CONSTRUCTION OF SOME FAMILIES OF 2-DIMENSIONAL CRYSTALLINE REPRESENTATIONS

by

Laurent Berger, Hanfeng Li & Hui June Zhu

Abstract. — We construct explicitly some analytic families of étale (φ,Γ)-modules, which give rise to analytic families of 2-dimensional crystalline representations. As an application of our constructions, we verify some conjectures of Breuil on the reduction modulo p of those representations, and extend some results (of Deligne, Edixhoven, Fontaine and Serre) on the representations arising from modular forms.

Résumé. — Nous construisons explicitement des familles analytiques de (φ,Γ)-modules étales, qui donnent lieu à des familles analytiques de représentations cristallines de dimension 2. Comme application de nos constructions, nous vérifions des conjectures de Breuil quant à la réduction modulo p de ces représentations, et nous étendons des résultats (de Deligne, Edixhoven, Fontaine et Serre) sur les représentations associées aux formes modulaires.

Contents

1. Introduction

Throughout this article p is a prime number and $\overline{\mathbf{Q}}_p$ is an algebraic closure of $\mathbf{Q}_p$. We are interested in p-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and we use the language of crystalline representations (see for example [**Fo88b**]).

2000 ***Mathematics Subject Classification.*** — 11F80, 11F33, 11F85, 14F30.

1.1. Main results. — The purpose of this article is to construct some explicit analytic families of 2-dimensional crystalline representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. More precisely, let $k \geqslant 2$ and for $a_p \in \mathfrak{m}_E$ (where $\mathfrak{m}_E$ is the maximal ideal of the ring of integers of a finite extension $E \subset \overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$) let D_{k,a_p} be the filtered φ-module given by $D_{k,a_p} = Ee_1 \oplus Ee_2$ where:

$$\begin{cases} \varphi(e_1) = p^{k-1}e_2 \\ \varphi(e_2) = -e_1 + a_p e_2 \end{cases} \quad \text{and} \quad \mathrm{Fil}^i D_{k,a_p} = \begin{cases} D_{k,a_p} & \text{if } i \leqslant 0, \\ Ee_1 & \text{if } 1 \leqslant i \leqslant k-1, \\ 0 & \text{if } i \geqslant k. \end{cases}$$

By the theorem of Colmez and Fontaine (see [**CF00**, théorème A] or [**Col02**, §11.6]), there exists a crystalline E-linear representation V_{k,a_p} such that we have $\mathbf{D}_{\mathrm{cris}}(V_{k,a_p}^*) = D_{k,a_p}$ where $V_{k,a_p}^* = \mathrm{Hom}(V_{k,a_p}, E)$ is the dual of V_{k,a_p}. The representations V_{k,a_p} are the representations studied by Breuil in [**Br03**]. They are crystalline, irreducible, and their Hodge-Tate weights are 0 and $k-1$. One can show that if V is any irreducible 2-dimensional crystalline $\overline{\mathbf{Q}}_p$-linear representation, then there exist $k \geqslant 2$, $a_p \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$ and η a crystalline character such that $V \simeq V_{k,a_p} \otimes \eta$ (see [**Br03**, prop 3.1] for a proof).

We will give a direct construction of the V_{k,a_p} (for those a_p in a small p-adic ball around 0) which provides a new proof of the theorem of Colmez-Fontaine for these representations, along the lines suggested by Fontaine in [**Fo91**, B.2.3]. We will actually construct a family of p-adic representations, that is a free $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[X]]$-module [(1)] $\mathbf{V}_k$ of rank 2 with a continuous linear action of $G_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that if one sets $m = \lfloor (k-2)/(p-1) \rfloor$, then for any $\alpha \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$ we have $\mathbf{V}_k(\alpha) = V_{k,p^m\alpha}^*$.

The family $\mathbf{V}_k$ gives an explicit 1-parameter deformation of $V_{k,0}^*$ (parameterized by a multiple of the trace of Frobenius). In particular, all the representations V_{k,a_p} with $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$ have the same semi-simplified reduction modulo p which partially answers some questions of Breuil [**Br03**, conjecture 6.1].

Let $\overline{V}_{k,a_p}$ be the semi-simplification of the reduction modulo p of a Galois stable lattice of V_{k,a_p}. Our main result is then (see theorem 4.1.1):

Theorem 1.1.1. — *If $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$, then $\overline{V}_{k,a_p} \simeq \overline{V}_{k,0}$.*

As a corollary of this result, we can describe the reduction modulo p of the representations arising from certain modular forms, thus generalizing some results of Deligne, Edixhoven, Fontaine and Serre.

1.2. Method of proof. — A (φ,Γ)-module is a finite dimensional vector space over a 2-dimensional complete local field along with some extra structure: a Frobenius operator φ and an action of the procyclic group $\Gamma_{\mathbf{Q}_p} = \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^\infty})/\mathbf{Q}_p)$, so that a (φ,Γ)-module is determined by two matrices (those of φ and of a generator of $\Gamma_{\mathbf{Q}_p}$ which is procyclic if $p \neq 2$) satisfying some conditions (the definition of these objects is recalled below in 2.2). Fontaine has constructed in [**Fo91**, A.3.4] an equivalence of categories from the category of p-adic representations to the category of étale (φ,Γ)-modules.

We will actually construct some explicit families of étale (φ,Γ)-modules. In order to do that, we only need to construct two matrices satisfying certain properties. By a theorem of Dee, a family of étale (φ,Γ)-modules gives rise to a family of p-adic representations.

The question is then: given an étale (φ,Γ)-module that corresponds to a p-adic representation V, how do we know whether that representation is crystalline and if it is, how do we compute $\mathbf{D}_{\mathrm{cris}}(V)$? The answer to those questions is given by the theory of Wach modules (developed in [**Wa96, Wa97, Col99, Ber03**] and recalled below in 2.2).

1.3. Plan of the article. — In the second chapter, we recall the definitions of (φ,Γ)-modules and of Wach modules. In the third chapter, we give the construction of the families of Wach modules, and then describe the families of crystalline representations obtained in this way. In the fourth chapter we apply those constructions and verify some conjectures of Breuil. After that, we give an application to modular forms. In the final chapter, we ask a couple of open questions related to our constructions.

---

(1) this definition of a family differs slightly from the one given in [**BC03**]

Acknowledgements: We thank C. Breuil, K. Buzzard, G. Chenevier, R. Coleman and P. Colmez for their comments and encouragements. We also thank the referee for his careful reading of this article. The research of Zhu is partially supported by an NSERC discovery grant, and she also thanks Laurent Berger and the Harvard mathematics department for hospitality and support during her stay at Harvard.

2. Representations of $G_{\mathbf{Q}_p}$

Let E be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_E$, maximal ideal $\mathfrak{m}_E$ and residue field k_E. An E-linear representation of $G_{\mathbf{Q}_p}$ is a finite dimensional E-vector space V with a continuous E-linear action of $G_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. The underlying $\mathbf{Q}_p$-vector space of V is then a $\mathbf{Q}_p$-linear representation of $G_{\mathbf{Q}_p}$, along with a $\mathbf{Q}_p$-algebra embedding $E \to \mathrm{End}_{\mathbf{Q}_p}(V)$ which commutes with the action of $G_{\mathbf{Q}_p}$. This observation allows us to extend most constructions on $\mathbf{Q}_p$-linear representations to constructions on E-linear representations, and below we recall those constructions which we will use.

2.1. Crystalline representations. — Let $\mathbf{B}_{\mathrm{cris}}$ be the ring constructed by Fontaine in [**Fo88a**, 2.3]. Recall that if V is a $\mathbf{Q}_p$-linear representation, then $\mathbf{D}_{\mathrm{cris}}(V) = (\mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_{\mathbf{Q}_p}}$ is a filtered φ-module of dimension $\leqslant \dim_{\mathbf{Q}_p}(V)$. We say that V is crystalline if equality holds. Colmez and Fontaine proved in [**CF00**, théorème A] that the functor $V \mapsto \mathbf{D}_{\mathrm{cris}}(V)$ is an equivalence of categories from the category of crystalline representations to the category of admissible filtered φ-modules.

We say that an E-linear representation V is crystalline if and only if the underlying $\mathbf{Q}_p$-linear representation is crystalline. In this case, $\mathbf{D}_{\mathrm{cris}}(V)$ is an E-vector space with an E-linear Frobenius and a filtration by E-vector spaces: it is an admissible E-linear filtered φ-module and the theorem of Colmez-Fontaine then implies that the functor $V \mapsto \mathbf{D}_{\mathrm{cris}}(V)$ is an equivalence of categories from the category of crystalline E-linear representations to the category of admissible E-linear filtered φ-modules (see [**BM02**, §3.1] for complete proofs).

2.2. Wach modules and (φ,Γ)-modules. — Let $\Gamma_{\mathbf{Q}_p} = \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^\infty})/\mathbf{Q}_p)$ and let χ be the cyclotomic character, so that $\chi : \Gamma_{\mathbf{Q}_p} \to \mathbf{Z}_p^*$ is an isomorphism. Let π be a variable and let $\mathbf{A}_{\mathbf{Q}_p}$ be the ring of power series $\sum_{i=-\infty}^{+\infty} a_i \pi^i$ such that $a_i \in \mathbf{Z}_p$ and $a_i \to 0$ as $i \to -\infty$. This is a local ring with maximal ideal (p) and its field of fractions is $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[1/p]$. Those two rings are endowed with a Frobenius φ defined by $\varphi(\pi) = (1+\pi)^p - 1$ and an action of $\Gamma_{\mathbf{Q}_p}$ defined by $\gamma(\pi) = (1+\pi)^{\chi(\gamma)} - 1$ for $\gamma \in \Gamma_{\mathbf{Q}_p}$.

A (φ,Γ)-module is an $\mathbf{A}_{\mathbf{Q}_p}$-module of finite rank, with semi-linear φ and continuous action of $\Gamma_{\mathbf{Q}_p}$ which commute with each other. We say that a (φ,Γ)-module D is étale if $\varphi(D)$ generates D over $\mathbf{A}_{\mathbf{Q}_p}$. Recall that Fontaine has constructed in [**Fo91**, A.3.4] a functor $T \mapsto \mathbf{D}(T)$ which associates to any $\mathbf{Z}_p$-representation T of $G_{\mathbf{Q}_p}$ an étale (φ,Γ)-module, and that the functor $T \mapsto \mathbf{D}(T)$ is then an equivalence of categories. By inverting p, one also gets an equivalence of categories between the category of ($\mathbf{Q}_p$-linear) p-adic representations and the category of étale (φ,Γ)-modules over $\mathbf{B}_{\mathbf{Q}_p}$.

If E is a finite extension of $\mathbf{Q}_p$, we extend the Frobenius and the action of $\Gamma_{\mathbf{Q}_p}$ to $E \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathbf{Q}_p}$ by E-linearity. By restricting our attention to $\mathcal{O}_E$-modules (or E-linear representations), we then get an equivalence of categories from the category of $\mathcal{O}_E$-modules (or E-linear representations) to the category of (φ,Γ)-modules over $\mathcal{O}_E \otimes_{\mathbf{Z}_p} \mathbf{A}_{\mathbf{Q}_p}$ (or (φ,Γ)-modules over $E \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathbf{Q}_p}$), given by $T \mapsto \mathbf{D}(T)$. The inverse functor will be denoted by $\mathbf{D} \mapsto T(\mathbf{D})$ (or $\mathbf{D} \mapsto V(\mathbf{D})$).

If V is a crystalline representation, we can be pretty specific about what its (φ,Γ)-module looks like. Let $\mathbf{A}_{\mathbf{Q}_p}^+ = \mathbf{Z}_p[[\pi]]$ and $\mathbf{B}_{\mathbf{Q}_p}^+ = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{A}_{\mathbf{Q}_p}^+ = \mathbf{A}_{\mathbf{Q}_p}^+[1/p]$. The following is proved in [**Ber03**, §II.1, §III.4] (for $\mathbf{Q}_p$-linear representations but the E-linear case follows at once):

If V is an E-linear representation, then V is crystalline with Hodge-Tate weights in $[a,b]$ if and only if there exists an $E \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathbf{Q}_p}^+$-module $\mathbf{N}(V)$ contained in $\mathbf{D}(V)$ such that:

1. $\mathbf{N}(V)$ is free of rank $d = \dim_E(V)$ over $E \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathbf{Q}_p}^+$;
2. The action of $\Gamma_{\mathbf{Q}_p}$ preserves $\mathbf{N}(V)$ and is trivial on $\mathbf{N}(V)/\pi\mathbf{N}(V)$;
3. $\varphi(\pi^b\mathbf{N}(V)) \subset \pi^b\mathbf{N}(V)$ and $\pi^b\mathbf{N}(V)/\varphi^*(\pi^b\mathbf{N}(V))$ is killed by q^{b-a} where $q = \varphi(\pi)/\pi$.

We say that a crystalline representation V is positive if we have $\mathbf{D}_{\mathrm{cris}}(V) = \mathrm{Fil}^0\,\mathbf{D}_{\mathrm{cris}}(V)$, or equivalently if $b \leqslant 0$. If V is a positive crystalline representation then we can take $b = 0$ above and if we endow $\mathbf{N}(V)$ with the filtration $\mathrm{Fil}^i\mathbf{N}(V) = \{x \in \mathbf{N}(V),\ \varphi(x) \in q^i\mathbf{N}(V)\}$, then $\mathbf{N}(V)/\pi\mathbf{N}(V)$ is an E-linear filtered φ-module and by [**Ber03**, §III.4] we then have an isomorphism: $\mathbf{N}(V)/\pi\mathbf{N}(V) \simeq \mathbf{D}_{\mathrm{cris}}(V)$.

If T is a $G_{\mathbf{Q}_p}$-stable lattice in V, then $\mathbf{N}(T) = \mathbf{D}(T) \cap \mathbf{N}(V)$ is an $\mathcal{O}_E \otimes_{\mathbf{Z}_p} \mathbf{A}^+_{\mathbf{Q}_p}$-lattice in $\mathbf{N}(V)$ (note that $\mathcal{O}_E \otimes_{\mathbf{Z}_p} \mathbf{A}^+_{\mathbf{Q}_p} = \mathcal{O}_E[[\pi]]$) and by [**Ber03**, §III.4] the functor $T \mapsto \mathbf{N}(T)$ gives a bijection between the $G_{\mathbf{Q}_p}$-stable lattices T in V and the $\mathcal{O}_E \otimes_{\mathbf{Z}_p} \mathbf{A}^+_{\mathbf{Q}_p}$-lattices $\mathbf{N}(T)$ in $\mathbf{N}(V)$ satisfying:

(1) $\mathbf{N}(T)$ is free of rank $d = \dim_E(V)$ over $\mathcal{O}_E \otimes_{\mathbf{Z}_p} \mathbf{A}^+_{\mathbf{Q}_p}$;
(2) The action of $\Gamma_{\mathbf{Q}_p}$ preserves $\mathbf{N}(T)$;
(3) $\varphi(\pi^b\mathbf{N}(T)) \subset \pi^b\mathbf{N}(T)$ and $\pi^b\mathbf{N}(T)/\varphi^*(\pi^b\mathbf{N}(T))$ is killed by q^{b-a}.

Such an object is called a Wach module. The aim of the following chapter is to construct families of Wach modules.

3. Families of Wach modules

In this chapter, we construct 1-parameter families of Wach modules. More precisely, fix $k \geqslant 2$ and define $m = \lfloor (k-2)/(p-1) \rfloor$; we construct a matrix $P(X) \in \mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$ and for every $\gamma \in \Gamma_{\mathbf{Q}_p}$ a matrix $G_\gamma(X) \in \mathrm{Id} + \pi\,\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$ such that:

(1) For any $\alpha \in \mathfrak{m}_E$, the matrices $P(\alpha)$ and $G_\gamma(\alpha)$ can be used to define a Wach module $\mathbf{N}_k(\alpha)$ which corresponds to a crystalline representation.

(2) If one sets $a_p = \alpha p^m$, then the 2-dimensional E-linear filtered φ-module associated to that crystalline representation is given by $D_{k,a_p} = Ee_1 \oplus Ee_2$ where:

$$\begin{cases} \varphi(e_1) = p^{k-1}e_2 \\ \varphi(e_2) = -e_1 + a_p e_2 \end{cases} \quad \text{and} \quad \mathrm{Fil}^i D_{k,a_p} = \begin{cases} D_{k,a_p} & \text{if } i \leqslant 0, \\ Ee_1 & \text{if } 1 \leqslant i \leqslant k-1, \\ 0 & \text{if } i \geqslant k. \end{cases}$$

These are the duals of the representations defined by Breuil in [**Br03**, §3.1]. They are crystalline, irreducible, and their Hodge-Tate weights are 0 and $-(k-1)$.

3.1. Construction of Wach modules.

— Let us now construct this family of Wach modules. Recall that $q = \varphi(\pi)/\pi$. For $n \geqslant 1$, we define $q_n = \varphi^{n-1}(q)$ so that $q_1 = q$. Let

$$\lambda_+ = \prod_{n \geqslant 0} \frac{\varphi^{2n+1}(q)}{p} = \frac{q_2}{p} \times \frac{q_4}{p} \times \frac{q_6}{p} \times \cdots \qquad \text{and} \qquad \lambda_- = \prod_{n \geqslant 0} \frac{\varphi^{2n}(q)}{p} = \frac{q_1}{p} \times \frac{q_3}{p} \times \frac{q_5}{p} \times \cdots$$

Proposition 3.1.1. — *The functions λ_+ and $\lambda_- \in \mathbf{Q}_p[[\pi]]$ satisfy the following properties:*

(1) $\lambda_+(0) = \lambda_-(0) = 1$;
(2) $\lambda_-/\gamma(\lambda_-)$ and $\lambda_+/\gamma(\lambda_+) \in 1 + \pi\mathbf{Z}_p[[\pi]]$;
(3) $\varphi(\lambda_-) = \lambda_+$ and $\varphi(\lambda_+) = \lambda_-/(q/p)$;
(4) Let $m = \lfloor (k-2)/(p-1) \rfloor$; if we write $p^m(\lambda_-/\lambda_+)^{k-1} = \sum_{i \geqslant 0} z_i\pi^i$ and we define $z = z_0 + z_1\pi + \cdots + z_{k-2}\pi^{k-2}$ then $z \in \mathbf{Z}_p[[\pi]]$.

Proof. — Since $q_n(0) = p$, point (1) is obvious. Point (2) follows from the fact that $\gamma(q)/q \in 1 + \pi\mathbf{Z}_p[[\pi]]$ and that:

$$\frac{\lambda_+}{\gamma(\lambda_+)} = \prod_{n \geqslant 0} \varphi^{2n+1}\left(\frac{q}{\gamma(q)}\right) \quad \text{and} \quad \frac{\lambda_-}{\gamma(\lambda_-)} = \prod_{n \geqslant 0} \varphi^{2n}\left(\frac{q}{\gamma(q)}\right).$$

Point (3) follows immediately from the definitions.

Let us now prove (4). Let R be the set of power series $\sum_{i \geqslant 0} a_i\pi^i$ such that $a_i \in \mathbf{Q}_p$ and $v_p(a_i) + i/(p-1) \geqslant 0$. One checks easily that R is a ring and that q_n/p and $p/q_n \in R$ for all $n \geqslant 1$ so that $(\lambda_-/\lambda_+)^{k-1} \in R$. This implies that if we write $p^m(\lambda_-/\lambda_+)^{k-1} = \sum_{i \geqslant 0} z_i\pi^i$ then $v_p(z_i) + i/(p-1) \geqslant m$. In particular, we have

$v_p(z_i) \geqslant m - (k-2)/(p-1)$ if $i = 0, \cdots, k-2$. Since $m = \lfloor (k-2)/(p-1) \rfloor$, this implies that $v_p(z_i) > -1$ and so that $v_p(z_i) \geqslant 0$. Therefore, $z \in \mathbf{Z}_p[[\pi]]$. □

We define

$$P(X) = \begin{pmatrix} 0 & -1 \\ q^{k-1} & Xz \end{pmatrix} \quad \text{and} \quad G_\gamma^{(k-1)} = \begin{pmatrix} \left(\frac{\lambda_+}{\gamma(\lambda_+)}\right)^{k-1} & 0 \\ 0 & \left(\frac{\lambda_-}{\gamma(\lambda_-)}\right)^{k-1} \end{pmatrix}.$$

Lemma 3.1.2. — *We have:*

$$P(X)\varphi(G_\gamma^{(k-1)}) - G_\gamma^{(k-1)}\gamma(P(X)) = \begin{pmatrix} 0 & 0 \\ 0 & \pi^{k-1}\star \end{pmatrix} \in \pi^{k-1}\,\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]]).$$

Proof. — Note that φ and $\gamma \in \Gamma_{\mathbf{Q}_p}$ act trivially on X. A direct computation using the fact that $\varphi(\lambda_+) = \lambda_-/(q/p)$ shows that

$$P(X)\varphi(G_\gamma^{(k-1)}) = \begin{pmatrix} 0 & -\left(\frac{\lambda_+}{\gamma(\lambda_+)}\right)^{k-1} \\ \gamma(q)^{k-1}\left(\frac{\lambda_-}{\gamma(\lambda_-)}\right)^{k-1} & Xz\left(\frac{\lambda_+}{\gamma(\lambda_+)}\right)^{k-1} \end{pmatrix}$$

and that

$$G_\gamma^{(k-1)}\gamma(P(X)) = \begin{pmatrix} 0 & -\left(\frac{\lambda_+}{\gamma(\lambda_+)}\right)^{k-1} \\ \gamma(q)^{k-1}\left(\frac{\lambda_-}{\gamma(\lambda_-)}\right)^{k-1} & X\gamma(z)\left(\frac{\lambda_-}{\gamma(\lambda_-)}\right)^{k-1} \end{pmatrix}$$

and to prove the lemma, we need to show that

$$z\left(\frac{\lambda_+}{\gamma(\lambda_+)}\right)^{k-1} - \gamma(z)\left(\frac{\lambda_-}{\gamma(\lambda_-)}\right)^{k-1} \in \pi^{k-1}\mathbf{Z}_p[[\pi]] = \mathbf{Z}_p[[\pi]] \cap \pi^{k-1}\mathbf{Q}_p[[\pi]].$$

It is clear by proposition 3.1.1 (2) and (4) that the above series belongs to $\mathbf{Z}_p[[\pi]]$. Finally, by definition of z, we have $z - p^m(\lambda_-/\lambda_+)^{k-1} \in \pi^{k-1}\mathbf{Q}_p[[\pi]]$ which proves the second inclusion. □

Proposition 3.1.3. — *There exists a unique matrix*

$$G_\gamma(X) \in \mathrm{Id} + \pi\,\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$$

such that $P(X)\varphi(G_\gamma(X)) = G_\gamma(X)\gamma(P(X))$.

Proof. — We will start by proving the uniqueness of a matrix $G_\gamma(X)$ satisfying the above conditions. Assume that there exist $G_\gamma(X)$ and $G'_\gamma(X)$ satisfying the above conditions and set $H = G'_\gamma(X)G_\gamma^{-1}(X)$. A short computation shows that $H \in \mathrm{Id} + \pi\,\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$ and that $HP(X) = P(X)\varphi(H)$. We will show that this implies $H = \mathrm{Id}$. Assume that this is not the case, and write $H = \mathrm{Id} + H_\ell\pi^\ell + \cdots$ where $H_\ell \neq 0$ and $P(X) = P_0 + P_1\pi + \cdots$. The facts that $HP(X) = P(X)\varphi(H)$ and that $\varphi(\pi^\ell)/\pi^\ell \equiv p^\ell \mod \pi$ imply that $H_\ell P_0 = p^\ell P_0 H_\ell$ which in turn implies that P_0 has two eigenvalues the quotient of which is p^ℓ. Since

$$P_0 = \begin{pmatrix} 0 & -1 \\ p^{k-1} & Xp^m \end{pmatrix},$$

this is impossible.

Let us now show the existence of $G_\gamma(X)$. Recall that by lemma 3.1.2, we have:

$$P(X)\varphi(G_\gamma^{(k-1)}) - G_\gamma^{(k-1)}\gamma(P(X)) = \begin{pmatrix} 0 & 0 \\ 0 & \pi^{k-1}\star \end{pmatrix} \in \pi^{k-1}\,\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]]),$$

and a direct computation shows that

$$\begin{pmatrix} 0 & 0 \\ 0 & \pi^{k-1}\star \end{pmatrix}\gamma(P(X)^{-1}) = \frac{1}{q^{k-1}}\begin{pmatrix} 0 & 0 \\ 0 & \pi^{k-1}\star \end{pmatrix}\begin{pmatrix} Xz & 1 \\ -q^{k-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -\pi^{k-1}\star & 0 \end{pmatrix}$$

so that we can write

$$G_\gamma^{(k-1)} - P(X)\varphi(G_\gamma^{(k-1)})\gamma(P(X)^{-1}) = \pi^{k-1}R^{(k-1)}$$

with $R^{(k-1)} \in \mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$.

We will prove by recurrence on $\ell \geqslant k-1$ that there exist matrices $R^{(\ell)}$ and $G_\gamma^{(\ell)}$ in $\mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$ such that $G_\gamma^{(\ell)} \equiv G_\gamma^{(\ell-1)} \mod \pi^{\ell-1}$ and such that we can write:

$$G_\gamma^{(\ell)} - P(X)\varphi(G_\gamma^{(\ell)})\gamma(P(X)^{-1}) = \pi^\ell R^{(\ell)} \in \pi^\ell\, \mathrm{M}(2, \mathbf{Z}_p[[\pi, X]]).$$

We already know this for $\ell = k-1$ and for $\ell \geqslant k$ we need to find $H^{(\ell)} \in \mathrm{M}(2, \mathbf{Z}_p[[X]])$ such that if we set $G_\gamma^{(\ell)} = G_\gamma^{(\ell-1)} + \pi^{\ell-1} H^{(\ell)}$ then the above equation holds.

Bearing in mind that $\varphi(\pi) = q\pi$, this gives the following equation for $H^{(\ell)}$:

$$\pi^{\ell-1}R^{(\ell-1)} + \pi^{\ell-1}H^{(\ell)} - P(X)\pi^{\ell-1}\varphi(H^{(\ell)})q^{\ell-1}\gamma(P(X)^{-1}) \in \pi^\ell\, \mathrm{M}(2, \mathbf{Z}_p[[\pi, X]]).$$

Notice that since $\ell \geqslant k$, we have $q^{\ell-1}\gamma(P(X)^{-1}) \in \mathrm{M}(2, \mathbf{Z}_p[[\pi, X]])$. Therefore, we can divide the above equation by $\pi^{\ell-1}$ and we see that we only need to find $H^{(\ell)} \in \mathrm{M}(2, \mathbf{Z}_p[[X]])$ such that

$$H^{(\ell)} - P_0 H^{(\ell)}(p^{\ell-1}P_0^{-1}) \equiv -R^{(\ell-1)} \mod \pi,$$

because $\varphi(H^{(\ell)}) = H^{(\ell)}$ if $H^{(\ell)} \in \mathrm{M}(2, \mathbf{Z}_p[[X]])$.

Notice that we have $p^{\ell-1}P_0^{-1} \in p^{\ell-k}\, \mathrm{M}(2, \mathbf{Z}_p[[X]])$. This implies that the operator $H \mapsto H - P_0 H(p^{\ell-1}P_0^{-1})$ is a bijection on $\mathrm{M}(2, \mathbf{Z}_p[[X]])$ if $\ell \geqslant k+1$ and to finish the proof, we only need to show that this also holds if $\ell = k$. However, a direct computation shows that modulo (p, X), this operator becomes:

$$\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \mapsto \begin{pmatrix} h_{11} & h_{12} + h_{21} \\ h_{21} & h_{22} \end{pmatrix},$$

which is obviously invertible. This shows that at each step, we can "lift" $G_\gamma^{(\ell-1)}$ to one and only one $G_\gamma^{(\ell)}$. To finish the proof, we need only take $G_\gamma(X) = \lim_{\ell \to +\infty} G_\gamma^{(\ell)}(X)$. □

3.2. Families of crystalline representations. — First, we check that the above construction does give rise to a Wach module, and therefore to a crystalline representation. If $\alpha \in \mathfrak{m}_E$, then the matrices $P(\alpha)$ and $G_\gamma(\alpha)$ belong to $\mathcal{O}_E[[\pi]]$.

Proposition 3.2.1. — *If $\alpha \in \mathfrak{m}_E$ and γ, $\eta \in \Gamma_K$ then $G_{\gamma\eta}(\alpha) = G_\gamma(\alpha)\gamma(G_\eta(\alpha))$ and*

$$P(\alpha)\varphi(G_\gamma(\alpha)) = G_\gamma(\alpha)\gamma(P(\alpha))$$

so that one can use the matrices $P(\alpha)$ and $G_\gamma(\alpha)$ to define a Wach module $\mathbf{N}_k(\alpha)$ over $\mathcal{O}_E[[\pi]]$.

Remark 3.2.2. — When $\alpha = 0$, the Wach module $\mathbf{N}_k(0)$ coincides with the last example of [**Ber03**, Appendice A].

Proof. — We already know that $P(X)\varphi(G_\gamma(X)) = G_\gamma(X)\gamma(P(X))$ and if γ, $\eta \in \Gamma_K$ then $G_{\gamma\eta}(X)$ and $G'_{\gamma\eta}(X) = G_\gamma(X)\gamma(G_\eta(X))$ both satisfy the conditions of proposition 3.1.3 so that they are equal. We then define $\mathbf{N}_k(\alpha)$ as the free $\mathcal{O}_E[[\pi]]$-module of rank 2 with basis n_1, n_2 as follows: $\mathbf{N}_k(\alpha) = \mathcal{O}_E[[\pi]]n_1 \oplus \mathcal{O}_E[[\pi]]n_2$. We then endow it with a Frobenius φ and an action of $\Gamma_{\mathbf{Q}_p}$ by deciding that the matrix of φ with respect to the basis (n_1, n_2) is $P(\alpha)$ and that the matrix of $\gamma \in \Gamma_{\mathbf{Q}_p}$ is $G_\gamma(\alpha)$. □

Definition 3.2.3. — If $\alpha \in \mathfrak{m}_E$, define $a_p = p^m\alpha$. Let V_{k,a_p} be the crystalline E-linear representation such that $E \otimes_{\mathcal{O}_E} \mathbf{N}_k(\alpha) = \mathbf{N}(V_{k,a_p}^*)$ and let T_{k,a_p} be the $\mathcal{O}_E$-lattice in V_{k,a_p} such that $\mathbf{N}_k(\alpha) = \mathbf{N}(T_{k,a_p}^*)$.

Proposition 3.2.4. — *The filtered φ-module $E \otimes_{\mathcal{O}_E} (\mathbf{N}_k(\alpha)/\pi\mathbf{N}_k(\alpha))$ is isomorphic to the filtered φ-module D_{k,a_p} described at the beginning of the chapter, so that we have $\mathbf{D}_{\mathrm{cris}}(V_{k,a_p}^*) = D_{k,a_p}$.*

Proof. — Recall that $D_{k,a_p} = Ee_1 \oplus Ee_2$ where:

$$\begin{cases} \varphi(e_1) = p^{k-1}e_2 \\ \varphi(e_2) = -e_1 + a_p e_2 \end{cases} \quad \text{and} \quad \mathrm{Fil}^i D_{k,a_p} = \begin{cases} D_{k,a_p} & \text{if } i \leqslant 0, \\ Ee_1 & \text{if } 1 \leqslant i \leqslant k-1, \\ 0 & \text{if } i \geqslant k. \end{cases}$$

and that

$$P(\alpha) = \begin{pmatrix} 0 & -1 \\ q^{k-1} & \alpha z \end{pmatrix} \quad \text{so that} \quad (P(\alpha) \mod \pi) = \begin{pmatrix} 0 & -1 \\ p^{k-1} & a_p \end{pmatrix}.$$

We will show that the map $n_i \mapsto e_i$ gives the required isomorphism from $E \otimes_{\mathcal{O}_E} (\mathbf{N}_k(\alpha)/\pi\mathbf{N}_k(\alpha))$ to D_{k,a_p}. It is obvious from the above that this is an isomorphism of φ-modules, and to finish the proof we need to compute the filtration on $\mathbf{N}_k(\alpha)$. The proposition will then follow from:

$$\mathrm{Fil}^i\mathbf{N}_k(\alpha) = \begin{cases} \mathbf{N}_k(\alpha) & \text{if } i \leqslant 0, \\ n_1\mathcal{O}_E[[\pi]] \oplus \pi^i n_2\mathcal{O}_E[[\pi]] & \text{if } 1 \leqslant i \leqslant k-1, \\ \pi^{i-(k-1)}n_1\mathcal{O}_E[[\pi]] \oplus \pi^i n_2\mathcal{O}_E[[\pi]] & \text{if } i \geqslant k. \end{cases}$$

Recall that $\mathrm{Fil}^i\mathbf{N} = \{x \in \mathbf{N},\ \varphi(x) \in q^i\mathbf{N}\}$. It is obvious that $\mathrm{Fil}^i\mathbf{N}_k(\alpha) = \mathbf{N}_k(\alpha)$ if $i \leqslant 0$.

Next, choose $1 \leqslant i \leqslant k-1$ and write $x = x_1n_1 + x_2n_2$. We have $\varphi(x) = -\varphi(x_2)n_1 + (q^{k-1}\varphi(x_1) + \alpha z\varphi(x_2))n_2$ and therefore, $x \in \mathrm{Fil}^i\mathbf{N}_k(\alpha)$ if and only if $q^i|\varphi(x_2)$ which is equivalent to $\pi^i|x_2$. If $i \geqslant k$, the proof is completely similar. $\square$

Remark 3.2.5. — By Dee's theorem [**Dee01**, theorem 2.1.27] (see also [**BC03**]), an étale family of (φ,Γ)-modules (in our case, $\mathbf{N}_k(X)$ over $\mathbf{Z}_p[[X]]$) gives rise to an analytic family of p-adic representations (in our case, a free $\mathbf{Z}_p[[X]]$-module $\mathbf{T}_k$ of rank 2 with a continuous linear action of $G_{\mathbf{Q}_p}$).

The family $\mathbf{V}_k = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{T}_k$ is a 1-dimensional subspace (parameterized by $p^m a_p$, a multiple of the trace of Frobenius) of the space of all representations deforming $V_{k,0}^*$.

4. Applications

4.1. Reduction modulo p. — We will now use the constructions of the previous chapter to verify some conjectures of Breuil about the reduction of the representations V_{k,a_p} defined above. Recall that $a_p = p^m\alpha$ where $m = \lfloor (k-2)/(p-1) \rfloor$ and $\alpha \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$.

Theorem 4.1.1. — *Given $\alpha \in \mathfrak{m}_E$, the two k_E-representations $k_E \otimes_{\mathcal{O}_E} T_{k,a_p}$ and $k_E \otimes_{\mathcal{O}_E} T_{k,0}$ are isomorphic.*

Proof. — Given $\alpha \in \mathfrak{m}_E$, we have $G_\gamma(\alpha) \equiv G_\gamma(0) \mod \mathfrak{m}_E$ and $P(\alpha) \equiv P(0) \mod \mathfrak{m}_E$ because $P,\ G_\gamma \in \mathrm{M}(2, \mathbf{A}^+_{\mathbf{Q}_p}[[X]])$. If $\mathbf{D}_{k,\alpha} = \mathbf{A}_{\mathbf{Q}_p} \otimes_{\mathbf{A}^+_{\mathbf{Q}_p}} \mathbf{N}_k(\alpha)$ is the (φ,Γ)-module associated to $\mathbf{N}_k(\alpha)$ then we have

$$\mathrm{Hom}_{\varphi,\Gamma}(\mathbf{D}_{k,0}, k_E((\pi))) = \mathrm{Hom}_{\varphi,\Gamma}(\mathbf{D}_{k,\alpha}, k_E((\pi)))\,.$$

Since $k_E \otimes_{\mathcal{O}_E} T_{k,a_p} = T(\mathrm{Hom}_{\varphi,\Gamma}(\mathbf{D}_{k,\alpha}, k_E((\pi))))$ where T is Fontaine's functor (since $T(\cdot)$ is an exact functor), we see that $k_E \otimes_{\mathcal{O}_E} T_{k,a_p} \simeq k_E \otimes_{\mathcal{O}_E} T_{k,0}$. $\square$

Remark 4.1.2. — (1) The constant $m = \lfloor (k-2)/(p-1) \rfloor$ is not necessarily the "best" possible one for every k. Indeed, in proposition 3.1.1-4 one only needs to take m such that $(p^m(\lambda_-/\lambda_+)^{k-1} \mod \pi^{k-1})$ has coefficients in $\mathbf{Z}_p$. For example, if $k = p+1$, then one may take $m = 0$;

(2) The same argument will show that if $i \geqslant 1$ and if we choose $\alpha_1,\ \alpha_2 \in \mathfrak{m}_E$ satisfying $v_E(\alpha_1 - \alpha_2) \geqslant i$ and set $a_p^{(j)} = p^m\alpha_j$ then

$$T_{k,a_p^{(1)}} \equiv T_{k,a_p^{(2)}} \mod \mathfrak{m}_E^i;$$

(3) Instead of using the (φ,Γ)-modules, one could also use the fact that by Dee's theorem, the T^*_{k,a_p}'s come from evaluating $\mathbf{T}_k$ at α where $a_p = p^m\alpha$ and the above congruences follow at once.

We can now prove some congruences which were conjectured (with slightly sharper bounds on $v_p(a_p)$) by Breuil (See Breuil's [**Br03**, conj 6.1]).

If $a_p \in \mathfrak{m}_E$ and $v_p(a_p) > m = \lfloor (k-2)/(p-1) \rfloor$, then there exists $\alpha \in \mathfrak{m}_E$ such that $a_p = \alpha p^m$ and the following is then a direct consequence of theorem 4.1.1 (and remark 4.1.2-1 for $k = p+1$) applied to $m = 0, 1, 2$ (for $k \leqslant p$, the first congruence is also a direct consequence of "Fontaine-Laffaille").

Corollary 4.1.3. — *The following congruences hold:*

(1) *If* $k \leqslant p+1$, *then* $\overline{V}_{k,a_p} \simeq \overline{V}_{k,0}$ *if* $v_p(a_p) > 0$;
(2) *If* $k \leqslant 2p-1$, *then* $\overline{V}_{k,a_p} \simeq \overline{V}_{k,0}$ *if* $v_p(a_p) > 1$;
(3) *If* $k \leqslant 3p-2$, *then* $\overline{V}_{k,a_p} \simeq \overline{V}_{k,0}$ *if* $v_p(a_p) > 2$.

To keep this article reasonably self-contained, let us recall the explicit description of $\overline{V}_{k,0}$ given by Breuil in [**Br03**, prop 6.2]. Recall that χ is the cyclotomic character; ω_2 stands for the fundamental character of level 2, $\mu_{\pm\sqrt{-1}}$ is the unramified character of $G_{\mathbf{Q}_p}$ which sends Frob_p to $\pm\sqrt{-1}$ and ind is the induction from $\mathbf{F}_{p^2}$ to $\mathbf{F}_p$.

Proposition 4.1.4. — *We have:*
(1) *If* $(p+1) \nmid (k-1)$, *then* $\overline{V}_{k,0} = \mathrm{ind}(\omega_2^{k-1})$;
(2) *If* $(p+1)|(k-1)$, *then*

$$\overline{V}_{k,0} = \begin{pmatrix} \mu_{\sqrt{-1}} & 0 \\ 0 & \mu_{-\sqrt{-1}} \end{pmatrix} \otimes \chi^{(k-1)/(p+1)}.$$

This proposition is itself a consequence of [**Br03**, prop 3.2] which describes $V_{k,0}$.

4.2. Application to modular forms. — In this paragraph, we give an application of theorem 4.1.1 above to the reduction modulo p of the representations attached to certain modular forms. This way, we can generalize results of Deligne, Edixhoven, Fontaine and Serre (see [**Edi92**, §2] and [**Br03**, théorème 6.7]). We follow [**Br03**, §6.2] very closely.

Fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. Let f be a normalized cuspidal modular form over $\Gamma_1(N)$, of level $N \geqslant 1$ coprime to p, of character η and of weight $k \geqslant 2$. We also assume that f is a newform (hence an eigenform) for the Hecke operators T_ℓ for all primes $\ell \nmid N$. The elements $a_\ell(f) \in \mathcal{O}_{\overline{\mathbf{Q}}_p}$ are defined by $T_\ell f = a_\ell(f) f$ and we assume in this paragraph that $a_p(f) \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$ (in other words, that f is not ordinary).

Let V_f be the restriction to $G_{\mathbf{Q}_p}$ of the p-adic representation attached to f and let $\overline{V}_f$ denote the semi-simplification of its reduction modulo p. Recall that we have

$$V_f \simeq V_{k,a_p(f)\eta^{1/2}(p)} \otimes \eta^{1/2},$$

where $\eta^{1/2}$ is an unramified character of $G_{\mathbf{Q}_p}$ whose square is η (see [**Br03**, théorème 6.2.1] for a statement and [**BM02**, §4.3] for precise references). We can therefore apply theorem 4.1.1 and get:

Theorem 4.2.1. — *Under the preceding hypotheses, we have* $\overline{V}_f \simeq \overline{V}_{k,0} \otimes \eta^{1/2}$ *if* $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$.

This way, we get an explicit description of $\overline{V}_f$ using [**Br03**, prop 6.1.2] recalled above in proposition 4.1.4.

5. Open questions

In this last chapter, we give a few open questions related to the construction of (φ, Γ)-modules.

(1) It is clear that our methods should extend to more general situations: given a filtered φ-module, can one find a Wach module whose reduction modulo π is that filtered φ-module? This article gives some evidence of how one can do that, but in general one problem is the following: given a lattice T in a crystalline representation V, then $\mathbf{N}(T)/\pi\mathbf{N}(T)$ is a lattice in $\mathbf{D}_{\mathrm{cris}}(V)$. Which lattices do we get in this way? Do we get all strongly divisible lattices (see [**FL82**] for a definition) in $\mathbf{D}_{\mathrm{cris}}(V)$ this way? When the length of the filtration is $\leqslant p-1$, the answer is yes (see [**Wa97**, §3.2] and [**Ber03**, §V.2]).

(2) In the ramified case or in the semi-stable case, we know even less. However, when the length of the filtration is $\leqslant p-1$ (or $\leqslant p-2$ in the semi-stable case) those representations are described by "Breuil modules" (see [**Br99, Br00**]). How does one compute the (φ, Γ)-module of such a representation directly from its Breuil module? In the unramified crystalline case, when the length of the filtration is $\leqslant p-1$, then a Breuil module is equivalent to the data of a strongly divisible lattice and the computation of the associated Wach module is done in [**Wa97**, §3.2] and in [**Ber03**, V.2].

References

[Ber03] Berger L.: *Limites de représentations cristallines.* To appear in Compositio Mathematica.

[BC03] Berger L., Colmez P.: *Familles de représentations p-adiques.* In preparation.

[Br99] Breuil C.: *Représentations semi-stables et modules fortement divisibles.* Invent. Math. 136 (1999), no. 1, 89–122.

[Br00] Breuil C.: *Integral p-adic Hodge theory.* Algebraic geometry 2000, Azumino (Hotaka), 51–80, Adv. Stud. Pure Math., 36, Math. Soc. Japan, Tokyo, 2002.

[Br03] Breuil C.: *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbf{Q}_p)$ *II.* J. Inst. Math. Jussieu 2 (2003), no. 1, 23–58.

[BM02] Breuil C., Mézard A.: *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbf{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ *en* $l = p$. With an appendix by Guy Henniart. Duke Math. J. 115 (2002), no. 2, 205–310.

[Col99] Colmez P.: *Représentations cristallines et représentations de hauteur finie.* J. Reine Angew. Math. 514 (1999), 119–143.

[Col02] Colmez P.: *Espaces de Banach de dimension finie.* J. Inst. Math. Jussieu 1 (2002), no. 3, 331–439.

[CF00] Colmez P., Fontaine J-M.: *Construction des représentations p-adiques semi-stables.* Invent. Math. 140 (2000) 1–43.

[Dee01] Dee J.: Φ-Γ *modules for families of Galois representations.* J. Algebra 235 (2001), no. 2, 636–664.

[Edi92] Edixhoven B.: *The weight in Serre's conjectures on modular forms.* Invent. Math. 109 (1992), no. 3, 563–594.

[Fo88a] Fontaine J-M.: *Le corps des périodes p-adiques.* Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque 223 (1994) 59–111.

[Fo88b] Fontaine J-M.: *Représentations p-adiques semi-stables.* Périodes p-adiques, (Bures-sur-Yvette, 1988), Astérisque 223 (1994) 113–184.

[Fo91] Fontaine J-M.: *Représentations p-adiques des corps locaux I.* The Grothendieck Festschrift, Vol. II, 249–309, Progr. Math. 87, Birkhäuser Boston, Boston, MA 1990.

[FL82] Fontaine J-M., Laffaille G.: *Construction de représentations p-adiques.* Ann. Sci. École Norm. Sup. (4) 15 (1982), no. 4, 547–608 (1983).

[Wa96] Wach N.: *Représentations p-adiques potentiellement cristallines.* Bull. Soc. Math. France 124 (1996), 375–400.

[Wa97] Wach N.: *Représentations cristallines de torsion.* Compositio Math. 108 (1997) 185–240.

January 2004

Laurent Berger, Harvard University, Department of Mathematics, One Oxford Street, Cambridge, MA 02138-2901, USA
E-mail : laurent@math.harvard.edu • *Url :* www.math.harvard.edu/~laurent

Hanfeng Li, Department of Mathematics, University of Toronto, Toronto, ON M5S 3G3, Canada.
E-mail : hli@fields.toronto.edu

Hui June Zhu, Department of Mathematics, McMaster University, Hamilton, ON L8S 4K1, Canada.
E-mail : zhu@cal.berkeley.edu