

THE CORRESPONDENCE BETWEEN BARSOTTI-TATE GROUPS AND KISIN MODULES WHEN $p = 2$

TONG LIU

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	1
2. Preliminaries and Preparations	3
2.1. Kisin modules and (φ, \hat{G}) -modules	3
2.2. Barsotti-Tate groups and lattices in crystalline representations	5
2.3. The proof of the main theorem	8
3. The proof of Proposition 2.3.1	8
3.1. A natural G -action on $T_{\mathfrak{S}}(\mathfrak{M})$	8
3.2. Compatibility of G -actions	10
References	12

1. INTRODUCTION

Let k be a perfect field of characteristic p , $W(k)$ its ring of Witt vectors, $K_0 = W(k)[\frac{1}{p}]$, K/K_0 a finite totally ramified extension, \overline{K} a fixed algebraic closure of K and $G := \text{Gal}(\overline{K}/K)$. 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 $p = 2$.

More precisely, let $E(u)$ be an Eisenstein polynomial for a fixed uniformizer π of K , $K_\infty = \bigcup_{n \geq 1} K(\sqrt[n]{\pi})$, $G_\infty = \text{Gal}(\overline{K}/K_\infty)$ and $\mathfrak{S} = W(k)[[u]]$. We equip \mathfrak{S} with the endomorphism φ which acts via Frobenius on $W(k)$, and sends u to u^p . Let $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ denote the category of finite free \mathfrak{S} -modules \mathfrak{M} equipped with a φ -semi-linear map $\varphi_{\mathfrak{M}} : \mathfrak{M} \rightarrow \mathfrak{M}$ such that the cokernel of the \mathfrak{S} -linear map

1991 *Mathematics Subject Classification*. Primary 14F30, 14L05.

The author is partially supported by NSF grant DMS-0901360.

$1 \otimes \varphi_{\mathfrak{M}} : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \rightarrow \mathfrak{M}$ is killed by $E(u)$. Objects in $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ are called φ -modules of $E(u)$ -height 1 or Kisin modules of height 1¹. 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 conjecture was first raised in [Bre]. If $p > 2$ then the above theorem was proved in [Kis06]. In [Kis09a], the equivalence between the category of connected Barsotti-Tate groups over \mathcal{O}_K and 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 prime p .

Let us sketch the idea of the proof of the main theorem. Let $\text{Rep}_{\mathbb{Z}_p}^{\text{cris}, 1}$ denote the category of G -stable \mathbb{Z}_p -lattices in crystalline representations with Hodge-Tate weights in $\{0, 1\}$. By Fontaine, Kisin, Raynaud and Tate, it has been known that the category of Barsotti-Tate groups over \mathcal{O}_K is equivalent to the category $\text{Rep}_{\mathbb{Z}_p}^{\text{cris}, 1}$ (see Theorem 2.2.1). So we need to establish the equivalence between the category $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ and the category $\text{Rep}_{\mathbb{Z}_p}^{\text{cris}, 1}$. For an object $\mathfrak{M} \in \text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$, we can associate a $\mathbb{Z}_p[G_{\infty}]$ -module $T_{\mathfrak{S}}(\mathfrak{M}) := \text{Hom}_{\varphi, \mathfrak{S}}(\mathfrak{M}, W(R))$ (see Section 2.1 for more details). In [Kis06], 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 $\mathfrak{M} \mapsto T_{\mathfrak{S}}(\mathfrak{M})$ establishes an anti-equivalence from the category $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ to the category $\text{Rep}_{\mathbb{Z}_p}^{\text{cris}, 1}$.

To prove that $T_{\mathfrak{S}}(\mathfrak{M})$ is G -stable in $V_{\mathfrak{S}}(\mathfrak{M})$, we use the idea developed in [CL]. We embed $T_{\mathfrak{S}}(\mathfrak{M})$ into $J(\mathfrak{M}) := \text{Hom}_{\varphi, \mathfrak{S}}(\mathfrak{M}, W(R)/uW(R))$ 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, and thus prove the main theorem.

In the end, let us mention an interesting consequence of Theorem 1.0.1 which has also been proved in [Kis06] except $p = 2$. Let $\text{Mod}_{/\mathfrak{S}}^{1, \text{tor}}$ denote the category whose objects are finite \mathfrak{S} -modules \mathfrak{M} which are killed by some power of p , have projective dimension 1 and are equipped with a φ -semi-linear map $\varphi_{\mathfrak{M}} : \mathfrak{M} \rightarrow \mathfrak{M}$ such that the cokernel of the \mathfrak{S} -linear map $1 \otimes \varphi_{\mathfrak{M}} : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \rightarrow \mathfrak{M}$ is killed by $E(u)$.

Theorem 1.0.2. *The category $\text{Mod}_{/\mathfrak{S}}^{1, \text{tor}}$ is equivalent to the category of finite flat group schemes over \mathcal{O}_K .*

When this paper is nearly complete, we have learnt that W. Kim and E. Lau also just post their preprints [Kim10], [Lau] in arXiv independently which proved similar results as ours. Here we comments that we use totally different approaches and methods from those used by Kim and Lau.

Acknowledgment: It is a pleasure to thank Christophe Breuil, Wansu Kim, Mark Kisin for very useful correspondences during the preparation of this paper.

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

Notations 1.0.3. We define various Frobenius and monodromy (derivation) structures on different rings and modules. The symbol φ and N are reserved to denote Frobenius and monodromy operators respectively. We sometime 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 confusions arise. We denote $\gamma_i(x)$ the standard divided power $\frac{x^i}{i!}$.

2. PRELIMINARIES AND PREPARATIONS

In first 2 subsections, we recall from references some facts and notations of objects 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 (φ, \hat{G}) -modules. In this subsection, we recall some standard notations, definitions and results from [Kis06] and [Liu10]. The reader may consult these papers for more details.

Recall that k is a perfect field of characteristic p , $W(k)$ its ring of Witt vectors, $K_0 = W(k)[\frac{1}{p}]$, K/K_0 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 $\varphi_{\mathfrak{M}} : \mathfrak{M} \rightarrow \mathfrak{M}$. 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 $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ 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 $1 \otimes \varphi : \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \rightarrow \mathfrak{M}$. Objects in $\text{Mod}_{/\mathfrak{S}}^{1, \text{fr}}$ 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 map (Frobenius) $\varphi : S \rightarrow S$ 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. By the universal property of the Witt vectors $W(R)$ of R , there is a unique surjective projection map $\theta : W(R) \rightarrow \widehat{\mathcal{O}}_{\overline{K}}$ to the p -adic completion of $\mathcal{O}_{\overline{K}}$, which lifts the projection $R \rightarrow \mathcal{O}_{\overline{K}}/p$ 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 $\text{Ker}(\theta)$. 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 Teichmüller representative. We embed the $W(k)$ -algebra $W(k)[u]$ into $W(R) \subset A_{\text{cris}}$ by the map $u \mapsto [\underline{\pi}]$. This embedding extends to embeddings $\mathfrak{S} \hookrightarrow S \hookrightarrow A_{\text{cris}}$ which are compatible with Frobenius endomorphisms. We denote by B_{dR}^+ the $\text{Ker}(\theta)$ -adic completion of $W(R)[1/p]$. For any subring $A \subset B_{\text{dR}}^+$, we define filtration on A by $\text{Fil}^i A = A \cap (\text{Ker}(\theta))^i B_{\text{dR}}^+ = A \cap (E(u)^i) B_{\text{dR}}^+$. As usual, we denote $A_{\text{cris}}[\frac{1}{p}]$ 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 $t := \log([\underline{\epsilon}]) \in A_{\text{cris}}$. 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 $\log([\underline{\varepsilon}(g)]) = \alpha(g)t$. Recall $K_\infty := \bigcup_{n=0}^{\infty} K(\pi_n)$ and $G_\infty := \text{Gal}(\overline{K}/K_\infty)$. We set $\hat{K} = \bigcup_{n=1}^{\infty} K_\infty(\zeta_{p^n})$ and $\hat{G} := \text{Gal}(\hat{K}/K)$.

As a subring of A_{cris} , S is not stable under the action of G , though S is fixed by G_∞ . Define $\mathcal{R}_{K_0} := \left\{ x = \sum_{i=0}^{\infty} f_i t^{\{i\}}, f_i \in S_{K_0} \text{ and } f_i \rightarrow 0 \text{ as } i \rightarrow +\infty \right\}$, 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 $\hat{\mathcal{R}} := W(R) \cap \mathcal{R}_{K_0}$. One can show that \mathcal{R}_{K_0} and $\hat{\mathcal{R}}$ are stable under the G -action and the G -action factors through \hat{G} (see [Liu10] §2.2). 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 $I_+ := \hat{\mathcal{R}} \cap W(I_+R)$. By Lemma 2.2.1 in [Liu10], one has $\hat{\mathcal{R}}/I_+ \simeq W(k)$.

Following [Liu10], a (φ, \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 $\hat{\mathcal{R}}$ -semi-linear \hat{G} -action on $\hat{\mathfrak{M}} := \hat{\mathcal{R}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$;
- (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 $H_K := \text{Gal}(\hat{K}/K_\infty)$;
- (5) \hat{G} acts on $W(k)$ -module $M := \hat{\mathfrak{M}}/I_+\hat{\mathfrak{M}} \simeq \mathfrak{M}/u\mathfrak{M}$ trivially.

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

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

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

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

One can show that $T_{\mathfrak{S}}(\mathfrak{M})$ is finite \mathbb{Z}_p -free and $\text{rank}_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M}) = \text{rank}_{\mathfrak{S}} \mathfrak{M}$ (see for example Corollary (2.1.4) in [Kis06]). Let $\text{Rep}_{\mathbb{Z}_p}[G_\infty]$ denote the category of continuous G_∞ -representations on finite free \mathbb{Z}_p -modules. The functor $T_{\mathfrak{S}}$ from $\text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$ to $\text{Rep}_{\mathbb{Z}_p}[G_\infty]$ is fully faithful (see Proposition (2.1.12) in [Kis06] or Corollary 4.2.6 in [Liu07]).

Remark 2.1.1. Usually, $T_{\mathfrak{S}}(\mathfrak{M})$ is defined as $\text{Hom}_{\varphi, \mathfrak{S}}(\mathfrak{M}, \mathfrak{S}^{\text{ur}})$ in [Kis06] or [Liu10], where \mathfrak{S}^{ur} is a subring of $W(R)$. But Lemma 2.2.1 in [CL] shows that these two definitions are equivalent.

We refer readers to [Fon94b] for definitions and basic facts on semi-stable representations and crystalline representations. The following summarizes the main result of [Liu10] 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 (φ, \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 (φ, \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:

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

Remark 2.1.3. Here we only care about crystalline representations with Hodge-Tate weights in $\{0, 1\}$ while the main result in [Liu10] deals with (φ, \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 [Tat67] and the appendix of [Kis06] for details. Let $\text{Rep}_{\mathbb{Q}_p}^{\text{cris},1}$ denote the category of crystalline representations of G with Hodge-Tate weights in $\{0, 1\}$ and $\text{Rep}_{\mathbb{Z}_p}^{\text{cris},1}$ denote the category of G -stable \mathbb{Z}_p -lattices in objects in $\text{Rep}_{\mathbb{Q}_p}^{\text{cris},1}$. We summarize several important results on Barsotti-Tate groups and crystalline representations into the following theorem.

Theorem 2.2.1. *There exists an equivalence between the category of Barsotti-Tate groups over \mathcal{O}_K and the category $\text{Rep}_{\mathbb{Z}_p}^{\text{cris},1}$.*

Proof. Let H be a Barsotti-Tate group over \mathcal{O}_K , $T_p(H)$ the p -adic Tate module of H and $V_p(H) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(H)$. It is Fontaine ([Fon79]) who proved that $V_p(H)$ is crystalline with Hodge-Tate weights in $\{0, 1\}$. Hence we have a functor $H \mapsto T_p(H)$ from the category of Barsotti-Tate groups over \mathcal{O}_K to the category $\text{Rep}_{\mathbb{Z}_p}^{\text{cris},1}$. The functor is fully faithful by Tate's isogeny theorem in [Tat67]. The proof for essentially surjectiveness of the functor needs two ingredients. First, Corollary (2.2.6) in [Kis09a] proved 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 [Ray74]. \square

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

The above proposition was proved in [Kis06] (see Proposition (2.2.2) in [Kis06]). Here we use a slightly different approach which will be useful later. Let $\text{Fil}^1 S$ denote the ideal in S generated by $E(u)$ and $\frac{E(u)^i}{i!}$ for $i \geq 1$. Note that $\varphi(\text{Fil}^1 S) \subset pS$ and we write $\varphi_1 = \varphi/p : \text{Fil}^1 S \rightarrow S$. A *Breuil module* is a data $(\mathcal{M}, \text{Fil}^1 \mathcal{M}, \varphi_1, N)$ where

- (1) \mathcal{M} is a finite free S -module.
- (2) $\text{Fil}^1 \mathcal{M}$ is a submodule of \mathcal{M} such that $\text{Fil}^1 S \mathcal{M} \subset \text{Fil}^1 \mathcal{M}$ and $\mathcal{M}/\text{Fil}^1 \mathcal{M}$ is finite \mathcal{O}_K -free.
- (3) $\varphi_1 : \text{Fil}^1 \mathcal{M} \rightarrow \mathcal{M}$ is a φ_S -semi-linear map such that $\varphi_1(\text{Fil}^1 \mathcal{M})$ generates \mathcal{M} and $\varphi_1(sm) = (c_1)^{-1} \varphi_1(s) \varphi_1(E(u)m)$ for $s \in \text{Fil}^1 S$ and $m \in \mathcal{M}$ with $c_1 = \varphi_1(E(u)) \in S^*$.
- (4) $N : \mathcal{M} \rightarrow \mathcal{M}$ 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 $x \in \text{Fil}^1 \mathcal{M}$.

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 other structures. There is a functor from $\text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$ to the category of Breuil modules defined below. Let $\mathfrak{M} \in \text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$. Define $\mathcal{M} := S \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$ and note that we have an S -linear map $1 \otimes \varphi : \mathcal{M} \rightarrow S \otimes_{\mathfrak{S}} \mathfrak{M}$. Set

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

and

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

One can easily check that $\text{Fil}^1 \mathcal{M}$ and φ_1 constructed satisfies the axioms (1) (2) (3) in the definition of Breuil module (see §(1.1.8) in [Kis09b]). The construction of the monodromy operator N is slightly more complicated. In fact, given $\mathfrak{M} \in \text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$, such N will *uniquely* exists if we further require that $N(\mathcal{M}) \subset I_+ S \mathcal{M}$, where $I_+ S := S \cap uK_0[[u]]$ if we regard S as a subring of $K_0[[u]]$. We follow the idea of Proposition 5.1.3 in [Bre00] to construct such N . Let $L : \mathcal{M} \rightarrow \mathcal{M}$ 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 $x_1, \dots, x_d \in \text{Fil}^1 \mathcal{M}$ such that $\{e_i := \varphi_1(x_i) \mid i = 1, \dots, d\}$ 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, 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 that $N_S(u) = -u$ and that $s = \sum_{i=0}^{\infty} a_i(u) \gamma_i(E(u))$ 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 $x \in \text{Fil}^1 \mathcal{M}$, as $\text{Fil}^1 \mathcal{M}$ is generated by x_i and $\text{Fil}^1 S \mathcal{M}$. 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

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

with A a matrix having coefficients in $\varphi(I_+ S)$. So $N - N'$ must be zero map and thus $N = N'$. 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} . The above proof contains a useful fact:

Lemma 2.2.3. $N^i(\mathfrak{M}) \subset u^p \tilde{\mathcal{M}}$ for each $i \geq 1$.

Proof. It suffices to prove the case $i = 1$ as the general case easy follows the induction on i . Let f_1, \dots, f_d be an \mathfrak{S} -basis of \mathfrak{M} . We easily see that there exists $x_1, \dots, x_d \in (\mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}) \cap \text{Fil}^1 \mathcal{M}$ such that $e_i = \varphi_1(x_i) = c_1 f_i$ is an basis of \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 $N(f_i) = N(c_1^{-1} e_i) + c_1^{-1} N(e_i) \in u^p \tilde{\mathcal{M}}$. Hence $N(\mathfrak{M}) \subset u^p \tilde{\mathcal{M}}$ as \mathfrak{M} is an $\varphi(\mathfrak{S})$ -submodule of \mathcal{M} . □

For each Breuil module \mathcal{M} , one define φ_S -semi-linear morphism $\varphi_{\mathcal{M}} : \mathcal{M} \rightarrow \mathcal{M}$ 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 the 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 $A_{\text{cris}} \otimes_S \mathcal{M} \simeq A_{\text{cris}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$. Using the monodromy operator N , we can define an A_{cris} -semi-linear G -action on $A_{\text{cris}} \otimes_S \mathcal{M}$ via

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

As Lemma 5.1.1 in [Liu08], we can show that the G -action preserves the φ -structure and $\text{Fil}^1(A_{\text{cris}} \otimes_S \mathcal{M}) := \text{Fil}^1 A_{\text{cris}} \otimes_S \mathcal{M} + A_{\text{cris}} \otimes_S \text{Fil}^1 \mathcal{M}$. Therefore, one can associate a $\mathbb{Z}_p[G]$ -module via

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

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

We need to show that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M})$ 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 [Liu08], we have a natural $\mathbb{Q}_p[G]$ -isomorphism between $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M})$ and $V_{\text{st}}(\mathcal{D}) := \text{Hom}_{S, \varphi, \text{Fil}^1, N}(\mathcal{D}, \widehat{A}_{\text{st}}[\frac{1}{p}])$, where \widehat{A}_{st} is the period ring constructed in [Bre97]. Proposition 2.2.5 in [Bre02] shows ² that $V_{\text{st}}(\mathcal{D})$ is semi-stable with Hodge-Tate weights with $\{0, 1\}$. Let D be the filtered (φ, N) -module associated to the semi-stable representation $V_{\text{st}}(\mathcal{D})$ via Fontaine's theory. Breuil's theory in [Bre97] show that one can recover N on D via $N_{\mathcal{D}} \bmod I_+ S\mathcal{D}$. Since $N(\mathcal{M}) \subset u^p \mathcal{M}$ by Lemma 2.2.3, we have $N_D = 0$ and then $V_{\text{st}}(\mathcal{D})$ must be crystalline.

Let us construct a \mathbb{Z}_p -linear map $\lambda : T_{\mathfrak{S}}(\mathfrak{M}) \rightarrow \tilde{T}_{\text{cris}}(\mathcal{M})$. Note that $A_{\text{cris}} \otimes_S \mathcal{M} = A_{\text{cris}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$. For each $f \in T_{\mathfrak{S}}(\mathfrak{M})$, set $\lambda(f)(a \otimes m) = a\varphi(f(m))$ for $a \in A_{\text{cris}}$ and $m \in \mathfrak{M}$. It is routine to check that λ is injective and compatible with G_{∞} -actions. Since $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M})) = \dim_{\mathbb{Q}_p} V_{\text{st}}(\mathcal{D}) = \dim_{K_0} D = \text{rank}_S \mathcal{M} = \text{rank}_{\mathfrak{S}} \mathfrak{M} = \text{rank}_{\mathbb{Z}_p}(T_{\mathfrak{S}}(\mathfrak{M}))$, we see that $\lambda[\frac{1}{p}] : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_{\mathfrak{S}}(\mathfrak{M}) \rightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M})$ 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 $\tilde{T}_{\text{cris}}(\mathcal{M}) \simeq T_{\text{cris}}(\mathcal{M}) := \text{Hom}_{S, \varphi, \text{Fil}^1}(\mathcal{M}, A_{\text{cris}})$ as $\mathbb{Z}_p[G_{\infty}]$ -modules and this fact is also valid if $p = 2$. Second, by Lemma 3.3.4 in [Liu08], the map $\lambda' : T_{\mathfrak{S}}(\mathfrak{M}) \rightarrow T_{\text{cris}}(\mathcal{M})$ 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 [Liu07].

In summary of the above discussion, we have a functor ι from the category $\text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$ to category $\text{Rep}_{\mathbb{Q}_p}^{\text{cris}, 1}$ via

$$\iota : \mathfrak{M} \mapsto T_{\mathfrak{S}}(\mathfrak{M}) \xrightarrow{\lambda} \tilde{T}_{\text{cris}}(\mathcal{M}) \hookrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M}).$$

Now suppose that $(\mathfrak{M}, \varphi, \hat{G})$ is a (φ, \hat{G}) -module such that $\hat{T}(\hat{\mathfrak{M}})$ is a G -stable \mathbb{Z}_p -lattice in an object in $\text{Rep}_{\mathbb{Q}_p}^{\text{cris}, 1}$. Note that $\hat{\mathfrak{M}} = \hat{\mathcal{R}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \subset A_{\text{cris}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$. It

²Strictly speaking, Prop. 2.2.5 in [Bre02] is only a sketch of the proof, one need check carefully the details of the proof in [Bre99]. In particular, to check the case $p = 2$.

is routine to check the natural map

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

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

$$(2.2.2) \quad \begin{array}{ccc} T_{\mathfrak{S}}(\mathfrak{M}) & \xrightarrow{\lambda} & \tilde{T}_{\mathrm{cris}}(\mathcal{M}) \\ & \searrow \theta & \uparrow \hat{\lambda} \\ & & \hat{T}(\widehat{\mathfrak{M}}). \end{array}$$

Furthermore $\hat{\lambda}$ is compatible with G -actions on the both sides. This is the consequence of the construction of the \hat{G} -action on $\widehat{\mathfrak{M}}$. In particular, the G -action on $A_{\mathrm{cris}} \otimes_{\widehat{\mathcal{R}}} \widehat{\mathfrak{M}} = A_{\mathrm{cris}} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$ is given by formula (2.2.1). The readers are refer to Section 3.2 in [Liu10] for full details. Finally, the full faithfulness and essential surjectiveness of ι can be proved by the full faithfulness and essential surjectiveness of \hat{T} in Theorem 2.1.2. Here we actually do not need the the full faithfulness and essential surjectiveness of ι .

Remark 2.2.5. Note that ι is a contravariant functor. To obtain a covariant functor, we can just define $\iota'(\mathfrak{M}) = (\iota(\mathfrak{M}))^\vee(1)$, where \vee means taking dual and (1) means twisting by the cyclotomic character.

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 devotes to prove the above Proposition. Let us assume this Proposition. Now we have a functor $\mathfrak{M} \mapsto \lambda(T_{\mathfrak{S}}(\mathfrak{M}))$ from the category $\mathrm{Mod}_{/\mathfrak{S}}^{1, \mathrm{fr}}$ to the category $\mathrm{Rep}_{\mathbb{Z}_p}^{\mathrm{cris}, 1}$. The full faithfulness of the functor follows from the full faithfulness of the functor $T_{\mathfrak{S}}$ and that λ is injective. The essential surjectiveness follows Theorem 2.1.2 and diagram (2.2.2). So the functor induces an equivalence between the category $\mathrm{Mod}_{/\mathfrak{S}}^{1, \mathrm{fr}}$ and the category $\mathrm{Rep}_{\mathbb{Z}_p}^{\mathrm{cris}, 1}$. Then Theorem 1.0.1 is proved by 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}^+

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

We write $I^{[1]} := W(R) \cap I^{[1]}B_{\mathrm{cris}}^+$. Since $\varphi(t) = pt$, we see that $t \in I^{[1]}B_{\mathrm{cris}}^+$. By Proposition 5.1.3 in [Fon94a], $I^{[1]}$ is a principal ideal and $[\epsilon] - 1$ 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 $\mathfrak{t} \not\equiv 0 \pmod{p}$ in $W(R)$. Such \mathfrak{t} is unique up to units of \mathbb{Z}_p , see Example 2.3.5 in [Liu07] for details. In the proof of Lemma 3.2.2 in [Liu10], it has been proved that $\varphi(\mathfrak{t})$ is a generator of $I^{[1]}$. Since $I^{[1]}$ and $u\mathfrak{t}W(R)$ are obviously φ -stable inside $W(R)$, there are natural Frobenius on $W(R)/uI^{[1]}$ and $W(R)/u\mathfrak{t}W(R)$. Define

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

and

$$(3.1.2) \quad J(\mathfrak{M}) = \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}, W(R)/uW(R)).$$

The natural projections $W(R) \rightarrow W(R)/u\varphi(\mathfrak{t})W(R) \rightarrow W(R)/uW(R)$ induce the following commutative diagram of natural maps

$$\begin{array}{ccc} T_{\mathfrak{S}}(\mathfrak{M}) & \xrightarrow{\eta'} & J'(\mathfrak{M}) \\ & \searrow \eta & \downarrow \mu \\ & & J(\mathfrak{M}). \end{array}$$

Proposition 3.1.1. (1) η and η' are injective.
(2) $\mu(J'(\mathfrak{M})) = \eta(T_{\mathfrak{S}}(\mathfrak{M}))$.

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 $X = (h(e_1), \dots, h(e_d))$ is in $u\mathfrak{t}W(R)$ and satisfies the relation $\varphi(X) = XA$. Write $X = u\mathfrak{t}Y$ with Y 's coefficients in $W(R)$. We have $\varphi(X) = \varphi(u\mathfrak{t}Y) = u\mathfrak{t}YA$. So $u^p\varphi(\mathfrak{t})\varphi(Y) = u\mathfrak{t}YA$. Note that $\varphi(\mathfrak{t}) = c_0^{-1}E(u)\mathfrak{t}$ and there exists a matrix B such that $AB = BA = E(u)I$. We obtain $Y = u^{p-1}c_0^{-1}\varphi(Y)B$. Then

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

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

Now let us prove (2), suppose that $h \in J'(\mathfrak{M})$ and let X be a vector with coefficients 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 coefficients of Y in $W(R)$ and A the matrix of φ under 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

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

Note that there exists a matrix B such that $AB = BA = E(u)I$. 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:

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

which is equivalent to

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

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 Z_l converges 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

$$Z_{l+1} - Z_l = \left(\prod_{i=0}^{l-1} \varphi^i(c_0^{-1}u^{p-1}) \right) (Z_1 - Z_0) (\varphi^{l-1}(B) \dots \varphi(B)B) \longrightarrow 0, \text{ as } l \rightarrow +\infty.$$

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.

Proof. Obviously, (2) is the consequence of (1) by the above Proposition. So it suffices to show (1). Let us first treat $J'(\mathfrak{M})$. Note that there is a natural G -action on $W(R)/uI^{[1]}$ as $uI^{[1]}$ is G -stable in $W(R)$. Let $h \in J'(\mathfrak{M})$, $g \in G$. 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 $g(u) - u = u([\underline{\varepsilon}(g)] - 1) \in uI^{[1]}$, 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 $utW(R)$ is G -stable in $W(R)$. To see this, for each $x = uty \in utW(R)$ with $y \in W(R)$, we have $\varphi(x) = u^p\varphi(t)\varphi(y) \in u^pI^{[1]}$. It is easy to check that $u^pI^{[1]}$ is G -stable in $W(R)$. Namely, for each $g \in G$, $g(\varphi(x)) = u^p\varphi(t)z$ with $z \in W(R)$ as $\varphi(t)$ is a generator of $I^{[1]}$. Hence there exists a $w \in W(R)$ such that $g(x) = utw$ with $\varphi(w) = z$ because $\varphi : W(R) \rightarrow W(R)$ is a bijection. \square

Corollary 3.1.3. *If $f : T_{\mathfrak{S}}(\mathfrak{M}) \rightarrow T_{\mathfrak{S}}(\mathfrak{N})$ 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 $\mathfrak{f} : \mathfrak{N} \rightarrow \mathfrak{M}$ in $\text{Mod}_{\mathfrak{S}}^{1, \text{fr}}$ 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 3.1.1, f is a morphism of $\mathbb{Z}_p[G]$ -modules. \square

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 $\iota(\mathfrak{M}) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}_{\text{cris}}(\mathcal{M})$ 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 a (φ, \hat{G}) -modules $(\mathfrak{L}, \varphi_{\mathfrak{L}}, \hat{G}_{\mathfrak{L}})$ 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, without loss of generality, we can assume that $\lambda(T_{\mathfrak{S}}(\mathfrak{M}))$ is G -stable and let $(\mathfrak{M}, \varphi, \hat{G})$ be the corresponding (φ, \hat{G}) -module of height 1. Recall from Theorem 2.1.2 (1) that there exists a natural $\mathbb{Z}_p[G_{\infty}]$ -isomorphism $\theta : T_{\mathfrak{S}}(\mathfrak{M}) \rightarrow \hat{T}(\mathfrak{M})$, which is given by

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

Now define

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

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

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

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 $W(R)/utW(R)$ and $W(R)/u^p\varphi(t)W(R)$, 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:

$$\begin{array}{ccc} T_{\mathfrak{S}}(\mathfrak{M}) & \xrightarrow{\sim \theta} & \hat{T}(\hat{\mathfrak{M}}) \\ \downarrow \eta & & \downarrow \hat{\eta} \\ J(\mathfrak{M}) & \xrightarrow{\sim \tilde{\theta}} & \hat{J}(\hat{\mathfrak{M}}) \end{array}$$

where $\hat{\eta}$ is defined by the projection $W(R) \rightarrow W(R)/u^p\varphi(t)W(R)$. 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 the G -action on $\hat{J}(\hat{\mathfrak{M}})$ via the isomorphism $\tilde{\theta}$. Now we reduce the proof of Proposition 2.3.1 to the following Proposition.

Proposition 3.2.1. *Notations as the 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 $a_i \in \hat{\mathcal{R}}$, we have to show that

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

By definition,

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

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

$$(g \circ \beta')\left(\sum_i a_i \otimes e_i\right) = \sum_i a_i g\left(\beta'(1 \otimes e_i)\right) \equiv \sum_i a_i g\left(\varphi(\alpha(e_i))\right) \pmod{u^p \varphi(\mathfrak{t})W(R)}.$$

We claim that $g^{-1}(1 \otimes e_i) \equiv 1 \otimes e_i \pmod{\tilde{I}\hat{\mathfrak{M}}}$ where $\tilde{I} = (u^p \varphi(\mathfrak{t})W(R)) \cap \hat{\mathcal{R}}$ ³. Let us accept this claim and postpone the proof in the end. Thus we have

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

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 $\gamma_i(-\log([\underline{\epsilon}(g)])) \in I^{[1]}B_{\text{cris}}^+$, then by Lemma 2.2.3, we obtain that

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

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

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

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

³It is not clear that $\tilde{I} = u^p \varphi(\mathfrak{t})\hat{\mathcal{R}}$ as $I_+S \neq uS$. Fortunately, we do not need this fact.

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

Proof. Write $y = ux$. It suffices to prove that for each integer $m > 0$ there exists $x_m, z_m \in W(R)$ such that $y = ux_m + p^m z_m$. To prove this, we first reduce the proof to the case that $x \in A_{\text{cris}}$. Assume that $p^s x \in A_{\text{cris}}$ and we are able to show 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 $W(R)$ followed by the fact that if $p|uw$ in $W(R)$ with $w \in W(R)$ then $p|w$ in $W(R)$. To prove that fact, note that $uw \equiv 0 \pmod{p}$. But $u \pmod{p} = \bar{\pi} \neq 0$ inside R , we conclude that $w \pmod{p} \equiv 0$ in R by the fact that R is an integral domain.

Now we may assume that $x \in A_{\text{cris}}$. Then x can be written as $x = \sum_{i=0}^{\infty} a_i \frac{E(u)^i}{i!}$ 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 $\tilde{x}_i = \sum_{j=0}^i p^{n_i} a_j \frac{E(u)^j}{j!}$ and $\tilde{z}_i = p^{n_i} \sum_{j=i+1}^{\infty} ua_j \frac{E(u)^j}{j!}$. We observe that \tilde{x}_i is in $W(R)$ and \tilde{z}_i is $\text{Fil}^{i+1} A_{\text{cris}} \cap W(R)$, 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 $E(u)^{i+1} = p^{i+1} a_i + uw_i$ with $a_i \in W(k)$ and $w_i \in W(k)[u]$. Now we get $p^{n_i} y = u\tilde{x}_i + p^{i+1} a_i \beta_i + uw_i \beta_i = ux'_i + p^{i+1} z'_i$ where $x'_i = \tilde{x}_i + w_i \beta_i$ and $z'_i = a_i \beta_i$. 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 $i_m + 1 - n_{i_m} \rightarrow +\infty$ as $m \rightarrow \infty$. 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 $i_m + 1 - n_{i_m} = m + 1 \rightarrow +\infty$. □

REFERENCES

- [Bre] Christophe Breuil, *Schémas en groupes et corps des normes*, Unpublished.
- [Bre97] ———, *Représentations p -adiques semi-stables et transversalité de Griffiths*, Math. Ann. **307** (1997), no. 2, 191–224.
- [Bre99] ———, *Représentations semi-stables et modules fortement divisibles*, Invent. Math. **136** (1999), no. 1, 89–122.
- [Bre00] ———, *Groupes p -divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), no. 2, 489–549.
- [Bre02] ———, *Integral p -adic Hodge theory*, Algebraic geometry 2000, Azumino (Hotaka), Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan, Tokyo, 2002, pp. 51–80.
- [CL] Xavier Caruso and Tong Liu, *Some bounds for ramification of p^n -torsion semi-stable representations*, Preprint, appear at Journal of Algebra.
- [Fon79] Jean-Marc Fontaine, *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate*, Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III, Astérisque, vol. 65, Soc. Math. France, Paris, 1979, pp. 3–80. MR MR563472 (82k:14046)
- [Fon94a] ———, *Le corps des périodes p -adiques*, Astérisque (1994), no. 223, 59–111.
- [Fon94b] ———, *Représentations p -adiques semi-stables*, Astérisque (1994), no. 223, 113–184, With an appendix by Pierre Colmez, Périodes p -adiques (Bures-sur-Yvette, 1988).
- [Kim10] Wansu Kim, *The classification of p -divisible groups over 2-adic discrete valuation rings*, Preprint, arXiv:1007.1904 (2010).
- [Kis06] Mark Kisin, *Crystalline representations and F -crystals*, Algebraic geometry and number theory, Progr. Math., vol. 253, Birkhäuser Boston, Boston, MA, 2006, pp. 459–496.

- [Kis09a] ———, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. **178** (2009), no. 3, 587–634.
- [Kis09b] ———, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180.
- [Lau] Eike Lau, *A relation between dieudonne displays and crystalline dieudonne theory*, arXiv:1006.2720.
- [Liu07] Tong Liu, *Torsion p -adic Galois representations and a conjecture of fontaine.*, Ann. Sci. École Norm. Sup. (4) **40** (2007), no. 4, 633–674.
- [Liu08] ———, *On lattices in semi-stable representations: a proof of a conjecture of Breuil*, Compos. Math. **144** (2008), no. 1, 61–88.
- [Liu10] ———, *A note on lattices in semi-stable representations*, Mathematische Annalen **346** (2010), no. 1, 117–138.
- [Ray74] Michel Raynaud, *Schémas en groupes de type (p, \dots, p)* , Bull. Soc. Math. France **102** (1974), 241–280.
- [Tat67] J. T. Tate, *p -divisible groups.*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183.

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, 47907, USA.

E-mail address: `tongliu@math.purdue.edu`,