LOCAL CONSTANCY FOR THE REDUCTION MOD p OF 2-DIMENSIONAL CRYSTALLINE REPRESENTATIONS

by

Laurent Berger

Abstract. — Irreducible crystalline representations of dimension 2 of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ depend up to twist on two parameters, the weight k and the trace of frobenius a_p. We show that the reduction modulo p of such a representation is a locally constant function of a_p (with an explicit radius) and a locally constant function of the weight k if $a_p \neq 0$. We then give an algorithm for computing the reductions modulo p of these representations. The main ingredient is Fontaine's theory of (φ, Γ)-modules as well as the theory of Wach modules.

Contents

Introduction

Let p be a prime number $\neq 2$ and E a finite extension of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}_E$ and maximal ideal $\mathfrak{m}_E$ and uniformizer π_E and residue field k_E. If $k \geqslant 2$ and $a_p \in \mathfrak{m}_E$, let D_{k,a_p} be the filtered φ-module given by $D_{k,a_p} = Ee_1 \oplus Ee_2$ where :

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

2000 ***Mathematics Subject Classification.*** — 11F, 11S, 11Y.
Key words and phrases. — Galois representations, (φ, Γ)-modules, Wach modules, weight space.

This research is partially supported by the ANR grant CETHop (calculs effectifs en théorie de Hodge p-adique) ANR-09-JCJC-0048-01.

By the theorem of Colmez-Fontaine (théorème A of [**CF00**]), there exists a crystalline E-linear representation V_{k,a_p} of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $\mathrm{D}_{\mathrm{cris}}(V_{k,a_p}^*) = D_{k,a_p}$ where V_{k,a_p}^* is the dual of V_{k,a_p}. The representation V_{k,a_p} is crystalline, irreducible, and its Hodge-Tate weights are 0 and $k-1$. Let T denote a $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-stable lattice of V_{k,a_p} and let $\overline{V}_{k,a_p}$ be the semisimplification of $T/\pi_E T$. It is well-known that $\overline{V}_{k,a_p}$ depends only on V_{k,a_p} and not on the choice of T.

We should therefore be able to describe $\overline{V}_{k,a_p}$ in terms of k and a_p but this seems to be a difficult problem. Note that it is easy to make a list of all semisimple 2-dimensional k_E-linear representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$: they are twists of $\mathrm{ind}(\omega_2^r)$ (in the notation of [**Bre03**]; ω_2 is the fundamental character of level 2) for some $r \in \mathbf{Z}$ or direct sums of two characters.

If $2 \leqslant k \leqslant p$, then the theory of Fontaine-Laffaille gives us $\overline{V}_{k,a_p} = \mathrm{ind}(\omega_2^{k-1})$. If $k = p+1$ or $k \geqslant p+2$ and $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$, then theorem 4.1.1, remark 4.1.2 and proposition 4.1.4 of [**BLZ04**] show that $\overline{V}_{k,a_p} = \mathrm{ind}(\omega_2^{k-1})$. For other values of a_p we can get a few additional results by using the p-adic Langlands correspondence (see [**BG09**] or conjecture 1.5 of [**Bre03**], combined with [**Ber10**]) or by computing the reduction in specific cases using congruences of modular forms (Savitt-Stein and Buzzard, see for instance §6.2 of [**Bre03**]). However, no general formula is known or even conjectured.

Our first result is that the function $a_p \mapsto \overline{V}_{k,a_p}$ is locally constant with an explicit radius and that if we see $k \gg \mathrm{val}_p(a_p)$ as an element of the weight space $\varprojlim_n \mathbf{Z}/p^{n-1}(p-1)\mathbf{Z}$, then $k \mapsto \overline{V}_{k,a_p}$ is locally constant for (most) $a_p \neq 0$.

Let $\alpha(k) = \sum_{n \geqslant 1} \lfloor k/p^{n-1}(p-1) \rfloor$ so that for example $\alpha(k-1) \leqslant \lfloor (k-1)p/(p-1)^2 \rfloor$.

Theorem A. — *If* $\mathrm{val}_p(a_p - a_p') > 2 \cdot \mathrm{val}_p(a_p) + \alpha(k-1)$, *then* $\overline{V}_{k,a_p'} = \overline{V}_{k,a_p}$.

The fact that $\overline{V}_{k,a_p}$ is a locally constant function of a_p had been observed by many people (Colmez, Fontaine, Kisin, Paškūnas, ...). The novelty in theorem A is the explicit radius. The proof uses the theory of Wach modules and consists in showing that if one knows the Wach module for V_{k,a_p} then one can deform it to a Wach module for $V_{k,a_p'}$ if a_p' is sufficiently close to a_p. By being careful, one can get the explicit radius of theorem A (this method is the one which is sketched in §10.3 of [**BB04**]; it is also used in [**Dou10**]).

Theorem B. — *If* $a_p \neq 0$ *and* $a_p^2 \notin p^{\mathbf{Z}}$ *and* $k > 3 \cdot \mathrm{val}_p(a_p) + \alpha(k-1) + 1$, *then there exists* $m = m(k, a_p)$ *such that* $\overline{V}_{k',a_p} = \overline{V}_{k,a_p}$ *if* $k' \geqslant k$ *and* $k' - k \in p^{m-1}(p-1)\mathbf{Z}$.

The main result of [**BG09**] shows for example that if $0 < \mathrm{val}_p(a_p) < 1$ and if $k \neq 3 \bmod p-1$, then $\overline{V}_{k,a_p}$ depends only on $k \bmod p-1$. The proof of theorem B consists in showing that the V_{k,a_p}'s occur in the families of trianguline representations constructed in §5.1 of [**Col08**]. Since Colmez excludes from his main result those representations for which (in his notations) "$\delta_0(p) \in p^{\mathbf{Z}}$", we have to exclude those a_p's for which $a_p^2 \in p^{\mathbf{Z}}$ but this can probably be easily overcome by the motivated reader. On the other hand, the restriction $a_p \neq 0$ is essential since the conclusion of theorem B fails for $a_p = 0$. In this case, the associated weight space is quite different: see [**Ber09**] for a construction of a p-adic family of representations which interpolates the $V_{k,0}$.

Our second result is an algorithm which can be programmed and which, given the data of k and $a_p \bmod \pi_E^n$, will return $\overline{V}_{k,a_p}$ if n is large enough. This algorithm is based on Fontaine's theory of (φ,Γ)-modules (see A.3 of [**Fon90**]) and its refinement for crystalline representations, the theory of Wach modules (see [**Ber04**]). In order to give the statement of the result, we give a few reminders about the theory of (φ,Γ)-modules for k_E-linear representations. Let Γ be a group isomorphic to $\mathbf{Z}_p^\times$ via a map $\chi : \Gamma \to \mathbf{Z}_p^\times$. The field $k_E(\!(X)\!)$ is endowed with a k_E-linear frobenius φ given by $\varphi(f)(X) = f(X^p)$ and an action of Γ given by $\gamma(f)(X) = f((1+X)^{\chi(\gamma)} - 1)$. A (φ,Γ)-module (over k_E) is a finite dimensional $k_E(\!(X)\!)$-vector space endowed with a semilinear frobenius whose matrix satisfies $\mathrm{Mat}(\varphi) \in \mathrm{GL}_d(k_E(\!(X)\!))$ in some basis and a commuting semilinear continuous action of Γ. By a theorem of Fontaine (see A.3.4 of [**Fon90**]), the category of (φ,Γ)-modules over k_E is naturally isomorphic to the category of k_E-linear representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. The group Γ is topologically cyclic (at least if $p \neq 2$) so that a (φ,Γ)-module is determined by two matrices P and G, the matrices of φ and of a topological generator γ of Γ in some basis. In the sequel, we denote by $\mathrm{rep}(P,G)$ the k_E-linear representation associated to the (φ,Γ)-module determined by P and G.

If $f(X) \in \mathcal{O}_E[\![X]\!]$, set $\varphi(f)(X) = f((1+X)^p - 1)$ so that in particular, $\varphi(X) = XQ$ where $Q = \Phi_p(1+X)$, and let Γ act on $\mathcal{O}_E[\![X]\!]$ by $\eta(f)(X) = f((1+X)^{\chi(\eta)} - 1)$. Recall that γ is a fixed topological generator of Γ; we write $\gamma_1 = \gamma^{p-1}$ so that $\chi(\gamma_1)$ is a topological generator of $1 + p\mathbf{Z}_p$ and if G is the matrix of γ in some basis, then the matrix of γ_1 is $G_1 = G\gamma(G)\cdots\gamma^{p-2}(G)$.

Definition. — *Let $W_{k,a_p}(n)$ be the set of pairs of matrices (P,G) with $P,G \in \mathrm{M}_2(\mathcal{O}_E[\![X]\!]/(\pi_E^n, \varphi(X)^k))$ satisfying the following conditions :*

1. $P\varphi(G) = G\gamma(P)$;
2. $G = \mathrm{Id} \bmod X$;
3. $\det(P) = Q^{k-1}$ *and* $\mathrm{Tr}(P) = a_p \bmod X$;
4. *if* $\Pi(Y) = (Y-1)(Y - \chi(\gamma_1)^{k-1})$, *then* $\Pi(G_1) = 0 \bmod Q$.

If $(P,G) \in W_{k,a_p}(n)$, then we denote by $\overline{P}$ and $\overline{G}$ two matrices in $\mathrm{M}_2(k_E[\![X]\!])$ which are equal modulo $\varphi(X)^k$ to the reductions modulo π_E of P and G (note that in $k_E[\![X]\!]$, we have $\varphi(X) = X^p$). They then satisfy the relation $\overline{P}\varphi(\overline{G}) = \overline{G}\gamma(\overline{P}) \bmod \varphi(X)^k$ and in proposition 4.1 below, we prove that we can modify $\overline{G}$ modulo X^k so that $\overline{P}\varphi(\overline{G}) = \overline{G}\gamma(\overline{P})$ and that the resulting representation $\mathrm{rep}(\overline{P},\overline{G})$ does not depend on the modification.

Theorem C. — *If $n \geqslant 1$, then $W_{k,a_p}(n)$ is nonempty and there exists $n(k,a_p) \geqslant 1$ with the property that if $n \geqslant n(k,a_p)$ and if $(\overline{P},\overline{G})$ is the image of any $(P,G) \in W_{k,a_p}(n)$, then* $\mathrm{rep}(\overline{P},\overline{G})^{\mathrm{ss}} = \overline{V}^*_{k,a_p}$.

This theorem suggests the following algorithm. Choose some integer $n \geqslant 1$; since the set $\mathrm{M}_2(\mathcal{O}_E[\![X]\!]/(\pi_E^n, \varphi(X)^k))$ is finite, we can determine all the elements of $W_{k,a_p}(n)$ by checking for each pair of matrices (P,G) whether it satisfies conditions (1), (2), (3) and (4). For each pair $(P,G) \in W_{k,a_p}(n)$, we compute $\mathrm{rep}(\overline{P},\overline{G})^{\mathrm{ss}}$. If we get two different k_E-linear representations from $W_{k,a_p}(n)$ in this way, then we replace n by $n+1$; otherwise, $n = n(k,a_p)$ and $\overline{V}^*_{k,a_p} = \mathrm{rep}(\overline{P},\overline{G})^{\mathrm{ss}}$. The theorem above ensures that the algorithm terminates and returns the correct answer. In order to implement the algorithm, we need to be able to identify $\mathrm{rep}(\overline{P},\overline{G})$ given P and G and one way of doing so is explained in §5. The proof of theorem C is a simple application of the theory of Wach modules. It would be useful to have an effective bound for $n(k,a_p)$ and theorem A is probably an ingredient in the determination of such a bound.

1. Crystalline representations and Wach modules

Let Γ be the group of the introduction and let $\mathcal{A}_E$ be the π_E-adic completion of $\mathcal{O}_E[\![X]\!][1/X]$, so that $\mathcal{A}_E$ is the ring of power series $f(X) = \sum_{n\in\mathbf{Z}} a_n X^n$ with $a_n \in \mathcal{O}_E$ and $a_{-n} \to 0$ as $n \to +\infty$. The ring $\mathcal{A}_E$ is endowed with an $\mathcal{O}_E$-linear frobenius φ given by $\varphi(f)(X) = f((1+X)^p - 1)$ and an action of Γ given by $\eta(f)(X) = f((1+X)^{\chi(\eta)} - 1)$ for $\eta \in \Gamma$. An étale (φ,Γ)-module (over $\mathcal{O}_E$) is a finite type $\mathcal{A}_E$-module D endowed with a semilinear frobenius such that $\varphi(\mathrm{D})$ generates D as an $\mathcal{A}_E$-module, and a commuting semilinear continuous action of Γ. By a theorem of Fontaine (see A.3.4 of [**Fon90**]), the category of étale (φ,Γ)-modules over $\mathcal{O}_E$ is naturally isomorphic to the category of $\mathcal{O}_E$-linear representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and we denote the corresponding functor by $\mathrm{D} \mapsto V(\mathrm{D})$, and the inverse functor by $V \mapsto \mathrm{D}(V)$. If we restrict this equivalence of categories to objects killed by π_E, then we recover the equivalence described in the introduction.

An effective Wach module of height h is a free $\mathcal{O}_E[\![X]\!]$-module N of finite rank, with a frobenius φ and an action of Γ such that :

1. $\mathcal{A}_E \otimes_{\mathcal{O}_E[\![X]\!]} \mathrm{N}$ is an étale (φ,Γ)-module;
2. Γ acts trivially on $\mathrm{N}/X\mathrm{N}$;
3. $\mathrm{N}/\varphi^*(\mathrm{N})$ is killed by Q^h.

If N is a Wach module, then we can associate to it the E-linear representation $V(\mathrm{N}) = E \otimes_{\mathcal{O}_E} V(\mathcal{A}_E \otimes_{\mathcal{O}_E[\![X]\!]} \mathrm{N})$. We can also define a filtration on N by $\mathrm{Fil}^j \mathrm{N} = \{y \in \mathrm{N}$ such that $\varphi(y) \in Q^j \cdot \mathrm{N}\}$ and the E-vector space $E \otimes_{\mathcal{O}_E} \mathrm{N}/X\mathrm{N}$ then has the structure of a filtered φ-module. By combining proposition III.4.2 and theorem III.4.4 of [**Ber04**], we get the following result.

Proposition 1.1. — *If* N *is an effective Wach module of height h, then* $V(\mathrm{N})$ *is crystalline with Hodge-Tate weights in* $[-h; 0]$ *and* $\mathrm{D_{cris}}(V(\mathrm{N})) \simeq E \otimes_{\mathcal{O}_E} \mathrm{N}/X\mathrm{N}$.

All crystalline representations with Hodge-Tate weights in $[-h; 0]$ *arise in this way.*

The matrix of φ gives a well-defined equivalence class in $\mathrm{M}_d(E \otimes_{\mathcal{O}_E} \mathcal{O}_E[\![X]\!])$ and we have the following result, which follows from §III.3 of [**Ber04**].

Proposition 1.2. — *If* N *is an effective Wach module, then the elementary divisors in the ring* $E \otimes_{\mathcal{O}_E} \mathcal{O}_E[\![X]\!]$ *of the matrix of* φ *are the ideals generated by* $Q^{h_1}, \dots, Q^{h_d}$ *where* $h_1, \dots, h_d$ *are the opposites of the Hodge-Tate weights of* $V(\mathrm{N})$.

Recall that $\mathcal{O}_E[\![X]\!]/Q \simeq \mathbf{Z}_p[\zeta_p]$. The $\mathbf{Q}_p(\zeta_p)$-vector space $E \otimes_{\mathcal{O}_E} \mathrm{N}/Q\mathrm{N}$ is endowed with an action of Γ and by propositions III.2.1 and III.2.2 of [**Ber04**], we have the following.

Proposition 1.3. — *If* N *is an effective Wach module, if* $V(\mathrm{N})$ *is the associated representation viewed as a* $\mathbf{Q}_p$*-linear representation, and if* $\eta \in \Gamma$ *is such that* $\chi(\eta) \in 1 + p\mathbf{Z}_p$, *then there exists a basis of* $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{N}/Q\mathrm{N}$ *over* $\mathbf{Q}_p(\zeta_p)$ *in which the matrix of* η *is diagonal and its coefficients on the diagonal are the* $\chi(\eta)^{h_j}$ *where* $h_1, \dots, h_d$ *are the opposites of the Hodge-Tate weights of* $V(\mathrm{N})$.

If $V(\mathrm{N})$ is an E-linear representation with Hodge-Tate weights $h_1, \dots, h_d$ then the Hodge-Tate weights of the underlying $\mathbf{Q}_p$-linear representations are the h_i's each counted $[E : \mathbf{Q}_p]$ times; in particular, $\prod_{i=1}^{d}(\gamma_1 - \chi(\gamma_1)^{h_i}) = 0$ on $E \otimes_{\mathcal{O}_E} \mathrm{N}/Q\mathrm{N}$ where $\gamma_1 = \gamma^{p-1}$.

2. Local constancy with respect to a_p

In this section, we give a proof of theorem A. The main idea is to deform a Wach module, and in order to do this we need to prove a few "matrix modification" results.

Lemma 2.1. — *If* $P_0 \in \mathrm{M}_2(\mathcal{O}_E)$ *is a matrix with eigenvalues* $\lambda \neq \mu$ *and* $\delta = \lambda - \mu$, *then there exists* $Y \in \mathrm{M}_2(\mathcal{O}_E)$ *such that* $Y^{-1} \in \delta^{-1} \mathrm{M}_2(\mathcal{O}_E)$ *and* $Y^{-1} P_0 Y = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$.

Proof. — The matrix P_0 corresponds to an endomorphism f of an E-vector space such that f preserves some lattice M. Let v and w be two eigenvectors for the eigenvalues λ and μ such that v and w are in M but not in $\pi_E M$. If $x \in M$, then we can write

$x = \alpha v + \beta w$ so that $f(x) = \alpha\lambda v + \beta\mu w$ and solving for αv and βw shows that they belong to $\delta^{-1}M$. The lemma follows by taking for Y the matrix of $\{v, w\}$. □

Corollary 2.2. — *If $\alpha \geqslant 0$ and $\varepsilon \in \mathcal{O}_E$ are such that $\mathrm{val}_p(\varepsilon) \geqslant 2\,\mathrm{val}_p(\delta) + \alpha$, then there exists $H_0 \in p^\alpha \mathrm{M}_2(\mathcal{O}_E)$ such that $\det(\mathrm{Id} + H_0) = 1$ and $\mathrm{Tr}(H_0 P_0) = \varepsilon$.*

Proof. — If $y \in \mathcal{O}_E$, let $H_0 = Y \left(\begin{smallmatrix} y & -y \\ y & -y \end{smallmatrix}\right) Y^{-1}$ so that $\det(\mathrm{Id} + H_0) = 1$ and $\mathrm{Tr}(H_0 P_0) = y\delta$. If $\mathrm{val}_p(y) \geqslant \mathrm{val}_p(\delta) + \alpha$, then $H_0 \in p^\alpha \mathrm{M}_2(\mathcal{O}_E)$ so that we can have $\mathrm{Tr}(H_0 P_0) = \varepsilon$ with $y \in \mathcal{O}_E$ as soon as $\mathrm{val}_p(\varepsilon) \geqslant 2\,\mathrm{val}_p(\delta) + \alpha$. □

Let γ be a topological generator of Γ so that

$$\alpha(k) = \mathrm{val}_p\left((1 - \chi(\gamma))(1 - \chi(\gamma)^2) \cdots (1 - \chi(\gamma)^k)\right).$$

The following two propositions appear already in §10.3 of [**BB04**].

Proposition 2.3. — *If $G \in \mathrm{Id} + X\,\mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ and $k \geqslant 2$ and $H_0 \in p^{\alpha(k-1)} \mathrm{M}_2(\mathcal{O}_E)$, then there exists $H \in \mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ such that $H(0) = H_0$ and $HG = G\gamma(H) \bmod X^k$.*

Proof. — Write $H = H_0 + XH_1 + \cdots + X^{k-1}H_{k-1}$ and $G = \mathrm{Id} + XG_1 + \cdots$. We prove by induction on $r \geqslant 0$ that $H_r \in ((1-\chi(\gamma)) \cdots (1-\chi(\gamma)^r))^{-1} p^{\alpha(k-1)} \mathrm{M}_d(\mathcal{O}_E)$. If $r = 0$ this is the hypothesis and if $r \geqslant 1$, then looking at the coefficient of X^r in the equation $HG = G\gamma(H) \bmod X^k$ shows that $(1 - \chi(\gamma)^r)H_r \in ((1-\chi(\gamma)) \cdots (1-\chi(\gamma)^{r-1}))^{-1} p^{\alpha(k-1)} \mathrm{M}_d(\mathcal{O}_E)$ which completes the induction. □

Proposition 2.4. — *Let $G \in \mathrm{Id} + X\,\mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ and $P \in \mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ satsify $\det(P) = Q^{k-1}$ and $P\varphi(G) = G\gamma(P)$.*

If $H_0 \in p^{\alpha(k-1)} \mathrm{M}_2(\mathcal{O}_E)$, then there exists $G' \in \mathrm{Id} + X\,\mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ and $H \in \mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ with $H(0) = H_0$ such that if $P' = (\mathrm{Id} + H)P$, then $P'\varphi(G') = G'\gamma(P')$.

Proof. — Let H be the matrix constructed in proposition 2.3 and let $G'_k = G$ so that we have $G'_k - P'\varphi(G'_k)\gamma(P')^{-1} = X^k R_k \in X^k \mathrm{M}_d(\mathcal{O}_E[\![X]\!])$. Assume that $j \geqslant k$ and that we have a matrix G'_j such that

$$G'_j - P'\varphi(G'_j)\gamma(P')^{-1} = X^j R_j \in X^j \mathrm{M}_d(\mathcal{O}_E[\![X]\!]).$$

If $S_j \in \mathrm{M}_d(\mathcal{O}_E)$ and if we set $G'_{j+1} = G'_j + X^j S_j$, then

$$\begin{aligned} G'_{j+1} - P'\varphi(G'_{j+1})\gamma(P')^{-1} &= G'_j - P'\varphi(G'_j)\gamma(P')^{-1} + X^j S_j - P' X^j Q^j S_j \gamma(P')^{-1} \\ &= X^j (R_j + S_j - Q^{j-k+1} P' S_j Q^{k-1} \gamma(P')^{-1}), \end{aligned}$$

and we can find S_j such that $R_j + S_j - Q^{j-k+1} P' S_j Q^{k-1} \gamma(P')^{-1} \in X\,\mathrm{M}_d(\mathcal{O}_E[\![X]\!])$ since the map $S \mapsto S - p^{j-k+1} P'(0) \cdot S \cdot (Q^{k-1}\gamma(P')^{-1})(0)$ is obviously a bijection from $\mathrm{M}_d(\mathcal{O}_E)$ to itself. By induction on $j \geqslant k$, this allows us to find a sequence $(G'_j)_{j \geqslant k}$ which converges for the X-adic topology to a matrix G' satisfying $P'\varphi(G') = G'\gamma(P')$. □

Proof of theorem A. — The representation V^*_{k,a_p} is crystalline with Hodge-Tate weights 0 and $-(k-1)$. By proposition 1.1, one can attach to it an effective Wach module N_{k,a_p} of height $k-1$. If we choose a basis of N_{k,a_p} and denote by P and G the matrices of φ and $\gamma \in \Gamma$, then $P\varphi(G) = G\gamma(P)$. In addition, $G \in \mathrm{Id} + X\,\mathrm{M}_d(\mathcal{O}_E[\![X]\!])$, $\det(P) = Q^{k-1}$, $\det(P(0)) = p^{k-1}$ and $\mathrm{Tr}(P(0)) = a_p$. If $a'_p \in \mathcal{O}_E$ satisfies $\mathrm{val}_p(a_p - a'_p) \geqslant \mathrm{val}_p(a_p^2 - 4p^{k-1}) + \alpha(k-1)$, then corollary 2.2 applied to $\varepsilon = a'_p - a_p$ and proposition 2.4 give us matrices $P' = (\mathrm{Id} + H)P$ and G' which define a Wach module N' coming from a crystalline representation V'.

The matrix of φ on $\mathrm{D}_{\mathrm{cris}}(V')$ is $P'(0)$ and has determinant p^{k-1} and trace a'_p. Since $\mathrm{Id} + H$ is invertible, the matrices P and P' are equivalent and proposition 1.2 implies that the filtration on $\mathrm{D}_{\mathrm{cris}}(V')$ has weights 0 and $-(k-1)$. This shows that $\mathrm{N}' = \mathrm{N}_{k,a'_p}$. If $\mathrm{val}_p(a_p - a'_p) > \mathrm{val}_p(a_p^2 - 4p^{k-1}) + \alpha(k-1)$, then the matrices P' and G' are congruent modulo π_E to P and G so that $\overline{V}_{k,a'_p} = \overline{V}_{k,a_p}$.

Finally, note that $\mathrm{val}_p(a_p^2 - 4p^{k-1}) = 2\,\mathrm{val}_p(a_p)$ if $\mathrm{val}_p(a_p) < (k-1)/2$ and that if $\mathrm{val}_p(a_p) \geqslant (k-1)/2$, then the main result of [**BLZ04**] actually gives a better bound than $2\,\mathrm{val}_p(a_p) + \alpha(k-1)$. □

3. Local constancy with respect to k

In this section, we give a proof of theorem B. The idea is to show that V_{k,a_p} is a point in one of the families of trianguline representations constructed by Colmez in §5.1 of [**Col08**]. We start by briefly recalling Colmez' constructions, referring the reader to Colmez' article for more details.

Let $\mathcal{R}_E$ denote the Robba ring with coefficients in E. If $\delta : \mathbf{Q}_p^\times \to E^\times$ is a continuous character, then one defines a 1-dimensional (φ,Γ)-module $\mathcal{R}(\delta)$ by $\mathcal{R}(\delta) = \mathcal{R} \cdot e_\delta$ where $\varphi(e_\delta) = \delta(p)e_\delta$ and $\gamma(e_\delta) = \delta(\chi(\gamma))e_\delta$. Given two characters δ_1 and δ_2, Colmez constructs non-trivial extensions $0 \to \mathcal{R}(\delta_1) \to \mathrm{D} \to \mathcal{R}(\delta_2) \to 0$ and under certain hypothesis on δ_1 and δ_2, the 2-dimensional (φ,Γ)-module D is étale in the sense of Kedlaya (see [**Ked04**]) and therefore gives a p-adic representation $V(\delta_1,\delta_2)$ using Fontaine's construction. These representations are the trianguline representations of [**Col08**] (note that if $\delta_1\delta_2^{-1}$ is of the form x^i with $i \geqslant 0$ or $|x|x^i$ with $i \geqslant 1$, then there are several non-isomorphic possible extensions and one needs to introduce an $\mathcal{L}$-invariant; this needs not bother us).

If $y \in E^\times$, let $\mu_y : \mathbf{Q}_p^\times \to E^\times$ be the character defined by $\mu_y(p) = y$ and $\mu_y|_{\mathbf{Z}_p^\times} = 1$. Let $\chi : \mathbf{Q}_p^\times \to E^\times$ be the character defined by $\chi(p) = 1$ and $\chi(x) = x$ if $x \in \mathbf{Z}_p^\times$. The following result follows from the computations of §4.5 of [**Col08**].

Proposition 3.1. — *If $y \in \mathfrak{m}_E$ and if $k-1 > \mathrm{val}_p(y)$, then $V(\mu_y, \mu_{1/y}\chi^{1-k}) = V^*_{k,a_p}$ with $a_p = y + p^{k-1}/y$.*

We now recall Colmez' construction of families of trianguline representations. Recall first that there is a natural parameter space $\mathscr{X}$ for characters $\delta : \mathbf{Q}_p^\times \to E^\times$. Denote by $\delta(x)$ the character corresponding to a point $x \in \mathscr{X}$.

Proposition 3.2. — *If δ_1 and δ_2 are two characters as above, such that $\delta_1\delta_2^{-1}(p) \notin p^{\mathbf{Z}}$, then there exists a neighborhood $\mathscr{U}$ of $(\delta_1, \delta_2) \in \mathscr{X}^2$ and a free $\mathcal{O}_{\mathscr{U}}$-module V of rank 2 with an action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $V(u) = V(\delta_1(u), \delta_2(u))$ if $u \in \mathscr{U}$.*

Proof of theorem B. — If $k-1 > \mathrm{val}_p(a_p)$, put $\delta_1 = \mu_{a_p}$ and $\delta_2 = \mu_{1/a_p}\chi^{1-k}$ so that $V(\delta_1, \delta_2) = V^*_{k,a_p+p^{k-1}/a_p}$ by proposition 3.1. Theorem A implies that if $\mathrm{val}_p(p^{k-1}/a_p) > 2 \cdot \mathrm{val}_p(a_p) + \alpha(k-1)$, then $\overline{V}(\delta_1, \delta_2) = \overline{V}^*_{k,a_p}$. Proposition 3.2 implies the existence of a neighborhood $\mathscr{U}$ of $(\delta_1, \delta_2) \in \mathscr{X}^2$ such that $\overline{V}(\delta_1(u), \delta_2(u))$ is constant. This implies that there exists m such that $\overline{V}^*_{k',a_p} = \overline{V}^*_{k,a_p}$ if $k' \geqslant k$ and $k' - k \in p^{m-1}(p-1)\mathbf{Z}$ and this finishes the proof of theorem B. $\square$

4. The algorithm for computing the reduction

We start by giving a proof of the main technical result which is used in order to justify that it is enough to work with truncations of (φ, Γ)-modules.

Proposition 4.1. — *If $1 \leqslant n \leqslant +\infty$ and P and G_k are two matrices in $\mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$ such that $\det(P) = Q^{k-1} \times \text{unit}$ and $G_k = \mathrm{Id} \bmod X$ and $P\varphi(G_k) = G_k\gamma(P) \bmod \varphi(X)^k$, then :*

1. *there exists $G \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$ such that $G = G_k \bmod X^k$ and $P\varphi(G) = G\gamma(P)$;*
2. *if P' and G' are two matrices equal to P and G modulo $\varphi(X)^k$ and X^k and satisfying the same conditions as P and G, then $\mathrm{rep}(P', G') = \mathrm{rep}(P, G)$.*

Proof. — We start by proving (1). Since $\det(P) = Q^{k-1} \times \text{unit}$, the same is true of $\det(\gamma(P))$ and hence we have $Q^{k-1}\gamma(P)^{-1} \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$. We can therefore rewrite $P\varphi(G_k) = G_k\gamma(P) \bmod \varphi(X)^k$ as

$$G_k - P\varphi(G_k)\gamma(P)^{-1} \in X^k Q\, \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!]),$$

since this is true after multiplying by Q^{k-1} and Q is not a zero divisor in $\mathcal{O}_E/\pi_E^n[\![X]\!]$. Assume that $j \geqslant k$ and that we have a matrix G_j such that

$$G_j - P\varphi(G_j)\gamma(P)^{-1} = X^j R_j \in X^j\, \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!]).$$

If $S_j \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ and if we set $G_{j+1} = G_j + X^j S_j$, then

$$\begin{aligned} G_{j+1} - P\varphi(G_{j+1})\gamma(P)^{-1} &= G_j - P\varphi(G_j)\gamma(P)^{-1} + X^j S_j - PX^j Q^j S_j \gamma(P)^{-1} \\ &= X^j(R_j + S_j - Q^{j-k+1} P S_j Q^{k-1}\gamma(P)^{-1}), \end{aligned}$$

and we can find S_j such that $R_j + S_j - Q^{j-k+1} P S_j Q^{k-1}\gamma(P)^{-1} \in X\,\mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$ since the map $S \mapsto S - p^{j-k+1}P(0)\cdot S\cdot(Q^{k-1}\gamma(P)^{-1})(0)$ is obviously a bijection from $\mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ to itself. By induction on $j \geqslant k$, this allows us to find a sequence $(G_j)_{j\geqslant k}$ which converges for the X-adic topology to a matrix G satisfying (1).

In order to prove (2), we start by showing that there exists a matrix $M \in \mathrm{GL}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$ such that $M^{-1}P'\varphi(M) = P$. We have by hypothesis $P' = P + \varphi(X)^k S$ and hence $P' = (1 + X^k R)P$ with $R = SQ^k P^{-1}$. By induction and successive approximations, we only need to show that if $P' = (1 + X^j R_j)P$ with $j \geqslant k$, then there exists $T_j \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ such that $(1 + X^j T_j)^{-1} P' \varphi(1 + X^j T_j) = (1 + X^{j+1} R_{j+1})P$. We have

$$\begin{aligned} &(1 + X^j T_j)^{-1} \cdot (1 + X^j R_j) \cdot P \cdot \varphi(1 + X^j T_j) \\ &\qquad = (1 + X^j(R_j - T_j + Q^{j-k+1} P T_j Q^{k-1} P^{-1}) + \mathrm{O}(X^{j+1})) \cdot P \end{aligned}$$

and the claim follows from the fact that $T \mapsto T - p^{j-k+1}P(0)\cdot T\cdot(Q^{k-1}P^{-1})(0)$ is obviously a bijection from $\mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ to itself. In order to prove (2), we are therefore reduced to the case $P = P'$. If we set $H = G'G^{-1}$, then the two equations $P\varphi(G) = G\gamma(P)$ and $P\varphi(G') = G'\gamma(P)$ give $P\varphi(H) = HP$, with $H = \mathrm{Id} \bmod X^k$. Let $H_0 = H$ and set $H_{m+1} = P\varphi(H_m)P^{-1}$. Since $H = \mathrm{Id} \bmod X^k$, we can write $H_0 = \mathrm{Id} + X^{k-1}\varphi^0(X)R_0$ and an easy induction shows that we can write $H_m = \mathrm{Id} + X^{k-1}\varphi^m(X)R_m$ with $R_m \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[\![X]\!])$ so that $H_m \to \mathrm{Id}$ as $m \to +\infty$. The equation $P\varphi(H) = HP$ implies that $H_m = H$ for all $m \geqslant 0$ and we are done. □

We now give a proof of theorem C, which we recall here.

Theorem 4.2. — *If $n \geqslant 1$, then $W_{k,a_p}(n)$ is nonempty and there exists $n(k,a_p) \geqslant 1$ with the property that if $n \geqslant n(k,a_p)$ and if $(\overline{P},\overline{G})$ is the image of any $(P,G) \in W_{k,a_p}(n)$, then* $\mathrm{rep}(\overline{P},\overline{G})^{\mathrm{ss}} = \overline{V}^*_{k,a_p}$.

Proof. — The representation V^*_{k,a_p} is a crystalline representation with Hodge-Tate weights $-(k-1)$ and 0 so that by proposition 1.1, there exists an effective Wach module N_{k,a_p} of height $k-1$ with the property that $V(\mathrm{N}_{k,a_p}) \simeq V^*_{k,a_p}$. If P and G are the matrices of φ and γ in some basis of N_{k,a_p} then they obviously satisfy the equation $P\varphi(G) = G\gamma(P)$ and $G = \mathrm{Id} \bmod X$ by definition. The determinant of V^*_{k,a_p} is χ^{k-1} so that $\det(P) = Q^{k-1} \times u$ with $u \in 1 + X\mathcal{O}_E[\![X]\!]$. The map $v \mapsto \varphi(v)/v$ from $1 + X\mathcal{O}_E[\![X]\!]$ to itself is a bijection and since $p \neq 2$, every element of $1 + X\mathcal{O}_E[\![X]\!]$ has a square root. We can therefore modify

P and G accordingly so that $\det(P) = Q^{k-1}$. The fact that $\mathrm{D}_{\mathrm{cris}}(V^*_{k,a_p}) = D_{k,a_p} = E \otimes_{\mathcal{O}_E} \mathrm{N}_{k,a_p}/X\mathrm{N}_{k,a_p}$ implies that $\mathrm{Tr}(P) = a_p \bmod X$. Finally by proposition 1.3, the operator $(\gamma_1 - 1)(\gamma_1 - \chi(\gamma_1)^{k-1})$ is zero on $E \otimes_{\mathcal{O}_E} \mathrm{N}_{k,a_p}/Q\mathrm{N}_{k,a_p}$ so that if $G_1 = G\gamma(G)\cdots\gamma^{p-2}(G)$ and $\Pi(Y) = (Y-1)(Y-\chi(\gamma_1)^{(k-1)})$, then $\Pi(G_1) = 0 \bmod Q$. This shows that the images of P and G in $\mathrm{M}_2(\mathcal{O}_E[\![X]\!]/(\pi_E^n, \varphi(X)^k))$ belong to $W_{k,a_p}(n)$ for all $n \geqslant 1$ so that $W_{k,a_p}(n)$ is nonempty.

We now prove the existence of $n(k, a_p)$. There are only finitely many semisimple k_E-linear 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ so that if for infinitely many n there exists $(P, G) \in W_{k,a_p}(n)$ whose image $(\overline{P}, \overline{G})$ satisfies $\mathrm{rep}(\overline{P}, \overline{G})^{\mathrm{ss}} \neq \overline{V}^*_{k,a_p}$ then there exists some semisimple k_E-linear 2-dimensional representation U of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ which arises from $(P, G) \in W_{k,a_p}(n)$ for infinitely many n's. By a standard compacity argument (recall that the $W_{k,a_p}(n)$ are finite sets), this implies that we can find a compatible sequence $(P_n, G_n)_{n\geqslant 1}$ with each term "reducing mod π_E" to U. The P_n and the G_n converge to P and G in $\mathrm{M}_2(\mathcal{O}_E[\![X]\!])$ and P and G still satisfy conditions (1), (2), (3) and (4) of the definition of $W_{k,a_p}(n)$ since these conditions are continuous. In particular, conditions (1), (2) and the first part of (3) imply that P and G define a Wach module, which then comes from a crystalline representation V. Condition (3) then implies that $\mathrm{D}_{\mathrm{cris}}(V) \simeq D_{k,a_p}$ as φ-modules while condition (4) along with proposition 1.3 implies that the Hodge-Tate weights of V belong to $\{0; -(k-1)\}$. The fact that $\mathrm{D}_{\mathrm{cris}}(V) \simeq D_{k,a_p}$ implies that the sum of the weights is $-(k-1)$ so that $\mathrm{D}_{\mathrm{cris}}(V) \simeq D_{k,a_p}$ as filtered φ-modules and hence $V \simeq V^*_{k,a_p}$. But then $U = \overline{V}^{\mathrm{ss}} = \overline{V}^*_{k,a_p}$ which is a contradiction. This shows the existence of $n(k, a_p)$ and finishes the proof of the theorem. □

5. Identifying mod p representations

If P and G are two matrices in $\mathrm{M}_2(k_E[\![X]\!])$ such that $\det(P) = Q^{k-1} \times$ unit and $G = \mathrm{Id} \bmod X$ and $P\varphi(G) = G\gamma(P) \bmod \varphi(X)^k$, then by proposition 4.1 there is a well-defined k_E-linear representation $\mathrm{rep}(P, G)$ associated to P and G. In this section, we give a crude method for determining which one it is.

Recall that if V is a k_E-linear representation of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, then by B.1.4 of [**Fon90**] there is a $k_E[\![X]\!]$-lattice $\mathrm{D}^+(V)$ inside $\mathrm{D}(V)$ which is stable under φ and the action of Γ and such that any other such lattice N satisfies $\mathrm{N} \subset \mathrm{D}^+(V)$. If M is the matrix of a basis of N in a basis of $\mathrm{D}^+(V)$ then $\det(\varphi|\mathrm{N}) = \det(\varphi|\mathrm{D}^+(V)) \cdot \varphi(\det(M))/\det(M)$. In particular, if $\det(\varphi|\mathrm{N})$ is $Q^{k-1} \times$ unit then $\det(M)$ divides X^{k-1}. The algorithm for determining $\mathrm{rep}(P, G)$ is then the following :

1. make a list of all the k_E-linear 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$;

2. for each of them, compute P and G, the matrices of φ and γ on $\mathrm{D}^+(V)$ to precision $X^{(p+1)k+k-1}$;
3. make a list of all the $M^{-1}P\varphi(M)$ and $M^{-1}G\gamma(M)$ for the finitely many $M \in \mathrm{M}_2(k_E[\![X]\!]/X^{(p+1)k+k-1})$ such that $\det(M)$ divides X^{k-1}

Step (2) is an interesting exercise in (φ, Γ)-modules. Note also that in step (3) we need to multiply by M^{-1} so that the precision drops from $X^{(p+1)k+k-1}$ to $X^{(p+1)k} = \varphi(X)^k$. This procedure gives a complete list of all possible (P, G) with the corresponding representation and given a pair (P, G), the representation $\mathrm{rep}(P, G)$ can then be determined by a simple table lookup.

References

[BB04] L. Berger & C. Breuil – "Towards a p-adic Langlands programme", Summer School on p-adic Arithmetic Geometry, Hangzhou, August 2004.

[Ber04] L. Berger – "Limites de représentations cristallines", *Compos. Math.* **140** (2004), no. 6, p. 1473–1498.

[Ber09] ———, "A p-adic family of dihedral (φ, Γ)-modules", preprint, 2009.

[Ber10] ———, "Représentations modulaires de $\mathrm{GL}_2(\mathbf{Q}_p)$ et représentations galoisiennes de dimension 2", *Astérisque* (2010), no. 330, p. 263–279.

[BG09] K. Buzzard & T. Gee – "Explicit reduction modulo p of certain two-dimensional crystalline representations", *Int. Math. Res. Not. IMRN* (2009), no. 12, p. 2303–2317.

[BLZ04] L. Berger, H. Li & H. J. Zhu – "Construction of some families of 2-dimensional crystalline representations", *Math. Ann.* **329** (2004), no. 2, p. 365–377.

[Bre03] C. Breuil – "Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbf{Q}_p)$. II", *J. Inst. Math. Jussieu* **2** (2003), no. 1, p. 23–58.

[CF00] P. Colmez & J.-M. Fontaine – "Construction des représentations p-adiques semistables", *Invent. Math.* **140** (2000), no. 1, p. 1–43.

[Col08] P. Colmez – "Représentations triangulines de dimension 2", *Astérisque* (2008), no. 319, p. 213–258.

[Dou10] G. Dousmanis, "On reductions of families of crystalline Galois representations", preprint, 2010.

[Fon90] J.-M. Fontaine – "Représentations p-adiques des corps locaux. I", The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, p. 249–309.

[Ked04] K. S. Kedlaya – "A p-adic local monodromy theorem", *Ann. of Math. (2)* **160** (2004), no. 1, p. 93–184.

September 2010

Laurent Berger, UMPA ENS de Lyon, UMR 5669 du CNRS, Université de Lyon
E-mail : `laurent.berger@ens-lyon.fr` • *Url :* `www.umpa.ens-lyon.fr/~lberger/`