Advanced Studies in Pure Mathematics 58, 2010
Algebraic and Arithmetic Structures of Moduli Spaces (Sapporo 2007)
pp. 461–479

Breuil's classification of p-divisible groups over regular local rings of arbitrary dimension

Adrian Vasiu and Thomas Zink

Abstract.

Let k be a perfect field of characteristic $p \geq 3$. We classify p-divisible groups over regular local rings of the form

$$W(k)[[t_1, \ldots, t_r, u]]/(u^e + pb_{e-1}u^{e-1} + \ldots + pb_1 u + pb_0),$$

where $b_0, \ldots, b_{e-1} \in W(k)[[t_1, \ldots, t_r]]$ and b_0 is an invertible element. This classification was in the case $r = 0$ conjectured by Breuil and proved by Kisin.

§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. 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

$$E(u) = u^e + a_{e-1}u^{e-1} + \cdots + a_1 u + a_0$$

Received July 16, 2008.
Revised December 17, 2008.
2000 *Mathematics Subject Classification.* 11G10, 11G18, 14F30, 14G35, 14K10, 14L05.

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 $W(k)[[t_1, \ldots, t_r]]$.

We define

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

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

The following notion was introduced in [B] for the case $r = 0$.

Definition 1. *A Breuil window relative to $\mathfrak{S} \to R$ is a pair (Q, ϕ), where Q is a free $\mathfrak{S}$-module of finite rank and where $\phi : Q \to Q^{(\sigma)}$ is a $\mathfrak{S}$-linear map whose cokernel is annihilated by E.*

As $\phi[\frac{1}{E}] : Q[\frac{1}{E}] \to Q^{(\sigma)}[\frac{1}{E}]$ is a $\mathfrak{S}[\frac{1}{E}]$-linear epimorphism between free $\mathfrak{S}[\frac{1}{E}]$-modules of the same finite rank, it is an injection. This implies that ϕ itself is an injection. We check that $C := \mathrm{Coker}(\phi)$ is a free R-module. For this, we can assume that $C \neq 0$ and thus that the $\mathfrak{S}$-module C has projective dimension 1. Since $\mathfrak{S}$ is a regular ring, we have $\operatorname{depth} C = \dim \mathfrak{S} - 1 = \dim R$. As C has the same depth viewed as an R-module or as a $\mathfrak{S}$-module, we conclude that C is a free R-module.

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

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

This theorem was proved by Kisin [K] in the case $r = 0$. We prove the generalization by a new method which is based on the theory of Dieudonné displays [Z2]. This theory works only for a perfect field k of characteristic $p \geq 3$.

Our method yields results for more general fields if we restrict ourself to formal p-divisible groups over R, i.e. p-divisible groups over R whose special fibers over k are connected. Then we can substitute Dieudonné displays by nilpotent displays. To state the result we have to define nilpotent Breuil windows relative to $\mathfrak{S} \to R$. Let (Q, ϕ) be a Breuil window relative to $\mathfrak{S} \to R$. Then we define a σ-linear map $F : Q^{(\sigma)} \to Q^{(\sigma)}$ by $F(x) = \mathrm{id} \otimes \phi^{-1}(Ex)$ for $x \in Q^{(\sigma)}$. If we tensor $(Q^{(\sigma)}, F)$ by the $W(k)$-epimorphism $\mathfrak{S} \to W(k)$ which maps the variables t_i and u to 0, we obtain a Dieudonné module over $W(k)$. In the theorem above this is the covariant Dieudonné module of the special fibre of the p-divisible group over R which corresponds to (Q, σ). We say that (Q, ϕ) is a nilpotent Breuil window relative to $\mathfrak{S} \to R$ if $(Q^{(\sigma)}, F) \otimes_{\mathfrak{S}} W(k)$ is the covariant Dieudonné module of a connected p-divisible group over k. Then the arguments of this paper show that for $p = 2$ the category of nilpotent Breuil windows is equivalent to the category of formal p-divisible groups over R. Exactly the same statement holds for non perfect fields of arbitrary characteristics $p > 0$ if we replace the ring $W(k)$ by a Cohen ring C_k and $\mathfrak{S}$ by $C_k[[t_1, \ldots t_r, u]]$.

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 (see [VZ] for applications with $r = 1$).

As in the case $r = 0$ (see [K]), Theorem 1 implies a classification of finite flat, commutative group schemes of p power order over R.

Definition 2. *A Breuil module relative to $\mathfrak{S} \to R$ is a pair (M, φ), where M is a $\mathfrak{S}$-module of projective dimension at most one and annihilated by a power of p and where $\varphi : M \to M^{(\sigma)}$ is a $\mathfrak{S}$-linear map whose cokernel is annihilated by E.*

Theorem 2. *The category of finite flat, commutative group schemes of p power order over R is equivalent to the category of Breuil modules relative to $\mathfrak{S} \to R$.*

The first author would like to thank MPI Bonn, Binghamton University, and Bielefeld University for good conditions to work on the paper. The second author would like to thank Eike Lau for helpful discussions. Both authors thank the referee for some valuable remarks.

§2. Breuil windows modulo powers of u

We need a slight variant of Breuil windows, which was also considered by Kisin in his proof of Theorem 1 for $r = 0$.

For $a \in \mathbb{N}$ we define $\mathfrak{S}_a := \mathfrak{S}/(u^{ae})$; it is a p-adic ring without p-torsion. Clearly E 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

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

where $\epsilon := (a_{e-1}/p)u^{e-1} + \ldots + (a_1/p)u + (a_0/p)$ is a unit in $\mathfrak{S}$. As u^{ae} and $p^a(-\epsilon)^a$ are congruent modulo the ideal (E), we have identities

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

Definition 3. *A Breuil window relative to $\mathfrak{S}_a \to R/p^aR$ is a pair (Q, ϕ), where Q is a free $\mathfrak{S}_a$-module of finite rank and where $\phi : Q \to$*

$Q^{(\sigma)}$ is a $\mathfrak{S}$-linear map whose cokernel is annihilated by E and is a free R/p^aR-module.

We will call this shortly a $\mathfrak{S}_a$-window, even though this is not a window in the sense of [Z3]. To avoid cases, we define $\mathfrak{S}_\infty := \mathfrak{S}$ and $R/p^\infty R := R$ and we will allow a to be ∞. Thus from now on $a \in \mathbb{N} \cup \{\infty\}$. We note down that a $\mathfrak{S}_\infty$-window will be a Breuil window relative to $\mathfrak{S} \to R$. Next we relate $\mathfrak{S}_a$-windows to the windows introduced in [Z3].

We will use the following convention from [Z1]. Let $\alpha : M \to N$ a σ-linear map of $\mathfrak{S}_a$-modules. Then we denote by

$$\alpha^\sharp : M^{(\sigma)} = \mathfrak{S}_a \otimes_{\sigma, \mathfrak{S}_a} M \to N$$

its linearisation. We say that α is a σ-linear epimorphism (etc.) if $\alpha^\sharp$ is an epimorphism.

We consider triples of the form (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 properties hold:

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

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

As $\sigma(E)$ is not a zero divisor in $\mathfrak{S}_a$, we can define $F_1 := (1/\sigma(E))F : Q \to P$.

Any triple (P, Q, F) has a *normal decomposition.* This means that there exist $\mathfrak{S}_a$-submodules J and L of P such that we have:

$$P = J \oplus L \quad \text{and} \quad Q = E \cdot J \oplus L. \tag{3}$$

This decomposition shows that Q is a free $\mathfrak{S}_a$-module. The map

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

is a σ-linear isomorphism. A normal decomposition of (P, Q, F) is not unique.

If $\tilde{P}$ is a free $\mathfrak{S}_a$-module of finite rank and if $\tilde{P} = \tilde{L} \oplus \tilde{J}$ is a direct sum decomposition, then each arbitrary σ-linear isomorphism $\tilde{J} \oplus \tilde{L} \to \tilde{P}$ defines naturally a triple $(\tilde{P}, \tilde{Q}, \tilde{F})$ as above. We can often identify the triple $(\tilde{P}, \tilde{Q}, \tilde{F})$ with an invertible matrix with coefficients in $\mathfrak{S}_a$ which is a matrix representation of the σ-linear isomorphism $\tilde{J} \oplus \tilde{L} \to \tilde{P}$. Each triple (P, Q, F) is isomorphic to a triple constructed as $(\tilde{P}, \tilde{Q}, \tilde{F})$.

Lemma 1. *The category of triples (P, Q, F) as above is equivalent to the category of $\mathfrak{S}_a$-windows.*

Proof. Assume we are given a triple (P, Q, F). By definition F_1 induces a $\mathfrak{S}_a$-linear epimorphism

$$F_1^\sharp : Q^{(\sigma)} = \mathfrak{S}_a \otimes_{\sigma, \mathfrak{S}_a} Q \twoheadrightarrow P. \tag{5}$$

Due to the existence of normal decomposition of (P, Q, F), Q is a free $\mathfrak{S}_a$-module of the same rank as P. Therefore $F_1^\sharp$ is in fact an isomorphism. To the triple (P, Q, F) we associate the $\mathfrak{S}_a$-window (Q, ϕ), where

$$\phi : Q \to Q^{(\sigma)}$$

is the composite of the inclusion $Q \subset P$ with $(F_1^\sharp)^{-1}$.

Conversely assume that we are given a $\mathfrak{S}_a$-window (Q, ϕ). We set $P := Q^{(\sigma)}$ and we consider Q as a submodule of P via ϕ. We denote by $F_1 : Q \to P$ the σ-linear map which induces the identity $Q^{(\sigma)} = P$. Finally we set $F(x) := F_1(Ex)$ for $x \in P$. Then (P, Q, F) is a triple as above. Q.E.D.

Henceforth we will not distinguish between triples and $\mathfrak{S}_a$-windows i.e., we will identify $(Q, \phi) \equiv (P, Q, F)$. We can describe a normal decomposition directly in terms of (Q, ϕ). Indeed, we can identify Q with $J \oplus L$ via $(1/E)\,\mathrm{id}_J \oplus \mathrm{id}_L$. Then a normal decomposition of (Q, ϕ) is a direct sum decomposition $Q = J \oplus L$ which induces a normal decomposition $P = Q^{(\sigma)} = (1/E)\phi(J) \oplus \phi(L)$. If $a \in \mathbb{N}$, then each $\mathfrak{S}_a$-window lifts to a $\mathfrak{S}_{a+1}$-window (this is so as each invertible matrix with coefficients in $\mathfrak{S}_a$ lifts to an invertible matrix with coefficients in $\mathfrak{S}_{a+1}$).

§3. The p-divisible group of a Breuil window

We relate $\mathfrak{S}_a$-windows to Dieudonné displays over R/p^aR as defined in [Z2], Definition 1. 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. From [Z2], Lemma 2 we get that there exists a unique subring $\hat{W}(S) \subset W(S)$, which is invariant under the Frobenius F and Verschiebung V endomorphisms of $W(S)$ 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 $\hat{W}(S)$.

For $a \in \mathbb{N} \cup \{\infty\}$ there exists a unique homomorphism

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

such that for all $x \in \mathfrak{S}_a$ and for all $n \in \mathbb{N}$ we have $\mathbf{w}_n(\delta_a(x)) = \sigma^n(x)$ (here $\mathbf{w}_n$ is the n-th Witt polynomial). It maps $t_i \mapsto [t_i] = (t_i, 0, 0, \ldots)$ and $u \mapsto [u] = (u, 0, 0, \ldots)$. If we compose δ_a with the canonical $W(k)$-homomorphism $\hat{W}(\mathfrak{S}_a) \to \hat{W}(R/p^a R)$ we obtain a $W(k)$-homomorphism

$$(7) \qquad \varkappa_a : \quad \mathfrak{S}_a \quad \to \quad \hat{W}(R/p^a R).$$

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

Lemma 2. *The element $\varkappa_\infty(\sigma(E)) \in \hat{W}(R)$ is divisible by p and the fraction $\tau := \varkappa_\infty(\sigma(E))/p$ is a unit in $\hat{W}(R)$.*

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

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

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

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

With the notation of (2) we have $\sigma(E) = u^{ep} + p\sigma(\epsilon)$. Since $u^{ep} \equiv (p\epsilon)^p$ *mod* (E) we see that $\sigma(E)/p$ is a unit in R. We note that this proof works for all primes p (i.e., even if $p = 2$). Q.E.D.

For $a \in \mathbb{N} \cup \{\infty\}$ we will define a functor:

$$(8) \qquad \mathfrak{S}_a\text{-windows} \longrightarrow \text{Dieudonné displays over } R/p^a R.$$

Let $(Q, \phi) \equiv (P, Q, F)$ be a $\mathfrak{S}_a$-window. Let $F_1 : Q \to P$ be as in Section 2. To (P, Q, F) we will associate a Dieudonné display (P', Q', F', F_1') over $R/p^a R$. Let $P' := \hat{W}(R/p^a R) \otimes_{\kappa_a, \mathfrak{S}_a} P$. Let Q' be the kernel of the natural $\hat{W}(R/p^a R)$-linear epimorphism:

$$P' = \hat{W}(R/p^a R) \otimes_{\kappa_a, \mathfrak{S}_a} P \twoheadrightarrow P/Q.$$

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

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

Using a normal decomposition of (P, Q, F), one checks that (P', Q', F', F_1') is a Dieudonné display over $R/p^a R$.

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

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

In particular, for the p-divisible group G associated to $(Q,\phi) \equiv (P,Q,F)$ we have identifications of R/p^aR-modules

$$\mathrm{Lie}(G) = P'/Q' = P/Q = \mathrm{Coker}(\phi). \tag{10}$$

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 Dieudonné $\mathfrak{S}_1$-window over R/pR introduced in [Z3], Definition 2. By Theorem 6 (or 3.2) of loc. cit. we get that the functor (9) is an equivalence of categories in the case $a=1$. We would like to mention that the contravariant analogue of this equivalence for $a=1$ also follows from [dJ], Theorem of Introduction and Proposition 7.1.

The faithfulness of the functors (8) and (9) follows from the mentioned equivalence in the case $a=1$ and from the following rigidity property:

Lemma 3. *Let $a \geq 1$ be a natural number. Let $\mathcal{P} = (P,Q,F)$ and $\mathcal{P}' = (P',Q',F')$ be $\mathfrak{S}_{ap}$-windows. By base change we obtain windows $\bar{\mathcal{P}}$ and $\bar{\mathcal{P}}'$ over $\mathfrak{S}_a$. Then the natural map*

$$Hom_{\mathfrak{S}_{ap}}(\mathcal{P},\mathcal{P}') \to Hom_{\mathfrak{S}_a}(\bar{\mathcal{P}},\bar{\mathcal{P}}')$$

is injective.

Proof. Let $\alpha : \mathcal{P} \to \mathcal{P}'$ be a morphism, which induces 0 over $\mathfrak{S}_a$. We have $\alpha(P) \subset u^{ae}P'$. To prove that $\alpha = 0$ it is enough to show that $\alpha(F_1 y) = 0$ for each $y \in Q$. We have $\alpha(y) \in u^{ae}P' \cap Q'$. We choose a normal decomposition $P' = J' \oplus L'$ and we write $\alpha(y) = j' + l'$. Then we have $j' \in u^{ae}J' \cap EJ' = u^{ae}EJ'$ and $l' \in u^{ae}L'$. In $\mathfrak{S}_{ap}$ we have $\sigma(u^{ae}) = u^{ape} = 0$. We conclude that $F_1'j' = 0$ and $F_1'l' = 0$. Finally we obtain $\alpha(F_1 y) = F_1'(\alpha y) = 0$. Q.E.D.

Lemma 4. *The functors (8) and (9) are essentially surjective on objects.*

Proof. We will first prove the lemma for $a \in \mathbb{N}$. We will use induction on $a \in \mathbb{N}$. We already know that this is true for $a = 1$. The inductive passage from a to $a+1$ goes as follows. It suffices to consider the case of the functor (8).

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 $\mathcal{P}' = (P', Q', F', F_1')$ 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 $\tilde{\mathcal{P}} = (\tilde{Q}, \tilde{\phi}) \equiv (\tilde{P}, \tilde{Q}, \tilde{F})$, cf. end of Subsection 2. Let $\tilde{F}_1 : \tilde{Q} \to \tilde{P}$ be obtained from $\tilde{F}$ as in Subsection 2.

We apply to $\tilde{\mathcal{P}}$ the functor (8) and we obtain a Dieudonné display $\tilde{\mathcal{P}}'' = (\tilde{P}'', \tilde{Q}'', \tilde{F}'', \tilde{F}_1'')$ over $R/p^{a+1}R$. By [Z2], Theorem 3 we can identify

$$(\tilde{P}', \tilde{F}', \Phi_1) = (\hat{W}(R/p^{a+1}R) \otimes_{\kappa_{a+1}, \mathfrak{S}_{a+1}} \tilde{P} = \tilde{P}'', \tilde{F}'', \Phi_1). \tag{11}$$

Here $\Phi_1 : \breve{Q}' \to \tilde{P}'$ is a Frobenius linear map from the inverse image $\breve{Q}'$ of Q' in $\tilde{P}' = \tilde{P}''$ which extends both $\tilde{F}_1'$ and $\tilde{F}_1''$ and which satisfies the identity $\Phi_1([p^a]\tilde{P}') = 0$ (this identity is due to the fact that we use the trivial divided power structure on the kernel of the epimorphism $R/p^{a+1}R \twoheadrightarrow R/p^aR$).

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 natural map $\tilde{P} \to \tilde{P}'/\tilde{Q}'$ deduced from the identity $\tilde{P}' = \hat{W}(R/p^{a+1}R) \otimes_{\kappa_{a+1}, \mathfrak{S}_{a+1}} \tilde{P}$. 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 exists 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 $\tilde{F}(y^*) = \tilde{F}(y) \in \sigma(E) \cdot \tilde{P}$. This proves that $\tilde{\mathcal{P}}^* = (\tilde{P}, \tilde{Q}^*, \tilde{F})$ is a $\mathfrak{S}_{a+1}$-window which lifts the $\mathfrak{S}_a$-window $\mathcal{P}$. Let $\tilde{F}_1^* : \tilde{Q}^* \to \tilde{P}$ be obtained from $\tilde{F}$ as in Subsection 2.

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

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

coincides with the composite map

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

This follows again from the decomposition $y^* = y + u^{ae}x$ and the facts that: (i) we have $\tilde{F}_1^*(y^*) = \tilde{F}_1(y)$ (as we have $\tilde{F}(y^*) = \tilde{F}(y)$) and (ii) the image of $u^{ae}x$ in $\check{Q}'$ 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.

The fact that the lemma holds even if $a = \infty$ follows from the above induction via a natural limit process. Q.E.D.

§4. Extending morphisms between $\mathfrak{S}_1$-windows

In this section we prove an extension result for an isomorphism between $\mathfrak{S}_1$-windows. We begin by considering for $a \in \mathbb{N} \cup \{\infty\}$ an extra $W(k)$-algebra:

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

with the convention that $v^\infty := 0$. This ring is without p-torsion. It is elementary to check that the canonical ring homomorphism

$$\mathfrak{S}_a \to \mathcal{T}_a$$

is injective. For $a = 1$ this is an isomorphism $\mathfrak{S}_1 \cong \mathcal{T}_1$.

We set $\mathcal{T} = \mathcal{T}_\infty$. In $\mathcal{T}_a$ we have $E = p(v + \epsilon)$ and thus the elements p and E differ by a unit. We have an isomorphism:

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

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

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

We note that the endomorphism σ on $\mathcal{T}_a$ no longer induces the Frobenius modulo p. But the notion of a window over $\mathcal{T}_a$ still makes sense as follows.

Definition 4. *A window over $\mathcal{T}_a$ is a triple (P, Q, F), 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, and $F : P \to P$ is a σ-linear endomorphism. We require that $F(Q) \subset pP$ and that this subset generates pP as a $\mathcal{T}_a$-module.*

We define a σ-linear map $F_1 : Q \to P$ by $pF_1(y) = F(y)$ for $y \in Q$. Its linearisation $F_1^\sharp$ is an isomorphism. Taking the composite of the inclusion $Q \subset P$ with $(F_1^\sharp)^{-1}$ we obtain a $\mathcal{T}_a$-linear map

$$\phi : Q \to Q^{(\sigma)},$$

whose cokernel is a free $\mathcal{T}_a/p\mathcal{T}_a$-module.

If we start with a triple (P, Q, F) in sense of Lemma 1 an tensor it with $\mathcal{T}_a \otimes_{\mathfrak{S}_a}$ we obtain a window over $\mathcal{T}_a$.

A $\mathcal{T}_a$-window is not a window in sense of [Z3] because σ on $\mathcal{T}_a/p\mathcal{T}_a$ is not the Frobenius endomorphism. We have still the following lifting property.

Proposition 1. *Let (Q_1, ϕ_1) and (Q_2, ϕ_2) be two Breuil windows relative to $\mathfrak{S} \to R$. Let $(\breve{Q}_1, \breve{\phi}_1)$ and $(\breve{Q}_2, \breve{\phi}_2)$ be the $\mathfrak{S}_1$-windows which are the reduction modulo u^e of (Q_1, ϕ_1) and (Q_2, ϕ_2) (respectively). Let $\breve{\alpha} : \breve{Q}_1 \to \breve{Q}_2$ be an isomorphism of windows relative to $\mathfrak{S}_1 \to R/pR$ i.e., a $\mathfrak{S}_1$-linear isomorphism such that we have $\breve{\phi}_2 \circ \breve{\alpha} = (1 \otimes \breve{\alpha}) \circ \breve{\phi}_1$.*

Then there exists a unique isomorphism

$$\alpha : \mathcal{T} \otimes_{\mathfrak{S}} Q_1 \to \mathcal{T} \otimes_{\mathfrak{S}} Q_2$$

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

$$Q_1 = J_1 \oplus L_1 \qquad \text{and} \qquad Q_2 = J_2 \oplus L_2.$$

We find an isomorphism $\gamma : Q_1 \to Q_2$ which lifts $\breve{\alpha}$ and such that $\gamma(L_1) = L_2$ and $\gamma(J_1) = J_2$. We identify the modules Q_1 and Q_2 via γ and we write:

$$Q = Q_1 = Q_2, \quad J = J_1 = J_2, \quad L = L_1 = L_2.$$

We choose a $\mathfrak{S}$-basis $\{e_1, \ldots, e_d\}$ for J and a $\mathfrak{S}$-basis $\{e_{d+1}, \ldots e_r\}$ for L. Then $\{1 \otimes e_1, \ldots, 1 \otimes e_r\}$ is a $\mathfrak{S}$-basis for $Q^{(\sigma)}$. For $i \in \{1, 2\}$ we write $\phi_i : Q \to Q^{(\sigma)}$ as a matrix with respect to the mentioned $\mathfrak{S}$-bases. It follows from the properties of a normal decomposition that this matrix has the form:

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

where A_1 and A_2 are invertible matrices in $\boldsymbol{GL}_r(\mathfrak{S})$ 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 $X \in \boldsymbol{GL}_r(\mathcal{T})$ which solves the equation

$$A_2CX = \sigma(X)A_1C \tag{13}$$

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 of $\mathcal{T}$, the matrix pC^{-1} has coefficients in $\mathcal{T}$. From the equations (13) and (14) we obtain the equation:

$$p(I_r + vY) = pC^{-1}A_2^{-1}(I_r + \sigma(v)\sigma(Y))A_1C.$$

We insert (12) in this equation. With the notation $D := pC^{-1}ZC$ we find:

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

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

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

We have $(u^{e(p-1)}/p) = vu^{e(p-2)}$. Thus the σ-linear operator

$$\Psi(Y) = (u^{e(p-1)}/p)pC^{-1}A_2^{-1}\sigma(Y)A_1C$$

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 $X = I_r + vY \in \boldsymbol{GL}_r(\mathcal{T})$ exists and is uniquely determined. Q.E.D.

§5. Proof of Theorem 1

In this section we prove Theorem 1. In Section 3 we constructed a functor (cf. (9) with $a = \infty$)

(16) Breuil windows relative to $\mathfrak{S} \to R \longrightarrow$ p-divisible groups over R

which is faithful and which (cf. Lemma 4) is essentially surjective on objects. Thus to end the proof of Theorem 1, it suffices to show that this functor is essentially surjective on isomorphisms (equivalently, on morphisms). This will be proved in Lemma 5 below. For the proof of Lemma 5, until the end we take $a \in \mathbb{N}$ and we will begin by first listing some basic properties of the rings $\mathfrak{S}_a$ and $\mathfrak{T}_a$.

5.1. On $\mathfrak{S}_a$ and $\mathfrak{T}_a$

There exists a canonical homomorphism

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

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 exists 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 $\nu(a) := \inf\{\mathrm{ord}_p(\frac{p^n}{n!})| \text{ for } n \geq a\}$. With the notation of (2), the horizontal homomorphism maps $u^{ne}/n!$ to $(p^n/n!)(-\epsilon)^n$. By [Z3], Theorem 6 or 3.2, the epimorphism $\mathcal{S}_a \to R/p^{\nu(a)}R$ is a frame which classifies p-divisible groups over $R/p^{\nu(a)}R$. In what follows, by a $\mathcal{S}_a$-window we mean a Dieudonné $\mathcal{S}_a$-window over $R/p^{\nu(a)}R$ in the sense of [Z3], Definition 2.

Both $\mathcal{S}_a$ and $\mathcal{T}_a$ are subrings of $\mathfrak{S}_a \otimes \mathbb{Q}$. Because of 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 an inclusion of $W(k)$-algebras:

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

The Frobenius endomorphism σ of $\mathfrak{S}$ induces a homomorphism

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

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 homomorphism by

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

Lemma 5. *Let (Q_1, ϕ_1) and (Q_2, ϕ_2) be two Breuil windows relative to $\mathfrak{S} \to R$. Let G_1 and G_2 be the corresponding p-divisible groups over R, cf. the functor (16). Let $\gamma : G_1 \to G_2$ be an isomorphism. Then there exists a unique homomorphism (automatically isomorphism) $\alpha_0 : (Q_1, \phi_1) \to (Q_2, \phi_2)$ of Breuil windows relative to $\mathfrak{S} \to R$ which maps to γ via the functor (16).*

Proof. For $i \in \{1,2\}$ let $(\breve{Q}_i, \breve{\phi}_i) \equiv (\breve{P}_i, \breve{Q}_i, \breve{F}_i)$ be the $\mathfrak{S}_1$-window which is the reduction of $(Q_i, \phi_i) \equiv (P_i, Q_i, F_i)$ modulo u^e. Since the category of $\mathfrak{S}_1$-windows is equivalent to the category of p-divisible groups over R/pR, the reduction of γ modulo p is induced via the functor (9) by an isomorphism $\breve{\alpha} : (\breve{Q}_1, \breve{\phi}_1) \to (\breve{Q}_2, \breve{\phi}_2)$. Due to Proposition 1, the last isomorphism extends to an isomorphism $\alpha : \mathcal{T} \otimes_{\mathfrak{S}} (Q_1, \phi_1) \to \mathcal{T} \otimes_{\mathfrak{S}} (Q_2, \phi_2)$ of windows over $\mathcal{T}$. Here and in what follows we identify $\mathcal{T}_a \otimes_{\mathfrak{S}} (Q_i, \phi_i) \equiv \mathcal{T}_a \otimes_{\mathfrak{S}} (P_i, Q_i, F_i)$ and therefore we will refer to $\mathcal{T}_a \otimes_{\mathfrak{S}} (Q_i, \phi_i)$ as a window over $\mathcal{T}_a$. As in the proof of Proposition 1 we can identify normal decompositions $Q_1 = J_1 \oplus L_1 = J_2 \oplus L_2 = Q_2$ and we can represent the mentioned isomorphism of windows over $\mathcal{T}$ by an invertible matrix $X \in \boldsymbol{GL}_r(\mathcal{T})$. Let $X_a \in \boldsymbol{GL}_r(\mathcal{T}_a)$ be the reduction of X modulo v^a.

The matrix X has the following crystalline interpretation. The epimorphism $\mathcal{T}_a \twoheadrightarrow (R/pR)[[v]]/(v^a)$ is a pd-thickening. (We emphasize that it is not a frame in the sense of [Z3], Definition 1 because σ modulo p is not the Frobenius endomorphism of $\mathcal{T}_a/p\mathcal{T}_a$.) We have a morphism of pd-thickenings

$$\text{(17)} \qquad \begin{array}{ccc} \mathcal{S}_a & \longrightarrow & \mathcal{T}_a \\ \downarrow & & \downarrow \\ R/p^{\nu(a)}R & \longrightarrow & (R/pR)[[v]]/(v^a). \end{array}$$

By the crystal associated to a p-divisible group $\square$ over $R/p^{\nu(a)}R$ we mean the Lie algebra crystal of the universal vector extension crystal of $\square$ as defined in [M]. The crystal of G_i evaluated at the pd-thickening $\mathcal{S}_a \to R/p^{\nu(a)}R$ coincides in a functorial way with $\mathcal{S}_a \otimes_{\mathfrak{S}_a} Q_i^{(\sigma)} = \mathcal{S}_a \otimes_{\mathfrak{S}_a} P_i$ (if G_i is a formal p-divisible group, this follows from either [Z1], Theorem 6 or from [Z3], Theorem 1.6; the general case follows from [L]). Let $\breve{G}_{i,a}$ be the push forward of G_i via the canonical homomorphism $R \to (R/pR)[[v]]/(v^a)$. The diagram (17) shows that $\mathcal{T}_a \otimes_{\mathfrak{S}} Q_i^{(\sigma)} = \mathcal{T}_a \otimes_{\mathfrak{S}} P_i$ is the crystal of $\breve{G}_{i,a}$ 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 α_a of $\mathcal{S}_a$-windows which is defined by a $\mathcal{S}_a$-linear isomorphism $\mathcal{S}_a \otimes_{\mathfrak{S}} P_1 \to \mathcal{S}_a \otimes_{\mathfrak{S}} P_2$. Via base change of α_a through the diagram (17), we get an isomorphism $\beta_a : \mathcal{T}_a \otimes_{\mathfrak{S}} (Q_1, \phi_1) \to \mathcal{T}_a \otimes_{\mathfrak{S}} (Q_2, \phi_2)$ of windows over $\mathcal{T}_a$ defined by an isomorphism $\mathcal{T}_a \otimes_{\mathfrak{S}} (P_1, Q_1, F_1) \to \mathcal{T}_a \otimes_{\mathfrak{S}} (P_2, Q_2, F_2)$. We note that after choosing a normal decomposition a window is simply an invertible matrix (to be compared with end of Section 2) and base change applies to the coefficients of this matrix the homomorphism

$\mathcal{S}_a \to \mathcal{T}_a$. The system of isomorphisms β_a induces in the limit an isomorphism of windows over $\mathcal{T}$:

$$\beta : \mathcal{T} \otimes_{\mathfrak{S}} (Q_1, \phi_1) \to \mathcal{T} \otimes_{\mathfrak{S}} (Q_2, \phi_2). \tag{18}$$

We continue the base change (17) using the following diagram:

$$\begin{array}{ccc} \mathcal{T}_a & \longrightarrow & \mathfrak{S}_1 \\ \downarrow & & \downarrow \\ (R/pR)[[v]]/(v^a) & \longrightarrow & R/pR. \end{array} \tag{19}$$

The vertical arrows are thickenings with divided powers. From α_a we obtain by base change the isomorphism $\breve{\alpha}$ since windows associated to p-divisible groups commute with base change. But this shows that the isomorphism β coincides with the isomorphism $\alpha : \mathcal{T} \otimes_{\mathfrak{S}} (Q_1, \phi_1) \to \mathcal{T} \otimes_{\mathfrak{S}} (Q_2, \phi_2)$, cf. the uniqueness part of Proposition 1.

We will show that the assumption that X has coefficients in $\mathfrak{S}$ implies the Lemma. This assumption implies that α is the tensorization with $\mathcal{T}$ of an isomorphisms $\alpha_0 : (Q_1, \phi_1) \to (Q_2, \phi_2)$. Let $\gamma_0 : G_1 \to G_2$ be the isomorphism associated to the isomorphism α_0 via the functor (16). As the functor (9) is an equivalence of categories for $a = 1$, we get that γ_0 and γ coincide modulo p. Therefore $\gamma = \gamma_0$ and thus the Lemma holds.

Thus to end the proof of the Lemma it suffices to show by induction on $a \in \mathbb{N}$ that the matrix X_a has coefficients in $\mathfrak{S}_a$. 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 $\tau_a(X_a) \in \boldsymbol{GL}_r(\tau(\mathcal{T}_a)) \subset \boldsymbol{GL}_r(\mathcal{S}_{pa})$ defines a $\mathcal{S}_{pa}$-linear isomorphism

$$\mathcal{S}_{pa} \otimes_{\mathfrak{S}} P_1 = \mathcal{S}_{pa} \otimes_{\mathfrak{S}} Q_1^{(\sigma)} \to \mathcal{S}_{pa} \otimes_{\mathfrak{S}} Q_2^{(\sigma)} = \mathcal{S}_{pa} \otimes_{\mathfrak{S}} P_2$$

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

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

$$\begin{array}{ccc} \mathfrak{S}_{pa} \otimes_{\mathfrak{S}} Q_1^{(\sigma)} & \longrightarrow & \operatorname{Lie} G_{1,R/p^{\nu(pa)}R} \\ \downarrow & & \downarrow \\ \mathfrak{S}_{pa} \otimes_{\mathfrak{S}} Q_2^{(\sigma)} & \longrightarrow & \operatorname{Lie} G_{1,R/p^{\nu(pa)}R}. \end{array}$$

Since $\nu(pa) \geq a+1$, from (10) we obtain a commutative diagram
(20)

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_1 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_1^{(\sigma)} \arrow[r] \arrow[d] & \operatorname{Lie} G_{1,R/p^{(a+1)}R} \arrow[d] \\
0 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_2 \arrow[r] & \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_2^{(\sigma)} \arrow[r] & \operatorname{Lie} G_{1,R/p^{(a+1)}R}
\end{tikzcd}$$

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

$$\mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_1 \to \mathfrak{S}_{a+1} \otimes_{\mathfrak{S}} Q_2. \tag{21}$$

As E is not a zero divisor in $\mathcal{T}_{a+1}$, by tensoring the short exact sequences of (20) with $\mathcal{T}_{a+1}$ we get short exact sequences of $\mathcal{T}_{a+1}$-modules. This implies that the tensorization of the $\mathfrak{S}_{a+1}$-linear isomorphism (21) with $\mathcal{T}_{a+1}$ is given by the matrix X_{a+1}. Therefore X_{a+1} has coefficients in $\mathfrak{S}_{a+1}$. This completes the induction and thus the proofs of the Lemma and of Theorem 1. Q.E.D.

§6. Breuil modules

To prove Theorem 2 we first need the following basic result on Breuil modules relative to $\mathfrak{S} \to R$.

Proposition 2. *Let (M, φ) be a Breuil module relative to $\mathfrak{S} \to R$. Then the following four properties hold:*

(i) *The $\mathfrak{S}$-linear map φ is injective.*
(ii) *There exists a short exact sequence $0 \to (Q', \phi') \to (Q, \phi) \to (M, \varphi) \to 0$, where (Q', ϕ') and (Q, ϕ) are Breuil windows relative to $\mathfrak{S} \to R$.*
(iii) *If $(M, \varphi) \to (\tilde{M}, \tilde{\varphi})$ is a morphism of Breuil modules relative to $\mathfrak{S} \to R$, then it is the cokernel of a morphism between two exact complexes $0 \to (Q', \phi') \to (Q, \phi)$ and $0 \to (\tilde{Q}', \tilde{\phi}') \to (\tilde{Q}, \tilde{\phi})$ of Breuil windows relative to $\mathfrak{S} \to R$.*
(iv) *The quotient $M^{(\sigma)}/\varphi(M)$ is an R-module of projective dimension at most one.*

Proof. Let $(p) := p\mathfrak{S}$; it is a principal prime ideal of $\mathfrak{S}$. Then σ induces an endomorphism of the discrete valuation ring $\mathfrak{S}_{(p)}$ which fixes p. Thus the length of a $\mathfrak{S}_{(p)}$-module remains unchanged if tensored by $\sigma_{(p)} : \mathfrak{S}_{(p)} \to \mathfrak{S}_{(p)}$. One easily checks that

$$(M_{(p)})^{(\sigma)} = \mathfrak{S}_{(p)} \otimes_{\sigma_{(p)}, \mathfrak{S}_{(p)}} M_{(p)} \cong (M^{(\sigma)})_{(p)}.$$

Let x, p be a regular sequence in $\mathfrak{S}$. As the $\mathfrak{S}$-module M has projective dimension at most one and as M is annihilated by a power of p, the multiplication by x is a $\mathfrak{S}$-linear monomorphism $x : M \hookrightarrow M$. Since no element of $\mathfrak{S} \setminus p\mathfrak{S}$ is a zero divisor in M, we conclude that $M \subset M_{(p)}$. The $\mathfrak{S}$-linear map $\varphi : M \to M^{(\sigma)}$ becomes an epimorphism when tensored with $\mathfrak{S}_{(p)}$. We obtain an epimorphism of $\mathfrak{S}_{(p)}$-modules of the same length:

$$\varphi_{(p)} : M_{(p)} \to (M_{(p)})^{(\sigma)}.$$

As M is a finitely generated $\mathfrak{S}$-module annihilated by a power of p, the $\mathfrak{S}_{(p)}$-module $M_{(p)}$ has finite length. From the last two sentences we get that $\varphi_{(p)}$ is injective. Thus φ is also injective i.e., (i) holds.

We consider free $\mathfrak{S}$-modules J and L of finite ranks and a $\mathfrak{S}$-linear epimorphism

$$J \oplus L \xrightarrow{\tau} M^{(\sigma)}$$

which maps the free $\mathfrak{S}$-submodule $EJ \oplus L$ surjectively to $\varphi(M)$. Let $\tau_1 : J \oplus L \to M$ be the unique $\mathfrak{S}$-linear map such that we have a commutative diagram

$$\begin{tikzcd}
EJ \oplus L \arrow[r] & \mathrm{Im}(\varphi) \\
J \oplus L \arrow[r] \arrow[u, "E\,\mathrm{id}_J + \mathrm{id}_L"] & M \arrow[u, "\varphi"']
\end{tikzcd}$$

whose vertical maps are isomorphisms. We consider a $\mathfrak{S}$-linear isomorphism $\gamma : J \oplus L \to J^{(\sigma)} \oplus L^{(\sigma)}$ which makes the following diagram commutative

$$\begin{tikzcd}
J \oplus L \arrow[rr, "\tau"] \arrow[dr, "\gamma"'] & & M^{(\sigma)} \\
& J^{(\sigma)} \oplus L^{(\sigma)}. \arrow[ur, "\tau_1^{(\sigma)}"'] &
\end{tikzcd}$$

The existence of γ is implied by the following general property. Let N be a finitely generated module over a local ring A. Let F_1 and F_2 be two free A-modules of the same rank equipped with A-linear epimorphisms $\tau_1 : F_1 \to N$ and $\tau_2 : F_2 \to N$. Then there exists an isomorphism $\gamma_{12} : F_1 \to F_2$ such that we have $\tau_2 \circ \gamma_{12} = \tau_1$.

We set $Q := J \oplus L$ and $\phi := \gamma \circ (E\,\mathrm{id}_J + \mathrm{id}_L) : J \oplus L \to J^{(\sigma)} \oplus L^{(\sigma)}$. Then the pair (Q, ϕ) is a Breuil window relative to $\mathfrak{S} \to R$. We have a commutative diagram

$$\begin{array}{ccc} Q & \xrightarrow{\tau_1} & M \\ {\scriptstyle\phi}\downarrow & & {\scriptstyle\varphi}\downarrow \\ Q^{(\sigma)} & \xrightarrow{\tau_1^{(\sigma)}} & M^{(\sigma)}. \end{array}$$

Hence τ_1 is a surjection from (Q,ϕ) to (M,φ). It is obvious that the kernel of $\tau_1 : (Q,\phi) \to (M,\varphi)$ is again a Breuil module (Q',ϕ') relative to $\mathfrak{S} \to R$. We obtain a short exact sequence:

$$0 \to (Q',\phi') \to (Q,\phi) \to (M,\varphi) \to 0.$$

Thus (ii) holds.

Next we prove (iii). We have seen above that for any Breuil module (M,φ) relative to $\mathfrak{S} \to R$ there is a Breuil window (Q,ϕ) relative to $\mathfrak{S} \to R$ and an epimorphism $(Q,\phi) \to (M,\varphi)$. We remark that our argument uses only the properties that $\varphi : M \to M^{(\sigma)}$ is injective and that its cokernel is annihilated by E.

In the situation (iii) we choose a surjection $(\tilde{Q},\tilde{\phi}) \to (\tilde{M},\tilde{\varphi})$ from a Breuil window $(\tilde{Q},\tilde{\phi})$ relative to $\mathfrak{S} \to R$. We form the fibre product of $\mathfrak{S}$-modules $N = M \times_{\tilde{M}} \tilde{Q}$. The functor which associates to an $\mathfrak{S}$-module L the $\mathfrak{S}$-module $L^{(\sigma)}$ is exact and therefore respects fibre products. We obtain a $\mathfrak{S}$-linear map $\psi : N \to N^{(\sigma)}$ which is compatible with φ and $\tilde{\phi}$. Clearly ψ is injective and its cokernel is annihilated by E. Therefore there is a surjection $(Q,\phi) \to (N,\psi)$ from a Breuil window (Q,ϕ) relative to $\mathfrak{S} \to R$. We deduce the existence of a commutative diagram

$$\begin{array}{ccc} (Q,\phi) & \longrightarrow & (M,\varphi) \\ \downarrow & & \downarrow \\ (Q,\tilde{\phi}) & \longrightarrow & (\tilde{M},\tilde{\varphi}). \end{array}$$

As remarked above the kernels of the horizontal arrows are Breuil modules relative to $\mathfrak{S} \to R$. This implies that (iii) holds.

To prove (iv) we consider the short exact sequence of (ii). As $\mathrm{Coker}(\phi)$ and $\mathrm{Coker}(\phi')$ are free R-modules and as we have a short exact sequence $0 \to \mathrm{Coker}(\phi') \to \mathrm{Coker}(\phi) \to \mathrm{Coker}(\varphi) \to 0$ of R-modules, we get that (iv) holds as well. Q.E.D.

6.1. Proof of Theorem 2

We prove Theorem 2. Let H be a finite flat, commutative group scheme of p power order over R. Due to a theorem of Raynaud (see

[BBM], Theorem 3.1.1), H is the kernel of an isogeny of p-divisible groups over R

$$0 \to H \to G' \to G \to 0.$$

Let (Q', ϕ') and (Q, ϕ) be the Breuil windows relative to $\mathfrak{S} \to R$ which correspond by Theorem 1 to the p-divisible groups G' and G. Let $(Q', \phi') \to (Q, \phi)$ be the morphism that corresponds to the isogeny $G' \to G$. This morphism is an isogeny i.e., it is a monomorphism and its cokernel is annihilated by a power of p (as $G' \to G$ is an isogeny). Then it is immediate that the cokernel (M, φ) of $(Q', \phi') \to (Q, \phi)$ is a Breuil module relative to $\mathfrak{S} \to R$. One can check that (M, ϕ) is independent of the chosen resolution of H and that the association $H \mapsto (M, \varphi)$ is a functor.

Conversely let (M, ϕ) be a Breuil module relative to $\mathfrak{S} \to R$. By Proposition 2 (ii) we have a short exact sequence $0 \to (Q', \phi') \to (Q, \phi) \to (M, \varphi) \to 0$, where (Q', ϕ') and (Q, ϕ) are Breuil windows relative to $\mathfrak{S} \to R$. By Theorem 1, the monomorphism $(Q', \phi') \to (Q, \phi)$ gives rise to an isogeny of p-divisible groups $G' \to G$. Based on this and Proposition 2 (iii) we obtain a functor which associates to (M, ϕ) the kernel of the isogeny $G' \to G$. This is a quasi-inverse to the functor of the previous paragraph. Thus Theorem 2 holds. Q.E.D.

References

[BBM] P. Berthelot, L. Breen and W. Messing, Théorie de Dieudonné Cristalline II, Lecture Notes in Math., **930**, Springer-Verlag, Berlin-New York, 1982.

[B] Ch. Breuil, Schémas en groupes et corps de normes, unpublished manuscript, 1998, 13 p.

[dJ] J. de Jong, Finite locally free group schemes in characteristic p and Dieudonné modules, Invent. Math., **114** (1993), 89–137.

[F] G. Faltings, Integral crystalline cohomology over very ramified valuation rings, J. Amer. Math. Soc., **12** (1999), 117–144.

[K] M. Kisin, Crystalline representations and F-crystals, In: Algebraic Geometry and Number Theory, Progr. Math., **253**, Birkhäuser Boston, Boston, MA, 2006, pp. 459–496.

[L] E. Lau, A comparison of crystals for Dieudonné displays, personal communication.

[M] W. Messing, The Crystals Associated to Barsotti–Tate Groups: with Applications to Abelian Schemes, Lecture Notes in Math., **264**, Springer-Verlag, Berlin-New York, 1972.

[VZ] A. Vasiu and Th. Zink, Purity results for finite flat group schemes over ramified bases, manuscript, July 2008.

[Z1] Th. Zink, The display of a formal p-divisible group, In: Cohomologies p-adiques et Applications Arithmétiques. I, Astérisque, **278**, Soc. Math. France, 2002, pp. 127–248.

[Z2] Th. Zink, A Dieudonné theory for p-divisible groups, In: Class Field Theory—Its Centenary and Prospect, Tokyo, 1998, Adv. Stud. Pure Math., **30**, Math. Soc. Japan, Tokyo, 2001, pp. 139–160.

[Z3] Th. Zink, Windows for displays of p-divisible groups, In: Moduli of Abelian Varieties, Texel Island, 1999, Progr. Math., **195**, Birkhäuser, Basel, 2001, pp. 491–518.

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

Thomas Zink
Fakultät für Mathematik, Universität Bielefeld
100 131, D-33 501 Bielefeld, Germany
E-mail address : zink@math.uni-bielefeld.de