $\mathbb{C}_p$ le complété p-adique de $\bar{K}$. Il s'agit à nouveau d'un corps algébriquement clos. On pose $G_K = \text{Gal}\,(\bar{K}/K)$.

On fixe en outre une uniformisante π de K, ainsi qu'une suite compatible $(\pi_s)_{s\geqslant 0}$ de racines p^s-ièmes de π, c'est-à-dire telle que l'on ait $\pi_0 = \pi$ et $\pi_{s+1}^p = \pi_s$ pour tout $s \geqslant 0$. Enfin, on appelle K_∞ la plus petite sous-extension de $\bar{K}$ contenant tous les π_s et on pose $G_\infty = \text{Gal}(\bar{K}/K_\infty) \subset G_K$.

1.1 Quelques objets de théorie de Hodge p-adique

On introduit dans ce numéro les objets de la théorie de Hodge p-adique qui seront utilisés constamment dans la suite de cet article : ce sont, d'une part, les (ϕ, N)-modules filtrés de Fontaine qui permettent de décrire les représentations semi-stables et, d'autre part, les modules de Breuil–Kisin qui classifient les réseaux stables par G_∞ à l'intérieur de celles-ci.

1.1.1 Brefs rappels sur les (ϕ, N)-modules filtrés

Un théorème célèbre de Colmez et Fontaine [12] affirme qu'il existe une équivalence de catégories notée traditionnellement D_{st} ou $D_{\mathrm{st},\star}$, entre la catégorie des représentations semi-stables[1] et la catégorie des (ϕ, N)-modules admissibles dont voici la définition :

Définition 1.1 (Fontaine)**.** *Un (ϕ, N)-module filtré sur K est la donnée de*

- *un K_0-espace vectoriel D de dimension finie,*
- *un opérateur σ-semi-linéaire (appelé Frobenius) $\phi : D \to D$ bijectif,*
- *un opérateur linéaire (appelé opérateur de monodromie) $N : D \to D$ vérifiant $N\phi = p\phi N$ et*
- *une filtration décroissante $(\mathrm{Fil}^h D_K)_{h\in\mathbb{Z}}$ de $D_K = D \otimes_{K_0} K$ telle que $\mathrm{Fil}^{-r} D_K = D_K$ et $\mathrm{Fil}^r D_K = 0$ pour r suffisamment grand.*

Si D est un (ϕ, N)-module filtré, on appelle

- nombre de Newton *de D, noté $t_N(D)$, la valuation p-adique du déterminant de ϕ[2] et*
- nombre de Hodge *de D, noté $t_H(D)$, la somme des dimensions de $\mathrm{Fil}^h D_K$ pour h variant dans $\mathbb{N}$.*

Un (ϕ, N)-module filtré D est dit admissible *si $t_H(D) = t_N(D)$ et si, pour tout $D' \subset D$ stable par ϕ et N et muni de la filtration induite, on a $t_H(D') \leqslant t_N(D')$.*

Dans la suite de cet article, nous travaillerons non pas avec D_{st} mais avec une version contravariante $D^\star_{\mathrm{st}}$ de ce foncteur définie par $D^\star_{\mathrm{st}}(V) = D_{\mathrm{st}}(V^\vee)$ où $V^\vee$ désigne la représentation contragrédiente de V. Le foncteur réciproque de $D^\star_{\mathrm{st}}$ est noté $V^\star_{\mathrm{st}}$; il associe une représentation galoisienne semi-stable à un (ϕ, N)-module filtré admissible.

Avec notre convention, si D est un (ϕ, N)-module filtré admissible, les sauts de la filtration $\mathrm{Fil}^h D_K$ — c'est-à-dire les entiers h tels que $\mathrm{Fil}^{h+1} D_K \subsetneq \mathrm{Fil}^h D_K$ comptées avec multiplicité $\dim_K \frac{\mathrm{Fil}^h D_K}{\mathrm{Fil}^{h+1} D_K}$ — sont exactement les poids de Hodge-Tate de la représentation $V^\star_{\mathrm{st}}(D)$[3]. En particulier, les poids de Hodge-Tate de $V^\star_{\mathrm{st}}(D)$ sont positifs ou nuls si, et seulement si $\mathrm{Fil}^0 D_K = D_K$; on dit dans ce cas que D est *effectif*.

1.1.2 Les modules de Breuil–Kisin

Après avoir classifié les représentations semi-stables à l'aide de des (ϕ, N)-modules filtrés, il est naturel, pour le problème que l'on a en vue, de chercher à décrire les réseaux à l'intérieur de ces représentations à l'aide d'objets de même type. La théorie de Breuil–Kisin, initiée par Breuil dans

[1] On renvoie à [13] pour la définition des représentations semi-stables.

[2] Le déterminant de ϕ dépend du choix d'une base mais sa valuation, elle, n'en dépend pas.

[3] C'est-à-dire les entiers h_i tels que $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V^\star_{\mathrm{st}}(D) \simeq \bigoplus_{i=1}^{\dim V} \mathbb{C}_p(h_i)$.

[2, 3], puis complétée par Kisin dans [15], donne une réponse partielle — mais suffisante pour les applications qui nous intéressent — à cette question. Plus précisément, elle permet de décrire, à l'aide de ϕ-modules définis sur l'anneau $\mathfrak{S} = \mathcal{O}_{K_0}[[u]]$, les $\mathbb{Z}_p$-réseaux vivant à l'intérieur d'une représentation semi-stables stables par l'action de G_∞ (et non celle de G_K)[4].

Pour décrire cette théorie, on a besoin de deux notations supplémentaires. *Primo*, on note $E(u)$ le polynôme minimal de π sur K_0 ; du fait que π est une uniformisante de K, on déduit que $E(u)$ est un polynôme d'Eisenstein à coefficients dans $\mathcal{O}_{K_0}$. *Secundo*, on pose $\mathfrak{S} = \mathcal{O}_{K_0}[[u]]$ et on munit cet anneau de l'opérateur $\phi : \sum_{i\in\mathbb{N}} a_i u^i \mapsto \sum_{i\in\mathbb{N}} \sigma(a_i) u^{pi}$.

Définition 1.2 (Breuil)**.** *Soit r un nombre entier positif. Un* module de Breuil–Kisin *sur $\mathfrak{S}$ de hauteur $\leqslant r$ est la donnée d'un $\mathfrak{S}$-module libre $\mathfrak{M}$ de rang fini muni d'une application $\phi : \mathfrak{M} \to \mathfrak{M}$ telle que :*

1. *pour tout $s \in \mathfrak{S}$ et tout $x \in \mathfrak{M}$, on a $\phi(sx) = \phi(s)\phi(x)$;*
2. *le sous-$\mathfrak{S}$-module engendré par l'image de ϕ contient $E(u)^r\mathfrak{M}$.*

On dispose en outre d'un foncteur contravariant $T^\star_{\text{st}}$ qui, à un module de Breuil–Kisin de hauteur $\leqslant r$, associe une $\mathbb{Z}_p$-représentation libre de G_∞. Ce foncteur a d'importantes propriétés qui ont été, pour la plupart, conjecturées par Breuil puis démontrées par Kisin dans [15]. Le théorème ci-après en donne deux qui nous seront particulièrement utiles dans la suite.

Théorème 1.3. *Soit V une représentation semi-stable à poids dans $\{0, \dots, r\}$. Alors :*

(1) il existe un module de Breuil–Kisin $\mathfrak{M}_0$ de hauteur $\leqslant r$ tel que $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T^\star_{\text{st}}(\mathfrak{M}_0)$ soit isomorphe à V comme G_∞-représentation

(2) le foncteur $T^\star_{\text{st}}$ induit une bijection décroissante entre l'ensemble des modules de Breuil–Kisin $\mathfrak{M} \subset \mathfrak{M}_0[1/p]$ tels que $\mathfrak{M}[1/p] = \mathfrak{M}_0[1/p]$ et l'ensemble des $\mathbb{Z}_p$-réseaux de V stables par G_∞.

Notons pour terminer ce numéro, qu'en plus de cela, si $\mathfrak{M}$ est un module de Kisin et si $T = T^\star_{\text{st}}(\mathfrak{M})$, alors la représentation quotient T/pT peut se retrouver à partir du quotient $\mathfrak{M}/p\mathfrak{M}$ grâce à une recette explicite que nous ne détaillons par davantage ici car elle ne nous sera pas utile.

1.2 Des (ϕ, N)-modules filtrés aux modules de Breuil–Kisin

D'après les rappels que nous venons de faire, à une représentation semi-stable V à poids de Hodge-Tate dans $\{0, \dots, r\}$ sont canoniquement associés deux objets, à savoir :

- le (ϕ, N)-module filtré admissible effectif $D^\star_{\text{st}}(V)$;
- l'espace $\mathfrak{D}(V) = \mathfrak{M}_0[1/p]$ (muni de son action de ϕ) si $\mathfrak{M}_0$ est un module de Breuil–Kisin tel que $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T^\star_{\text{st}}(\mathfrak{M}_0)$ soit isomorphe à V comme G_∞-représentation.

Étant donné que $D^\star_{\text{st}}(V)$ détermine V, il détermine aussi $\mathfrak{D}(V)$. Le but de ce numéro est d'expliquer comment il est possible d'obtenir $\mathfrak{D}(V)$ (ou, du moins, une certaine approximation de celui-ci) directement à partir de $D^\star_{\text{st}}(V)$. Nous suivrons pour cela les travaux de Génestier et Lafforgue exposés dans [14]. Les anneaux $\mathfrak{S}_\nu$, qui sont déjà apparus dans l'introduction, intervenant de façon cruciale dans la construction de Génestier et Lafforgue, nous consacrons le numéro suivant à rappeler quelques unes de leurs propriétés essentielles.

[4] Notez que ceci sera suffisant pour le calcul de la semi-simplifiée modulo p qui nous intéresse car les $\mathbb{F}_p$-représentations semi-simples de G_∞ se trouvent être en bijection avec les $\mathbb{F}_p$-représentations semi-simples de G_K. On renvoie au §2.4 pour plus de détails à ce sujet.

1.2.1 Généralités sur les anneaux $\mathfrak{S}_\nu$

Soit ν un nombre *rationnel* positif ou nul. On rappelle, tout d'abord, que $\mathfrak{S}_\nu$ est défini comme suit :

$$\mathfrak{S}_\nu = \Big\{ \sum_{i\in\mathbb{N}} a_i u^i \quad \Big| \quad a_i \in K_0 \text{ et } \mathrm{val}(a_i) + \nu i \geqslant 0, \, \forall i \geqslant 0 \Big\}.$$

Clairement, pour $\nu = 0$, on a $\mathfrak{S}_\nu = \mathfrak{S}$ et, si $\nu' \geqslant \nu$, on a une inclusion $\mathfrak{S}_\nu \subset \mathfrak{S}_{\nu'}$. En particulier, on a toujours $\mathfrak{S} \subset \mathfrak{S}_\nu$ ou, autrement dit, $\mathfrak{S}_\nu$ est naturellement une $\mathfrak{S}$-algèbre. D'un point de vue analytique, l'anneau $\mathfrak{S}_\nu$ apparaît comme l'anneau des fonctions analytiques convergentes et bornées par 1 sur le disque D_ν de centre 0 et de rayon $|p|^\nu$. L'anneau $\mathfrak{S}_\nu[1/p]$ jouera un rôle particulier dans la suite ; on le note $\mathcal{E}^+_\nu$ et, lorsque $\nu = 0$, on s'affranchira de l'indice et notera simplement $\mathcal{E}^+$. D'un point de vue analytique, $\mathcal{E}^+_\nu$ s'identifie à l'anneau des fonctions analytiques convergentes bornées sur D_ν.

Le Frobenius ϕ défini par $\phi(\sum a_i u^i) = \sum \sigma(a_i) u^{pi}$ induit des morphismes d'anneaux $\phi : \mathfrak{S}_\nu \to \mathfrak{S}_{\nu/p}$ et $\phi : \mathcal{E}^+_\nu \to \mathcal{E}^+_{\nu/p}$ et donc, en particulier, puisque $\nu \geqslant 0$, il induit des endomorphismes de $\mathfrak{S}_\nu$ et $\mathcal{E}^+_\nu$.

On introduit la *valuation de Gauss* v_ν définie par :

$$v_\nu(f) = \inf_{i\in\mathbb{N}} (\mathrm{val}(a_i) + i\nu)$$

pour une série $f = \sum_{i\in\mathbb{N}} a_i u^i \in \mathcal{E}^+_\nu$. On vérifie sans difficulté que v_ν vérifie les propriétés suivantes : pour tous $f, g \in \mathcal{E}_\nu$, on a $v_\nu(fg) = v_\nu(f) + v_\nu(g)$ et $v_\nu(f+g) \geqslant \min(v_\nu(f), v_\nu(g))$. De plus, une série f comme précédemment est dans $\mathfrak{S}_\nu$ si, et seulement si $v_\nu(f) \geqslant 0$. Comme ν est supposé rationnel, la quantité $\mathrm{val}(a_i) + i\nu$ varie dans le sous-groupe discret $\mathbb{Z} + \nu\mathbb{Z}$ de $\mathbb{R}$. Il en résulte que v_ν prend également ses valeurs dans ce sous-groupe discret, et est donc une valuation discrète. Concrètement, si $\frac{a}{b}$ est une écriture de ν sous forme irréductible, alors $\mathbb{Z} + \nu\mathbb{Z} = \frac{1}{b}\mathbb{Z}$ et, si s et t désignent deux entiers tels que $as - bt = 1$, l'élement $\frac{u^s}{p^t}$ a pour valuation $\frac{1}{b}$. On définit le *degré de Weierstrass* $\deg_\nu(f)$ d'une série $f \in \mathcal{E}^+_\nu$ non nulle comme le plus petit entier i tel que $v_\nu(f) = \mathrm{val}(a_i) + i\nu$. On vérifie que, pour $f, g \in \mathcal{E}^+_\nu$ tous les deux non nuls, on a $\deg_\nu(fg) = \deg_\nu(f) + \deg_\nu(g)$. On a alors la proposition suivante qui implique, en particulier, que $\mathcal{E}^+_\nu$ est un anneau euclidien (pour le stathme $\deg_\nu$), ce qui s'avèrera fort utile au §2 pour les applications algorithmiques.

Proposition 1.4 (Division euclidienne)**.** *Soient f et g deux éléments de $\mathfrak{S}_\nu$ avec $v_\nu(g) \geqslant v_\nu(f)$. Alors, il existe un unique couple $(q, r) \in \mathfrak{S}^2_\nu$ tel que (1) r est un* polynôme *de degré $< \deg_\nu(f)$ et (2) on a la relation $g = fq + r$.*

Comme corollaire de cette proposition, on démontre le théorème de préparation de Weierstrass qui affirme que tout élément $f \in \mathcal{E}^+_\nu$ s'écrit comme un produit $f_1 f_2$ où f_1 est un *polynôme* et f_2 un élément inversible de $\mathcal{E}^+_\nu$. Si, en outre, f est pris dans $\mathfrak{S}_\nu$, alors on peut choisir f_1 et f_2 de sorte qu'ils appartiennent eux aussi à $\mathfrak{S}_\nu$ et, de surcroît, que f_2 soit inversible dans cet anneau (et pas uniquement dans $\mathcal{E}^+_\nu$).

On rappelle enfin qu'à chaque élément $f = \sum a_i u^i \in \mathcal{E}^+_\nu$, on peut associer un polygone de Newton F défini comme l'enveloppe convexe des points de coordonnées $(i, \mathrm{val}(a_i))$ et d'un point à l'infini de coordonnées $(0, \infty)$; il s'agit donc d'un sous-ensemble convexe de $\mathbb{R}^2$. Le fait que $f \in \mathcal{E}^+_\nu$ entraîne que les pentes de ce polygone qui sont strictement inférieures à $-\nu$, comptées avec multiplicité[5], sont en nombre fini. De surcroît, elles correspondent aux valuations des racines de f (vue comme fonction analytique) dans le disque D_ν, comptées également avec multiplicité.

[5] La multiplicité d'une pente est, par définition, sa longueur sur l'axe des abscisses.

On en déduit que les pentes $< -\nu$ du produit fg sont exactement les réunion des pentes $< -\nu$ de f et de g, comptées avec multiplicité. Attention, ceci n'est plus vrai pour les pentes $\geqslant -\nu$. Un contre-exemple très simple avec $\nu = 0$ est donné par $f = 1 - u$ et $g = \frac{1}{1-u} = 1 + u + u^2 + \cdots$. En effet, f a alors une unique pente 0 de multiplicité 1, g a une unique pente 0 de multiplicité $+\infty$, mais pourtant le produit $fg = 1$ n'a aucune pente. On a toutefois le lemme suivant qui nous sera utile dans la suite.

Lemme 1.5. *Soient f et g deux éléments de $\mathcal{E}_\nu^+$. Soit μ un nombre rationnel. On note m_f (resp. m_g) la multiplicité (éventuellement nulle) de la pente μ dans le polygone de Newton de f (resp. de g). On suppose que l'on est dans un des deux cas suivants (non exclusifs) :*

(i) les deux multiplicités m_f et m_g sont finies ;

(ii) l'une des multiplicités parmi m_f et m_g est nulle.

Alors la multiplicité de la pente μ dans le polygone de Newton de fg est $m_f + m_g$.

Démonstration. Quitte à remplacer, dans la définition de $\mathfrak{S}_\nu$, le corps des coefficients K_0 par une extension finie totalement ramifiée, puis à effectuer un changement de variables et à multiplier f et g par des puissances adéquates de l'uniformisante de K_0, on peut supposer que $\mu = 0$, que f et g sont à coefficients dans $\mathfrak{S}$ et que $v_0(f) = v_0(g) = 0$. Soient $\bar{f}$ et $\bar{g}$ les réductions respectives de f et g modulo l'idéal maximal de $\mathcal{O}_{K_0}$; ce sont *a priori* des éléments de l'anneau $k[[u]]$ des séries formelles à coefficients dans k, qui ne sont pas nuls d'après la condition sur v_0 qui a été supposée. Soit v_f (resp. v_g) la valuation de $\bar{f}$ (resp. $\bar{g}$).

Dans le cas (i), les séries $\bar{f}$ et $\bar{g}$ sont des polynômes et on a $\deg(\bar{f}) = v_f + m_f$ et $\deg(\bar{g}) = v_g + m_g$. Ainsi $\deg(\bar{f}\bar{g}) = (v_f + v_g) + (m_f + m_g)$. Étant donné que $v_f + v_g$ est la valuation du produit $\bar{f}\bar{g}$, on en déduit que la multiplicité de la pente $\mu = 0$ dans le polygone de Newton de fg est $m_f + m_g$, comme souhaité.

Passons maintenant au cas (ii). On suppose $m_f = 0$ pour fixer les idées. On peut supposer de surcroît que $m_g = +\infty$ car sinon la situation relève du cas précédent. La série $\bar{f}$ est alors un monôme, tandis que $\bar{g}$ n'est pas un polynôme. On en déduit que $\bar{f}\bar{g}$ n'est pas non plus un polynôme et donc que la multiplicité de la pente $\mu = 0$ dans le polygone de Newton de fg est infinie. C'est bien ce que l'on voulait démontrer. □

1.2.2 La méthode de Génestier et Lafforgue

Soit D un (ϕ, N)-module filtré effectif admissible dont la représentation galoisienne semi-stable correspondante est notée V. Le premier alinéa du théorème 1.3 affirme qu'il existe un module de Breuil–Kisin $\mathfrak{M}_0$ tel que $T_{\text{st}}^\star(\mathfrak{M}_0)$ soit un réseau pour G_∞ à l'intérieur de V, tandis que le second alinéa de ce même théorème montre que $\mathfrak{D} = \mathfrak{M}_0[1/p]$ ne dépend pas du choix de $\mathfrak{M}_0$. Ainsi, l'espace $\mathfrak{D}$ muni de l'action de ϕ est canoniquement associé à D. Le but de ce numéro est d'expliquer, en suivant [14], comment construire $\mathfrak{D}$ directement à partir de D, sans passer par les représentations galoisiennes.

En suivant la terminologie de Génestier et Lafforgue, la première étape consiste à associer à D une structure de Hodge-Pink. Soit $\hat{\mathfrak{S}}$ le complété de $\mathcal{E}^+$ pour la topologie $E(u)$-adique (*i.e.* celle relative à l'idéal principal engendré par $E(u)$). La flèche $u \mapsto \pi + u_\pi$ définit un isomorphisme canonique $\mathcal{E}^+/E(u)^n \to K[u_\pi]/u_\pi^n$ pour tout entier n et donc, par passage à la limite, un isomorphisme canonique entre $\hat{\mathfrak{S}}$ et l'anneau $K[[u_\pi]]$ des séries formelles à coefficients dans K. En particulier, cette identification permet de définir une structure canonique de K-algèbre sur $\hat{\mathfrak{S}}$. D'autre part, on remarque que l'idéal principal $(E(u))$ correspond, dans $K[[u_\pi]]$, à l'idéal maximal $u_\pi K[[u_\pi]]$. Ainsi l'identification $\hat{\mathfrak{S}} \simeq K[[u_\pi]]$ se prolonge en un isomorphisme canonique

$\hat{\mathfrak{S}}[\frac{1}{E(u)}] \simeq K((u_\pi))$. La dérivation $u\,\frac{d}{du}$ envoie $E(u)^h$ sur un multiple de $E(u)^{h-1}$ pour tout h et définit de ce fait un endomorphisme K_0-linéaire de $\hat{\mathfrak{S}}$; on le note $\hat{N}$. *Via* l'identification $\hat{\mathfrak{S}} \simeq K[[u_\pi]]$, on a $\hat{N} = (u_\pi + \pi)\frac{d}{du_\pi}$. Ceci montre en particulier que $\hat{N}$ est K-linéaire (et pas seulement K_0-linéaire). Bien sûr, on dispose également de la formule de Leibniz habituelle $\hat{N}(ab) = a\hat{N}(b) + b\hat{N}(a)$ pour tous $a, b \in \hat{\mathfrak{S}}$.

Étant donné un (ϕ, N)-module filtré D, on s'intéresse à l'espace $\hat{\mathfrak{D}} = \hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_{\phi,K_0} D$ où le ϕ en indice dans le produit tensoriel signifie que $\mathfrak{S}[\frac{1}{E(u)}]$ est vu comme une K_0-algèbre *via* le Frobenius $\phi : K_0 \to K_0 \to \mathfrak{S}[\frac{1}{E(u)}]$ où la première flèche est le Frobenius σ et la seconde est l'inclusion canonique. En « développant » le produit tensoriel, on obtient une identification canonique $\hat{\mathfrak{D}} \simeq \hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_K D_K^\phi$ avec $D_K^\phi = K \otimes_{\phi,K_0} D$. Le Frobenius ϕ définit un isomorphisme K_0-linéaire $K_0 \otimes_{\phi,K_0} D$ qui s'étend de façon unique en un isomorphisme K-linéaire $\phi_K : D_K^\phi \to D_K$. L'opérateur de monodromie N s'étend lui aussi par linéarité en un endomorphisme N_K de D_K. On appelle également N_K^ϕ l'endomorphisme de D_K^ϕ défini par $N_K^\phi = p \otimes N$. La relation $N\phi = p\phi N$ se réécrit alors $N_K\phi_K = \phi_K N_K^\phi$. On définit, à présent, un opérateur différentiel $\hat{N}$ agissant sur $\hat{\mathfrak{D}} \simeq \hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_K D_K^\phi$ par la formule

$$\hat{N} = \hat{N} \otimes \mathrm{id} + \mathrm{id} \otimes N_K^\phi.$$

La relation de Leibniz est à nouveau vérifiée pour ce dernier $\hat{N}$: pour tout $s \in \hat{\mathfrak{S}}$ et tout $x \in \hat{\mathfrak{D}}$, on a $\hat{N}(sx) = \hat{N}(s)\,x + s\,\hat{N}(x)$.

On est enfin prêt à introduire les structures de Hodge-Pink de Génestier et Lafforgue :

Définition 1.6 (Génestier-Lafforgue)**.** *Soit D un (ϕ, N)-module filtré. Une* structure de Hodge-Pink *V_D sur D est un $\hat{\mathfrak{S}}$-module libre de rang d inclus dans $\hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_{\phi,K_0} D$.*

On dit que V_D satisfait à la transversalité de Griffiths *si $\hat{N}(V_D) \subset \frac{1}{E(u)} V_D$.*

Une structure de Hodge-Pink sur D définit une filtration $\mathrm{Fil}_{\mathrm{HP}}^h D_K$ indexée par $\mathbb{Z}$ sur l'espace $D_K = K \otimes_{K_0} D$ déterminée par la relation :

$$\phi_K^{-1}(\mathrm{Fil}_{\mathrm{HP}}^h D_K) = \text{image de } E(u)^h V_D \cap (\hat{\mathfrak{S}} \otimes_{K_0} D) \text{ dans } \mathfrak{S}/E(u)\mathfrak{S} \otimes_{K_0} D$$

ce dernier espace s'identifiant à D_K^ϕ par l'intermédiaire de l'isomorphisme canonique $\mathfrak{S}/E(u)\mathfrak{S} \to K$, $u \mapsto \pi$. Le fait que $\mathrm{Fil}_{\mathrm{HP}}^h D_K = D_K$ pour tout $h \leqslant 0$ est équivalent à $\hat{\mathfrak{S}} \otimes_{K_0} D \subset V_D$. De même $\mathrm{Fil}_{\mathrm{HP}}^{r+1} D_K = 0$ si, et seulement si $V_D \subset E(u)^{-r}\hat{\mathfrak{S}} \otimes_{K_0} D$.

Lemme 1.7. *Soit D un (ϕ, N)-module filtré. Alors, il existe une unique structure de Hodge-Pink V_D sur D satisfaisant à la transversalité de Griffiths et dont la filtration associée s'identifie à la filtration* $\mathrm{Fil}^h D_K$ *donnée.*

Démonstration. Voir lemme 1.3 de [14]. □

Pour pouvoir continuer à appliquer la méthode de Génestier et Lafforgue, on a besoin d'une structure de Hodge-Pink incluse dans $\hat{\mathfrak{S}} \otimes_{\phi,K_0} D$. Or cela n'est manifestement pas le cas de V_D. Pour se ramener au cas où cette hypothèse est satisfaite, on fixe un entier r supérieur ou égal à tous les poids de Hodge-Tate de la représentation associée au (ϕ, N)-module filtré D et on *twiste* D comme ceci : on pose $D' = D$ que l'on munit de $\phi' = \frac{\phi}{p^r}$ et de la filtration décalée définie par $\mathrm{Fil}^h D' = \mathrm{Fil}^{h+r} D$ pour tout $h \in \mathbb{Z}$. Le structure de Hodge-Pink associée à D' est alors $V_{D'} = E(u)^r V_D$; elle est donc incluse dans $\hat{\mathfrak{S}} \otimes_{\phi,K_0} D$ comme voulu. Toujours suivant Génestier

et Lafforgue, étant donné L un sous-$\mathcal{O}_{K_0}$-module de D, on définit à présent une suite $(\beta_n(L))_{n\geqslant 0}$ de sous-$\mathfrak{S}$-modules de $\mathcal{E}^+ \otimes_{K_0} D' = \mathcal{E}^+ \otimes_{K_0} D$ par la formule récurrente suivante :

$$\begin{aligned}\beta_0(L) &= \mathfrak{S} \otimes_{\mathcal{O}_{K_0}} L,\\ \beta_{n+1}(L) &= \phi'\big((\mathfrak{S} \otimes_{\phi,\mathfrak{S}} \beta_n(L)) \cap V_{D'}\big) = \frac{\phi}{p^r}\big((\mathfrak{S} \otimes_{\phi,\mathfrak{S}} \beta_n(L)) \cap E(u)^r V_D\big). \qquad (1)\end{aligned}$$

La formule que l'on vient d'écrire présente deux petites subtilités : *primo*, l'intersection $(\mathfrak{S} \otimes_{\phi,\mathfrak{S}} \beta_n(L)) \cap E(u)^r V_D$ est calculée dans l'espace $\hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_{\phi,K_0} D$ et *secundo*, la lettre ϕ (resp. ϕ') désigne ici l'application *linéaire* $\mathcal{E}^+ \otimes_{\phi,K_0} D \to \mathcal{E}^+ \otimes D$ déduite du Frobenius ϕ (resp. $\phi' = \frac{\phi}{p^r}$) agissant sur D. On prendra garde au fait que l'on ne peut pas définir un Frobenius sur $\hat{\mathfrak{S}}[\frac{1}{E(u)}]$ étant donné qu'aucune puissance de $\phi(E(u))$ n'est divisible par $E(u)$; ainsi on ne peut pas non plus définir de Frobenius sur le gros espace $\hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_{\phi,K_0} D$; toutefois, cela n'est aucunement nécessaire car l'intersection que l'on considère est incluse dans l'espace $\mathcal{E}^+ \otimes_{\phi,K_0} D$ sur lequel les opérateurs ϕ et ϕ' sont bien définis.

Lorsque $L = D$, on note simplement β_n à la place de $\beta_n(D)$. Les β_n sont des sous-$\mathcal{E}^+$-modules libres de $\mathcal{E}^+ \otimes_{\phi,K_0} D$ et on démontre sans difficulté, par récurrence sur n, que $\mathcal{E}^+ \otimes_{\mathfrak{S}} \beta_n(L) = \beta_n$ pour tout entier n et tout sous-$\mathcal{O}_{K_0}$-module L de D. Grâce à cette remarque, le théorème suivant résulte des travaux de Génestier et Lafforgue.

Théorème 1.8 (Génestier-Lafforgue)**.** *Pour tout entier n, l'espace $\mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \beta_n \subset \mathcal{E}^+_{1/(ep^n)} \otimes_{K_0} D$ est stable par l'opérateur $(\frac{E(u)}{E(0)})^r \phi \otimes \phi$. De plus, on a un isomorphisme canonique ξ_n : $\mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \beta_n \to \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \mathfrak{D}$ rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc} \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \beta_n & \xrightarrow[\xi_n]{\sim} & \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \mathfrak{D} \\ \Big\downarrow{\scriptstyle (\frac{E(u)}{E(0)})^r \phi\otimes\phi} & & \Big\downarrow{\scriptstyle \phi\otimes\phi} \\ \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \beta_n & \xrightarrow[\xi_n]{\sim} & \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \mathfrak{D} \end{array}$$

où la flèche de droite provient du Frobenius ϕ agissant sur $\mathfrak{D}$ donné par la théorie de Breuil–Kisin.

Remarque 1.9. *Il suit du résultat de Génestier et Lafforgue que l'on vient d'énoncer que si L est un $\mathcal{O}_{K_0}$-réseau de D, il existe une constante C et un module de Breuil–Kisin $\mathfrak{M}_{1/(ep^n)}$ tels que :*

$$\mathfrak{S}_\nu \otimes_{\mathfrak{S}} \beta_n(L) \subset \mathfrak{M}_{1/(ep^n)} \subset p^{-C} \cdot (\mathfrak{S}_\nu \otimes_{\mathfrak{S}} \beta_n(L)).$$

En réalité, en examinant de près la démonstration de Génestier et Lafforgue, on se rend compte que la constante C ci-dessus dépend de façon explicite et polynômiale[6] *de la dimension d, de l'entier n et du plus petit entier v tel que $p^v \phi(L) \subset L$.*

1.3 Surconvergence des modules de Breuil–Kisin

Dans le §1.2.2, nous avons été amené à considérer l'extension des scalaires à certains anneaux $\mathfrak{S}_\nu$ de modules de Breuil–Kisin. L'objectif de cette partie est de montrer que ce foncteur d'extension des scalaires possède d'excellentes propriétés lorsque ν reste petit.

On introduit pour cela la définition suivante, copie conforme de la définition des modules de Breuil–Kisin usuels.

[6]Cela sera très important dans la suite lorsque l'on étudiera la complexité de l'algorithme du calcul de la semi-simplifiée modulo p.

Définition 1.10. *Soient ν un nombre rationnel positif ou nul et r un nombre entier strictement positif. Un* module de Breuil–Kisin *sur $\mathfrak{S}_\nu$ de hauteur $\leqslant r$ est la donnée d'un $\mathfrak{S}_\nu$-module libre $\mathfrak{M}_\nu$ de rang fini muni d'une application $\phi : \mathfrak{M}_\nu \to \mathfrak{M}_\nu$ telle que :*

1. *pour tout $s \in \mathfrak{S}_\nu$ et tout $x \in \mathfrak{M}_\nu$, on a $\phi(sx) = \phi(s)\phi(x)$;*
2. *le sous-$\mathfrak{S}_\nu$-module engendré par l'image de ϕ contient $E(u)^r\mathfrak{M}_\nu$.*

Pour un nombre rationnel $\nu \geqslant 0$, on note $\mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_\nu}$ la catégorie des modules de Kisin de hauteur $\leqslant r$ sur $\mathfrak{S}_\nu$ et, si $0 \leqslant \nu \leqslant \nu'$, on note $F_{\nu\to\nu'} : \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_\nu} \to \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_{\nu'}}$ le foncteur d'extension des scalaires de $\mathfrak{S}_\nu$ à $\mathfrak{S}_{\nu'}$.

Théorème 1.11. *Le foncteur $F_{0\to\nu}$ est une équivalence de catégories dès que $\nu < \frac{p-1}{per}$.*

La démonstration de ce théorème va occuper toute la fin de cette partie. Elle repose sur les deux lemmes suivants que nous démontrerons respectivement dans le §1.3.1 et le §1.3.2.

Lemme 1.12. *Si ν et ν' sont des nombres rationnels positifs ou nuls vérifiant $\nu' \leqslant \nu < \frac{p-1}{er}$ et $\nu' < \frac{p-1}{per}$, alors le foncteur $F_{\nu'\to\nu}$ est pleinement fidèle.*

Lemme 1.13. *Pour tout $\nu < \frac{p-1}{per}$ et tout objet $\mathfrak{M}_\nu$ de $\mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_\nu}$, il existe un objet $\mathfrak{M} \in \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}}$ et un isomorphisme $F_{0\to\nu'}(\mathfrak{M}) \to F_{\nu\to\nu'}(\mathfrak{M}_\nu)$ dans la catégorie $\mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_{\nu'}}$ où ν' est défini comme le rationnel solution de l'équation $\frac{1}{\nu'} = \frac{1}{\nu} - er$.*

Expliquons à présent comment le théorème 1.11 se déduit des deux lemmes précédents. Clairement la pleine fidélité de $F_{0\to\nu}$ suit du lemme 1.12 en prenant $\nu' = 0$. Il ne reste donc plus qu'à démontrer l'essentielle surjectivité. Pour cela, on remarque qu'en termes plus concis mais plus abstraits, le lemme 1.13 affirme que, si $\nu < \frac{p-1}{per}$ et si ν' est défini par l'égalité $\frac{1}{\nu'} = \frac{1}{\nu} - er$ alors, dans le diagramme suivant :

$$\begin{array}{ccc} & \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}} & \\ {\scriptstyle F_{0\to\nu}}\swarrow & & \searrow{\scriptstyle F_{0\to\nu'}} \\ \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_\nu} & \xrightarrow[F_{\nu\to\nu'}]{} & \mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_{\nu'}} \end{array}$$

les foncteurs $F_{0\to\nu'}$ et $F_{\nu\to\nu'}$ ont même image essentielle. L'essentielle surjectivité de $F_{0\to\nu}$ suit alors directement de la pleine fidélité des $F_{0\to\nu'}$ et $F_{\nu\to\nu'}$, résultats que l'on connaît grâce au lemme 1.12.

1.3.1 Démonstration du lemme 1.12

Soient ν et ν' deux nombres rationnels tels que $0 \leqslant \nu' \leqslant \nu < \frac{p-1}{er}$ et $\nu' < \frac{p-1}{per}$. On se donne $\mathfrak{M}_{\nu'}$ et $\mathfrak{M}'_{\nu'}$ deux modules de Breuil–Kisin sur $\mathfrak{S}_{\nu'}$, ainsi qu'un morphisme $f : \mathfrak{S}_\nu \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}_{\nu'} \to \mathfrak{S}_\nu \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}$ dans la catégorie $\mathrm{Mod}^{r,\phi}_{/\mathfrak{S}_\nu}$. On souhaite démontrer que f envoie $\mathfrak{M}_{\nu'}$ sur $\mathfrak{M}'_{\nu'}$. L'argument de base se développe comme suit. Si on sait que $f(\mathfrak{M}_{\nu'}) \subset A \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}$, pour un certain $\mathfrak{S}_{\nu'}$-module $A \subset \mathfrak{S}_\nu$, alors

$$\begin{aligned} E(u)^r f(\mathfrak{M}_{\nu'}) &= f(E(u)^r\mathfrak{M}_{\nu'}) \subset f(\langle\phi(\mathfrak{M}_{\nu'})\rangle_{\mathfrak{S}_{\nu'}}) = \langle f\circ\phi(\mathfrak{M}_{\nu'})\rangle_{\mathfrak{S}_{\nu'}} \\ &= \langle\phi\circ f(\mathfrak{M}_{\nu'})\rangle_{\mathfrak{S}_{\nu'}} \subset \left\langle\phi(A\otimes_{\mathfrak{S}_{\nu'}}\mathfrak{M}'_{\nu'})\right\rangle_{\mathfrak{S}_{\nu'}} \subset \langle\phi(A)\rangle_{\mathfrak{S}_{\nu'}} \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}. \end{aligned}$$

Ainsi, si l'on note $\frac{\phi}{E(u)^r}(A)$ le sous-$\mathfrak{S}_{\nu'}$-module de $\mathfrak{S}_\nu$ formé des x tels que $E(u)^r x \in \langle \phi(A)\rangle_{\mathfrak{S}_{\nu'}}$, on a démontré que $f(\mathfrak{M}_{\nu'}) \subset \frac{\phi}{E(u)^r}(A) \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}$. En appliquant le même argument avec $\frac{\phi}{E(u)^r}(A)$ à la place de A, on obtient alors $f(\mathfrak{M}_{\nu'}) \subset (\frac{\phi}{E(u)^r})^2(A) \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}$ et, ainsi de suite, $f(\mathfrak{M}_{\nu'}) \subset (\frac{\phi}{E(u)^r})^n(A) \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}'_{\nu'}$ pour tout entier n. Pour conclure, il reste donc à montrer que :

$$\bigcap_{n\geqslant 0} \Big(\frac{\phi}{E(u)^r}\Big)^n(\mathfrak{S}_\nu) = \mathfrak{S}_{\nu'}. \tag{2}$$

Lemme 1.14. *Pour tout réel $\mu \in [0, \frac{p-1}{er}[$ on a $\frac{\phi}{E(u)^r}(\mathfrak{S}_{1/\mu}) \subset \mathfrak{S}_{1/\mu'}$ avec $\mu' = \min\big(\frac{1}{\nu}, p\mu - er\big)$.*

Démonstration. Il suffit de montrer que si f est un élément de $\mathfrak{S}_{\nu'}$ tel que $E(u)^r f \in \phi(\mathfrak{S}_{1/\mu})$, alors $f \in \mathfrak{S}_{1/\mu'}$. Supposons donc qu'il existe $g \in \mathfrak{S}_{1/\mu}$ tel que $E(u)^r f = \phi(g)$. Soit F (resp. G) le polygone du Newton de f (resp. de g). Si on appelle Φ la fonction de $\mathbb{R}^2$ dans $\mathbb{R}^2$ qui à (x, y) associe (px, y), l'épigraphe du polygone de Newton de $\phi(g)$ est $\Phi(G)$. On note encore E l'épigraphe du polygone de Newton de $E(u)$. Comme $\nu' < \frac{p-1}{per}$, la pente $-\frac{1}{e}$ ne peut avoir une multiplicité infinie dans le polygone F. On déduit alors du lemme 1.5 et de l'égalité $E(u)^r f = \phi(g)$, que $E + F = \Phi(G)$.

Or, par définition, G est inclus dans le demi-espace défini par l'inégalité $y + \frac{x}{\mu} \geqslant 0$. Ainsi les couples (x, y) dans $\Phi(G)$ vérifie $y + \frac{x}{p\mu} \geqslant 0$. Si maintenant $(x, y) \in F$, on déduit de l'égalité $E + F = \Phi(G)$ que $(x + er, y) \in \Phi(G)$ et donc que $y + \frac{x+er}{p\mu} \geqslant 0$. En d'autres termes, si on écrit $f = \sum_{i\in\mathbb{N}} a_i u^i$, on vient de démontrer que $\mathrm{val}(a_i) \geqslant -\frac{i+er}{p\mu}$ pour tout i. Comme $\mathrm{val}(a_i)$ est un entier, on en déduit que $\mathrm{val}(a_i) \geqslant \lceil -\frac{i+er}{p\mu} \rceil$ pour tout i (où $\lceil x \rceil$ dénote la partie entière supérieure du réel x). En particulier, si $i < p\mu - er$, on obtient $\mathrm{val}(a_i) \geqslant 0$. Si, au contraire, $i \geqslant p\mu - er$, on peut écrire :

$$\mathrm{val}(a_i) \geqslant -\frac{i+er}{p\mu} \geqslant -\frac{i}{p\mu - er} \geqslant -\frac{i}{\mu'}$$

l'inégalité du milieu résultant de l'hypothèse faite sur μ. Ainsi, dans tous les cas (*i.e.* quelle que soit la valeur de i), on a $\mathrm{val}(a_i) + \frac{i}{\mu'} \geqslant 0$ pour tout i. Cela signifie que $f \in \mathfrak{S}_{1/\mu'}$ comme souhaité. □

Il suit du lemme 1.14 que $(\frac{\phi}{E(u)^r})^n(\mathfrak{S}_\nu) \subset \mathfrak{S}_{1/\mu_n}$ où la suite $(\mu_n)_{n\geqslant 0}$ est définie par récurrence par $\mu_0 = \frac{1}{\nu}$ et $\mu_{n+1} = \min\big(\frac{1}{\nu'},\ p\mu_n - er\big)$ pour tout entier $n \geqslant 0$. Puisque $\nu < \frac{p-1}{er}$, on a $\mu_0 > \frac{er}{p-1}$ et il suit de là que la suite des μ_n converge vers $\frac{1}{\nu'}$ (s'il n'y avait pas le $\min$, elle tendrait par $+\infty$). On en déduit l'égalité (2) de laquelle résulte, comme cela a déjà été expliqué, la pleine fidélité du foncteur $F_{\nu'\to\nu}$.

1.3.2 Démonstration du lemme 1.13

On en vient maintenant à la démonstration du lemme 1.13. On se donne pour cela ν et $\mathfrak{M}_\nu$ comme dans l'énoncé. On fixe une $\mathfrak{S}_\nu$-base de $\mathfrak{M}_\nu$ et on note G_0 la matrice du Frobenius ϕ dans cette base. Par hypothèse, il existe une matrice H_0 telle que $H_0 G_0 = E(u)^r$.

Lemme 1.15. *Tout élément $g \in \mathfrak{S}_\nu$ se décompose sous la forme $E(u)^r x + y$ avec $x = \sum_{i\geqslant 1/\nu'} x_i u^i \in \mathfrak{S}_{\nu'}$ et $y \in \mathfrak{S}$.*

Démonstration. Comme $E(u)$ est un polynôme d'Eisenstein de degré e, on peut décomposer $E(u)^r$ sous la forme $E(u)^r = u^{er} - pF(u)$ où $F(u)$ est un polynôme à coefficients dans $\mathcal{O}_{K_0}$. Soit $g = \sum_{i\in\mathbb{N}} a_i u^i$ un élément de $\mathfrak{S}_\nu$. Il se décompose sous la forme $g = E(u)^r x_1 + y_1 + g_1$ avec

$$x_1 = \sum_{i\geqslant 1/\nu} a_i u^{i-er} = \sum_{i\geqslant 1/\nu'} a_{i+er} u^i \quad ; \quad y_1 = \sum_{0\leqslant i<1/\nu} a_i u^i \quad ; \quad g_1 = pF(u)\cdot x_1.$$

Un calcul facile montre, d'une part, que $x_1 \in \mathfrak{S}_{\nu'}$, $y_1 \in \mathfrak{S}$ et $g_1 \in \mathfrak{S}_\nu$ et, d'autre part, que $v_{\nu'}(x_1) \geqslant v_\nu(g_1)$, $v_\nu(y_1) \geqslant v_\nu(g_1)$ et $v_\nu(g_1) \geqslant v_\nu(x_1) + (1 - er\nu) > v_\nu(x_1) + \frac{1}{p-1}$. Répétant maintenant la construction précédente à partir de g_1, puis itérant le procédé, on obtient des suites (x_n), (y_n) et (g_n) prenant leurs valeurs respectivement dans $\mathfrak{S}_{\nu'}$, $\mathfrak{S}$ et $\mathfrak{S}_\nu$ telles que, pour tout entier n, on ait $g = E(u)^r(x_1 + x_2 + \cdots + x_n) + (y_1 + y_2 + \cdots + y_n) + g_n$. On dispose en outre des estimations suivantes sur les valuations :

$$v_{\nu'}(x_n) \geqslant v_\nu(g_1) + \frac{n-1}{p-1} \quad ; \quad v_\nu(y_n) \geqslant v_\nu(g_1) + \frac{n-1}{p-1} \quad ; \quad v_\nu(g_n) \geqslant v_\nu(g_1) + \frac{n}{p-1}$$

valables pour tout entier $n \geqslant 1$. Il en résulte que les suites (x_n), (y_n) et (g_n) tendent toutes les trois vers 0. On peut donc définir $x = \sum_{n\in\mathbb{N}} x_n \in \mathfrak{S}_{\nu'}$ et $y = \sum_{n\in\mathbb{N}} y_n \in \mathfrak{S}$. Ces éléments vérifient l'égalité $g = E(u)^r x + y$; on a donc bien établi la décomposition annoncée. □

Par le lemme, la matrice G_0 se décompose sous la forme $G_0 = Y_0 - E(u)^r X_0$ où X_0 est une matrice à coefficients dans $\mathfrak{S}_{\nu'} \ll$ multiple de $u^{1/\nu'} \gg$ et Y_0 est à coefficients dans $\mathfrak{S}$. On pose $P_0 = I + X_0 H_0$, où I désigne la matrice identité (de taille adéquate). Manifestement, P_0 est à coefficients dans $\mathfrak{S}_{\nu'}$ et la condition sur X_0 entraîne qu'elle est inversible. En outre, la matrice produit $G_1 = P_0 G_0 \phi(P_0)^{-1} = (G_0 + E(u)^r X_0)\phi(P_0)^{-1} = Y_0 \phi(P_0)^{-1}$ est, elle, à coefficients dans $\mathfrak{S}_{\nu'/p}$ puisque le premier facteur est à coefficients dans $\mathfrak{S}$ et que le second est à coefficients dans $\mathfrak{S}_{\nu'/p}$.

Comme la matrice $P_0 G_0 = Y_0$ est à coefficients dans $\mathfrak{S}$, son déterminant δ appartient aussi à $\mathfrak{S}$. Par ailleurs, celui-ci s'écrit comme le produit de $\det P_0$, qui est un élément inversible dans $\mathfrak{S}_{\nu'}$, et de $\det G_0$ qui s'écrit, à son tour, comme le produit d'une certaine puissance $E(u)^N$ de $E(u)$ et d'une unité de $\mathfrak{S}_\nu$. Ainsi $\delta = aE(u)^N$ où a est un élément inversible de $\mathfrak{S}_{\nu'}$. En particulier, le coefficient constant de a est inversible dans $\mathcal{O}_{K_0}$. Grâce au lemme 1.5, on en déduit que le polygone de Newton de δ passe par le point de coordonnées $(0, N)$ et contient un segment de pente $-\frac{1}{e}$ qui a une longueur eN sur l'axe des abscisses. Comme ce polygone est entièrement situé au-dessus de l'axe des abscisses (puisque $\delta \in \mathfrak{S}$), tous ses autres segments ont nécessairement une pente $\geqslant 0$. Comme ces autres segments sont exactement ceux qui forment le polygone de Newton de a, il s'ensuit que a est en fait élément de $\mathfrak{S}$ et, mieux encore, qu'il est inversible dans cet anneau.

Les diviseurs élémentaires de la matrice $P_0 G_0$ vue comme matrice à coefficients dans l'anneau principal $\mathcal{E}^+ = \mathfrak{S}[1/p]$ sont donc tous (à multiplication par des unités près) des puissances de $E(u)$, qui est premier dans cet anneau. Lorsque l'on étend les scalaires à $\mathcal{E}^+_{\nu'}$, ces diviseurs élémentaires restent les mêmes et sont également ceux de G_0 puisque $P_0 G_0$ s'obtient manifestement à partir de G_0 en multipliant à gauche par une matrice inversible à coefficients dans $\mathfrak{S}_{\nu'}$, et donc *a fortioti* dans $\mathcal{E}^+_{\nu'}$. Ceci entraîne que les exposants sur ces diviseurs élémentaires sont tous $\leqslant r$ et donc qu'il existe une matrice H' à coefficients dans $\mathcal{E}^+$ vérifiant $H' P_0 G_0 = E(u)^r$. Par ailleurs, vue la forme de δ, il existe également une matrice H'' à coefficients dans $\mathfrak{S}$ telle que $H'' P_0 G_0 = E(u)^N$ pour un entier N que l'on peut bien sûr choisir supérieur à r. On en déduit que $E(u)^{N-r} H' = H''$ et donc que $E(u)^{N-r} H'$ est à coefficients dans $\mathfrak{S}$. De $v_0(E(u)) = 0$, on déduit que H' est également à coefficients dans $\mathfrak{S}$. La matrice produit $H_1 = \phi(P_0) H'$ est alors à coefficients dans $\mathfrak{S}_{\nu'/p}$ et vérifie $H_1 G_1 = \phi(P_0) H' P_0 G_0 \phi(P_0)^{-1} = E(u)^r$. On en déduit que la matrice G_1 définit un module de Breuil–Kisin $\mathfrak{M}_{\nu'/p}$ sur $\mathfrak{S}_{\nu'/p}$ qui est isomorphe à $\mathfrak{M}_\nu$ après extension des scalaires à $\mathfrak{S}_{\nu'}$. Or un calcul immédiat montre que $\frac{\nu'}{p} = \frac{\nu}{p - per\nu}$ et donc, par l'hypothèse faite sur ν, que $\frac{\nu'}{p} < \nu$.

On itère maintenant le processus précédent. On construit comme ceci des matrices G_n à coefficients dans $\mathfrak{M}_{\nu_n}$ définissant des modules de Breuil–Kisin sur ces anneaux qui deviennent isomorphes à $\mathfrak{M}_\nu$ après extension des scalaires à $\mathfrak{S}_{\nu'}$. Ici, la suite réelle $(\nu_n)_{n\geqslant 0}$ est définie récursivement par $\nu_0 = \nu$ et $\nu_{n+1} = \frac{\nu_n}{p - per\nu_n}$. De la décroissance de la suite des ν_n (déjà mentionnée précédemment), on déduit que $\nu_n \leqslant \nu \cdot (p - per\nu)^{-n}$. Comme le facteur élevée à la puissance

$(-n)$ dans l'expression précédente est par hypothèse > 1, on obtient la convergence vers 0 de la suite des ν_n. Il en résulte que, si ν'_n est le réel associé à ν_n, la suite des ν'_n tend aussi vers 0 quand n tend vers l'infini. La condition de $\ll$ divisibilité par $u^{1/\nu'} \gg$ qui apparaît dans le lemme 1.15 assure ainsi que le produit infini $\prod_{n\geqslant 0}(I + X_n H_n)$ converge dans $\mathfrak{S}_{\nu'}$ vers une limite P_∞. La matrice $G_\infty = P_\infty G_0 \phi(P_\infty)^{-1}$ est alors la limite des G_n, et elle est donc à coefficients dans $\mathfrak{S}$. Comme précédemment, on montre qu'il existe H_∞ tel que $H_\infty G_\infty = E(u)^r$, et donc que G_∞ définit un module de Breuil–Kisin sur $\mathfrak{S}$. Enfin, l'égalité $G_\infty = P_\infty G_0 \phi(P_\infty)^{-1}$ montre que celui-ci est isomorphe à $\mathfrak{M}_\nu$ après extension des scalaires à $\mathfrak{S}_{\nu'}$.

2 L'algorithme de calcul de la semi-simplifiée modulo p

Le but de cette seconde partie est de décrire un algorithme qui prend en entrée une représentation semi-stable V — donnée par l'intermédiaire de son (ϕ, N)-module filtré admissible D — et renvoie sa semi-simplifiée modulo p notée $\bar{V}^{\mathrm{ss}}$. Quitte à twister par une puissance du caractère cyclotomique, on peut toujours supposer que tous les poids de Hodge-Tate de V sont positifs ou nuls ; du point de vue des (ϕ, N)-modules filtrés, cela revient à supposer que D est effectif. Cette hypothèse permet de simplifier l'exposition ; nous la ferons systématiquement dans la suite.

De façon très schématique, l'algorithme que nous voulons décrire se décompose en trois étapes que voici :

Étape 1 : Calcul du module $\mathfrak{D}$ associé à D (voir §1.2.2 pour la définition de $\mathfrak{D}$)

Étape 2 : Calcul d'un module de Breuil–Kisin $\mathfrak{M}$ à l'intérieur de $\mathfrak{D}$

Étape 3 : Calcul de la représentation $\bar{V}^{\mathrm{ss}}$ à partir de $\mathfrak{M}/p\mathfrak{M}$

Chacune de ces trois étapes fait l'objet d'une sous-partie de ce numéro : l'étape 1 est traitée au §2.2, l'étape 2 au §2.3 et l'étape 3 au §2.4. Le §2.1 regroupe un certain nombre de préliminaires algorithmiques concernant la représentation des objets sur machine ; ces précisions aboutiront notamment à une explication précise et rigoureuse des spécifications de l'algorithme que l'on cherche à écrire, ainsi que quelques hypothèses simples sur le modèle de calcul que l'on considère. Enfin, au §2.5, on détermine la complexité de l'algorithme.

2.1 Représentation des objets sur machine

Avant toute chose, il est important d'expliquer comment les différents objets que nous serons amenés à manipuler, à savoir :

- les éléments des différents anneaux de nombres p-adiques : $\mathcal{O}_{K_0}$, K_0, $\mathcal{O}_K$ et K,
- les éléments des anneaux de séries $\mathfrak{S}_\nu$ et $\mathcal{E}^+_\nu$,
- les (ϕ, N)-modules filtrés (c'est l'entrée de notre algorithme !),
- les $\mathbb{F}_p$-représentations semi-simples de G_K (c'est la sortie des notre algorithme !), et
- les modules de Breuil–Kisin sur $\mathfrak{S}$ et $\mathfrak{S}_\nu$,

peuvent se représenter sur machine. C'est l'objet de ce numéro.

Les corps p-adiques et leurs éléments

Par définition, un élément $x \in \mathcal{O}_{K_0} = W(k)$ est une suite *infinie* $x = (x_1, x_2, \ldots)$ de composantes appartenant à k. Or, stocker — et *a fortiori* manipuler — une telle suite sur machine est tout simplement impossible, la mémoire d'un ordinateur n'étant certainement pas infinie.

Traditionnellement (comme c'est d'ailleurs le cas pour les nombres réels), on résout ce problème en travaillant avec des approximations. Concrètement, un élément $x \in \mathcal{O}_{K_0}$ sera représenté en machine par un couple $(n, \tilde{x})$ où n est un entier positif — la *précision* — et $\tilde{x}$ est une *approximation* de x vivant dans un anneau exact et vérifiant $x \equiv \tilde{x} \pmod{p^n}$. Si $\mathcal{O}_{K_0} = \mathbb{Z}_p[X]/F(X)$ pour un certain polynôme P à coefficients entiers, l'anneau exact dont il vient d'être question peut, par exemple, être $\mathbb{Z}[X]/F(X)$ et, bien sûr, au lieu de considérer $\tilde{x}$ lui-même, on peut se contenter de travailler avec $\tilde{x} \bmod p^n$, ce qui revient à dire que l'on peut considérer que $\tilde{x}$ est élément de $\mathbb{Z}[X]/(p^n, P(X)) \simeq \mathbb{Z}_q/p^n$ (mais le modulo p^n dépend alors de l'élément x considéré).

Pareillement, on représente les éléments de K_0 par une donnée de précision et une approximation qui vit dans l'anneau exact $\mathbb{Z}[1/p][X]/P(X)$. En ce qui concerne $\mathcal{O}_K$ et K, on procède de même en considérant un nouveau polynôme définissant l'extension K/K_0, qui peut par exemple être le polynôme $E(u)$. À l'instar de ce qui se passe avec les nombres réels, cette représentation n'empêche nullement d'effectuer des opérations ; par exemple, si x et y sont connus à précision p^n, alors on peut calculer $x+y$ et xy à précision p^n également, simplement en effectuant ces opérations modulo p^n.

Les anneaux de séries $\mathfrak{S}_\nu$ et leurs éléments

Attardons-nous à présent sur les anneaux $\mathfrak{S}_\nu$ et $\mathfrak{S}_\nu[1/p]$. Comme précédemment, on est contraint de représenter leurs éléments par une approximation complétée par des données supplémentaires décrivant la nature de cette approximation. Au vu des résultats de [11] (voir en particulier §4), nous choisissons de représenter en machine une série $f = \sum a_i u^i \in \mathfrak{S}_\nu[1/p]$ par les trois données suivantes :

- la *précision* : un entier strictement positif N et un N-uplet d'entiers relatifs $(N_0, \ldots, N_{N-1})$
- l'*approximation* : pour $i \in \{0, \ldots, N-1\}$, des éléments $\tilde{a}_i$ (vivant dans un anneau exact approximant K_0) tels que $\tilde{a}_i \equiv a_i \pmod{p^{N_i}}$.
- la *garantie* : un nombre rationnel g tel que $v_p(a_i) \geqslant g - \nu i$ pour tout $i \geqslant N$.

Dans la suite, on appellera *représentation PAG* (pour Précision-Approximation-Garantie) la représentation ci-dessus. Effectuer les opérations arithmétiques élémentaires (addition, soustraction, multiplication) sur la représentation PAG ne pose pas de problème. Il en va pareillement de la division euclidienne dans $\mathfrak{S}_\nu[1/p]$, comme cela est expliqué dans [11], §4.3.

Les (ϕ, N)-modules filtrés

Revenant à la définition, on voit qu'un (ϕ, N)-module filtré admissible est la donnée de :

- un K_0-espace vectoriel de dimension finie D ;
- un opérateur semi-linéaire $\phi : D \to D$;
- un opérateur linéaire $N : D \to D$;
- une filtration $(Fil^h D_K)_{h \in \mathbb{Z}}$ sur l'espace $D_K = K \otimes_{K_0} D$.

Les trois premières données ne sont pas difficiles à représenter : en effet, se donner D revient à s'en donner une base et les opérateurs ϕ et N sont alors donnés par leur matrice dans la base retenue. En ce qui concerne la filtration, une possibilité pour la décrire est la suivante : on se donne les sauts de la filtrations $h_1 \geqslant h_2 \geqslant \cdots \geqslant h_d$ (où d est la dimension de D) ainsi que des vecteurs $f_1, \ldots, f_d$ tels que, pour tout entier h, le cran $\mathrm{Fil}^h D_K$ soit engendré sur K par les vecteurs f_i tels que $h_i \geqslant h$.

En résumé, un (ϕ, N)-module filtré D peut se décrire par la donnée d'un quadruplet $(\texttt{Phi}, \texttt{N}, \texttt{H}, \texttt{F})$ où l'on a fixé une base de D et

- `Phi` est la matrice de ϕ dans cette base ;
- `N` est la matrice de N dans cette base ;
- `H` est le d-uplet d'entiers $h_1 \geqslant h_2 \geqslant \cdots \geqslant h_d$ donnant les sauts de la filtration ;
- `F` est une matrice à coefficients dans K dont les vecteurs colonne sont les vecteurs $f_1, \ldots, f_d$ définis précédemment (chaque vecteur étant exprimé par ses coordonnées dans la base qui a été fixée).

Dans la suite, nous utiliserons cette écriture pour représenter les (ϕ, N)-modules filtrés sur machine. Toutefois, conformément à ce qui a été expliqué précédemment, tous les coefficients des matrices `Phi`, `N` et `F` ne sont pas connus exactement mais à une certaine précision p^n (ou π^n dans le dernier cas) qu'il nous faudra préciser.

Les représentations semi-simples modulo p

La représentation sur machine des $\mathbb{F}_p$-représentations semi-simples de G_K passe par un théorème de classification. Soit I le sous-groupe d'inertie ; on rappelle qu'il s'agit du sous-groupe distingué de G_K formé des éléments qui agissent trivialement sur le corps résiduel. Le quotient G_K/I s'identifie canoniquement au groupe de Galois absolu du corps résiduel k qui, on le rappelle, est supposé fini. Si q désigne le cardinal de k, le groupe G_K/I est un procyclique et engendré par le Frobenius $\mathrm{Frob}_q : x \mapsto x^q$. On rappelle aussi que I admet un unique pro-p-Sylow, classiquement noté I_p et appelé sous-groupe d'inertie sauvage. Le quotient $I/I_p = I_t$ est appelé le groupe d'inertie modérée ; il est isomorphe à $\varprojlim_n \mu_{p^n-1}(\bar{k})$ où $\mu_{p^n-1}(\bar{k})$ désigne le sous-groupe de $\bar{k}^\star$ des racines (p^n-1)-ièmes de l'unité et s'identifie donc à $\mathbb{F}_{p^n}^\star$ si $\mathbb{F}_{p^n}$ désigne l'unique sous-corps de cardinal p^n de $\bar{k}$. On déduit, en particulier, de cet isomorphisme que I_t est procyclique, c'est-à-dire topologiquement engendré par un unique générateur. Enfin, le quotient G_K/I_p s'identifie au produit semi-direct $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$ où le générateur $\mathrm{Frob}_q \in \mathrm{Gal}\,(\bar{k}/k)$ agit sur I_t par élévation à la puissance q. Le corps découpé par les sous-groupe distingué I et I_p est l'extension maximale non ramifiée (resp. modérément ramifiée) de K et sera notée K^{nr} (resp. K^{mr}). On a bien sûr $K \subset K^{\mathrm{nr}} \subset K^{\mathrm{mr}} \subset \bar{K}$; de plus, le corps K^{mr} s'obtient à partir de K^{nr} en ajoutant les racines (p^n-1)-ièmes de π.

Si maintenant V est une $\mathbb{F}_p$-représentation de G_K, un lemme classique sur les actions de groupes assure que l'ensemble V^{I_p}, constitué des éléments $x \in V$ tel que $gx = x$ pour tout $g \in I_p$, n'est pas réduit à 0. Par ailleurs, du fait I_p est un distingué dans G_K, on déduit que V^{I_p} est stable par l'action de G_K tout entier. Ainsi, si l'on suppose en outre que V est irréductible, on a nécessairement $V^{I_p} = V$; autrement dit, le sous-groupe I_p agit trivialement sur V, ce qui signifie encore que l'action de G_K se factorise par $G_K/I_p \simeq I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$. Ainsi, pour décrire complètement une $\mathbb{F}_p$-représentation de G_K, il suffit de se donner :

- la matrice (à coefficients dans $\mathbb{F}_p$) donnant l'action d'un générateur topologique de I_t, et
- la matrice (à coefficients dans $\mathbb{F}_p$) donnant l'action de Frob_q.

À vrai dire, on peut encore simplifier cette représentation car, étant donné sa forme particulièrement simple, on dispose d'une classification très concrète des représentations irréductibles de I_t. Précisément, en notant ϖ_n une racine (p^n-1)-ième de π, on dispose du caractère fondamental de Serre de niveau n défini comme suit :

$$\begin{array}{rccc} \omega_n : & I_t & \to & \mu_{p^n-1}(\bar{K}) \simeq \mu_{p^n-1}(\bar{k}) = \mathbb{F}_{p^n}^\star \\ & g & \mapsto & \dfrac{g(\varpi_n)}{\varpi_n}. \end{array}$$

Ce caractère définit bien sûr une $\mathbb{F}_{p^n}$-représentation de dimension 1 de I_t mais, en considérant $\mathbb{F}_{p^n}$ comme un $\mathbb{F}_p$-espace vectoriel de dimension n, on s'aperçoit qu'il définit aussi une $\mathbb{F}_p$-représentation de I_t de dimension n qui sera notée dans la suite $\mathbb{F}_{p^n}(\omega)$. Évidemment, il est possible de faire la même construction à partir des puissances ω^s du caractère ω. On obtient, ce faisant, des $\mathbb{F}_p$-représentations de dimension n que l'on note $\mathbb{F}_{p^n}(\omega^s)$. On montre que ces représentations sont irréductibles dès que la fraction $\frac{s}{p^n-1}$ ne peut s'écrire sous la forme $\frac{s'}{p^{n'}-1}$ pour un entier $n' < n$. Mieux encore, toute représentation irréductible de I_t est de cette forme et on sait que deux représentations $\mathbb{F}_{p^n}(\omega^s)$ et $\mathbb{F}_{p^m}(\omega^t)$ sont isomorphes si, et seulement si $n = m$ et il existe un entier a tel que $s \equiv p^a t \pmod{p^n-1}$.

Pour étendre cette classification aux représentations de $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$, on introduit la définition classique suivante.

Définition 2.1. *Soit F un corps de caractéristique p. Un* ϕ-module *sur (F, Frob_q) est un F-espace vectoriel D de dimension finie muni d'une application additive $\phi : D \to D$ vérifiant $\phi(ax) = a^q\phi(x)$ pour tout $a \in F$ et tout $x \in D$.*

Le ϕ-module D est dit étale *si ϕ est bijectif. Il est dit* simple *s'il n'admet aucun sous-F-espace vectoriel strict stable par ϕ.*

On se donne, à présent, des entiers s et n comme précédemment ainsi qu'un ϕ-module D sur $(\mathbb{F}_{p^n}, \mathrm{Frob}_q)$ qui soit étale et simple. On pose $V = D$ et on munit cet espace de l'action $\mathbb{F}_p$-linéaire de $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$ en faisant agir I_t par multiplication par ω_n^s et Frob_q *via* l'endomorphisme ϕ. (La relation $\mathrm{Frob}_q \cdot g \cdot \mathrm{Frob}_q^{-1} = g^q$ valable pour $g \in I_t$ montre que cette définition a bien un sens.) En oubliant maintenant la structure de $\mathbb{F}_{p^n}$-espace vectoriel sur V (pour ne retenir que celle de $\mathbb{F}_p$-espace vectoriel), on fait de V une $\mathbb{F}_p$-représentation de $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$. On note cette représentation $V(\omega_n^s, D)$.

Proposition 2.2. *Les représentations $V(\omega_n^s, D)$ définies ci-dessus sont irréductibles et, réciproquement, toute $\mathbb{F}_p$-représentation irréductible de $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$ est de la forme $V(\omega_n^s, D)$ pour certains paramètres n, s et D.*

Par ailleurs, $V(\omega_n^s, D) \simeq V(\omega_m^t, E)$ si, et seulement si $n = m$ et il existe un entier a tel que l'on ait simultanément $s' \equiv p^a t \pmod{p^n-1}$ et l'existence d'un isomorphisme de ϕ-modules $E \simeq \mathbb{F}_{p^n} \otimes_{x \mapsto x^{p^a}, \mathbb{F}_{p^n}} D$.

Démonstration. Exercice. □

On déduit de la proposition que, pour représenter une $\mathbb{F}_p$-représentation simple V de $I_t \rtimes \mathrm{Gal}\,(\bar{k}/k)$, il suffit de se donner les paramètres s, n et D tels que $V = V(\omega_n^s, D)$. En vertu de la première réduction que l'on a expliquée, ceci s'applique également aux $\mathbb{F}_p$-représentation simples de G_K. Ainsi, pour décrire une représentation semi-simple de ce groupe, il suffit de se donner une liste de paramètres (s, n, D), chacun de ces triplets correspondant à un facteur simple de la représentation.

Il reste à expliquer comment on peut représenter concrètement un ϕ-module D sur (F, Frob_q) où F est un corps fini de caractéristique p. Une possibilité est de se donner la matrice de l'opérateur

ϕ dans une certaine base de D. Une autre solution consiste à introduite l'anneau $F[X, \mathrm{Frob}_q]$ des polynômes tordus[7] et à se rappeler que la donnée d'un ϕ-module étale simple sur (F, Frob_q) équivaut à la donnée d'une classe de similarité[8] de polynômes tordus irréductibles dans $F[X, \mathrm{Frob}_q]$ (voir par exemple [16], §I). Ainsi, il est également possible de représenter le ϕ-module par un représentant de la classe de similarité dans $F[X, \mathrm{Frob}_q]$; on obtient, comme ceci, une représentation compacte et également plus agréable à manipuler.

Les modules de Breuil–Kisin

Soit ν un nombre rationnel positif ou nul. Par définition, un module de Breuil–Kisin sur l'anneau $\mathfrak{S}_\nu$ est un $\mathfrak{S}_\nu$-module libre $\mathfrak{M}$ muni d'un endomorphisme semi-linéaire ϕ dont le conoyau du linéarisé est annulé par une puissance de $E(u)$.

On peut ainsi raisonner comme dans le cas des (ϕ, N)-modules filtrés et représenter un module de Breuil–Kisin sur $\mathfrak{S}_\nu$ par la matrice `PhiBK` (`BK` pour Breuil–Kisin) de l'opérateur ϕ dans une certaine base de $\mathfrak{M}$ fixée à l'avance. Cette matrice est à coefficients dans $\mathfrak{S}_\nu$ et la condition sur le conoyau de ϕ se traduit par l'existence d'une autre matrice `PhiBK'` à coefficients dans $\mathfrak{S}_\nu$ telle que

$$\texttt{PhiSK}' \cdot \texttt{PhiSK} = E(u)^r$$

pour un certain entier r.

2.2 Étape 1 : Des (ϕ, N)-modules filtrés aux modules de Breuil–Kisin

On se donne, dans ce numéro, un (ϕ, N)-module filtré effectif admissible D que l'on représente par un quadruplet $(\texttt{Phi}, \texttt{N}, \texttt{H}, \texttt{F})$ comme expliqué au §2.1. Ceci sous-entend en particulier que l'on a fixé une base de D, que l'on notera parfois $(e_1, \ldots, e_d)$ avec $d = \dim_{K_0} D$. Dans la suite, on utilisera constamment de façon implicite cette base pour identifier D à K_0^d. On note $L \subset D$ le réseau « standard », c'est-à-dire le sous-$\mathcal{O}_{K_0}$-module de D engendré par les e_i. Pour des questions de précision, on suppose, en outre, que la matrice `F` est à coefficients dans l'anneau des entiers $\mathcal{O}_K$ et, de plus, qu'elle appartient GL $_d(\mathcal{O}_K)$. Il est facile de vérifier qu'une matrice `F` satisfaisant à cette hypothèse supplémentaire existe toujours ; de plus, s'il nous est donnée une matrice `F` ne vérifiant pas cette hypothèse, il n'est pas difficile de la transformer — à l'aide d'un algorithme de type « pivot de Gauss », voir lemme 2.5, page 20 — en une matrice `F` convenable. Notons cependant que cette opération peut entraîner des pertes de précision p-adique.

On considère un nombre entier r tel que $\mathrm{Fil}^{r+1} D_K = 0$; par exemple, r peut être pris égal au plus grand poids de Hodge-Tate de V. Par ailleurs, pour ne pas alourdir les notations lors de l'étude de la perte de précision, nous faisons également les deux hypothèses simplificatrices suivantes : *primo*, le polynôme $E(u)$ est connu exactement et *secundo*, les matrices `Phi`, `N` et `F` sont à coefficients entiers.

Notre objectif est de calculer le module de Breuil–Kisin $\mathfrak{D}$ — ou plutôt $\mathfrak{D}_\nu = \mathfrak{S}_\nu \otimes_{\mathfrak{S}} \mathfrak{D}$ pour $\nu > 0$ — et nous suivons pour cela la méthode de Génestier et Lafforgue rappelée au §1.2.2. Nous reprenons également les notations de ce numéro : on considère l'anneau $\hat{\mathfrak{S}} = \varprojlim_n \mathfrak{S}/E(u)^n$, on pose $\hat{\mathfrak{D}} = \hat{\mathfrak{S}}[\frac{1}{E(u)}] \otimes_{\phi, K_0} D$ et on note V_D l'unique structure de Hodge-Pink satisfaisant à la transversalité de Griffiths qui correspond à la filtration $\mathrm{Fil}^h D_K$ sur le (ϕ, N)-module filtré D (voir lemme 1.7). D'après les hypothèses que l'on a faites, on a $\mathrm{Fil}^0 D_K = D_K$ et $\mathrm{Fil}^{r+1} D_K = 0$, ce qui

[7] Les éléments de $F[X, \mathrm{Frob}_q]$ sont les polynômes à coefficients dans F, l'addition sur $F[X, \mathrm{Frob}_q]$ est également l'addition usuelle sur les polynômes, tandis que la multiplication découle la règle $X \cdot a = a^q \cdot X$. En particulier, l'anneau $F[X, \mathrm{Frob}_q]$ n'est pas commutatif.

[8] Deux polynômes tordus P et Q dans $K[X, \mathrm{Frob}_q]$ sont dit similaires s'il existe U et V dans $K[X, \mathrm{Frob}_q]$ tels que P et V soient premiers entre eux à droite, Q et U soient premiers entre eux à gauche et $UP = QV$.

se traduit par les inclusions $\hat{\mathfrak{S}} \otimes_{K_0} D \subset V_D \subset E(u)^{-r}\hat{\mathfrak{S}} \otimes_{K_0} D$. On pose $W_D = E(u)^r V_D$; on a alors $E(u)^r\hat{\mathfrak{S}} \otimes_{K_0} D \subset W_D \subset \hat{\mathfrak{S}} \otimes_{K_0} D$.

2.2.1 Le calcul de V_D

La première étape consiste à calculer une famille explicite de générateurs de V_D. Pour ce faire, le lemme suivant nous sera fort utile.

Lemme 2.3. *Le morphisme de réduction modulo $E(u)$ induit un isomorphisme :*

$$(\hat{\mathfrak{S}} \otimes_{\phi,K_0} D)^{\hat{N}=0} \to D_K^{\phi}.$$

Démonstration. Il s'agit de montrer que tout $w \in D_K^{\phi}$ se relève de manière unique en un élément $\hat{w} \in \hat{\mathfrak{S}} \otimes_{\phi,K_0} D$ vérifiant $\hat{N}(\hat{w}) = 0$. On raisonne par approximations successives : on va démontrer par récurrence que, pour tout entier $i \geqslant 0$, il existe $\hat{w}^{(i)} \in \hat{\mathfrak{S}} \otimes_{\phi,K_0} D$ tel que $\hat{w}_i \equiv w \pmod{E(u)}$ et $\hat{N}(\hat{w}^{(i)}) \equiv 0 \pmod{E(u)^i}$ et, de plus, deux $\hat{w}^{(i)}$ solutions de deux congruences précédentes sont congrus entre eux modulo $E(u)^i$. L'assertion est clairement vraie pour $i = 1$. On la suppose à présent pour un certain i et on cherche à la démontrer pour $i + 1$. Cherchant $\hat{w}^{(i+1)}$ sous la forme $\hat{w}^{(i)} + E(u)^i x$, on est amené à résoudre la congruence

$$\hat{N}(\hat{w}^{(i)}) + iuE(u)^{i-1}\,\frac{dE(u)}{du} \cdot x \equiv 0 \pmod{E(u)^i}.$$

Or, on sait, par hypothèse de récurrence, que $\hat{N}(\hat{w}^{(i)})$ est multiple de $E(u)^{i-1}$. On peut donc écrire $\hat{N}(\hat{w}^{(i)}) = E(u)^{i-1}y$ et la congruence que l'on cherche à résoudre se réduit alors à :

$$iu\,\frac{dE(u)}{du} \cdot x + y \equiv 0 \pmod{E(u)}.$$

Étant donné que $\hat{\mathfrak{S}}/E(u)\hat{\mathfrak{S}} \simeq K$ est un corps dans lequel le produit $iu\frac{dE(u)}{du}$ est non nul, la congruence ci-dessus admet une solution modulo $E(u)$. Ceci termine la récurrence et démontre le lemme. □

Il est à noter que la démonstration que l'on vient de donner est entièrement constructive (bien sûr, si l'on se limite à calculer les $\hat{w}^{(i)}$ pour un entier i fini) et peut-être transformée aisément en algorithme (voir algorithme 1). Il est, en outre, possible d'estimer les pertes de précision engendrées par cet algorithme.

Lemme 2.4. *On suppose que le polynôme $E(u)$ est connu à précision arbitrairement grande. Si le vecteur w est à coefficients dans $\mathcal{O}_K$ et que w ainsi que* `N` *sont connus à précision $O(p^N)$, alors l'algorithme 1 appelé sur l'entrée $(w, \mathtt{N}, i)$ renvoie un vecteur $\hat{w}$ connu à précision $O(p^{N-\rho_1})$ avec*

$$\rho_1 = (i-2) \cdot \left\lceil \frac{1}{e} + \mathrm{val}(\mathfrak{d}_{K/K_0}) \right\rceil + \frac{i-1}{p-1}$$

où $\mathfrak{d}_{K/K_0}$ désigne la différente de K/K_0 et $\lceil x \rceil$ désigne la partie entière supérieure du réel x.

Démonstration. D'après l'hypothèse sur $E(u)$, il est possible de calculer les polynômes A et B avec une précision arbitrairement grande. Comme, en outre, A est à coefficients dans $\mathcal{O}_{K_0}$, les multiplications par A n'engendrent pas de perte de précision. De la même façon, étant donné que $E(u)$ est unitaire, la division par $E(u)$ n'entraîne pas non plus de perte de précision. Le polynôme B, quant à lui, n'a pas de raison d'être à coefficients dans $\mathcal{O}_{K_0}$; cependant, on connait la valuation de son image dans K : c'est l'opposé de $\frac{1}{e} + \mathrm{val}(\mathfrak{d}_{K/K_0})$. Ainsi, si l'on note δ la partie entière supérieure de $\frac{1}{e} + \mathrm{val}(\mathfrak{d}_{K/K_0})$, on peut choisir B de façon à ce que $v_0(B) \geqslant -\delta$. Ainsi les multiplications par B font chuter la précision de p^{δ}.

Lors de l'exécution de l'algorithme 1, les seules pertes de précision interviennent :

Algorithme 1: RELEVEHP$(w, \mathtt{N}, i)$

Entrée : un vecteur $w \in D_K^{\phi}$

Sortie : l'unique vecteur $\hat{w} \in (\hat{\mathfrak{S}} \otimes_{\phi,K_0} D)^{\hat{N}=0}$ relevant w calculé modulo $E(u)^i$

1 $A \leftarrow u \frac{dE(u)}{du}$, ;
2 $B \leftarrow$ inverse de A modulo $E(u)$;
3 $\hat{w} \leftarrow$ relevé de w dans $K_0[u]$;
4 $y \leftarrow p\mathtt{N} \cdot \hat{w} + u \frac{d\hat{w}}{du}$;
5 **pour** *j allant de* 1 *à* $i-1$ **faire**
6 $\quad x \leftarrow -j^{-1} B \cdot y \mod E(u)$;
7 $\quad \hat{w} \leftarrow \hat{w} + E(u)^i x$;
8 $\quad y \leftarrow p\mathtt{N} \cdot x + u \frac{dx}{du} + \frac{Y+jAx}{E(u)}$;
9 **retourner** $\hat{w}$;

- à la ligne 6 lors de la multiplication par j^{-1},
- à la ligne 8 lors de la multiplication par X et de la multiplication par B.

Ainsi, si l'on note $v_{x,j}$, $v_{y,j}$ et $v_{\hat{w},j}$ (resp. $p_{x,j}$, $p_{y,j}$ et $p_{\hat{w},j}$) les valuations respectives (resp. les exposants des précisions respectives) des variables x, y et $\hat{w}$ à la sortie de la j-ième itération de la boucle, on a les formules récurrentes suivantes :

$$\begin{aligned}
v_{x,j} &\geqslant v_{y,j-1} - \text{val}(j) && (3)\\
v_{y,j} &\geqslant \min(v_{y,j-1}, v_{x,j}, v_{x,j} + \delta + \text{val}(j)) && (4)\\
v_{\hat{w},j} &\geqslant \min(v_{\hat{w},j-1}, v_{x,j}) && (5)\\
p_{x,j} &\geqslant p_{y,j-1} - \text{val}(j) && (6)\\
p_{y,j} &\geqslant \min(p_{y,j-1}, N + v_{x,j}, p_{x,j}, p_{x,j} + \delta + \text{val}(B)) && (7)\\
p_{\hat{w},j} &\geqslant \min(p_{\hat{w},j-1}, p_{x,j}). && (8)
\end{aligned}$$

Par ailleurs, à la ligne 3, il est certainement possible de choisir un relevé $\hat{w}$ connu à précision $O(p^N)$ (simplement en écrivant w comme un polynôme en π). Ainsi, si l'on convient que $v_{\hat{w},0}$ et $p_{\hat{w},0}$ désignent la valuation et la précision de $\hat{w}$ avant l'entrée dans la boucle, on obtient les conditions initiales $v_{\hat{w},0} \geqslant 0$, $p_{\hat{w},0} \geqslant N$. De même, on a $v_{y,1} \geqslant 0$ et $p_{y,1} \geqslant N$. En remplaçant dans l'inégalité (4), la quantité $v_{x,j}$ par le minorant donné par 3, on obtient la formule de récurrence :

$$v_{y,j} \geqslant \min(v_{y,j-1} - \text{val}(j), v_{y,j-1} - \delta) \geqslant v_{y,j-1} - \text{val}(j) - \delta$$

qui entraîne immédiatement la formule close $v_{y,j} \geqslant -j \cdot \delta - \text{val}(j!) \geqslant -j \cdot \delta - \frac{j}{p-1}$. On en déduit que $v_{x,j} \geqslant -(j-1) \cdot \delta - \frac{j}{p-1}$ et, par suite, que le même minorant vaut pour $v_{\hat{w},j}$. De la même façon, en combinant (6) et (7), on obtient $p_{y,j} \geqslant N - j\delta - \frac{j}{p-1}$, $p_{x,j} \geqslant N - j\delta - \frac{j}{p-1}$ et $p_{\hat{w},j} \geqslant N - (j-1)\delta - \frac{j}{p-1}$. Comme la boucle est exécutée $j-1$ fois, on a bien le résultat souhaité. □

On revient à présent au problème de calculer la structure de Hodge-Pink W_D à partir de la donnée du quadruplet $(\mathtt{Phi}, \mathtt{N}, \mathtt{H}, \mathtt{F})$. On pose $W = \mathtt{Phi}^{-1} \cdot \mathtt{F}$. Les vecteurs colonne de W vus comme éléments de $K \otimes_{\phi,K_0} D$ (et exprimées dans la base $(1 \otimes e_1, \ldots, 1 \otimes e_d)$) sont alors égaux aux $\phi_K^{-1}(f_i)$ où les f_i sont les vecteurs colonnes de $\mathtt{F}$. On rappelle le lemme classique suivant :

Lemme 2.5. *Toute matrice $M \in M_d(K)$ se décompose sous la forme $M = M'U$ avec $M' \in \mathrm{GL}_d(\mathcal{O}_K)$ et U triangulaire supérieure.*

Démonstration. Il s'agit de démontrer qu'en effectuant des opérations élémentaires inversibles dans $\mathcal{O}_K$ sur les lignes de M, on peut obtenir une matrice triangulaire supérieure. Voici comment on peut procéder : (1) on sélectionne un élément de valuation minimale sur la première colonne, (2) on déplace cet élément sur la première ligne en permutant les lignes correspondantes, (3) on utilise cet élément comme pivot pour annuler, à l'aide d'opérations élémentaires sur les lignes de M, tous les autres coefficients de la première colonne de M, (4) on recommence tout le processus précédent à partir de la sous-matrice de M obtenue en retirant la première ligne et la première colonne. □

Soit $W = W'U$ une décomposition satisfaisant aux conditions du lemme précédent. Sachant que U est triangulaire supérieure et que les h_i sont rangés par ordre croissant, on déduit qu'en notant $(w'_1, \ldots, w'_d)$ les vecteurs colonne de W' considérés comme éléments de $K \otimes_{\phi,K_0} D$, pour tout $h \geqslant 0$, l'espace $\phi_K^{-1}(\mathrm{Fil}^h D_K)$ est engendré par les vecteurs w'_i pour les indices i tels que $h_i \geqslant h$. Pour tout i, on note $\hat{w}'_i$ l'unique élément de $(\hat{\mathfrak{S}} \otimes_{\phi,K_0} D)^{\hat{N}=0}$ relevant w'_i (voir lemme 2.3 ci-dessus).

Proposition 2.6. *Avec les notations précédentes, V_D est engendré comme $\hat{\mathfrak{S}}$-module par les vecteurs $E(u)^{-h_i}\hat{w}'_i$ ($1 \leqslant i \leqslant d$).*

Démonstration. Si l'on note V'_D la structure de Hodge-Pink engendrée par les vecteurs $E(u)^{-h_i}\hat{w}'_i$, il suffit de vérifier que :

(i) V'_D vérifie la transversalité de Griffiths, et

(ii) la filtration de D_K associée à V'_D s'identifie à la filtration $\mathrm{Fil}^h D_K$ du (ϕ, N)-module filtré D.

Le premier point découle directement de la condition $\hat{N}(\hat{w}'_i) = 0$ tandis que le second est une conséquence immédiate des congruences $\hat{w}'_i \equiv w'_i = \phi_K^{-1}(v_i) \pmod{E(u)}$. □

Étant donné que l'on sait par avance que $\hat{\mathfrak{S}} \otimes_{\phi,K_0} D \subset V_D$, la proposition 2.6 ci-dessus vaut encore si, pour chaque i, on remplace $\hat{w}_i$ par un élément qui lui est congru modulo $E(u)^{h_i}$. Ainsi, en reprenant les notations de la démonstration du lemme 2.3, les $E(u)^{-h_i}\hat{w}_i^{(h_i)}$ forment aussi une famille de générateurs de V_D. Or, ces $\hat{w}_i^{(h_i)}$ ont l'énorme avantage de pouvoir être calculé efficacement par l'algorithme 1. En plus de cela, les vecteurs $E(u)^{r-h_i}\hat{w}_i^{(h_i)}$ — qui engendrent donc $W_D = E(u)^r V_D$ — possèdent le second avantage d'être éléments de $\mathcal{E}^+ \otimes_{\phi,K_0} D$. Ainsi, non seulement ils forment une $\hat{\mathfrak{S}}$ base de W_D mais également une $\mathcal{E}^+$-base de l'intersection $W_D \cap (\mathcal{E}^+ \otimes_{\phi,K_0} D)$.

L'algorithme 2 récapitule la construction d'une famille génératrice de V_D que nous venons de présenter. Au niveau de la précision, l'admissibilité de D, combinée au fait que tous les h_i sont dans $\{0, \ldots, r\}$, implique que tous les diviseurs élémentaires de `Phi` divisent p^r. À partir de là, un examen de la méthode de calcul de la matrice W' (voir démonstration du lemme 2.5) montre que les pertes de précision pour le calcul de W' sont majorées par p^{dr} ; autrement dit, si W est connu à précision $O(p^N)$, la matrice W' est au pire connue avec une précision $O(p^{N-dr})$. En combinant ceci avec le résultat du lemme 2.5, on obtient une formule explicite pour les pertes de précision totales de l'algorithme 2.

Algorithme 2: HODGEPINK(Phi, N, H, F)

Entrée : Un (ϕ, N)-module filtré D

Sortie : Une matrice $\hat{W}'$ telle que les vecteurs colonne de $\hat{W}' \cdot \mathrm{Diag}(E(u)^{-h_1}, \dots, E(u)^{-h_d})$ engendrent V_D

1 $W \leftarrow \mathtt{Phi}^{-1} \cdot \mathtt{F}$;
2 **écrire** $W = W'U$ (*cf* lemme 2.5);
3 **pour** *i allant de* 1 *à* d **faire** $\hat{w}'_i \leftarrow$ RELEVEHP$(W'[\cdot, i], \mathtt{N}, \mathtt{H}[i])$;
4 **retourner** *la matrice dont les vecteurs colonne sont* $\hat{w}'_1, \dots, \hat{w}'_d$;

2.2.2 Le calcul de β_n

On rappelle que l'on a défini au §1.2.2 une suite β_n de sous-$\mathcal{E}^+$-modules de $\mathcal{E}^+ \otimes_{K_0} D$ (voir formule 1) et que ceux-ci sont reliés au module de Breuil–Kisin $\mathfrak{D}_\nu$ que l'on souhaite calculer grâce au théorème 1.8 : on a un isomorphisme canonique

$$\mathfrak{D}_{1/(ep^n)} \simeq \mathcal{E}^+_{1/(ep^n)} \otimes_{\mathcal{E}^+} \beta_n$$

et l'action de ϕ sur $\mathfrak{D}_{1/(ep^n)}$ correspond *via* cette identification à l'action de $(\frac{E(u)}{E(0)})^r \phi \otimes \phi$ sur le membre de droite. Dans ce paragraphe, nous expliquons comment calculer des générateurs de β_n pour un entier n que l'on se donne.

On remarque pour commencer que les β_n ne sont pas modifiés si, dans la formule (1), on replace W_D par son intersection avec $\mathcal{E}^+ \otimes_{\phi, K_0} D$. Or, d'après les résultats du §2.2.1, une base de cette intersection est donnée par les vecteurs colonne de la matrice produit $\hat{W}'\Delta_1$ où $\hat{W}'$ est la matrice calculée par l'algorithme 2 et Δ_1 est la matrice diagonale suivante :

$$\Delta_1 = \begin{pmatrix} \lambda_1^{r-h_1} & & \\ & \ddots & \\ & & \lambda_1^{r-h_d} \end{pmatrix} \quad \text{avec} \quad \lambda_1 = \frac{E(u)}{E(0)}.$$

À partir de là, on s'aperçoit qu'il est possible de calculer les β_n en calculant des intersections de $\mathcal{E}^+$-modules complètement explicites. Comme $\mathcal{E}^+$ est un anneau euclidien, cela est possible en utilisant les algorithmes standard de manipulation de modules sur les anneaux euclidiens (qui reposent essentiellement sur l'existence d'une forme normale d'Hermite). Toutefois, ces méthodes peuvent s'avérer lentes et très instables. Dans la suite, nous allons présenter une autre approche qui repose sur l'écriture d'une formule quasiment explicite pour β_n.

Pour tout entier $m \geqslant 1$, on pose $\lambda_m = \lambda_1 \phi(\lambda_1) \cdots \phi^{m-1}(\lambda_1)$ et, de même que l'on a défini Δ_1, on note Δ_m la matrice diagonale dont les termes diagonaux sont $\lambda_m^{r-h_1}, \dots, \lambda_m^{r-h_d}$. On convient également que $\lambda_0 = 1$ et que Δ_0 est la matrice identité de taille d.

Lemme 2.7. *Soit $\hat{W}'$ la matrice calculée par l'algorithme 2. Soient n un entier strictement positif et X une matrice à coefficients dans $\mathcal{E}^+$ telle que pour tout entier $m \in \{0, \dots, n-1\}$:*

$$X \equiv \mathtt{Phi} \cdot \phi(\mathtt{Phi}) \cdots \phi^m(\mathtt{Phi}) \cdot \phi^m(\hat{W}'\Delta_1) \cdot P_m \pmod{\phi^m(E(u)^r)}$$

pour une certaine matrice P_m à coefficients dans $\mathcal{E}^+$, inversible modulo $\phi^m(E(u))$. Alors β_n est engendré par les vecteurs $\lambda_n^r e_i$ ($1 \leqslant i \leqslant d$) et les vecteurs colonne de la matrice X.

Démonstration. Pour simplifier les écritures, on pose $M = \hat{W}'\Delta_1$. On raisonne par récurrence sur n. Lorsque $n = 1$, l'espace β_1 est, par définition, égal à $\frac{\phi}{p^r}(W_D)$ et est donc engendré par

les vecteurs colonne de la matrice produit $\texttt{Phi} \cdot M$. Par ailleurs, la matrice P_0 étant inversible modulo $E(u)$, elle l'est aussi modulo $E(u)^r$. On conclut la démonstration dans le cas $n = 1$ en remarquant que multiplier à droite par une matrice inversible revient à faire une combinaison linéaire « inversible » des colonnes et donc ne change pas l'espace engendré par les colonnes.

On suppose maintenant que le lemme est vrai pour l'entier n. Du fait que $E(u)^r\mathcal{E}^+ \otimes_{\phi,K_0} D \subset W_D$, on déduit aisément que $\lambda_{n+1}^r\mathcal{E}^+ \otimes_{K_0} D \subset \beta_{n+1}$. Ainsi, il suffit de démontrer que les colonnes de la matrice X du lemme engendrent l'image de β_{n+1} dans le quotient $(\mathcal{E}^+/\lambda_{n+1}^r\mathcal{E}^+) \otimes_{K_0} D$. Par le lemme chinois, ce dernier est isomorphe à la somme directe $(A_0 \otimes_{K_0} D) \oplus \cdots \oplus (A_n \otimes_{K_0} D)$ où on a noté $A_m = \frac{\mathcal{E}^+}{\phi^m(E(u)^r)\mathcal{E}^+}$. Or, d'après l'hypothèse de récurrence, si $0 \leqslant m < n$, l'image de β_n dans $A_m \otimes_{K_0} D$ est engendrée par les vecteurs colonne de $\texttt{Phi} \cdot \phi(\texttt{Phi}) \cdots \phi^m(\texttt{Phi}) \cdot \phi^m(M)$ (on peut à nouveau supprimer la multiplication par P_m, cela ne modifie pas l'espace engendré). Ainsi, après un twist, l'image de $\mathcal{E}^+ \otimes_{\phi,\mathcal{E}^+} \beta_n$ dans $A_{m+1} \otimes_{K_0} D$ est engendrée par les vecteurs colonne de la matrice $\phi(\texttt{Phi}) \cdots \phi^{m+1}(\texttt{Phi}) \cdot \phi^{m+1}(M)$. Il en est, en réalité, de même de l'image de l'intersection $\mathcal{E}^+ \otimes_{\phi,\mathcal{E}^+} \beta_n \cap W_D$ étant donné que $E(u)^r$ est inversible dans A_{m+1} (puisque $m+1 > 0$). Par ailleurs, l'image de cette intersection dans $A_0 \otimes_{K_0} D$ est engendrée par les vecteurs colonne de M puisque $\mathcal{E}^+ \otimes_{\phi,\mathcal{E}^+} \beta_n$ contient $\phi(\lambda_n)\mathcal{E}^+ \otimes_{\phi,K_0} D$ et que $\phi(\lambda_n)$ est inversible dans A_0. Il résulte de cela que, pour tout $m \in \{0, \ldots, n\}$, l'image de β_{n+1} dans $A_m \otimes_{K_0} D$ est engendrée par les vecteurs colonne de $\texttt{Phi} \cdot \phi(\texttt{Phi}) \cdots \phi^m(\texttt{Phi}) \cdot \phi^m(M)$. L'assertion du lemme au rang $n + 1$ en découle. □

À partir de maintenant, on fixe l'entier n. Si l'on se donne n'importe quelle famille de matrices P_m, il est possible de calculer une matrice X vérifiant les conditions du même lemme par des applications successives du lemme chinois. Étant donné que $\mathcal{E}^+$ est un anneau euclidien, calculer une base de β_n peut alors se faire en réduisant sous forme d'Hermite la matrice par blocs $(X_n \quad \lambda_n^r I)$. Toutefois, le fait de pouvoir choisir librement les P_m permet de limiter les calculs, comme on se propose de l'expliquer maintenant.

Pour tout entier m, on considère l'application $\phi_K^{(m)} : K \otimes_{\phi^m,K_0} D \to K \otimes_{K_0} D = D_K$ obtenue en linéarisant ϕ^m ; c'est une application K-linéaire bijective. En désignant par $f_1, \ldots, f_d$ les vecteurs colonne de $\texttt{F}$, on appelle W_m la matrice dont la i-ième colonne est l'unique antécédent de f_i par $\phi_K^{(m)}$. Un calcul simple montre que l'on a l'expression suivante :

$$W_m = \phi^{m-1}(\texttt{Phi}^{-1}) \cdots \phi(\texttt{Phi}^{-1}) \cdot \texttt{Phi}^{-1} \cdot \texttt{F}. \tag{9}$$

On décompose, à présent, W_m sous la forme $W_m = W'_m U_m$ où $W'_m \in \mathrm{GL}_d(\mathcal{O}_K)$ et U_m est triangulaire supérieure (voir lemme 2.5). Pour tout $j \leqslant d$, les j premiers vecteurs colonne de W'_m forment une base de l'image réciproque par $\phi_K^{(m)}$ de $\mathrm{Fil}^h D_K$ lorsque $h_j \geqslant h > h_{j+1}$.

On considère l'espace $\hat{\mathfrak{S}} \otimes_{\phi^m,K_0} D$. Comme précédemment, on dispose d'une application $\hat{\phi}^{(m)} : \hat{\mathfrak{S}} \otimes_{\phi^m,K_0} D \to \hat{\mathfrak{S}} \otimes_{K_0} D$ obtenue en linéarisant ϕ^m. D'autre part, $\hat{\mathfrak{S}} \otimes_{\phi^m,K_0} D$ est également muni de la dérivation $\hat{N}_m = p^m \otimes N + u\frac{d}{du} \otimes \mathrm{id}$. De la relation $N\phi = p\phi N$, on déduit $\hat{\phi}^{(m)} \circ \hat{N}_m = \hat{N}_0 \circ \hat{\phi}^{(m)}$. Par ailleurs, en copiant la démonstration du lemme 2.3, on montre que le morphisme de réduction modulo $E(u)$ induit une bijection :

$$(\hat{\mathfrak{S}} \otimes_{\phi^m,K_0} D)^{\hat{N}_m=0} \xrightarrow{\sim} K \otimes_{\phi^m,K_0} D. \tag{10}$$

En outre, l'algorithme 1 s'adapte sans difficulté à cette nouvelle situation. Ainsi, on sait calculer une matrice à coefficients dans $K_0[u]$ dont le i-ième vecteur colonne est congru modulo $E(u)^{h_i}$ à l'unique antécédent dans $(\hat{\mathfrak{S}} \otimes_{\phi^m,K_0} D)^{\hat{N}_m=0}$ du i-ième vecteur colonne de W'_m. On note $\hat{W}'_m$ cette matrice. Comme précédemment, on pose $W' = W'_1$, $U = U_1$ et $\hat{W}' = \hat{W}'_1$.

Lemme 2.8. *On a la congruence :*

$$\hat{W}' \cdot \Delta_1 \equiv \phi(\texttt{Phi}) \cdots \phi^{m-1}(\texttt{Phi}) \cdot \hat{W}'_m \cdot U_m \cdot U^{-1} \cdot \Delta_1 \pmod{E(u)^r}.$$

Démonstration. On note $\hat{W}_m$ (resp. $\hat{W}$) la matrice à coefficients dans $\mathfrak{S}$ dont les colonnes relèvent les colonnes de W_m (resp. de W) par la bijection (10) (resp. avec $m = 1$). On considère la composée suivante :

$$(\hat{\mathfrak{S}} \otimes_{\phi^m, K_0} D)^{\hat{N}_m = 0} \xrightarrow{f} (\hat{\mathfrak{S}} \otimes_{\phi, K_0} D)^{\hat{N}=0} \xrightarrow{\sim} D_K^{\phi} = K \otimes_{\phi, K_0} D$$

où la première flèche, notée f, est l'application $\hat{\phi}^{(m-1)}$ twistée par ϕ. La matrice de f dans les bases canoniques est $\phi(\texttt{Phi}) \cdots \phi^{m-1}(\texttt{Phi})$. Soit w_i l'image réciproque de $f_i \in D_K$ dans D_K^{ϕ}. Les vecteurs colonne de $\hat{W}_m$ (resp. $\hat{W}$) correspondent alors aux éléments de $(\hat{\mathfrak{S}} \otimes_{\phi^m, K_0} D)^{\hat{N}_m = 0}$ (resp. $(\hat{\mathfrak{S}} \otimes_{\phi, K_0} D)^{\hat{N}=0}$) qui ont pour image dans D_K les vecteurs w_i. On en déduit que $\hat{W} = \phi(\texttt{Phi}) \cdots \phi^{m-1}(\texttt{Phi}) \cdot \hat{W}_m$. D'autre part, comme la bijection (10) est K-linéaire, on a $\hat{W}_m \cdot \Delta_1 \equiv \hat{W}'_m \cdot U_m \cdot \Delta_1 \pmod{E(u)^r}$ et, pareillement, $\hat{W} \cdot \Delta_1 \equiv \hat{W}' \cdot U \cdot \Delta_1 \pmod{E(u)^r}$. Des congruences et égalité précédentes, on déduit :

$$\hat{W}' \cdot U \cdot \Delta_1 \equiv \phi(\texttt{Phi}) \cdots \phi^{m-1}(\texttt{Phi}) \cdot \hat{W}'_m \cdot U_m \cdot \Delta_1 \pmod{E(u)^r}.$$

On conclut en multipliant à droite la congruence précédente par $\Delta_1^{-1} U^{-1} \Delta_1$, après avoir remarqué que cette matrice produit est à coefficients dans $\mathfrak{S}$ parce qu'elle s'obtient à partir de U^{-1} qui est triangulaire supérieure en multipliant le coefficient en position (i, j) par $\lambda_1^{h_i - h_j}$ et que l'on a bien $h_i \geqslant h_j$ dès que $i \leqslant j$. □

Théorème 2.9 (Décompositions PLU simultanées)**.** *On considère un entier $v \geqslant \log_p(2nd)$. Alors, une matrice aléatoire ω à coefficients dans $\mathbb{Z}_p$ vérifie les conditions suivantes avec probabilité $\geqslant \frac{1}{2}$:*

(i) considérée comme matrice à coefficients dans $\mathbb{Q}_p$, la matrice ω est inversible et on a $\omega^{-1} \in p^{-v} M_d(\mathbb{Z}_p)$.

(ii) pour tout entier $m \in \{1, \ldots, n\}$, il existe des matrices L_m et V_m (uniquement déterminées modulo $E(u)^r$) qui sont respectivement triangulaire inférieure unipotente et triangulaire supérieure et qui vérifient la congruence :

$$\omega \cdot \hat{W}'_m \equiv L_m V_m \pmod{E(u)^r} \tag{11}$$

de plus, les matrices L_m et V_m sont uniquement déterminées si on impose de plus que tous leurs coefficients sont des polynômes de degré $< er$.

(iii) pour tout m, l'image de L_m dans $M_d(\mathfrak{S}/E(u)^r) \simeq M_d(K[u_\pi]/u_\pi^r)$ appartient à $\pi^{-e\rho_2} M_d(\mathcal{O}_K[u_\pi]/u_\pi^r)$ avec

$$\rho_2 = r(\tfrac{1}{e} + v + \mathrm{val}(\mathfrak{d}_{K/K_0})).$$

(iv) si les $\hat{W}'_m$ sont connus à précision $O(p^N)$, alors on peut calculer les images de L_m dans $M_d(K[u_\pi]/u_\pi^r)$ à précision $O(p^{N - 2\lceil \rho_2 \rceil})$.

Démonstration. Pour $r = 1$, il s'agit du théorème 2.12 de [9] étant donné que, par construction, l'image de $\hat{W}'_m$ dans $M_d(\mathfrak{S}/E(u)) \simeq M_d(K)$ est inversible dans l'anneau $M_d(\mathcal{O}_K)$.

Pour $r > 1$, on montre, en reprenant la démonstration du lemme 2.4, que, pour tout $j < r$, l'image de $\hat{W}'_m$ dans $M_d(K[u_\pi]/u_\pi^j)$ appartient à $\pi^{-jw} \cdot M_d(\mathcal{O}_K[u_\pi]/u_\pi^j)$ avec $w = \frac{1}{e} + \mathrm{val}(\mathfrak{d}_{K/K_0})$. Ainsi l'image de $\hat{W}'_m$ dans $M_d(K[u_\pi]/u_\pi^r)$ appartient à $M_d(\mathcal{O}_K[X]/X^r)$ où $X = \frac{u_\pi}{\pi^w}$. Donc les réductions modulo $E(u)^r$ de tous les mineurs de $\omega \cdot \hat{W}'_m$ sont dans $\mathcal{O}_K[X]/X^r$. Or, par ailleurs, on sait que :

(1) les coefficients de L_m s'obtiennent comme quotient de deux tels mineurs, le dénominateur étant toujours un mineur principal (voir par exemple §1.1.1 de [9]) ;

(2) qu'avec probabilité $\geqslant \frac{1}{2}$, on a $\omega^{-1} \in p^{-v}M_d(\mathbb{Z}_p)$ et les images dans $\mathfrak{S}/E(u) \simeq K$ des mineurs principaux de $\omega\hat{W}'_m$ est divisible par π^v (cela résulte de la démonstration du théorème 2.12 de [9]).

On conclut en remarquant qu'un élément de $\mathcal{O}_K[X]/X^r$ dont le terme constant est divisible par π^v a pour inverse un élément de $\pi^{-v}\mathcal{O}_K[Y]/Y^r$ avec $Y = \frac{X}{\pi^v}$. □

Remarque 2.10. *En utilisant non pas une décomposition LU mais une décomposition LU par blocs (en regroupant entre eux les h_i qui sont égaux), on peut remplacer la borne $\log_q(2nd)$ qui apparait dans le théorème 2.9 par $\log_q(2nr_{\text{Card}})$ où r_{Card} est le cardinal de l'ensemble $\{h_1, \dots, h_d\}$ (c'est-à-dire le nombre de poids de Hodge-Tate de la représentation semi-stable V, comptés* sans *multiplicité). On a évidemment $r_{\text{Card}} \leqslant \min(r, d)$. On renvoie au théorème 2.12 de [9] pour plus de précisions à ce sujet.*

À partir de maintenant, on fixe des matrices ω, L_m et V_m vérifiant les conditions du théorème précédent. On note $t_0 = 1$ et pour tout $m \geqslant 1$, on pose $t_m = t_{m-1}\cdot\phi^m(\lambda_1^r)\cdot\big(\phi^m(\lambda_1^r)^{-1} \bmod E(u)^r\big)$ où, si $s \in \mathcal{E}^+$, la notation $s^{-1} \bmod E(u)^r$ désigne un inverse de s modulo $E(u)^r$. Pour tout indice $m > 0$, on a alors $t_m \equiv 1 \pmod{E(u)^r}$ et $t_m \equiv 0 \pmod{\phi^{m'}(E(u)^r)}$ si $1 \leqslant m' \leqslant m$. On définit une suite de matrices $(Y_m)_{1\leqslant m\leqslant n}$ par

$$Y_1 = L_1 \quad \text{et} \quad Y_{m+1} = t_m L_{m+1} + (1 - t_m)\phi(Y_m) \tag{12}$$

pour $m \in \{1, \dots, n-1\}$. On pose enfin :

$$X_n = \texttt{Phi}\cdot\phi(\texttt{Phi})\cdots\phi^{n-1}(\texttt{Phi})\cdot\omega^{-1}\cdot Y_n\cdot\Delta_n \tag{13}$$

où on rappelle que Δ_n est la matrice diagonale dont le i-ième coefficient diagonal est $\lambda_n^{r-h_i}$.

Proposition 2.11. *Avec les notations précédentes, les vecteurs colonne de X_n forment une base de β_n.*

Démonstration. Il est facile de montrer par récurrence sur s que si $0 \leqslant m < s \leqslant n$, la matrice Y_s est triangulaire inférieure unipotente et congrue à $\phi^m(L_{s-m})$ modulo $\phi^m(E(u)^r)$. Par ailleurs, il suit de l'égalité (11) que la matrice V_m est inversible modulo $E(u)^r$: il existe une matrice V'_m à coefficients dans $\mathcal{E}^+$ telle que $V_mV'_m \equiv I \pmod{E(u)^r}$. Comme, en outre, V_m est triangulaire supérieure, on peut supposer que V'_m l'est également. Il suit alors des congruences $Y_n \equiv \phi^m(L_{n-m}) \pmod{\phi^m(E(u)^r)}$ $(0 \leqslant m < n)$ et du fait que ω^{-1} soit à coefficients dans $\mathbb{Q}_p$ (et donc fixe par ϕ) que :

$$\begin{aligned} X_n \;\equiv\; & \texttt{Phi}\cdot\phi(\texttt{Phi})\cdots\phi^{n-1}(\texttt{Phi})\cdot\phi^m(\hat{W}'_{n-m}\Delta_1) \\ & \phi^m(\Delta_1^{-1}V'_{n-m}\Delta_1)\cdot(\phi^m(\Delta_1)^{-1}\Delta_n) \pmod{\phi^m(E(u)^r)} \end{aligned}$$

On remarque que, bien que Δ_1 ne soit pas inversible, l'écriture précédente a bien un sens et définit une matrice à coefficients dans $\mathcal{E}^+$. En effet, *primo*, le fait que $\phi^m(\lambda_1)$ divise λ_n (car $m < n$) permet de donner un sens au second facteur $\phi^m(\Delta_1)^{-1}\Delta_n$ (il s'agit de la matrice diagonale dont le i-ième coefficient diagonal est $(\frac{\lambda_n}{\phi^m(\lambda_1)})^{r-h_i}$) et *secundo*, le fait que V_{n-m} soit triangulaire supérieure permet de définir le produit $\Delta_1^{-1}V_{n-m}\Delta_1$ comme la matrice triangulaire supérieure dont le coefficient à la position (i, j) (avec $i \leqslant j$) est obtenu en multipliant le coefficient (i, j) de V_{n-m}

par $\lambda_1^{h_i-h_j}$ (ce qui a bien un sens car $h_i \geqslant h_j$ étant donné que $i \leqslant j$). En utilisant à présent le lemme 2.8, on obtient :

$$X_n \equiv \texttt{Phi} \cdot \phi(\texttt{Phi}) \cdots \phi^m(\texttt{Phi}) \cdot \phi^m(\hat{W}'\Delta_1) \cdot P_m \pmod{\phi^m(E(u)^r)}.$$

avec

$$P_m = \phi^m(\Delta_1^{-1}U_m\Delta_1) \cdot \phi^m(\Delta_1^{-1}V'_{n-m}\Delta_1) \cdot (\phi^m(\Delta_1)^{-1}\Delta_n).$$

Comme précédemment, le fait que U_m soit triangulaire supérieure montre que le facteur $\Delta_1^{-1}U_m\Delta_1$ est bien défini. De plus, on vérifie sans mal que la matrice P_m est inversible modulo $\phi^m(E(u)^r)$. On est ainsi dans les conditions d'application du lemme 2.7 duquel on déduit que la famille formée des vecteurs colonne de X_n et des $\lambda_n^r e_i$ ($1 \leqslant i \leqslant d$) engendre β_n. Par ailleurs, on sait que la matrice Y_n est triangulaire inférieure unipotente ; elle est donc inversible. Ceci implique, en revenant à la définition de X_n (voir formule 13), que tous les $\lambda_n^r e_i$ ($1 \leqslant i \leqslant d$) sont dans l'espace engendré par les vecteurs colonne de X_n. Le lemme en découle. □

2.2.3 La matrice de ϕ sur le module de Breuil–Kisin

Nous venons de déterminer une $\mathcal{E}^+$-base de β_n ce qui correspond d'après le théorème 1.8 de Génestier et Lafforgue à une $\mathfrak{S}_\nu$-base du module de Breuil–Kisin $\mathfrak{D}_\nu$ dès que $\nu \leqslant \frac{1}{ep^n}$. Dans cette base, la matrice de l'opérateur ϕ est donnée par la formule $\lambda_1^r \cdot X_n^{-1} \cdot \texttt{Phi} \cdot \phi(X_n)$ et vaut donc :

$$\texttt{PhiBK} = \lambda_1^r \cdot \Delta_n^{-1} \cdot Y_n^{-1} \cdot \omega \cdot \phi^n(\texttt{Phi}) \cdot \phi(Y_n) \cdot \omega^{-1} \cdot \phi(\Delta_n) \tag{14}$$

(on rappelle que ω^{-1} est à coefficients dans $\mathbb{Q}_p$ et donc fixe par ϕ). On pourra noter que, dans le produit ci-dessus, rien n'est véritablement difficile à calculer. En effet, clairement déjà, appliquer le Frobenius et multiplier des matrices ne pose aucun problème particulier au niveau calculatoire et, en particulier, n'entraîne aucune perte de précision. L'inversion de P n'est pas non plus très délicate, étant donné qu'il s'agit d'une matrice à coefficients dans K_0 et que, par ailleurs, on dispose d'un contrôle sur les dénominateurs qui peuvent apparaître (voir théorème 2.9). Enfin, les matrices Δ_n et Y_n sont respectivement diagonale et triangulaire supérieure unipotente et s'inversent donc aisément. On notera toutefois que Δ_n n'est, en réalité, pas inversible comme matrice à coefficients dans $\mathcal{E}^+$. Toutefois on sait, par avance, que la matrice PhiBK définie comme le produit (14) est à coefficients dans $\mathcal{E}^+_{1/(ep^n)}$. On a donc la garantie *a priori* que Δ_n divise $\lambda_1^r \cdot Y_n^{-1} \cdot \omega \cdot \phi^n(\texttt{Phi}) \cdot \phi(Y_n) \cdot \omega^{-1} \cdot \phi(\Delta_n)$. Ainsi, pour faire le calcul, il suffit de prendre le quotient de la division euclidienne de chaque entrée (i,j) de la matrice produit précédente par $\lambda_n^{r-h_i}$.

L'objectif de la suite de ce numéro est d'obtenir une minoration de la valuation v_ν de la matrice PhiBK. Si A est une matrice à coefficients dans $\mathcal{E}^+_\nu$, on note $v_\nu(A)$ la plus petite valuation d'un coefficient de A. Étant donné que P et Phi sont à coefficients dans $\mathcal{O}_{K_0}$, la relation (14) implique

$$v_\nu(\Delta_n \cdot \texttt{PhiBK}) \geqslant v_\nu(\lambda_1^r) + v_\nu(\omega^{-1}) + v_\nu(Y_n^{-1}) + v_\nu(\phi(Y_n)) + v_\nu(\phi(\Delta_n)).$$

Or, du fait que $E(u)$ est un polynôme à coefficients dans $\mathcal{O}_{K_0}$, on déduit que $v_\nu(\phi^m(E(u))) \geqslant 0$ pour tout m. Ainsi, on trouve $v_\nu(\lambda_1) \geqslant -1$ et $v_\nu(\phi(\Delta_n)) \geqslant -nr$ (puisque les h_i sont tous compris entre 0 et r). Par ailleurs, on vérifie directement que $v_\nu(\phi(x)) \geqslant v_\nu(x)$ pour tout $x \in \mathcal{E}^+_\nu$, d'où on déduit que $v_\nu(\phi(Y_n)) \geqslant v_\nu(Y_n)$. D'autre part, en utilisant le fait que Y_n est triangulaire inférieure unipotente, on montre facilement en exprimant son inverse que $v_\nu(Y_n^{-1}) \geqslant (d-1)v_\nu(Y_n)$. De plus, on rappelle que l'on a supposé que ω vérifiait les conditions du théorème 2.9 ; ainsi, en particulier, on a $v_\nu(\omega^{-1}) \geqslant -v$ où on rappelle que v est un entier $\geqslant \log_p(2nr_{\text{Card}})$ (voir remarque 2.10). On remarque enfin que pour $m \leqslant n$, on a $v_\nu(\phi^m(E(u))) = \nu e p^n \leqslant 1$. Ainsi $v_\nu(\lambda_n) \leqslant 0$ et,

comme le produit $\Delta_n \cdot \texttt{PhiBK}$ s'obtient en multipliant la i-ième ligne de $\texttt{PhiBK}$ par $\lambda_n^{r-h_i}$, on a $v_\nu(\Delta_n \cdot \texttt{PhiBK}) \leqslant v_\nu(\texttt{PhiBK})$. En mettant ensemble tout ce qui précède, on trouve :

$$v_\nu(\texttt{PhiBK}) \geqslant d \cdot v_\nu(Y_n) - v - r(n+1). \tag{15}$$

Il ne reste donc plus qu'à obtenir une borne inférieure pour $v_\nu(Y_n)$. Or, en revenant aux définitions, on obtient facilement que :

$$v_\nu(Y_n) \geqslant \min_{0 \leqslant m \leqslant n} v_\nu(L_m) + c_m + \cdots + c_n \tag{16}$$

où on a posé $c_i = \min(v_\nu(t_i), 0)$. On rappelle que les t_i sont définis par récurrence par les formules $t_0 = 1$ et $t_i = t_{i-1} \cdot \phi^i(\lambda_1^r) \cdot t_i'$ où $t_i' \in \mathcal{E}_\nu^+$ désigne un inverse de $\phi^i(\lambda_1^r)$ modulo $E(u)^r$. Ainsi défini, t_i' est uniquement déterminé modulo $E(u)^r$. À partir de maintenant, pour fixer les idées, on supposera que c'est un polynôme à coefficients dans K_0 de degré $< er$; il est ainsi uniquement déterminé.

Pour minorer la valuation de Y_n, on doit minorer celle de L_m, celles des $\phi^i(\lambda_1^r)$ ainsi que celles des t_i'. En ce qui concerne $\phi^i(\lambda_1^r)$, on a déjà dit que $v_\nu(\phi^i(\lambda_1)) \geqslant -1$, ce qui donne directement $v_\nu(\phi^i(\lambda_1^r)) \geqslant -r$. Pour les deux autres, on considère l'isomorphisme K_0-linéaire :

$$\begin{array}{rccl} T : & K_0^{<er}[u] & \to & K[u_\pi]/u_\pi^r \\ & f & \mapsto & T(f) = \displaystyle\sum_{s=0}^{r-1} \frac{1}{s!} \cdot \frac{d^s f}{du^s}(\pi) \cdot u_\pi^s. \end{array}$$

où la notation $K_0^{<er}[u]$ désigne l'ensemble des polynômes à coefficients dans K_0 de degré $< er$. D'après la démonstration du lemme 2.4.4 de [10], on a

$$T^{-1}(\mathcal{O}_K[u_\pi]/u_\pi^r) \subset p^{-r\lceil \mathrm{val}(\mathfrak{d}_{K/K_0})\rceil}\ \mathcal{O}_{K_0}[u].$$

De la condition (iii) du théorème 2.9, on déduit ainsi que, si parmi toutes les matrices L_m possibles, on choisit celle à coefficients à $K_0^{<er}[u]$, alors on aura $v_0(L_m) \geqslant -r \cdot \lceil \frac{1}{e} + v + 2\,\mathrm{val}(\mathfrak{d}_{K/K_0})\rceil$ et donc *a fortiori*

$$v_\nu(L_m) \geqslant r \cdot \left\lceil \frac{1}{e} + v + 2 \cdot \mathrm{val}(\mathfrak{d}_{K/K_0}) \right\rceil. \tag{17}$$

De même, pour minorer $v_\nu(t_i)$, il suffit de minorer la valuation de $T(t_i')$. C'est l'objet du lemme suivant.

Lemme 2.12. *Pour tout entier i, on a $T(t_i') \in p^{-m_i}\,\mathcal{O}_K[u_\pi]/u_\pi^r$ où m_i est la partie entière de $\frac{r}{e(p^i-1)}$.*

Démonstration. On pose $f = \phi^i(\lambda_1)$ de sorte que $T(t_i') = T(f)^{-r}$. Par ailleurs, comme $E(u)$ est un polynôme d'Eisenstein de degré e, l'élément f s'écrit sous la forme $\frac{u^{ep^i}}{p} + \sum_{j=0}^{e-1} a_j u^{jp^i}$ pour certains $a_j \in \mathcal{O}_{K_0}$ avec $a_0 = 1$. Les coefficients b_s de $T(f)$ sont alors donnés par :

$$b_s = \frac{1}{s!} \cdot \frac{d^s f}{du^s}(\pi) = \frac{1}{p}\binom{ep^i}{s}\pi^{ep^i-s} + \sum_{j=0}^{e-1} \binom{jp^i}{s} a_j \pi^{jp^i-s}.$$

En examinant cette formule, on remarque que tous les b_s sont dans $p^{-1}\mathcal{O}_K$ et, mieux encore, que $b_s \in \mathcal{O}_K$ pour $s \leqslant e(p^i-1)$. Quant à b_0, il est congru à 1 modulo π et donc, en particulier, inversible dans $\mathcal{O}_K$. On en déduit que $T(f)$ est inversible dans $K[u_\pi]/u_\pi^r$ et que son inverse appartient à l'image de l'application $\mathcal{O}_K[u_\pi, \frac{u_\pi^{e(p^i-1)}}{p}] \to K[u_\pi]/u_\pi^r$. L'inverse de $T(f^r) = T(f)^r$ appartient donc également à cette image et, à plus forte raison, à $p^{-m_i}\,\mathcal{O}_K[u_\pi]/u_\pi^r$. □

On déduit du lemme 2.12 que $v_\nu(t'_i) \geqslant -r(\frac{1}{e(p^i-1)}+\lceil \mathrm{val}(\mathfrak{d}_{K/K_0})\rceil)$. En revenant aux définitions, cela implique $c_i \geqslant -ri(2+\lceil \mathrm{val}(\mathfrak{d}_{K/K_0})\rceil)$, ce qui donne, pour finir, en combinant avec (15), (16) et (17),

$$v_\nu(\texttt{PhiBK}) \geqslant -dr\left(\frac{n(n+1)}{2}\cdot(2+\lceil \mathrm{val}(\mathfrak{d}_{K/K_0})\rceil)+\left\lceil \frac{1}{e}+v+2\cdot\mathrm{val}(\mathfrak{d}_{K/K_0})\right\rceil\right)-v-r(n+1). \tag{18}$$

La formule précédente n'est pas très ragoutante, mais on peut néanmoins estimer simplement son ordre de grandeur en fonction uniquement de r, d, ν et des constantes liées au corps K. En effet, si l'on souhaite uniquement calculer l'action de ϕ sur $\mathfrak{D}_\nu$, on peut choisir pour n n'importe quel entier $\geqslant -\log_p(e\nu)$. De la même façon, la seule contrainte portant sur v, hormis le fait qu'il soit entier, est $v \geqslant \log_p(2nr_{\text{Card}})$ où on rappelle que r_{Card} est un entier inférieur ou égal à $\min(r,d)$. Ainsi, en prenant pour n et v les entiers les plus proches des bornes précédentes, on obtient l'estimation :

$$v_\nu(\texttt{PhiBK}) \geqslant O(dr\cdot\log_p^2(\tfrac{1}{\nu})+dr\cdot\log_p(r_{\text{Card}}))$$

où la constante (négative) cachée dans le O ne dépend que du corps K. Par ailleurs, afin de pouvoir utiliser le théorème 1.11, nous allons devoir choisir un paramètre $\nu < \frac{per}{p-1}$. Sous cette hypothèse, on voit que le terme $dr\log_p(r_{\text{Card}})$ qui apparaît dans le O devient négligeable devant son compagnon. On obtient ainsi simplement $v_\nu(\texttt{PhiBK}) \geqslant O(dr\cdot\log_p^2(\frac{1}{\nu}))$.

2.2.4 L'algorithme sous forme synthétique

Rappelons pour commencer que l'objectif de cette première étape est, étant donné

- un (ϕ,N)-module filtré admissible effectif D donné par le quadruplet $(\texttt{Phi},\texttt{N},\texttt{H},\texttt{F})$ (voir §2.1),
- un nombre rationnel $\nu > 0$ et
- un nombre entier N

de calculer le module de Breuil–Kisin $\mathfrak{D}_\nu$ sur $\mathfrak{S}_\nu[1/p]$ avec précision $O(u^N)$. Comme $\mathfrak{D}_\nu$ est un $\mathfrak{S}_\nu[1/p]$-module libre de rang $d=\dim_{K_0} D$, se donner $\mathfrak{D}_\nu$ revient à se donner la matrice $\texttt{PhiBK}$ donnant l'action de ϕ sur $\mathfrak{D}_\nu$ dans une certaine base. En mettant ensemble tout ce qui a été dit dans les §§2.2.1, 2.2.2, 2.2.3, on obtient l'algorithme suivant pour calculer $\texttt{PhiBK}$.

(1) Déterminer un entier n tel que $\frac{1}{ep^n} \leqslant \nu$

(2) Calculer les matrices W_m $(0 \leqslant m < n)$ données par la formule (9)

(3) Écrire W_m sous la forme $W_m = W'_m\cdot U_m$ avec $W'_m \in \mathrm{GL}_d(\mathcal{O}_K)$ et U_m triangulaire supérieure (voir lemme 2.5)

(4) Calculer les matrices $\hat{W}'_m$ $(0 \leqslant m < n)$ par une variante de l'algorithme 1

(5) Tirer aléatoirement une matrice $\omega \in M_d(\mathbb{Z}_p)$

(6) Calculer la décomposition LU des matrices $\omega\cdot\hat{W}'_m$ mod $E(u)^r$ $(0 \leqslant m < n)$:

$$\omega\cdot\hat{W}'_m \equiv L_m V_m \pmod{E(u)^r}.$$

Si l'une des matrices $\omega\cdot\hat{W}'_m$ n'est pas connue avec suffisamment de précision pour pouvoir déterminer sa décomposition LU, revenir en (5)

(7) Calculer les matrices $Y_1, \dots, Y_n$ modulo u^N par la formule de récurrence (12)

(8) Calculer et retourner la matrice `PhiBK` donnée par la formule (14)

La correction de l'algorithme ci-dessus est une conséquence de la discussion menée dans les §§2.2.1, 2.2.2, 2.2.3. De plus, si tous les coefficients des matrices `Phi`, `N` et `F` sont connus avec précision $O(p^M)$, en suivant les pertes de précision au fil des calculs, on trouve successivement que :

- les coefficients des matrices W_m sont connus avec précision au moins $O(p^{M-mr})$;
- les coefficients des matrices W'_m sont connus avec précision au moins $O(p^{M-mr-dr})$;
- par le lemme 2.4, les coefficients de la matrice $\hat{W}'_m$ sont connus avec précision au moins $O(p^{M-mr-dr-\rho_1})$ où ρ_1 est la constante définie dans ce lemme où on a pris $i = r$;
- par l'alinéa (iii) du théorème 2.9, avec probabilité $\geqslant \frac{1}{2}$, le calcul de l'étape (6) n'échoue pas et les coefficients de la matrice L_m sont connus avec précision au moins $O(p^{M-mr-dr-\rho_1-2\lceil\rho_2\rceil})$ où ρ_2 est la constante définie dans ce théorème ;
- d'après l'estimation $v_\nu(t'_i) \geqslant -r(\frac{1}{e(p^i-1)} + \lceil \mathrm{val}(\mathfrak{d}_{K/K_0})\rceil)$ qui se déduit du lemme 2.12, les coefficients des matrices Y_m puis de la matrice `PhiBK` que l'on renvoie sont connus avec précision au moins $O(p^{M-M_0})$ où M_0 est une constante que l'on peut exprimer explicitement.

De même qu'à la fin du §2.2.3, on peut déduire de l'expression explicite de M_0 que, sous l'hypothèse supplémentaire $\nu < \frac{per}{p-1}$, on a :

$$M_0 = O(dr \cdot \log_p^2(\tfrac{1}{\nu})). \tag{19}$$

2.3 Étape 2 : Calcul d'un réseau dans un module de Breuil–Kisin

Maintenant que nous avons calculé $\mathfrak{D}_\nu$, l'étape suivante consiste à déterminer un $\mathfrak{S}_\nu$-réseau $\mathfrak{M}_\nu$ à l'intérieur de $\mathfrak{D}_\nu$ qui soit un module de Kisin de hauteur $\leqslant r$. Remarquons que l'on connaît déjà un réseau à l'intérieur de $\mathfrak{D}_\nu$: c'est celui donné par les vecteurs d'une base de la matrice `PhiBK` que l'on a calculée lors de la première étape et que l'on notera à partir de maintenant $\mathfrak{M}_\nu^{\text{G-L}}$. En outre, de même que précédemment on a obtenu une estimation de la constante M_0, on peut déterminer, par des arguments analogues, une constante C' qui dépend de façon polynômiale de d, r et $\log_p(\frac{1}{\nu})$ et qui vérifie :

$$p^{C'}\mathfrak{M}_\nu^{\text{G-L}} \subset \mathfrak{S}_\nu \otimes_{\mathfrak{S}} \beta_n(L) \subset p^{-C'}\mathfrak{M}_\nu^{\text{G-L}}$$

où $L \subset D$ est le $\mathcal{O}_{K_0}$-réseau standard engendré par les vecteurs de la base de D qui a été fixée au départ[9]. Par ailleurs, d'après la remarque 1.9, il existe une constante C qui s'exprime de façon polynômiale en d, r et $-\log_p(\nu)$ et un module de Breuil–Kisin $\mathfrak{M}_\nu$ sur $\mathfrak{S}_\nu$ tels que

$$p^{-C'}\mathfrak{S}_\nu \otimes_{\mathfrak{S}} \beta_n(L) \subset \mathfrak{M}_\nu \subset p^{C'-C} \cdot (\mathfrak{S}_\nu \otimes_{\mathfrak{S}} \beta_n(L)).$$

En posant $c_\nu = C + 2C'$, on obtient $p^{c_\nu} \cdot \mathfrak{M}_\nu^{\text{G-L}} \subset \mathfrak{M}_\nu \subset \mathfrak{M}_\nu^{\text{G-L}}$. De plus, par les résultats du §2.2.3, on sait calculer une constante explicite c telle que $\phi(\mathfrak{M}_\nu^{\text{G-L}}) \subset p^{-c} \cdot \mathfrak{M}_\nu^{\text{G-L}}$. On a en outre $c = O(dr \cdot \log_p^2(\frac{1}{\nu}))$ où la constante dans le $O(\cdot)$ dépend du corps K et, à vrai dire, plus précisément, de la valuation de la différente de K à K_0. De plus, en revenant au calcul de §2.2.3, on se rend compte que cette dépendance est, au pire, polynômiale.

[9] Il s'agit de la base de D dans lesquelles les matrices `Phi`, `N` et `F` ont été écrites.

Dans cette partie, nous expliquons comment déterminer $\mathfrak{M}_\nu$ — ou plutôt un $\mathfrak{M}_\nu$ convenable — connaissant $\mathfrak{M}_\nu^{\text{G-L}}$ et c_0. Le §2.3.1 est consacré à quelques rappels, extraits de [11], concernant la manipulation algorithmique des $\mathfrak{S}_\nu$-modules. On entre dans le cœur du sujet avec les numéros suivants. Dans les §§2.3.2 et 2.3.3, on montre comment, en itérant le Frobenius, on parvient à construire un module de Breuil–Kisin $\mathfrak{M}_{\nu,D}$ défini non pas sur $\mathfrak{S}_\nu$ mais sur un anneau de séries formelles à coefficients dans $K_0[\sqrt[p]{p}]$ (pour un certain entier D bien choisi). Dans le §2.3.4, on explique comment, quitte à faire quelques petites modifications, on peut redescendre $\mathfrak{M}_{\nu,D}$ en un authentique module de Breuil–Kisin défini (et libre) sur $\mathfrak{S}_\nu$ et, enfin, dans le §2.3.5, on présente l'algorithme obtenu sous forme synthétique.

2.3.1 L'algorithmique des $\mathfrak{S}_\nu$-modules : rappels et compléments

On rappelle dans ce numéro quelques algorithmes tirés de [11] pour la manipulation des $\mathfrak{S}_\nu$-modules. Ceux-ci seront constamment utilisés dans la suite.

D'un point de vue algorithmique, le fait que $\mathfrak{S}$ ne soit pas un anneau principal est un souci majeur. En effet, sur un anneau A non principal, il existe par définition des sous-modules de A^d qui ne sont pas libres, et travailler sur machine avec des modules non libres est nettement plus difficile. Par chance, la structure de $\mathfrak{S}$ est suffisamment simple (il s'agit d'un anneau local régulier de dimension 2) pour que l'on puisse quand même systématiquement se ramener à des modules libres quitte à ajouter de temps en temps un morceau fini. Plus précisément, si $\mathfrak{M}$ est un sous-$\mathfrak{S}$-module de type fini de $(\mathcal{E}^+)^d$, on définit

$$\text{Max}(\mathfrak{M}) = \Big\{ x \in (\mathcal{E}^+)^d \;\Big|\; \exists n \in \mathbb{N},\, p^n x \in \mathfrak{M} \text{ et } u^n x \in \mathfrak{M} \Big\}.$$

Il est clair que le quotient $\text{Max}(\mathfrak{M})/\mathfrak{M}$ est annulé, à la fois, par une puissance de p et une puissance de u. Comme $\mathfrak{M}$ est finiment engendré, ceci implique que $\text{Max}(\mathfrak{M})/\mathfrak{M}$ est de longueur fini comme $\mathfrak{S}$-module. En particulier, c'est un ensemble fini si le corps résiduel k est lui-même fini. Il fait ainsi sens de dire que l'on passe de $\mathfrak{M}$ à $\text{Max}(\mathfrak{M})$ en « ajoutant un morceau fini ».

Théorème 2.13 (Iwasawa)**.** *Pour tout $\mathfrak{S}$-module de type fini $\mathfrak{M} \subset (\mathcal{E}^+)^d$, le module* $\text{Max}(\mathfrak{M})$ *est le plus petit sous-module libre de $(\mathcal{E}^+)^d$ qui contient $\mathfrak{M}$.*

Si l'on suppose que l'on sait manipuler dans leur intégralité les éléments de $\mathfrak{S}$, le Max que l'on a défini ci-dessus a, de surcroît, la propriété intéressante de pouvoir être calculé explicitement ; un « algorithme », pour ce faire, est décrit dans le §3.3.1 de [11]. Pour le propos de cet article, on aura besoin de l'appliquer uniquement dans un cas particulier plus simple qui est celui du calcul de $\text{Max}(\mathfrak{M} + x\mathfrak{S})$ où $\mathfrak{M}$ est un sous-module libre de $(\mathcal{E}^+)^d$ de rang maximal donné par l'intermédiaire d'une base et x est un vecteur de $\mathfrak{S}^d$. Dans ce cas, si on note v_0 (resp. $\deg_0$) la valuation de Gauss (resp. le degré de Weierstrass) sur $\mathfrak{S}$, l'algorithme fonctionne comme suit :

Algorithme 3: AJOUTVECTEUR$(\mathfrak{M}, x)$

Entrée : une base $(e_1, \dots, e_d)$ de $\mathfrak{M} \subset (\mathcal{E}^+)^d$ et un vecteur $X \in (\mathcal{E}^+)^d$
Sortie : une base de $\mathrm{Max}(\mathfrak{M} + X\mathfrak{S})$

$(x_1, \dots, x_d) \leftarrow$ coordonnées de x sur la base $(e_1, \dots, e_d)$;
tant que *l'un des* x_i *n'est pas dans* $\mathfrak{S}$ **faire**
  $i \leftarrow$ indice tel que $v_0(x_i)$ est minimal;
  $j \leftarrow$ indice distinct de i tel que $v_0(x_j)$ est minimal;
  $\delta \leftarrow \min(0, v_0(x_j)) - v_0(x_i)$; $x_i \leftarrow p^\delta x_i$; $e_i \leftarrow p^{-\delta} e_i$;
  si $v_0(x_j) < 0$ **alors**
    si $\deg_0(x_i) < \deg_0(x_j)$ **alors** échanger i et j;
    $(q, r) \leftarrow$ quotient et reste de la division euclidienne de x_i par x_j;
    $x_i \leftarrow r$; $e_i \leftarrow e_i + q e_j$;
retourner $(e_1, \dots, e_d)$;

La démonstration de la correction de l'algorithme précédent n'est pas très difficile. On commence par remarquer qu'après chaque itération, la famille des e_i reste toujours libre, que l'espace qu'elle engendre est inclus dans $\mathrm{Max}(\mathfrak{M} + x\mathfrak{S})$ et, finalement, que la relation $x = x_1 e_1 + \cdots + x_d e_d$ continue d'être vérifiée. Ainsi, lorsque l'on quitte la boucle, x s'écrit comme combinaison linéaire à coefficients dans $\mathfrak{S}$ des e_i ; autrement dit, si on appelle $\mathfrak{M}'$ l'espace engendré par ces e_i, on a $x \in \mathfrak{M}'$ et donc $\mathfrak{M} + x\mathfrak{S} \subset \mathfrak{M}'$. Par ailleurs, comme les e_i forment une famille libre, le module $\mathfrak{M}'$ est libre et l'inclusion précédente donne alors $\mathrm{Max}(\mathfrak{M} + x\mathfrak{S}) \subset \mathfrak{M}'$. L'égalité en résulte puisque l'on a déjà dit que l'inclusion précédente était vraie.

Dans la suite, on aura besoin de travailler non seulement avec des $\mathfrak{S}$-modules, mais aussi avec $\mathfrak{S}_\nu$-modules. Or, malheureusement, le théorème 2.13 ne vaut plus lorsque l'on remplace $\mathfrak{S}$ par $\mathfrak{S}_\nu$. Pour résoudre ce problème, on suppose que ν est un nombre rationnel s'écrivant sous la forme $\nu = \frac{a}{b}$, on fixe un élément $\varpi_b \in \bar{K}$ tel que $\varpi_b^b = p$ et on introduit l'anneau

$$\mathfrak{S}_{\nu,b} = \left\{ \sum_{i \in \mathbb{N}} a_i u^i \quad \middle| \quad \begin{array}{l} a_i \in K_0[\varpi_b] \\ \mathrm{val}(a_i) + \nu i \geqslant 0,\ \forall i \end{array} \right\}.$$

Celui-ci s'identifie à l'anneau des séries formelles à coefficients dans $\mathcal{O}_{K_0}[\varpi_b]$ — qui est l'anneau des entiers de $K_0[\varpi_b]$ — en la variable $\frac{u}{\varpi_b^a}$, d'où on déduit que le théorème d'Iwasawa s'applique à cet anneau. Pour éviter les confusions, on notera $\mathrm{Max}_{\nu,b}$ le foncteur Max correspondant ; en posant $\mathcal{E}^+_{\nu,b} = \mathfrak{S}_{\nu,b}[1/p]$, on a donc

$$\mathrm{Max}_{\nu,b}(\mathfrak{M}_{\nu,b}) = \left\{ x \in (\mathcal{E}^+_{\nu,b})^d \;\middle|\; \exists n \in \mathbb{N},\ p^n x \in \mathfrak{M}_{\nu,b} \text{ et } (\tfrac{u}{\varpi_b^a})^n x \in \mathfrak{M}_{\nu,b} \right\}$$

pour un $\mathfrak{S}_{\nu,b}$-module de type fini $\mathfrak{M}_{\nu,b} \subset (\mathcal{E}^+_{\nu,b})^d$. Lorsqu'en outre $\mathfrak{M}_{\nu,b}$ est défini sur $\mathfrak{S}_\nu$, on peut démontrer (voir proposition 3.9 et lemme 3.18 de [11]) que $\mathrm{Max}_{\nu,b}(\mathfrak{M}_{\nu,b})$ admet une base formée des vecteurs de la forme $e_i = \varpi_b^{-b_i} B_i$ avec $b_i \in \mathbb{N}$ et $B_i \in (\mathcal{E}^+_\nu)^d$. Mieux encore, si l'on applique l'algorithme 3 avec pour entrée des vecteurs e_i et x prenant la forme précédente, alors la sortie a également cette forme[10].

Enfin, dans le §3.3.4 de [11], il est présenté un algorithme qui, étant donné un $\mathfrak{S}_{\nu,b}$-module libre $\mathfrak{M}_{\nu,b}$ engendré par des vecteurs $e_i = \varpi_b^{-b_i} B_i$ avec $b_i \in \mathbb{N}$ et $B_i \in (\mathcal{E}^+_\nu)^d$, calcule l'intersection

[10] On peut utiliser cette remarque pour démontrer que $\mathrm{Max}_{\nu,b}(\mathfrak{M}_{\nu,b})$ prend la forme annoncée lorsque $\mathfrak{M}_{\nu,b}$ est défini sur $\mathfrak{S}_\nu$; il s'agit d'ailleurs de l'approche qui est suivie dans [11].

$\mathfrak{M}_{\nu,b} \cap (\mathcal{E}_\nu^+)^b$. Dans le cas général, la description de cet algorithme n'est pas triviale[11] mais elle prend une forme particulièrement simple lorsque $\nu = \frac{1}{b}$; en effet, dans ce cas, on montre que, si q_i et r_i désignent respectivement le quotient et le reste de la division euclidienne de $-b_i$ par b, l'intersection $\mathfrak{M}_{\nu,b} \cap (\mathcal{E}_\nu^+)^b$ est engendrée par les vecteurs

$$p^{q_i+1} B_i \quad \text{et} \quad p^{q_i} u^{r_i} B_i$$

pour i variant de 1 à d.

Tel qu'il est écrit, l'algorithme 3 souffre d'un défaut majeur lié à la précision : lorsqu'un élément $x \in \mathcal{E}^+$ n'est connu qu'à précision u-adique fini, il n'est pas possible de calculer $v_0(x)$! En effet, si $x = \sum_{i \in \mathbb{N}} a_i u^i$ (avec $a_i \in K_0$) et si l'on ne connaît que les a_i pour $i < N$, il est impossible de dire avec certitude quel est le minimum des $\mathrm{val}(a_i)$. Or, manifestement, savoir calculer les valuations d'éléments de $\mathcal{E}^+$ est essentiel au bon déroulement de l'algorithme 3.

Résoudre ce problème sans hypothèse supplémentaire paraît très délicat. Il est toutefois possible d'y apporter une réponse satisfaisante si l'on suppose en outre que $X \in p^{-c}\,\mathfrak{M}$ pour un certain entier c connu, ce qui revient encore à dire que tous les x_i sont dans $p^{-c}\,\mathfrak{S}$. Or, si on travaille sur machine avec la représentation PAG des éléments de $\mathfrak{S}$ (voir §2.1), un entier c vérifiant la condition précédente est facile à obtenir : c'est le minimum des garanties des éléments x_i. Toutefois, dans un souci de simplification, plutôt que de recourir aux informations contenues dans les représentations PAG, nous supposons simplement par la suite qu'un entier c convenable est passé en argument à l'algorithme 3. Ceci ne portera pas à préjudice car, dans la situation qui nous occupe, un tel entier c sera connu *a priori* grâce au calcul du §2.2.3.

Expliquons à présent comment utiliser cette hypothèse supplémentaire que nous venons de formuler. Cela ne coule pas de source car elle n'est, de fait, pas suffisante pour garantir que l'on puisse calculer les $v_0(x_i)$. Cependant, si les calculs se font à la précision u-adique $O(u^N)$, elle assure que l'on peut déterminer sans ambiguïté les $v_{c/N}(x_i)$ au moins si ceux-ci sont négatifs ou nuls : si un élément $x = \sum_{i \in \mathbb{N}} a_i u^i$ est dans $p^{-c}\,\mathfrak{S}$, tous les coefficients a_i ont une valuation $\geqslant -c$, d'où on tire que $\mathrm{val}(a_i) + \frac{c}{N} i \geqslant 0$ dès que $i \geqslant N$. Or, un examen rapide de l'algorithme 3 montre que son comportement n'est pas modifié si l'on commet une erreur sur le calcul d'une valuation positive (dans la mesure, bien sûr, où l'on obtient quand même un résultat positif). Ainsi, sous l'hypothèse supplémentaire que l'on a faite, afin de faire fonctionner l'algorithme 3 avec des calculs à précision finie u^N, il suffit de remplacer partout v_0 par $v_{c/N}$ et $\mathcal{E}^+$ par $\mathcal{E}^+_{\nu,N}$. Le résultat renvoyé est une base de $\mathrm{Max}_{2c/N,N}(\mathfrak{S}_{2c/N,N} \otimes_{\mathfrak{S}_\nu} \mathfrak{M} + x\,\mathfrak{S}_{2c/N,N})$ si l'on souhaite un résultat exact. Si l'on peut se contenter d'un résultat approché à u^N, l'algorithme renvoie une base de $\mathrm{Max}_{c/N,N}(\mathfrak{S}_{c/N,N} \otimes_{\mathfrak{S}_\nu} \mathfrak{M} + x\,\mathfrak{S}_{c/N,N})$ avec $\frac{c}{N}$ à la place de $\frac{2c}{N}$; exactement, cela signifie que, quitte à ajouter des multiples de u^N aux vecteurs renvoyés par l'algorithme, ceux-ci forment une base du dernier espace que l'on a écrit. Tout ceci s'étend au cas où l'on part d'un module $\mathfrak{M}$ et d'un vecteur x définis sur $\mathfrak{S}_{\nu,b}$ et que l'on prend pour N un multiple de b.

Utilisation de l'algorithme 3 pour la suite Dans la suite de cet article, on manipulera essentiellement des modules sur les anneaux $\mathfrak{S}_{\nu,b}$ munis d'un opérateur semi-linéaire ϕ et, plutôt que de calculer une base d'un tel module, il sera souvent plus intéressant, pour ce que l'on souhaite faire, de calculer l'action de ϕ sur ce module. Ainsi, plutôt qu'un algorithme qui prend en entrée un module $\mathfrak{M}$, un vecteur x et renvoie le Max du module engendré par $\mathfrak{M}$ et x (après une extension éventuelle des scalaires), on utilisera avec plaisir un algorithme qui prend en entrée une matrice `PhiBK` donnant l'action d'un opérateur ϕ agissant sur un module $\mathfrak{M}$ et un vecteur x et qui renvoie une nouvelle matrice `PhiBK` donnant cette fois-ci l'action de ϕ sur le Max du module engendré par $\mathfrak{M}$ et x (encore une fois, éventuellement, après extension des scalaires).

[11] Elle fait appel à la théorie des fractions continues, au moins si l'on souhaite une version efficace.

C'est exactement ce que fait l'algorithme 4, présenté page 32. En plus de cela, il prend en compte toutes les remarques et améliorations qui ont été mises en lumière précédemment et met à profit la remarque sur la forme particulière $\varpi_N^{-b_i} B_i$ que prennent les vecteurs de base que l'on calcule pour faire en sorte de toujours travailler uniquement sur les anneaux $\mathcal{E}_\nu^+$, et non sur les $\mathcal{E}_{\nu,b}^+$.

Algorithme 4: CHANGEBASE$(b, \texttt{PhiBK}, a, X, c, N, \nu)$ *Hypothèse : $N\nu$ est entier*

Notation : : Si V est un vecteur, on désigne par $V[i]$ sa i-ième composante
: Si A est une matrice, on désigne par :
: $A[i,j]$ son coefficient en i-ième ligne et j-colonne
: $A[i,\cdot]$ sa i-ième ligne
: $A[\cdot,j]$ sa j-ième colonne

NB : : Tous les calculs dans cet algorithme sont effectués à précision u^N

Entrée : : $\star$ un vecteur $b = (b_1 \ \dots \ b_d)$ d'entiers relatifs
: $\star$ une matrice $\texttt{PhiBK} \in M_d(\mathcal{E}_\nu^+)$ donnant l'action, dans la base canonique $(e_i)_{1\leqslant i\leqslant d}$,
: d'un opération semi-linéaire $\phi : (\mathcal{E}_{\nu,N}^+)^d \to (\mathcal{E}_{\nu,N}^+)^d$
: $\star$ un vecteur $x \in (\mathcal{E}_{\nu,N}^+)^d$ donné sous la forme $x = \varpi_N^{-a} X$
: où a est un entier et X un vecteur colonne à coefficients dans $\mathcal{E}_\nu^+$
: $\star$ les paramètres habituels c, N et ν

Sortie : : $\star$ un vecteur $b' = (b'_1 \ \dots \ b'_d)$ d'entiers relatifs
: $\star$ la matrice $\texttt{PhiBK}'$ de ϕ écrite dans la base des e'_i où les $\varpi_N^{-b'_i} e'_i$
: forme une base de $\mathrm{Max}_{\nu+c/N,N}\big(\langle x,\ \varpi_N^{-b_i} e_i \,(1 \leqslant i \leqslant d)\rangle\big)$

$\nu' \leftarrow \nu + \frac{c}{N}$;
tant que *il existe i tel que* $v_{\nu'}(X[i]) + b_i < a$ **faire**
  $i \leftarrow$ indice tel que $v_{\nu'}(X[i]) + b_i$ est minimal; $v_i \leftarrow v_{\nu'}(X[i]) + b_i$;
  $j \leftarrow$ indice distinct de i tel que $v_{\nu'}(X[j]) + b_j$ est minimal; $v_j \leftarrow v_{\nu'}(X[j]) + b_j$;
  $\delta \leftarrow \min(a, v_j) - v_i$; $b_i \leftarrow b_i + \delta$;
  si $v_j < a$ **alors**
    si $\deg_{\nu'}(X[i]) < \deg_{\nu'}(X[j])$ **alors** échanger i et j;
    $(q, r) \leftarrow$ quotient et reste de la division euclidienne (dans $\mathcal{E}_\nu^+$) de $X[i]$ par $X[j]$;
    $X[i] \leftarrow r$;
    $\texttt{PhiBK}[\cdot, i] \leftarrow \texttt{PhiBK}[\cdot, i] + \phi(q) \cdot \texttt{PhiBK}[\cdot, j]$;
    $\texttt{PhiBK}[i, \cdot] \leftarrow \texttt{PhiBK}[i, \cdot] - q \cdot \texttt{PhiBK}[j, \cdot]$;
retourner $b, \texttt{PhiBK}$;

2.3.2 Une idée simple

On revient à présent à la situation du début du §2.3. Cependant, dans cette partie introductive destinée simplement à présenter les idées sous-jacente à l'algorithme, on suppose pour simplifier que $\nu = 0$. On suppose donc donnés un $\mathfrak{S}$-module $\mathfrak{M}^{\text{G-L}}$, ainsi que des entiers c et c_0 vérifiant $\phi(\mathfrak{M}^{\text{G-L}}) \subset p^{-c} \cdot \mathfrak{M}^{\text{G-L}}$ et $p^{c_0} \cdot \mathfrak{M}^{\text{G-L}} \subset \mathfrak{M} \subset \mathfrak{M}^{\text{G-L}}$ pour un certain module de Breuil–Kisin $\mathfrak{M}$.

Puisque $\mathfrak{M}$ doit être un module de Breuil–Kisin, il est particulier stable par ϕ et donc, s'il

contient $\mathfrak{M}^{\text{G-L}}$, il contient nécessairement aussi $\phi(\mathfrak{M}^{\text{G-L}})$ et donc par suite la somme $\mathfrak{M}^{\text{G-L}} + \big\langle \phi(\mathfrak{M}^{\text{G-L}}) \big\rangle_{\mathfrak{S}}$. Comme en outre $\mathfrak{M}$ est libre, il contient nécessairement le Max de cette somme d'après le théorème 2.13. En répétant l'argument, on trouve que $\mathfrak{M}$ contient tous les sous-modules $\mathfrak{M}^{(s)} \subset \mathcal{E}^+ \otimes_{\mathfrak{S}} \mathfrak{M}^{\text{G-L}}$ définis par récurrence par :

$$\mathfrak{M}^{(1)} = \mathfrak{M}^{\text{G-L}} \quad ; \quad \mathfrak{M}^{(s+1)} = \text{Max}\Big(\mathfrak{M}^{(s)} + \big\langle \phi(\mathfrak{M}^{(s)}) \big\rangle_{\mathfrak{S}} \Big). \tag{20}$$

Comme tous les $\mathfrak{M}^{(s)}$ sont inclus dans $p^{-c_0}\,\mathfrak{M}^{\text{G-L}}$ qui est libre de rang fini sur l'anneau $\mathfrak{S}$ qui est noethérien, la suite des $\mathfrak{M}^{(s)}$, qui est manifestement croissante, est stationnaire. Soit $\mathfrak{M}^{(\infty)}$ sa limite ; à l'évidence, c'est un sous-$\mathfrak{S}$-module libre de $\mathfrak{D}$ qui est stable par ϕ. La proposition suivante montre que cela suffit à en faire un module de Breuil–Kisin.

Proposition 2.14. *Soient $\mathfrak{M}$ un module de Breuil–Kisin de hauteur $\leqslant r$ sur $\mathfrak{S}$ et $\mathfrak{D} = \mathcal{E}^+ \otimes_{\mathfrak{S}} \mathfrak{M}$. Soit $\mathfrak{M}'$ un sous-$\mathfrak{S}$-module de $\mathfrak{D}$ libre de rang fini, stable par ϕ tel que $\mathfrak{D} = \mathcal{E}^+ \otimes_{\mathfrak{S}} \mathfrak{M}'$. Alors $\mathfrak{M}'$ est un module de Breuil–Kisin de hauteur $\leqslant r$.*

Démonstration. On suppose pour commencer que $\mathfrak{M}$ est de rang 1 ; il en est alors de même de $\mathfrak{M}'$. On note x (resp. x') une base de $\mathfrak{M}$ (resp. de $\mathfrak{M}'$) sur $\mathfrak{S}$ et on note s (resp. s') l'unique élément de $\mathfrak{S}$ tel que $\phi(x) = sx$ (resp. $\phi(x') = s'x'$). On introduit également l'élément $a \in \mathcal{E}^+$ défini par l'égalité $x' = ax$. Il est inversible dans $\mathcal{E}^+$ (puisque $\mathcal{E}^+ \otimes_{\mathfrak{S}} \mathfrak{M} = \mathcal{E}^+ \otimes_{\mathfrak{S}} \mathfrak{M}' = \mathfrak{D}$) et s'écrit donc sous la forme $a = p^n b$ avec $n \in \mathbb{Z}$ et b inversible dans $\mathfrak{S}$. Par ailleurs, de $\phi(x') = \phi(ax) = \phi(a)\phi(x) = \phi(a)sx$, on déduit la relation $s' = \frac{\phi(a)}{a}\, s = \frac{\phi(b)}{b}\, s$. Or, comme $\mathfrak{M}$ est un module de Breuil–Kisin de hauteur $\leqslant r$, il est clair que s divise $E(u)^r$. Ainsi s' divise lui aussi $E(u)^r$, ce qui implique réciproquement que $\mathfrak{M}'$ est un module de Breuil–Kisin de hauteur $\leqslant r$.

Si maintenant $\mathfrak{D}$ est de rang d, on considère sa d-ième puissance extérieure $\Lambda^d\mathfrak{D}$. À l'intérieur de ce $\mathcal{E}^+$-module de rang 1 vivent les réseaux $\Lambda^d\mathfrak{M}$ et $\Lambda^d\mathfrak{M}'$. Le premier est un module de Breuil–Kisin de hauteur $\leqslant dr$, d'où il résulte, *via* le premier point, qu'il en est de même du second. Cela implique facilement que $\mathfrak{M}'$, lui-même, est un module de Breuil–Kisin de hauteur $\leqslant dr$. Il faut à présent montrer qu'il est en fait de hauteur $\leqslant r$. Pour cela, on fixe une $\mathfrak{S}$-base $(e'_1, \dots, e'_d)$ de $\mathfrak{M}'$ et on considère un élément $x \in \mathfrak{M}'$. Puisque $\mathfrak{M}$ est de hauteur $\leqslant r$ et que les e'_i forment une $\mathcal{E}^+$-base de $\mathfrak{D} = \mathfrak{M}[1/p]$, on peut écrire le produit $E(u)^r x$ sous la forme :

$$E(u)^r x = a_1\phi(e'_1) + a_2\phi(e'_2) + \cdots + a_d\phi(e'_d)$$

pour des éléments $a_i \in \mathcal{E}^+$. Pour conclure, il suffit de démontrer que tous les a_i sont dans $\mathfrak{S}$. Or, puisque l'on a prouvé que $\mathfrak{M}'$ est de hauteur $\leqslant dr$, on sait que $E(u)^{rd}x$ appartient au $\mathfrak{S}$-module engendré par les $\phi(e'_1)$, ce qui revient à dire que tous les $E(u)^{r(d-1)}a_i$ appartiennent à $\mathfrak{S}$. En prenant les valuations de Gauss, on trouve $r(d-1)v_0(E(u)) + v_0(a_i) \geqslant 0$, soit encore $v_0(a_i) \geqslant 0$ car $v_0(E(u)) = 0$. Ainsi $a_i \in \mathfrak{S}$ pour tout i et on a bien démontré ce qui avait été annoncé. □

À ce stade, on a compris ce que l'on a à faire pour calculer un module de Breuil–Kisin $\mathfrak{M}$ à l'intérieur de $\mathfrak{D}$: on calcule les $\mathfrak{M}^{(n)}$ définis par la formule récurrence (20) jusqu'à ce que celle-ci stationne et, à ce moment, le module $\mathfrak{M}^{(\infty)}$ obtenu est un module de Breuil–Kisin comme souhaité. On peut en outre borner explicitement le rang à partir duquel la suite des $\mathfrak{M}^{(n)}$ stationne, comme le précise le lemme suivant.

Lemme 2.15. *Sous les hypothèses précédentes, on a $\mathfrak{M}^{(\infty)} = \mathfrak{M}^{(d)}$.*

Démonstration. Soit $\mathcal{O}_{\mathcal{E}}$ le complété p-adique de $\mathfrak{S}[1/u]$. La valuation de Gauss v_0 s'étend à $\mathcal{O}_{\mathcal{E}}$ et fait de ce dernier un anneau de valuation discrète complet de corps résiduel $k((u))$. De même, il est clair que le Frobenius ϕ se prolonge en un endomorphisme de $\mathcal{O}_{\mathcal{E}}$. Par ailleurs, il suit du théorème 3.12 (appliqué avec $\nu = 0$) de [11] qu'en posant $M^{(n)} = \mathcal{O}_{\mathcal{E}} \otimes_{\mathfrak{S}} \mathfrak{M}^{(n)}$, on a les deux propriétés suivantes valables pour tout $n \geqslant 0$:

(i) l'égalité $\mathfrak{M}^{(n)} = \mathfrak{M}^{(n+1)}$ est équivalente à $M^{(n)} = M^{(n+1)}$;

(ii) $\mathfrak{M}^{(n+1)} = \mathfrak{M}^{(n)} + (\phi \otimes \phi)(\mathfrak{M}^{(n)})$.

Pour tout entier n, notons $f_n : \frac{M^{(n)}}{p\,M^{(n)}} \to \frac{M^{(\infty)}}{p\,M^{(\infty)}}$ l'application déduite de l'inclusion $M^{(n)} \subset M^{(\infty)}$; il s'agit d'une application $k((u))$-linéaire entre $k((u))$-espaces vectoriels de dimension d. De la suite d'inclusions $M^{(n)} \subset M^{(n+1)} \subset M^{(\infty)}$, on déduit que f_n se factorise par f_{n+1} et, par suite, que l'image de f_{n+1} contient celle de f_n. On a ainsi la suite d'inclusions :

$$\text{im } f_0 \subset \text{im } f_1 \subset \cdots \subset \text{im } f_{d+1}.$$

Comme tous les espaces ci-dessus sont des sous-$k((u)$-espaces vectoriels de $\frac{M^{(\infty)}}{p\,M^{(\infty)}}$ qui est de dimension d, il existe nécessairement un entier $\ell \leqslant d$ tel que im $f_\ell =$ im $f_{\ell+1}$. En revenant aux définitions, cela signifie que, pour cet entier ℓ, on a $M^{(\ell+1)} \subset M^{(\ell)} + pM^{(\infty)}$. En appliquant $\phi \otimes \phi$ à cette égalité puis en sommant, on obtient $M^{(\ell+2)} \subset M^{(\ell+1)} + pM^{(\infty)} \subset M^{(\ell)} + pM^{(\infty)}$. En répétant l'argument, on démontre par récurrence que, pour tout entier n, l'inclusion $M^{(\ell+n)} \subset M^{(\ell)} + pM^{(\infty)}$ est vérifiée. En passant à la limite, on en déduit que $M^{(\infty)} \subset M^{(\ell)} + pM^{(\infty)}$. Ceci implique que $M^{(\infty)} \subset M^{(\ell)}$ puis que ces deux espaces coïncident étant donné que l'inclusion réciproque est vraie par construction. Comme $\ell \leqslant d$, on en déduit l'énoncé du lemme. □

Remarque 2.16. *Plutôt que de calculer les $\mathfrak{M}^{(n)}$ un par un à l'aide de la formule itérative* (20)*, il est bien plus efficace de procéder comme suit. On pose $\phi_0 = \phi$, $\mathfrak{M}_{(0)} = \mathfrak{M}^{\text{G-L}}$ et on définit par récurrence :*

$$\phi_{m+1} = \phi_m \circ \phi_m \quad ; \quad \mathfrak{M}_{(m+1)} = \text{Max}\Big(\mathfrak{M}_{(m)} + \big\langle \phi_m(\mathfrak{M}_{(m)})\big\rangle_{\mathfrak{S}}\Big). \tag{21}$$

Il est facile de montrer que $\mathfrak{M}_{(m)} = \mathfrak{M}^{(2^m)}$ pour tout entier $i \geqslant 0$. Ainsi comme on sait par le lemme 2.15 que la suite des $\mathfrak{M}^{(n)}$ stationne au plus après d étapes, la limite sera atteinte au bout de $\log_2 d$ étapes pour la suite des $\mathfrak{M}_{(m)}$. Ceci constitue un gain important pour la complexité.

Les complications Les principales complications viennent du fait que, malheureusement, on ne peut pas faire comme si tout se passait sur $\mathfrak{S}$. En effet,

(i) on ne dispose en général pas du module $\mathfrak{M}^{\text{G-L}}$ — qui, rappelons-le, sert de point de départ pour les itérations que l'on souhaite faire — mais uniquement d'un $\mathfrak{M}_\nu^{\text{G-L}}$ pour un certain $\nu > 0$ (que l'on peut, certes, choisir), et

(ii) comme cela a été expliqué au §2.3.1, on ne peut pas calculer un Max en restant à ν constant à cause des problèmes de précision.

On est ainsi amené à reprendre tout ce qui précède en essayant de remplacer partout $\mathfrak{S}$ par $\mathfrak{S}_\nu$. Or, déjà sans aller très loin, on voit apparaître de nombreux problèmes ; en vrac

- la notion de Max n'a pas été définie sur les anneaux $\mathfrak{S}_\nu$: il va donc falloir, comme cela est expliqué au §2.3.1 travailler sur des extensions $\mathfrak{S}_{\nu,b}$ puis redescendre à $\mathfrak{S}_\nu$ en prenant des intersections ;

- il n'est pas vrai, en général, que l'intersection de $\mathfrak{D}_\nu$ avec un $\mathfrak{S}_{\nu,b}$-module libre est libre sur $\mathfrak{S}_\nu$; il faudra donc travailler davantage pour obtenir un module de Breuil–Kisin ;

- afin de pouvoir appliquer le théorème 1.11, il faut que la pente à laquelle on aboutit finalement reste $< \frac{p-1}{per}$; comme la pente est modifiée après chaque calcul de Max, il faudra faire attention à contrôler le nombre de ces calculs.

Ces problèmes sont résolus dans les numéros suivants. Précisément, dans le §2.3.3 ci-après, on explique comment à partir de la donnée de $\mathfrak{M}_\nu^{\text{G-L}}$ (pour un $\nu > 0$) et de l'entier c_ν correspondant, on peut construire, en itérant le Frobenius, un $\mathfrak{S}_{\nu',b}$-module libre $\mathfrak{M}_{\nu',b}$ stable par ϕ (pour un certain b et un certain $\nu' > \nu$). L'intersection $\mathfrak{S}_{\nu',b} \cap (\mathcal{E}^+_{\nu'} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}})$ — que l'on sait calculer (voir §2.3.1) — apparaît alors comme un candidat raisonnable pour être un module de Breuil–Kisin $\mathfrak{M}_{\nu'}$. Hélas, en général, cela ne fonctionne pas tel quel car rien n'assure qu'elle est libre sur $\mathfrak{S}_{\nu'}$. Nous résolvons ce problème, ainsi que quelques autres, dans le §2.3.4.

2.3.3 Itération du Frobenius

À partir de maintenant, on oublie le cas d'école « $\nu = 0$ » et on se place à nouveau dans le cas « $\nu > 0$ » : précisément, on suppose donnés un $\mathfrak{S}_\nu$-module $\mathfrak{M}_\nu^{\text{G-L}}$ muni d'une application semi-linéaire $\phi : \mathfrak{M}_\nu^{\text{G-L}} \to p^{-c} \cdot \mathfrak{M}_\nu^{\text{G-L}}$ pour un certain entier $c = O(dr \cdot \log_p^2(\frac{1}{\nu}))$ connu. On suppose en outre que l'on connaît un entier c_ν pour lequel on a la garantie qu'il existe un module de Breuil–Kisin de hauteur $\leqslant r$ compris entre $p^{-c_\nu}\,\mathfrak{M}_\nu^{\text{G-L}}$ et $\mathfrak{M}_\nu^{\text{G-L}}$. On rappelle que l'application ϕ dont il a été question ci-dessus est donnée par l'intermédiaire de sa matrice (dans une certaine base) notée `PhiBK` et que celle-ci est connue modulo u^N pour un certain entier N que l'on peut choisir comme on le souhaite.

À partir de maintenant, on notera $c_{\text{G-L}}$ à la place de c_ν ; cela permettra, malgré les apparences, d'éviter quelques confusions : en effet, dans la suite, on sera amené à considérer de multiples autres pentes que ν, alors que la constance $c_{\text{G-L}}$, elle, sera toujours la même.

La suite des $\mathfrak{M}^{(n)}$ revisitée Pour pouvoir appliquer les algorithmes rappelés au §2.3.1 à la situation présente, on introduit deux nouveaux paramètres entiers D et N, que l'on choisira judicieusement plus tard. Conformément aux notations du §2.3.1, l'entier N désignera la précision u-adique à laquelle les calculs seront effectués. Pour le moment, on conserve une certaine liberté sur le choix de D et N et on impose seulement que N soit un dénominateur de ν (*i.e.* que $N\nu$ soit entier), que D soit un dénominateur de ν' et que D divise N. On va adapter la définition de la suite des $\mathfrak{M}^{(n)}$ afin que l'action du Frobenius sur ceux-ci puisse être calculée à l'aide de l'algorithme 4. En fait, plutôt qu'une seule suite, on va en définir trois : $(\mathfrak{M}^{(n)}_{\nu_n,N})$ avec $\nu_n = \nu + \frac{2nc}{N}$, $(\mathfrak{M}^{(n)}_{\nu_n,D})$ et $(\mathfrak{M}^{(n)}_{\nu',D})$. Dans l'écriture précédente, l'exposant (n) correspond, bien entendu, au rang dans la suite tandis que les indices indiquent sur quel anneau le module correspondant est défini. On notera en particulier que N est un dénominateur commun à tous les ν_n ; les anneaux $\mathfrak{S}_{\nu_n,N}$ sont donc des anneaux de séries formelles en une variable, au même titre d'ailleurs que l'anneau $\mathfrak{S}_{\nu',D}$ d'après l'hypothèse faite sur D. Pour l'initialisation, on pose :

$$\mathfrak{M}^{(0)}_{\nu,N} = \mathfrak{S}_{\nu,N} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}} \quad ; \quad \mathfrak{M}^{(0)}_{\nu,D} = \mathfrak{S}_{\nu,D} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}} \quad ; \quad \mathfrak{M}^{(0)}_{\nu',D} = \mathfrak{S}_{\nu',D} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}}.$$

Si on suppose maintenant que les suites précédentes sont construites jusqu'au rang n, on distingue les deux cas suivants :

- soit le module $\mathfrak{M}^{(n)}_{\nu',D}$ est stable par ϕ et, à ce moment, on arrête le processus,
- soit il existe un vecteur $x_n \in \phi(\mathfrak{M}^{(n)}_{\nu_n,D})$, $x_n \notin \mathfrak{M}^{(n)}_{\nu',D}$ et on définit alors

$$\begin{aligned}
\mathfrak{M}^{(n+1)}_{\nu_{n+1},N} &= \text{Max}_{\nu_{n+1},N}\big(\mathfrak{S}_{\nu_{n+1},N} \otimes_{\mathfrak{S}_{\nu_n,N}} \mathfrak{M}^{(n)}_{\nu_n,N} + x_n\,\mathfrak{S}_{\nu_{n+1},N}\big) \\
\mathfrak{M}^{(n+1)}_{\nu_{n+1},D} &= \mathfrak{M}^{(n+1)}_{\nu_{n+1},N} \cap \big(\mathcal{E}^+_{\nu_{n+1},D} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}}\big) \\
\mathfrak{M}^{(n+1)}_{\nu',D} &= \big(\mathfrak{S}_{\nu',N} \otimes_{\mathfrak{S}_{\nu_{n+1},N}} \mathfrak{M}^{(n+1)}_{\nu_{n+1},N}\big) \cap \big(\mathcal{E}^+_{\nu',D} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}}\big).
\end{aligned}$$

On remarquera que, dans ce qui précède, on a fait l'hypothèse implicite que $\nu_{n+1} \leqslant \nu'$; en effet, dans le cas contraire, les produits tensoriels que l'on a écrits n'ont aucun sens. Dans la suite, on choisira les paramètres D et N de sorte que le processus s'arrête toujours avant que cette inégalité ne soit violée. On notera également qu'il n'est *a priori* pas évident que les deux cas que l'on a séparés recouvrent tous les possibles ; en effet, il se pourrait très bien, à première vue, que $\phi(\mathfrak{M}^{(n)}_{\nu_n,D})$ soit inclus dans $\mathfrak{M}^{(n)}_{\nu',D}$ sans pour autant que $\phi(\mathfrak{M}^{(n)}_{\nu',D})$ le soit. Toutefois, d'après le lemme 2.17 ci-après, cela ne peut se produire.

Avec ce qui a été rappelé au §2.3.1, une récurrence immédiate montre que, tant qu'il est bien défini, le module $\mathfrak{M}^{(n)}_{\nu_n,N}$ admet une base sur $\mathfrak{S}_{\nu_n,N}$ composée de vecteurs de la forme $\varpi_N^{-b_i^{(n)}} B_i^{(n)}$ où les $b_i^{(n)}$ sont des entiers, les $B_i^{(n)}$ appartiennent à $\mathcal{E}^+_{\nu_n} \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu^{\text{G-L}}$ et où on rappelle que $\varpi_N \in \bar{K}$ est un élément vérifiant $\varpi_N^N = p$.

Lemme 2.17. *On conserve les notations précédentes. Soit n est un entier pour lequel $\mathfrak{M}^{(n)}_{\nu_n,N}$ est défini. Alors le module $\mathfrak{M}^{(n)}_{\nu',D}$ est libre sur $\mathfrak{S}_{\nu',D}$ et admet pour base la famille des $\varpi_D^{-a_i^{(n)}} B_i^{(n)}$ $(1 \leqslant i \leqslant d)$ où $a_i^{(n)}$ désigne la partie entière de $\frac{D}{N}\, b_i^{(n)}$.*

En particulier, $\mathfrak{M}^{(n)}_{\nu_n,D}$ engendre $\mathfrak{M}^{(n)}_{\nu',D}$ comme $\mathfrak{S}_{\nu',D}$-module.

Démonstration. Pour la première assertion, il s'agit de montrer que si b est un entier, alors $\varpi_N^{-b}\mathfrak{S}_{\nu',N} \cap \mathcal{E}^+_{\nu',D} = \varpi_D^{-a}\mathfrak{S}_{\nu',D}$ où a est la partie entière de $\frac{bD}{N}$. Or, si un élément $x = \sum_{i\in\mathbb{N}} a_i u^i$ appartient à cette intersection, on doit avoir $\mathrm{val}(a_i) \in \frac{1}{D}\mathbb{Z}$ et $\mathrm{val}(a_i) \geqslant \nu' i - \frac{b}{N}$ pour tout i. Le produit $D \cdot \mathrm{val}(a_i)$ doit alors être un entier $\geqslant D\nu' i - \frac{bD}{N}$. Comme on a supposé que D est un dénominateur de ν', on en déduit que $D\nu' i$ est entier, puis que $D \cdot \mathrm{val}(a_i) \geqslant D\nu' i - a$. Cela signifie exactement que $x \in \varpi_D^{-a}\mathfrak{S}_{\nu',D}$.

La seconde assertion est maintenant claire puisque, d'une part, $\mathfrak{M}^{(n)}_{\nu_n,D} \subset \mathfrak{M}^{(n)}_{\nu',D}$ et, d'autre part, tous les $\varpi_D^{b_i^{(n)}} B_i^{(n)}$ sont éléments de $\mathfrak{M}^{(n)}_{\nu_n,D}$. □

Lemme 2.18. *Le processus itératif que l'on a défini précédemment prend fin au plus au bout de $c_{\text{G-L}} \cdot dD$ étapes.*

Remarque 2.19. *La borne ci-dessus peut paraître bien pâle par rapport à ce que nous avions prouvé dans le cas d'école « $\nu = 0$ » (voir lemme 2.15). Toutefois, nous n'avons pas réussi à adapter la démonstration de ce lemme à cette nouvelle situation ; de nombreux problèmes se posent et, en particulier, celui de la non-stabilité de $\mathfrak{S}_{\nu',D}[(\frac{u}{\varpi_D^{D\nu'}})^{-1}]$ par ϕ. Pire encore, des simulations numériques montrent qu'il n'est pas vrai que, dans le cas $\nu > 0$, le processus prend nécessairement fin en moins de d étapes ; toutefois, la borne donnée par le lemme 2.18 ne nous paraît pas optimale.*

Démonstration. Soit ℓ le plus grand entier tel que $\mathfrak{M}^{(\ell)}_{\nu',D}$ soit défini. On veut démontrer que $\ell \leqslant c_{\text{G-L}} \cdot dD$. Pour cela, on va mettre à profit la suite d'inclusions suivante :

$$\mathfrak{M}^{(0)}_{\nu',D} \subsetneq \mathfrak{M}^{(1)}_{\nu',D} \subsetneq \mathfrak{M}^{(2)}_{\nu',D} \subsetneq \cdots \subsetneq \cdots \subsetneq \mathfrak{M}^{(\ell)}_{\nu',D} \subset p^{-c_{\text{G-L}}}\, \mathfrak{M}^{(0)}_{\nu',D}$$

qui, après passage au déterminant, donne une suite d'inclusions analogue sur les $\Lambda^d\, \mathfrak{M}^{(n)}_{\nu',D}$ sauf que le coefficient $p^{-c_{\text{G-L}}}$ est remplacé par $p^{-dc_{\text{G-L}}}$ dans le dernier module. Soit x une base de $p^{-dc_{\text{G-L}}}\, \Lambda^d\, \mathfrak{M}^{(0)}_{\nu',D}$ sur $\mathfrak{S}_{\nu',D}$, et soient $s_1, \ldots, s_\ell$ des éléments de $\mathfrak{S}_{\nu',D}$ tels que $s_n x$ soit une base de $\Lambda^d\, \mathfrak{M}^{(n)}_{\nu'}$. On a alors $s_0 = p^{c_{\text{G-L}} \cdot d} = \varpi_D^{c_{\text{G-L}} \cdot dD}$ et s_{n+1} divise s_n pour tout $n \in \{0, \ldots, \ell - 1\}$. Or ϖ_D engendre un idéal premier dans $\mathfrak{S}_{\nu',D}$. Il en résulte qu'à multiplication par des éléments inversibles près, tous les s_n sont des puissances de ϖ_D. Les exposants qui apparaissent forment une

suite d'entiers strictement décroissante qui commence à $c_{\text{G-L}} \cdot dD$ et se termine à 0. Clairement, sa longueur est donc majorée par $c_{\text{G-L}} \cdot dD + 1$. □

Ainsi, si l'on choisit N supérieur ou égal à $\frac{2c\, c_{\text{G-L}} \cdot dD}{\nu' - \nu}$, on a $\nu_n \leqslant \nu'$ pour tout $n \leqslant c_{\text{G-L}} \cdot dD$, et le lemme ci-dessus implique que le processus itératif que l'on a défini précédemment ne peut s'arrêter en raison d'une violation de l'inégalité $\nu_n \leqslant \nu'$. Autrement dit, il s'arrête nécessairement lorsque l'on a trouvé un $\mathfrak{M}^{(n)}_{\nu',D}$ stable par ϕ.

L'algorithme proprement dit Le procédé itératif précédent peut, sans problème, être transformé en un véritable algorithme qui calcule la matrice donnant l'action de ϕ sur $\mathfrak{M}^{(n)}_{\nu_n,N}$ et s'arrête lorsque $\mathfrak{M}^{(n)}_{\nu',D}$ est stable par ϕ. En effet, du fait que $\mathfrak{M}^{(0)}_{\nu,N}$ est stable par $p^{-c} \cdot \phi$, on déduit que l'on peut utiliser l'algorithme 4 pour calculer l'action de ϕ sur $\mathfrak{M}^{(1)}_{\nu_1,N}$ et, en examinant cet algorithme, on montre que $\mathfrak{M}^{(1)}_{\nu_1,N}$ est, lui aussi, stable par $p^{-c} \cdot \phi$. On peut ainsi itérer le procédé et calculer, comme annoncé, l'action de ϕ sur chacun des $\mathfrak{M}^{(n)}_{\nu_n,D}$. Comme en outre, le processus précédent prend fin au bout d'au plus $c_{\text{G-L}} \cdot dD$ étapes (par le lemme 2.18), la pente ν se dépasse jamais la valeur critique ν'.

Par ailleurs, pour tester la stabilité de $\mathfrak{M}^{(n)}_{\nu',D}$, on peut procéder comme suit : (1) à partir du lemme 2.17 et la matrice donnant l'action de ϕ sur $\mathfrak{M}^{(n)}_{\nu_n,N}$ calculée précedemment, on détermine la matrice de l'action de ϕ sur $\mathfrak{M}^{(n)}_{\nu',D}$ et (2) on vérifie que cette matrice est à coefficients dans $\mathfrak{S}_{\nu'}$ ce qu'il est possible de tester en ne regardant que les termes en u^i pour $i < N$ étant donné que $\nu' \geqslant \nu_n + \frac{c}{N}$[12],

L'algorithme 5 résume, de façon concise ce que l'on vient de dire.

Remarque 2.20. *Dans la remarque 2.16, nous avions présenté une idée permettant, semble-t-il, d'aboutir à une convergence beaucoup plus rapide vers la solution et consistant à itérer non pas l'opérateur ϕ lui-même mais ses puissances. Toutefois, lorsque l'on essaie de l'appliquer à notre situation précise, on se heurte à un certain nombre de difficultés que les auteurs de l'article n'ont pas réussi à surmonter. Le souci majeur est que la « construction* Max *» ne commute pas avec les sommes lorsque les pentes changent.*

2.3.4 La liberté rendue

À ce niveau, on a réussi à calculer un d-uplet d'entiers $a = (a_1, \dots, a_d)$ et une matrice `PhiBK` à coefficients dans $\mathfrak{S}_\nu$ pour lesquels on est assuré qu'il existe une $\mathcal{E}^+_{\nu'}$-base $(e_1, \dots, e_d)$ de $\mathfrak{D}_{\nu'} = \mathcal{E}^+_{\nu'} \otimes_{\mathcal{E}^+} \mathfrak{D}$ (où on rappelle que $\mathfrak{D}$ désigne le module de Breuil–Kisin sur $\mathcal{E}^+$ associé au (ϕ, N)-module filtré D avec lequel on est parti) telle que `PhiBK` soit la matrice de ϕ dans la base $(\varpi_D^{-a_1} e_1, \dots, \varpi_D^{-a_d} e_d)$. En particulier, l'espace

$$\mathfrak{M}_{\nu',D} = \mathfrak{S}_{\nu',D} \varpi_D^{-a_1} e_1 \oplus \cdots \oplus \mathfrak{S}_{\nu',D} \varpi_D^{-a_d} e_d$$

est stable par ϕ. Toutefois, pour obtenir un module de Breuil–Kisin, on ne souhaite pas un espace défini sur $\mathfrak{S}_{\nu',D}$ mais, bel et bien, un module *libre* défini sur $\mathfrak{S}_{\nu'}$. Il reste donc encore à redescendre $\mathfrak{M}_{\nu',D}$ en un $\mathfrak{S}_{\nu'}$-module et, pour cela, il est naturel de considérer l'intersection $\mathfrak{M}_{\nu'} = \mathfrak{M}_{\nu',D} \cap \mathfrak{D}$

[12] Cela pourrait éventuellement ne pas se produire si $n = c_{\text{G-L}} \cdot dD$. Mais, dans ce cas[13], la borne du lemme 2.18 apporte la garantie que $\mathfrak{M}^{(n)}_{\nu',D}$ est automatiquement stable par ϕ et on peut donc se dispenser de faire le test.

[13] En fait, ce cas ne se produit jamais. En effet, toujours d'après le lemme 2.18, si l'on arrive à calculer $\mathfrak{M}^{(n)}_{\nu',D}$ pour $n = cdD$, nécessairement $\mathfrak{M}^{(n)}_{\nu'} = p^{-c}\, \mathfrak{M}^{(0)}_{\nu',D}$ et celui-ci est stable par ϕ. Ainsi $\mathfrak{M}^{(0)}_{\nu,D'}$ serait lui aussi stable par ϕ et on n'aurait dû s'arrêter avant même la première itération.

Algorithme 5: ITERATIONFROBENIUS$(\nu, \nu', \texttt{PhiBK}, c)$

Entrée : : $\star$ des nombres rationnels $0 < \nu < \nu'$

: $\star$ une matrice $\texttt{PhiBK} \in M_d(\mathcal{E}_\nu^+)$

: donnant l'action, dans la base canonique, d'un opérateur ϕ-semi-linéaire ϕ sur $(\mathcal{E}_\nu^+)^d$

: $\star$ une constante $c \geqslant 0$ telle que $p^c \cdot \texttt{PhiBK} \in M_d(\mathfrak{S}_\nu)$

: $\star$ une constante $c_{\text{G-L}} \geqslant 0$ telle qu'il existe

: un module de Breuil–Kisin $\mathfrak{M}_\nu$ compris entre $p^{-c}\,(\mathcal{E}_\nu^+)^d$ et $(\mathcal{E}_\nu^+)^d$

Sortie : : $\star$ la matrice de ϕ agissant sur un module de Breuil–Kisin $\mathfrak{M}_{\nu'}$ sur $\mathfrak{S}_{\nu'}$

: tel que $p^{-c}\,\mathfrak{S}_{\nu'}^d \subset \mathfrak{M}_{\nu'} \subset \mathfrak{S}_{\nu'}^d$

$D \leftarrow$ un dénominateur de ν';
$N \leftarrow$ plus petit multiple de D supérieur ou égal à $\frac{c_{\text{G-L}} \cdot dD}{\nu' - \nu}$;
$a \leftarrow (0, \dots, 0)$; $b \leftarrow (0, \dots, 0)$;
tant que *il existe* (i, j) *tel que* $D \cdot v_\nu(\texttt{PhiBK}[i, j]) < a[j] - a[i]$ **faire**
  $(i, j) \leftarrow$ un tel couple;
  $b, \texttt{PhiBK} \leftarrow$ CHANGEBASE$(b, \texttt{PhiBK}, \frac{N}{D} a[j], \texttt{PhiBK}[\cdot, j], c, N, \nu)$;
  pour i *allant de* 1 *à* d **faire** $a[i] \leftarrow \text{Floor}(\frac{b[i]D}{N})$;
  $\nu \leftarrow \nu + \frac{c}{N}$;
retourner $a, \texttt{PhiBK}$;

qui est à l'évidence, elle aussi, stable par ϕ. Par contre, *a priori*, rien n'indique qu'elle est libre. Toutefois si $\nu' = \frac{1}{D}$ — ce que l'on supposera à partir de maintenant — on sait (voir les rappels du §2.3.1) que cette intersection est engendrée par les vecteurs $p^{q_i+1} e_i$ et $p^{q_i} u^{r_i} e_i$ ($1 \leqslant i \leqslant d$) où q_i et r_i désignent respectivement le quotient et le reste de la division euclidienne de $-a_i$ par D. Or, on peut manifestement écrire :

$$p^{q_i} u^{r_i} = p^{q_i+1} \cdot \frac{u^{r_i}}{p} \in p^{q_i+1} \mathfrak{S}_{1/r_i}$$

ce qui prouve que si ν'' est supérieur ou égal à ν' et à tous les $\frac{1}{r_i}$ dès que $r_i \neq 0$, alors le module $\mathfrak{M}_{\nu''} = \mathfrak{S}_{\nu''} \otimes_{\mathfrak{S}_{\nu'}} \mathfrak{M}_{\nu'}$ est libre sur $\mathfrak{S}_{\nu''}$ et admet pour base la famille des $u^{q_i+\varepsilon_i} e_i$ où ε_i vaut 0 si $r_i = 0$ et 1 sinon. Toutefois, cela n'est pas encore satisfaisant car si l'un des r_i vaut 1, l'argument précédent nous oblige à choisir un $\nu'' \geqslant 1$ et l'on ne peut alors plus appliquer le théorème de surconvergence des modules de Breuil–Kisin. Il faudrait donc pouvoir réussir à s'assurer que tous les restes r_i non nuls sont suffisamment grands ; c'est, en quelque sorte, le contenu du lemme suivant.

Lemme 2.21. *Il existe un entier t tel que, pour tout $i \in \{1, \dots, d\}$, le reste de la division euclidienne de $-(t + a_i)$ par D soit égal à 0 ou $\geqslant \frac{D}{d}$.*

Démonstration. On note $\rho_1 < \cdots < \rho_d$ les restes des divisions euclidiennes des $-a_i$ par D rangés par ordre croissant et on pose $\rho_{d+1} = \rho_1 + D$. Il est alors clair qu'il existe un i tel que $\rho_{i+1} \geqslant \rho_i + \frac{D}{d}$ et l'entier $t = \rho_i$ vérifie la propriété du lemme. □

Soit t un entier satisfaisant la condition du lemme. Si on remplace le d-uplet a par $t + a = (t + a_1, \dots, t + a_d)$, le module $\mathfrak{M}_{\nu',D}$ est remplacé par $\varpi_D^{-t} \mathfrak{M}_{\nu',D}$ et reste donc stable par ϕ. Il en

va donc de même de $\mathfrak{M}_{\nu'}$ et de $\mathfrak{M}_{\nu''}$ et, comme précédemment, ce dernier est libre sur $\mathfrak{S}_{\nu''}$. La différence est que, maintenant, grâce à la modification que l'on a faite, on peut choisir $\nu'' = d\nu'$.

Pour conclure, il reste encore à vérifier que $\mathfrak{M}_{\nu''}$ est bien un module de Breuil–Kisin, c'est-à-dire qu'il est bien de hauteur finie. Cela se fait simplement en reprenant la première partie de la démonstration de la proposition 2.14 : on obtient[14], ce faisant, que $\mathfrak{M}_{\nu''}$ est de hauteur $\leqslant dr$. Ainsi si ν'' est strictement inférieur à $\frac{p-1}{perd}$, le théorème de surconvergence des modules de Breuil–Kisin s'applique et affirme que le $\mathfrak{M}_{\nu''}$ que l'on vient de calculer provient par extension des scalaires d'un module de Breuil–Kisin $\mathfrak{M}$ sur $\mathfrak{S}$. En particulier, $\mathfrak{M}_{\nu''}$ correspond bien à un réseau stable par G_∞ dans la représentation semi-stable associée à au (ϕ, N)-module filtré D duquel on est parti !

2.3.5 L'algorithme sous forme synthétique

On rappelle qu'à l'issue de l'étape 1 (*cf* §2.2), on a calculé :

(i) une matrice `PhiBK` connue à précision u-adique u^N donnant l'action du Frobenius ϕ sur le module de Breuil–Kisin $\mathfrak{D}_\nu$;

(ii) une constante c tel que $p^c \cdot$ `PhiBK` soit à coefficients dans $\mathfrak{S}_\nu$;

(iii) une constante $c_\nu = c_{\text{G-L}}$ pour laquelle on a la garantie qu'il existe un module de Breuil–Kisin $\mathfrak{M}_\nu$ de hauteur $\leqslant r$ compris entre $\mathfrak{M}_\nu^{\text{G-L}}$ et $p^{-c} \cdot \mathfrak{M}_\nu^{\text{G-L}}$ sachant que $\mathfrak{M}_\nu^{\text{G-L}}$ désigne le $\mathfrak{S}_\nu$-module ayant pour base celle dans laquelle est écrite la matrice `PhiBK`.

Les paramètres N et ν qui sont apparus ci-dessus sont respectivement un entier strictement positif et un nombre rationnel strictement positif qui peuvent être choisis comme on le souhaite. Dans la suite, conformément aux contraintes qui ont été dégagées précédemment, on choisira un entier D strictement supérieur à $\frac{perd^2}{p-1}$ et on prendra :

$$N = 4c\, c_{\text{G-L}} \cdot D^2 \quad \text{et} \quad \nu = \frac{1}{2D}. \tag{22}$$

On posera également $\nu' = \frac{1}{D} = 2\nu$. Dans les numéros précédents, nous avons présenté une méthode algorithmique pour calculer la matrice donnant l'action de ϕ sur un module de Breuil–Kisin $\mathfrak{M}_\nu$ satisfaisant à la condition de l'alinéa (iii) ci-dessus, qui peut se résumer ainsi :

(1) Appliquer l'algorithme 5 avec les paramètres précédents et noter a, `PhiBK` le couple renvoyé

(2) Appliquer l'algorithme 6 ci-après.

La matrice `PhiBK` renvoyée par l'algorithme 6 est la matrice de l'action de ϕ sur un module de Breuil–Kisin $\mathfrak{M}_{d\nu'}$ de hauteur $\leqslant rd$. Comme en outre, par notre choix de ν', on a $d\nu' < \frac{p-1}{perd}$, le théorème de surconvergence des modules de Kisin s'applique.

Étant donné que l'algorithme 4 n'effectue des divisions euclidiennes qu'entre éléments de $\mathcal{E}_\nu^+$ (pour différents ν) qui sont des polynômes, il est en outre facile d'analyser les pertes de précision p-adiques engendrées par la méthode ci-dessus : on trouve que si les coefficients de la matrice `PhiBK` initiale sont connus modulo $(p^M\, \mathfrak{S}_\nu + u^N\, \mathfrak{S}_\nu)$, alors ceux de la matrice `PhiBK` calculée sont connus au pire modulo $(p^{M-2}\, \mathfrak{S}_{\nu''} + u^N\, \mathfrak{S}_{\nu''})$. En effet, on remarque dans un premier temps que l'algorithme 4 n'entraîne aucune perte de précision, dans le sens où si les coefficients de

$$\varpi_N^{-a} X \quad \text{et} \quad \Delta(b,N)^{-1} \cdot \texttt{PhiBK} \cdot \Delta(b,N) \quad \text{avec} \quad \Delta(b,N) = \text{Diag}(\varpi_N^{b_1}, \dots, \varpi_N^{b_d})$$

[14] Nous n'avons pas réussi à adapter la deuxième partie de la preuve ; nous ne savons donc pas si $\mathfrak{M}_{\nu''}$ est nécessairement de hauteur $\leqslant r$. Pouvoir montrer cela améliorerait la complexité finale de l'algorithme.

Algorithme 6: LIBERTE$(a, \texttt{PhiBK})$

// On calcule un entier t vérifiant la condition du lemme 2.21
$(\rho_1, \dots, \rho_d) \leftarrow$ restes des divisions euclidiennes de $-a_i$ par D triés par ordre croissant;
pour *i allant de 1 à $d-1$* **faire**
  si $\rho_{i+1} \geqslant \rho_i + \frac{D}{d}$ **alors** $t \leftarrow \rho_i$; **break**;
// On calcule la matrice PhiBK *de ϕ agissant sur $\mathfrak{M}_{\nu''}$*
pour *i allant de 1 à d* **faire**
  $(q_i, r_i) \leftarrow$ quotient et reste de la division euclidienne de $-(a_i + t)$ par D;
  si $r_i > 0$ **alors** $q_i \leftarrow q_i + 1$;
$D \leftarrow$ la matrice diagonale dont les éléments diagonaux sont $p^{q_1}, \dots, p^{q_d}$;
$\texttt{PhiBK} \leftarrow D \cdot \texttt{PhiBK} \cdot D^{-1}$;
retourner PhiBK

calculées à partir des entrées sont connus modulo $(p^M \mathfrak{S}_\nu + u^N \mathfrak{S}_\nu)$, alors ceux de la matrice $\Delta(b,N)^{-1} \cdot \texttt{PhiBK} \cdot \Delta(b,N)$ calculée à partir de la sortie sont connus modulo $(p^M \mathfrak{S}_{\nu'} + u^N \mathfrak{S}_{\nu'})$ où, dans cette phrase et dans cette phrase uniquement, ν et ν' désignent les rationnels pris en entrée par l'algorithme 4. Il résulte de ceci que les coefficients de la matrice $\Delta(a,D)^{-1} \cdot \texttt{PhiBK} \cdot \Delta(a,D)$ calculée à partir de la sortie de l'algorithme 5 sont connus modulo $(p^M \mathfrak{S}_{\nu'} + u^N \mathfrak{S}_{\nu'})$ avec, cette fois-ci, à nouveau, $\nu' = \frac{1}{D}$. On en déduit enfin la propriété annoncée en remarquant que les q_i calculés dans l'algorithme 6 diffèrent d'au plus 1 des $\frac{-a_i}{D}$.

2.4 Étape 3 : Réduction modulo p et semi-simplification

À l'issue de l'étape précédente, nous avons calculé $\mathfrak{M}_{\nu''} = \mathfrak{S}_{\nu''} \otimes_{\mathfrak{S}} \mathfrak{M}$ pour un certain nombre rationnel $\nu'' < \frac{perd}{p-1}$. Le théorème de surconvergence des modules des modules de Breuil–Kisin nous assure que cela est suffisant pour retrouver $\mathfrak{M}$. Toutefois, bien que la démonstration de ce théorème soit assez constructive, il n'est pas aisé, dans la pratique, de calculer $\mathfrak{M}$ à partir de $\mathfrak{M}_{\nu''}$. Par chance, nous n'en avons pas besoin ! En effet, en se rappelant de surcroît que $\nu'' = \frac{1}{dD}$ est l'inverse d'un nombre entier, l'égalité $\mathfrak{M}_{\nu''} = \mathfrak{S}_{\nu''} \otimes_{\mathfrak{S}} \mathfrak{M}$ montre que la connaissance de $\mathfrak{M}_{\nu''}$ suffit à déterminer le quotient

$$\mathfrak{M}/(p\mathfrak{M} + u^{1/\nu''}\mathfrak{M}) \simeq \mathfrak{M}_{\nu''}/(p\,\mathfrak{M}_{\nu''} + u^{1/\nu''}\mathfrak{M}_{\nu''}).$$

Or, étant donné que $\frac{1}{\nu''} = dD \geqslant \frac{perd}{p-1}$, il est facile de démontrer par ailleurs (voir par exemple lemme 5 de [7]) que deux modules de Breuil–Kisin de hauteur $\leqslant rd$ sur $\mathfrak{S}/p\mathfrak{S} \simeq k[[u]]$ qui deviennent égaux après réduction modulo $u^{1/\nu''}$ sont isomorphes. Ainsi, en pratique, connaissant $\mathfrak{M}_{\nu''}$, il suffit de réduire ce module modulo $(p, u^{1/\nu''})$ puis de le relever n'importe comment sur $k[[u]]$.

À partir de là, calculer la semi-simplifiée de la représentation associée fait l'objet du chapitre 3 de la thèse de Le Borgne [16]. Nous ne nous attarderons donc pas davantage sur ce point et nous contentons de renvoyer le lecteur à cette référence.

2.5 Étude de la complexité

Nous terminons cette section par une étude sommaire de la complexité de l'algorithme que nous venons de présenter. Nous nous proposons, plus précisément, de montrer que celle-ci est polynômiale en tous les paramètres pertinents du problème, qui sont :

- l'entier e qui est l'indice de ramification absolue de K ;
- l'entier f qui est le degré de k (que l'on suppose fini, on rappelle) sur son sous-corps premier $\mathbb{F}_p$;
- la valuation p-adique de la différente de K/K_0, notée δ ;
- l'entier r qui correspond (quitte à twister correctement V) à la différence entre les deux poids de Hodge-Tate extrèmes de V.

Avant de poursuivre, remarquons que, d'après les précisions qui ont été faites au §2.1 sur la représentation des éléments, la complexité des opérations arithmétiques élémentaires — à savoir l'addition, la soustraction et la multiplication — dans les anneaux $\mathcal{O}_{K_0} \simeq \mathbb{Z}_q$, $\mathcal{O}_K$, $K_0 \simeq \mathbb{Q}_q$, K, $\mathfrak{S}_\nu$ et $\mathcal{E}_\nu^+$ est polynômiale en la taille de l'entrée, et même quasi-linéaire[15] si on utilise des algorithmes basées sur la transformée de Fourier rapide. Ceci vaut également pour la division euclidienne dans $\mathfrak{S}_\nu$; on renvoie le lecteur aux §§2.3 et 4.2 de [11] à ce propos.

2.5.1 Coût de l'algorithme CHANGEBASE

L'algorithme CHANGEBASE (algorithme 4, page 32) joue un rôle essentiel dans la deuxième étape de notre algorithme. Dans cette partie, nous étudions sa complexité. On note M un entier pour lequel tous les coefficients des matrices

$$\varpi_N^{-a} X \quad \text{et} \quad \Delta(b,N)^{-1} \cdot \texttt{PhiBK} \cdot \Delta(b,N) \quad \text{avec} \quad \Delta(b,N) = \text{Diag}(\varpi_N^{b_1}, \ldots, \varpi_N^{b_d})$$

sont connus modulo $p^M \cdot \mathfrak{S}_\nu$ ou, ce qui revient au même, un entier qui majore tous les N_i de la représentation PAG (voir §2.1) des coefficients des matrices ci-dessus.

Le calcul de la division euclidienne de la ligne 8 se fait en temps polynômial en $N(M+c)$; en effet, la représentation PAG des éléments $X[i]$ et $X[j]$ que l'on divise entre eux ont une taille qui ne dépasse pas $O(N(M+c))$. Il est alors clair que chaque exécution de la boucle *tant que* (lignes 3 à 11) prend aussi un temps polynômial en $N(M+c)$.

Il ne reste donc plus qu'à majorer le nombre d'exécutions de cette boucle. Pour cela, on considère le triplet $(-v, \delta, n)$ où :

- v désigne le minimum des $v_{\nu'}(X[i]) + b_i$ pour i variant dans $\{1, \ldots, d\}$,
- δ désigne le maximum des $\deg_{\nu'}(X[i])$ pour i parcourant les indices tels que $v_{\nu'}(X[i]) + b_i = v$,
- n désigne le nombre d'indices i tels que $v = v_{\nu'}(X[i]) + b_i$ et $d = \deg_{\nu'}(X[i])$

et on remarque qu'à chaque itération de la boucle, celui-ci diminue strictement pour l'ordre lexicographique donnant le poids le plus fort à la première coordonnée. En effet, on constate tout d'abord que v ne peut qu'augmenter, et donc $-v$ ne peut que diminuer. De plus, en reprenant les notations de l'algorithme, on s'aperçoit que si le minimum des $v_{\nu'}(X[i]) + b_i$ est atteint pour un unique indice i, alors b_i augmente strictement à la ligne 5 et, par suite, que v augmente strictement dans ce cas. Si le minimum des $v_{\nu'}(X[i]) + b_i$ est atteint pour au moins deux indices i et j, c'est-à-dire si $v_i = v_j$, on s'arrange à la ligne 7 pour que $\deg_{\nu'}(X[i]) \geqslant \deg_{\nu'}(X[j])$ puis on remplace à la ligne 9 le coefficient $X[i]$ par le reste de sa division euclidienne par $X[j]$, faisant ainsi chuter son degré de Weierstrass à un entier $< \deg_{\nu'}(X[j])$. Ainsi, en supposant que v n'augmente pas,

[15] Au moins, dans la cas des éléments de $\mathfrak{S}_\nu$ et $\mathcal{E}_\nu^+$, si l'on suppose que les coeffcients des séries à multiplier sont tous connus avec à peu près la même précision.

si $X[i]$ et $X[j]$ avait même degré de Weierstrass, le nombre δ reste inchangé alors que n diminue tandis que si on avait $\deg_{\nu'}(X[i]) > \deg_{\nu'}(X[j])$, le nombre δ diminue. Dans tous les cas, le triplet $(-v, d, n)$ diminue donc strictement pour l'ordre lexicographique.

Pour conclure, il suffit de majorer le nombre de valeurs distinctes que peut prendre le triplet $(-v, d, n)$. La coordonnée d (resp. n) est un entier qui varie entre 0 et $N-1$ (resp. entre 1 et d) ; elle peut donc prendre N (resp. d) valeurs. Le nombre v, quant à lui, est un rationnel dont le dénominateur est divisible par le dénominateur de ν, à savoir N. Par ailleurs, il ne peut descendre en dessous de $-a$ (c'est la condition d'arrêt de l'algorithme) et, par définition de l'entier c, il ne peut excéder $c-a$. Ainsi, il varie dans un ensemble de cardinal cN. En mettant tout ensemble, on en déduit que le triplet $(-v, d, n)$ prend au maximum $N^2 \cdot cd$ valeurs et, par suite, que la boucle *tant que* de l'algorithme 4 est exécutée au maximum $N^2 \cdot cd$.

Il résulte de ce qui précède que la complexité de l'algorithme 4 est polynômiale en les paramètres N, M, c, d et, également, e et f qui contrôlent la « taille » de K.

2.5.2 Examen de la précision p-adique

Avant de pouvoir conclure, il nous reste à estimer la précision p-adique avec laquelle l'entrée de notre algorithme — c'est-à-dire le (ϕ, N)-module filtré D de départ donné, on le rappelle, par le quadruplet $(\texttt{Phi}, \texttt{N}, \texttt{H}, \texttt{F})$ — doit être connue pour que tout le calcul puisse fonctionner correctement.

À cet effet, on remarque qu'à l'entrée de la troisième étape, le module $\mathfrak{M}_{\nu''}$ que l'on a calculé est réduit modulo $(p\,\mathfrak{M}_{\nu''} + u^{1/\nu''}\,\mathfrak{M}_{\nu''})$. Ainsi, il suffit de connaître les coordonnées de la matrice PhiBK donnant l'action de ϕ sur $\mathfrak{M}_{\nu''}$ modulo $(p\,\mathfrak{S}_{\nu''} + u^N\,\mathfrak{S}_{\nu''})$ car $N \geqslant \frac{1}{\nu''}$. Ainsi, l'entier M du §2.3.5 peut être choisi égal à 3 étant donné que l'on a vu que le résultat calculé à l'issue de l'étape 2 est connu modulo $(p^{M-2}\,\mathfrak{S}_{\nu''} + u^N\,\mathfrak{S}_{\nu''})$. On en déduit que l'entier M du §2.2.4, c'est-à-dire la précision de l'entrée que l'on cherche à évaluer, peut être choisi égal $M_0 + 3$ où M_0 est le nombre qui a été défini au §2.2.4. En particulier, il résulte de la formule (19) que M_0 dépend de façon polynômiale des paramètres d, r et $\log_p(\frac{1}{\nu})$. En outre, d'après la formule (22), la quantité $\frac{1}{\nu}$ est contrôlée polynomialement par les paramètres c, $c_{\text{G-L}}$, e, r et d. Or, dans l'introduction du §2.3, on a vu que c et $c_{\text{G-L}}$ sont eux-mêmes controlés polynomialement par e, r, d et δ (qui désigne, on rappelle, la valuation p-adique de la différente de K à K_0). On trouve ainsi que M_0, et donc également $M_0 + 3$, est inférieur à un certain polynôme dépendant des variables e, r, d et δ.

2.5.3 Un algorithme de complexité polynômiale

À la lumière de ce qui précède, il n'est pas difficile de conclure que l'algorithme de calcul de la semi-simplifiée modulo p que nous avons présenté dans cet article a une complexité polynômiale en e, f, r, d et δ. En effet, revenant à la synthèse du §2.2.4, on démontre immédiatement que l'étape 1 de notre algorithme a une complexité polynômiale en e, f, r, d, N, $n \approx \log_p(\frac{1}{\nu})$ et M_0 et donc, d'après les dépendances qui ont été explicitées ci-dessus, a également une complexité polynômiale en e, f, r, d et δ. De manière similaire, en étudiant la synthèse du §2.3.5, on obtient une complexité polynômiale en e, f, r, d et δ pour l'étape 2 de notre algorithme. Enfin, les résultats de §III.2.5.2 de [16] montrent que l'étape 3 de notre algorithme a également une complexité polynômiale en e, f, r et d. Mettant tout ensemble, on conclut.

Références

[1] L. Berger, H. Li, H. J. Zhu, *Construction of some families of 2-dimensional crystalline representations*, Math. Ann. **329** (2004), 365–377.

[2] C. Breuil, *Schémas en groupes et corps des normes*, prépublication (1998), `http://www.math.u-psud.fr/~breuil/PUBLICATIONS/groupesnormes.pdf`

[3] C. Breuil, *Une application du corps des normes*, Compositio Math. **117** (1999), 189–203

[4] C. Breuil *Sur quelques representations modulaires et p-adiques de $GL_2(\mathbb{Q}_p)$, II*, J. Inst. Math. Jussieu **2** (2003), p. 23–58

[5] C. Breuil, A. Mézard, *Multiplicités modulaires et représentations de $GL_2(\mathbb{Z}_p)$ et de* Gal $(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en $\ell = p$*, Duke Math. J. **115** (2002), 205–310

[6] K. Buzzard, T. Gee *Explicit reduction modulo p of certain two-dimensional crystalline representations*, Int. Math. Res. Not. **12** (2009), 2303–2317

[7] X. Caruso, *Sur la classification de quelques φ-modules simples*, Mosc. Math. J. **9** (2009), 562–568

[8] X. Caruso, *Représentations galoisiennes p-adiques et (φ, τ)-modules*, prépublication (2010)

[9] X. Caruso, *Random matrices over a DVR and LU factorization*, prépublication (2012)

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

[11] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, prépublication (2012)

[12] P. Colmez, J.-M. Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), 1–43

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

[14] A. Génestier, V. Lafforgue, *Structures de Hodge-Pink pour les $\varphi/\mathfrak{S}$-modules de Breuil et Kisin*, à paraître à Compositio Math.

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

[16] J. Le Borgne, *Représentations galoisiennes et φ-modules : aspects algorithmiques* thèse de doctorat (2012)

[17] D. Savitt, *On a Conjecture of Conrad, Diamond, and Taylor*, Duke Math. J. **128** (2005), no. 1, 141-197

[18] M. Vienney, *Constructions de (φ, Γ)-modules en caractéristique p*, thèse (2012)

[19] G. Yamashita, S. Yasuda, *Reduction of two dimensional crystalline representations and Hypergeometric polynomials*, en préparation.