

FROBENIUS MODULES AND DE JONG’S THEOREM

KIRAN S. KEDLAYA

ABSTRACT. Let k be an algebraically closed field of characteristic $p > 0$. A theorem of de Jong shows that morphisms of modules over $W(k)[[t]]$ with Frobenius and connection structure descend from the completion of $W(k)((t))$. A careful reading of de Jong’s proof suggests the possibility that an analogous theorem holds for modules with only a Frobenius structure. We show that this analogue holds in one natural formulation, but fails in a stronger formulation in which $W(k)[[t]]$ is replaced by $W(k[[t]])$.

1. Introduction: de Jong’s theorem

In the course of proving the equal characteristic analogue of Tate’s extension theorem for p -divisible groups over local fields, de Jong [dJ] proved a theorem to the effect that morphisms of certain F -crystals descend. Such crystals can be regarded as modules equipped with Frobenius and connection structures, and de Jong’s proof primarily uses the Frobenius structure, as observed in [Ke1] and [MZ]. It thus makes sense to ask whether one can give a version of de Jong’s theorem using only the Frobenius structure. The purpose of this note is to describe one successful generalization of de Jong’s theorem (Theorem 1.2 below), and to present a counterexample against a second, more optimistic generalization (Proposition 6.1). In the process, we give a partial exposition of de Jong’s theorem which we hope may be of some value in its own right.

The successful generalization may have some applications in the theory of p -adic differential equations, and consequently in rigid cohomology. However, it is more likely to be relevant in contexts where Frobenius structures arise on their own, or in conjunction with connections that have “too many singularities”. Two such contexts are: the work of Berger [B] relating p -adic Galois representations to modules with Frobenius and connection (in which any representation corresponds to a Frobenius structure, but the connection has poles which can only be removed if the representation is de Rham-admissible); and the work of André and di Vizio [AdV] on a q -difference analogue of the theory of p -adic differential equations (in which the form of the connection is perturbed but the notion of a Frobenius structure does not change).

Before proceeding further, we recall the statement of de Jong’s theorem [dJ, Theorem 9.1]. Let k be an algebraically closed field of characteristic $p > 0$, and let W denote the ring of (p -typical) Witt vectors over k . Put $\Omega = W[[t]]$, and

Received March 11, 2004.

let Γ be the p -adic completion of $W((t))$; elements of Γ can be written as power series $\sum_{n \in \mathbb{Z}} c_n t^n$ with $c_n \in W$ and $c_n \rightarrow 0$ as $n \rightarrow -\infty$. Fix a power q of p , let $\sigma : W \rightarrow W$ denote the $(\log_p q)$ -th power of the Witt vector Frobenius, and extend σ to a map on Γ sending $\sum c_n t^n$ to $\sum c_n^\sigma t^{nq}$.

An F -crystal over Ω is a finite free Ω -module M equipped with a W -linear connection $\nabla : M \rightarrow M \otimes dt$ (i.e., a map satisfying the Leibniz rule $\nabla(r\mathbf{v}) = r\nabla(\mathbf{v}) + \frac{dr}{dt}\mathbf{v} \otimes dt$ for $r \in \Omega$ and $\mathbf{v} \in M$) and an isogeny $F : \sigma^*M \rightarrow M$ of Ω -modules with connection, called its “Frobenius structure”. (An *isogeny* here means a morphism whose kernel and cokernel are killed by some power of p . One could turn isogenies into isomorphisms by working over $\Omega[\frac{1}{p}]$ instead of Ω , as in [MZ]; we will not do so here.) Then F induces a σ -linear map from M to itself, which we denote by the same letter F .

In this language, de Jong’s theorem is the following. (Strictly speaking, de Jong only addressed the case $q = p$, but the general case follows immediately by a “restriction of scalars” argument, as in [Ke2, Proposition 6.11].)

Theorem 1.1 (de Jong). *Let M be an F -crystal over Ω , and suppose $\mathbf{v} \in M \otimes \Gamma$ satisfies $\nabla \mathbf{v} = 0$ and $F\mathbf{v} = p^\ell \mathbf{v}$ for some integer ℓ . Then $\mathbf{v} \in M$.*

Note that the category of F -crystals contains internal Homs (up to Tate twists), so this implies that morphisms over Γ between F -crystals over Ω are themselves defined over Ω . (It is in this form in which Theorem 1.1 implies the extension theorem for p -divisible groups, by application to the corresponding Dieudonné modules.)

It should be noted that the choice of σ above was a bit artificial, made for convenience in the proof. Define a *Frobenius lift* on Ω to be any ring map $\sigma : \Omega \rightarrow \Omega$ extending the $(\log_p q)$ -th power of the Witt vector Frobenius on W and lifting the q -power map modulo p ; we say σ is *standard* if $t^\sigma = t^q$. Then as described in [Ka, 2.4], the data of an F -crystal M over Ω determines a Frobenius structure $F_\sigma : \sigma^*M \rightarrow M$ for any Frobenius lift σ on Ω , so de Jong’s theorem is equally true for any σ .

In this terminology, the purpose of this note is to explore the possibility of establishing Theorem 1.1 in the presence of a Frobenius structure but not a connection. Our main affirmative result in this direction is the following. Define an F -module over Ω , with respect to the Frobenius lift σ , to be a finitely generated torsion-free Ω -module M equipped with an isogeny $F : \sigma^*M \rightarrow M$ of Ω -modules. (Note that in the absence of a connection, the category of F -modules depends on the choice of σ . Note also that the freeness hypothesis in the theorem is needed for trivial reasons; see Remark 2.4.)

Theorem 1.2. *Let M be a free F -module over Ω with respect to a Frobenius lift σ , and suppose $\mathbf{v} \in M \otimes \Gamma$ satisfies $F\mathbf{v} = p^\ell \mathbf{v}$ for some integer ℓ . Then $\mathbf{v} \in M$.*

Most of the work in proving this theorem goes into an auxiliary result extending [dJ, Proposition 6.4], which may be of interest in its own right. That result is Theorem 3.4, which asserts that given an F -module M over Ω , any submodule

of $M \otimes \Gamma_c$, where Γ_c is the “overconvergent” subring of Γ (see Section 3), is actually defined over Ω .

We conclude this introduction by describing our negative observation. An F -module over Ω gives rise naturally to an F -module over the Witt ring $W(k[[t]])$, so one can ask even more generally whether the analogue of Theorem 1.2 holds for F -modules over $W(k[[t]])$ (namely, whether morphisms descend to this ring from $W(k((t)))$). This analogue turns out to fail; we give a counterexample in Proposition 6.1.

2. Initial observations

In this section, we make some initial observations in connection with Theorem 1.2. These are based on the fact that (as is evident upon reading [dJ] closely) the arguments of [dJ] use the connection data of an F -crystal only in an incidental fashion. For the “standard” Frobenius $t \mapsto t^q$, this was observed in [Ke1, Theorem 6.3.1] and [MZ, Theorem 3] (though both arguments include similar subtle errors; see Remark 5.8). By being more careful, one can also eliminate the dependence on the standard Frobenius (and the erroneous arguments).

To begin with, note that it is not necessary to work with completely general Frobenius lifts. We call a Frobenius lift σ *zero-centered* if t^σ is divisible by t . Then one has the following easy result.

Lemma 2.1. *Every Frobenius lift is conjugate (by an automorphism of Ω reducing to the identity map modulo p) to a zero-centered Frobenius lift.*

Proof. Given the Frobenius lift σ , put $t^\sigma = \sum_{i=0}^{\infty} a_i t^i$. Then the map $\tau : pW \rightarrow pW$ defined by

$$\tau(x) = \left(\sum_{i=0}^{\infty} a_i x^i \right)^{\sigma^{-1}}$$

is a contraction mapping, since

$$|\tau(x) - \tau(y)| \leq \max_{i \geq 0} \{ |a_i| \cdot |y - x| \cdot |(y^i - x^i)/(y - x)| \} < |y - x|.$$

(The latter holds because $|a_i| < 1$ if $i \neq q$, and $|y^q - x^q| < |y - x|$.) Thus τ has a unique fixed point c , and the equation $\tau(c) = c$ means that $t^\sigma - c^\sigma$ is divisible by $t - c$. Thus the conjugation by $t \mapsto t - c$ does the job. \square

In practice one usually wants to work only with F -modules which are free. A simple observation, adapted from [dJ, Lemma 6.1], makes this possible.

Lemma 2.2. *Let M be an F -module over Ω . Then $M' = \text{Hom}_\Omega(\text{Hom}_\Omega(M, \Omega))$ is free and admits a natural F -module structure under which the natural map $M \rightarrow M'$ is an isogeny of F -modules.*

Proof. The freeness of M' follows from the fact that Ω is a regular local ring (of dimension 2), so the dual of any finitely generated Ω -module is free. (Thus $\text{Hom}_\Omega(M, \Omega)$ is free, and thence M' is free.) The natural map $M \rightarrow M'$ is

injective and has finite length cokernel (so in particular is an isogeny). Thus we may choose a positive integer n such that $t^n \mathbf{v}' \in M$ and $p^n \mathbf{v}' \in M$ whenever $\mathbf{v}' \in M'$.

For $\mathbf{v}' \in M'$, we have $(t^\sigma)^n F(p^n \mathbf{v}') = p^n F(t^n \mathbf{v}')$; since M' is free and Ω is factorial, there must exist $\mathbf{w} \in M'$ such that $F(t^n \mathbf{v}') = (t^\sigma)^n \mathbf{w}$ and $F(p^n \mathbf{v}') = p^n \mathbf{w}$. We set $F(\mathbf{v}') = \mathbf{w}$; this map clearly has the desired properties. \square

We need the classification of F -modules of rank 1, following [dJ, Lemma 6.2].

Lemma 2.3. *Let M be an F -module of rank 1 over Ω . Then M is isogenous to Ω equipped with $p^\ell \sigma$ for some nonnegative integer ℓ ; if M is free, then the isogeny can be taken to be an isomorphism.*

Proof. By Lemma 2.2, we may reduce to the case where M is free. Choose a generator \mathbf{v} of M and write $F\mathbf{v} = p^\ell c\mathbf{v}$ for $c \in \Omega$ not divisible by p . Recall that the definition of an F -module requires that F be an isogeny, so that $\Omega/c\Omega$ is annihilated by a power of p . That is only possible if c is a unit in Ω , that is, $c \not\equiv 0 \pmod{t}$.

Since k is algebraically closed, we can find $a \in W^*$ such that $b = a^{-1}ca^\sigma \equiv 1 \pmod{(p, t)}$. Now note that the infinite product $bb^\sigma b^{\sigma^2} \cdots$ converges (p, t) -adically to a limit $u \in \Omega^*$ satisfying $bu^\sigma = u$. If we put $\mathbf{w} = au\mathbf{v}$, we then have $F\mathbf{w} = p^\ell \mathbf{w}$, as desired. \square

Remark 2.4. Note that the freeness hypothesis in the last assertion of Lemma 2.3 is needed, else we could take M to be the ideal (p, t) in Ω equipped with the standard Frobenius lift, which is isogenous to Ω via the natural inclusion but is not isomorphic to Ω . Indeed, this same example shows that the freeness hypothesis is needed in Theorem 1.2, since $\mathbf{v} = 1 \in M \otimes \Gamma \cong \Gamma$ does not lie in M .

To conclude this section, we state a dual form of Theorem 1.2, which is what we will actually prove.

Theorem 2.5. *Let M be an F -module over Ω with respect to a Frobenius lift σ . Suppose $\phi : M \rightarrow \Gamma$ is an Ω -linear map with the property that for some integer $\ell \geq 0$,*

$$\phi(F\mathbf{v}) = p^\ell \phi(\mathbf{v})^\sigma \quad \text{for all } \mathbf{v} \in M.$$

Then $\phi(M) \subseteq \Omega$.

To reduce Theorem 1.2 to Theorem 2.5, take M, \mathbf{v} as in Theorem 1.2 and put $d = \text{rank } M$. Then exterior product with \mathbf{v} induces a map of F -modules from $\wedge^{d-1} M$, viewed as an F -module in the natural fashion, to $(\wedge^d M) \otimes \Gamma$ with its natural F -action multiplied by p^ℓ . Since $\wedge^d M$ has rank 1 over Ω , Lemma 2.3 implies that $\wedge^d M$ is isogenous to Ω with Frobenius given by $p^m \sigma$ for some integer m . Thus \mathbf{v} induces a map $\phi : \wedge^{d-1} M \rightarrow \Gamma$ such that $\phi(F\mathbf{v}) = p^m \phi(\mathbf{v})^\sigma$. Theorem 2.5 implies that $\phi(\wedge^{d-1} M) \subseteq \Omega$, so \mathbf{v} belongs to the double dual of M over Ω . Since M is free, that double dual coincides with M , so $\mathbf{v} \in M$ as desired.

3. Sketch of the proof

The proof of Theorem 2.5 runs parallel to that of [dJ, Theorem 9.1]. In this section, we collect some statements analogous to various statements in [dJ], then describe how they are used to prove Theorem 2.5. It will then remain to establish some of the analogues in our more general setting.

Before proceeding further, we recall some auxiliary rings from [dJ]. To begin with, let Γ_c denote the subring of Γ consisting of series $\sum c_n t^n$ such that $v(c_n) + rn \rightarrow \infty$ as $n \rightarrow -\infty$ for some $r > 0$ depending on the series. (These are sometimes called “overconvergent” elements of Γ .) The discrete valuation ring Γ_c is not complete; it is henselian (see, e.g., [Ke2, Lemma 3.9]), but we won't need this fact. Put $\Gamma_2 = W(k((t))^{\text{alg}})$; we may embed Γ into Γ_2 by first identifying the completion of the direct limit $\Gamma \xrightarrow{\sigma} \Gamma \xrightarrow{\sigma} \dots$ with $W(k((t))^{\text{perf}})$, then using Witt vector functoriality to embed $W(k((t))^{\text{perf}})$ into $W(k((t))^{\text{alg}})$. We then have a subring $\Gamma_{2,c}$ of Γ_2 analogous to Γ_c , consisting of series $\sum p^i [c_i]$ such that $i + rv_t(c_i) \rightarrow \infty$ as $i \rightarrow \infty$ for some $r > 0$. (Here v_t is the t -adic valuation on $k((t))^{\text{alg}}$ and brackets denote Teichmüller lifts.) Note that $\Gamma \cap \Gamma_{2,c} = \Gamma_c$. (In the notation of [Ke2], the rings $\Gamma_c, \Gamma_2, \Gamma_{2,c}$ would be denoted $\Gamma_{\text{con}}, \Gamma^{\text{alg}}, \Gamma_{\text{con}}^{\text{alg}}$, respectively.) For R one of the aforementioned rings, or indeed any ring equipped with an endomorphism σ , we define an F -module over R , with respect to σ , as a finite torsion-free R -module M equipped with an isogeny $F : \sigma^* M \rightarrow M$.

To describe a key result of [dJ, Section 5] we will use, we must recall the notion of slopes and the Dieudonné-Manin classification of F -modules over R , for R a complete discrete valuation ring of mixed characteristics $(0, p)$ with algebraically closed residue field [Ma], [Ka]. Namely, for any F -module M over R , there exists a positive integer m and an isogeny basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ of M (i.e., a basis of a submodule M' of M with $p^m M \subseteq M'$ for some m) such that $F^m \mathbf{v}_i = p^{\ell_i} \mathbf{v}_i$ for some nonnegative integers ℓ_i . The multiset $\{\ell_1/m, \dots, \ell_n/m\}$ does not depend on any choices; its elements are called the *slopes* of M . For M an F -module over Γ (or Ω or Γ_c), we define slopes by base extension to Γ_2 .

One consequence of [dJ, Corollary 5.7] is the following.

Proposition 3.1. *Let M be an F -module over $\Gamma_{2,c}[p^{1/b}]$ for some positive integer b , and suppose $\phi : M \rightarrow \Gamma_2[p^{1/b}]$ is a $\Gamma_{2,c}[p^{1/b}]$ -linear map such that for some nonnegative integer ℓ , we have $\phi(F\mathbf{v}) = p^{\ell/b} \phi(\mathbf{v})^\sigma$. If ℓ/b is greater than every slope of M , then $\phi = 0$.*

Proof. In case $q = p$ and σ is standard, this is part (iii) of [dJ, Corollary 5.7]. However, the Frobenius on $\Gamma_{2,c}$ or Γ_2 is independent of the initial choice of σ (it is the Witt vector Frobenius), so changing σ does not affect the truth of this result.

The case of q general can be treated by imitating the arguments of [dJ] *mutatis mutandis*. More explicitly, one may replace the invocation of [dJ, Proposition 5.5] in the proof of [dJ, Corollary 5.7] by [Ke2, Proposition 5.11]. This argument remains encumbered by the running hypothesis in [Ke2] that the Frobenius lift σ is a power of a p -power Frobenius lift; however, that assumption is only actually

used starting with [Ke2, Proposition 6.11], so no prior results of [Ke2] actually depend on it. \square

A further consequence is the following result.

Proposition 3.2. *Let M be a nonzero F -module over Γ_c , and suppose $\phi : M \rightarrow \Gamma$ is an injective Γ_c -linear map such that for some nonnegative integer ℓ , $\phi(F\mathbf{v}) = p^\ell \phi(\mathbf{v})^\sigma$ for all $\mathbf{v} \in M$. Then the largest slope of M is equal to ℓ with multiplicity 1, and $\phi^{-1}(\Gamma_c)$ is a rank 1 sub- F -module of M of slope ℓ .*

Proof. This result is [dJ, Corollary 8.2] when the Frobenius lift is standard and $q = p$. It is [Ke3, Lemma 4.2] if the Frobenius lift is a power of a p -power Frobenius lift; however, the argument goes through unchanged without this hypothesis (as in the previous proof). \square

We quote one additional result, namely [dJ, Proposition 7.1], which allows us to split certain exact sequences under a restriction on slopes. The proof of this result for a general Frobenius is the same as for the standard Frobenius (except that [dJ, Lemma 6.1] is replaced by our Lemma 2.2).

Proposition 3.3. *Let M be an F -module over Ω . Suppose that $N \subseteq M$ is a saturated rank 1 sub- F -module of slope ℓ and that the slopes of M/N are all less than ℓ . Then there is a sub- F -module N' of M such that the natural map $N \oplus N' \rightarrow M$ is an isogeny.*

Finally, we state one result which we cannot cite directly from [dJ]; its proof will occupy much of the rest of the paper.

Theorem 3.4. *Let M be an F -module over Ω , and let N_c be a saturated sub- F -module of $M_c = M \otimes \Gamma_c$. Then $N_c = N \otimes \Gamma_c$ for some saturated sub- F -module N of M .*

Remark 3.5. Note that Theorem 3.4 does not hold with Γ_c replaced by Γ , even in the presence of a connection; one obtains a counterexample by considering the middle cohomology of the Legendre family of elliptic curves near a fibre with supersingular reduction, together with its “unit root” sub- F -module.

With these ingredients, we can now give the proof of Theorem 2.5 conditioned on Theorem 3.4.

Proof of Theorem 2.5. We may of course assume that ϕ is injective, and in particular that M is torsion-free. Given ϕ , let ϕ_c be the composite map

$$M_c \xrightarrow{\phi \otimes 1} \Gamma \otimes_\Omega \Gamma_c \xrightarrow{\mu} \Gamma \otimes_{\Gamma_c} \Gamma_c = \Gamma,$$

where μ denotes the multiplication map.

We first proceed assuming that ϕ_c is injective. Put $N_c = \phi_c^{-1}(\Gamma_c)$; then by Proposition 3.2, N_c is a saturated rank 1 sub- F -module of M_c of slope ℓ , and all other slopes of M are strictly less than ℓ . Let N be a saturated sub- F -module of M with $N \otimes \Gamma_c = N_c$ given by Theorem 3.4; then N also has rank 1, so Lemma 2.3

implies that N is isogenous as an F -module to Ω with Frobenius action given by $p^m \sigma$ for some integer m . The slope of the latter is m , so we must have $\ell = m$. Choose $\mathbf{v} \in N$ such that $F\mathbf{v} = p^\ell \mathbf{v}$; then $g = \phi(\mathbf{v})$ satisfies $g^\sigma = g$, so it must belong to a finite unramified extension of \mathbb{Z}_p . Hence $\phi(N) \subseteq \Omega[\frac{1}{p}] \cap \Gamma = \Omega$.

By Proposition 3.3, there is an isogeny $N \oplus N_1 \rightarrow M$ for some saturated sub- F -module N_1 of M . The map $N_1 \rightarrow M \xrightarrow{\phi} \Gamma$ is the composite of injections, so is also injective. On the other hand, the slopes of N_1 are all strictly less than ℓ , so the composite

$$N_1 \otimes_\Omega \Gamma_{2,c}[p^{1/b}] = (N_1 \otimes_\Omega \Gamma_c) \otimes_{\Gamma_c} \Gamma_{2,c}[p^{1/b}] \rightarrow (\Gamma \otimes_{\Gamma_c} \Gamma_{2,c})[p^{1/b}] \xrightarrow{\mu} \Gamma_2[p^{1/b}]$$

is zero by Proposition 3.1.

Since the map $\mu : \Gamma \otimes_{\Gamma_c} \Gamma_{2,c} \rightarrow \Gamma_2$ is injective by [Ke3, Proposition 4.1] (again with the appropriate modifications in case σ is not a power of a p -power Frobenius lift), the map $N_1 \otimes_\Omega \Gamma_c \rightarrow \Gamma$ becomes zero after tensoring over Γ_c with $\Gamma_{2,c}$, and so is itself zero. (Here it matters that $\Gamma_{2,c}$ is flat over Γ_c , which is clear: Γ_c is a principal ideal domain, so a module over Γ_c is flat if and only if it is torsion-free, which $\Gamma_{2,c}$ evidently is.) Since ϕ_c is injective, it follows that $N_1 \otimes_\Omega \Gamma_c = 0$. By Lemma 2.2, there is an isogeny $N_1 \rightarrow N'_1$ with N'_1 free over Ω ; tensoring with Γ_c , we see that $N'_1 \otimes_\Omega \Gamma_c \rightarrow (N'_1/N_1) \otimes_\Omega \Gamma_c$ is a bijection. Since the source of this map is free over Γ_c and the target is killed by a power of p , both must vanish. Thus $N'_1 = 0$; since N_1 is isogenous to N'_1 , it is also zero. In other words, the inclusion $N \subseteq M$ is an isogeny. Since $\phi(N) \subseteq \Omega$, we have $\phi(M) \subseteq \Omega[\frac{1}{p}] \cap \Gamma = \Omega$, as desired.

We now treat the case where ϕ_c is not injective. Put $N'_c = \ker(\phi_c) \subseteq M_c$. Clearly N'_c is a saturated sub- F -module of M_c , so by Theorem 3.4 again, $N'_c = N' \otimes_\Omega \Gamma_c$ for some saturated sub- F -module N' of M . Clearly $N' \subseteq \ker(\phi)$; thus we may apply the previous argument to M/N' to deduce that again $\phi(M) \subseteq \Omega$, as desired. \square

4. Some nonarchimedean function theory: Dwork's trick

As we have just seen, to complete the proof of Theorem 2.5, we must supply Theorem 3.4 to replace [dJ, Proposition 6.4]. This is harder than one might expect; as noted in [MZ], this is perhaps the subtlest aspect of the proof of [dJ, Theorem 9.1].

We begin with a version of the ‘‘Dwork trick’’ [dJ, Lemma 6.3]. Let \mathcal{R}^+ denote the subring of $W[\frac{1}{p}][[t]]$ consisting of series $\sum_{n=0}^{\infty} c_n t^n$ such that for any $r > 0$, $v(c_n) + rn \rightarrow \infty$ as $n \rightarrow \infty$. That is, such series converge for t in the open unit disc in W^{alg} , i.e., are the rigid analytic functions on the open unit disc D . (Correspondingly, this ring is denoted $\Gamma(D, \mathcal{O}_D)$ in [dJ].) For each $r > 0$, the function

$$(4.1) \quad w_r \left(\sum c_i t^i \right) = \min_i \{v(c_i) + ri\}$$

gives a valuation on \mathcal{R}^+ (which induces the supremum norm on the disc of radius p^{-r}). The ring \mathcal{R}^+ is complete for the Fréchet topology generated by the valuations w_r over all $r > 0$, or even any cofinal set of $r > 0$ (e.g., all rational $r > 0$).

The proof of Dwork's trick in [dJ] uses crucially the property of the standard Frobenius that t^σ is divisible by t^2 , so that repeatedly applying σ to t gives terms which converge to zero t -adically. To make the argument work more generally, one must be a bit more careful.

Lemma 4.2. *Suppose that σ is zero-centered. For any $s > 0$ and any $r \in (0, \min\{qs, s+1\}]$, we have*

$$w_s((t^h)^\sigma) \geq rh$$

for all $h > 0$.

Proof. Write $t^\sigma = t^q + pu$, where $u \equiv 0 \pmod{t}$ because σ is zero-centered; then $w_s(pu) \geq 1 + s$, and so

$$w_s((t^h)^\sigma) \geq \min_{0 \leq i \leq h} \{qsi + (s+1)(h-i)\} \geq \min\{qsh, (s+1)h\}.$$

The claim thus follows. \square

Proposition 4.3. *Let M be a free F -module over Ω , with respect to a Frobenius lift σ . Then $M \otimes_\Omega \mathcal{R}^+$ admits a basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ such that $F^m \mathbf{v}_i = p^{\ell_i} \mathbf{v}_i$ for some integers $m > 0$ and $\ell_i \geq 0$.*

The proposition can also be formulated for free F -modules over \mathcal{R}^+ ; the proof goes through unchanged.

Proof. We may assume σ is zero-centered. By the Dieudonné-Manin classification, we can choose a basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of $M \otimes_\Omega \Omega[\frac{1}{p}]$ such that $F^m \mathbf{e}_i \equiv p^{\ell_i} \mathbf{e}_i \pmod{tM}$ for some integers $m > 0$ and $\ell_i \geq 0$. Define the $n \times n$ matrix Φ by

$$F^m \mathbf{e}_j = \sum_i \Phi_{ij} \mathbf{e}_i,$$

let I denote the $n \times n$ identity matrix, and let D be the $n \times n$ diagonal matrix with $D_{ii} = p^{\ell_i}$. Define $c \in pW$ by $t^\sigma \equiv ct \pmod{t^2}$, and choose h_0 large enough so that

$$h_0 v(c) \geq \max_{i,j} \{v(D_{ii}) - v(D_{jj})\}.$$

We first verify that for any integer $h > 0$, there exists an invertible matrix U_h over $W[\frac{1}{p}][[t]]$ with $U_h \equiv I \pmod{t}$ such that $U_h^{-1} \Phi U_h^{\sigma^m} \equiv D \pmod{t^h}$. For $h = 1$, we may take $U_h = I$. Given U_h , put

$$Y_h = U_h^{-1} \Phi U_h^{\sigma^m} D^{-1} - I,$$

and define the matrix X_h over $W[\frac{1}{p}]$ by $Y_h + X_h t^h \equiv 0 \pmod{t^{h+1}}$. Then there exists a matrix V_h over $W[\frac{1}{p}]$ such that

$$(4.4) \quad X_h = c^h D V_h^{\sigma^m} D^{-1} - V_h,$$

since this equation reduces to a separate equation $(X_h)_{ij} = c^h D_{ii}(V_h)_{ij}^{\sigma^m} D_{jj}^{-1} - (V_h)_{ij}$ for each matrix entry $(V_h)_{ij}$, and each of these is solvable when k is algebraically closed. Moreover, the solution is unique when $v(c^h D_{ii} D_{jj}^{-1}) \neq 0$, which is automatic for $h > h_0$. We may thus take $U_{h+1} = U_h(I + V_h t^h)$.

Because U_h modulo t^h determines U_{h+1} modulo t^{h+1} for $h > h_0$, we can take t -adic limits to obtain an invertible matrix U over $W[\frac{1}{p}][[t]]$ such that $U^{-1} \Phi U^{\sigma^m} = D$. We next show that $w_r(U)$ is defined for r sufficiently large. Here we say “ $w_r(x)$ is defined” for $x = \sum c_i t^i \in W[\frac{1}{p}][[t]]$ if the right side of (4.1) is defined, in which case we use (4.1) as the definition. Also, we define w_r of a matrix as the minimum over its entries.

Choose $r_0 > h_0 v(c)$ such that $w_r(Y_{h_0})$ is defined and positive for $r \geq r_0$. (This is possible because by induction on h , $w_r(Y_h)$ is defined for r sufficiently large, depending on h .) Note that if $U_{h+1} = U_h(I + V_h t^h)$ as above, then

$$I + Y_{h+1} = (I + V_h t^h)^{-1} (I + Y_h) (I + D V_h t^h D^{-1})^{\sigma^m}.$$

For $h \geq h_0$, we have $w_r(D_{ii}(t^h)^{\sigma^m} D_{jj}^{-1}) > w_r(t^h)$; also, if $w_r(Y_h)$ is defined, then $w_r(V_h t^h) \geq w_r(X_h t^h) \geq w_r(Y_h)$. Hence if $w_r(Y_h)$ is defined and positive, then $w_r(Y_{h+1}) \geq w_r(Y_h)$; by induction on h , we see that $w_r(Y_h)$ is defined and positive for all $h \geq h_0$. Moreover, we have $w_r(Y_{h+1}) \geq w_r(Y_h)$, with strict inequality when $w_r(Y_h - V_h t^h) > w_r(Y_h)$. The latter happens infinitely often unless the Y_h eventually become all zero, in which case so do the V_h . Hence $w_r(U_h^{-1} U_{h+1} - I) \rightarrow \infty$ as $h \rightarrow \infty$, so that $w_r(U)$ is defined.

From r_0 , define the sequence r_0, r_1, \dots by setting $r_{i+1} = \max\{r_i/q, r_i - 1\}$. By Lemma 4.2, if $w_r(U)$ is defined for $r \geq r_i$, then $w_r(U^{\sigma^m})$ is defined for $r \geq r_{i+m}$. Since $U = \Phi U^{\sigma^m} D^{-1}$, it then follows that $w_r(U)$ is defined for $r \geq r_{i+m}$. Since $w_r(U)$ is defined for $r \geq r_0$, we deduce by induction on i that $w_r(U)$ is defined for $r \geq r_{im}$ for all i . Since $r_{im} \rightarrow 0$ as $i \rightarrow \infty$, it follows that $w_r(U)$ is defined for all $r > 0$; in other words, U has entries in \mathcal{R}^+ .

The same argument as above, applied to the inverse transpose of U , shows that U^{-1} also has entries in \mathcal{R}^+ . We may thus define a basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ of $M \otimes \mathcal{R}^+$ by

$$\mathbf{v}_j = \sum_i U_{ij} \mathbf{e}_i$$

and we will have $F^m \mathbf{v}_i = p^{\ell_i} \mathbf{v}_i$, as desired. \square

Remark 4.5. Note that in the above argument, if D is a scalar matrix, we may take $h_0 = 0$. In particular, in the one-dimensional case, one may deduce that if σ is zero-centered and $u \in \Omega[\frac{1}{p}]$ is congruent to 1 modulo t , then the infinite product $uu^\sigma u^{\sigma^2} \dots$ converges in \mathcal{R}^+ .

5. More nonarchimedean function theory: descent of submodules

We now proceed towards a proof of Theorem 3.4. Even for σ standard, the proof in the absence of a connection is subtle, and the arguments in [Ke1] and [MZ] are inadequate on this point; see Remark 5.8.

By a *principal unit* of Ω , we will mean a unit which, as a series in t , has constant coefficient 1.

Lemma 5.1. *Suppose $a \in \Gamma_c[\frac{1}{p}]$ has the property that the series a and a^{-1} converge for $0 < |t| < 1$. Then $a = ct^nu$ for some $c \in W[\frac{1}{p}]$, some integer n and some principal unit u of Ω .*

Proof. We can choose c, n, u such that $b = a/(ct^nu)$ has the form $1 + \sum_{i=1}^{\infty} b_i t^{-i}$ with $|b_i| < 1$ for all i , as in [Ke2, Proposition 6.5]. It then remains to prove that $b = 1$, given that b converges to nonzero values for $0 < |t| < 1$. Suppose on the contrary that $b \neq 1$. Since b converges for $0 < |t| < 1$, the sequence $\{|b_i|^{1/i}\}_{i=1}^{\infty}$ tends to zero. In particular, there is some i which maximizes $|b_i|^{1/i}$; choose the largest such i and put $\rho = |b_i|^{1/i}$, so that $0 < \rho < 1$. By Weierstrass preparation, b factors as a nonconstant polynomial in t^{-1} whose roots have absolute value ρ^{-1} , times a series in t^{-1} which is invertible on the disc $|t^{-1}| \leq \rho^{-1}$. Thus b vanishes for some t with $0 < |t| < 1$, contradiction. Hence $b = 1$ and $a = ct^nu$, as desired. \square

Let D denote the open unit disc over W , or more precisely, the set of elements of W^{alg} of norm less than 1. Fix a choice of an extension of σ to an automorphism of W^{alg} (which exists by standard Galois theory). Define $a_0, a_1, \dots \in W$ by the formula $t^\sigma = \sum a_i t^i$, and let $\tau : D \rightarrow D$ denote the map

$$\tau(x) = \left(\sum_{i=0}^{\infty} a_i x^i \right)^{\sigma^{-1}},$$

so that if we view $f \in \Omega$ as a function of t , then for $y \in D$,

$$f^\sigma(y) = f(\tau(y))^\sigma.$$

Define the function $\mu : (0, 1) \rightarrow (0, 1)$ by

$$\mu(\eta) = \min_{1 \leq i \leq q} \{(\eta/|a_i|)^{1/i}\}.$$

Then μ is a continuous monotone bijection, so it has an inverse function λ . Since $\mu(\eta) > \eta$, we have $\lambda(\eta) < \eta$ for all η . Moreover, for $\eta \in (0, 1)$ sufficiently close to 1, the term $i = q$ dominates and we have $\mu(\eta) = \eta^{1/q}$.

Lemma 5.2. *Suppose σ is zero-centered. Then for any $x \in D$, if y is an element of D of minimum norm for the property that $\tau(y) = x$, then $\lambda(|y|) = |x|$.*

Proof. Exercise with Newton polygons. \square

Corollary 5.3. *If $a \in \Gamma_c$ and a^σ converges for $\delta < |t| < 1$ for some $\delta > 0$, then a converges for $\lambda(\delta) < |t| < 1$.*

Lemma 5.4. *If $a \in \Gamma_c$ and $f = a^\sigma/a$ is a rational function of t , then a factors as a rational function of t times a unit of Ω .*

Proof. We may suppose σ is zero-centered. We will also allow tensoring over W by an unspecified finite extension of W (which will be necessary in order to factor some polynomials); we will use the same symbols Ω and Γ_c for the resulting rings, and extend σ to these rings via the chosen extension of σ to W^{alg} . Also, write $\text{ord}(m, x)$ for the order of vanishing of an analytic function m at a point x where it is defined.

Suppose the contrary, and choose a counterexample with f of minimal total degree. Then all zeroes and poles of f must lie in D . Write $f = g/h$, where g and h are relatively prime polynomials, so that $a^\sigma h = ag$. Introduce an equivalence relation on D defined by $r \sim r'$ if $\tau(r) = \tau(r')$. Let S_1, \dots, S_n be the equivalence classes containing roots of h . For $i = 1, \dots, n$, let $r_{i1}, \dots, r_{i\ell}$ be the elements of S_i (we should really write ℓ_i for ℓ , because ℓ depends on i , but we will suppress that subscript for notational simplicity). For $j = 1, \dots, \ell$, let c_{ij} and m_{ij} be the multiplicities of r_{ij} as roots of the equations (in x) $\tau(x) = \tau(r_{i1})$ and $h(x) = 0$, respectively; then $c_{ij} > 0$, $m_{ij} \geq 0$, $\sum_{j=1}^{\ell} c_{ij} = q$ (by Weierstrass preparation), and $\max_j \{m_{ij}\} > 0$ (otherwise the class S_i would not have been labeled as such). Put

$$m_i = \max_j \left\{ \left\lceil \frac{m_{ij}}{c_{ij}} \right\rceil \right\}.$$

Let e be the polynomial whose roots are $\tau(r_{i1})$ with multiplicity m_i for $i = 1, \dots, n$. Then e^σ factors by Weierstrass preparation as a unit of Ω times a polynomial whose roots are the r_{ij} , each with multiplicity $c_{ij}m_i$. In particular, h divides the polynomial factor of e^σ .

Choose $\delta > 0$ such that a and a^{-1} converge for $\delta < |t| < 1$. We have

$$(ae)^\sigma = ag(e^\sigma/h),$$

and the right side converges for $\delta < |t| < 1$. Hence ae converges for $\lambda(\delta) < |t| < 1$. Suppose e has a zero s with $\lambda(\delta) < |s| < 1$. Then $s = \tau(r_{ij})$ for some i, j , and we would have $\delta < |r_{ij}| < 1$ for all such j by Lemma 5.2.

Choose i and j such that $s = \tau(r_{ij})$ and $m_i = \lceil m_{ij}/c_{ij} \rceil$, so that in particular $m_{ij} > 0$. Then r_{ij} cannot be a root of g , since g and h are coprime polynomials and r_{ij} is a root of h . Since a and a^{-1} both converge in the region $\delta < |t| < 1$ containing r_{ij} , we have

$$\begin{aligned} \text{ord}((ae)^\sigma, r_{ij}) &= \text{ord}(ag(e^\sigma/h), r_{ij}) \\ &= \text{ord}(e^\sigma/h, r_{ij}) \\ &= m_i c_{ij} - m_{ij} \\ &\in \{0, \dots, c_{ij} - 1\}. \end{aligned}$$

But $\text{ord}((ae)^\sigma, r_{ij})$ is divisible by c_{ij} , so it must be zero. Hence $(ae)^\sigma$ does not vanish at r_{ij} , so ae does not vanish at $\tau(r_{ij})$, and so $(ae)^\sigma$ does not vanish at $r_{ij'}$ for $j' = 1, \dots, \ell$. (Beware that we cannot conclude that a does not vanish at

$\tau(r_{ij})$ because it is not known to converge there!) In particular, e^σ/h does not vanish at $r_{ij'}$ for $j' = 1, \dots, \ell$; hence $m_i c_{ij'} = m_{ij'}$ for $j' = 1, \dots, \ell$.

Now $((t-s)^{m_i})^\sigma$ factors by Weierstrass preparation as a unit of Ω times a polynomial with roots $r_{i1}, \dots, r_{i\ell}$ of respective multiplicities $m_i c_{i1}, \dots, m_i c_{i\ell}$. The latter polynomial is equal to h times a scalar, because we just showed that $m_i c_{ij} = m_{ij}$ for $j = 1, \dots, \ell$. If we now write

$$\frac{g((t-s)^{m_i})^\sigma}{h(t-s)^{m_i}} = \frac{(a(t-s)^{m_i})^\sigma}{a(t-s)^{m_i}},$$

the left side is a unit of Ω times a rational function with total degree strictly smaller than that of f . This yields a smaller counterexample to the original assertion than the one we chose, contradicting that choice. Thus it cannot be that e has a zero s with $\lambda(\delta) < |s| < 1$.

Since ae converges for $\lambda(\delta) < |t| < 1$ and e is a polynomial with no zeroes in $\lambda(\delta) < |t| < \infty$, a must also converge for $\lambda(\delta) < |t| < 1$. By a similar argument, a^{-1} also converges for $\lambda(\delta) < |t| < 1$. But we can now repeat the whole argument with δ replaced by $\lambda(\delta)$, and so on. Since λ is a continuous monotone bijection of $(0, 1)$ onto itself and $\lambda(\eta) < \eta$ for all η , the sequence $\delta, \lambda(\delta), \lambda(\lambda(\delta)), \dots$ must converge to zero. In other words, a and a^{-1} converge for $0 < |t| < 1$. By Lemma 5.1, $a = cut^n$ for some $c \in W[\frac{1}{p}]$, some integer n and some principal unit u of Ω . But then a and f did not form a counterexample to the desired assertion to begin with, contradiction. Thus the claim of the lemma holds, as desired. \square

For our next lemma, we must move to a ring that relates to \mathcal{R}^+ the same way that Γ_c relates to Ω . Namely, let \mathcal{R} denote the ring of formal Laurent series $\sum_{n \in \mathbb{Z}} c_n t^n$ with $c_n \in W[\frac{1}{p}]$, such that $v(c_n) + rn \rightarrow \infty$ as $n \rightarrow -\infty$ for some $r > 0$ and $v(c_n) + sn \rightarrow \infty$ as $n \rightarrow +\infty$ for every $s > 0$. Each element of \mathcal{R} can be viewed as a rigid analytic function on some unspecified open annulus of outer radius 1. The ring \mathcal{R} occurs commonly in the theory of p -adic differential equations, where it is known as the Robba ring; it contains both Γ_c and \mathcal{R}^+ .

Remark 5.5. The conclusion of Lemma 5.4 fails if we allow $a \in \mathcal{R}$; for instance, if $f = (1 + t/p)^{-1}$, we can take a to be the convergent product $\prod_{i=1}^{\infty} (1 + t/p)^{\sigma^i}$.

Lemma 5.6. *If $x, y \in \mathcal{R}$ nonzero satisfy $x^\sigma = gx$ and $y^\sigma = gp^\ell y$ for some $g \in \Gamma_c[\frac{1}{p}]$ and some nonnegative integer ℓ , then $\ell = 0$ and $y/x \in W[\frac{1}{p}]^*$.*

Proof. We may suppose σ is zero-centered. As in [La] or [Ke2], we can factor $x = abb^\sigma b^{\sigma^2} \dots$ for some $a \in \Gamma_c[\frac{1}{p}]$ and some $b \in K[t]$ with constant coefficient 1 having all roots in the open unit disc, as follows. Pick $\delta < 1$ large enough so that $\mu(\eta) = \eta^{1/q}$ for $\eta \in (\delta, 1)$, and take the roots of b to be the zeroes r of x (with multiplicity) for which $\eta < |r| \leq \eta^{1/q}$. Then the roots of b^{σ^i} in D lie in the annulus $\eta^{1/q^i} < |t| \leq \eta^{1/q^{i+1}}$ by Lemma 5.2; hence b^{σ^i} and b^{σ^j} are relatively prime in $\Omega[\frac{1}{p}]$ whenever $i \neq j$. Moreover, the infinite product

$bb^\sigma b^{\sigma^2} \cdots$ converges in \mathcal{R}^+ (see Remark 4.5), x is divisible by the limit (since x is divisible by each factor and the factors are pairwise coprime), and the quotient a is a unit in \mathcal{R} , hence is a nonzero element of $\Gamma_c[\frac{1}{p}]$. Factor $y = cdd^\sigma d^{\sigma^2} \cdots$ analogously.

Now $g = a^\sigma/(ab)$ and $gp^\ell = c^\sigma/(cd)$, so we have an equality

$$p^\ell \frac{(a/c)^\sigma}{a/c} = b/d$$

within $\Gamma_c[\frac{1}{p}]$. By Lemma 5.4, a/c is a rational function of t times a unit of Ω . Write $a/c = hu(r/s)$, where $h \in W[\frac{1}{p}]$, u is a principal unit in Ω , and r and s are polynomials in t with constant coefficient 1. We then have the equality

$$(5.7) \quad bs^\sigma r = p^\ell (dr^\sigma s) \frac{(hu)^\sigma}{hu}$$

in $\Omega[\frac{1}{p}]$; since $bs^\sigma r$ and $dr^\sigma s$ have constant coefficient 1, so does $p^\ell(hu)^\sigma/(hu)$. In other words, $p^\ell h^\sigma = h$, which implies that $\ell = 0$.

From (5.7), we have

$$\prod_{i=0}^{n-1} (bs^\sigma r u)^{\sigma^i} = \prod_{i=0}^{n-1} (dr^\sigma s u^\sigma)^{\sigma^i},$$

which upon cancellation yields

$$us^{\sigma^n} r \prod_{i=0}^{n-1} b^{\sigma^i} = u^{\sigma^n} r^{\sigma^n} s \prod_{i=0}^{n-1} d^{\sigma^i};$$

taking limits (thanks to Remark 4.5 again) yields

$$ur(x/a) = s(y/c).$$

That is, $y/x = (cur)/(as) = 1/h$, as desired. \square

Remark 5.8. The errors in [Ke1] and [MZ] referred to earlier lie in their analogues of Lemma 5.6. In [Ke1, Lemma 3.2.4], it is argued that for $x, y \in \mathcal{R}$, $(x/y)^\sigma = c(x/y)$ implies $x/y \in W$ by noting that this would be true if x/y were a formal Laurent series. However, there is no natural way to perform this division in a fashion compatible with the action of σ . In [MZ, Lemma 32], there is an attempt to rectify this by clarifying that the division x/y takes place in the ring R_r of series $\sum c_n t^n$ with $v(c_n) + rn \rightarrow \infty$ as $n \rightarrow \pm\infty$ for some particular value of r . The subtlety here is that the key equation $x^\sigma/y^\sigma = (x/y)^\sigma$ only holds when the division on the left is performed in R_r and the division on the right is performed in $R_{r/q}$. Thus knowing that $y^\sigma/y = x^\sigma/x$ does not imply that $(x/y)^\sigma = (x/y)$ in any meaningful sense: the symbols x/y on the left and right side are computed in different ways, so represent different formal Laurent series.

With Lemma 5.6 in hand, we can now establish Theorem 3.4, which will complete the proof of Theorem 2.5.

Proof of Theorem 3.4. We begin with some reductions as in [dJ, Proposition 6.4]. We first reduce to the case of M free. By Lemma 2.2, there is an isogeny $\psi : M \rightarrow M'$ with M' free as an Ω -module. Let $\psi_c : M_c \rightarrow M'_c = M' \otimes \Gamma_c$ be the induced map, and let N'_c be the saturation of $\psi_c(N_c)$ in M'_c . If Theorem 3.4 is already known for free modules, then $N'_c = N' \otimes \Gamma_c$ for some saturated sub- F -module N' of M' . Let N be the saturation of $\psi^{-1}(N')$; then $N \otimes \Gamma_c = N_c$, as desired.

We may thus assume that M is free. We next reduce to the case where N_c has rank 1. Suppose instead that $\text{rank } N_c = d > 1$. If the rank 1 case is already known, we may apply it to $\wedge^d N_c \subseteq \wedge^d M_c = (\wedge^d M) \otimes \Gamma_c$ to obtain a saturated sub- F -module N_1 of $\wedge^d M$ such that $N_1 \otimes \Gamma_c = \wedge^d N_c$. Let K be the p -adic valuation subring of $\text{Frac } \Omega$. The set of $\mathbf{v} \in M_c$ such that $\mathbf{v} \wedge \mathbf{w} = 0$ for any $\mathbf{w} \in N_1$ is exactly N_c ; this set is defined by linear conditions, so the set of $\mathbf{v} \in M \otimes K$ such that $\mathbf{v} \wedge \mathbf{w} = 0$ for any $\mathbf{w} \in N_1$ spans N_c over Γ_c . In particular, if we let N denote the set of $\mathbf{v} \in M$ such that $\mathbf{v} \wedge \mathbf{w} = 0$ for any $\mathbf{w} \in N_1$, then N is a saturated sub- F -module of M which spans N_c over Γ_c . Hence $N \otimes \Gamma_c = N_c$, as desired.

We may thus reduce to the case where M is free and N_c has rank 1. By Proposition 4.3, we can find a basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ of $M \otimes \mathcal{R}^+$ such that $F^m \mathbf{v}_i = p^{\ell_i} \mathbf{v}_i$ for some integers $m > 0$ and $\ell_i \geq 0$. Choose a generator \mathbf{w} of N_c ; in $M \otimes \mathcal{R}$, we then have the equality $\mathbf{w} = \sum_i h_i \mathbf{v}_i$ for some $h_i \in \mathcal{R}$. Assume without loss of generality that $h_1 \neq 0$. Then $F^m \mathbf{w} = g \mathbf{w}$ for some nonzero $g \in \Gamma_c$, which implies

$$\begin{aligned} g \mathbf{w} &= F^m \mathbf{w} \\ &= \sum_i F^m (h_i \mathbf{v}_i) \\ &= \sum_i h_i^{\sigma^m} p^{\ell_i} \mathbf{v}_i. \end{aligned}$$

That is, $h_i^{\sigma^m} = gp^{-\ell_i} h_i$ for each i . By Lemma 5.6 applied to $x = h_i$ and $y = h_1$, we see that if $h_i \neq 0$, then $\ell_1 = \ell_i$ and $h_i/h_1 \in W[\frac{1}{p}]^*$. In particular, each h_i is divisible by h_1 ; on the other hand, the h_i generate the unit ideal since \mathbf{w} is part of a basis of $M \otimes \mathcal{R}$. (That is because \mathbf{w} is already part of a basis of M_c , which is true because \mathbf{w} generates a saturated submodule of M_c and Γ_c is a principal ideal domain.) Hence h_1 is a unit in \mathcal{R} , that is, $h_1 \in \Gamma_c[\frac{1}{p}]$.

Now set $\mathbf{v} = (p^r/h_1) \mathbf{w} = \sum_i p^r (h_i/h_1) \mathbf{v}_i$, where r is the smallest integer for which the quantity on the right lies in M_c (rather than $M \otimes \Gamma_c[\frac{1}{p}]$). Then $F^m \mathbf{v}$ is a multiple of \mathbf{v} , but by comparing the coefficients of \mathbf{v}_1 in \mathbf{v} and $F^m \mathbf{v}$, we see that in fact $F^m \mathbf{v} = p^{\ell_1} \mathbf{v}$. Thus \mathbf{v} is in the W -span of the \mathbf{v}_i , and so belongs to $M \otimes_{\Omega} (\mathcal{R}^+ \cap \Gamma_c) = M \otimes_{\Omega} \Omega = M$. Let N be the Ω -span of \mathbf{v} in M ; then N is saturated and $N_c = N \otimes \Gamma_c$, as desired. \square

We conclude this section with two examples illustrating subtleties in the above arguments. First, observe that for σ standard and n an integer, the equation

$x^\sigma = p^n x$ has a solution $x \in \mathcal{R}$ if and only if $n = 0$. However, consider the Frobenius lift σ defined by

$$t^\sigma = (t + 1)^p - 1,$$

which arises naturally in the theory of (ϕ, Γ) -modules (see for instance [B]). Then

$$x = \log(1 + t) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} t^n}{n}$$

clearly belongs to \mathcal{R}^+ and $x^\sigma = px$. In particular, the non-uniqueness visible in the proof of Proposition 4.3 (in the choices of the V_h for $h < h_0$) is more than just an artifact of the proof technique; the matrix U therein really may fail to be unique.

Second, note that even for σ standard, so that $x^\sigma = p^\ell x$ has no solutions with $x \in \mathcal{R}$ when $\ell \neq 0$, it is still possible to have $x^\sigma = gx$ for $x \in \mathcal{R}$ and $g \in \Gamma_c$ of nonzero valuation. For instance, if $x = bb^\sigma b^{\sigma^2} \cdots$ with $b = (1 + t/p)$, then $x^\sigma = gx$ for

$$g = (1 + t/p)^{-1} = p/t(1 + p/t)^{-1} = \sum_{i=0}^{\infty} (-1)^i (p/t)^{i+1}.$$

6. A Witt vector counterexample

Instead of considering F -modules, which depend on the choice of a Frobenius lift, one might prefer to consider modules over a ring that lifts $k[[t]]$ and comes equipped with a *canonical* Frobenius. In crystalline cohomology, this point of view leads to the de Rham-Witt complex introduced by Deligne-Illusie [I]. One has an analogous construction in our context: given an F -crystal over Ω , one obtains by base extension a finite free $W(k[[t]])$ -module M equipped with an isogeny $F : \sigma^* M \rightarrow M$, where σ here denotes the Witt vector Frobenius, and the isogeny property means there exists an additive map $V : M \rightarrow \sigma^* M$ such that $F \circ V = V \circ F$ is multiplication by some power of p .

From the F -crystal structure, one can also obtain a “de Rham-Witt connection” that maps M to the tensor product of M with a suitable quotient of the module of Kähler differentials of $W(k[[t]])$, on which the Frobenius and Verschiebung operators of the Witt ring act. One can use this extra data to give an equivalent formulation of de Jong’s theorem that does not require an auxiliary choice of Frobenius lift; we will not work this out here (but compare the construction of Gauss-Manin connections in the de Rham-Witt context given by Langer and Zink in [LZ]).

However, as in the introduction, one can find situations in this context in which a Frobenius structure naturally arises by itself, e.g., in Zink’s theory of displays of p -divisible groups [Z]. One can then ask whether one has an analogue of Theorem 1.2 to the effect that given a free F -module M over $W(k((t)))$ and an element $\mathbf{v} \in M \otimes W(k((t)))$ such that $F\mathbf{v} = p^\ell \mathbf{v}$ for some integer ℓ , it follows that $\mathbf{v} \in M$. This would in fact generalize Theorem 1.2 if it were true; however, we can exhibit a counterexample as follows.

Proposition 6.1. *There exists a free $W(k[[t]])$ -module M of rank 2, an isogeny $F : \sigma^* M \rightarrow M$ and an element \mathbf{v} of $(M \otimes W(k((t)))) \setminus M$ such that $F\mathbf{v} = \mathbf{v}$.*

Proof. Put $R = W(k[[t]])$ for brevity, let brackets denote Teichmüller lifts, and let V denote the Verschiebung map on R . We first define sequences $\{x_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ over R satisfying

$$\begin{aligned} b_n &\equiv [t] \pmod{R^V}, \\ x_n &\equiv [t]^{p^2-p} \pmod{pR}, \\ -b_n^{\sigma^2} + x_n b_n^\sigma - p^2 b_n &\equiv 0 \pmod{p^2 R^{V^n}}, \end{aligned}$$

as follows. Begin by setting $x_0 = [t]^{p^2-p}$ and $b_0 = [t]$. Given x_n and b_n , define $\Delta_n \in R$ by the equation $p^2 \Delta_n^{V^n} = -b_n^{\sigma^2} + x_n b_n^\sigma - p^2 b_n$, and set

$$b_{n+1} = b_n + \Delta_n^{V^{n+2}}, \quad x_{n+1} = x_n - [t]^{p^2-2p} p \Delta_n^{V^{n+1}}.$$

We then have

$$\begin{aligned} -b_{n+1}^{\sigma^2} + x_{n+1} b_{n+1}^\sigma - p^2 b_{n+1} &\equiv -b_n^{\sigma^2} - \Delta_n^{V^{n+2}\sigma^2} + x_{n+1} b_{n+1}^\sigma - p^2 b_n - p^2 \Delta_n^{V^{n+2}} \\ &\equiv -b_n^{\sigma^2} + x_n b_n^\sigma - p^2 b_n - \Delta_n^{V^{n+2}\sigma^2} + x_{n+1} b_{n+1}^\sigma - x_n b_n^\sigma \\ &\equiv p^2 \Delta_n^{V^n} - p^2 \Delta_n^{V^n} + x_{n+1} b_{n+1}^\sigma - x_n b_n^\sigma \\ &\equiv (x_{n+1} - x_n) b_{n+1}^\sigma + x_n (b_{n+1} - b_n)^\sigma \\ &\equiv -[t]^{p^2-2p} p \Delta_n^{V^{n+1}} b_{n+1}^\sigma + p x_n \Delta_n^{V^{n+1}} \\ &\equiv p \Delta_n^{V^{n+1}} (-[t]^{p^2-2p} b_{n+1}^\sigma + x_n) \\ &\equiv 0 \pmod{p^2 R^{V^{n+1}}}, \end{aligned}$$

the last congruence holding because $[t]^{p^2-2p} b_{n+1}^\sigma \equiv [t]^{p^2-p} \pmod{pR}$ and $x_n \equiv [t]^{p^2-p} \pmod{pR}$.

Note that in the above construction, $x_{n+1} \equiv x_n \pmod{pR^{V^{n+1}}}$ and $b_{n+1} \equiv b_n \pmod{R^{V^{n+2}}}$. Thus the sequences $\{x_n\}$ and $\{b_n\}$ converge in R to limits x and b , respectively, satisfying

$$-b^{\sigma^2} + x b^\sigma = p^2 b.$$

We now define the module M to be the module of rank 2 column vectors over R with the σ -linear map F given by

$$F \begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} 0 & p^2 \\ -1 & x \end{pmatrix} \begin{pmatrix} y^\sigma \\ z^\sigma \end{pmatrix}.$$

By construction, the column vector

$$\mathbf{w} = \begin{pmatrix} b^\sigma \\ b \end{pmatrix}$$

then satisfies $F\mathbf{w} = p^2 \mathbf{w}$.

We next construct a sequence $\{d_n\}_{n=1}^\infty$ of elements of $S = W(k((t))^{\text{sep}})$ such that $d_{n+1} - d_n \in S^{V^n}$ and

$$-p^2 d_n^{\sigma^2} + x d_n^\sigma - d_n \equiv 0 \pmod{S^{V^n}}.$$

To begin, set $d_1 = [t]^{-p}$. Given d_n , define Δ_n by the equation $\Delta_n^{V^n} = -p^2 d_n^{\sigma^2} + x d_n^\sigma - d_n$. Since the polynomial $z^p - z - c$ in z is separable over $k((t))^{\text{sep}}$ for any $c \in k((t))^{\text{sep}}$, we can find $z_n \in S$ such that $z_n^p - z_n + [t]^{p^{n+1}} \Delta_n \equiv 0 \pmod{S^V}$. Now put $d_{n+1} = d_n + [t]^{-p} z_n^{V^n}$; then

$$\begin{aligned} -p^2 d_{n+1}^{\sigma^2} + x d_{n+1}^\sigma - d_{n+1} &\equiv \Delta_n^{V^n} - p^2 ([t]^{-p} z_n^{V^n})^{\sigma^2} + x ([t]^{-p} z_n^{V^n})^\sigma - [t]^{-p} z_n^{V^n} \\ &\equiv \Delta_n^{V^n} + x [t]^{-p^2} z_n^{V^n \sigma} - [t]^{-p} z_n^{V^n} \\ &\equiv \Delta_n^{V^n} + p [t]^{-p} z_n^{V^{n-1}} - [t]^{-p} z_n^{V^n} \\ &\equiv (\Delta_n^V + p [t]^{-p^n} z_n - [t]^{-p^n} z_n^V)^{V^{n-1}} \\ &\equiv (\Delta_n + [t]^{-p^{n+1}} z_n^p - [t]^{-p^{n+1}} z_n)^{V^n} \\ &\equiv 0 \pmod{S^{V^{n+1}}}. \end{aligned}$$

The sequence $\{d_n\}$ converges to a limit $d \in S$ such that

$$-p^2 d^{\sigma^2} + x d^\sigma = d.$$

Moreover, any $D \in S$ such that $-p^2 D^{\sigma^2} + x D^\sigma = D$ must be of the form dr for some $r \in \mathbb{Z}_p$. Namely, it suffices to check that if $D \in S^{V^n}$ satisfies the equation, then $D - rd \in S^{V^{n+1}}$ for some $r \in \mathbb{Z}_p$; but the set of all such D generates a subgroup of $S^{V^n}/S^{V^{n+1}}$ of order p , as do the multiples of $p^n d$.

Now put $e = b^\sigma d - p^2 b d^\sigma \in S$; then

$$\begin{aligned} e^\sigma &= b^{\sigma^2} d^\sigma - p^2 b^\sigma d^{\sigma^2} \\ &= d^\sigma (x b^\sigma - p^2 b) - b^\sigma (x d^\sigma - d) \\ &= b^\sigma d - p^2 b d^\sigma = e, \end{aligned}$$

and so $e \in \mathbb{Z}_p$. Given $\tau \in \text{Gal}(k((t))^{\text{sep}}/k((t)))$, we have a natural action of τ on S commuting with σ , and so $-p^2 d^{\tau\sigma^2} + x d^{\tau\sigma} = d^\tau$. As noted above, this implies that $d^\tau = \chi(\tau)d$ for some $\chi(\tau) \in \mathbb{Z}_p$; in fact, $\chi(\tau) \in \mathbb{Z}_p^*$ since d and d^τ are both nonzero modulo S^V . However,

$$\begin{aligned} e &= e^\tau \\ &= (b^\sigma d - p^2 b d^\sigma)^\tau \\ &= b^\sigma d^\tau - p^2 b d^{\sigma\tau} \\ &= \chi(\tau)(b^\sigma d - p^2 b d^\sigma) \\ &= \chi(\tau)e, \end{aligned}$$

forcing $\chi(\tau) = 1$ for all τ . That is, d actually belongs to the subring of S fixed by $\text{Gal}(k((t))^{\text{sep}}/k((t)))$, which is precisely $W(k((t)))$.

To conclude, note that the column vector

$$\mathbf{v} = \begin{pmatrix} p^2 d^\sigma \\ d \end{pmatrix}$$

of $M \otimes W(k((t)))$ satisfies $F\mathbf{v} = \mathbf{v}$, but it is evident that $\mathbf{v} \notin M$ since $d \equiv [t]^{-p} \pmod{W(k((t)))^V}$. This yields the desired counterexample. \square

We note in concluding that the counterexample constructed above is not quite as magical as it might look. In the language of [Ke2], \mathbf{v} and \mathbf{w} generate the first steps in the descending and ascending slope filtrations; all that was necessary was to adjust M so that \mathbf{v} would come out defined over $W(k[[t]])$, not just over $W(k[[t]]^{\text{alg}})$. Moreover, the “generic” slopes had to be taken more than 1 apart, otherwise M would automatically admit a “de Rham-Witt connection” and de Jong’s theorem would apply; indeed, this is what happens in the case of displays of p -divisible groups, in which the slopes are constrained to lie in $[0, 1]$.

Acknowledgments

Thanks to Thomas Zink for helpful discussions, notably in suggesting the Witt vector generalization and in providing a copy of [MZ]. Thanks also to the Institute for Advanced Study for its hospitality. The author was supported by the National Science Foundation (grant number DMS-0111298).

References

- [AdV] Y. André and L. di Vizio, *q-difference equations and p-adic local monodromy*, to appear in *Astérisque*; preprint available at picard.ups-tlse.fr/~divizio.
- [B] L. Berger, *Représentations p-adiques et équations différentielles*, *Invent. Math.* **148** (2002), 219–284.
- [dJ] A.J. de Jong, *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic*, *Invent. Math.* **134** (1998), 301–333; erratum, *ibid.* **138** (1999), 225.
- [I] L. Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, *Ann. Sci. Éc. Norm. Sup.* **12** (1979), 501–661.
- [Ka] N.M. Katz, *Slope filtrations of F-crystals*, *Astérisque* **63** (1979), 113–163.
- [Ke1] K.S. Kedlaya, *Descent theorems for overconvergent F-crystals*, Ph.D. thesis, Massachusetts Institute of Technology, 2000; available at math.mit.edu/~kedlaya.
- [Ke2] ———, *A p-adic local monodromy theorem*, *Ann. of Math.* **160** (2004), 93–184.
- [Ke3] ———, *Full faithfulness for overconvergent F-isocrystals*, in A. Adolphson et al. (eds.), *Geometric Aspects of Dwork Theory (Volume II)*, de Gruyter (Berlin), 2004, 819–835.
- [LZ] A. Langer and Th. Zink, *De Rham-Witt cohomology for a proper and smooth morphism*, *J. Inst. Math. Jussieu* **3** (2004), 231–314.
- [La] M. Lazard, *Les zéros des fonctions analytiques d’une variable sur un corps valué complet*, *Publ. Math. IHES* **14** (1962), 47–75.
- [Ma] Yu.I. Manin, *The theory of commutative formal groups over fields of positive characteristic*, *Russian Math. Surveys* **18** (1963), 1–83.
- [MZ] W. Messing and Th. Zink, *de Jong’s theorem on homomorphisms of p-divisible groups*, preprint, 2001; available at www.mathematik.uni-bielefeld.de/~zink.
- [Z] Th. Zink, *The display of a formal p-divisible group*, in *Cohomologies p-adiques et applications arithmétiques, I*, *Astérisque* **278** (2002), 127–248.

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVENUE, CAMBRIDGE, MA 02139

E-mail address: kedlaya@math.mit.edu