JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Tong LIU

The correspondence between Barsotti-Tate groups and Kisin modules when $p = 2$

Tome 25, n° 3 (2013), p. 661-676.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_3_661_0>

Journal de Théorie des Nombres de Bordeaux **25** (2013), 661–676

The correspondence between Barsotti-Tate groups and Kisin modules when $p = 2$

par Tong LIU

Résumé. Soit K une extension finie de $\mathbb{Q}_2$ d'anneau des entiers $\mathcal{O}_K$. Dans cet article, on construit une équivalence de catégories entre la catégorie des modules de Kisin de hauteur 1 et la catégorie des groupes de Barsotti-Tate sur $\mathcal{O}_K$.

Abstract. Let K be a finite extension over $\mathbb{Q}_2$ and $\mathcal{O}_K$ the ring of integers. We prove the equivalence of categories between the category of Kisin modules of height 1 and the category of Barsotti-Tate groups over $\mathcal{O}_K$.

Contents

1. Introduction

Let k be a perfect field of characteristic p, with $W(k)$ the ring of Witt vectors of k and $K_0 = W(k)[\frac{1}{p}]$. Let K/K_0 be a finite totally ramified extension with a fixed algebraic closure $\overline{K}$ of K and $G := \mathrm{Gal}(\overline{K}/K)$. The aim of this paper is to prove the equivalence between the category of Barsotti-Tate groups over $\mathcal{O}_K$ and the category of Kisin modules of height 1 when $p = 2$.

Manuscrit reçu le 11 juin 2012.
The author is partially supported by NSF grant DMS-0901360.
Classification math. 14F30, 14L05.

More precisely, let $E(u)$ be an Eisenstein polynomial for a fixed uniformizer π of K, $K_\infty = \bigcup\limits_{n\geq 1} K(\sqrt[p^n]{\pi})$, $G_\infty = \mathrm{Gal}(\overline{K}/K_\infty)$ and $\mathfrak{S} = W(k)[\![u]\!]$. We equip $\mathfrak{S}$ with the semi-linear endomorphism φ which acts via Frobenius on $W(k)$, and sends u to u^p. Let $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ denote the category of finite free $\mathfrak{S}$-modules $\mathfrak{M}$ equipped with a φ-semi-linear map $\varphi_\mathfrak{M} : \mathfrak{M} \to \mathfrak{M}$ such that the cokernel of the $\mathfrak{S}$-linear map $1 \otimes \varphi_\mathfrak{M} : \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$ is killed by $E(u)$. Objects in $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ are called *φ-modules of $E(u)$-height* 1 or *Kisin modules* of height 1[1]. The main result proved in this note is the following:

Theorem 1.0.1. *There exists an equivalence between the category of Barsotti-Tate groups over $\mathcal{O}_K$ and the category of Kisin modules of height 1.*

The theorem was first conjectured by Breuil [1]. If $p > 2$ then the above theorem was proved in [10]. In [11], the equivalence between the category of connected Barsotti-Tate groups over $\mathcal{O}_K$ and a certain subcategory of Kisin modules of height 1 was established when $p = 2$. So we focus on the case $p = 2$ in this paper though our method works for all primes p.

Let us sketch the idea of the proof of the main theorem. Let $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$ denote the category of G-stable $\mathbb{Z}_p$-lattices in crystalline representations with Hodge-Tate weights in $\{0, 1\}$. By Fontaine [6], Kisin [10], Raynaud [17] and Tate [18], it is known that the category of Barsotti-Tate groups over $\mathcal{O}_K$ is equivalent to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$ (see Theorem 2.2.1). Therefore we need to establish the equivalence between the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ and the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$. For an object $\mathfrak{M} \in \mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$, we can associate a $\mathbb{Z}_p[G_\infty]$-module $T_\mathfrak{S}(\mathfrak{M}) := \mathrm{Hom}_{\varphi,\mathfrak{S}}(\mathfrak{M}, W(R))$ (see Section 2.1 for more details). In [10], Kisin proved that the G_∞-action on $V_\mathfrak{S}(\mathfrak{M}) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_\mathfrak{S}(\mathfrak{M})$ can be extended to a G-action such that $V_\mathfrak{S}(\mathfrak{M})$ is crystalline with Hodge-Tate weights in $\{0, 1\}$. It is not hard to prove that if $T_\mathfrak{S}(\mathfrak{M})$ is G-stable in $V_\mathfrak{S}(\mathfrak{M})$ then the functor $\mathfrak{M} \rightsquigarrow T_\mathfrak{S}(\mathfrak{M})$ establishes an anti-equivalence from the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$.

To prove that $T_\mathfrak{S}(\mathfrak{M})$ is G-stable in $V_\mathfrak{S}(\mathfrak{M})$, we use the idea developed in [5]. We embed $T_\mathfrak{S}(\mathfrak{M})$ into $J(\mathfrak{M}) := \mathrm{Hom}_{\varphi,\mathfrak{S}}(\mathfrak{M}, W(R)/utW(R))$ which is constructed in Section 3.1 and has a natural G-action. It turns out that $T_\mathfrak{S}(\mathfrak{M})$ is G-stable in $J(\mathfrak{M})$ and the G-action obtained from $J(\mathfrak{M})$ is compatible with the G-action on $V_\mathfrak{S}(\mathfrak{M})$ via Kisin's construction, from which we deduce the main theorem.

[1] One may define Kisin modules of height r, which are very useful in the study of semi-stable representation with Hodge-Tate weights in $\{0, \dots, r\}$. But we are only concern with Kisin modules of height 1 in this paper.

When this paper was nearly complete, we learned of the preprints [9], [13] in which W. Kim and E. Lau have independently proved Theorem 1.0.1. Here we comment that we use totally different approaches and methods from those used by Kim and Lau. More precisely, Lau extended Zink's theory of windows and displays which allows him to also obtain the classification of 2-divisible group over more general base rings. However his theory does not provide the proof that $T_{\mathfrak{S}}(\mathfrak{M}) \simeq T_p(H)$ where $T_p(H)$ is the Tate module of the 2-divisible group H corresponding to $\mathfrak{M}$. Kim uses a similar idea to ours but our methods are different: Kim proves that $T_{\mathfrak{S}}(\mathfrak{M})$ is G-stable in $V_{\mathfrak{S}}(\mathfrak{M})$ by some explicit calculations only for $p = 2$, while we directly construct a natural G-action on $T_{\mathfrak{S}}(\mathfrak{M})$ which is compatible with that of $V_{\mathfrak{S}}(\mathfrak{M})$, and this works for all primes p. Of course, Kim also proved that $S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \simeq \mathbb{D}(H)(S)$ where S is the ring defined and discussed in §2.1 and $\mathbb{D}(H)$ is the Dieudonné crystal attached to H. Unfortunately, we can not provide a new proof for this fact in the present paper.

Acknowledgment: It is a pleasure to thank Christophe Breuil, Wansu Kim and Mark Kisin for very useful correspondences during the preparation of this paper. We are grateful to the anonymous referee for lots of useful comments, which have improved the exposition of this paper.

Notations 1.0.2. We define various Frobenius and monodromy (derivation) structures on different rings and modules. The symbols φ and N are reserved to denote Frobenius and monodromy operators respectively. We sometimes add subscripts to indicate on which object Frobenius or monodromy is defined. For example, $\varphi_{\mathfrak{M}}$ is the Frobenius defined on $\mathfrak{M}$. We always drop these subscripts if no confusion will arise. We write $\gamma_i(x)$ the standard divided power "$\frac{x^i}{i!}$" when it exists.

2. Preliminaries and Preparations

In first 2 subsections, we recall some facts and notations involved in the main theorem. The last subsection reduces the proof of the main theorem to Proposition 2.3.1, which will be proved in the next section.

2.1. Kisin modules and $(\varphi, \hat{G})$-modules. In this subsection, we recall some standard notations, definitions and results from [10] and [16]. The reader may consult these papers for more details.

Recall that k is a perfect field of characteristic p with ring of Witt vectors $W(k)$, $K_0 = W(k)[\frac{1}{p}]$ and K/K_0 is a finite totally ramified extension. Throughout this paper we fix a uniformiser $\pi \in K$ with Eisenstein polynomial $E(u)$. Recall that $\mathfrak{S} = W(k)[\![u]\!]$ is equipped with a Frobenius endomorphism φ via $u \mapsto u^p$ and the natural Frobenius on $W(k)$. A *φ-module* (over $\mathfrak{S}$) is an $\mathfrak{S}$-module $\mathfrak{M}$ equipped with a $\varphi_{\mathfrak{S}}$-semi-linear map $\varphi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$. A morphism between two φ-modules $(\mathfrak{M}_1, \varphi_1)$, $(\mathfrak{M}_2, \varphi_2)$ is an $\mathfrak{S}$-linear map compatible with the φ_i. Recall that $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ denotes the category of *φ-modules of $E(u)$-height* 1 in the sense that $\mathfrak{M}$ is finite free over $\mathfrak{S}$ and the cokernel of φ^* is killed by $E(u)$, where φ^* is the $\mathfrak{S}$-linear map $1 \otimes \varphi : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$. Objects of $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ are also called *Kisin modules* of height 1.

We denote by S the p-adic completion of the divided power envelope of $W(k)[u]$ with respect to the ideal generated by $E(u)$. Write $S_{K_0} := S[\frac{1}{p}]$. There is a unique continuous (for the p-adic topology) map (Frobenius) $\varphi : S \to S$ which extends the Frobenius on $\mathfrak{S}$. We write N_S for the K_0-linear derivation on S_{K_0} such that $N_S(u) = -u$.

Let $R = \varprojlim \mathcal{O}_{\overline{K}}/p$ where the transition maps are given by Frobenius. There exists a unique surjective projection map $\theta : W(R) \to \widehat{\mathcal{O}}_{\overline{K}}$ to the p-adic completion of $\mathcal{O}_{\overline{K}}$, which lifts the projection $R \to \mathcal{O}_{\overline{K}}/p$ onto the first factor in the inverse limit. We denote by A_{cris} the p-adic completion of the divided power envelope of $W(R)$ with respect to $\mathrm{Ker}(\theta)$. Let $\pi_n \in \overline{K}$ be a p^n-th root of π, such that $(\pi_{n+1})^p = \pi_n$. Write $\underline{\pi} = (\pi_n)_{n \geq 0} \in R$ and let $[\underline{\pi}] \in W(R)$ be the Techmüller representative. We embed the $W(k)$-algebra $W(k)[u]$ into $W(R) \subset A_{\mathrm{cris}}$ by the map $u \mapsto [\underline{\pi}]$. This embedding extends to embeddings $\mathfrak{S} \hookrightarrow S \hookrightarrow A_{\mathrm{cris}}$ which are compatible with Frobenius endomorphisms. We denote by B^+_{dR} the $\mathrm{Ker}(\theta)$-adic completion of $W(R)[1/p]$. For any subring $A \subset B^+_{\mathrm{dR}}$, we define a filtration on A by $\mathrm{Fil}^i A = A \cap (\mathrm{Ker}(\theta))^i B^+_{\mathrm{dR}} = A \cap (E(u)^i) B^+_{\mathrm{dR}}$. As usual, we denote $A_{\mathrm{cris}}[\frac{1}{p}]$ by B^+_{cris}.

We fix a choice of *primitive* p^i-root of unity ζ_{p^i} for $i \geq 0$ and set $\underline{\epsilon} := (\zeta_{p^i})_{i \geq 0} \in R$ and $t := \log([\underline{\epsilon}]) \in A_{\mathrm{cris}}$. For any $g \in G$, write $\underline{\epsilon}(g) := \frac{g(\underline{\pi})}{\underline{\pi}}$, which is a cocycle from G to R^*. We see that $g(t) = \chi(g)t$ with χ the p-adic cyclotomic character, and there exists an $\alpha(g) \in \mathbb{Z}_p$ such that $\log([\underline{\epsilon}(g)]) = \alpha(g)t$. Recall $K_\infty := \bigcup\limits_{n=0}^{\infty} K(\pi_n)$ and $G_\infty := \mathrm{Gal}(\overline{K}/K_\infty)$. We set $\hat{K} = \bigcup\limits_{n=1}^{\infty} K_\infty(\zeta_{p^n})$ and $\hat{G} := \mathrm{Gal}(\hat{K}/K)$.

As a subring of A_{cris}, S is not stable under the action of G, though S is fixed by G_∞. Define

$$\mathcal{R}_{K_0} := \left\{ x = \sum_{i=0}^{\infty} f_i t^{\{i\}}, f_i \in S_{K_0} \text{ and } f_i \to 0 \ p\text{-adically as } i \to +\infty \right\},$$

where $t^{\{i\}} = \frac{t^i}{p^{\tilde{q}(i)} \tilde{q}(i)!}$ and $\tilde{q}(i)$ satisfies $i = \tilde{q}(i)(p-1) + r(i)$ with $0 \leq r(i) < p-1$. Set $\widehat{\mathcal{R}} := W(R) \cap \mathcal{R}_{K_0}$. One can show that $\mathcal{R}_{K_0}$ and $\widehat{\mathcal{R}}$ are stable under the G-action as subrings of B^+_{cris} and the G-action factors through $\hat{G}$ (see [16] §2.2). Moreover, R is a valuation ring. Write $v_R(\cdot)$ for the valuation and let $I_+R = \{x \in R | v_R(x) > 0\}$ be the maximal ideal of R. Set $I_+ := \widehat{\mathcal{R}} \cap W(I_+R)$. By Lemma 2.2.1 in [16], one has $\widehat{\mathcal{R}}/I_+ \simeq W(k)$.

Following [16], a $(\varphi, \hat{G})$-*module of height* 1 is a triple $(\mathfrak{M}, \varphi, \hat{G})$ where

1. $(\mathfrak{M}, \varphi_{\mathfrak{M}})$ is a Kisin module of height 1;
2. $\hat{G}$ is a $\widehat{\mathcal{R}}$-semi-linear $\hat{G}$-action on $\hat{\mathfrak{M}} := \widehat{\mathcal{R}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$;
3. $\hat{G}$ commutes with $\varphi_{\hat{\mathfrak{M}}}$ on $\hat{\mathfrak{M}}$, *i.e.,* for any $g \in \hat{G}$, $g\varphi_{\hat{\mathfrak{M}}} = \varphi_{\hat{\mathfrak{M}}} g$;
4. regard $\mathfrak{M}$ as a $\varphi(\mathfrak{S})$-submodule in $\hat{\mathfrak{M}}$, then $\mathfrak{M} \subset \hat{\mathfrak{M}}^{H_K}$, where $H_K := \mathrm{Gal}(\hat{K}/K_\infty)$;
5. $\hat{G}$ acts on the $W(k)$-module $M := \hat{\mathfrak{M}}/I_+\hat{\mathfrak{M}} \simeq \mathfrak{M}/u\mathfrak{M}$ trivially.

A morphism between two $(\varphi, \hat{G})$-modules is a morphism in $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ that commutes with the $\hat{G}$-action on $\hat{\mathfrak{M}}$'s. For a $(\varphi, \hat{G})$-module $\hat{\mathfrak{M}} = (\mathfrak{M}, \varphi, \hat{G})$, we can associate a $\mathbb{Z}_p[G]$-module:

$$\hat{T}(\hat{\mathfrak{M}}) := \mathrm{Hom}_{\widehat{\mathcal{R}}, \varphi}(\widehat{\mathcal{R}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}, W(R)), \tag{2.1.1}$$

where G acts on $\hat{T}(\hat{\mathfrak{M}})$ via $g(f)(x) = g(f(g^{-1}(x)))$ for any $g \in G$ and $f \in \hat{T}(\hat{\mathfrak{M}})$.

For any $\mathfrak{M} \in \mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$, we can associate a $\mathbb{Z}_p[G_\infty]$-module by

$$T_{\mathfrak{S}}(\mathfrak{M}) := \mathrm{Hom}_{\varphi, \mathfrak{S}}(\mathfrak{M}, W(R)).$$

One can show that $T_{\mathfrak{S}}(\mathfrak{M})$ is finite $\mathbb{Z}_p$-free and of $\mathrm{rank}_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M}) = \mathrm{rank}_{\mathfrak{S}} \mathfrak{M}$ (see for example Corollary (2.1.4) in [10]). Let $\mathrm{Rep}_{\mathbb{Z}_p}[G_\infty]$ denote the category of continuous G_∞-representations on finite free $\mathbb{Z}_p$-modules. The functor $T_{\mathfrak{S}}$ from $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to $\mathrm{Rep}_{\mathbb{Z}_p}[G_\infty]$ is fully faithful (see Proposition (2.1.12) in [10] or Corollary 4.2.6 in [14]).

Remark 2.1.1. Usually, $T_{\mathfrak{S}}(\mathfrak{M})$ is defined as $\mathrm{Hom}_{\varphi, \mathfrak{S}}(\mathfrak{M}, \mathfrak{S}^{\mathrm{ur}})$ in [10] or [16], where $\mathfrak{S}^{\mathrm{ur}}$ is a subring of $W(R)$. But Lemma 2.2.1 in [5] shows that these two definitions are equivalent.

We refer readers to [8] for definitions and basic facts on semi-stable representations and crystalline representations. The following summarizes the main result of [16] on G-stable $\mathbb{Z}_p$-lattices in semi-stable representations.

Theorem 2.1.2. (1) *Let* $\hat{\mathfrak{M}} := (\mathfrak{M}, \varphi, \hat{G})$ *be a* $(\varphi, \hat{G})$*-module. There is a natural isomorphism of* $\mathbb{Z}_p[G_\infty]$*-modules* $\theta : T_{\mathfrak{S}}(\mathfrak{M}) \xrightarrow{\sim} \hat{T}(\hat{\mathfrak{M}})$.

(2) $\hat{T}$ *induces an anti-equivalence between the category of* $(\varphi, \hat{G})$*-modules of height* 1 *and the category of* G*-stable* $\mathbb{Z}_p$*-lattices in semi-stable representations with Hodge-Tate weights in* $\{0, 1\}$.

The isomorphism θ in Theorem 2.1.2 (1) is defined as the following:

$$\theta(f)(a \otimes x) := a\varphi(f(x)), \quad \forall f \in T_{\mathfrak{S}}(\mathfrak{M}),\ \forall a \in \widehat{\mathcal{R}},\ \forall x \in \mathfrak{M}. \tag{2.1.2}$$

Remark 2.1.3. Here we only care about crystalline representations with Hodge-Tate weights in $\{0,1\}$ while the main result in [16] deals with $(\varphi, \hat{G})$-module of height r and lattices in semi-stable representations with Hodge-Tate weights in $\{0,\dots,r\}$.

2.2. Barsotti-Tate groups and lattices in crystalline representations. For the generalities of Barsotti-Tate groups over $\mathcal{O}_K$, we refer [18] and the appendix of [10] for details. Let $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Q}_p}$ denote the category of crystalline representations of G with Hodge-Tate weights in $\{0,1\}$ and $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$ denote the category of G-stable $\mathbb{Z}_p$-lattices in objects in $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Q}_p}$. Morphisms in $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$ are morphisms of $\mathbb{Z}_p[G]$-modules. Let H be a Barsotti-Tate group over $\mathcal{O}_K$. We denote by $T_p(H)$ the p-adic Tate module of H and by $V_p(H) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(H)$. We summarize several important results on Barsotti-Tate groups and crystalline representations into the following theorem.

Theorem 2.2.1 (Fontaine, Kisin, Raynaud, Tate)**.** *The functor $H \rightsquigarrow T_p(H)$ induce an equivalence between the category of Barsotti-Tate groups over $\mathcal{O}_K$ and the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$.*

Proof. Fontaine ([6]) proved that $V_p(H)$ is crystalline with Hodge-Tate weights in $\{0,1\}$. Hence we have a functor $H \rightsquigarrow T_p(H)$ from the category of Barsotti-Tate groups over $\mathcal{O}_K$ to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$. The functor is fully faithful by Tate's isogeny theorem in [18]. The proof for essentially surjectiveness of the functor needs two ingredients. First, Corollary (2.2.6) in [11] shows that for each crystalline representation V of G with Hodge-Tate weights in $\{0,1\}$ there exists a Barsotti-Tate group H such that $V_p(H) \simeq V$. Then any G-stable $\mathbb{Z}_p$-lattice T inside V can be seen as a lattice in $V_p(H)$ and then there must exist a Barsotti-Tate group H' such that $T_p(H') \simeq T$ by the trick of scheme-theoretic closure of finite flat group schemes and Proposition 2.3.1 in [17].

□

Proposition 2.2.2. *There exists an functor ι from the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Q}_p}$ and ι induces an anti-equivalence on the corresponding isogeny category.*

The above proposition was proved in [10] (see Proposition (2.2.2) in [10]). Here we use a slightly different approach which will be useful later. Let $\mathrm{Fil}^1 S$ denote the ideal in S generated by $\frac{E(u)^i}{i!}$ for $i \geq 1$. Note that $\varphi(\mathrm{Fil}^1 S) \subset pS$ and write $\varphi_1 = \varphi/p : \mathrm{Fil}^1 S \to S$. A *Breuil module* is a quadruple $(\mathcal{M}, \mathrm{Fil}^1\mathcal{M}, \varphi_1, N)$ where

(1) $\mathcal{M}$ is a finite free S-module;

(2) $\mathrm{Fil}^1\mathcal{M}$ is a submodule of $\mathcal{M}$ such that $\mathrm{Fil}^1 S\mathcal{M} \subset \mathrm{Fil}^1\mathcal{M}$ and $\mathcal{M}/\mathrm{Fil}^1\mathcal{M}$ is finite free over $\mathcal{O}_K$;

(3) $\varphi_1 : \mathrm{Fil}^1\mathcal{M} \to \mathcal{M}$ is a φ_S-semi-linear map such that $\varphi_1(\mathrm{Fil}^1\mathcal{M})$ generates $\mathcal{M}$ and $\varphi_1(sm) = (c_1)^{-1}\varphi_1(s)\varphi_1(E(u)m)$ for $s \in \mathrm{Fil}^1 S$ and $m \in \mathcal{M}$ with $c_1 = \varphi_1(E(u)) \in S^*$;

(4) $N : \mathcal{M} \to \mathcal{M}$ is a $W(k)$-linear map such that $N(sm) = N_S(s)m + sN(m)$ for $s \in S$ and $m \in \mathcal{M}$ and $\varphi_1(E(u)N(x)) = c_1 N(\varphi_1(x))$ for $x \in \mathrm{Fil}^1\mathcal{M}$.

The operator N is always called the *monodromy* operator. A morphism between two Breuil modules is just an S-linear map that preserves Fil^1 and commutes with φ_1 and N. There is a functor from $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to the category of Breuil modules defined below. Let $\mathfrak{M} \in \mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$. Define $\mathcal{M} := S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$ and note that we have an S-linear map $1 \otimes \varphi : \mathcal{M} \to S \otimes_{\mathfrak{S}} \mathfrak{M}$. Set

$$\mathrm{Fil}^1\mathcal{M} := \{x \in \mathcal{M} | (1 \otimes \varphi)(x) \in \mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M} \subset S \otimes_{\mathfrak{S}} \mathfrak{M}\}$$

and

$$\varphi_1 : \ \mathrm{Fil}^1\mathcal{M} \xrightarrow{1\otimes\varphi} \mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M} \xrightarrow{\varphi_1 \otimes 1} S \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} = \mathcal{M}.$$

One can easily check that $\mathrm{Fil}^1\mathcal{M}$ and φ_1 so constructed satisfy the axioms (1) (2) (3) in the definition of a Breuil module (see §(1.1.8) in [12]). The construction of the monodromy operator N is slightly more complicated. Let $I_+S := S \cap uK_0[\![u]\!]$ if we regard S as a subring of $K_0[\![u]\!]$. We regard $\mathfrak{M}$ as an $\varphi(\mathfrak{S})$-submodule of $\mathcal{M}$ and let $\tilde{\mathcal{M}}$ denote the $\varphi(S)$-submodule of $\mathcal{M}$ generated by $\mathfrak{M}$.

Lemma 2.2.3. (1) *There exists a unique monodromy operator N on $\mathcal{M}$ such that $N(\mathcal{M}) \subset I_+S\mathcal{M}$.*

(2) *$N^i(\mathfrak{M}) \subset u^p\tilde{\mathcal{M}}$ for each $i \geq 1$.*

Proof. (1) is Proposition 5.1.3 of [3]. Note that proof of the proposition does not need the running assumptions of the paper: $p > 2$ and k is finite. We repeat the proof here so that we can prove (2).

Let $L : \mathcal{M} \to \mathcal{M}$ be a $W(k)$-linear map, we call L a *derivation* if $L(sm) = N_S(s)m + sL(m)$ for $s \in S$ and $m \in \mathcal{M}$. Obviously, a derivation depends on its values on a basis of $\mathcal{M}$. Let $x_1, \ldots, x_d \in \mathrm{Fil}^1\mathcal{M}$ be such that $\{e_i := \varphi_1(x_i) | i = 1, \ldots, d\}$ is a basis of $\mathcal{M}$. Define a sequence of derivations N_n on $\mathcal{M}$ inductively via $N_0(e_i) = 0$ and $N_n(e_i) = (c_1)^{-1}\varphi_1(E(u)N_{n-1}(x_i))$. Now we prove by induction that $(N_n - N_{n-1})(\mathcal{M}) \in u^{p^n}\mathcal{M}$. First note that $N_n - N_{n-1}$ is an S-linear map, so it suffices to show that $(N_n - N_{n-1})(e_i) \in u^{p^n}\mathcal{M}$ for each i. For $n = 1$, $(N_1 - N_0)(e_i) = (c_1)^{-1}\varphi_1(E(u)N_0(x_i))$. As $N_0(e_i) = 0$, it suffices to show that $N_S(s) \in uS$ for each $s \in S$. This easily follows from the fact that $N_S(u) = -u$ and that $s = \sum\limits_{i=0}^{\infty} a_i(u)\gamma_i(E(u))$ with $a_i(u) \in$

$W(k)[u]$. If $n = m$ then we have $(N_m - N_{m-1})(e_i) = (c_1)^{-1}\varphi_1(E(u)(N_{m-1} - N_{m-2})(x_i))$. By induction, we have $(N_{m-1} - N_{m-2})(x_i) \in u^{p^{m-1}}\mathcal{M}$ and then $(N_m - N_{m-1})(e_i) \in u^{p^m}\mathcal{M}$. Hence N_n converges to a derivation N satisfying that $\varphi_1(E(u)N(x)) = c_1 N(\varphi_1(x))$ for $x \in \mathrm{Fil}^1\mathcal{M}$, as $\mathrm{Fil}^1\mathcal{M}$ is generated by x_i and $\mathrm{Fil}^1 S\mathcal{M}$. To see the uniqueness of N, assume that there exist two such derivations N and N'. Then $N - N'$ is an S-linear map. By $\varphi_1(E(u)(N - N')(x_i)) = c_1(N - N')(\varphi_1(x_i))$, we can easily show that

$$((N - N')(e_1), \ldots, (N - N')(e_d)) = ((N - N')(e_1), \ldots, (N - N')(e_d))A$$

with A a matrix having coefficients in $\varphi(I_+S)$. So $N - N'$ must be zero map and thus $N = N'$.

To prove (2), it suffices to prove the case $i = 1$ as the general case easily follows by induction on i. Let $f_1, \ldots, f_d$ be an $\mathfrak{S}$-basis of $\mathfrak{M}$. We easily see that there exists $x_1, \ldots, x_d \in (\mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}) \cap \mathrm{Fil}^1\mathcal{M}$ such that $e_i = \varphi_1(x_i) = c_1 f_i$ is a basis of $\tilde{\mathcal{M}}$. From the above construction of N on e_i, we easily see that $N(e_i) \in u^p\tilde{\mathcal{M}}$ for each i. Then $N(f_i) = N(c_1^{-1})e_i + c_1^{-1}N(e_i) \in u^p\tilde{\mathcal{M}}$ (note that $c_1^{-1} \in K_0[\![u^p]\!]$, so $N(c_1^{-1}) \in u^p K_0[\![u^p]\!]$). Hence $N(\mathfrak{M}) \subset u^p\tilde{\mathcal{M}}$ as $\mathfrak{M}$ is an $\varphi(\mathfrak{S})$-submodule of $\tilde{\mathcal{M}}$.

□

For each Breuil module $\mathcal{M}$, one defines a φ_S-semi-linear morphism $\varphi_{\mathcal{M}} : \mathcal{M} \to \mathcal{M}$ via $\varphi(x) = (c_1)^{-1}\varphi_1(E(u)x)$ for $x \in \mathcal{M}$. If $\mathcal{M}$ comes from a Kisin module $\mathfrak{M}$ as above then $\varphi_{\mathcal{M}}$ is just the natural extension of $\varphi_{\mathfrak{M}}$, namely $\varphi_{\mathcal{M}}(s \otimes x) = \varphi_S(s) \otimes \varphi_{\mathfrak{M}}(x)$ for $s \in S$ and $x \in \mathfrak{M}$. Similarly, one can extend the φ-structure to $A_{\mathrm{cris}} \otimes_S \mathcal{M} \simeq A_{\mathrm{cris}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$. Using the monodromy operator N, we can define an A_{cris}-semi-linear G-action on $A_{\mathrm{cris}} \otimes_S \mathcal{M}$ via

$$(2.2.1)\quad g(a \otimes x) = \sum_{i=0}^{\infty} g(a)\gamma_i(-\log([\underline{\epsilon}(g)])) \otimes N^i(x) \text{ for } a \in A_{\mathrm{cris}},\ x \in \mathcal{M}.$$

As in Lemma 5.1.1 of [15], we can show that the G-action preserves the φ-structure and $\mathrm{Fil}^1(A_{\mathrm{cris}} \otimes_S \mathcal{M}) := \mathrm{Fil}^1 A_{\mathrm{cris}} \otimes_S \mathcal{M} + A_{\mathrm{cris}} \otimes_S \mathrm{Fil}^1\mathcal{M}$. Therefore, one can associate a $\mathbb{Z}_p[G]$-module via

$$\tilde{T}_{\mathrm{cris}}(\mathcal{M}) := \mathrm{Hom}_{A_{\mathrm{cris}},\varphi,\mathrm{Fil}^1}(A_{\mathrm{cris}} \otimes_S \mathcal{M}, A_{\mathrm{cris}}),$$

where G acts on $\tilde{T}_{\mathrm{cris}}(\mathcal{M})$ via $g(f)(x) = g(f(g^{-1}(x)))$ for any $g \in G$ and $f \in \tilde{T}_{\mathrm{cris}}(\mathcal{M})$.

We need to show that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\mathrm{cris}}(\mathcal{M})$ is crystalline with Hodge-Tate weights in $\{0, 1\}$. Write $\mathcal{D} := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{M}$. First by Lemma 5.2.1 in [15], we have a natural $\mathbb{Q}_p[G]$-isomorphism between $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\mathrm{cris}}(\mathcal{M})$ and $V_{\mathrm{st}}(\mathcal{D}) := \mathrm{Hom}_{S,\varphi,\mathrm{Fil}^1,N}(\mathcal{D}, \widehat{A_{\mathrm{st}}}[\frac{1}{p}])$, where $\widehat{A_{\mathrm{st}}}$ is the period ring constructed in [2].

Proposition 2.2.5 in [4] shows that $V_{\mathrm{st}}(\mathcal{D})$ is semi-stable with Hodge-Tate weights with $\{0, 1\}$. Let D be the filtered (φ, N)-module associated to the semi-stable representation $V_{\mathrm{st}}(\mathcal{D})$ via Fontaine's theory. Breuil's theory in [2] show that one can recover N on D via $N_{\mathcal{D}} \mod I_+ S\mathcal{D}$. Since $N(\mathcal{M}) \subset u^p\mathcal{M}$ by Lemma 2.2.3, we have $N_D = 0$ and then $V_{\mathrm{st}}(\mathcal{D})$ must be crystalline.

Let us construct a $\mathbb{Z}_p$-linear map $\lambda : T_{\mathfrak{S}}(\mathfrak{M}) \to \tilde{T}_{\mathrm{cris}}(\mathcal{M})$. Note that $A_{\mathrm{cris}} \otimes_S \mathcal{M} = A_{\mathrm{cris}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$. For each $f \in T_{\mathfrak{S}}(\mathfrak{M})$, set $\lambda(f)(a \otimes m) = a\varphi(f(m))$ for $a \in A_{\mathrm{cris}}$ and $m \in \mathfrak{M}$. It is routine to check that λ is injective and compatible with G_∞-actions. Since $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\mathrm{cris}}(\mathcal{M})) = \dim_{\mathbb{Q}_p} V_{\mathrm{st}}(\mathcal{D}) = \dim_{K_0} D = \mathrm{rank}_S \mathcal{M} = \mathrm{rank}_{\mathfrak{S}} \mathfrak{M} = \mathrm{rank}_{\mathbb{Z}_p}(T_{\mathfrak{S}}(\mathfrak{M}))$, we see that $\lambda[\frac{1}{p}] : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M}) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\mathrm{cris}}(\mathcal{M})$ is an isomorphism of $\mathbb{Q}_p[G_\infty]$-modules.

Remark 2.2.4. If $p > 2$ then λ is indeed an isomorphism of $\mathbb{Z}_p[G_\infty]$-modules. First, one can easily show that $\tilde{T}_{\mathrm{cris}}(\mathcal{M}) \simeq T_{\mathrm{cris}}(\mathcal{M}) := \mathrm{Hom}_{S,\varphi,\mathrm{Fil}^1}(\mathcal{M}, A_{\mathrm{cris}})$ as $\mathbb{Z}_p[G_\infty]$-modules and this fact is also valid if $p = 2$. Second, by Lemma 3.3.4 in [15], the map $\lambda' : T_{\mathfrak{S}}(\mathfrak{M}) \to T_{\mathrm{cris}}(\mathcal{M})$ given by $\lambda'(f)(s \otimes m) = s\varphi(f(m))$ for $f \in T_{\mathfrak{S}}(\mathfrak{M})$, $s \in S$ and $m \in \mathfrak{M}$ is an isomorphism of $\mathbb{Z}_p[G_\infty]$-modules. But when $p = 2$ then λ' is not necessarily an isomorphism. See Example 5.3.3 in [14].

To summarize the above discussion, we have a functor ι from the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Q}_p}$ via

$$\iota : \mathfrak{M} \rightsquigarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \lambda(T_{\mathfrak{S}}(\mathfrak{M})).$$

Now suppose that $(\mathfrak{M}, \varphi, \hat{G})$ is a $(\varphi, \hat{G})$-module such that $\hat{T}(\hat{\mathfrak{M}})$ is an object in $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$. Note that $\hat{\mathfrak{M}} = \widehat{\mathcal{R}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \subset A_{\mathrm{cris}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$. It is routine to check that the natural map

$$\hat{\lambda} : \mathrm{Hom}_{\widehat{\mathcal{R}}}(\hat{\mathfrak{M}}, W(R)) \to \mathrm{Hom}_{A_{\mathrm{cris}}}(A_{\mathrm{cris}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}, A_{\mathrm{cris}})$$

induces a $\mathbb{Z}_p$-linear map from $\hat{T}(\hat{\mathfrak{M}})$ to $\tilde{T}_{\mathrm{cris}}(\mathcal{M})$ which we still denote by $\hat{\lambda}$. One easily checks that the following diagram commutes

$$\begin{tikzcd}
T_{\mathfrak{S}}(\mathfrak{M}) \arrow[r, hook, "\lambda"] \arrow[dr, "\theta", "\simeq"'] & \tilde{T}_{\mathrm{cris}}(\mathcal{M}) \\
& \hat{T}(\hat{\mathfrak{M}}). \arrow[u, "\hat{\lambda}"']
\end{tikzcd} \tag{2.2.2}$$

Furthermore $\hat{\lambda}$ is compatible with G-actions on the both sides. This is a consequence of the construction of the $\hat{G}$-action on $\hat{\mathfrak{M}}$, and the G-action on $A_{\mathrm{cris}} \otimes_{\widehat{\mathcal{R}}} \hat{\mathfrak{M}} = A_{\mathrm{cris}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$ given by formula (2.2.1). The reader is referred to Section 3.2 of [16] for details. Finally, the full faithfulness and essential surjectivity of ι can be proved by the full faithfulness and essential surjectivity of $\hat{T}$ in Theorem 2.1.2. Here we actually do not need the the full faithfulness and essential surjectivity of ι.

Remark 2.2.5. Note that ι is a contravariant functor. To obtain a covariant functor, we can just define $\iota'(\mathfrak{M}) = (\iota(\mathfrak{M}))^*(1)$, where $*$ means taking dual and (1) means twisting by the cyclotomic character. Indeed, $\iota'(\mathfrak{M}) \simeq \iota(\mathfrak{M}^\vee)$ where $\mathfrak{M}^\vee$ denotes the Cartier dual of $\mathfrak{M}$ (for details of Cartier dual, see for example §3.1 of [14]).

2.3. The proof of the main theorem.

Proposition 2.3.1. *$\lambda(T_{\mathfrak{S}}(\mathfrak{M}))$ is G-stable in $\tilde{T}_{\mathrm{cris}}(\mathcal{M})$.*

The next section is devoted to proving the above Proposition. Let us assume this Proposition for the moment. Now we have a functor $\mathfrak{M} \rightsquigarrow \lambda(T_{\mathfrak{S}}(\mathfrak{M}))$ from the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ to the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$. The full faithfulness of the functor follows from the full faithfulness of the functor $T_{\mathfrak{S}}$ and the injectivity of λ. The essential surjectivity follows from Theorem 2.1.2 and diagram (2.2.2). So the functor induces an equivalence between the category $\mathrm{Mod}^{1,\mathrm{fr}}_{/\mathfrak{S}}$ and the category $\mathrm{Rep}^{\mathrm{cris},1}_{\mathbb{Z}_p}$. Then Theorem 1.0.1 follows from Theorem 2.2.1.

3. The proof of Proposition 2.3.1

3.1. A natural *G*-action on $T_{\mathfrak{S}}(\mathfrak{M})$. Define an ideal in B^+_{cris}

$$I^{[1]}B^+_{\mathrm{cris}} = \{a \in B^+_{\mathrm{cris}} | \varphi^m(a) \in \mathrm{Fil}^1 B^+_{\mathrm{cris}}, \forall m \geq 1.\}$$

We write $I^{[1]} := W(R) \cap I^{[1]}B^+_{\mathrm{cris}}$ as an ideal of $W(R)$. Since $\varphi(t) = pt$, we see that $t \in I^{[1]}B^+_{\mathrm{cris}}$. By Proposition 5.1.3 in [7], $I^{[1]}$ is a principal ideal and $[\underline{\epsilon}] - 1$ is a generator of $I^{[1]}$. Write pc_0 for the constant term of $E(u)$ with $c_0 \in W(k)^\times$. Select a $\mathfrak{t} \in W(R)$ such that $\varphi(\mathfrak{t}) = c_0^{-1}E(u)\mathfrak{t}$ and $\mathfrak{t} \not\equiv 0 \mod p$ in $W(R)$. Such $\mathfrak{t}$ exists and is unique up to units of $\mathbb{Z}_p$. See Example 2.3.5 in [14] for details. In the proof of Lemma 3.2.2 in [16], it has been shown that $\varphi(\mathfrak{t})$ is a generator of $I^{[1]}$. Since $uI^{[1]}$ and $u\mathfrak{t}W(R)$ are obviously φ-stable inside $W(R)$, there are natural Frobenius endomorphisms on $W(R)/uI^{[1]}$ and on $W(R)/u\mathfrak{t}W(R)$. Define

$$J'(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W(R)/uI^{[1]}) \tag{3.1.1}$$

and

$$J(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W(R)/u\mathfrak{t}W(R)). \tag{3.1.2}$$

The natural projections $W(R) \to W(R)/uI^{[1]} \to W(R)/u\mathfrak{t}W(R)$ induce the following commutative diagram of natural maps

$$\begin{tikzcd} T_{\mathfrak{S}}(\mathfrak{M}) \arrow[r, "\eta'"] \arrow[dr, "\eta"'] & J'(\mathfrak{M}) \arrow[d, "\mu"] \\ & J(\mathfrak{M}). \end{tikzcd}$$

Proposition 3.1.1. (1) *η and η' are injective.*

(2) *μ and η have the same images inside $J(\mathfrak{M})$, i.e., $\mu(J'(\mathfrak{M})) = \eta(T_{\mathfrak{S}}(\mathfrak{M}))$.*

Proof. (1) It suffices to show that η is injective. Let $e_1, \dots, e_d$ be a basis of $\mathfrak{M}$ and A the matrix such that $\varphi(e_1, \dots, e_d) = (e_1, \dots, e_d)A$. Assume that h is in the kernel of η. Then the vector $X := (h(e_1), \dots, h(e_d))$ has coordinates in $u\mathfrak{t}W(R)$ and satisfies the relation $\varphi(X) = XA$. Write $X = u\mathfrak{t}Y$ with Y's coordinates in $W(R)$. We have

$$u\mathfrak{t}YA = XA = \varphi(X) = \varphi(u\mathfrak{t}Y).$$

So $u^p\varphi(\mathfrak{t})\varphi(Y) = u\mathfrak{t}YA$. Since the cokernel of $1 \otimes \varphi_{\mathfrak{M}}$ is killed by $E(u)$, there exists a matrix B such that $AB = BA = E(u)I_d$. Here I_d is the $d \times d$-identity matrix. Note that $\varphi(\mathfrak{t}) = c_0^{-1}E(u)\mathfrak{t}$. We obtain $Y = u^{p-1}c_0^{-1}\varphi(Y)B$. Then

$$Y = c_0^{-1}u^{p-1}\varphi(u^{p-1}c_0^{-1}\varphi(Y)B)B = c_0^{-1}\varphi(c_0^{-1})u^{(p-1)+p(p-1)}\varphi^2(Y)\varphi(B)B.$$

Continuing in this way, we see that the entries of Y are in $\bigcap_{n=0}^{\infty} u^nW(R) = \{0\}$.

Now let us prove (2). Suppose that $h \in J'(\mathfrak{M})$ and let X be a vector with coordinates in $W(R)$ such that X lifts $(h(e_1), \dots, h(e_d))$. Then we obtain an equation $\varphi(X) = XA + u\varphi(\mathfrak{t})Y$ with the coordinates of Y in $W(R)$ and A the matrix of φ in the basis $e_1, \dots, e_d$ as the above. To show that $\mu(h) \in \eta(T_{\mathfrak{S}}(\mathfrak{M}))$, it suffices to show there exists a matrix Z with coefficients in $W(R)$ such that

$$\varphi(X + u\mathfrak{t}Z) = (X + u\mathfrak{t}Z)A.$$

Recall that there exists a matrix B such that $AB = BA = E(u)I_d$. Then the above equation is equivalent to $\varphi(X + u\mathfrak{t}Z)B = E(u)(X + u\mathfrak{t}Z)$. Note that $\varphi(\mathfrak{t}) = c_0^{-1}E(u)\mathfrak{t}$ and $\varphi(X) = XA + u\varphi(\mathfrak{t})Y$. So it suffices to solve the following equation for Z:

$$(u\varphi(\mathfrak{t})Y + u^p\varphi(\mathfrak{t})\varphi(Z))B = u\mathfrak{t}ZE(u),$$

which is equivalent to

$$c_0^{-1}YB + c_0^{-1}u^{p-1}\varphi(Z)B = Z. \tag{3.1.3}$$

Now we define $Z_0 = 0$ and $Z_l = c_0^{-1}YB + c_0^{-1}u^{p-1}\varphi(Z_{l-1})B$. We claim that the coordinates of Z_l converge in $W(R)$. In fact, we see that $Z_{l+1}-Z_l = c_0^{-1}u^{p-1}\varphi(Z_l - Z_{l-1})B$. Thus

$$Z_{l+1} - Z_l = (\prod_{i=0}^{l-1} \varphi^i(c_0^{-1}u^{p-1}))(Z_1 - Z_0)(\varphi^{l-1}(B)\dots\varphi(B)B)$$

This shows that $Z_{l+1} - Z_l \in u^{n(l)}W(R)$ with $n(l) \to \infty$ as $l \to \infty$. Hence Z_l converges and Z exists.

□

Proposition 3.1.2. (1) *$J(\mathfrak{M})$ and $J'(\mathfrak{M})$ have natural G-actions.*

(2) *$T_{\mathfrak{S}}(\mathfrak{M})$ has a natural G-action.*

(3) *All G-actions here are compatible the natural G_∞-action on $T_{\mathfrak{S}}(\mathfrak{M})$.*

Proof. Obviously, (2) is a consequence of (1) by Proposition 3.1.1. So it suffices to show (1). Let us first treat $J'(\mathfrak{M})$. We first check that $uI^{[1]}$ is G-stable in $W(R)$ so that $W(R)/uI^{[1]}$ has a natural G-action. Since $\mathrm{Fil}^1 W(R)$ is G-stable in $W(R)$, it is easy to check that $I^{[1]}$ is G-stable. Given $g \in G$ and $m \in W(R)$, we have $g(um) = u[\underline{\epsilon}(g)]g(m)$ with $\underline{\epsilon}(g) = \frac{g(\underline{\pi})}{\underline{\pi}}$ a unit in R. So $[\underline{\epsilon}(g)]g(m)$ is in $I^{[1]}$ and $uI^{[1]}$ is G-stable.

Let $h \in J'(\mathfrak{M})$, $g \in G$. To show that $J'(\mathfrak{M})$ has a natural G-action induced from that on $W(R)/uI^{[1]}$, we have to show that $g(h) \in J'(\mathfrak{M})$. It is obvious that h is still φ-equivariant. To see that h is $\mathfrak{S}$-linear, note that $g(h(um)) = g(u)g(h(m))$. Since $g(u) - u = u([\underline{\epsilon}(g)] - 1) \in uI^{[1]}$, we see that $g(h)$ is $\mathfrak{S}$-linear. The proof for $J(\mathfrak{M})$ is almost the same except we need to check that $u\mathfrak{t}W(R)$ is G-stable in $W(R)$. To see this, for each $x = u\mathfrak{t}y \in u\mathfrak{t}W(R)$ with $y \in W(R)$, we have $\varphi(x) = u^p\varphi(\mathfrak{t})\varphi(y) \in u^pI^{[1]}$. It is easy to check that $u^pI^{[1]}$ is G-stable in $W(R)$. Namely, for each $g \in G$, $g(\varphi(x)) = u^p\varphi(\mathfrak{t})z$ with $z \in W(R)$ as $\varphi(\mathfrak{t})$ is a generator of $I^{[1]}$. Hence there exists a $w \in W(R)$ such that $g(x) = u\mathfrak{t}w$ with $\varphi(w) = z$ because $\varphi : W(R) \to W(R)$ is a bijection. Finally, (3) is obvious from (1) (2) and the constructions of $J(\mathfrak{M})$, $J'(\mathfrak{M})$ and $T_{\mathfrak{S}}(\mathfrak{M})$. □

Corollary 3.1.3. *If $f : T_{\mathfrak{S}}(\mathfrak{M}) \to T_{\mathfrak{S}}(\mathfrak{N})$ is a morphism of $\mathbb{Z}_p[G_\infty]$-modules then it is a morphism of $\mathbb{Z}_p[G]$-modules.*

Proof. Since $T_{\mathfrak{S}}$ is fully faithful, there exists a morphism $\mathfrak{f} : \mathfrak{N} \to \mathfrak{M}$ in $\mathrm{Mod}_{/\mathfrak{S}}^{1,\mathrm{fr}}$ such that $T_{\mathfrak{S}}(\mathfrak{f}) = f$. Note that $\mathfrak{f}$ induces natural maps between $J'(\mathfrak{M})$, $J(\mathfrak{M})$ and $J'(\mathfrak{N})$, $J(\mathfrak{N})$ respectively, so by Proposition 3.1.2, f is a morphism of $\mathbb{Z}_p[G]$-modules. □

3.2. Compatibility of G-actions. To prove Proposition 2.3.1, one has to show that the G-action on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M})$ obtained via $J(\mathfrak{M})$ is compatible with that induced from $\iota(\mathfrak{M}) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\mathrm{cris}}(\mathcal{M})$ constructed in §2.2.

Choose a G-stable $\mathbb{Z}_p$-lattice L inside $\iota(\mathfrak{M})$ such that L contains $\lambda(T_{\mathfrak{S}}(\mathfrak{M}))$. Then L corresponds to a $(\varphi, \hat{G})$-module $(\mathfrak{L}, \varphi_{\mathfrak{L}}, \hat{G}_{\mathfrak{L}})$ by Theorem 2.1.2. By Corollary 3.1.3, it is easy to check that if two G-actions are compatible on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{L})$ then they are compatible on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M})$. So to prove such compatibility, it remains to prove the following statement: Given a $(\varphi, \hat{G})$-module $\hat{\mathfrak{M}} = (\mathfrak{M}, \varphi, \hat{G})$ such that $\hat{T}(\hat{\mathfrak{M}})$ is an object in $\mathrm{Rep}_{\mathbb{Z}_p}^{\mathrm{cris},1}$, the G-action on $T_{\mathfrak{S}}(\mathfrak{M})$ obtained from $J(\mathfrak{M})$ agrees with that induced from $\hat{T}(\hat{\mathfrak{M}})$ via isomorphism θ in Theorem 2.1.2 (1).

Recall from Theorem 2.1.2 (1) that the natural $\mathbb{Z}_p[G_\infty]$-isomorphism $\theta : T_{\mathfrak{S}}(\mathfrak{M}) \to \hat{T}(\mathfrak{M})$ is given by

$$\theta(\alpha)(a \otimes x) = a\varphi(\alpha(x)) \text{ for } \alpha \in T_{\mathfrak{S}}(\mathfrak{M}), a \in \widehat{\mathcal{R}}, x \in \mathfrak{M}.$$

Now define

$$\hat{J}(\hat{\mathfrak{M}}) := \mathrm{Hom}_{\widehat{\mathcal{R}},\varphi}(\widehat{\mathcal{R}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}, W(R)/u^p\varphi(\mathfrak{t})W(R)),$$

and a map $\tilde{\theta} : J(\mathfrak{M}) \to \hat{J}(\hat{\mathfrak{M}})$ via

$$\tilde{\theta}(\alpha)(a \otimes x) = a\varphi(\alpha(x)) \text{ for } \alpha \in J(\mathfrak{M}), a \in \widehat{\mathcal{R}}, x \in \mathfrak{M}.$$

It is easy to check that $\tilde{\theta}$ is a well-defined map. Since $\mathfrak{M}$ is finite $\mathfrak{S}$-free and φ induces a ring isomorphism between $W(R)/u\mathfrak{t}W(R)$ and $W(R)/u^p\varphi(\mathfrak{t})W(R)$, we easily check that $\tilde{\theta}$ is an isomorphism of $\mathbb{Z}_p$-modules. Now we have the following commutative diagram of $\mathbb{Z}_p$-modules:

$$\begin{tikzcd}
T_{\mathfrak{S}}(\mathfrak{M}) \arrow[r, "\theta", "\sim"'] \arrow[d, hook, "\eta"] & \hat{T}(\hat{\mathfrak{M}}) \arrow[d, "\hat{\eta}"] \\
J(\mathfrak{M}) \arrow[r, "\tilde{\theta}", "\sim"'] & \hat{J}(\hat{\mathfrak{M}})
\end{tikzcd}$$

where $\hat{\eta}$ is defined by the projection $W(R) \to W(R)/u^p\varphi(\mathfrak{t})W(R)$. Note that both $\hat{T}(\hat{\mathfrak{M}})$ and $J(\mathfrak{M})$ are $\mathbb{Z}_p[G]$-modules, and θ, η are morphisms of $\mathbb{Z}_p[G_\infty]$-modules. We equip $\hat{J}(\hat{\mathfrak{M}})$ with an action of G via the isomorphism $\tilde{\theta}$. The proof of Proposition 2.3.1 is now reduced to the following Proposition.

Proposition 3.2.1. *Notations as above, $\hat{\eta}$ is a morphism of $\mathbb{Z}_p[G]$-modules.*

Proof. Select a basis $e_1, \dots, e_d$ of $\mathfrak{M}$ and $\alpha \in T_{\mathfrak{S}}(\mathfrak{M})$. Write $\beta = \theta(\alpha)$ and $\beta' = \tilde{\theta}(\eta(\alpha))$. For each g in G and $a_i \in \widehat{\mathcal{R}}$, we have to show that

$$(g \circ \beta)(\sum_i a_i \otimes e_i) \equiv (g \circ \beta')(\sum_i a_i \otimes e_i) \mod u^p\varphi(\mathfrak{t})W(R).$$

By definition,

$$(g \circ \beta)(\sum_i a_i \otimes e_i) = g(\beta(g^{-1}(\sum_i a_i \otimes e_i))) = \sum_i a_i g(\beta(g^{-1}(1 \otimes e_i))).$$

Since $\hat{J}(\hat{\mathfrak{M}})$ uses the G-action from that on $J(\mathfrak{M})$, we have

$$\begin{aligned}(g\circ\beta')(\sum_i a_i\otimes e_i) &= \sum_i a_i g(\beta'(1\otimes e_i))\\ &\equiv \sum_i a_i g(\varphi(\alpha(e_i))) \mod u^p\varphi(\mathfrak{t})W(R).\end{aligned}$$

We claim that $g^{-1}(1\otimes e_i)\equiv 1\otimes e_i \mod \tilde{I}\hat{\mathfrak{M}}$ where $\tilde{I}=(u^p\varphi(\mathfrak{t})W(R))\cap\widehat{\mathcal{R}}$.[2] Let us assume this claim for a moment. Then we have

$$\begin{aligned}(g\circ\beta)(\sum_i a_i\otimes e_i) &= \sum_i a_i g(\beta(g^{-1}(1\otimes e_i)))\\ &\equiv \sum_i a_i g(\beta(1\otimes e_i)) \mod u^p\varphi(\mathfrak{t})W(R)\\ &\equiv \sum_i a_i g(\varphi(\alpha(e_i))) \mod u^p\varphi(\mathfrak{t})W(R)\\ &\equiv (g\circ\beta')(\sum_i a_i\otimes e_i) \mod u^p\varphi(\mathfrak{t})W(R).\end{aligned}$$

This proves the proposition and it suffices to prove the claim. By formula (2.2.1), we see the G-action on $B^+_{\text{cris}}\otimes_{\varphi,\mathfrak{S}}\mathfrak{M}=B^+_{\text{cris}}\otimes_S\mathcal{M}$ is given by

$$g(1\otimes e_i)=\sum_{j=0}^{\infty}\gamma_j(-\log([\underline{\epsilon}(g)]))\otimes N^j(1\otimes e_i),$$

where N is the monodromy operator on $\mathcal{M}$ constructed above Lemma 2.2.3. Note that $\gamma_i(-\log([\underline{\epsilon}(g)]))\in I^{[1]}B^+_{\text{cris}}$, so by Lemma 2.2.3, we have that

$$g(1\otimes e_i)\equiv 1\otimes e_i \mod u^p(I^{[1]}B^+_{\text{cris}})\hat{\mathfrak{M}}.$$

Therefore, we have a matrix A with coefficients in $u^pI^{[1]}B^+_{\text{cris}}$ such that

$$g(1\otimes e_1,\dots,1\otimes e_d)=(1\otimes e_1,\dots,1\otimes e_d)(I_d+A),$$

where I_d denotes the identity matrix. On the other hand, since $\hat{\mathfrak{M}}=\widehat{\mathcal{R}}\otimes_{\mathfrak{S},\varphi}\mathfrak{M}$ is G-stable in $B^+_{\text{cris}}\otimes_{\mathfrak{S},\varphi}\mathfrak{M}$, the entries of A are in $\widehat{\mathcal{R}}\subset W(R)$. Now the entries of A must be in $u^pI^{[1]}B^+_{\text{cris}}\cap W(R)$. By Lemma 3.2.2 below, the entries of A must be in $u^p(I^{[1]}B^+_{\text{cris}}\cap W(R))=u^pI^{[1]}=u^p\varphi(\mathfrak{t})W(R)$. This proves the claim. □

Lemma 3.2.2. *Let $x\in B^+_{\text{cris}}$. If $ux\in W(R)$ then $x\in W(R)$.*

Proof. We first check a useful fact: suppose that $w\in W(R)$ and $p^s|uw$ in $W(R)$ then $p^s|w$ in $W(R)$. It suffices to check this when $s=1$. Note that $u \mod p=\underline{\pi}\neq 0$ inside R, so $uw \mod p=0$ in R implies that $w \mod p=0$ because R is an integral domain. This checks the fact.

[2] It is not clear that $\tilde{I}=u^p\varphi(\mathfrak{t})\widehat{\mathcal{R}}$ as $I_+S\neq uS$. Fortunately, we do not need this fact.

Write $y = ux$. It suffices to prove that for each integer $m > 0$ there exists $x_m, z_m \in W(R)$ such that $y = ux_m + p^m z_m$. Let us first assume that $x \in A_{\mathrm{cris}}$. Then x can be written as $x = \sum\limits_{i=0}^{\infty} a_i \frac{E(u)^i}{i!}$ with $a_i \in W(R)$. Denote $n_i := v_p(i!)$. We have

$$p^{n_i} y = p^{n_i} ux = u \sum_{j=0}^{i} p^{n_i} a_j \frac{E(u)^j}{j!} + p^{n_i} \sum_{j=i+1}^{\infty} ua_j \frac{E(u)^j}{j!}.$$

Put $\tilde{x}_i = \sum\limits_{j=0}^{i} p^{n_i} a_j \frac{E(u)^j}{j!}$ and $\tilde{z}_i = p^{n_i} \sum\limits_{j=i+1}^{\infty} ua_j \frac{E(u)^j}{j!}$. We observe that $\tilde{x}_i$ is in $W(R)$ and $\tilde{z}_i$ is in $\mathrm{Fil}^{i+1} A_{\mathrm{cris}} \cap W(R)$, which is $E(u)^{i+1} W(R)$. Hence we may write $\tilde{z}_i = E(u)^{i+1} \beta_i$ with $\beta_i \in W(R)$. We easily compute that $E(u)^{i+1} = p^{i+1} b_i + uw_i$ with $b_i \in W(k)$ and $w_i \in W(k)[u]$. Now we get

$$p^{n_i} y = u\tilde{x}_i + p^{i+1} b_i \beta_i + uw_i \beta_i = ux'_i + p^{i+1} z'_i$$

where $x'_i = \tilde{x}_i + w_i \beta_i$ and $z'_i = b_i \beta_i$. Since $n_i < i+1$, $p^{n_i} | ux'_i$ in $W(R)$. So $p^{n_i} | x'_i$ in $W(R)$ by the fact proved above. Now we may write $y = ux_{(i)} + p^{i+1-n_i} z_{(i)}$ with $x_{(i)} = x'_i / p^{n_i} \in W(R)$ and $z_{(i)} = z'_i \in W(R)$. To prove the lemma, we have to show that we can select a sequence i_m such that $i_m + 1 - n_{i_m} \to +\infty$ as $m \to \infty$. If $p > 2$ then we can just choose $i_m = m$ as $n_i = v_p(i!) \leq \frac{i}{p-1}$. It remains to deal with the case $p = 2$. In this case, we select $i_m = 2^m - 1$. One computes that $v_2((2^m - 1)!) = 2^m - m - 1$ and thus $i_m + 1 - n_{i_m} = m + 1 \to +\infty$.

Now suppose that $x \in B^+_{\mathrm{cris}}$ and $p^s x \in A_{\mathrm{cris}}$. Then we have shown that $p^s x \in W(R)$. Since $p^s y$ is in $p^s W(R)$, we see that $p^s | u(p^s x)$ in $W(R)$. Then $p^s | p^s x$ in $W(R)$ by the above fact. That is $x \in W(R)$. □

References

[1] C. Breuil, *Schémas en groupes et corps des normes.* Unpublished.

[2] C. Breuil, *Représentations p-adiques semi-stables et transversalité de Griffiths.* Math. Ann., **307(2)** (1997), 191–224.

[3] C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés.* Ann. of Math.(2) **152(2)** (2000), 489–549.

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

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

[6] J.-M. Fontaine, *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate.* In Journées de Géométrie Algébrique de Rennes, (Rennes, 1978), Vol.III, volume 65 of Astérisque, . Soc. Math. France Paris (1979), 3–80.

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

[8] J.-M. Fontaine, *Représentations p-adiques semi-stables.* Astérisque, **223** (1994), 113–184. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[9] W. Kim, *The classification of p-divisible groups over 2-adic discrete valuation rings.* Math. Res. Lett., **19(1)** (2012), 121–141.

[10] M. Kisin, *Crystalline representations and F-crystals*. In Algebraic geometry and number theory,Progr. Math. **253**, Birkhäuser Boston, Boston, MA, (2006), 459–496.

[11] M. Kisin *Modularity of 2-adic Barsotti-Tate representations*. Invent. Math., **178(3)** (2009), 587–634.

[12] M. Kisin *Moduli of finite flat group schemes, and modularity*. Ann. of Math.(2), **170(3)** (2009), 1085–1180.

[13] E. Lau, *A relation between dieudonne displays and crystalline dieudonne theory*. arXiv:1006.2720.

[14] T. Liu, *Torsion p-adic Galois representations and a conjecture of fontaine*. Ann. Sci. École Norm. Sup. (4), **40(4)** (2007), 633–674.

[15] T. Liu, *On lattices in semi-stable representations: a proof of a conjecture of Breuil*. Compos. Math., **144(1)** (2008), 61–88.

[16] T. Liu, *A note on lattices in semi-stable representations*. Mathematische Annalen, **346(1)** (2010), 117–138.

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

[18] J. T. Tate, p-divisible groups. In Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, (1967), 158–183.

Tong Liu
Department of Mathematics
Purdue University
West Lafayette, 47907, USA.
E-mail: tongliu@math.purdue.edu,