Invent. math. 134, 301–333 (1998)

Inventiones mathematicae

Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic

A.J. de Jong

School of Mathematics, Princeton University, Princeton, NJ 08540, USA

Oblatum 5-XII-95 & 14-XI-1997

1 Introduction

Let G, H be p-divisible groups over a discrete valuation ring R. Set K equal to the fraction field of R. There is a natural map

$$\mathrm{Hom}_R(G,H) \longrightarrow \mathrm{Hom}_K(G_K,H_K) \ . \tag{1}$$

In [13, Theorem 4] Tate proved that (1) is a bijection when the characteristic of K is zero.

From now on we assume that the characteristic of K is $p > 0$. Set $S = \mathrm{Spec}\, R$ and $\eta = \mathrm{Spec}\, K$. There is an open immersion $j : \eta \to S$. Hence there is a natural functor

$$F\text{-crystals over } S \xrightarrow{j^*} F\text{-crystals over } \eta \ .$$

Here, an F-crystal is a nondegenerate F-crystal of [12, 3.1.1]. We recall that any characteristic p discrete valuation ring essentially of finite type over a field has a p-basis, see e.g. [10]. A complete discrete valuation ring of characteristic p has a p-basis if its residue field has a finite p-basis.

1.1 Theorem. *Assume R has a p-basis. The functor j^* is fully faithful.*

1.2 Corollary. (*No assumption on R.*) *The map* (1) *is bijective.*

The theorem implies the corollary by [1] or [2, Section 1] (there is an immediate reduction to the case where R is complete with algebraically closed residue field, see [13, page 181]). To establish the bijectivity of (1) in the characteristic p case was mentioned as a problem in the introduction of [6, Exposé IX]. The corollary implies a result on extensions of homomorphisms of p-divisible groups over normal base schemes, [13, page 180] and [2, Section 1]. In [1] it was shown, using a result of [9], that 1.2 holds in case the Newton polygons of G and H are constant. The results of [1] are now well understood, as the main difficulty in [1] was to produce a suitable Dieudonné module theory, which we have due to [3] and [4]. (See [7, 8] for further results.)

The author sees Theorem 1.1 as an indication that (overconvergent) F-crystals over schemes of characteristic p are the p-adic analogue of the lisse ℓ-adic sheaves. The author hopes that the methods of this article may be used to study the bad reduction behavior of overconvergent F-crystals.

In Section 2 we indicate some known applications of 1.2. First, one can deduce a good reduction criterion for abelian varieties in terms of associated p-divisible groups, [6, Exposé IX]. Second, the result that the natural map

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}(X[p^\infty], Y[p^\infty])$$

is an isomorphism for abelian varieties X, Y over a field finitely generated over $\mathbb{F}_p$.

In Section 3 we reduce Theorem 1.1 to Theorem 9.1. The proof of Theorem 9.1 in Sections 4–9 takes up most of this paper. In Section 4 all notations are introduced and fixed till the end of the paper. The idea of the proof of Theorem 9.1 is roughly the following. First one writes any F-module (see 4.4) in a standard form 5.5 over a ring of convergent power series $\Gamma_{2,c}$; this is a ring which is not p-adically complete. The important point is that the slopes decrease in 5.5. Going up to this ring preserves enough information so that one can deduce results about slopes from the existence of $\varphi : M \to \Gamma$, see 5.7. Then one descends back to $\Omega = W[[t]]$ using a linear independence result (Section 8) and Dwork's trick (Section 6). The final step is in Section 7 where a rank 1 submodule of highest slope is split off.

Acknowledgements. The author thanks P. Berthelot, C. Deninger, B. Gross, N. Katz, B. Mazur, W. Messing, and T. Scanlon for discussions on the problem and its applications. He thanks B. Edixhoven for some pertinent remarks concerning Section 2. He especially thanks U. Zannier, who first proved Theorem 9.1 in the case that M has rank 2; the idea to consider the equations over the ring Γ_c of convergent power series is due to U. Zannier.

2 Applications of 1.2

In this section R is a *henselian* discrete valuation ring of characteristic $p > 0$. We have K, S, η as above and $s \in S$ is the closed point. We will use Corollary 1.2 a lot, sometimes without explicitly referring to it.

Some remarks on p-divisible groups. If $G \to H$ is a homomorphism of p-divisible groups over a *field*, then the image of $G \to H$ is a p-divisible group. The height of this image might be called the rank of the homomorphism; it is actually the rank of the induced map on Dieudonné modules. The kernel K of $G \to H$ has the following structure: there is a canonical exact sequence $0 \to K' \to K \to K'' \to 0$, where K' is a p-divisible group and K'' is a finite group scheme. The p-divisible group K' is the image of p^n on K for sufficiently large n. The following lemma says that the rank of a homomorphism of p-divisible groups over S is constant over S.

2.1 Lemma. *With the notations above.*

(i) *If G is a p-divisible group over S and $H \subset G$ is an fppf subsheaf which is a p-divisible group, then G/H is a p-divisible group.*

(ii) *If $G \to H$ is a morphism of p-divisible groups over S, then the height of the image of $G_\eta \to H_\eta$ is equal to the height of the image of $G_s \to H_s$.*

(iii) *Let $\alpha : G \to H$ be a morphism of p-divisible groups over S and suppose that the kernel of the generic fibre α_η of α is a p-divisible group. Then the kernel of α is a p-divisible group and so is the cokernel.*

Proof. The proof of (i) is left to the reader. We defer the proofs of (ii) and (iii) to the appendix. □

2.2 Definition. *Let G_η be a p-divisible group over η.*

(i) *We say that G_η has good reduction over S if it extends to a p-divisible group G over S* (*uniquely by* 1.2).

(ii) *We say that G_η has semi-stable reduction over S if there exists a filtration* $(0) \subset G_\eta^\mu \subset G_\eta^f \subset G_\eta$ *by p-divisible groups such that the following conditions hold*:

a) *Both G_η^f and G_η/G_η^μ extend to p-divisible groups G_1 and G_2 over S. By* 1.2 *there is a unique morphism $G_1 \to G_2$ extending $G_\eta^f \to G_\eta/G_\eta^\mu$. Note that $G_1 \to G_2$ satisfies the conditions of Lemma* 2.1 (iii). *Thus* $G^\mu = \mathrm{Ker}(G_1 \to G_2)$ *and* $G^{\mathrm{et}} = \mathrm{Coker}(G_1 \to G_2)$ *are p-divisible groups over S.*

b) *The sheaf G^μ, resp. G^{et} is a multiplicative, resp.* étale *p-divisible group.*

2.3 Remark. The condition on semi-stable reduction of a p-divisible group G_η over η implies that G_η has "virtuellement bonne reduction d'echelon 2" [6, Exposé IX 5.12]. The author does not know whether the concepts are equivalent in general. If $G_\eta = X_\eta[p^\infty]$ for some abelian variety X_η over η, then the concepts do coincide. We won't use this; the proof is left to the reader as an exercise. (Hint: Use 2.5 and consider a finite Galois extension of K over which X_η becomes semi-stable, compare the two filtrations and use the Galois action to show that the semi-stable filtration comes from a filtration over K.) $\square$

2.4 Lemma. (i) *If G_η has semi-stable reduction over S, then $(0) \subset G^\mu_\eta \subset G^f_\eta \subset G_\eta$ can be chosen such that $G^\mu \otimes \kappa(s)$ is the multiplicative part of G_1 and G^{et} is the étale part of G_2.*

(ii) *Suppose both G_η and H_η are p-divisible groups having semi-stable reduction over S. Let $\varphi_\eta : G_\eta \to H_\eta$ be a morphism. If we choose the filtrations as in* (i) *then φ_η induces morphisms $G_i \to H_i$ fitting into a commutative square with the morphisms $G_1 \to G_2$ and $H_1 \to H_2$.*

The first application of Corollary 1.2 is a criteriom for good reduction of Abelian varieties in terms of their p-divisible groups. Below we sketch the argument; for more precise information the reader should consult [6, Exposé IX].

2.5 Criterion for good reduction. *Let X_η be an abelian variety over η with p-divisible group G_η. Then X_η has good reduction if and only if G_η has good reduction. Same for semi-stable reduction.*

Proof. The direct implication is well known and follows from the description of the semi-stable model of X_η, the description of the semi-stable model of the dual abelian variety X^t_η, and the fact that $X^t_\eta[p^\infty]$ is dual to $X_\eta[p^\infty]$. See [6, Exposé IX]

Suppose G_η has semi-stable reduction. Let $K \subset K'$ be a finite separable Galois extension such that $X_{\eta'}$ has a semi-abelian model X' over S'. Let $G' \subset X'[p^\infty]$ be the union of the finite parts of the quasi-finite group schemes $X'[p^n]$. It is a p-divisible group. If we take the filtration $(0) \subset G^\mu_\eta \subset G^f_\eta \subset G_\eta$ as in Lemma 2.4 (i), then there is a morphism $G_1 \times_S S' \to G'$. Note that this induces an isomorphism on formal groups (look at étale parts). There is an action of $\mathrm{Gal}(K'/K)$ on the scheme X'. The inertia subgroup $I \subset \mathrm{Gal}(K'/K)$ acts trivially on the special fibre of the formal group $\hat{G}'$ over S' as $\hat{G}' \cong \hat{G}_1 \times_S S'$. Hence I acts trivially on $X'_{s'}$, as $\hat{X}' \cong \hat{G}'$. This implies that X_η has semi-stable reduction over S: For example one concludes this by looking at the action of inertia on the ℓ-adic Tate module of X_η for some prime ℓ not equal to p. (See [6, Exposé IX 3.5].)

Next, assume that G_η has good reduction. We already know that X_η has a semi-abelian model X over S. Let $X \to X^{\text{Néron}}$ be the morphism of X to the Néron model of X_η. Let $X[p^n]^f$ be the finite part of $X[p^n]$. The cokernel of the inclusion morphism $X[p^n]^f \to G[p^n]$ is an étale group scheme. Thus $Y_n = \big(X \oplus G[p^n]\big)/X[p^n]^f$ is a smooth group scheme over S (we divide out by the anti-diagonal). As $G[p^n]_\eta = X_\eta[p^n]$, we have a map $Y_{n,\eta} \to X_\eta$ induced by $a \oplus b \mapsto a + b$. This extends to a homomorphism of group schemes $Y_n \to X^{\text{Néron}}$ by the Néron property. This implies that $X^{\text{Néron}}[p^n] \otimes \kappa(s)$ has order $p^{2n \dim X_\eta}$ for all n. It follows that $X^{\text{Néron}}$ is an abelian scheme over S. $\square$

The second application of Corollary 1.2 is a theorem relating endomorphisms of Abelian varieties to endomorphisms of their p-divisible groups. For the ideas in the proof we refer to [5] and the references therein.

2.6 Theorem. *Let F be a field finitely generated over $\mathbb{F}_p$. Let X_F, Y_F be abelian varieties over F. Then*

$$\operatorname{Hom}(X_F, Y_F) \otimes \mathbb{Z}_p \cong \operatorname{Hom}(X_F[p^\infty], Y_F[p^\infty])$$

Proof. It is well known that the map is injective, and identifies the left hand side with a saturated submodule of the right hand side.

There is a standard reduction to the case that the transcendence degree of F over $\mathbb{F}_p$ is 1: The case of a finite field is known [14], hence we may assume the transcendence degree is more than 1. Both X and Y have models X_U and Y_U defined over a variety U with $R(U) = F$. We can find an irreducible divisor $Z \subset U$ such that the specialization mapping $\operatorname{Hom}(X_F, Y_F) \to \operatorname{Hom}(X_{R(Z)}, Y_{R(Z)})$ is an isomorphism. (E.g. by looking at the ℓ-adic representations and using Bertini.) On the other hand, Corollary 1.2 insures there is a specialization mapping $\operatorname{Hom}(X_F[p^\infty], Y_F[p^\infty]) \to \operatorname{Hom}(X_{R(Z)}[p^\infty], Y_{R(Z)}[p^\infty])$. Thus if we prove the theorem for $R(Z)$ then the theorem for F follows. By induction we may assume that the transcendence degree of F over $\mathbb{F}_p$ is 1.

Let C be the smooth projective curve over $\mathbb{F}_p$ defined by F. By Galois descent, it suffices to prove the equality after a finite separable extension of F. Therefore, we may assume that both X_F and Y_F have semi-abelian models X and Y over C.

We first give the argument in case both X and Y are actually abelian schemes over C. Take $\gamma_F \in \operatorname{Hom}(X_F[p^\infty], Y_F[p^\infty])$. By 1.2, we get $\gamma : X[p^\infty] \to Y[p^\infty]$ over C with generic fibre equal to γ_F. Let

$$\Gamma \subset X[p^\infty] \oplus Y[p^\infty]$$

be the graph of γ. Put $Z_n = (X \oplus Y)/\Gamma[p^n]$. This is an abelian scheme over C; we have an exact sequence of truncated Barsotti-Tate group schemes of level 1 over C as follows

$$0 \to \Gamma[p] \to X[p] \oplus Y[p] \to Z_n[p] \to \Gamma[p] \to 0 \ .$$

And hence an exact sequence

$$(*) \qquad 0 \to \omega_\Gamma \to \omega_{Z_n} \to \omega_X \oplus \omega_Y \to \omega_\Gamma \to 0 \ .$$

We conclude that $\det(\omega_{Z_n}) \cong \det(\omega_X \oplus \omega_Y)$ independent of n. It is known [15] that this implies there are only a finite number of isomorphism classes of abelian schemes among the Z_n (this is explained in [5, Section 7]). This implies that $\Gamma = \mathrm{Im}(\gamma' : X[p^\infty] \oplus Y[p^\infty] \to X[p^\infty] \oplus Y[p^\infty])$ for some $\gamma' \in \mathrm{End}(X \oplus Y) \otimes \mathbb{Z}_p$ by known arguments, see the proof of Proposition 1 in [14]. This statement for all γ gives the equality of the theorem.

In the case X and Y are only semi-abelian schemes one has to be a little more careful. We still have $\Gamma_U \subset X[p^\infty]_U \oplus Y[p^\infty]_U$, where $U \subset C$ is the open subscheme over which X and Y are abelian. Let R_v be the complete local ring of C at a place v of F not in U. The abelian schemes $Z_{n,U} = (X_U \oplus Y_U)/\Gamma_U[p^n]$ have semi-abelian models Z_n over C. The p-divisible group Γ_U has semi-stable reduction over R_v. Let $\Gamma_{1,v}$ over R_v be as in Lemma 2.4 (i). Remark that there is a morphism $\Gamma_{1,v} \to X[p^\infty]_{R_v} \oplus Y[p^\infty]_{R_v}$. Then there is a morphism

$$(X_{R_v} \oplus Y_{R_v})/\Gamma_{1,v}[p^n] \longrightarrow Z_{n,R_v}$$

and this morphism is étale, as follows from the definitions. Using this one checks that (*) remains true, taking for ω_Γ the sheaf $\omega_{\widehat{\Gamma}}$, where $\widehat{\Gamma}$ is the formal group over C with $\widehat{\Gamma} = \widehat{\Gamma}_U$ over U and $\widehat{\Gamma} = \widehat{\Gamma}_{1,v}$ over R_v.

3 Preliminary reduction

Let R, K, S and η be as in Theorem 1.1. Let $R \to R'$ be an injective local homomorphism of discrete valuation rings with $e(R'/R) = 1$ and assume that R' is complete and that the residue field k' of R' is algebraically closed. We have assumed R has a p-basis and R' has a p-basis as it is complete with algebraically closed residue field. Hence R (resp. R') has a lift (Ω, σ) (resp. (Ω', σ')), see [4, Section 1] and [8, 1.2]. We can choose a lift $\Omega \to \Omega'$ of the map $R \to R'$ [4]. We do not assume that it is compatible with σ and σ' (although we could choose it that way with some effort). An F-crystal $\mathscr{E}$ over $\operatorname{Spec} R$ corresponds to a triple (M, F, ∇) over Ω, see [4, Proposition 1.3.3]. Then $\mathscr{E}_{S'}$ corresponds to a triple $(M \otimes_\Omega \Omega', F', \nabla')$. Here ∇' is induced from ∇. But since we did not assume $\Omega \to \Omega'$ to be compatible with our σ's the F' is not just deduced from F by linear extension, but also involves ∇ and ∇'. Let us put Γ equal to the p-adic completion of $\Omega[t^{-1}]$, where t maps to an uniformizer of R. Similar for Γ'. Then $\mathscr{E}_\eta$ corresponds to the triple $(M \otimes \Gamma, F \otimes \sigma, \nabla \otimes 1 + 1 \otimes d)$. Similar for $\mathscr{E}_{\eta'}$.

We claim that if $\mathscr{E}_1$, $\mathscr{E}_2$ are F-crystals over S, then

$$\operatorname{Hom}_S(\mathscr{E}_1, \mathscr{E}_2) = \operatorname{Hom}_\eta(\mathscr{E}_{1,\eta}, \mathscr{E}_{2,\eta}) \cap \operatorname{Hom}_{S'}(\mathscr{E}_{1,S'}, \mathscr{E}_{2,S'}) \ .$$

The intersection is taken in $\operatorname{Hom}_{\eta'}(\mathscr{E}_{1,\eta'}, \mathscr{E}_{2,\eta'})$. This follows from the remarks above, by looking at the coefficients of the linear maps over Γ and Ω' in terms of a basis of M_1 and M_2 over Ω and the remark that

$$\Omega = \Omega' \cap \Gamma \ .$$

The intersection takes place in Γ'. Thus it suffices to prove Theorem 1.1 in case $R \cong k[[t]]$ with k algebraically closed.

By [4, 1.3.3] the category of F-crystals over $\operatorname{Spec} k[[t]]$ is equivalent to a full subcategory of the category of (F, θ)-modules (M, F, θ) (see Definitions 4.4 and 4.9) over $\Omega = W[[t]]$ (it is unimportant which full subcategory this is). This is true as $\{t\}$ is a p-basis of the ring $k[[t]]$, hence a connection on an Ω-module M corresponds to a $\frac{d}{dt}$-derivation on the module M. Thus we have to show that any horizontal linear map of (F, θ)-modules M_1 and M_2

$$\varphi : M_1 \otimes_\Omega \Gamma \longrightarrow M_2 \otimes_\Omega \Gamma$$

compatible with F_1 and F_2 maps M_1 into M_2. Of course φ defines a map

$$\varphi' : (M_1 \otimes_\Omega M_2^*) \otimes_\Omega \Gamma \to \Gamma \ .$$

There is a standard way to get a connection θ_2^* on M_2^* and for some $\ell \in \mathbb{Z}_{\geq 0}$ the map $p^\ell (F_2^{-1})^*$ defines the structure of an F-module on M_2^*. Thus $M_1 \otimes M_2^*$ has the structure of (F, θ)-module over Ω. Then φ' is horizontal (using $\frac{d}{dt}$ on Γ) and has the property that $\varphi'(F(m)) = p^\ell \sigma(\varphi'(m))$ for all $m \in M_1 \otimes M_2^*$. We see that Theorem 9.1 implies Theorem 1.1.

4 Notations

In this section we introduce notations and give some definitions that will be fixed in the rest of the article.

p	A prime number.
k	An algebraically closed field of characteristic p.
t	An indeterminate.
$\mathcal{O} = k[[t]]$	The ring of power series over k.
$K = k((t))$	The fraction field of $\mathcal{O}$.
K_1	A perfect closure of K.
$\mathcal{O}_1$	The integral closure of $\mathcal{O} = k[[t]]$ in K_1.
K_2	An algebraic closure of K_1.
$\mathcal{O}_2$	The integral closure of $\mathcal{O}_1$ in K_2.
$v : K_2^* \to \mathbb{Q}$	The valuation on K_2 with $v(t) = 1$. We will also consider v as a valuation on the fields K and K_1. Note that $\mathcal{O}$ (resp. $\mathcal{O}_i$) is the valuation ring of v on K (resp. K_i).
$\{s_n\}_{n\in\mathbb{N}}$	A sequence of elements in K_2 with $s_{nm}^m = s_n$ and $s_1 = t$. We will also write $s_n = t^{1/n}$, $s_n^m = t^{m/n}$, etc. Note that $s_n \in \mathcal{O}_2$. Remark that $\mathcal{O} \subset \mathcal{O}_1 \subset \mathcal{O}_2$ and that $\mathcal{O}_1 = \bigcup_{n\in\mathbb{N}} \mathcal{O}[t^{1/p^n}]$. Also remark that $\mathcal{O}_1$ and $\mathcal{O}_2$ are perfect domains of characteristic p.
$W = W(k)$	The Witt ring of the field k. The reduction map $W \to k$ will be denoted $a \mapsto \bar{a}$. A similar notation will be used for other (Witt) rings as well.
$\sigma : W \to W$	Frobenius. We will use σ to denote Frobenius on all rings of Witt vectors; it will denote a lift of Frobenius on other rings as well.
W_b	This is the ring $W[\pi]/(\pi^b - p)$, where b is a positive integer. We will also write $\pi = p^{1/b}$. The map σ is extended to W_b by setting $\sigma(p^{1/b}) = p^{1/b}$. The reduction modulo π is a map $W_b \to k$ and is denoted $a \mapsto \bar{a}$.
$L_0,\ L_{0,b}$	These denote the fraction field of W and of W_b.
$\Omega = W[[t]]$	The ring of power series in t over W. Again we use $a \mapsto \bar{a}$ to denote the reduction map $\Omega \to \mathcal{O}$.
$\sigma : \Omega \to \Omega$	The unique lift of Frobenius on Ω such that $\sigma(t) = t^p$.
$D = (\mathrm{Spf}\,\Omega)^{\mathrm{rig}}$	This is the rigid analytic space over L_0 associated to the formal scheme $\mathrm{Spf}\,\Omega$, see [8, Section 7]. It is the open unit disc with coordinate $t : D = \{t : \lvert t\rvert < 1\}$ and can be characterized as the

	strong Stein space D over L_0 such that $\Gamma(D, \mathcal{O}^\circ) \cong \Omega$. Associated to $\sigma : \Omega \to \Omega$ there is a general morphism of analytic spaces $\sigma : D \to D$ over $\sigma : L_0 \to L_0$, see [8, 7.2.6]. It can be viewed as a morphism $D \to D \hat{\otimes}_\sigma L_0$.
$\Gamma(D, \mathcal{O})$	The global rigid analytic functions on D. These can be represented as power series $f = \sum_{n \geq 0} a_n t^n$, with $a_n \in L_0$ such that for any $\epsilon > 0$ the function $n \mapsto v_p(a_n) - \epsilon n$ is bounded. The map σ maps f to $\sigma(f) = \sum_{n \geq 0} (a_n) t^{pn}$.
$\Omega_i = W(\mathcal{O}_i)$	The rings of p-Witt vectors for $\mathcal{O}_1$ and $\mathcal{O}_2$. The map $\sigma : \Omega_i \to \Omega_i$ is Frobenius. By functoriality of the Witt vectors there is unique a map $\Omega_1 \to \Omega_2$ compatible with σ and reducing to the inclusion $\mathcal{O}_1 \subset \mathcal{O}_2$ modulo p. This map is an inclusion; we think of Ω_1 as a subring of Ω_2.
$t^{1/n} \in \Omega_2$	Denotes the Teichmüller lift of $s_n \in \mathcal{O}_2$. The elements t^{1/p^n} are in Ω_1. The element $t^{1/1}$ is also written t again.
$\Omega \to \Omega_1$	The unique homomorphism j of rings, with $t \mapsto t$, compatible with σ and reducing to the inclusion $\mathcal{O} \subset \mathcal{O}_1$ modulo p. Such a map exists; a construction can be given as follows. Fix $n \in \mathbb{N}$. Any element $x \in \Omega = W[[t]]$ can be written $$x = \sum_{j=0}^{n-1} p^j \sum_{i=0}^{p^{n-1-j}-1} (a_{i,j})^{p^{n-1-j}} t^i$$ with $a_{i,j} \in \Omega$ and we set $$j(x) \bmod p^n = \sum_{i,j} p^j [\bar{a}_{i,j}]^{p^{n-1-j}} t^i \bmod p^n \ .$$ Here $[a] \in \Omega_1$ for $a \in \mathcal{O}_1$ is the Teichmüller lift of a. Taking the limit for $n \to \infty$ gives the map j. Compare [4, Section 1]. This map is an injection of W-algebras; we think of Ω as a sub W-algebra of Ω_1.
$\Omega_{2,b}$	$\Omega_2[\pi]/(\pi^b - p)$. We will also write $\pi = p^{1/b}$. Here $b \in \mathbb{N}$. We extend σ to $\Omega_{2,b}$ by $\sigma(\pi) = \pi$. Note that if b divides b', there is a finite free map $\Omega_{2,b} \to \Omega_{2,b'}$.

Γ, Γ_i, $\Gamma_{2,b}$ — The p-adic completions of the rings $\Omega[1/t]$, $\Omega_i[1/t], \Omega_{2,b}[1/t]$. Note that Γ (resp. Γ_i, resp. $\Gamma_{2,b}$) is a complete discrete valuation ring (as Γ_i is p-adically complete, flat over $\mathbb{Z}_p$ and $\Gamma_i/p\Gamma_i = K_i$) with residue field K (resp. K_i, resp. K_2) and uniformizer p (resp. p, resp. $p^{1/b}$). It follows that there are canonical identifications $\Gamma_1 = W(K_1)$ and $\Gamma_2 = W(K_2)$. Note that $\Gamma_{2,b} = \Gamma_2[p^{1/b}]$. There are reduction maps $\Gamma \to K$, $\Gamma_i \to K_i$ ($i = 1,2$) and $\Gamma_{2,b} \to K_2$; these are denoted by $a \mapsto \bar{a}$.

L_i — The fraction field of Γ_i, where the index i is 1, 2, or $2, b$.

$v(f,-)$, $v_i(f,-)$ — The "pole order" function of an element $f \in \Gamma$ or $f \in \Gamma_i$ (the index i is 1, 2, or $2, b$). For a precise definition see 4.1.

$\Gamma_c \subset \Gamma$, $\Gamma_{i,c} \subset \Gamma_i$ — These will denote the subrings of "convergent" power series in Γ and Γ_i (the index i is 1, 2, or $2, b$). More precisely, if $f \in \Gamma$, then by definition $f \in \Gamma_c$ if there exist constants C_1, C_2 such that $v(f,n) \leq C_1 + nC_2$. The same definition is used in the case of Γ_i using $v_i(f,-)$. It is proved in 4.3 that the maps $\Gamma_c \to \Gamma$ and $\Gamma_{i,c} \to \Gamma_i$ are local morphisms of discrete valuation rings with relative ramification index $e = 1$ and inducing an isomorphism on residue fields.

v_p — The p-adic valuation on the discrete valuation rings $\Gamma, \Gamma_c, \Gamma_i$ and $\Gamma_{i,c}$. It is normalized such that $v_p(p) = 1$ and $v_p(p^{1/b}) = 1/b$.

4.1 Let f be an element of Γ. It will be convenient to introduce the function $v(f,-) : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{Z} \cup \{-\infty\}$ defined by

$$v(f,n) = \min\{a \in \mathbb{Z} \mid t^a f \in \Omega + p^{n+1}\Gamma\} \ .$$

For convenience we set $v(f,-1) = -\infty$. We explain this in more down to earth terms. We can write f uniquely in the form $f = \sum_{m \in \mathbb{Z}} a_m t^m$, with $a_m \in W$ and $a_m \to 0$ p-adically when $m \to -\infty$. Thus we can also write (but not uniquely)

$$f = \sum_{n \geq 0} p^n t^{-v_n} \omega_n$$

with $\omega_n \in \Omega$. We may take $v_0 = \cdots = v_{n-1} = \infty$ and $\omega_0 = \cdots = \omega_{n-1} = 0$ if f is divisible by p^n in Γ. Our definition of $v(f,n)$ implies that we can find such a presentation of f with $v_n \leq v(f,n)$ for all n. In fact we can write f as

$$(4.1.1) \qquad f = \sum_{n \text{ such that } v(f,n) > v(f,n-1)} p^n t^{-v(f,n)} \omega_n$$

with $\omega_n \in \Omega^*$. We leave the proof of this fact to the reader.

In the same manner we define for $f \in \Gamma_1$, resp. $f \in \Gamma_2$, resp. $f \in \Gamma_{2,b}$ a function

$$\begin{array}{rcccll} v_1(f,-) & : & \mathbb{N} \cup \{0\} & \longrightarrow & \mathbb{Z}[1/p] \cup \{-\infty\}, & \text{resp.} \\ v_2(f,-) & : & \mathbb{N} \cup \{0\} & \longrightarrow & \mathbb{Q} \cup \{-\infty\}, & \text{resp.} \\ v_{2,b}(f,-) & : & \{0, 1/b, 2/b, \ldots\} & \longrightarrow & \mathbb{Q} \cup \{-\infty\} \; . & \end{array}$$

We remark that these behave well under restriction to subrings (e.g. $v_2|_{\Gamma_1} = v_1$).

4.2 Lemma. *Properties of the functions* $v(f,-)$.

(i) *The function* $v(f,-)$ *is increasing, i.e., we have* $v(f,n) \geq v(f,n-1)$.

(ii) *If* $f, g \in \Gamma$, *then* $v(f+g,n) \leq \max\{v(f,n), v(g,n)\}$ *with equality if* $v(f,n) \neq v(g,n)$.

(iii) *If* $f, g \in \Gamma$, *then* $v(fg,n) \leq \max_{\ell=0,\ldots,n} v(f,\ell) + v(g,n-\ell)$ *with equality if there is exactly one* ℓ *for which the expression* $v(f,\ell) + v(g,n-\ell)$ *is maximal.*

(iv) *If* $f \in \Gamma$ *and* $m \in \mathbb{N}$, *then* $v(p^m f, n) = v(f, n-m)$.

(v) *If* $f \in \Gamma$, *then* $v(\sigma(f),n) = pv(f,n)$. *Similar properties hold for the functions* $v_i(-,-)$, *where the index* i is 1, 2, or $i = 2, b$.

Proof. Left to the reader. □

4.3 The rings Γ_c, $\Gamma_{1,c}$, $\Gamma_{2,c}$ and $\Gamma_{2,b,c}$ are discrete valuation rings whose p-adic completions are Γ, Γ_1, Γ_2 and $\Gamma_{2,b}$. Let us prove this in the case of Γ_c. It is easy to show that $\Gamma_c/p\Gamma_c \to \Gamma/p\Gamma = K$ is an isomorphism. So we just need to check that $p\Gamma_c$ is the unique maximal ideal of Γ_c. To do this we will show that any $f \in \Gamma_c$ with $f \notin p\Gamma_c$ is a unit in Γ_c.

We have $f \notin p\Gamma$, hence $f \in \Gamma^*$, i.e., there is an element $g \in \Gamma$ such that $fg = 1$. In particular, $v(fg,n) = 0$ for all $n \geq 0$. By Lemma 4.2 (iii) we get for all $n \in \mathbb{N}$ the following inequality

$$v(g,n) + v(f,0) \leq \max\{0; v(f,\ell) + v(g; n-\ell), n \geq \ell \geq 1\} \; .$$

Assume that $C > 0$ is a constant such that $v(f, n) \leq nC$ for all $n \geq 1$, and such that $|v(f, 0)| \leq C$, $v(g, 0) \leq C$ and $v(g, 1) \leq C$. Such a constant exists as $f \in \Gamma_c$. We prove by induction on n the statement $H_n : v(g, \ell) \leq 2\ell C, \forall \ell, 1 \leq \ell \leq n$. Clearly this implies that $g \in \Gamma_c$. The assertion H_1 is true by our choice of C. We assume H_{n-1} and prove H_n for $n \geq 2$. The inequalities above and H_{n-1} imply

$$\begin{aligned} v(g, n) &\leq -v(f, 0) + \max\{0; nC + C; \ell C + 2(n-\ell)C, n-1 \geq \ell \geq 1\} \\ &\leq |v(f, 0)| + \max\{0; (n+1)C; (2n-\ell)C, n-1 \geq \ell \geq 1\} \\ &\leq 2nC \end{aligned}$$

Thus we get H_n.

4.4 Definition. *Let (R, σ) be an integral domain with an endomorphism $\sigma : R \to R$. An F-module over R is a pair (M, F), where M is a finitely generated torsion free R-module and $F : M \to M$ is a σ-linear map such that the kernel and cokernel of the R-linear map*

$$M \underset{R,\sigma}{\otimes} R \longrightarrow M$$

are annihilated by some power of p.

Our use of this definition will be restricted to cases where p is not zero in R. In case R is a perfect field of characteristic p and σ is the Frobenius of R, the definition above does not correspond to what is usually called an F-crystal over $\operatorname{Spec} R$. (Such an F-crystal over $\operatorname{Spec} R$ corresponds rather to an F-module over $W(R)$.)

There is an obvious notion of *morphisms of F-modules*. A *sub F-module* N of (M, F) is a submodule $N \subset M$ such that $F(N) \subset N$ and such that the pair $(N, F|_N)$ is itself an F-module. We say that N is a *saturated* sub F-module if M/N is torsion free. In this case $(M/N, F|_{M/N})$ is an F-module. An *isogeny* of F-modules is a morphism $(M, F) \to (M', F')$ such that both the kernel and cokernel of the map $M \to M'$ are killed by a power of p.

Assume that σ is flat. (This condition will be satisfied in the case of the rings we will consider in this article.) In this case $M \otimes_{R,\sigma} R$ is torsion free for any finitely generated R-module M which is torsion free. (Use that there is an injection $M \hookrightarrow R^n$.) Thus given a pair (M, F), with M torsion free and F σ-linear, to see that the pair defines an F-module it suffices to check that the cokernel of $M \otimes_{R,\sigma} R \to M$ is killed by some power of p. Any finitely generated sub module $N \subset M$ such that $F(N) \subset N$ and all torsion of M/N is p-power torsion will be a sub F-module. In particular any finitely generated saturated sub module N of M such that $F(N) \subset N$ will be a sub F-module.

If $(R, \sigma) \to (R', \sigma')$ is a morphism of integral domains with endomorphisms then there is a base change functor $(M, F) \mapsto (M \otimes_R R'/T, F \otimes \sigma')$. Here $T \subset M \otimes_R R'$ is the R'-torsion submodule.

4.5 Slopes

Let R be a complete discrete valuation ring of mixed characteristic with algebraically closed residue field κ of characteristic p. Let L be the quotient field of R. Let $\sigma : R \to R$ be an automorphism inducing the Frobenius map $x \mapsto x^p$ on κ. Let (V, F) be an F-module over L. (Also called an *isocrystal over* L in the literature.) Note that V is a finite dimensional L-vector space and that F is bijective.

There exists a basis $e_1, \dots, e_r$ of V over L and rational numbers $s_1, \dots, s_r \in \mathbb{Q}$ such that $F^n(e_i) = p^{ns_i} e_i$ for sufficiently divisible $n \in \mathbb{N}$ (with $ns_i \in \mathbb{Z}$). See [9]. The rational numbers $s_1, \dots, s_r$ (listed with multiplicities) are unique and are called the *slopes* of the F-module (V, F). The *slope-decomposition*

$$V = \bigoplus_{s \in \mathbb{Q}} V^s \quad \text{with} \quad V^s = \langle e_i ; s_i = s \rangle$$

can be defined intrinsically (interms of V, F and the topology on V). We have

$$\bigoplus_{s > s_0} V^s = \left\{ v \in V \mid \lim_{n \to \infty} p^{-ns_0} F^n(v) = 0 \right\}$$

and

$$\bigoplus_{s < s_0} V^s = \left\{ v \in V \mid \lim_{n \to \infty} p^{ns_0} F^{-n}(v) = 0 \right\} .$$

Two remarks on slopes. If there exists an R-lattice $M \subset V$ with $F(M) \subset M$ then all the slopes of V are ≥ 0. (This is clear from the fact that $\lim p^{n\epsilon} F^n(m) = 0$ for any $m \in M$ and any $\epsilon > 0$.) Suppose $\{v_1, \dots, v_n\}$ is any basis of V, and $F(v_i) = \sum a_{ij} v_j$. Then one has $s_1 + \dots + s_n = v_p(\det(a_{ij}))$. See [9].

Let $\alpha : R \to R$ be an automorphism of R commuting with σ. It induces a continuous automorphism α of L. If V is a vector space over L we write $V_\alpha = V \otimes_{L,\alpha} L$. If (V, F) is an isocrystal over L, then $(V_\alpha, F \otimes \sigma)$ is an isocrystal over L. It follows from the above that the slope decomposition $V = \oplus V^s$ of (V, F) determines the slope decomposition of $(V_\alpha, F \otimes \sigma)$. The slope s submodule of V_α is equal to $V^s \otimes_{L,\alpha} L$. In particular the set of slopes with multiplicities of V_α is equal to that of V.

4.6 Suppose that (M, F) is an F-module over one of the rings $R = \Omega, \Omega_i, \Gamma, \Gamma_c, \Gamma_i, \Gamma_{i,c}, L_i$ (the index i is 1, 2, or $2, b$). Then we can look at the F-module $(M \otimes_R L_{2,b}, F \otimes \sigma)$ over $L_{2,b}$. By the above it has slopes.

4.7 Definition. *The slopes $s_1 \leq \cdots \leq s_r$ of a rank r F-module (M, F) over one of the rings R listed above are the slopes of the isocrystal $M \otimes L_{2,b}$ over $L_{2,b}$ as defined in* 4.5.

We note that (after making b more divisible) $M \otimes L_{2,b}$ has a basis $e_1, \ldots, e_r$ such that $F(e_i) = p^{s_i} e_i$. We say that (M, F) is *isoclinic of slope s* if all the slopes s_i are equal to s.

We remark that if $R = \Omega, \Omega_i$ then there is another F-module associated to M over R, namely the F-module $\big((M \otimes_R W_b)/\text{torsion}, F \otimes \sigma\big)$ over W_b. This gives rise to an isocrystal over $L_{0,b}$ with slopes s'_i. The slopes s_i are in general different from the slopes s'_i. A fundamental result, see [9], is that the Newton polygon of the slopes s'_i lies above the Newton polygon defined by the slopes s_i. In particular, if M is isoclinic of slope s, then all s'_i are equal to s as well. Although we do not use this fact it is one of the ideas behind the arguments in Section 6.

4.8 In case of the ring R is equal to Ω, Γ, Γ_c or $\Gamma(D, \mathcal{O}_D)$ we have the derivation $\frac{d}{dt} : R \to R$. In any of these rings an element f has a unique expansion $f = \sum_{n \in \mathbb{Z}} a_n t^n$, with $a_n \in W$ or L_0. We put $\frac{d}{dt} f = \sum_n n a_n t^{n-1}$, which again lies in R. The map $\frac{d}{dt} : R \to R$ is a derivation.

4.9 Definition. *Let R be as above. An (F, θ)-module over R is a triple (M, F, θ), where (M, F) is an F-module over R and $\theta : M \to M$ is an additive map such that $\theta(fm) = f\theta(m) + \frac{d}{dt}(f)m$ and $pt^{p-1}F(\theta(m)) = \theta(F(m))$ for all $m \in M$ and $f \in R$.*

Note that if we take $M = R$, $F = p^\ell \sigma$ and $\theta = \frac{d}{dt}$, then (M, F, θ) is an (F, θ)-module.

5 Splitting an equation

We will work in the noncommutative polynomial algebra $\Gamma_{2,b,c}[F]$, where $F\gamma = \sigma(\gamma)F$ for all $\gamma \in \Gamma_{2,b,c}$. It is a subring of the ring $\Gamma_{2,b}[F]$.

5.1 Proposition. *Let $F^n + a_1 F^{n-1} + \cdots + a_n \in \Gamma_{2,b,c}[F]$ be a monic polynomial in F. There exists a $b' \in \mathbb{N}$, $b | b'$ and elements $\lambda_1, \ldots, \lambda_n \in \Gamma_{2,b',c}$ such that we have*

(i) $F^n + a_1F^{n-1} + \cdots + a_n = (F - \lambda_1)(F - \lambda_2)\cdots(F - \lambda_n)$.
(ii) $v_p(\lambda_1) \geq v_p(\lambda_2) \geq \cdots \geq v_p(\lambda_n)$.

Proof. We will prove this by induction on n; the case $n = 1$ is trivial. We will try to solve

$$F^n + a_1F^{n-1} + \cdots + a_n = \left(F^{n-1} + b_1F^{n-2} + \cdots + b_{n-1}\right)(F - \lambda)$$

with $b_i, \lambda \in \Gamma_{2,b,c}$. This equation is equivalent to the set of equations:

$$\begin{aligned} b_1 &= a_1 + \sigma^{n-1}(\lambda) \\ b_2 &= a_2 + \sigma^{n-2}(\lambda)b_1 \\ &\cdots\cdots \\ b_{n-1} &= a_{n-1} + \sigma(\lambda)b_{n-2} \\ 0 &= a_n + \lambda b_{n-1} \end{aligned}$$

If we solve $b_1, \ldots, b_{n-1}$ in terms of $a_1, \ldots, a_{n-1}, \lambda$ from the first $n - 1$ equations then the last equation becomes

$$\begin{aligned} 0 = a_n + \lambda a_{n-1} + \lambda\sigma(\lambda)a_{n-2} + \cdots + \lambda\sigma(\lambda)\cdots\sigma^{n-2}(\lambda)a_1 \\ + \lambda\sigma(\lambda)\cdots\sigma^{n-1}(\lambda)\ . \end{aligned} \tag{1}$$

Put

$$\alpha = \min_{i=1,\ldots,n} \frac{v_p(a_i)}{i}\ .$$

We may assume that $\alpha = a/b$ for some $a \in \mathbb{Z}_{\geq 0}$ if we make b more divisible. We are going to solve (1) for some $\lambda \in \Gamma_{2,b,c}$ of the form $\lambda = p^\alpha u$ with $u \in \Gamma^*_{2,b,c}$. If we can do this then the proposition follows. Indeed, if we have such a solution λ, then $b_1 = a_1 + \sigma^{n-1}(\lambda)$ will be an element of $\Gamma_{2,b,c}$ with $v_p(b_1) \geq \alpha$. And $b_2 = a_2 + \sigma^{n-2}(\lambda)b_1$ implies $b_2 \in \Gamma_{2,b,c}$ has $v_p(b_2) \geq 2\alpha$, etc. Continuing we get $v_p(b_i) \geq i\alpha$, so that the invariant $\min v_p(b_i)/i \geq \alpha$ has gone up. By induction we get a splitting $F^{n-1} + b_1F^{n-2} + \cdots + b_{n-1} = (F - \lambda_1)\cdots(F - \lambda_{n-1})$, with $v_p(\lambda_{n-1}) = \min v_p(b_i)/i$ and we are done.

We re-write (1), by setting $\lambda = p^\alpha u$ and dividing by $p^{n\alpha}$:

$$0 = p^{-n\alpha}a_n + p^{-(n-1)\alpha}a_{n-1}u + \cdots + u\sigma(u)\cdots\sigma^{n-1}(u)\ . \tag{2}$$

Note that all the elements $a'_i = p^{-i\alpha}a_i \in \Gamma_{2,b,c}$ and for some i we have $a'_i \in \Gamma^*_{2,b,c}$. Recall that $a \mapsto \bar{a}$ denotes the map $\Gamma_{2,b,c} \subset \Gamma_{2,b} \to K_2$. The equation (2) reduces to the equation

$$0 = \bar{a}'_n + \cdots + \bar{a}'_i \bar{u}^{1+p+\ldots+p^{n-i-1}} + \cdots + \bar{u}^{1+p+\cdots+p^{n-1}}$$

in K_2. This has a non zero solution $\bar{u} \in K_2$, as it is a polynomial equation with at least two nonzero coefficients and K_2 is algebraically closed. (We remark for later reference that if $v_p(a_n) = n\alpha$ and $n \geq 2$, then there are at least two distinct nonzero solutions.)

We will first show that (2) has a solution $u \in \Gamma_{2,b}$ which is congruent to the solution $\bar{u}$ we found above; after this we will prove that actually $u \in \Gamma_{2,b,c}$. (Then necessarily $u \in \Gamma^*_{2,b,c}$.) Suppose that $u_r \in \Gamma_{2,b}$, $r \geq 1$ is a solution of (2) modulo $p^{r/b}$ and that $\bar{u}_r = \bar{u} \neq 0$. In order that $u_{r+1} = u_r + p^{r/b}\delta_r$ is a solution of (2) modulo $p^{(r+1)/b}$, we have to solve a polynomial equation in terms of $\bar{\delta}_r$ with leading term

$$\bar{u}^{1+\cdots+p^{n-2}} (\bar{\delta}_r)^{p^{n-1}} \quad .$$

As K_2 is algebraically closed, we can solve this equation and we get u_{r+1}. The limit of the elements u_r will be an element $u \in \Gamma^*_{2,b}$ solving (2). We are going to prove such a solution lies in $\Gamma_{2,b,c}$. (If $n = 2$ and $v_p(a_2) = 2\alpha$ there are at least 2 solutions, see previous remark.)

Let us write $\tilde{v}(f, m) = v_{2,b}(f, m/b)$ for $f \in \Gamma_{2,b}$ and $m \in \mathbb{Z}_{\geq 0}$. We choose a constant $C > 0$ such that $v(a'_i, m) \leq mC$ for all $m \geq 1$, all i and such that C is much larger then $|\tilde{v}(a'_i, 0)|$ and $|\tilde{v}(u, 0)|$. (A factor p^{n+1} will do.) This is possible as all a'_i are elements of $\Gamma_{2,b,c}$. We are going to prove by induction on m the statement $H_m : \tilde{v}(u, \ell) \leq \ell C$, $1 \leq \ell \leq m$. The assertion H_0 is empty. We assume H_{m-1} and $m \geq 1$ and prove H_m. By Lemma 4.2 we have

$$\tilde{v}(u\sigma(u)\cdots\sigma^{n-1}(u), m) \leq \max_{i_1,\ldots,i_n} \tilde{v}(u, i_1) + p\tilde{v}(u, i_2) + \cdots + p^{n-1}\tilde{v}(u, i_n) \tag{3}$$

where the maximum is taken over all n-tuples $(i_1, \ldots, i_n)$ with $i_j \geq 0$ and $\sum i_j = m$. One of the terms on the right hand side is

$$\left(1 + \cdots + p^{n-2}\right)\tilde{v}(u, 0) + p^{n-1}\tilde{v}(u, m) \quad . \tag{4}$$

It occurs if $(i_1, \ldots, i_n) = (0, \ldots, 0, m)$. If this term does not strictly exceed all others, then there exists an n-tuple $(i_1, \ldots, i_n)$ with $i_j \geq 0$ and $\sum i_j = m$ and $i_n < m$ such that

$$\begin{aligned}\left(1 + \cdots + p^{n-2}\right)\tilde{v}(u, 0) + p^{n-1}\tilde{v}(u, m) \leq{}& \tilde{v}(u, i_1) + p\tilde{v}(u, i_2) \\ &+ \cdots + p^{n-1}\tilde{v}(u, i_n) \quad .\end{aligned} \tag{5}$$

The case that $i_j = m$ for some $j < n$ in (5), which implies $i_{j'} = 0$ for $j' \neq j$, leads to the inequality

$$\left(p^{n-1} - p^j\right)\tilde{v}(u,m) \leq -p^j\tilde{v}(u,0) \ .$$

By our choice of C and as $m \geq 1$, we conclude $\tilde{v}(u,m) \leq mC$ in this case. Thus we may assume $i_j < m$ for all j in (5). This gives using H_{m-1} the following inequality:

$$\begin{aligned}\tilde{v}(u,i_1) + p\tilde{v}(u,i_2) + \cdots + p^{n-1}\tilde{v}(u,i_n) &\leq \sum_{i_j=0} p^{j-1}\tilde{v}(u,0) + \sum_{i_j\neq 0} p^{j-1}i_jC \\ &\leq \left(1 + \cdots + p^{n-1}\right)|\tilde{v}(u,0)| + p^{n-2}C + p^{n-1}(m-1)C \ .\end{aligned}$$

The last inequality holds because $\sum i_j = m$ and $i_n < m$. Combining this with (5) gives

$$v(u,m) \leq \frac{2(1 + \cdots + p^{n-1})|\tilde{v}(u,0)|}{p^{n-1}} + (m-1)C + p^{-1}C \leq mC \ ,$$

where the last inequality uses $C \gg |\,\tilde{v}(u,0)|$ (e.g. $C \geq p^{n+1}|\tilde{v}(u,0)|$). This proves H_m in case the term (4) does not dominate in the right hand side of (3).

Therefore we may assume that (4) does dominate in the right hand side of (3) and hence we have that $\tilde{v}(u\sigma(u)\cdots\sigma^{n-1}(u),m)$ equals (4) by Lemma 4.2 (iii). Hence, by Lemma 4.2 (ii), we see that (4) is dominated by the maximum of the values of $\tilde{v}(-,m)$ evaluated on the other terms that appear in (2). We have for $\ell \geq 1$ the following bound

$$\begin{aligned}\tilde{v}\left(a'_\ell u\sigma(u)\cdots\sigma^{n-\ell-1}(u),m\right) \leq \max_{i_0,i_1,\ldots,i_{n-\ell}} &\ \tilde{v}(a'_\ell,i_0) + \tilde{v}(u,i_1) \\ &+ \cdots + p^{n-\ell-1}\tilde{v}(u,i_{n-\ell}) \ ,\end{aligned}$$

where the maximum is taken over all $(n-\ell+1)$-tuples $(i_0,\ldots,i_{n-\ell})$, with $i_j \geq 0$ and $\sum i_j = m$. Again the assumption that a term with $i_j = m$ for some $j \in \{1,\ldots,n-\ell\}$ is biggest leads to an inequality of the form $\tilde{v}(u,m) \leq C_2$, where C_2 is a constant depending only on $\tilde{v}(a'_i,0)$, p, n and $\tilde{v}(u,0)$. Hence we get H_m as $m \geq 1$ and C was chosen large enough. For the other terms one gets a majoration by

$$\begin{aligned}&i_0C + p^{n-\ell-1}(m-i_0)C + |\tilde{v}(a'_\ell,0)| + \left(1 + \cdots + p^{n-\ell-1}\right)|\tilde{v}(u,0)| \\ &\quad \leq p^{n-\ell-1}mC + C_3 \ .\end{aligned}$$

The fact that (4) is bounded by this suffices to imply $\tilde{v}(u,m) \leq mC$, as $\ell \geq 1$ and C was chosen large enough. $\square$

5.2 Corollary. *Let (M,F) be an F-module over $\Gamma_{2,b,c}$. There exists a $b' \in \mathbb{N}$, $b|b'$ such that $M \otimes \Gamma_{2,b',c}$ has a filtration $0 \subset N_1 \subset N_2 \subset \cdots \subset N_r = M \otimes \Gamma_{2,b',c}$ by saturated sub F-modules N_i such that* $\operatorname{rank} N_i = i$.

Proof. Take a non zero element $m \in M$. There is a monic polynomial $P(F) = F^n + \cdots + a_n \in \Gamma_{2,b,c}[F]$ such that $P(F)m = 0$ in M. Say P has minimal degree. After replacing b by b' as in the proposition we get $P(F) = (F - \lambda_1) \cdots (F - \lambda_n)$. The submodule N_1' of M generated by $(F - \lambda_2) \cdots (F - \lambda_n)m$ has rank 1. We have $F(N_1') \subset N_1'$ as $P(F)m = 0$. The same hold for its saturation $N_1 = \{x \in M \mid p^a x \in N_1' \text{ some } a\}$. Thus N_1 is a sub F-module and M/N_1 is an F-module with strictly smaller rank than M. We win by applying induction (on the rank of M) to M/N_1. $\square$

5.3 Corollary. *Let $0 \to N_1 \to M \to N_2 \to 0$ be a short exact sequence of F-modules over $\Gamma_{2,b,c}$. Assume N_i has rank* 1 *and let s_i be its slope* 4.5. *If $s_1 \leq s_2$, then there is a rank* 1 *sub F-module $N' \subset M$ such that $N' \to N_2$ is an isogeny.*

Proof. Choose a generator n_i of N_i. We have $F(n_i) = \mu_i n_i$ for some $\mu_i \in \Gamma_{2,b,c}$. Note that $s_i = v_p(\mu_i)$ by the remarks in 4.5, hence $v_p(\mu_1) \leq v_p(\mu_2)$ by assumption. Choose $\tilde{n}_2 \in M$ lifting n_2. We have

$$(F - \mu_2)\tilde{n}_2 = \mu n_1$$

for some $\mu \in \Gamma_{2,b,c}$. If $\mu = 0$, then the extension is split; if not then we have $v_p(\sigma(\mu)\mu^{-1}) = 0$. (This computation takes place in $L_{2,b,c}$; note that $v_p \circ \sigma = v_p$.) Thus we have $\sigma(\mu)\mu^{-1} \in \Gamma^*_{2,b,c}$. Since $(F - \sigma(\mu)\mu^{-1}\mu_1)(\mu n_1) = 0$, we see that

$$\begin{aligned} 0 &= \big(F - \sigma(\mu)\mu^{-1}\mu_1\big)(F - \mu_2)\tilde{n}_2 \\ &= \big(F^2 - \big(\sigma(\mu)\mu^{-1}\mu_1 + \sigma(\mu_2)\big)F + \sigma(\mu)\mu^{-1}\mu_1\mu_2\big)(\tilde{n}_2)\ . \end{aligned}$$

By the proposition we get a splitting of the degree 2 polynomial as $(F - \lambda_1)(F - \lambda_2)$, with $v_p(\lambda_1) \geq v_p(\lambda_2)$. Note that we do not need to enlarge b, as the invariant α used in the proof of Proposition 5.1 equals $v_p(\mu_1)$. If $s_1 < s_2$ then $v_p(\lambda_2) \neq v_p(\mu_2)$, since $\lambda_1\lambda_2 = \sigma(\mu)\mu^{-1}\mu_1\mu_2$. In case $v_p(\mu_1) = v_p(\mu_2)$, we also do not need to enlarge b and $v_p(\sigma(\mu)\mu^{-1}\mu_1\mu_2) = 2\alpha$ so that we may choose $\lambda_2 \neq \mu_2$ according to the remarks made on the number of solutions in the proof of the proposition. The element $(F - \lambda_2)\tilde{n}_2$ will generate the rank 1 sub F-module N' of M we are looking for: we have $N' \cap N_1 = (0)$ as $\lambda_2 \neq \mu_2$. $\square$

5.4 Lemma. *Let N be a rank 1 F-module over $\Gamma_{2,b,c}$. There is a generator $n \in N$ such that $F(n) = p^s n$, where $s = a/b$ is the slope of N.*

Proof. Take any generator n of N. Then $F(n) = p^s \eta n$ for some unit $\eta \in \Gamma^*_{2,b,c}$ and some $s \in 1/b\mathbb{Z}$. We have to solve $\sigma(\epsilon) = \eta\epsilon$ with $\epsilon \in \Gamma_{2,b,c}$ a unit. Arguing as in the proof of Proposition 5.1 a solution $\epsilon \in \Gamma^*_{2,b}$ is found. A consideration using the functions $v_{2,b}(\epsilon, -)$ and $v_{2,b}(\eta, -)$ shows that ϵ is in $\Gamma_{2,b,c}$ (use Lemma 4.2 (ii) and (iii)). $\square$

5.5 Proposition. *Let (M, F) be an F-module over $\Gamma_{2,b,c}$.*

(i) *There exists a unique filtration by saturated sub F-modules $0 \subset M_1 \subset M_2 \subset \cdots \subset M_a = M$ such that M_i/M_{i-1} is an isoclinic F-module of slope s_i and $s_1 > s_2 > \cdots > s_a$.*

(ii) *If M is isoclinic of slope s, then for some $b' \in \mathbb{N}$, $b|b'$ the F-module $M \otimes \Gamma_{2,b',c}$ over $\Gamma_{2,b',c}$ is isogenous to a direct sum of copies of the rank 1 module $(\Gamma_{2,b',c} \cdot e, F)$, with $F(e) = p^s e$.*

Proof. Note that if b divides b', then $\Gamma_{2,b',c} = \Gamma_{2,b,c} \oplus \pi\Gamma_{2,b,c} \oplus \cdots \oplus \pi^{r-1}\Gamma_{2,b,c}$ with $r = b'/b$ and $\pi = p^{1/b'}$ as F-modules over $\Gamma_{2,b,c}$ (with $F = \sigma$ since $\sigma(\pi) = \pi$). Suppose $M_1 \subset M \otimes_{\Gamma_{2,b,c}} \Gamma_{2,b',c}$ is a sub F-module. We get $\Gamma_{2,b,c}$-linear F-compatible maps

$$M_1 \longrightarrow M \otimes_{\Gamma_{2,b,c}} \Gamma_{2,b',c} = \bigoplus_{i=0}^{r-1} \pi^i M \xrightarrow{\mathrm{pr}_i} M \ .$$

Also, if M_1 has rank r_1 over $\Gamma_{2,b',c}$, then M_1 has rank rr_1 over $\Gamma_{2,b,c}$, so at least one of these composite maps has rank at least r_1. Furthermore, if the slopes of the F-module M_1 over $\Gamma_{2,b',c}$ are $s_1, \ldots, s_{r_1}$, then the slopes of M_1 considered as an F-module over $\Gamma_{2,b,c}$ are $s_1, \ldots, s_1, s_2, \ldots, s_2, \ldots, s_{r_1}, \ldots, s_{r_1}$ (each s_i is repeated r times). Thus if M_1 is a maximal isoclinic $\Gamma_{2,b',c}$-subspace of $M \otimes_{\Gamma_{2,b,c}} \Gamma_{2,b',c}$ with slope s_1 and rank r_1, we get a $\Gamma_{2,b,c}$-subspace of M of slope s_1 and of rank at least r_1. We conclude by uniqueness of slope decomposition that M_1 is defined over $\Gamma_{2,b,c}$. Arguing by induction we see that a slope filtration over $\Gamma_{2,b',c}$ descends to a slope filtration over $\Gamma_{2,b,c}$.

Therefore we may assume b is sufficiently divisible and we get a filtration of M as in Corollary 5.2. By Corollary 5.3 we may assume the filtration $0 \subset N_1 \subset N_2 \subset \cdots \subset N_r = M$ is such that the slopes of

N_i/N_{i-1} decrease when i increases. This proves (i). The second statement is proved in the same manner using Lemma 5.4. $\square$

5.6 Remark. In fact, if (M, F) over $\Gamma_{2,b,c}$ is isoclinic of slope $s = a/b'$, $\gcd(a, b') = 1$ then it is isogenous over $\Gamma_{2,b,c}$ to a direct sum of copies of the module $M(s)$ described below. Let $r = b'/\gcd(b, b')$ and let $M(s)$ be the free $\Gamma_{2,b,c}$ module with basis $e_1, \ldots, e_r$. Put $F(e_i) = e_{i+1}$, $i < r$ and $F(e_r) = p^{rs}e_1$. Note that $rs \in (1/b)\mathbb{Z}$ so that this makes sense. We will not use this result. $\square$

5.7 Corollary. *Let (M, F) be an F-module over $\Gamma_{2,b,c}$. Say M has a slope filtration $0 \subset M_1 \subset \cdots \subset M_a = M$ with slopes $s_1 > s_2 > \cdots > s_a$ as in the proposition. Let*

$$\varphi : M \longrightarrow \Gamma_{2,b}$$

be $\Gamma_{2,b,c}$-linear and such that for some $\ell \in (1/b)\mathbb{Z}$, $\ell \geq 0$ we have $\varphi(F(m)) = p^{\ell}\sigma(\varphi(m))$ for all $m \in M$. Then

(i) *The kernel of φ contains M_i whenever $s_i > \ell$.*

(ii) *If φ is injective and $M \neq (0)$, then $s_1 = \ell$,* $\operatorname{rank} M_1 = 1$ and $\varphi(M_1) \subset \Gamma_{2,b,c} \subset \Gamma_{2,b}$.

(iii) *If $\ell > s_1$, then $\varphi = 0$.*

Proof. Since $\operatorname{Ker}(\varphi)$ is a saturated submodule of M and stable under F, we may replace M by $M/\operatorname{Ker}(\varphi)$ and it suffices to prove (ii) for this module. Thus we assume that φ is injective. We are allowed to make b more divisible in proving (ii), as the extension $\Gamma_{2,b,c} \subset \Gamma_{2,b',c}$ is finite free and $\Gamma_{2,b'} = \Gamma_{2,b} \otimes_{\Gamma_{2,b,c}} \Gamma_{2,b',c}$. Hence we may assume by Proposition 5.5 that there is an isogeny

$$N_1 \oplus \cdots \oplus N_r \longrightarrow M_1$$

with $\operatorname{rank} N_i = 1$. In fact we can find nonzero $n_i \in N_i$ such that $F(n_i) = p^{s_1}n_i$ for each i. Thus $\varphi(n_i) = f_i \in \Gamma_{2,b}$ is an element with

$$p^{\ell}\sigma(f_i) = p^{s_1}f_i \ .$$

This relation implies $\ell = s_1$ as $v_p(\sigma(f_i)) = v_p(f_i)$. Note that $f_i \neq 0$ as φ is injective. Thus we have $\sigma(f_i) = f_i$. We apply $v_{2,b}(-, m)$ and we get

$$pv_{2,b}(f_i, m) = v_{2,b}(f_i, m) \ ,$$

whence $v_{2,b}(f_i, m) \in \{-\infty, 0\}$ for all m. Thus $f_i \in \Gamma_{2,b,c}$. This means that $f_1, \dots, f_r$ are linearly dependent over $\Gamma_{2,b,c}$. As we assumed that φ is injective it follows that $r = 1$. $\square$

5.8 Proposition. *Suppose (M, F) is an F-module over $\Gamma_{1,c}$. The slope filtration of $M \otimes_{\Gamma_{1,c}} \Gamma_{2,c}$ given by Proposition 5.5 is defined over $\Gamma_{1,c}$. More precisely, there exists a unique filtration by saturated sub F-modules*

$$0 \subset M_1 \subset \cdots \subset M_a = M$$

with M_i/M_{i-1} isoclinic of slope s_i and $s_1 > s_2 > \cdots > s_a$.

Proof. Let $\mathcal{G} = \mathrm{Gal}(K_2/K_1)$. For any $\tau \in \mathcal{G}$ we get a continuous automorphism $W(\tau) : W(K_2) \to W(K_2)$ by definition of the ring of Witt vectors. Note that τ commutes with Frobenius σ. The automorphism τ also preserves the subring $\Gamma_{2,c} \subset \Gamma_2 = W(K_2)$. Indeed, it preserves the functions $v(f, -)$ as $\tau(t^{1/n}) = \zeta t^{1/n}$ for some root of unity $\zeta \in K_2$ and $\zeta \in \mathcal{O}_2^*$. By the remarks made in the Section 4.5 we see that the map

$$M \otimes_{\Gamma_{1,c}} \Gamma_{2,c} \xrightarrow{\mathrm{id}_M \otimes W(\tau)} M \otimes_{\Gamma_{1,c}} \Gamma_{2,c}$$

preserves the filtration by slopes $0 \subset M_1' \subset \cdots \subset M_a' = M \otimes \Gamma_{2,c}$ given by Proposition 5.5.

Note that M is a free $\Gamma_{1,c}$-module of finite rank. Let $\mathcal{F}$ be the partial flag scheme of M over $\mathrm{Spec}\,\Gamma_{1,c}$ parametrizing flags $0 \subset F_1 \subset \cdots \subset F_a = M$ in M with $\mathrm{rank}\, F_i = \mathrm{rank}\, M_i'$. A morphism of a scheme S over $\Gamma_{1,c}$ into $\mathcal{F}$ is given by a filtration of the sheaf $\mathcal{O}_S \otimes_{\Gamma_{1,c}} M$. Then $\mathcal{F}$ is a smooth projective scheme over $\mathrm{Spec}\,\Gamma_{1,c}$. The filtration M_*' defines a morphism $x : \mathrm{Spec}\,\Gamma_{2,c} \to \mathcal{F}$ over $\mathrm{Spec}\,\Gamma_{1,c}$. Take any affine open $U \subset \mathcal{F}$ such that $\mathrm{Im}(x) \subset U$. Take any element $f \in \Gamma(U, \mathcal{O}_U)$. The fact proven above that the filtration M_*' is stable for all $W(\tau)$, $\tau \in \mathcal{G}$ means that the element $x^*(f) \in \Gamma_{2,c}$ is fixed by all automorphisms $W(\tau)$ of $\Gamma_{2,c}$. Then it is easy to see that $x^*(f) \in \Gamma_{1,c}$. This means that x and hence M_*' are defined over $\Gamma_{1,c}$. $\square$

6 Entire versus convergent power series

Let (M, F, θ) be an (F, θ)-module over $\Omega = W[[t]]$.

6.1 Lemma. *There is an isogeny $M \to M'$ to a free (F, θ)-module (M', F, θ) over Ω* (i.e., *M' is a finite free Ω-module*).

Proof. The dual of a finitely generated Ω-module W is finite free, since Ω is a regular local ring of dimension 2. Thus we take for M' the double dual of M:

$$M' = \mathrm{Hom}_\Omega(\ \mathrm{Hom}_\Omega(M, \Omega),\ \Omega\ )\ .$$

The evaluation map $ev : M \to M'$ has a finite length cokernel. If $m' \in M'$, then $t^n m' \in M$ and $p^n m' \in M$ for some large $n \in \mathbb{N}$. Define $F(m')$ to be the element in M' such that $p^n F(m') = F(p^n m')$ and $t^{pn} F(m') = F(t^n m')$. Such an element $F(m') \in M'$ exists as $t^{pn} F(p^n m') = p^n F(t^n m')$. Clearly $F(m')$ is independent of the choice of n.

To define θ, we take such an n as above. Then we define $\theta(m') \in M'$ as the element such that $t^n \theta(m') = -nt^{n-1} m' + \theta(t^n m')$ and $p^n \theta(m') = \theta(p^n m')$. Existence is proved as above. It is readily proved that F and θ on M' have the desired properties. $\square$

6.2 Lemma. *Classification of rank* 1 *modules over* Ω.

(i) *Let* (M, F) *be a rank* 1 *F-module over* Ω. *Then M is isogenous to* $(\Omega, p^\ell \sigma)$ *for some* $\ell \in \mathbb{Z}_{\geq 0}$. *If M is free then M is isomorphic to* $(\Omega, p^\ell \sigma)$.

(ii) *Let* (M, F, θ) *be a rank* 1 (F, θ)*-module over* Ω. *Then M is isogenous to* $(\Omega, p^\ell \sigma, \frac{d}{dt})$ *for some* $\ell \in \mathbb{Z}_{\geq 0}$. *If M is free of rank one then M is isomorphic to* $(\Omega, p^\ell \sigma, \frac{d}{dt})$.

Proof. Proof of (i). We may assume that M is free by Lemma 6.1 (without θ). Let $m \in M$ be a basis element. We have $F(m) = \lambda m$ and we have $\Omega/\lambda\Omega$ killed by some power of p (axiom of F-modules). Since Ω is a UFD in which p is irreducible, $\lambda = p^\ell \eta$ for some unit $\eta \in \Omega^*$ and some $\ell \in \mathbb{Z}_{\geq 0}$. If we replace m by ϵm, with $\epsilon \in \Omega^*$, then η is replaced by $\eta\sigma(\epsilon)\epsilon^{-1}$. Thus we have to solve the equation $\eta\sigma(\epsilon)\epsilon^{-1} = 1$ for a unit $\epsilon \in \Omega^*$. It is well-known (classification of rank 1 F-modules over W) that one can solve this equation in W^*. Hence we may assume we have ϵ such that $\eta\sigma(\epsilon)\epsilon^{-1} = 1 + t\omega$, some $\omega \in \Omega$. In this case $\eta\sigma(\epsilon + t\delta)(\epsilon + t\delta)^{-1} \equiv 1 + t(\omega - \epsilon^{-1}\delta) \bmod t^2\Omega$ (recall that $\sigma(t) = t^p$ and $p \geq 2$). Hence we can find a solution modulo t^2. By induction one finds compatible solutions modulo any power of t, hence a solution.

Proof of (ii). Again we may assume that M is free. By (i) there exists a basis element $e \in M$ such that $F(e) = p^\ell e$. It is easy to see that also $\theta(e) = 0$, as we have $p^\ell \theta(e) = \theta(F(e)) = pt^{p-1} F(\theta(e))$ in this case, see Definition 4.9. $\square$

Let (M, F, θ) be an arbitrary (F, θ)-module and let $M \to M'$ be the isogeny of Lemma 6.1. Let $r = \operatorname{rank} M$. In the following we will use the map $\Omega = W[[t]] \to W$ with $t \mapsto 0$. Choose elements $e_1, \dots, e_r \in M' \otimes_\Omega W$ linearly independent over W such that

$$F^n(e_i) = p^{a_i} e_i \ .$$

This is possible if n is the common denominator of the slopes of the F-module $M' \otimes_\Omega W$ and its slopes are a_i/n. See 4.5, it was remarked there that $a_i/n \geq 0$ in this case so that $a_i \in \mathbb{Z}_{\geq 0}$. We lift e_i to an element $m_i \in M'$. Note that the quotient $M'/\langle m_1, \dots, m_r \rangle$ is p-power torsion. We have

$$F^n(m_i) = p^{a_i} m_i + t\delta_i$$

for certain $\delta_i \in M'$. If we apply F^n once again we get $F^{2n}(m_i) = p^{2a_i} m_i + p^{a_i} t\delta_i + t^{p^n} F^n(\delta_i)$. Proceeding by induction we see that

$$F^{Nn}(m_i) = p^{Na_i} m_i + \sum_{j=1}^{N} p^{(N-j)a_i} t^{p^{n(j-1)}} F^{n(j-1)}(\delta_i) \ .$$

In particular we have $F^{Nn}(m_i) - p^{a_i} F^{(N-1)n}(m_i) \in t^{p^{n(N-1)}} M'$ for $N \geq 1$. We conclude that

$$m_{i,\infty} = \lim_{N \to \infty} p^{-Na_i} F^{Nn}(m_i)$$

is a well defined element of $M' \otimes_\Omega \Gamma(D, \mathcal{O}_D)$. (To see this more explicitly: note that $m_{i,\infty} = m_i + \sum_{j=1}^{\infty} p^{-j} t^{p^{n(j-1)}} F^{n(j-1)}(\delta_i)$ and writing this in terms of a basis for M' will give coefficients which are elements of $\Gamma(D, \mathcal{O}_D)$. See Section 4 for an explicit description of elements of $\Gamma(D, \mathcal{O}_D)$.) Note that $M' \otimes_\Omega \Gamma(D, \mathcal{O}_D) = M \otimes_\Omega \Gamma(D, \mathcal{O}_D)$ as $M \to M'$ is an isogeny and $p^{-1} \in \Gamma(D, \mathcal{O}_D)$. The $m_{i,\infty}$ are elements of the (F, θ)-module $M \otimes_\Omega \Gamma(D, \mathcal{O}_D)$ over $\Gamma(D, \mathcal{O}_D)$ such that $F^n(m_{i,\infty}) = p^{a_i} m_{i,\infty}$. Furthermore,

$$\theta\big(p^{Na_i} m_{i,\infty}\big) = \theta\big(F^{Nn}(m_{i,\infty})\big) = p^{Nn} t^{p^{Nn}-1} F^{Nn}(\theta(m_{i,\infty})) \ .$$

We conclude that the elements $\theta(m_{i,\infty})$ of the module $M \otimes_\Omega \mathcal{O}_D$ have vanishing power series expansions around $t = 0$ (with respect to any basis of M'). Thus they are zero. Therefore the elements $m_{i,\infty}$ are horizontal for the integrable connection on $M \otimes \mathcal{O}_D$ given by letting θ act as $\theta \otimes 1 + 1 \otimes \frac{d}{dt}$. They also give a basis of the fiber at $t = 0$ of

$M \otimes \mathcal{O}_D$, as $m_{i,\infty} \equiv e_i \bmod t$. The exterior power $m_{1,\infty} \wedge \cdots \wedge m_{r,\infty}$ is a horizontal element of $\Lambda^r(M') \otimes \Gamma(D, \mathcal{O}_D)$. By Lemma 6.2 we know that $\Lambda^r(M')$ has a horizontal basis element e. Thus $m_{1,\infty} \wedge \cdots \wedge m_{r,\infty} = e \otimes f$ with $f \in \Gamma(D, \mathcal{O}_D)$ and $\frac{d}{dt}(f) = 0$, hence $f \in W$. By the above $f \not\equiv 0 \bmod t$, so $f \neq 0$. Therefore the elements $m_{i,\infty}$ form a basis of $M \otimes_\Omega \Gamma(D, \mathcal{O}_D)$. This proves Dwork's trick.

6.3. Lemma. (*Dwork's trick.*) *For any (F, θ)-module (M, F, θ) the (F, θ)-module $M \otimes_\Omega \Gamma(D, \mathcal{O}_D)$ over $\Gamma(D, \mathcal{O}_D)$ has a basis of elements d_i, which are horizontal and satisfy $F^n(d_i) = p^{a_i} d_i$ for certain $n \in \mathbb{N}$ and $a_i \in \mathbb{Z}_{\geq 0}$.*

6.4 Proposition. *Notations as in previous lemma. If $N' \subset M \otimes_\Omega \Gamma_c$ is a saturated sub (F, θ)-module then $N' = N \otimes \Gamma_c$ for some saturated sub (F, θ)-module $N \subset M$.*

Proof. We may replace M by M' as in Lemma 6.1 and N' by its saturation in $M' \otimes \Gamma_c$. Thus we may assume that M is free over Ω (and N' & $M \otimes \Gamma_c / N'$ are free over Γ_c). Let $r = \operatorname{rank} N'$. It suffices to prove the proposition for $\wedge^r N' \subset \wedge^r(M) \otimes \Gamma_c$, so we may assume $\operatorname{rank} N' = 1$.

Say $r = \operatorname{rank} M$ and let $m_1, \ldots, m_r$ be a basis of M over Ω. Write a generator $n' \in N'$ in the form

$$n' = \sum m_i \otimes g_i, \;\; g_i \in \Gamma_c \;\; .$$

We may assume $g_1 \in \Gamma_c^*$ as Γ_c is a discrete valuation ring and N' is saturated in $M \otimes \Gamma_c$. Thus we may assume $g_1 = 1$. There is a constant $C > 0$ such that for all i

$$v(g_i, m) \leq mC, \;\; \forall m \geq 1 \;\; .$$

Using the discussion in Section 4.1 (especially equation 4.1.1) this implies that g_i can be viewed as a rigid analytic function on the annulus $A : \{t; |p|^\epsilon < |t| < 1\}$ for some small $\epsilon \in \mathbb{Q}_{>0}$. Therefore we can (and we will) view n' as an element of $M \otimes \Gamma(A, \mathcal{O}_A)$. As $A \subset D$ we may write $n' = \sum d_i \otimes h_i$ with $h_i \in \Gamma(A, \mathcal{O}_A)$ and d_i as in Lemma 6.3. (We are using that $M \otimes \Gamma(A, \mathcal{O}_A) = M \otimes \Gamma(D, \mathcal{O}_D) \otimes \Gamma(A, \mathcal{O}_A)$.) It is still true that $n' \Gamma(A, \mathcal{O}_A) \subset M \otimes \Gamma(A, \mathcal{O}_A)$ is a locally direct summand. (Use that $g_1 = 1$.) The fact that $\theta(N') \subset N'$ implies that $\frac{d}{dt} h_i = h h_i$ for some $h \in \Gamma(A, \mathcal{O}_A)$. Intuitively this means that $\frac{d}{dt} \log(h_i) = h$ and it implies that h_i / h_j is a constant (whenever h_j is not zero; the computations are formal). Thus we see that there exist $\lambda_1, \ldots, \lambda_r \in W$ (not all zero) such that $n' = (\lambda_1 d_1 + \cdots + \lambda_r d_r) \otimes f$ for some nonvanishing $f \in \Gamma(A, \mathcal{O}_A)$. We have shown that N' is defined over $\Gamma(D, \mathcal{O}_D)$ as well, as it corresponds to the submodule spanned by $\lambda_1 d_1 + \cdots + \lambda_r d_r$ which is defined over $\Gamma(D, \mathcal{O}_D)$.

More precisely, this means that we have

$$m_1 + m_2 \otimes g_2 + \cdots + m_r \otimes g_r = (m_1 \otimes q_1 + \cdots + m_r \otimes q_r) \otimes f$$

for certain $q_i \in \Gamma(D, \mathcal{O}_D)$ and $f \in \Gamma(A, \mathcal{O}_A)$ as above. (Just write $d_i = \sum m_j \otimes q_{ij}$ with $q_{ij} \in \Gamma(D, \mathcal{O}_D)$ by Lemma 6.3 and put $q_j = \sum \lambda_i q_{ij}$.) We conclude that f is a meromorphic function on D, invertible on A. Hence it has only finitely many poles on D. (The pole-locus of f is a closed analytic subset of some affinoid subdomain of D.) Therefore, we can find a polynomial $P(t) \in W[t]$, $P(t) \notin pW[t]$ such that $P(t)f \in \Gamma(D, \mathcal{O}_D)$. This implies that $P(t)g_i = P(t)fh_i$ ($i \geq 2$) can be viewed as an element of Γ_c and as an element of $\Gamma(D, \mathcal{O}_D)$. However, the elements in $\Gamma(D, \mathcal{O}_D)$ are power series in t with coefficients in $L_0 = W[1/p]$, and the elements of Γ_c are power series in t and t^{-1} with coefficients in W. We conclude that $P(t)g_i \in \Omega$ for all i. Thus the subspace generated by n' over Γ_c (equal to the subspace generated by $P(t)n'$ over Γ_c, since $P(t) \notin pW[t]$) is defined over Ω: we have shown $0 \neq P(t)n' \in (M \otimes 1) \cap N'$. Let N be this intersection, seen as a submodule of M. We clearly have $F(N) \subset N$ and $\theta(N) \subset N$, by the corresponding properties of N'. It is a saturated Ω-submodule, hence it is a sub (F, θ)-module. Also, $N \otimes \Gamma_c \subset N'$ is an inclusion of saturated rank 1 Γ_c modules, so it is an equality. □

6.5 Remark. The proposition holds in the following more general situation: Suppose (M, θ) is a finitely generated torsion free Ω-module with a $\frac{d}{dt}$-derivation θ such that $M \otimes \Gamma(D, \mathcal{O}_D)$ has an horizontal basis. Any θ-invariant subspace $N' \subset M \otimes \Gamma_c$ comes from an Ω-submodule $N \subset M$. The only point in the proof of the proposition where we used the existence of F, was to ensure that the local system on D was trivial, i.e., we used Dwork's trick. □

7 Some crystals over power series rings

We claim that we may "split off" an F-submodule N of an F-module M over Ω if all its slopes are bigger than all the slopes occurring on M/N. This follows from the following proposition using some tensor algebra. We will not use the claim in the sequel.

7.1 Proposition. *Let (M, F) be an F-module over Ω. Assume $N \subset M$ is a rank 1 sub F-module of slope ℓ and assume that all other slopes on M are strictly smaller than ℓ. Then there is a complement for N, i.e., a sub F-module $N' \subset M$ such that $N \oplus N' \to M$ is an isogeny.*

Proof. We may assume that N is a saturated submodule of M. We dualize and we get an homomorphism $M^* \to N^*$ of Ω-modules whose cokernel has finite length. (Since $N_{\mathfrak{p}} \subset M_{\mathfrak{p}}$ is a locally direct summand for all height 1 primes $\mathfrak{p}$ of $\Omega = W[[t]]$.) Let Q be the torsion free, saturated kernel of this map. For a module T over Ω, write $T^{(\sigma)} = T \otimes_{\Omega,\sigma} \Omega$. If T is finitely generated we have $(T^*)^{(\sigma)} \cong (T^{(\sigma)})^*$, as $\sigma : \Omega \to \Omega$ is finite free [11, 3.E]. By definition of F-modules the linear maps $F_{\text{lin}} : M^{(\sigma)} \to M$ and $F_{\text{lin}} : N^{(\sigma)} \to N$ induced by F have an "almost inverse" $p^n F_{\text{lin}}^{-1}$ for some n large enough. Dualizing this, we get a linear map $(M^*)^{(\sigma)} = (M^{(\sigma)})^* \to M^*$ and similar for N^*. Thus M^* and N^* are F-modules in a natural way (up to the choice of n), and so is Q (and Q is a sub F-module of M^*). The slope ℓ^* of N^* is strictly smaller then all other slopes of M^*. (Note that $\ell^* = n - \ell$ and any slope s^* of M^* is of the form $s^* = n - s$ for some slope s of M.)

By Lemma 6.2 we may choose an isogeny $(\Omega, p^{\ell^*}\sigma) \to (N^*, F)$, and scale by a power of p so that the image of $\Omega \to N^*$ is contained in the image of $M^* \to N^*$. Further we choose an isogeny $(Q, F) \to (Q', F)$, with Q' a free module over Ω (see 6.1). We define the F-module M' by the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q & \longrightarrow & M^* & \longrightarrow & N^* & & \\
 & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & Q & \longrightarrow & M'' & \longrightarrow & \Omega & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & Q' & \longrightarrow & M' & \longrightarrow & \Omega & \longrightarrow & 0
\end{array}$$

(We leave it to the reader to verify that the pushout and the pullback give F-modules.) The Ω-module M' is free. Let s_1 be the smallest slope occurring on Q'. By assumption $s_1 > \ell^*$. The extension of isocrystals (the last one having slope ℓ^*)

$$0 \longrightarrow Q' \otimes_\Omega L_2 \longrightarrow M' \otimes_\Omega L_2 \longrightarrow \Omega \otimes_\Omega L_2 \longrightarrow 0$$

is canonically split by the theory of isocrystals over L_2, see 4.5. Thus the extension class of the exact sequence

$$0 \longrightarrow Q' \otimes_\Omega W(K_2) \longrightarrow M' \otimes_\Omega W(K_2) \longrightarrow \Omega \otimes_\Omega W(K_2) \longrightarrow 0$$

is p-power torsion. (The category of isocrystals over L_2 with non-negative slopes is equivalent to the category of F-modules over $W(K_2)$ up to isogeny.) Replacing Ω by $p^m\Omega$ for m sufficiently large, i.e., doing another pullback, we may assume that

$$0 \longrightarrow Q' \longrightarrow M' \longrightarrow \Omega \longrightarrow 0$$

becomes split after tensoring with $W(K_2)$.

By the structure theory over L_2 (and $W(K_2)$) we see that the map

$$F^N : Q' \otimes W(K_2) \to Q' \otimes W(K_2)$$

for N large becomes divisible by $p^{N\ell^*}$, as all slopes on Q' are $\geq s_1 > \ell^*$. (Compare Section 4.5.) The same divisibility holds in $M' \otimes W(K_2) \cong \big(Q' \otimes W(K_2)\big) \oplus \big(\Omega \otimes W(K_2)\big)$. But then the map $F^N : M' \to M'$ is also so divisible: We remark that p divides an element $m \in M'$ if and only if it divides the element $m \otimes 1 \in M' \otimes W(K_2)$. Let us write

$$\psi = p^{-N\ell^*} F^N : M' \to M' \ .$$

It preserves $Q' \subset M'$ and induces σ^N on $\Omega = M'/Q'$.

Let $e \in M'$ be an element mapping to $1 \in \Omega$. Consider the sequence of elements

$$e_a = \psi^a(e) \in M', \ a \geq 1 \ .$$

Of course e_a maps to the element 1 in Ω for all a. Further, if in the decomposition $M' \otimes W(K_2) \cong \big(Q' \otimes W(K_2)\big) \oplus \big(\Omega \otimes W(K_2)\big)$ we have $e = q \oplus 1$, then

$$e_a = p^{-aN\ell^*} F^{aN}(q) \oplus 1 \ .$$

The terms in the first factor $Q' \otimes W(K_2)$ converge to zero p-adically as all slopes of Q' are $\geq s_1 > \ell^*$. So e_a converges p-adically to the element $0 \oplus 1 \in M' \otimes W(K_2)$. The p-adic topology on M' is induced from the p-adic topology on $M' \otimes W(K_2)$, as is clear from the remark on divisibility above, hence e_a converges to an element $e_\infty \in M'$. This element obviously gives the desired splitting of M'; then dualize and "isogenize" back to M, keeping track of things. $\square$

8 Equality of kernels

8.1 Proposition. *The map* $\Gamma_{2,b,c} \otimes_{\Gamma_c} \Gamma \to \Gamma_{2,b}$, $g \otimes f \mapsto gf$ *is injective.*

Proof. Note that we have $\Gamma_{2,b,c} \otimes_{\Gamma_{2,c}} \Gamma_2 \cong \Gamma_{2,b}$. Further the map $\Gamma_{2,c} \to \Gamma_{2,b,c}$ is finite free, hence flat. Thus we reduce to the case $b = 1$.

Write $M = \Gamma_{2,c} \otimes_{\Gamma_c} \Gamma$. We may consider M as a Γ_c or $\Gamma_{2,c}$ or Γ-module. Note that $M \xrightarrow{p} M$ is injective as $\Gamma_{2,c} \xrightarrow{p} \Gamma_{2,c}$ is injective and $\Gamma_c \to \Gamma$ is flat. Hence M injects into

$$(1) \qquad \left(\Gamma_{2,c} \otimes_{\Gamma_c} \Gamma\right)[1/p] \cong \Gamma_{2,c}[1/p] \otimes_{\Gamma_c[1/p]} \Gamma[1/p] \ .$$

Let us write $\mu : M \to \Gamma_2$ for the multiplication map of the lemma.

Assume that $x = \sum_{i=1}^r g_i \otimes f_i \in M$ is a non zero element such that $\mu(x) = \sum_{i=1}^r g_i f_i$ is zero. We may assume r is minimal among all $r \in \mathbb{N}$ occurring in this fashion. We claim the elements $f_1, \ldots, f_r \in \Gamma$ are linearly independent over Γ_c. If not, then one of them may be expressed as a linear combination of the others with coefficients from Γ_c. (Here we use as always that Γ_c is a discrete valuation ring.) Say $f_1 = \sum_{i=2}^r a_i f_i$, $a_i \in \Gamma_c$. Thus

$$x = \sum_{i=1}^r g_i \otimes f_i = g_1 \otimes \left(\sum_{i=2}^r a_i f_i\right) + \sum_{i=2}^r g_i \otimes f_i = \sum_{i=2}^r (a_i g_1 + g_i) \otimes f_i$$

in contradiction with the minimality of r.

After renumbering if necessary, we have $v_p(g_1) \leq v_p(g_i)$, for all i. Then $x' = \sum_{i=1}^r (g_i/g_1) \otimes f_i \in M$ is nonzero, as $g_1 x' = x$ and $x \neq 0$. Further, $\mu(x') = \sum (g_i/g_1) f_i = (1/g_1) \sum g_i f_i = 0$ (this computation takes place in $\Gamma_2[1/p]$). We see that we may assume $g_1 = 1$.

Let $\alpha : \Gamma_2 \to \Gamma_2$ be an injective ring map such that $\alpha|_\gamma = \mathrm{id}_\Gamma$ and $\alpha(\Gamma_{2,c}) \subset \Gamma_{2,c}$. In this case

$$\mu\left(\sum_{i=1}^r \alpha(g_i) \otimes f_i\right) = \sum_{i=1}^r \alpha(g_i) f_i = \alpha\left(\sum_{i=1}^r g_i f_i\right) = 0 \ .$$

Therefore the element $\sum_{i=1}^r g_i \otimes f_i - \sum_{i=1}^r \alpha(g_i) \otimes f_i = \sum_{i=2}^r (g_i - \alpha(g_i)) \otimes f_i$ of M lies in the kernel of μ. Hence it is zero as r was assumed minimal. Since $f_1, f_2, \ldots, f_r$ are linearly independent over Γ_c (with $f_1 = 1$ fixed by α) we get by minimality of r that $g_i = \alpha(g_i)$, $i = 2, \ldots, r$. (Use that $f_2, \ldots, f_r$ are part of a basis of the $\Gamma_c[1/p]$-vector space $\Gamma[1/p]$ and that M injects into the space (1).) By taking $\alpha = W(\tau)$ with $\tau \in \mathcal{G} = \mathrm{Gal}(K_2/K_1)$, we conclude that $g_i \in \Gamma_{1,c}$. (Compare with the proof of Proposition 5.8.)

Note that Γ_1 is the p-adic completion of the ring $\bigcup_n \Gamma[t^{1/p^n}]$. (This can be seen by looking at the mod p^N quotients of both rings.) Thus we can write any element g of Γ_1 *uniquely* in the form

$$g = \sum_{\alpha \in \mathbb{Z}[1/p],\ 1 > \alpha \geq 0} t^\alpha \omega_\alpha \tag{2}$$

with $\omega_\alpha \in \Gamma$. Not all sequences $\{\omega_\alpha\}_\alpha$ occur in this way: the sets $\{\alpha | v_p(\omega_\alpha) \leq C\}$ are finite for all $C > 0$. If this condition holds, then the sum (2) converges in Γ_1. If $g \in \Gamma_{1,c}$, then all $\omega_\alpha \in \Gamma_c$, as is easy to prove using the properties of the function $v_1(-,-)$. We write our $g_i \in \Gamma_{1,c}$ in this manner

$$g_i = \sum_\alpha t^\alpha \omega_{i,\alpha},\ \ \omega_{i,\alpha} \in \Gamma_c \ \ .$$

We conclude that

$$0 = f_1 + \omega_{2,0} f_2 + \cdots + \omega_{r,0} f_r + \sum_{\alpha > 0} t^\alpha \left(\sum_{i=2}^r \omega_{i,\alpha} f_i \right) \ \ .$$

By uniqueness in (2) for $g = 0$, we get $f_1 + \omega_{2,0} f_2 + \cdots + \omega_{r,0} f_r = 0$ in contradiction with the linear independence of the f_i over Γ_c. $\square$

8.2 Corollary. *Assume (M, F) is a nonzero F-module over Γ_c and $\varphi : M \to \Gamma$ is Γ_c-linear and injective such that $\varphi(F(m)) = p^\ell \sigma(\varphi(m))$ for some $\ell \in \mathbb{Z}_{\geq 0}$. The largest slope* (*see Definition* 4.7) *of M is ℓ and it has multiplicity* 1. *In fact $N = \varphi^{-1}(\Gamma_c)$ is a rank* 1 *sub F-module of M having slope ℓ.*

Proof. Consider the composition $\varphi_{2,b,c}$

$$M \otimes_{\Gamma_c} \Gamma_{2,b,c} \xrightarrow{\varphi \otimes \mathrm{id}} \Gamma \otimes_{\Gamma_c} \Gamma_{2,b,c} \xrightarrow{\mu} \Gamma_{2,b} \ \ .$$

It is injective being the composite of two injective maps ($\Gamma_c \to \Gamma_{2,b,c}$ is flat). We take b so divisible that $M \otimes \Gamma_{2,b,c}$ has a slope filtration in the sense of Proposition 5.5 (ii). The result on the largest slope and its multiplicity as a slope of M follows from Corollary 5.7 (ii). By Proposition 5.8 the slope ℓ subspace of $M \otimes \Gamma_{2,b,c}$ is defined over $\Gamma_{1,c}$. Thus there is a saturated sub F-module $N' \subset M \otimes_{\Gamma_c} \Gamma_{1,c}$ of rank 1 and slope ℓ with

$$N' = \varphi_{1,c}^{-1}(\Gamma_{1,c}) \ \ .$$

Here the map $\varphi_{1,c}$ is defined by a composition as $\varphi_{2,b,c}$ above. To prove the corollary it will suffice to find one nonzero element $n \in M$ such that $\varphi(n) \in \Gamma_c$.

Let $m_1, \ldots, m_r$ be a basis of M over Γ_c. Take a generator $n' \in N'$ and write $n' = \sum g_i m_i$, $g_i \in \Gamma_{1,c}$. As in the proof of the previous proposition we may write

$$g_i = \sum_{\alpha \in \mathbb{Z}[1/p],\ 1 > \alpha \geq 0} t^\alpha \omega_{i,\alpha}$$

with $\omega_{i,\alpha} \in \Gamma_c$. If $\varphi(m_i) = f_i \in \Gamma$, then we get

$$\varphi_{1,c}(n') = \sum_\alpha t^\alpha \left(\sum_i \omega_{i,\alpha} f_i \right) \in \Gamma_{1,c} \quad .$$

Hence $\sum_i \omega_{i,\alpha} f_i \in \Gamma_c$ for all α. For some α the element $n = \sum \omega_{i,\alpha}$ $m_i \in M$ will be nonzero and have $\varphi(n) \in \Gamma_c$. $\square$

9 The theorem

9.1 Theorem. *Let (N, F, θ) be an (F, θ)-module over Ω. Let*

$$\varphi : M \longrightarrow \Gamma$$

be an Ω-linear map such that

(i) *for some $\ell \in \mathbb{Z}_{\geq 0}$ we have $\varphi(F(m)) = p^\ell \sigma(\varphi(m))$ for all $m \in M$, and*

(ii) *we have $\varphi(\theta(m)) = \frac{d}{dt} \varphi(m)$ for all $m \in M$.*

Then $\varphi(M) \subset \Omega$.

Proof. Consider the extension φ_c of φ to $M \otimes \Gamma_c$ defined by the composition

$$M \otimes_\Omega \Gamma_c \longrightarrow \Gamma \otimes_\Omega \Gamma_c \longrightarrow \Gamma \quad .$$

It is easy to check that φ_c satisfies the analogues of (i) and (ii). Let $N' = \mathrm{Ker}(\varphi_c) \subset M \otimes_\Omega \Gamma_c$. Clearly, $F(N') \subset N'$ and $\theta(N') \subset N'$ and N' is a saturated submodule of $M \otimes_\Omega \Gamma_c$. Therefore, by Proposition 6.4 we get $N' = N \otimes \Gamma_c$ for some (saturated) sub (F, θ)-module $N \subset M$ of M. It is clear that $N = \mathrm{Ker}(\varphi)$ and replacing M by M/N we may assume that φ_c is injective.

By Corollary 8.2 we conclude that $N' = \varphi_c^{-1}(\Gamma_c)$ is a rank 1 slope ℓ sub F-module of $M \otimes \Gamma_c$ and that all other slopes on M are strictly smaller than ℓ. Clearly, N' is also preserved by θ, hence it is a sub (F,θ)-module. We apply Proposition 6.4 and we get a saturated rank 1 sub F-module $N \subset M$ over Ω with $N \otimes \Gamma_c = N'$. By Lemma 6.2 we have that there is an isogeny $(\Omega, p^\ell\sigma) \to (N,F)$ of F-modules, i.e., a non zero element $n \in N$ with $F(n) = p^\ell n$ such that $N/\Omega n$ is p-power torsion. The elements $g \in \Gamma_c$ (or even $g \in \Gamma$) that satisfy $\sigma(g) = g$ are $g \in W(\mathbb{F}_p) \subset \Omega$. Thus $\varphi(N) \subset \Omega[1/p] \cap \Gamma = \Omega$.

We have seen above that the assumptions of Proposition 7.1 are satisfied for (M,F) and $N \subset M$. The proposition gives us an isogeny

$$N \oplus N' \longrightarrow M \ .$$

The map $N' \to M \to \Gamma$ is zero, since the slopes on N' are all strictly smaller than ℓ (which implies that $N' \otimes \Gamma_{2,b,c} \to \Gamma_{2,b}$ is zero by Corollary 5.7) (iii). This contradicts the injectivity of φ unless $N' = (0)$, so $N \to M$ is an isogeny. Since N is saturated in M we have $N = M$. We have won. □

10 Appendix: proof of Lemma 2.1

The author does not know how to prove Lemma 2.1 (ii) and (iii) without using crystalline Dieudonné module theory. In both cases we can reduce to the case where $R = k[[t]]$ with k algebraically closed (details left to the reader). Hence we may apply the theory of the preceding sections.

Proof of (ii). Let

$$(M(H), F, V, \nabla) \xrightarrow{M(\alpha)} (M(G), F, V, \nabla)$$

be the associated morphism of crystalline Dieudonné modules over $\Omega = W[[t]]$. See e.g. [8, Section 2] for definitions and notations. Say the rank of α_η is a, i.e., that the height of the image of α_η is a. Thus

$$\Lambda^a : \Lambda^a M(H) \longrightarrow \Lambda^a M(G)$$

is not zero. Therefore the horizontal map

$$\Lambda^a M(H) \otimes \mathcal{O}_D \longrightarrow \Lambda^a M(G) \otimes \mathcal{O}_D$$

of $\mathcal{O}_D$ modules with connections is not zero. Hence it cannot vanish at any point, in particular not at $t = 0$. We conclude that the map $\Lambda^a M(H_s) \longrightarrow \Lambda^a M(G_s)$ induced by α_s is not zero. Hence the height of the image of α_s is at least a. Vanishing of the map $\Lambda^{a+1}M(\alpha)$ shows that it is not more than a. The equality of heights has been proved.

Proof of (iii). The kernel of a map of finite free $W[[t]]$-modules is finite free. Consider the map of Dieudonné modules

$$M(H) \longrightarrow M(G)$$

induced by α as above. Let M_1 be the kernel. The operations F, V, ∇ on $M(H)$ and $M(G)$ induce F, V and ∇ on M_1. This gives a Dieudonné module (M_1, F, V, ∇). Similarly the kernel of the dual map

$$M(H)^\wedge = M(H^t) \longrightarrow M(G)^\wedge = M(G^t)$$

gives a Dieudonné module, whose dual we write (M_2, F, V, ∇). Putting everything back together we get a complex of Dieudonné modules

$$(*) \qquad 0 \to M_1 \to M(H) \to M(G) \to M_2 \to 0 \ .$$

Our assumption on α_η implies that the complex $(*)$ becomes exact after taking the tensor product with Γ.

Let us write

$$L = \lambda(M_1) \otimes \lambda(M(G)) \otimes (\lambda(M(H)) \otimes \lambda(M_2))^{\otimes -1} \ ,$$

where $\lambda(-)$ indicates highest exterior power. We note that L is a free rank 1 (F, θ)-module over Ω. By the above $(*)$ gives an element e of $L \otimes \Gamma$ which is horizontal, which satisfies $F(e) = p^\ell e$ for some ℓ and which is a generator of L. By our main theorem $e \in L$. By a classification of rank 1 (F, θ)-modules over Ω (compare Lemma 6.2) we know that $(L, \theta) \cong (\Omega, \frac{\mathrm{d}}{dt})$. Therefore e generates L, and hence $(*)$ is exact. By the equivalence of categories [8, 2.4.4, 2.4.8, 4.1.1] the Dieudonné modules M_1 and M_2 correspond to p-divisible groups over S. These p-divisible groups are the kernel and cokernel of α since $(*)$ is exact. This ends the proof.

References

[1] P. Berthelot, Théorie de Dieudonné sur un anneau de valuation parfait, Ann. Scient. Éc. Nrom. Sup. **13**, 225–268 (1980)

[2] P. Berthelot, W. Messing, Théorie de Dieudonné cristalline I, in: Journées de géométrie algébrique de Rennes I, Astérisque **63**, 17–37 (1979)

[3] P. Berthelot, L. Breen, W. Messing, Théorie de Dieudonné cristalline II, Lecture notes in mathematics, **930**, Springer-Verlag (1982)

[4] P. Berthelot, W. Messing, Théorie de Dieudonné cristalline III, in: The Grothendieck Festschrift I, Progress in Mathematics, **86**, Birkhäuser, 171–247 (1990)

[5] G. Faltings, Some historical notes, Chapter I in: Arithmetic Geometry, G. Cornell, J.H. Silverman (eds.), Springer Verlag 1986

[6] SGA 7, Groupes de monodromie en géométrie algébrique I, Dirigé par A. Grothendieck avec la collaboration de M. Raynaud et D.S. Rim, Lecture notes in mathematics **288**, Springer Verlag (1973)

[7] A.J. de Jong, Finite locally free group schemes in characteristic p and Dieudonné modules, Inventiones Mathematicae, **114**, 89–137 (1993)

[8] A.J. de Jong, Crystalline Dieudonné module theory via formal and rigid geometry, Publications Mathematiques I.H.E.S **82**, 5–96 (1995)

[9] N. Katz, Slope filtrations of F-crystals, in: Journées de géométrie algébrique de Rennes I, Astérisque **63**, 113–164 (1979)

[10] T. Kimura, H. Niitsuma, Regular local rings of characteristic p and p-basis, J. Math. Soc. Japan **32**, 363-371 (1980)

[11] H. Matsumura, Commutative algebra, Mathematics lecture note series, **56**, The Benjamin/Cummings Publishing Company, Inc, 1980

[12] N. Saavedra Rivano, Catégries tannakiennes, Lecture Notes in Mathematics **265**, Springer Verlag (1972)

[13] J. Tate, p-divisible groups, Proceedings of a conference on local fields, Driebergen (1966), Springer-Verlag

[14] J. Tate, Endomorphisms of abelian varieties over finite fields, Inventiones mathematicae **2**, 134–144 (1966)

[15] J.G. Zarhin, Isogenies of abelian varieties over fields of finite characteristics, Math. USSR Sbornik **24**, 451–461 (1974)