Kisin's classification of p-divisible groups over regular local rings

Adrian Vasiu and Thomas Zink

August 13, 2007

Abstract. Let k be a perfect field of characteristic $p \geq 3$. We classify in terms of Kisin modules the p-divisible groups over regular rings of the form $W(k)[[t_1, \ldots, t_r, u]]/(u^e + pb_{e-1}u^{e-1} + \ldots + pb_1u + pb_0)$, where $b_0, \ldots, b_{e-1} \in W(k)][[t_1, \ldots, t_r]]$ and b_0 is an invertible element.

MSC 2000: 11G10, 11G18, 14F30, 14G35, 14K10, and 14L05.

1 Introduction

Let $p \in \mathbb{N}$ be an odd prime. Let k be a perfect field of characteristic p. Let $W(k)$ be the ring of Witt vectors with coefficients in k and let $B(k)$ be the field of fractions of $W(k)$. Let $r \in \mathbb{N} \cup \{0\}$. We consider the ring of formal power series

$$\mathfrak{S} := W(k)[[t_1, \ldots, t_r, u]].$$

We extend the Frobenius endomorphism σ of $W(k)$ to $\mathfrak{S}$ by the rules

$$\sigma(t_i) = t_i^p \quad \text{and} \quad \sigma(u) = u^p. \tag{1}$$

If M is a $\mathfrak{S}$-module we define

$$M^{(\sigma)} := \mathfrak{S} \otimes_{\sigma, \mathfrak{S}} M.$$

Let $e \in \mathbb{N}$. Let

$$E = E(u) = u^e + a_{e-1}u^{e-1} + \cdots + a_1u + a_0$$

be a polynomial with coefficients in $W(k)[[t_1,\ldots,t_r]]$ such that p divides a_i for all $i\in\{0,\ldots,e-1\}$ and moreover a_0/p is a unit in $W(k)[[t_1,\ldots,t_r]]$. The polynomial E is irreducible by the Eisenstein criterion applied modulo the ideal $(t_1,\ldots,t_r)$.

We define

$$R:=\mathfrak{S}/E\cdot\mathfrak{S};$$

it is a regular local ring of dimension $r+1$ with parameter system $t_1,\ldots,t_r,u$.

The following definition is suggested by Kisin's work on crystalline representations (see [K], etc.).

Definition 1 *A Kisin module relative to $\mathfrak{S}\to R$ is a free $\mathfrak{S}$-module M of finite rank which is equipped with a homomorphism $\phi: M\to M^{(\sigma)}$ whose cokernel is annihilated by E.*

We note down that the cokernel of ϕ is then a free R-module. Indeed, since $\mathfrak{S}$ and R are regular local rings it follows that the depth of this cokernel over $\mathfrak{S}$ (or R) is equal to the of dimension R and thus the cokernel is free over R.

The goal of the paper is to prove the following result whose validity is suggested by previous works of Breuil and Kisin (see [Br], [K], etc.).

Theorem 1 *The category of p-divisible groups over R is equivalent to the category of Kisin modules relative to $\mathfrak{S}\to R$.*

This theorem was proved by Kisin in the case $r=0$ (see [K]). We prove the generalization by a new method which uses the theory of windows and displays developed in [Z3] and elementary matrix computations. One can easily get a version of Theorem 1 for $p=2$, provided one restricts to connected p-divisible groups over R and to connected Kisin modules relative to $\mathfrak{S}\to R$. One can view Theorem 1 as a ramified analogue of Faltings deformation theory over rings of the form $W(k)[[t_1,\ldots,t_r]]$ (see [F, Thm. 10]). The importance of Theorem 1 stems from its potential applications to modular and moduli properties and aspects of Shimura varieties of Hodge type.

2 Kisin modules

Let $a\geq 1$ be an integer. We define $\mathfrak{S}_a:=\mathfrak{S}/(u^{ae})$; it is a torsionfree p-adic ring. The element E of $\mathfrak{S}_a$ (i.e., the reduction of E modulo (u^{ae})) is not a zero divisor in $\mathfrak{S}_a$. The Frobenius endomorphism σ of $\mathfrak{S}$ induces naturally a Frobenius endomorphism σ of $\mathfrak{S}_a$.

We write

$$E = u^e + p\epsilon, \tag{2}$$

where $\epsilon := (a_{e-1}/p)u^{e-1} + \ldots + (a_1/p)u + (a_0/p)$ is a unit in $\mathfrak{S}$. We have identities

$$\mathfrak{S}_a/(E) = \mathfrak{S}/(E, p^a) = R/p^a R,$$

because $u^{ae} \equiv p^a \epsilon^a$ modulo the ideal (E).

Definition 2 *A $\mathfrak{S}_a$-window is a triple (P, Q, F), where P is a free $\mathfrak{S}_a$-module of finite rank, Q is a $\mathfrak{S}_a$-submodule of P, and $F : P \to P$ is a σ-linear map, such that the following two axioms hold:*

(i) $E \cdot P \subset Q$ and P/Q is a free $R/p^a R$-module.

(ii) $F(Q) \subset \sigma(E) \cdot P$ and $F(Q)$ generates $\sigma(E) \cdot P$ as a $\mathfrak{S}$-module.

We define $F_1 := (1/\sigma(E))F : Q \to P$. This makes sense because $\sigma(E)$ is not a zero divisor in $\mathfrak{S}_a$.

We have also the notion of a $\mathfrak{S}$-window. It has the same definition but the index a is removed. In this case P/Q is a free R-module.

Each $\mathfrak{S}_a$-window has a *normal decomposition*:

$$P = T \oplus L, \quad Q = E \cdot T \oplus L. \tag{3}$$

The map

$$F \oplus F_1 : T \oplus L \to P \tag{4}$$

is a σ-linear isomorphism. Conversely such a σ-linear isomorphism defines naturally a $\mathfrak{S}_a$-window. Choosing a $\mathfrak{S}_a$-basis of $T \oplus L$, one can identify a $\mathfrak{S}_a$-window with an invertible matrix with coefficients in $\mathfrak{S}_a$.

From the normal decomposition we see that Q is a free $\mathfrak{S}_a$-module. Indeed, E is not a zero divisor in $\mathfrak{S}_a$. We see that the $\mathfrak{S}_a$-linear map

$$F_1^\sharp : \mathfrak{S}_a \otimes_{\sigma, \mathfrak{S}_a} Q \to P \tag{5}$$

induced by F_1 is an isomorphism.

The notion of a $\mathfrak{S}_a$-window was first introduced by Kisin in the following form:

Definition 3 *A Kisin module relative to $\mathfrak{S}_a \to R/p^aR$ (or over $\mathfrak{S}_a$) is a free $\mathfrak{S}_a$-module M of finite rank which is equipped with a homomorphism $\phi : M \to M^{(\sigma)}$ whose cokernel is annihilated by E and is a free R/p^aR-module.*

If $\mathcal{P} = (P, Q, F, F_1)$ is a $\mathfrak{S}_a$-window, we can identify $Q^{(\sigma)} := \mathfrak{S}_a \otimes_{\sigma,\mathfrak{S}_a} Q$ with P by (5). The inclusion $Q \subset P$ induces a $\mathfrak{S}_a$-linear map $\phi : Q \to Q^{(\sigma)}$. This is a Kisin module relative to $\mathfrak{S}_a \to R/p^aR$.

Conversely let $\phi : M \to M^{(\sigma)}$ be a Kisin module relative to $\mathfrak{S}_a \to R/p^aR$. Then we obtain a $\mathfrak{S}_a$-window by setting:

$$P = M^{(\sigma)} \quad \text{and} \quad Q = M.$$

The inclusion $Q \subset P$ is given by ϕ and $F_1 : Q \to P$ is given by the natural σ-linear map $M \to M^{(\sigma)}$ which takes m to $1 \otimes m$ for all $m \in M$. Finally we take $F(x) = F_1(Ex)$ for all $x \in P$.

Based on the last two paragraphs, we easily conclude that a Kisin module relative to $\mathfrak{S}_a \to R/p^aR$ is the same thing as a $\mathfrak{S}_a$-window.

In this paragraph we consider the case $a = 1$. In $\mathfrak{S}_1$ the elements E and p differ by a unit. Therefore the notion of a $\mathfrak{S}_1$-window is the same as that of a window relative to the frame $\mathfrak{S}_1 \to R/pR$. By [Z3] Introduction Thm. 6 it follows that the category of $\mathfrak{S}_1$-windows is equivalent to the category of p-divisible groups over R/pR.

We relate $\mathfrak{S}_a$-windows to Dieudonné displays. Let S be a complete local ring with residue field k and maximal ideal $\mathfrak{n}$. We denote by $\hat{W}(\mathfrak{n})$ the subring of all Witt vectors in $W(\mathfrak{n})$ whose components converge to zero in the $\mathfrak{n}$-adic topology. There is a unique subring $\hat{W}(S) \subset W(S)$, which is invariant by Frobenius F and Verschiebung V and which sits in a short exact sequence:

$$0 \to \hat{W}(\mathfrak{n}) \to \hat{W}(S) \to W(k) \to 0.$$

It is shown in [Z2] that the category of p-divisible groups over S is equivalent to the category of Dieudonné displays over $\hat{W}(S)$.

There is a unique homomorphism

$$\delta : \mathfrak{S} \to \hat{W}(\mathfrak{S}) \tag{6}$$

such that for all $x \in \mathfrak{S}$ we have $\mathbf{w}_n(\delta(x)) = \sigma^n(x)$. It maps $t_i \mapsto [t_i]$ and $u \mapsto [u]$. In the same way we obtain homomorphisms

$$\delta_a : \mathfrak{S}_a \to \hat{W}(\mathfrak{S}_a).$$

If we compose δ and δ_a with the canonical $W(k)$-homomorphisms $\hat{W}(\mathfrak{S}) \to \hat{W}(R)$ and $\hat{W}(\mathfrak{S}_a) \to \hat{W}(R/p^aR)$ (respectively) we obtain homomorphisms

$$\begin{array}{rcll} \varkappa: & \mathfrak{S} & \to & \hat{W}(R) \\ \varkappa_a: & \mathfrak{S}_a & \to & \hat{W}(R/p^a). \end{array} \tag{7}$$

We note that p is not a zero divisor in $\hat{W}(R)$.

Lemma 1 *The element $\varkappa(\sigma(E)) \in \hat{W}(R)$ is divisible by p and the fraction $\tau = \varkappa(\sigma(E))/p$ is a unit $\hat{W}(R)$.*

Proof: We have $\varkappa(E) \in V\hat{W}(R)$. Since $\varkappa$ is equivariant with respect to σ and the Frobenius F we find:

$$\varkappa(\sigma(E)) = F(\varkappa(E)) \in p\hat{W}(R).$$

We have to verify that $\mathbf{w}_0(\tau)$ is a unit in R. But we have:

$$\mathbf{w}_0(\tau) = \mathbf{w}_0(\varkappa(\sigma(E)))/p = \sigma(E)/p.$$

But since $p \geq 3$ the last element is clearly a unit in R. □

We are going to define a functor:

$$\mathfrak{S}_a - \text{windows} \longrightarrow \text{Dieudonné Displays over } R/p^aR. \tag{8}$$

Let (P, Q, F, F_1) be a $\mathfrak{S}_a$-window. To it we associate a Dieudonné display (P', Q', F', F_1') over R/p^aR as follows. We define $P' := \hat{W}(R/p^aR) \otimes_{\mathfrak{S}_a} P$. We define Q' to be the kernel of the natural homomorphism:

$$P' = \hat{W}(R/p^aR) \otimes_{\mathfrak{S}_a} P \to P/Q.$$

We define $F' : P' \to P'$ as the canonical F-linear extension of F. We define $F_1' : Q' \to P'$ by the rules:

$$\begin{array}{rcll} F_1'(\xi \otimes y) & = & {}^F\xi \otimes \tau F_1 y, & \text{for } \xi \in \hat{W}(R/p^aR) \text{ and } y \in Q, \\ F_1'({}^V\xi \otimes x) & = & \xi \otimes Fx, & \text{for } \xi \in \hat{W}(R/p^aR) \text{ and } x \in P. \end{array}$$

Using a normal decomposition one checks that (P', Q', F', F_1') is a Dieudonné display over $\hat{W}(R/p^aR)$.

Since the category of Dieudonné displays over $\hat{W}(R/p^aR)$ is equivalent to the category of p-divisible groups over R/p^aR (see [Z2]) we obtain from (8) a functor

$$\mathfrak{S}_a - \text{windows} \longrightarrow \ p - \text{divisible groups over } R/p^aR. \tag{9}$$

As we already noted this functor is an equivalence of categories for $a = 1$.

Lemma 2 *For each integer $a \geq 1$ the functor (9) is essentially surjective on objects.*

Proof: We prove this by induction on $a \in \mathbb{N}$. By [Z3] Thm. 3.2 the Lemma is true for $a = 1$. The inductive passage from a to $a + 1$ goes as follows.

Let $\tilde{\mathcal{P}}' = (\tilde{P}', \tilde{Q}', \tilde{F}', \tilde{F}_1')$ be a Dieudonné display over $R/p^{a+1}R$. We denote by $\mathcal{P}'$ its reduction over R/p^aR. Then we find by induction a $\mathfrak{S}_a$-window $\mathcal{P}$ which is mapped to $\mathcal{P}'$ by the functor (8). We lift $\mathcal{P}$ to a $\mathfrak{S}_{a+1}$-window $\tilde{\mathcal{P}}$. This is possible since a $\mathfrak{S}_a$-window is simply given by an invertible matrix with coefficients in R/p^aR which is liftable to an invertible matrix with coefficients in $R/p^{a+1}R$.

We apply to $\tilde{\mathcal{P}}$ the functor (8) and obtain a Dieudonné display $\tilde{\mathcal{P}}''$ over $R/p^{a+1}R$. By [Z2] Thm. 3 we may identify the triples associated to the Dieudonné displays $\tilde{\mathcal{P}}'$ and $\tilde{\mathcal{P}}''$. We denote this triple by

$$(\hat{W}(R/p^{a+1}R) \otimes_{\mathfrak{S}_{a+1}} \tilde{P} = \tilde{P}', \tilde{F}', \Phi_1). \tag{10}$$

Here $\Phi_1 : \breve{Q} \to \tilde{P}'$ is a Frobenius linear map from the inverse image of Q' in $\tilde{P}'$. Since we use the trivial divided powers on the kernel of $R/p^{a+1}R \to R/p^aR$, we have by definition $\Phi_1([p^a]\tilde{P}') = 0$. On the other hand the composite map:

$$\tilde{Q} \xrightarrow{\tilde{F}_1} \tilde{P} \to \tilde{P}' \xrightarrow{\tau} \tilde{P}',$$

coincides with the composite map

$$\tilde{Q} \to \breve{Q} \xrightarrow{\Phi_1} \tilde{P}'.$$

We define $\tilde{Q}^* \subset \tilde{P}$ as the inverse image of the map $\tilde{P} \to \tilde{P}'/\tilde{Q}'$ deduced from (10). The images of $\tilde{Q}$ and $\tilde{Q}^*$ by the canonical map $\tilde{P} \to P$ are the same. Therefore for each $y^* \in \tilde{Q}^*$ there is an $y \in \tilde{Q}$ such that we have $y^* = y + u^{ae}x$ for some $x \in \tilde{P}$. Since $\tilde{F}(u^{ae}x) = 0$ we conclude that

$F(y_1) = F(y) \in \sigma(E) \cdot \tilde{P}$. This proves that $\mathcal{P}^* = (\tilde{P}, \tilde{Q}^*, \tilde{F}, \tilde{F}_1)$ is a $\mathfrak{S}_{a+1}$-window.

We claim that the image $\mathcal{P}^*$ by the functor (8) coincides with the Dieudonné display $\tilde{\mathcal{P}}'$. For this we have to show that the map

$$\tilde{Q}^* \xrightarrow{\tilde{F}_1} \tilde{P} \to \tilde{P}' \xrightarrow{\tau} \tilde{P}',$$

coincides with the map

$$\tilde{Q}^* \to \breve{Q} \xrightarrow{\Phi_1} \tilde{P}'.$$

This follows again from the decomposition $y^* = y + u^{ae}x$ and the fact that the image of $u^{ae}x$ in $\breve{Q}$ is mapped to zero by Φ_1. We conclude that $\tilde{\mathcal{P}}'$ is in the essential image of the functor (8). This ends the induction. $\square$

3 Lifting Isomorphisms

We consider the rings:

$$\mathcal{T} := \mathfrak{S}[[v]]/(pv - u^e) \quad \text{and} \quad \mathcal{T}_a := \mathfrak{S}[[v]]/(pv - u^e, v^a).$$

In these rings we have $E = p(v + \epsilon)$ and therefore the elements p and E differ by a unit. We have isomorphisms:

$$\mathcal{T}/p\mathcal{T} \cong (R/pR)[[v]] \quad \text{and} \quad \mathcal{T}_a/p\mathcal{T}_a \cong (R/pR)[[v]]/(v^a).$$

We extend the Frobenius endomorphism σ to $\mathcal{T}$ and $\mathcal{T}_0$ by the rule:

$$\sigma(v) = u^{e(p-1)}v.$$

By very definitions we can identify $\mathcal{T}_1 = \mathfrak{S}_1 = \mathfrak{S}/(u^e)$.

We have the notion of a $\mathcal{T}_a$-window and equivalently of a Kisin module relative to $\mathcal{T}_a \to \mathcal{T}_a/p\mathcal{T}_a$. For instance, a $\mathcal{T}_a$-window is a quadruple (P, Q, F, F_1), where P is a free $\mathcal{T}_a$-module, Q is a $\mathcal{T}_a$-submodule of P such that P/Q is a free $\mathcal{T}_a/p\mathcal{T}_a$-module, $F : P \to P$ is a σ-linear map, and $F_1 : Q \to P$ is a σ-linear map whose linearization is surjective (and thus an isomorphism).Moreover for each $y \in Q$ we have an identity $F(y) = pF_1(y)$.

It follows from a normal decomposition of (P, Q, F, F_1), that Q is a free $\mathcal{T}_a$-module and therefore the notion of a $\mathcal{T}_a$-window and a Kisin module relative to $\mathcal{T}_a \to \mathcal{T}_a/p\mathcal{T}_a$ are the same.

Definition 4 *A normal decomposition of a Kisin module $\phi : M \to M^{(\sigma)}$ relative to $\mathfrak{S} \to R$ is a direct sum decomposition*

$$M = U \oplus L$$

such that we have an identity $M^{(\sigma)} = (1/E)\phi(U) \oplus \phi(L)$.

A normal decomposition is obtained as follows. We consider the short exact sequence:

$$0 \to M \xrightarrow{\phi} M^{(\sigma)} \to \bar{T} \to 0. \tag{11}$$

We choose a lift of $\bar{T}$ to a free $\mathfrak{S}$- module T and a lift $T \to M^{(\sigma)}$ of the $\mathfrak{S}$-linear epimorphism $M^{(\sigma)} \to \bar{T}$. Let $\bar{L} \subset R \otimes_{\mathfrak{S}} M$ be an R-submodule which maps isomorphically onto the kernel of the R-linear map $R \otimes_{\mathfrak{S}} M^{(\sigma)} \to \bar{T}$. We have a direct decomposition $M^{(\sigma)} = T \oplus \phi(L)$. The kernel M of the $\mathfrak{S}$-linear map $M^{(\sigma)} \to \bar{T}$ (i.e., $\phi(M)$) is then isomorphic to $E \cdot T \oplus \phi(L)$. Taking $U := \phi^{-1}(E \cdot T)$, we get the normal decomposition $M = U \oplus L$.

We define a normal decomposition of a Kisin module relative to $\mathfrak{S}_1 \to R/pR$ as above. A Kisin module (M, ϕ) relative to $\mathfrak{S} \to R$ induces by tensorization with $\mathfrak{S}/(u^e)\otimes_{\mathfrak{S}}$ a Kisin module $(\breve{M}, \breve{\phi})$ relative to $\mathfrak{S}_1 \to R/pR$. One can easily see that each normal decomposition of $(\breve{M}, \breve{\phi})$ lifts to a normal decomposition of (M, ϕ).

Proposition 1 *Let $\phi_1 : M_1 \to M_1^{(\sigma)}$ and $\phi_2 : M_2 \to M_2^{(\sigma)}$ be two Kisin modules relative to $\mathfrak{S} \to R$. Let $(\breve{M}_1, \breve{\phi}_1)$ and $(\breve{M}_2, \breve{\phi}_2)$ be the induced Kisin modules relative to $\mathfrak{S}_1 \to R/pR$. Let $\breve{\alpha} : \breve{M}_1 \to \breve{M}_2$ be an isomorphism of Kisin modules relative to $\mathfrak{S}_1 \to R/pR$ (i.e., a $\mathfrak{S}/(u^e)$-linear isomorphism such that we have an identity $\breve{\phi}_2 \circ \breve{\alpha} = (1 \otimes \breve{\alpha}) \circ \breve{\phi}_1$).*

Then there is a unique isomorphism

$$\alpha : \mathcal{T} \otimes_{\mathfrak{S}} M_1 \to \mathcal{T} \otimes_{\mathfrak{S}} M_2$$

which commutes in the natural sense with ϕ_1 and ϕ_2 and which lifts $\breve{\alpha}$ with respect to the $\mathfrak{S}$-epimorphism $\mathcal{T} \to \mathfrak{S}_1$ that maps v to 0.

Proof: We choose a normal decomposition $\breve{M}_1 = \breve{L}_1 \oplus \breve{U}_1$. Applying $\breve{\alpha}$ we obtain a normal decomposition $\breve{M}_2 = \breve{L}_2 \oplus \breve{U}_2$. We lift these normal decompositions to $\mathfrak{S}$:

$$M_1 = U_1 \oplus L_1, \qquad M_2 = U_2 \oplus L_2.$$

We find an isomorphism $\gamma : M_1 \to M_2$ which lifts $\breve{\alpha}$ and such that $\gamma(L_1) = L_2$ and $\gamma(U_1) = U_2$. We identify the modules M_1 and M_2 by γ and write:

$$M = M_1 = M_2, \quad U = U_1 = U_2, \quad \text{and} \quad L = L_1 = L_2.$$

We choose a basis $e_1, \ldots, e_d$ of U and a basis $e_{d+1}, \ldots e_r$ of L. Then $1 \otimes e_1, \ldots, 1 \otimes e_r$ is a basis of $M^{(\sigma)}$. We write $\phi_i : M \to M^{(\sigma)}$ for $i = 1, 2$ as matrices with respect to these basis. It follows from the properties of a normal decomposition that the matrices have the form:

$$A_i \begin{pmatrix} E \cdot I_d & 0 \\ 0 & I_c \end{pmatrix}$$

for $i = 1, 2$, where A_1 and A_2 are invertible matrices in $\mathrm{GL}_r(\mathfrak{S})$ and where $c := r - d$. By the construction of γ, the $\mathfrak{S}$-linear maps ϕ_1 and ϕ_2 coincide modulo (u^e). From this and the fact that E modulo (u^e) is a non-zero divisor of $\mathfrak{S}/(u^e)$, we get that we can write

$$(A_2)^{-1} A_1 = I_r + u^e Z, \tag{12}$$

where $Z \in M_r(\mathfrak{S})$. We set

$$C := \begin{pmatrix} E \cdot I_d & 0 \\ 0 & I_c \end{pmatrix}.$$

To find the isomorphism α is the same as to find a matrix $X \in \mathrm{GL}_r(\mathcal{T})$ which solves the equation

$$A_2 C X = \sigma(X) A_1 C \tag{13}$$

and whose reduction modulo the ideal (v) of $\mathcal{T}$ is the matrix representation of $\breve{\alpha}$ i.e., it is the identity matrix. Therefore we set:

$$X = I_r + vY \tag{14}$$

for a matrix $Y \in M_r(\mathcal{T})$.

As $E/p = v + \epsilon$ is a unit in the ring $\mathcal{T}$, the matrix pC^{-1} has coefficients in $\mathcal{T}$. Thus $D := pC^{-1} Z C \in M_r(\mathcal{T})$.

From the equations (13) and (14) we obtain the equation:

$$p(I_r + vY) = pC^{-1} A_2^{-1} (I_r + \sigma(v)\sigma(Y)) A_1 C.$$

By inserting (12) and the definition of D in this equation we get:

$$u^e Y = u^e D + (u^{ep}/p)pC^{-1}A_2^{-1}\sigma(Y)A_1C.$$

Since u^e is not a zero divisor in $\mathcal{T}$ we can write:

$$Y - (u^{e(p-1)}/p)pC^{-1}A_2^{-1}\sigma(Y)A_1C = D. \tag{15}$$

The σ-linear operator $\Psi(\bigstar) = (u^{e(p-1)}/p)pC^{-1}A_2^{-1}\sigma(\bigstar)A_1C$ on the $\mathcal{T}$-module $M_r(\mathcal{T})$ is topologically nilpotent. Therefore the equation(15) has a unique solution $Y = \sum_{n=0}^{\infty}\Psi(D) \in M_r(\mathcal{T})$. Therefore $X = I_r + vY \in \mathrm{GL}_r(\mathcal{T})$ exists and is uniquely determined. $\square$

3.1 Reductions modulo powers of u

There is a canonical homomorphism

$$\mathfrak{S}_a \to R/p^aR$$

whose kernel is the principal ideal of $\mathfrak{S}_a$ generated by E modulo (u^{ae}). Let

$$\mathcal{S}_a \subset \mathfrak{S}_a \otimes \mathbb{Q}$$

be the subring generated by all elements $u^{ne}/n!$ over $\mathfrak{S}_a$ with $n \in \{0, \ldots, a\}$. Then $\mathcal{S}_a$ is a p-adic ring without p-torsion. There is a commutative diagram

$$\begin{tikzcd} \mathfrak{S}_a \arrow[d] \arrow[dr] & \\ \mathcal{S}_a \arrow[r] & R/p^{\nu(a)}R, \end{tikzcd}$$

where $\nu(a) = \inf\{\mathrm{ord}_p(p^n)/n! \mid \text{for } n \geq a\}$ The lower horizontal map maps $u^{ne}/n!$ to $(p^n/n!)(-\epsilon)^n$ with the notation of (2). By [Z3] $\mathcal{S}_a \to R/p^{\nu(a)}R$, is a frame which classifies p-divisible groups over $R/p^{\nu(a)}R$.

Both $\mathcal{S}_a$ and $\mathcal{T}_a$ are naturally subrings of $\mathfrak{S}_a \otimes \mathbb{Q}$. Due to the identity

$$\frac{u^{ne}}{n!} = \frac{p^n}{n!}\left(\frac{u^e}{p}\right)^n = \frac{p^n}{n!}v^n$$

we have the inclusion of rings:

$$\mathcal{S}_a \subset \mathcal{T}_a.$$

The Frobenius morphism σ on $\mathfrak{S}$ induces a morphism

$$\mathfrak{S}_a \to \mathfrak{S}_{pa}.$$

It maps the subalgebra $\mathcal{T}_a \subset \mathfrak{S}_a \otimes \mathbb{Q}$ to $\mathcal{S}_{pa} \subset \mathfrak{S}_{pa} \otimes \mathbb{Q}$. We denote this map by

$$\tau_a : \mathcal{T}_a \to \mathcal{S}_{pa}.$$

Lemma 3 *Let $\phi_1 : M_1 \to M_1^{(\sigma)}$ and $\phi_2 : M_2 \to M_2^{(\sigma)}$ be two Kisin modules relative to $\mathfrak{S} \to R$. Let G_1 and G_2 be the corresponding p-divisible groups over R, cf. the functors (9). Then each isomorphism $\gamma : G_1 \to G_2$ is induced by a unique homomorphism of Kisin modules relative to $\mathfrak{S} \to R$.*

Proof: Since the category of Kisin modules relative to $\mathfrak{S}_1 \to R/pR$ is equivalent to the category of p-divisible groups over R/pR, the reduction of τ modulo p induces an isomorphism of the induced Kisin modules $(\breve{M}_i, \breve{\phi}_i)$ relative to $\mathfrak{S}_1 \to R/pR$ with $i = 1, 2$. Due to Proposition 1 we obtain an isomorphism of Kisin modules relative to $\mathcal{T} \to \mathcal{T}/p\mathcal{T}$. As in the proof of Proposition 1 we can identity normal decompositions $M_1 = U_1 \oplus L_1 = U_2 \oplus L_2 = M_2$ and we can represent the isomorphism of Kisin modules relative to $\mathcal{T} \to \mathcal{T}/p\mathcal{T}$ by an invertible matrix $X \in \mathrm{GL}_r(\mathcal{T})$.

The matrix X has the following crystalline interpretation. We denote by X_a the reduction of X over the ring $\mathcal{T}_a$.

The homomorphism $\mathcal{T}_a \to (R/pR)[[v]]/(v^a)$ is a pd-thickening. (This is not a frame in the sense of [Z3] because σ modulo p is not the Frobenius endomorphism of $\mathcal{T}_a/p\mathcal{T}_a$!) We have a morphism of pd-thickenings

$$\begin{tikzcd} \mathcal{S}_a \arrow[r] \arrow[d] & \mathcal{T}_a \arrow[d] \\ R/p^{\nu(a)}R \arrow[r] & (R/pR)[[v]]/(v^a). \end{tikzcd} \tag{16}$$

For crystals associated to p-divisible groups we refer to [M]. We know by [L] and [Z3] that the crystal of G_i evaluated at the pd-thickening $\mathcal{S}_a \to R/p^{\nu(a)}R$ coincides with $\mathcal{S}_a \otimes_{\mathfrak{S}_a} M_i^{(\sigma)}$. Let $\breve{G}_i$ be the pushforward of G_i by the canonical homomorphism $R \to (R/pR)[[v]]/(v^a)$. The diagram (16) shows that $\mathcal{T}_a \otimes_{\mathfrak{S}_a} M_i^{(\sigma)}$ is the crystal of $\breve{G}_i$ evaluated at the pd-thickening $\mathcal{T}_a \to (R/pR)[[v]]/(v^a)$. The isomorphism $\gamma : G_1 \to G_2$ induces an isomorphism of $\mathcal{S}_a$-windows α_a and via base change an isomorphism $\beta_a : (P_{1,a}, Q_{1,a}, F_{1,a}, F_{1,1,a}) \to$

$(P_{2,a}, Q_{2,a}, F_{2,a}, F_{2,1,a})$ of $\mathcal{T}_a$-windows. We note that after choosing a normal decomposition an $\mathcal{S}_a$-window is simply an invertible matrix with coefficients in $\mathcal{S}_a$ and the mentioned base change only applies to the coefficients the homomorphism $\mathcal{S}_a \to \mathcal{T}_a$. The sequence of morphisms $(\beta_a)_{a\in\mathbb{N}}$ induces naturally a morphism of Kisin modules relative to $\mathcal{T} \to \mathcal{T}/p\mathcal{T}$:

$$\beta : \mathcal{T} \otimes_{\mathfrak{S}} (M_1, \phi_1) \to \mathcal{T} \otimes_{\mathfrak{S}} (M_2, \phi_2). \tag{17}$$

We continue the base change (16) using the following diagram of pd-thickenings:

$$\begin{tikzcd} \mathcal{T}_a \arrow[r] \arrow[d] & \mathfrak{S}_1 \arrow[d] \\ (R/pR)[[v]]/(v^a) \arrow[r] & R/pR. \end{tikzcd} \tag{18}$$

From α_a we obtain by base change the morphism $\breve{\alpha}$ since windows associated to p-divisible groups commute with base change. But this shows that the isomorphism β coincides with the isomorphism α of Proposition 1, which we have represented by the matrix $X \in \mathrm{GL}_r(\mathcal{T})$. In other words for each $a \in \mathbb{N}$, the $\mathcal{T}_a$-linear isomorphism $Q_{1,a} \to Q_{2,a}$ is defined by the matrix X_a and the isomorphism β_a (i.e., $P_{1,a} \to P_{2,a}$) is induced naturally by $\sigma(X_a)$.

We will show by induction on a that the matrix X_a has coefficients in $\mathfrak{S}_a$. As we have inclusions $\mathfrak{S}_a \subset \mathcal{S}_a \subset \mathcal{T}_a$ and as the isomorphism α_a of $\mathcal{S}_a$-windows induced by γ is determined by the matrix $\sigma(X_a)$ (cf. previous paragraph), this would imply the Lemma.

The case $a = 1$ is clear. The inductive passage from a to $a + 1$ goes as follows. We can assume that X_a has coefficients in $\mathfrak{S}_a$.

Therefore the invertible matrix $\tau_a(X_a) \in \mathrm{GL}_r(\mathcal{S}_{pa})$ defines an $\mathcal{S}_{pa}$-linear isomorphism

$$\mathcal{S}_{pa} \otimes_{\mathfrak{S}} M_1^{(\sigma)} \to \mathcal{S}_{pa} \otimes_{\mathfrak{S}} M_2^{(\sigma)}$$

which respects the Hodge filtration i.e., it is compatible with the $R/p^{\nu(pa)}R$-linear map $\mathrm{Lie}\, G_{1,R/p^{\nu(pa)}R} \to \mathrm{Lie}\, G_{2,R/p^{\nu(pa)}R}$ induced by γ.

Since $\tau_a(X_a)$ has coefficients in $\mathfrak{S}_{pa}$, we obtain a commutative diagram:

$$\begin{tikzcd} \mathfrak{S}_{pa} \otimes_{\mathfrak{S}} M_1^{(\sigma)} \arrow[r] \arrow[d] & \mathrm{Lie}\, G_{1,R/p^{\nu(pa)}R} \arrow[d] \\ \mathfrak{S}_{pa} \otimes_{\mathfrak{S}} M_2^{(\sigma)} \arrow[r] & \mathrm{Lie}\, G_{1,R/p^{\nu(pa)}R}. \end{tikzcd}$$

Since $\nu(pa) \geq a+1$ we obtain a commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_1 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_1^{(\sigma)} \arrow[r] \arrow[d] & \operatorname{Lie} G_{1,R/p^{(a+1)}R} \arrow[d] \\ 0 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_2 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_2^{(\sigma)} \arrow[r] & \operatorname{Lie} G_{1,R/p^{(a+1)}R}. \end{tikzcd} \tag{19}$$

The left vertical arrow is induced by $\sigma(X_{a+1})$. On the kernels of the horizontal maps we obtain an $\mathfrak{S}_{a+1}$-linear map

$$\mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_1 \to \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} M_2. \tag{20}$$

Since E is not a zero divisor in $\mathcal{T}_{a+1}$, the tensorizations of the exact sequences of (19) with $\mathcal{T}_{a+1}$ are as well exact sequences. This shows that the tensorization of the $\mathfrak{S}_{a+1}$-linear map (20) with $\mathcal{T}_{a+1}$ is given by the matrix X_{a+1}. Thus X_{a+1} has coefficients in $\mathfrak{S}_{a+1}$. This completes the induction. □

4 Proof of Theorem 1

From (9), by taking the limit $a \to \infty$ we deduce the existence of a functor

$$\mathfrak{S} - \text{windows} \longrightarrow p - \text{divisible groups}/R. \tag{21}$$

This functor is essentially surjective on objects (cf. Lemma 2) and obviously it is faithful. To show that this functor is fully faithful, it is enough to show that it is surjective on isomorphisms. But this is implied by Lemma 3. This ends the proof of Theorem 1.

Acknowledgments

The first author would like to thank Max-Planck Institute, Bonn for good conditions with which to write this note. The second author would like to thank Eike Lau for helpful discussions.

References

[Br] Breuil, Ch.: *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), no. 2, pp. 489–549.

[F] Faltings, G.: *Integral crystalline cohomology over very ramified valuation rings,* J. Amer. Math. Soc. **12** (1999), no. 1, pp. 117–144.

[K] Kisin, M.: *Crystalline representations and F-crystals,* Algebraic geometry and number theory, pp. 459–496, Progr. Math., Vol. **253**, Birkhäuser Boston, Boston, MA, 2006.

[L] Lau, E: in preparation.

[M] Messing, W.: *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes,* Lecture Notes in Mathematics, Vol. **264**, Springer-Verlag, Berlin-New York, 1972.

[Z1] Zink, Th.: *The display of a formal p-divisible group,* Cohomologies p-adiques et applications arithmétiques. I, J. Astérisque, No. **278** (2002), pp. 127–248.

[Z2] Zink, Th.: *A Dieudonn theory for p-divisible groups,* Class field theory—its centenary and prospect (Tokyo, 1998), pp. 139–160, Adv. Stud. Pure Math., Vol. **30**, Math. Soc. Japan, Tokyo, 2001.

[Z3] Zink, Th.: *Windows for displays of p-divisible groups.* Moduli of abelian varieties (Texel Island, 1999), pp. 491–518, Progr. Math., Vol. **195**, Birkhäuser, Basel, 2001.

Adrian Vasiu, Email: adrian@math.binghamton.edu
Address: Department of Mathematical Sciences, Binghamton University, Binghamton, New York 13902-6000, U.S.A.

Thomas Zink, Email: zink@math.uni-bielefeld.de
Address: Fakultät für Mathematik, Universität Bielefeld, P.O. Box 100 131, D-33 501 Bielefeld, Germany.