

Dimensions of group schemes of automorphisms of truncated Barsotti–Tate groups

Ofer Gabber and Adrian Vasiu

December 15, 2011

Abstract. Let D be a p -divisible group over an algebraically closed field k of characteristic $p > 0$. Let $n_D \in \mathbb{N}$ be the smallest number such that D is determined by $D[p^{n_D}]$ within the class of p -divisible groups over k of the same codimension c and dimension d as D . We study n_D , lifts of $D[p^m]$ to truncated Barsotti–Tate groups of level $m + 1$ over k , and the numbers $\gamma_D(i) := \dim(\mathbf{Aut}(D[p^i]))$. We show that $n_D \leq cd$, $(\gamma_D(i+1) - \gamma_D(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} , for $cd > 0$ we have $\gamma_D(1) < \gamma_D(2) < \cdots < \gamma_D(n_D)$, and for $m \in \{1, \dots, n_D - 1\}$ there exists an infinite set of truncated Barsotti–Tate groups of level $m + 1$ which are pairwise non-isomorphic and lift $D[p^m]$. Different generalizations to p -divisible groups with a smooth integral group scheme in the crystalline context are also proved.

KEY WORDS: p -divisible groups, truncated Barsotti–Tate groups, affine group schemes, and group actions.

MSC 2010: 11G10, 11G18, 14F30, 14G35, 14L05, 14L15, 14L30, 20G15.

1 Introduction

Let $p \in \mathbb{N}$ be a prime. Let k be an algebraically closed field of characteristic p . Let $c, d \in \mathbb{N}$ be such that $r := c + d > 0$. Let $m \in \mathbb{N}^*$. By a BT_m over a scheme S we mean a *truncated Barsotti–Tate group* of level m over S which has codimension c and dimension d . In this paper we put forward *principles*

that govern: (i) the classification of BT_m 's over k and (ii) the specializations of BT_m 's over an algebraic closure k_1 of $k((x))$ to BT_m 's over k .

Let D be a p -divisible group over k of codimension c and dimension d . Its height is r . Let n_D be the i -number of D , i.e. the smallest non-negative integer for which the following statement holds: if C is a p -divisible group over k of codimension c and dimension d and such that $C[p^{n_D}]$ is isomorphic to $D[p^{n_D}]$, then C is isomorphic to D . We have $n_D = 0$ if and only if $cd = 0$. For the existence of n_D we refer to [Ma, Ch. III, Sect. 3], [Tr1, Thm. 3], [Tr2, Thm. 1], [Va1, Cor. 1.3], or [Oo2, Cor. 1.7]. One has a first estimate $n_D \leq cd + 1$, cf. [Tr1, Thm. 3]. *Traverso's isomorphism conjecture* predicts that $n_D \leq \min\{c, d\}$, cf. [Tr3, Sect. 40, Conj. 4].

Thus to classify all BT_m 's over k and to decide which BT_m 's over k_1 specialize to which BT_m 's over k , one is led to consider four basic problems.

Problem 1. Determine the set $N_{c,d}$ of possible values of n_D .

Problem 2. For $1 \leq m \leq \max(N_{c,d})$ classify all BT_m 's over k .

Problem 3. Find invariants that go up under specializations of BT_m 's.

Problem 4. Find basic principles that govern *group actions* whose *orbits* parametrize isomorphism classes of BT_m 's over algebraically closed fields.

Significant progress towards the solution of Problem 1 was made in [Va3]. Thus in this paper we will present progress towards the solution of Problems 2 to 4 and will provide basic tools for future extra progress towards the solution of Problem 1 (see already [LNV]). We begin by referring to Problem 3.

1.1 Group schemes of automorphisms

Let B be a BT_m over k . Let $\mathbf{Aut}(B)$ be the group scheme over k of automorphisms of B and let $\gamma_B := \dim(\mathbf{Aut}(B))$. The importance of the numbers γ_B stems out from the following three main facts:

- They are codimensions of versal *level m strata*, cf. [Va2, Thm. 1.2 (c)].
- They can compute the i -numbers n_D (see Theorem 1 below).
- They are a main source of invariants that go up under specializations.

More precisely, we have the following elementary fact:

(a) Let \mathcal{R} be a local domain which is a k -subalgebra of k_1 and has residue field k . If \mathcal{B} is a BT_m over \mathcal{R} that lifts B (i.e. $\mathcal{B}_k = B$), then $\gamma_{\mathcal{B}_{k_1}} \leq \gamma_B$.

Besides γ_B 's, we know only two other invariants that go up under specializations of BT_m 's. Unfortunately, they are defined only for some specific values of m . To describe them, let $j := \lceil \frac{cd}{r} \rceil$. It is known that j is the smallest non-negative integer such that the Newton polygon of each p -divisible group C over k of codimension c and dimension d , is uniquely determined by the isomorphism class of $C[p^j]$ (cf. [NV2, Thm. 1.2]). Thus if $m \geq j$, we can speak about the Newton polygon ν_B of B : it is the Newton polygon of every p -divisible group over k whose associated BT_m is isomorphic to B .

(b) We assume that $m \geq j$. Let \mathcal{R} and \mathcal{B} be as in (a). Then a classical theorem of Grothendieck implies that $\nu_{\mathcal{B}_{k_1}}$ is below ν_B . To check this we can assume that \mathcal{R} is noetherian. There exists a p -divisible group $\widehat{\mathcal{D}}$ over the completion $\widehat{\mathcal{R}}$ of \mathcal{R} such that $\widehat{\mathcal{D}}[p^m] = \mathcal{B}_{\widehat{\mathcal{R}}}$, cf. [Il, Thm. 4.4 e)]. Thus the statement on Newton polygons follows from [Ka, Cor. 2.3.2] applied to the Dieudonné F -crystal of $\widehat{\mathcal{D}}$.

(c) We assume that $m = 1$. Then the set of isomorphism classes of BT_1 's over either k or k_1 is in bijection to the finite quotient set $S_r/(S_c \times S_d)$. Thus one can define naturally an invariant $w_B \in S_r/(S_c \times S_d)$. Moreover there exists a well understood relation of order \leq on $S_r/(S_c \times S_d)$ such that if \mathcal{R} and \mathcal{B} are as in (a), then we have $w_{\mathcal{B}_{k_1}} \leq w_B$. See [We] and [PWZ] for all these facts (see also [Kr], [Oo1], [Mo], [MW], and [Va4]). We emphasize that the invariant w_B is a refinement of the classical invariants of B (like the a -number of B , the p -rank of B , the p -rank of the Cartier dual B^t of B , etc.).

We recall that the a -number a_D of $D[p]$ (or of D) is the greatest non-negative integer such that $\alpha_p^{a_D}$ is a subgroup scheme of $D[p]$. For $i \in \mathbb{N}$ let $\gamma_D(i) := \dim(\mathbf{Aut}(D[p^i]))$; thus $\gamma_D(0) = 0$. We call $(\gamma_D(i))_{i \in \mathbb{N}}$ the *centralizing sequence* of D and we call $s_D := \gamma_D(n_D)$ the *specializing height* of D .

Theorem 1 *The centralizing sequence of D has the following three basic properties:*

(a) *For each $l \in \mathbb{N}$, the sequence $(\gamma_D(i+l) - \gamma_D(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} .*

(b) *If $cd > 0$, then we have $a_D^2 \leq \gamma_D(1) < \gamma_D(2) < \dots < \gamma_D(n_D)$.*

(c) *For $i \geq n_D$ we have $\gamma_D(i) = \gamma_D(n_D) \leq cd$.*

The proof of Theorem 1 (a) relies on properties of the group scheme $\mathbf{End}(D[p^i])$ over k of endomorphisms of $D[p^i]$ presented in Subsection 2.1

(see Subsection 2.2). The proof of Theorem 1 (b) relies on Theorem 1 (a) and on properties of the group actions of Section 3 (see Section 5). If $n_D > 0$ (i.e. if $cd > 0$), then Theorem 1 (c) was proved in [Va2, Thm. 1.2 (d) and Cor. 1.2.1]. The case $n_D = 0$ of Theorem 1 (c) is trivial.

The identity component (resp. the reduced group) of an affine group scheme \sharp over k will be denoted as \sharp^0 (resp. \sharp_{red}). A connected smooth affine group over k is called *unipotent* if \mathbb{G}_m is not a subgroup of it.

The following three consequences of Theorem 1 and its proof are proved in Subsections 5.1 to 5.3 (respectively).

Corollary 1 *We have $n_D \leq cd$. If D is not ordinary, then we have $n_D \leq cd + 1 - a_D^2 \leq cd$.*

Corollary 2 (a) *Let $i, l \in \mathbb{N}^*$ with $i < l$. Then the image of the restriction homomorphism $\mathbf{Aut}(D[p^l]) \rightarrow \mathbf{Aut}(D[p^i])$ (or of $\mathbf{End}(D[p^l]) \rightarrow \mathbf{End}(D[p^i])$) is finite if and only if $l - i \geq n_D$.*

(b) *We assume that D is not ordinary. Let n be the greatest positive integer such that the image of the restriction homomorphism $\mathbf{Aut}(D[p^n]) \rightarrow \mathbf{Aut}(D[p])$ (or of $\mathbf{End}(D[p^n]) \rightarrow \mathbf{End}(D[p])$) has positive dimension. Then we have $n = n_D$.*

(c) *For all $s \in \mathbb{N}^*$ we have $n_{D^s} = n_D$.*

Corollary 3 *Let $i, l \in \mathbb{N}^*$ with $i < l$. Then the following five properties hold:*

(a) *The restriction homomorphism $\mathbf{Aut}(D[p^l])_{\text{red}}^0 \rightarrow \mathbf{Aut}(D[p^i])_{\text{red}}^0$ is trivial if and only if $l - i \geq n_D$.*

(b) *The connected smooth affine group scheme $\mathbf{Aut}(D[p^i])_{\text{red}}^0$ is unipotent.*

(c) *If $i \geq n_D + 1$, then the exponent of the group $\mathbf{Aut}(D[p^i])^0(k)$ is p^{n_D} .*

(d) *If $i \geq 2n_D$, then $\mathbf{Aut}(D[p^i])_{\text{red}}^0$ is commutative.*

(e) *If $i \geq n_D + 1$, then there exist canonical bijections $\mathbf{Aut}(D[p^l])^0(k) \rightarrow \mathbf{Aut}(D[p^i])^0(k)$. If moreover $i \geq 2n_D$, then these bijections are group isomorphisms.*

Corollary 1 refines [Tr1, Thm. 3] (if D is not ordinary, then a_D could be any integer in the interval $[1, \min\{c, d\}]$). See Subsection 5.4 for a refinement of Corollary 1 in terms of Newton polygon slopes of D . Based on the above results and [Va3], in [LNV] it is proved a corrected, refined, and optimal version of Traverso's isomorphism conjecture.

1.2 Applications of group actions

In Section 3 we introduce certain group actions over k whose sets of orbits parametrize isomorphism classes of (truncations of) p -divisible groups over k of codimension c and dimension d . These group actions *encode all the data one could possibly think of* in connection to (truncations of) p -divisible groups over k of codimension c and dimension d (e.g., encode their i -numbers, their group schemes of automorphisms, their specializations, all possible stratifications associated to them, their local deformations, etc.). As in [Tr3, Sects. 26 to 39], [Va2, Sect. 2], and [Va4, Subsect. 4.2.2 and Sect. 5.1], these group actions involve (projective limits of) connected smooth affine groups over k . The idea of using group actions to study isomorphism classes of (truncations of) p -divisible groups over k goes back to Manin (see [Ma, Ch. III, Sect. 3]). But Manin used disjoint unions (indexed by finite sets of isomorphism classes of special p -divisible groups over k) of discrete actions (i.e. of actions involving finite groups). In this paper, we only use group actions in order to prove the below two principles and to apply the first principle to the proofs of Theorem 1 (b) and (c) and of Theorem 4 below.

We call two group schemes over k *radicially isogenous* if their perfectiones are isomorphic group schemes over k (to be compared with [Se, Subsect. 1.2, Def. 1], where the terminology *equivalent* is used). The next two theorems are proved in Subsections 3.3 and 3.5 (respectively) and form progress towards the solution of Problems 2 and 4.

Theorem 2 (Unipotent Principle) *Let c, d, m , and D be as above. Then the set of isomorphism classes of lifts of $D[p^m]$ to BT_{m+1} 's over k is in natural bijection to the set of orbits of a suitable action $\mathcal{T}_{m+1} \times_k \mathcal{V}_{m+1} \rightarrow \mathcal{V}_{m+1}$ over k which has the following three properties:*

- (i) *the group scheme \mathcal{T}_{m+1} over k is smooth, affine, and its identity component is a unipotent group of dimension $r^2 + \gamma_D(m)$;*
- (ii) *the k -scheme \mathcal{V}_{m+1} is an affine space of dimension r^2 ;*
- (iii) *we have a short exact sequence $1 \rightarrow \mathbb{G}_a^{r^2} \rightarrow \mathcal{T}_{m+1} \rightarrow \mathcal{C}_m \rightarrow 1$, where \mathcal{C}_m is a smooth, affine group over k that is radicially isogenous to $\mathbf{Aut}(D[p^m])_{\text{red}}$.*

Theorem 3 (Centralizing Principle) *Let D be as above. Let \mathcal{R} be the normalization of $k[[x]]$ in an algebraic closure k_1 of $k((x))$. Let \mathfrak{D} be a p -divisible group over $\text{Spec } \mathcal{R}$ whose fibre over k is D . We assume that there*

exists a p -divisible group D' over k such that D'_{k_1} is isomorphic to \mathfrak{D}_{k_1} . Then the following two properties hold:

- (a) If there exists $l \in \mathbb{N}^*$ such that $\gamma_{D'}(l) = \gamma_D(l)$, then $D'[p^l]$ is isomorphic to $D[p^l]$; thus for $i \in \{1, \dots, l\}$ we have $\gamma_{D'}(i) = \gamma_D(i)$.
- (b) We have $s_{D'} \leq s_D$. If $s_{D'} = s_D$, then D' is isomorphic to D .

One could phrase the Centralizing Principle as: *centralizing sequences go quasi-strictly up under specializations*. Theorem 3 (b) justifies our terminology specializing height s_D of D . In Section 4 we use the strict inequalities of Theorem 1 (b) and the Unipotent Principle to prove the following theorem.

Theorem 4 *Let B be an arbitrary BT_m over k . Let D be a p -divisible group over k such that $B = D[p^m]$, cf. [Il, Thm. 4.4 e)]. If $m < n_D$, then there exists an infinite set of BT_{m+1} 's over k which are pairwise non-isomorphic and which lift B .*

The case $m = 1$ of Theorem 4 is a stronger form of [Oo3, Thm. B].

1.3 Generalizations

In Section 6 we present different generalizations of Theorem 1 to relative contexts provided by quadruples of the form (M, ϕ, ϑ, G) , where (M, ϕ, ϑ) is the contravariant Dieudonné module of D and where G is a smooth integral closed subgroup scheme of \mathbf{GL}_M subject to a weakening of the two axioms of [Va2, Subsect. 4.1] (the case $G = \mathbf{GL}_M$ corresponds to the above classical context provided by D itself). Three examples of special interest are presented in Section 7. They pertain to group schemes of homomorphisms between BT_m 's, to group schemes of automorphisms of filtered BT_m 's, and to group schemes of automorphisms of BT_m 's equipped with (symmetric) principal quasi-polarizations. The motivation for all these generalizations stems out from applications to level m stratifications of special fibres of good integral models of Shimura varieties of Hodge type in unramified mixed characteristic $(0, p)$ (see [Va2, Sect 4]).

Appendix A contains basic properties of affine group schemes over discrete valuation rings that are needed to present the group actions of Sections 3 and 6. Appendix B presents properties of exponential and logarithmic maps for matrices in p -adic contexts that are required for the mentioned generalizations.

2 Group schemes of endomorphisms

Always $c, d, r, m, D, a_D, \mathbf{Aut}(D[p^i])$, and $\mathbf{End}(D[p^i])$ will be as in Section 1. Let $l, i \in \mathbb{N}$ be such that $l \geq i$. We first list three properties of $\mathbf{End}(D[p^i])$ (see Subsection 2.1) and then we use them to prove Theorem 1 (a) (see Subsection 2.2). A homomorphism between affine group schemes over k is called an epimorphism (resp. a monomorphism) if it is faithfully flat (resp. is a closed embedding).

2.1 Basic properties

As the scheme $\mathbf{Aut}(D[p^i])$ is an open subscheme of $\mathbf{End}(D[p^i])$ and as all connected components of $\mathbf{End}(D[p^i])$ have the same dimension, we get that:

(i) We have $\gamma_D(i) = \dim(\mathbf{End}(D[p^i]))$.

Let $j_{l,i} : D[p^l] \twoheadrightarrow D[p^i]$ be the epimorphism defined by the multiplication by p^{l-i} . Let $i_{i,l} : D[p^i] \hookrightarrow D[p^l]$ be the natural inclusion monomorphism.

We consider the monomorphism

$$\kappa_{i,l} : \mathbf{End}(D[p^i]) \hookrightarrow \mathbf{End}(D[p^l])$$

defined on valued points as follows. If R is a commutative k -algebra, then $\kappa_{i,l}(R)$ maps $f_i \in \mathbf{End}(D[p^i])(R)$ to $i_{i,l,R} \circ f_i \circ j_{l,i,R} \in \mathbf{End}(D[p^l])(R)$. Let

$$r_{l,i} : \mathbf{End}(D[p^l]) \rightarrow \mathbf{End}(D[p^i])$$

be the restriction homomorphism (associated to the monomorphism $i_{i,l} : D[p^i] \hookrightarrow D[p^l]$). Let $f_l \in \mathbf{End}(D[p^l])(R)$. It is easy to see that there exists $f_i \in \mathbf{End}(D[p^i])(R)$ such that $\kappa_{i,l}(R)(f_i) = f_l$ if and only if $\text{Ker}(f_l)$ contains $D[p^{l-i}]_R = \text{Ker}(j_{l,i,R})$ (i.e. if and only if $r_{l,i}(R)(f_l) = 0 \in \mathbf{End}(D[p^{l-i}](R))$). From this we get that:

(ii) We have an exact complex

$$0 \rightarrow \mathbf{End}(D[p^i]) \xrightarrow{\kappa_{i,l}} \mathbf{End}(D[p^l]) \xrightarrow{r_{l,i}} \mathbf{End}(D[p^{l-i}]).$$

From properties (i) and (ii), at the level of dimensions we get that:

(iii) The image $\text{Im}(r_{l,i})$ has dimension $\gamma_D(l) - \gamma_D(i)$.

2.2 Proof of Theorem 1 (a)

Let $i, l \in \mathbb{N}$. As we have $r_{i+1+l,l} = r_{i+l,l} \circ r_{i+1+l,i+l}$, $\mathrm{Im}(r_{i+1+l,l})$ is a subgroup scheme of $\mathrm{Im}(r_{i+l,l})$. Thus we have $\dim(\mathrm{Im}(r_{i+l,l})) \geq \dim(\mathrm{Im}(r_{i+1+l,l}))$. From this and the property 2.1 (iii) we get that the sequence $(\gamma_D(i+l) - \gamma_D(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} . Therefore Theorem 1 (a) holds. \square

3 Isomorphism classes of p -divisible groups as orbits of group actions

We construct group actions over k whose sets of orbits parametrize isomorphism classes of p -divisible groups over k of codimension c and dimension d (see Subsections 3.1 and 3.2 that follow the pattern of [Va2]). Theorem 2 is proved in Subsection 3.3. Subsection 3.4 recalls basic results on group actions over k ; we use them to prove Theorem 3 in Subsection 3.5.

Let $W(k)$ be the ring of Witt vectors with coefficients in k . Let $B(k)$ be the field of fractions of $W(k)$. Let σ be the Frobenius automorphism of k , $W(k)$, and $B(k)$. Let (M, ϕ, ϑ) be the contravariant Dieudonné module of D in the sense of [BBM, Def. 3.1.5], where ϕ and ϑ are the F and V of loc. cit. Thus M is a free $W(k)$ -module of rank r , $\phi : M \rightarrow M$ is a σ -linear endomorphism, $\vartheta : M \rightarrow M$ is a σ^{-1} -linear endomorphism, and we have $\phi \circ \vartheta = \vartheta \circ \phi = p1_M$. We denote also by ϕ the σ -linear automorphism of $\mathrm{End}(M)[\frac{1}{p}]$ which takes $e \in \mathrm{End}(M)[\frac{1}{p}]$ to $\phi(e) := \phi \circ e \circ \phi^{-1} \in \mathrm{End}(M)[\frac{1}{p}]$. We refer to [BBM] for the crystalline contravariant Dieudonné functor \mathbb{D} defined on the category of p -divisible groups over k -schemes.

We recall that $m \in \mathbb{N}^*$. Let $\phi_m, \vartheta_m : M/p^m M \rightarrow M/p^m M$ be the reductions modulo p^m of $\phi, \vartheta : M \rightarrow M$. Let $\mathfrak{h}^{(\sigma^m)}$ be the pull-back (or the tensorization) of \mathfrak{h} with σ^m . Thus $M^{(\sigma)} := W(k) \otimes_{\sigma, W(k)} M$, etc.

3.1 Group schemes

In this subsection we introduce several affine group schemes.

3.1.1 A dilatation

Let \bar{F}^1 be the kernel of ϕ_1 ; it is a k -vector subspace of M/pM of dimension d . Let \mathcal{W} be the normalizer of \bar{F}^1 in $\mathbf{GL}_{M/pM}$. If $cd = 0$, then $\mathcal{W} = \mathbf{GL}_{M/pM}$.

If $cd > 0$, then \mathcal{W} is a maximal parabolic subgroup of $\mathbf{GL}_{M/pM}$. Let $\tilde{\mathcal{H}}$ be the *dilatation* of \mathbf{GL}_M centered on the smooth subgroup \mathcal{W} of $\mathbf{GL}_{M/pM}$ (see Appendix A). Thus $\tilde{\mathcal{H}}$ is a smooth affine group scheme over $\mathrm{Spec} W(k)$ equipped with a homomorphism $\tilde{\mathcal{P}} : \tilde{\mathcal{H}} \rightarrow \mathbf{GL}_M$ that has the following universal property: a morphism $f : S \rightarrow \mathbf{GL}_M$ of flat $\mathrm{Spec} W(k)$ -schemes factors (uniquely) through $\tilde{\mathcal{P}}$ if and only if the morphism $f_k : S_k \rightarrow \mathbf{GL}_{M/pM}$ factors through \mathcal{W} . The generic fibre of $\tilde{\mathcal{P}}$ is an isomorphism of $\mathrm{Spec} B(k)$ -scheme and thus the relative dimension of $\tilde{\mathcal{H}}$ over $\mathrm{Spec} W(k)$ is r^2 . The special fibre $\tilde{\mathcal{H}}_k$ is connected and we can redefine $\tilde{\mathcal{P}}$ as follows (cf. Example 1 of Appendix A for details). We can identify $\tilde{\mathcal{H}}$ with the schematic closure $\mathbf{GL}_{M, \phi^{-1}(M)}$ in $\mathbf{GL}_M \times_{W(k)} \mathbf{GL}_{\phi^{-1}(M)}$ of $\mathbf{GL}_{M[\frac{1}{p}]}$ embedded diagonally in $\mathbf{GL}_M \times_{W(k)} \mathbf{GL}_{\phi^{-1}(M)}$. Under this identification, $\tilde{\mathcal{P}}$ gets identified with the first projection homomorphism $\mathbf{GL}_{M, \phi^{-1}(M)} \rightarrow \mathbf{GL}_M$. The homomorphism $\tilde{\mathcal{H}} \rightarrow \mathbf{GL}_{\phi^{-1}(M)}$ which is the composite of the identification $\tilde{\mathcal{H}} = \mathbf{GL}_{M, \phi^{-1}(M)}$ with the second projection homomorphism $\mathbf{GL}_{M, \phi^{-1}(M)} \rightarrow \mathbf{GL}_{\phi^{-1}(M)}$, is isomorphic to the dilatation of $\mathbf{GL}_{\phi^{-1}(M)}$ centered on the parabolic subgroup of $\mathbf{GL}_{\phi^{-1}(M)/p\phi^{-1}(M)}$ that normalizes the k -vector subspace $M/p\phi^{-1}(M)$ of $\phi^{-1}(M)/p\phi^{-1}(M)$.

For a commutative $W(k)$ -algebra R and for $\tilde{h} \in \tilde{\mathcal{H}}(R)$, let $h := \tilde{\mathcal{P}}(R)(\tilde{h}) \in \mathbf{GL}_M(R)$. For $e \in \mathrm{End}(M)$, $g \in \mathbf{GL}_M(W(k))$, and $\tilde{h} \in \tilde{\mathcal{H}}(W(k))$, let $e[m] \in \mathrm{End}(M/p^m M)$, $g[m] \in \mathbf{GL}_M(W_m(k))$, and $\tilde{h}[m] \in \tilde{\mathcal{H}}(W_m(k))$ be the reductions modulo p^m (here $W_m(k) = W(k)/p^m W(k)$).

Fact 1 *Let $g, g_1 \in \mathbf{GL}_M(W(k))$. Let $g_2 := gg_1\phi(g^{-1}) \in \mathbf{GL}_M(B(k))$ (thus $gg_1\phi = g_2\phi g$). Then we have $g_2 \in \mathbf{GL}_M(W(k))$ if and only if there exists $\tilde{h} \in \tilde{\mathcal{H}}(W(k))$ such that $g = h$.*

Proof: We have $g_2 = gg_1\phi(g^{-1}) \in \mathbf{GL}_M(W(k))$ if and only if g normalizes $\phi^{-1}(M)$ and thus if and only if $g[1]$ normalizes $p\phi^{-1}(M)/pM = \bar{F}^1$. But $g[1]$ normalizes \bar{F}^1 (i.e. we have $g[1] \in \mathcal{W}(k)$) if and only if there exists $\tilde{h} \in \tilde{\mathcal{P}}(W(k))$ such that $g = h$, cf. the above universal property. \square

3.1.2 On $\tilde{\mathcal{H}}^{(\sigma)}$

The group scheme $\tilde{\mathcal{H}}^{(\sigma)}$ is the dilatation of $\mathbf{GL}_{M^{(\sigma)}}$ centered on the subgroup scheme $\mathcal{W}^{(\sigma)}$ of $\mathbf{GL}_{M^{(\sigma)}/pM^{(\sigma)}}$. One can define $\tilde{\mathcal{H}}^{(\sigma)}$ more intrinsically as follows. We identify ϕ and ϑ with $W(k)$ -linear maps $\phi : M^{(\sigma)} \rightarrow M$ and $\vartheta : M \rightarrow M^{(\sigma)}$. Let $\mathbf{Aut}(\phi, \vartheta)$ be the closed subgroup scheme of

$\mathbf{GL}_{M^{(\sigma)}} \times_{W(k)} \mathbf{GL}_M$ that represents the functor of automorphisms of the pair of $W(k)$ -linear maps ϕ and ϑ . If R is a commutative $W(k)$ -algebra, then $\mathbf{Aut}(\phi, \vartheta)(R)$ is the group of those pairs $(\tilde{a}, \tilde{b}) \in \mathbf{GL}_{M^{(\sigma)}}(R) \times \mathbf{GL}_M(R)$ for which we have $\tilde{b} \circ (1_R \otimes \phi) = (1_R \otimes \phi) \circ \tilde{a}$ and $\tilde{a} \circ (1_R \otimes \vartheta) = (1_R \otimes \vartheta) \circ \tilde{b}$.

Under the $W(k)$ -linear isomorphism $M \rightarrow \phi^{-1}(M)^{(\sigma)}$ induced by ϕ^{-1} (here $\phi^{-1}(M)$ is as in Subsection 3.1.1 computed with ϕ viewed as a σ -linear map), the group scheme $\mathbf{Aut}(\phi, \vartheta)$ becomes isomorphic to the group scheme over $\text{Spec } W(k)$ that represents the functor of automorphisms of the pair of

$W(k)$ -linear maps $M^{(\sigma)} \xrightleftharpoons[p]{j^{(\sigma)}} \phi^{-1}(M)^{(\sigma)}$, where $j : M \hookrightarrow \phi^{-1}(M)$ is the inclu-

sion. Thus $\mathbf{Aut}(\phi, \vartheta)$ is isomorphic to the schematic closure $\mathbf{GL}_{M^{(\sigma)}, \phi^{-1}(M)^{(\sigma)}}$ in $\mathbf{GL}_{M^{(\sigma)}} \times_{W(k)} \mathbf{GL}_{\phi^{-1}(M)^{(\sigma)}}$ of $\mathbf{GL}_{M^{(\sigma)}[\frac{1}{p}]}$ embedded diagonally in the product $\mathbf{GL}_{M^{(\sigma)}} \times_{W(k)} \mathbf{GL}_{\phi^{-1}(M)^{(\sigma)}}$, cf. Example 1 of Appendix A. Thus we have natural isomorphisms $\tilde{\mathcal{H}}^{(\sigma)} \rightarrow \mathbf{GL}_{M^{(\sigma)}, \phi^{-1}(M)^{(\sigma)}} \rightarrow \mathbf{Aut}(\phi, \vartheta)$ (cf. Subsubsection 3.1.1 for the first one) and under their composite, the homomorphism $\tilde{\mathcal{P}}^{(\sigma)} : \tilde{\mathcal{H}}^{(\sigma)} \rightarrow \mathbf{GL}_M^{(\sigma)} = \mathbf{GL}_{M^{(\sigma)}}$ gets identified with the first projection homomorphism $\mathbf{Aut}(\phi, \vartheta) \rightarrow \mathbf{GL}_{M^{(\sigma)}}$. The first (resp. second) projection homomorphism $\mathbf{Aut}(\phi, \vartheta) \rightarrow \mathbf{GL}_{M^{(\sigma)}}$ (resp. $\mathbf{Aut}(\phi, \vartheta) \rightarrow \mathbf{GL}_M$) is the dilatation of $\mathbf{GL}_{M^{(\sigma)}}$ centered on the parabolic subgroup $\mathcal{W}^{(\sigma)}$ of $\mathbf{GL}_{M^{(\sigma)}/pM^{(\sigma)}}$ (resp. is the dilatation of \mathbf{GL}_M centered on the parabolic subgroup of $\mathbf{GL}_{M/pM}$ which is the normalizer of the kernel of ϑ_1).

3.1.3 The \mathbb{W}_m functor

Let Aff_k be the category of affine schemes over k . Let Set be the category of sets. Let X be an affine scheme over $\text{Spec } W(k)$ of finite type. Let $\mathbb{W}_m(X) : \text{Aff}_k \rightarrow \text{Set}$ be the contravariant functor that associates to an affine k -scheme $\text{Spec } R$ the set $X(W_m(R))$, where $W_m(R)$ is the ring of Witt vectors of length m with coefficients in R . It is well known that this functor is representable by an affine k -scheme of finite type (cf. [Gre, Sect. 4, Cor. 1, p. 639]) to be also denoted as $\mathbb{W}_m(X)$. We have $\mathbb{W}_m(X)(k) = X(W_m(k))$ as well as a functorial identification $\mathbb{W}_1(X) = X_k$. If $f : Y \rightarrow X$ is a closed embedding, then $\mathbb{W}_m(f) : \mathbb{W}_m(Y) \rightarrow \mathbb{W}_m(X)$ is also a closed embedding (cf. [Gre, Sect. 4, Cor. 2, p. 639]).

We assume that X is smooth over $\text{Spec } W(k)$. If J is an ideal of R of square 0, then the ideal $\text{Ker}(W_m(R) \rightarrow W_m(R/J))$ is of square 0 and therefore the reduction map $X(W_m(R)) \rightarrow X(W_m(R/J))$ is surjective (cf. [BLR, Ch. 2,

Sect. 2.2, Prop. 6]). From this and loc. cit. we get that the affine k -scheme $\mathbb{W}_m(X)$ of finite type is smooth.

We assume that X is a smooth affine group scheme over $\text{Spec } W(k)$. Then $\mathbb{W}_m(X)$ is a smooth affine group over k . The length reduction $W(k)$ -epimorphisms $W_{m+1}(R) \twoheadrightarrow W_m(R)$ define naturally an epimorphism

$$\text{Red}_{m+1,X} : \mathbb{W}_{m+1}(X) \twoheadrightarrow \mathbb{W}_m(X)$$

of affine groups over k . The kernel of $\text{Red}_{m+1,X}$ is the vector group over k defined by the Lie algebra $\text{Lie}(X_k)^{(\sigma^m)}$ and thus it is a unipotent, commutative group isomorphic to $\mathbb{G}_a^{\dim(X_k)}$. Using this and the identification $\mathbb{W}_1(X) = X_k$, by induction on $m \in \mathbb{N}^*$ we get that:

- (i) we have $\dim(\mathbb{W}_m(X)) = m \dim(X_k)$;
- (ii) the group $\mathbb{W}_m(X)$ is connected if and only if X_k is connected.

3.2 The group actions \mathbb{T}

Let $\mathcal{H}_m := \mathbb{W}_m(\tilde{\mathcal{H}})$ and $\mathcal{D}_m := \mathbb{W}_m(\mathbf{GL}_M)$. In this paper we will use only occasionally the fact that \mathcal{D}_m has a natural group structure over k . Thus we will view \mathcal{H}_m as a connected smooth affine group over k of dimension mr^2 and (except in few places) we will view \mathcal{D}_m as a connected smooth affine variety over k of dimension mr^2 , cf. Subsubsection 3.1.3. We have an action

$$\mathbb{T}_m : \mathcal{H}_m \times_k \mathcal{D}_m \rightarrow \mathcal{D}_m$$

defined on k -valued points as follows. If $\tilde{h} \in \tilde{\mathcal{H}}(W(k))$ and $g \in \mathbf{GL}_M(W(k))$, then the product of $\tilde{h}[m] \in \mathcal{H}_m(k) = \tilde{\mathcal{H}}(W_m(k))$ and $g[m] \in \mathcal{D}_m(k) = \mathbf{GL}_M(W_m(k))$ is the element (see Subsubsection 3.1.1 for h)

$$\mathbb{T}_m(\tilde{h}[m], g[m]) := (hg\phi(h^{-1}))[m].$$

This makes sense, cf. Fact 1. We recall that (see [Va2, Lemma 2.2.1]):

Lemma 1 *Let $g_1, g_2 \in \mathbf{GL}_M(W(k))$. Then the points $g_1[m], g_2[m] \in \mathcal{D}_m(k)$ belong to the same orbit of the action \mathbb{T}_m if and only if the Dieudonné modules $(M/p^m M, g_1[m]\phi_m, \vartheta_m g_1[m]^{-1})$ and $(M/p^m M, g_2[m]\phi_m, \vartheta_m g_2[m]^{-1})$ are isomorphic.*

3.2.1 The limit process

Let $\rho_{m+1} := \text{Red}_{m+1, \tilde{\mathcal{H}}}$ and $\tau_{m+1} := \text{Red}_{m+1, \mathbf{GL}_M}$ (see Subsubsection 3.1.3 for notations). Thus $\rho_{m+1} : \mathcal{H}_{m+1} \twoheadrightarrow \mathcal{H}_m$ is the natural reduction epimorphism of affine groups over k and $\tau_{m+1} : \mathcal{D}_{m+1} \twoheadrightarrow \mathcal{D}_m$ is the natural reduction epimorphism of affine (group) varieties over k . The action \mathbb{T}_m is a natural reduction of the action \mathbb{T}_{m+1} . In other words, the following identity holds:

$$\tau_{m+1}(\mathbb{T}_{m+1}(\tilde{h}[m+1], g[m+1])) = \mathbb{T}_m(\tilde{h}[m], g[m]).$$

As ρ_{m+1} and τ_{m+1} are morphisms of affine schemes, the projective limits

$$\mathcal{H}_\infty := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{H}_m \quad \text{and} \quad \mathcal{D}_\infty := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{D}_m$$

in the category of ringed spaces are also projective limits in the category of k -schemes (cf. [Gro, Sect. 8, Rm. 8.2.14]), \mathcal{H}_∞ is an affine group scheme over k , and \mathcal{D}_∞ is an affine (group) scheme over k . We have a limit action

$$\mathbb{T}_\infty : \mathcal{H}_\infty \times_k \mathcal{D}_\infty \rightarrow \mathcal{D}_\infty$$

with the property that for all elements $\tilde{h} \in \mathcal{H}_\infty(k) = \tilde{\mathcal{H}}(W(k))$ and $g \in \mathcal{D}_\infty(k) = \mathbf{GL}_M(W(k))$, the product $\mathbb{T}_\infty(\tilde{h}, g) \in \mathcal{D}_\infty(k)$ is the unique element such that for all $m \in \mathbb{N}^*$ we have $\mathbb{T}_\infty(\tilde{h}, g)[m] = \mathbb{T}_m(\tilde{h}[m], g[m])$; thus we have $\mathbb{T}_\infty(\tilde{h}, g) = hg\phi(h^{-1}) \in \mathcal{D}_\infty(k) = \mathbf{GL}_M(W(k))$.

There exist several equivalent ways to define orbits of the action \mathbb{T}_∞ (see [GV]). To be short, in what follows by an orbit of \mathbb{T}_∞ we mean a reduced, quasi-compact, locally closed subscheme \mathcal{O}'_∞ of \mathcal{D}_∞ which is a natural projective limit $\text{proj.lim.}_{m \rightarrow \infty} \mathcal{O}'_m$ in the category of ringed spaces of orbits \mathcal{O}'_m of \mathbb{T}_m (i.e. classical orbits of k -points) under faithfully flat transition morphisms $\mathcal{O}'_{m+1} \rightarrow \mathcal{O}'_m$ that are induced by τ_{m+1} . As we have surjective transition morphisms between non-empty varieties over k , \mathcal{O}'_∞ has k -valued points.

3.2.2 Notations

Let \mathcal{O}_m be the orbit of $1_M[m] \in \mathcal{D}_m(k)$ under the action \mathbb{T}_m ; it is a locally closed subscheme of \mathcal{D}_m which is integral (as \mathcal{H}_m is connected). Let \mathcal{S}_m be the subgroup scheme of \mathcal{H}_m which is the stabilizer of $1_M[m]$. Let $\mathcal{C}_m := \mathcal{S}_{m, \text{red}}$. We have

$$\dim(\mathcal{S}_m) = \dim(\mathcal{C}_m) = \dim(\mathcal{C}_m^0) = \dim(\mathcal{H}_m) - \dim(\mathcal{O}_m).$$

Let \mathcal{T}_{m+1} be the reduced group of the group subscheme $\rho_{m+1}^{-1}(\mathcal{S}_m)$ (equivalently, $\rho_{m+1}^{-1}(\mathcal{C}_m)$) of \mathcal{H}_{m+1} . We have short exact sequences

$$1 \rightarrow \text{Ker}(\rho_{m+1}) \rightarrow \mathcal{T}_{m+1} \rightarrow \mathcal{C}_m \rightarrow 1 \quad \text{and} \quad 1 \rightarrow \text{Ker}(\rho_{m+1}) \rightarrow \mathcal{T}_{m+1}^0 \rightarrow \mathcal{C}_m^0 \rightarrow 1.$$

Thus $\dim(\mathcal{T}_{m+1}) = \dim(\mathcal{T}_{m+1}^0) = r^2 + \dim(\mathcal{C}_m) = r^2 + \dim(\mathcal{C}_m^0)$.

Let \mathcal{V}_{m+1} be the inverse image of the point $1_M[m] \in \mathcal{O}_m(k) \subset \mathcal{D}_m(k)$ under the epimorphism $\tau_{m+1} : \mathcal{D}_{m+1} \rightarrow \mathcal{D}_m$; it is isomorphic to an affine space over k of dimension r^2 (cf. Subsubsection 3.1.3 applied to \mathbf{GL}_M). Let $\mathbb{O}_{m+1,m,1_M}$ be the set of orbits of the action \mathbb{T}_{m+1} which map to \mathcal{O}_m (i.e. which are contained in $\tau_{m+1}^{-1}(\mathcal{O}_m)$). Let $\mathbb{O}_{m+1,m,1_M[m]}$ be the set of orbits of the natural action of \mathcal{T}_{m+1} on \mathcal{V}_{m+1} . We have the following obvious principle:

Fact 2 *There exists a natural bijection $\mathbb{O}_{m+1,m,1_M} \rightarrow \mathbb{O}_{m+1,m,1_M[m]}$ defined by the rule: the orbit $o \in \mathbb{O}_{m+1,m,1_M}$ is mapped to the element of $\mathbb{O}_{m+1,m,1_M[m]}$ which is the reduced scheme of $o \cap \mathcal{V}_{m+1}$.*

3.2.3 Geometric interpretations of sets of orbits

Lemma 2 (a) *The set of orbits of the action \mathbb{T}_m is in natural bijection to the set of (representatives of) isomorphism classes of BT_m 's over k .*

(b) *The set of orbits $\mathbb{O}_{m+1,m,1_M}$ (or $\mathbb{O}_{m+1,m,1_M[m]}$) is in natural bijection to the set of (representatives of) isomorphism classes of BT_{m+1} 's over k which lift $D[p^m]$.*

(c) *If $m \geq n_D$, then $\mathbb{O}_{m+1,m,1_M}$ (or $\mathbb{O}_{m+1,m,1_M[m]}$) has only one orbit.*

Proof: Let \tilde{B} be a BT_m over k . Let \tilde{D} be a p -divisible group over k which lifts \tilde{B} , cf. [Il, Thm. 4.4 e)]. As \tilde{D} has codimension c and dimension d , its Dieudonné module is isomorphic to $(M, \tilde{g}\phi, \vartheta\tilde{g}^{-1})$ for some element $\tilde{g} \in \mathbf{GL}_M(W(k)) = \mathcal{D}_\infty(k)$. The Dieudonné module of \tilde{B} is isomorphic to $(M/p^m M, \tilde{g}[m]\phi_m, \vartheta_m\tilde{g}[m]^{-1})$. Thus (a) and (b) are implied by Lemma 1 and the classical Dieudonné theory which provides an antiequivalence between the category of BT_m 's over k and the category of Dieudonné modules of BT_m 's over k (see [Fo, pp. 153 and 160], [BBM, Chs. 3 and 4], etc.).

We prove (c). Let B be a BT_{m+1} over k such that $B[p^m] = D[p^m]$. As $m \geq n_D$, each p -divisible group over k that lifts B is isomorphic to D . Thus B is isomorphic to $D[p^{m+1}]$. From this and (b), we get that (c) holds. \square

Corollary 4 (a) *In the situation of the last paragraph of Subsubsection 3.2.1, each projective limit $\mathcal{O}'_\infty := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{O}'_m$ taken in the category of ringed spaces is also a projective limit in the category of k -schemes and it is an integral, quasi-compact, locally closed subscheme of \mathcal{D}_∞ whose k -valued points form one orbit of the action $\mathbb{T}_\infty(k) : \mathcal{H}_\infty(k) \times \mathcal{D}_\infty(k) \rightarrow \mathcal{D}_\infty(k)$ in the category of sets. Thus $\mathcal{O}_\infty := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{O}_m$ is the orbit of \mathbb{T}_∞ that contains 1_M .*

(b) *Two points $g_1, g_2 \in \mathcal{D}_\infty(k) = \mathbf{GL}_M(W(k))$ belong to the same orbit of the action \mathbb{T}_∞ (equivalently $\mathbb{T}_\infty(k)$) if and only if the Dieudonné modules $(M, g_1\phi, \vartheta g_1^{-1})$ and $(M, g_2\phi, \vartheta g_2^{-1})$ are isomorphic. Therefore the set of orbits of \mathbb{T}_∞ is in natural bijection to the set of (representatives of) isomorphism classes of p -divisible groups over k of codimension c and dimension d .*

(c) *If K is an algebraically closed field that contains k , then $n_{D_K} = n_D$.*

Proof: The classical Dieudonné theory also provides an antiequivalence between the category of p -divisible groups over k of codimension c and dimension d and the category of Dieudonné modules over k which are isomorphic to $(M, g\phi, \vartheta g^{-1})$ for some element $g \in \mathbf{GL}_M(W(k))$.

Due to Lemma 2 (c), for $m \geq n_D$ we have $\mathcal{O}_{m+1} = \tau_{m+1}^{-1}(\mathcal{O}_m)$. Thus the morphism $\mathcal{O}_{m+1} \rightarrow \mathcal{O}_m$ induced by τ_{m+1} is affine (as τ_{m+1} is so). Thus \mathcal{O}_∞ is an integral k -scheme. Moreover, \mathcal{O}_∞ is the quasi-compact, locally closed subscheme of \mathcal{D}_∞ which for each $m \geq n_D$ is the inverse image of \mathcal{O}_m under the limit affine morphism $\tau_{\infty, m} : \mathcal{D}_\infty \rightarrow \mathcal{D}_m$. As $1_M \in \mathcal{O}_\infty(k)$ and $\mathcal{O}_\infty = \tau_{\infty, m}^{-1}(\mathcal{O}_m)$ for $m \geq n_D$, $\mathcal{O}_\infty(k)$ is the set of elements $g \in \mathcal{D}_\infty(k) = \mathbf{GL}_M(W(k))$ such that (cf. Lemma 2 (a)) the reduction modulo p^m of $(M, g\phi, \vartheta g^{-1})$ is isomorphic to the Dieudonné module of $D[p^m]$ for some $m \geq n_D$ and thus (cf. the definition of n_D and the classical Dieudonné theory) it is the set of elements $g \in \mathbf{GL}_M(W(k))$ such that there exists an isomorphism $h : (M, \phi, \vartheta) \rightarrow (M, g\phi, \vartheta g^{-1})$, i.e. we have $g = h\phi(h^{-1})$ for some element $h \in \mathbf{GL}_M(W(k))$. From this, Fact 1, and the definition of \mathbb{T}_∞ we get that $\mathcal{O}_\infty(k)$ is the orbit of 1_M under the action $\mathbb{T}_\infty(k)$.

As n_D admits upper bounds that depend only on c and d (cf. beginning of Section 1), there exists a p -divisible group D' over k such that for each $m \in \mathbb{N}^*$ the orbit \mathcal{O}'_m corresponds to the isomorphism class of $D'[p^m]$ via the bijection of Lemma 2 (a). Thus as above we argue that \mathcal{O}'_∞ is an integral, quasi-compact, locally closed subscheme of \mathcal{D}_∞ whose k -valued points form one orbit of the action $\mathbb{T}_\infty(k)$.

Part (b) follows from (the proof of) (a) and the classical Dieudonné theory.

To prove (c), we first remark that the action $\mathbb{T}_{m,K}$ is the analogue of the action \mathbb{T}_m but working with D_K instead of D . From Lemma 2 (b) and the very definition of n_D we get that: (i) we have $n_D = 0$ if and only if for each $m \in \mathbb{N}^*$ the action \mathbb{T}_m has only one orbit, and (ii) for $n \in \mathbb{N}^*$, we have $n \geq n_D$ if and only if for all $m \geq n$ the set of orbits $\mathbb{O}_{m+1,m,1_M}$ has only one element. From the last two sentences we get that for $n \in \mathbb{N}$ we have $n \geq n_D$ if and only if $n \geq n_{D_K}$. Thus $n_D = n_{D_K}$, i.e. (c) holds. \square

The following result is a version of [Va2, Thm. 2.4].

Theorem 5 *Let $m \in \mathbb{N}^*$. Let $\mathbf{Aut}(D[p^m])_{\text{crys}}$ be the group scheme over k of automorphisms of $(M/p^m M, \phi_m, \vartheta_m)$. With the notations of Subsubsection 3.2.2, the following four properties hold:*

- (a) *the connected smooth affine group \mathcal{C}_m^0 is unipotent;*
- (b) *there exist two finite homomorphisms*

$$\iota_m : \mathcal{S}_m \twoheadrightarrow \mathbf{Aut}(D[p^m])_{\text{crys}} \quad \text{and} \quad \zeta_m : \mathbf{Aut}(D[p^m]) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}$$

which at the level of k -valued points induce isomorphisms $\iota_m(k) : \mathcal{S}_m(k) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}(k)$ and $\zeta_m(k) : \mathbf{Aut}(D[p^m])(k) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}(k)$;

- (c) *we have $\dim(\mathcal{S}_m) = \dim(\mathcal{C}_m) = \dim(\mathcal{C}_m^0) = \gamma_D(m)$;*
- (d) *the connected smooth affine group \mathcal{T}_{m+1}^0 is unipotent and has dimension $r^2 + \gamma_D(m)$.*

Proof: Parts (a) to (c) are proved in [Va2, Thm. 2.4] using reduced groups. We will only recall here the definitions of ζ_m and ι_m . We will view \mathcal{D}_m as a connected smooth affine group over k . If R is a commutative k -algebra and if σ_R is the Frobenius endomorphism of the ring $W_m(R)$ of Witt vectors of length m with coefficients in R , then $\mathbf{Aut}(D[p^m])_{\text{crys}}(R)$ is the subgroup of $\mathcal{D}_m(R) = \mathbf{GL}_M(W_m(R))$ formed by elements that commute with $1_{W_m(R)} \otimes \phi_m$ and $1_{W_m(R)} \otimes \vartheta_m$; here ϕ_m and ϑ_m are viewed as $W_m(k)$ -linear maps $(M/p^m M)^{(\sigma)} \rightarrow M/p^m M$ and $M/p^m M \rightarrow (M/p^m M)^{(\sigma)}$ (respectively).

The crystalline Dieudonné theory provides us with a homomorphism

$$\zeta_m : \mathbf{Aut}(D[p^m]) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}$$

that maps a point $x \in \mathbf{Aut}(D[p^m])(R)$ to the inverse of the element of $\mathbf{Aut}(D[p^m])_{\text{crys}}(R)$ which is the evaluation of $\mathbb{D}(x)$ at the thickening $\text{Spec } R \hookrightarrow$

$\text{Spec } W_m(R)$ defined by the natural divided power structure on the kernel of the epimorphism $W_m(R) \twoheadrightarrow R$.

The homomorphism $\tilde{\mathcal{P}} : \tilde{\mathcal{H}} \rightarrow \mathbf{GL}_M$ provides us with a homomorphism

$$\iota_m : \mathcal{S}_m \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}$$

that maps a point $\tilde{h}_R[m] \in \mathcal{S}_m(R) \subset \mathcal{H}_m(R) = \tilde{\mathcal{H}}(W_m(R))$ to the point $h_R[m] := \tilde{\mathcal{P}}(W_m(R))(\tilde{h}_R[m]) \in \mathbf{Aut}(D[p^m])_{\text{crys}}(R) \subset \mathcal{D}_m(R) = \mathbf{GL}_M(W_m(R))$.

We prove (d). The group $\text{Ker}(\rho_{m+1})$ is a unipotent, commutative group of dimension r^2 , cf. Subsubsection 3.1.3. As the connected group \mathcal{C}_m^0 is unipotent (cf. (a)) of dimension $\gamma_D(m)$ (cf. (c)) and as we have a short exact sequence $1 \rightarrow \text{Ker}(\rho_{m+1}) \rightarrow \mathcal{T}_{m+1}^0 \rightarrow \mathcal{C}_m^0 \rightarrow 1$ (see Subsubsection 3.2.2), from [DGr, Vol. II, Exp. XVII, Prop. 2.2 iv)] we get that the group \mathcal{T}_{m+1}^0 is a unipotent group of dimension $r^2 + \gamma_D(m)$. Thus (d) holds. \square

Corollary 5 *The smooth groups \mathcal{C}_m , $\mathbf{Aut}(D[p^m])_{\text{crys,red}}$, and $\mathbf{Aut}(D[p^m])_{\text{red}}$ are radicially isogenous.*

Proof: The finite homomorphisms ι_m and ζ_m of Theorem 5 (b) are bijective. Thus the corollary follows from [Se, Subsect. 1.2, Props. 1 and 2] (loc. cit. is stated for commutative group schemes over k but its proofs do not require the commutativity assumption). \square

3.2.4 Digression: a variant of the action \mathbb{T}_m

For the sake of completeness, we describe here a variant of the action \mathbb{T}_m that appeals to Subsubsection 3.1.2.

We consider the functor $\text{Aff}_k \rightarrow \text{Sets}$ which takes $\text{Spec } R$ to $W_m(R)$ -linear isomorphisms from $W_m(R) \otimes_{W(k)} M^{(\sigma)}$ to $W_m(R) \otimes_{W(k)} M$. This functor is represented by a connected smooth affine k -scheme of finite type \mathcal{D}'_m . If $\mathcal{H}'_m := \mathbb{W}_m(\mathbf{Aut}(\phi, \vartheta))$, then we have a natural action $\mathbb{T}'_m : \mathcal{H}'_m \times_k \mathcal{D}'_m \rightarrow \mathcal{D}'_m$ defined by transport of structure.

One can check that \mathbb{T}'_m is isomorphic to $\mathbb{T}_m^{(\sigma)}$ and has properties similar to the ones enjoyed by \mathbb{T}_m (see below; the isomorphism $\mathcal{H}'_m = \mathbb{W}_m(\mathbf{Aut}(\phi, \vartheta)) \rightarrow \mathbb{W}_m(\tilde{\mathcal{H}}^{(\sigma)}) = \mathcal{H}_m^{(\sigma)}$ is \mathbb{W}_m of the isomorphism $\mathbf{Aut}(\phi, \vartheta) \rightarrow \tilde{\mathcal{H}}^{(\sigma)}$ of Subsubsection 3.1.2). In particular, one can use the action \mathbb{T}'_m to show that the three smooth groups of the Corollary 5 are in fact isomorphic. More precisely, ι_m can be identified with the Frobenius endomorphism of \mathcal{S}_m , $\zeta_{m,\text{red}}$ can be identified with the m^{th} -power of the Frobenius endomorphism of $\mathbf{Aut}(D[p^m])_{\text{red}}$,

and $\text{Ker}(\zeta_m)$ contains (and it is quite likely to be equal to) the kernel of the m^{th} -power of the Frobenius endomorphism of $\mathbf{Aut}(D[p^m])$.

Let $S = \text{Spec } A$ be a smooth affine k -scheme. Let the crystalline site $\text{CRIS}(S/W_m(k))$ be as in [BBM, Subsect. 1.1.1] over the natural divided power thickening $\text{Spec } k \hookrightarrow \text{Spec } W_m(k)$. One identifies the sections of $\mathcal{O}_{\text{CRIS}(S/W_m(k))}$ with $W_m(A^{(\sigma^m)})$, cf. [IR, III, (1.5.2), p. 142].

For $i \in \{1, 2\}$ let B_i be a BT_m over k with Dieudonné F -crystal $\mathbb{D}(B_i) = (N_i, \phi_{m,i}, \vartheta_{m,i})$. Due to the previous paragraph, morphisms $\mathbb{D}(B_{2,S}) \rightarrow \mathbb{D}(B_{1,S})$ of Dieudonné F -crystals of $\text{CRIS}(S/W_m(k))$ correspond to $W_m(A^{(\sigma^m)})$ -linear maps $W_m(A^{(\sigma^m)}) \otimes_{W_m(k)} N_2 \rightarrow W_m(A^{(\sigma^m)}) \otimes_{W_m(k)} N_1$ compatible with the $\phi_{m,i}$'s and $\vartheta_{m,i}$'s. In view of [BM, Thm. 4.1.1], such $W_m(A^{(\sigma^m)})$ -linear maps describe the abelian group $\text{Hom}(B_{1,S}, B_{2,S})$. One can check via a direct inspection that the orbits of the action \mathbb{T}'_m are in bijection to the set of (representatives) of isomorphism classes of BT_m 's over k , to be compared with [Il, p. 156].

3.3 Proof of Theorem 2

The set of (representatives of) isomorphism classes of BT_{m+1} 's over k which lift $D[p^m]$ is in bijection to the set $\mathcal{O}_{m+1, m, 1_M[m]}$ of orbits of the action of \mathcal{T}_{m+1} on \mathcal{V}_{m+1} , cf. Lemma 2 (b). The group \mathcal{T}_{m+1}^0 is unipotent of dimension $r^2 + \gamma_D(m)$, cf. Theorem 5 (d). Moreover \mathcal{V}_{m+1} is isomorphic to the affine space of dimension r^2 over k . We have a short exact sequence $1 \rightarrow \text{Ker}(\rho_{m+1}) \rightarrow \mathcal{T}_{m+1} \rightarrow \mathcal{C}_m \rightarrow 1$, where $\text{Ker}(\rho_{m+1})$ is isomorphic to $\mathbb{G}_a^{r^2}$ (cf. Subsubsection 3.1.3) and where \mathcal{C}_m is radicially isogenous to $\mathbf{Aut}(D[p^m])_{\text{red}}$ (cf. Corollary 5). Theorem 2 follows from the last four sentences. \square

3.4 Properties of orbits

Proposition 1 *Let U be a smooth affine group over k whose identity component U^0 is unipotent. Let V be a reduced affine variety over k equipped with an action $\Lambda : U \times_k V \rightarrow V$. Then all orbits of Λ are closed. Thus, if Λ has an open, Zariski dense orbit o , then Λ has a unique orbit (i.e. $o = V$).*

Proof: All orbits of the action of U^0 on V are closed, cf. [Sp, Prop. 2.4.14] or [DGa, Ch. IV, Sect. 2, Subsect. 2, Cor. 2.7]. Each orbit of Λ is a finite union of translations of orbits of the action of U^0 on V via elements of $U(k)$. Thus the orbits of Λ are finite unions of reduced closed subvarieties of V and

therefore are closed. The last part of the proposition follows from the fact that V is the only closed, Zariski dense subscheme of itself. \square

We will need the following two applications of Proposition 1.

Corollary 6 *Let $\mathbf{End}(D[p^m])_{\text{crys}}$ be the group scheme over k of endomorphisms of $(M/p^m M, \phi_m, \vartheta_m)$. Then the following three properties hold:*

(a) *The following two open embeddings $\mathbf{Aut}(D[p^m]) \hookrightarrow \mathbf{End}(D[p^m])$ and $\mathbf{Aut}(D[p^m])_{\text{crys}} \hookrightarrow \mathbf{End}(D[p^m])_{\text{crys}}$ are also closed.*

(b) *The identity component $\mathbf{Aut}(D[p^m])^0$ (resp. $\mathbf{Aut}(D[p^m])_{\text{crys}}^0$) is the translation of the identity component $\mathbf{End}(D[p^m])^0$ (resp. $\mathbf{End}(D[p^m])_{\text{crys}}^0$) via the k -valued point $1_{D[p^m]}$ (resp. $1_{M/p^m M}$).*

(c) *Each k -valued point of $\mathbf{End}(D[p^m])_{\text{crys}}^0$ is a nilpotent endomorphism of $M/p^m M$.*

Proof: We will only prove (a) and (b) for $\mathbf{Aut}(D[p^m])$ and $\mathbf{End}(D[p^m])$ as the arguments for their crystalline versions are the same. To prove (a), it suffices to show that $U := \mathbf{Aut}(D[p^m])_{\text{red}}$ is an open and closed subvariety of $V := \mathbf{End}(D[p^m])_{\text{red}}$. As the identity component of U is a unipotent group (cf. Theorem 5 (a) and (b)) and as U is an orbit of the canonical left composite action of U on the affine variety V , from Proposition 1 we get that U is an open and closed subvariety of V . Part (b) follows from (a).

To prove (c), we can assume that $m = 1$. As each k -valued point of the unipotent subgroup $\mathbf{Aut}(D[p])_{\text{crys,red}}^0$ of $\mathbf{GL}_{M/pM}$ is unipotent, the case $m = 1$ follows from (b).

For the sake of completeness we include an elementary second proof of the corollary that does not depend on Proposition 1. It suffices to prove that if \mathcal{U} is a connected component of $\mathbf{End}(D[p])_{\text{crys}}$, then the characteristic polynomial $\chi_e(T) = \det(T1_M[1] - e)$ of an element $e \in \mathcal{U}(k)$ belongs to $\mathbb{F}_p[T]$ and thus due to continuity reasons it depends only on \mathcal{U} (if $\mathcal{U} = \mathbf{End}(D[p])_{\text{crys}}^0$, then $\chi_e(T) = \chi_{1_{M/pM}}(T) = T^r$). As e commutes with ϕ_1 and ϑ_1 and as we have $\text{Im}(\phi_1) = \text{Ker}(\vartheta_1)$ and $\text{Ker}(\phi_1) = \text{Im}(\vartheta_1)$, the short exact sequences of k -vector spaces $0 \rightarrow \text{Im}(\phi_1) \rightarrow M/pM \rightarrow (M/pM)/\text{Im}(\phi_1) \rightarrow 0$ and $0 \rightarrow (M/pM)/\text{Im}(\phi_1) \rightarrow (M/pM)^{(\sigma)} \rightarrow \text{Im}(\phi_1) \rightarrow 0$ are invariant under e and $e^{(\sigma)}$. Thus $\chi_e(T) = \chi_{e^{(\sigma)}}(T)$ and therefore $\chi_e(T) \in \mathbb{F}_p[T]$. \square

Lemma 3 *The following three statements are equivalent:*

(i) *we have $\dim(\mathcal{O}_{m+1}) = \dim(\mathcal{O}_m) + \dim(\text{Ker}(\rho_{m+1})) = \dim(\mathcal{O}_m) + r^2$;*

- (ii) we have $\mathcal{O}_{m+1} = \tau_{m+1}^{-1}(\mathcal{O}_m)$ (i.e. we have $\mathcal{V}_{m+1} \subset \mathcal{O}_{m+1}$);
- (iii) the set of orbits $\mathbb{O}_{m+1,m,1_M}$ (equivalently, $\mathbb{O}_{m+1,m,1_M[m]}$) is finite.

Proof: The k -scheme \mathcal{V}_{m+1} is an affine space of dimension r^2 . The fibres of the faithfully flat morphism $\mathcal{O}_{m+1} \rightarrow \mathcal{O}_m$ induced by τ_{m+1} have equal dimensions. Thus $\dim(\mathcal{O}_{m+1}) = \dim(\mathcal{O}_m) + \dim(\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1})$. If (ii) holds, then $\dim(\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1}) = \dim(\mathcal{V}_{m+1}) = r^2$ and therefore $\dim(\mathcal{O}_{m+1}) = \dim(\mathcal{O}_m) + r^2$. Thus (ii) implies (i). Obviously (ii) implies (iii).

We check that (i) implies (ii). The orbit of $1_M[m+1]$ under \mathcal{T}_{m+1} is $(\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1})_{\text{red}}$. If (i) holds, then $\dim(\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1}) = \dim(\mathcal{O}_{m+1}) - \dim(\mathcal{O}_m) = r^2 = \dim(\mathcal{V}_{m+1})$ and therefore $\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1}$ is an open subscheme of \mathcal{V}_{m+1} . Thus the action of \mathcal{T}_{m+1} on \mathcal{V}_{m+1} has an open, Zariski dense orbit. As \mathcal{T}_{m+1}^0 is a unipotent group (cf. Theorem 5 (d)), from the second part of Proposition 1 we get that $\mathcal{V}_{m+1} \cap \mathcal{O}_{m+1} = \mathcal{V}_{m+1}$, i.e. $\mathcal{V}_{m+1} \subset \mathcal{O}_{m+1}$. Thus (i) implies (ii).

We check that (iii) implies (ii). As (iii) holds, the action of \mathcal{T}_{m+1} on \mathcal{V}_{m+1} has a finite number of orbits and thus it has an open, Zariski dense orbit. As in the previous paragraph we argue that this orbit is \mathcal{V}_{m+1} , i.e. $\mathcal{V}_{m+1} \subset \mathcal{O}_{m+1}$. Therefore (iii) implies (ii). Thus the three statements are equivalent. \square

3.5 Proof of Theorem 3

We prove that Theorem 3 holds. The integral domain \mathcal{R} is normal and its field of fractions k_1 is algebraically closed. Thus \mathcal{R} is a perfect ring. Let $\sigma_{\mathcal{R}}$ be the Frobenius automorphism of the ring $W(\mathcal{R})$ of Witt vectors with coefficients in \mathcal{R} . Let $(M_{\mathcal{R}}, \phi_{\mathcal{R}}, \vartheta_{\mathcal{R}})$ be the Dieudonné module of \mathfrak{D} over \mathcal{R} (i.e. the projective limit indexed by $s \in \mathbb{N}^*$ of the evaluation of the Dieudonné F -crystal $\mathbb{D}(\mathfrak{D})$ of \mathfrak{D} at the thickening $\text{Spec } \mathcal{R} \hookrightarrow \text{Spec } W_s(\mathcal{R})$ defined by the natural divided power structure of the ideal (p) of $W_s(\mathcal{R})$). Thus $M_{\mathcal{R}}$ is a free $W(\mathcal{R})$ -module of rank r , $\phi_{\mathcal{R}} : M_{\mathcal{R}} \rightarrow M_{\mathcal{R}}$ is a $\sigma_{\mathcal{R}}$ -linear endomorphism, $\vartheta_{\mathcal{R}} : M_{\mathcal{R}} \rightarrow M_{\mathcal{R}}$ is a $\sigma_{\mathcal{R}}^{-1}$ -linear endomorphism, and we have $\phi_{\mathcal{R}} \circ \vartheta_{\mathcal{R}} = \vartheta_{\mathcal{R}} \circ \phi_{\mathcal{R}} = p1_{M_{\mathcal{R}}}$. Let $\bar{F}_{\mathcal{R}}^1$ be the kernel of the reduction modulo p of $\phi_{\mathcal{R}}$. As \mathfrak{D} has codimension c and dimension d and as \mathcal{R} is local, the pair $(M_{\mathcal{R}}, \bar{F}_{\mathcal{R}}^1 \subset M_{\mathcal{R}}/pM_{\mathcal{R}})$ is isomorphic to $W(\mathcal{R}) \otimes_{W(k)} (M, \bar{F}^1 \subset M/pM)$. Thus there exists an element $g_{\mathcal{R}} \in \mathbf{GL}_M(W(\mathcal{R}))$ such that the triple $(M_{\mathcal{R}}, \phi_{\mathcal{R}}, \vartheta_{\mathcal{R}})$ is isomorphic to the triple $(W(\mathcal{R}) \otimes_{W(k)} M, g_{\mathcal{R}}(\sigma_{\mathcal{R}} \otimes \phi), (\sigma_{\mathcal{R}}^{-1} \otimes \vartheta)g_{\mathcal{R}}^{-1})$. We view $g_{\mathcal{R}}$ as a point $g_{\mathcal{R}} \in \mathcal{D}_{\infty}(\mathcal{R})$. For $m \in \mathbb{N}^*$, let $g_{\mathcal{R}}[m] \in \mathcal{D}_m(\mathcal{R})$ be the

point defined by the reduction modulo p^m of $g_{\mathcal{R}}$. Let $g_{k_1}[m] \in \mathcal{D}_m(k_1)$ and $g_k[m] \in \mathcal{D}_m(k)$ be the points defined naturally by $g_{\mathcal{R}}[m]$.

Let $g' \in \mathbf{GL}_M(W(k))$ be such that the Dieudonné module of D' is isomorphic to $(M, g'\phi, \vartheta(g')^{-1})$. Let \mathcal{O}'_m be the orbit of $g'[m] \in \mathcal{D}_m(k)$ under the action \mathbb{T}_m . As \mathfrak{D}_{k_1} is isomorphic to D'_{k_1} , for all $m \in \mathbb{N}^*$ we have $g_{k_1}[m] \in \mathcal{O}'_m(k_1) \subset \mathcal{D}_m(k_1)$ (cf. Lemma 1 applied to \mathbb{T}_{m,k_1}). As $D = \mathfrak{D}_k$, we have $g_k[m] \in \mathcal{O}_m(k)$. Thus, as $g_{k_1}[m]$ specializes to $g_k[m]$ (via $g_{\mathcal{R}}[m]$), the schematic closure $\bar{\mathcal{O}}'_m$ of \mathcal{O}'_m in \mathcal{D}_m contains points of \mathcal{O}_m . Thus $\mathcal{O}_m \subset \bar{\mathcal{O}}'_m$ and therefore we have

$$(1) \quad \dim(\mathcal{O}_m) \leq \dim(\mathcal{O}'_m) = \dim(\bar{\mathcal{O}}'_m).$$

As $\gamma_D(m) = \dim(\mathcal{S}_m)$ (cf. Theorem 5 (d)), we have

$$(2) \quad \gamma_D(m) = \dim(\mathcal{H}_m) - \dim(\mathcal{O}_m).$$

Similarly $\gamma_{D'}(m) = \dim(\mathcal{H}_m) - \dim(\mathcal{O}'_m)$. Thus for all $m \in \mathbb{N}^*$ we have $\gamma_{D'}(m) \leq \gamma_D(m)$, cf. either (1) or property (a) of Subsection 1.1.

We assume that there exists a number $l \in \mathbb{N}^*$ such that $\gamma_{D'}(l) = \gamma_D(l)$. Thus $\dim(\mathcal{O}_l) = \dim(\mathcal{O}'_l) = \dim(\bar{\mathcal{O}}'_l)$, cf. (2). From these equalities and the fact that $\bar{\mathcal{O}}'_l$ contains points of \mathcal{O}_l , we get that the two orbits \mathcal{O}'_l and \mathcal{O}_l coincide. Thus $D'[p^l]$ is isomorphic to $D[p^l]$, cf. Lemma 2 (a). This ends the proof of Theorem 3 (a).

We prove Theorem 3 (b). Let $m \geq \max\{n_D, n_{D'}\}$. We have $s_{D'} = \gamma_{D'}(m) \leq \gamma_D(m) = s_D$. Next we assume that $s_{D'} = s_D$. Thus $\gamma_{D'}(m) = \gamma_D(m)$. Therefore $D'[p^m]$ is isomorphic to $D[p^m]$, cf. Theorem 3 (a). As $m \geq n_D$, we get that D' is isomorphic to D . This ends the proof of Theorem 3 (b) and thus also of Theorem 3. \square

4 Proof of Theorem 4

Let B, D , and $1 \leq m < n_D$ be as in Theorem 4. To prove Theorem 4 it suffices to show that there exists an infinite set \mathcal{I} of BT_{m+1} 's over k that has the following two properties:

- (i) if $B_1, B_2 \in \mathcal{I}$ are distinct elements, then B_1 is not isomorphic to B_2 ;
- (ii) if $B_1 \in \mathcal{I}$, then $B_1[p^m]$ is isomorphic to $B = D[p^m]$.

We will use the notations of Subsections 3.1 to 3.2, with (M, ϕ, ϑ) as the Dieudonné module of D . Based on the first sentence of Subsection 3.3, the

existence of \mathcal{I} is equivalent to the fact that the set of orbits $\mathbb{O}_{m+1,m,1_M[m]}$ introduced in Subsubsection 3.2.2 is infinite. We will show that the assumption that the set of orbits $\mathbb{O}_{m+1,m,1_M[m]}$ is finite, leads to a contradiction. Based on Lemma 3, we get that $\dim(\mathcal{O}_{m+1}) = \dim(\mathcal{O}_m) + r^2$.

For $i \in \mathbb{N}^*$, from (2) and the fact that $\dim(\mathcal{H}_{i+1}) - \dim(\mathcal{H}_i) = r^2$ we get:

$$(3) \quad \gamma_D(i+1) - \gamma_D(i) = r^2 - \dim(\mathcal{O}_{i+1}) + \dim(\mathcal{O}_i).$$

Thus $\gamma_D(m+1) - \gamma_D(m) = 0$.

To end the argument of the existence of the set \mathcal{I} , it suffices to show that the assumptions that $m \in \{1, \dots, n_D - 1\}$ and $\gamma_D(m+1) - \gamma_D(m) = 0$ lead to a contradiction. As $\gamma_D(m+1) - \gamma_D(m) = 0$, from Theorem 1 (a) (proved in Subsection 2.2) we get that the sequence $(\gamma_D(i))_{i \geq m}$ is constant, i.e. for each integer $i \geq m$ we have $\gamma_D(i) = \gamma_D(m)$. In particular, as $m \in \{1, \dots, n_D - 1\}$ we get that $\gamma_D(n_D) = \gamma_D(n_D - 1)$.

Therefore we have $\dim(\mathcal{O}_{n_D}) = r^2 + \dim(\mathcal{O}_{n_D-1})$, cf (3). Thus the set of orbits $\mathbb{O}_{n_D,n_D-1,1_M}$ (equivalently, $\mathbb{O}_{n_D,n_D-1,1_M[n_D-1]}$) has one element (cf. the equivalence of statements (i) and (ii) of Lemma 3). Therefore each BT_{n_D} over k that lifts $D[p^{n_D-1}]$ is isomorphic to $D[p^{n_D}]$, cf. Lemma 2 (b).

Let D' be a p -divisible group over k such that $D'[p^{n_D-1}]$ is isomorphic to $D[p^{n_D-1}]$. We know that $D'[p^{n_D}]$ is isomorphic to $D[p^{n_D}]$, cf. previous paragraph. Thus D' is isomorphic to D , cf. the very definition of n_D . Therefore we have $n_D \leq n_D - 1$, again cf. the very definition of n_D . Contradiction. This ends the argument of the existence of an infinite set \mathcal{I} for which properties (i) and (ii) hold. This also ends the proof of Theorem 4. \square

5 Proof of Theorem 1 (b) and applications

We prove Theorem 1 (b). In Section 4 we checked that the assumptions that $m \in \{1, \dots, n_D - 1\}$ and $\gamma_D(m+1) - \gamma_D(m) = 0$ lead to a contradiction. Based on this and Theorem 1 (a), we get that the strict inequalities of Theorem 1 (b) hold. Thus to end the proof of Theorem 1 (b) it suffices to show that $\gamma_D(1) \geq a_D^2$. Taking the Cartier dual of the exact complex $0 \rightarrow \alpha_p^{a_{D^t}} \rightarrow D[p]^t$, we get an exact complex $D[p] \rightarrow \alpha_p^{a_{D^t}} \rightarrow 0$. Using it and the exact complex $0 \rightarrow \alpha_p^{a_D} \rightarrow D[p]$, we get that the group scheme of homomorphisms $\mathbf{Hom}(\alpha_p^{a_{D^t}}, \alpha_p^{a_D}) = \mathbf{End}(\alpha_p)^{a_D a_{D^t}}$ is a subgroup scheme of $\mathbf{End}(D[p])$. At the level of dimensions we get that $\gamma_D(1) \geq a_D a_{D^t}$. Thus to prove that $\gamma_D(1) \geq a_D^2$ it suffices to check that $a_D = a_{D^t}$. We will use the

classical Dieudonné theory. We recall that the Dieudonné module of $D[p]$ is $(M/pM, \phi_1, \vartheta_1)$. Then $a_D = \dim_k((M/pM)/(\text{Im}(\phi_1) + \text{Im}(\vartheta_1)))$ is equal to $r - \dim_k(\text{Im}(\phi_1)) - \dim_k(\text{Im}(\vartheta_1)) + \dim_k(\text{Im}(\phi_1) \cap \text{Im}(\vartheta_1))$ and thus also to $r - c - d + \dim_k(\text{Ker}(\vartheta_1) \cap \text{Ker}(\phi_1)) = \dim_k(\text{Ker}(\vartheta_1) \cap \text{Ker}(\phi_1)) = a_{D^t}$.

This ends the proof of Theorem 1 (b) and thus also of Theorem 1 (cf. Subsection 2.2 and paragraph after Theorem 1). \square

5.1 Proof of Corollary 1

To prove Corollary 1 we can assume that $cd > 0$. If D is ordinary, then we have $\gamma_D(i) = 0$ for all $i \in \mathbb{N}$ and $n_D = 1 \leq cd$. Thus we can also assume that D is not ordinary (equivalently, that $a_D \geq 1$). From Theorem 1 (b) and (c) we get that $n_D \leq cd + 1 - \gamma_D(1) \leq cd + 1 - a_D^2 \leq cd$. Thus Corollary 1 holds. \square

5.2 Proof of Corollary 2

To prove Corollary 2 (a) we can assume $cd > 0$. Each connected component of the image of $r_{l,i}$ has dimension $\gamma_D(l) - \gamma_D(l - i)$, cf. property 2.1 (iii). If an endomorphism of $D[p^l]$ restricts to an automorphism of $D[p^i]$, then it is an automorphism. Thus the image of the restriction homomorphism $a_{l,i} : \mathbf{Aut}(D[p^l]) \rightarrow \mathbf{Aut}(D[p^i])$ is $\text{Im}(r_{l,i}) \cap \mathbf{Aut}(D[p^i])$ and therefore it is a nonempty open subscheme of $\text{Im}(r_{l,i})$. Thus the images of $a_{l,i}$ and $r_{l,i}$ have equal dimension $\gamma_D(l) - \gamma_D(l - i)$. We have $\gamma_D(l) - \gamma_D(l - i) = 0$ if and only if $l - i \geq n_D$, cf. Theorem 1 (b) and (c). Therefore the image of $a_{l,i}$ (or $r_{l,i}$) has positive dimension if and only if $l - i \geq n_D$. Thus Corollary 2 (a) holds.

From Corollary 2 (a) and Theorem 1 (b) and (c) we get that if D is not ordinary (i.e. if $n_D > 0$ and $\gamma_D(1) > 0$) and if n is as in Corollary 2 (b), then we have $n = n_D$. Thus Corollary 2 (b) holds.

To prove Corollary 2 (c), we can assume that D is not ordinary. Thus Corollary 2 (c) follows from Corollary 2 (b) and the fact that the image of the restriction homomorphism $r_{l,1}$ is finite if and only if the image of the analogue restriction homomorphism obtained working with D^s instead of D is finite. \square

5.3 Proof of Corollary 3

Corollary 3 (a) follows from Corollary 2 (a). Corollary 3 (b) follows from Theorem 5 (b) and (c). To check that Corollary 3 (c) to (e) hold, we can assume that D is not ordinary and that $i \geq n_D + 1 \geq 2$. Let $a_i \in \mathbf{Aut}(D[p^i])^0(k)$. Let $b_i := \zeta_i(k)(a_i) \in \mathcal{D}_i(k) = \mathbf{GL}(W_i(k))$ be the crystalline realization of a_i , cf. the notations of Subsection 3.2. Due to Corollary 3 (a), we can write $b_i = 1_M[i] + p^{s(a_i)}e_i$, where $s(a_i) \in \{i - n_D, \dots, i\}$ and $e_i \in \text{End}(M/p^i M) \setminus p \text{End}(M/p^i M)$; moreover there exist elements a_i with $s(a_i) = i - n_D$. Corollary 3 (c) follows from this once we check that the order of the element b_i (equivalently a_i) is $p^{i-s(a_i)}$. It suffices to consider the case when $n_D \geq 2$ and $(p, i, s(a_i)) = (2, n_D + 1, 1)$ and to show that $b_i^2 = 1_M[i] + 4(e_i + e_i^2)$ is not congruent to $1_M[i]$ modulo 8. In such a case, the reduction \bar{e}_i modulo 2 of e_i is a non-zero unipotent element of $\text{End}(M/2M)$ (the elements \bar{e}_i together with 0 are the k -valued points of a connected smooth subgroup of $\mathbf{End}(D[2])_{\text{crys}}^0$ and thus are unipotent, cf. Corollary 6 (c) applied with $m = 1$); thus $\bar{e}_i \neq \bar{e}_i^2$ (i.e. b_i^2 is not congruent to $1_M[i]$ modulo 8).

If $a'_i \in \mathbf{Aut}(D[p^i])^0(k)$ is another element whose crystalline realization is $b'_i = 1_M[i] + p^{s(a'_i)}e'_i \in \mathbf{GL}(W_i(k))$ with $e'_i \in \text{End}(M/p^i M) \setminus p \text{End}(M/p^i M)$, then b_i and b'_i commute modulo $p^{\min\{s(a_i)+s(a'_i), i\}}$. If $i \geq 2n_D$, then $s(a_i) + s(a'_i) \geq 2(i - n_D) \geq i$ and thus b_i and b'_i commute. Thus Corollary 3 (d) holds. If $l > i \geq n_D + 1$ and $a_l \in \mathbf{Aut}(D[p^l])^0(k)$ has crystalline realization $b_l = 1_M[l] + p^{s(a_l)}e_l$, then there exists a unique element ${}_i a_l \in \mathbf{Aut}(D[p^i])^0(k)$ whose crystalline realization is ${}_i b_l = 1_M[i] + p^{s(a_l)-l+i}e_l[i]$, where $e_l[i]$ is the reduction modulo p^i of e_l . The rule $a_l \mapsto {}_i a_l$ defines the canonical bijection $\mathbf{Aut}(D[p^l])^0(k) \rightarrow \mathbf{Aut}(D[p^i])^0(k)$ which has the desired properties. Thus Corollary 3 (e) holds. \square

5.4 A refinement of Corollary 1

We recall that $s_D = \gamma_D(n_D)$. If D is ordinary, then $s_D = 0 = a_D$ and $n_D \leq 1$. Thus in this subsection we will assume that D is not ordinary. From Theorem 1 (b) we get that $n_D \leq s_D + 1 - \gamma_D(1) \leq s_D + 1 - a_D^2$. As D is not ordinary, we have $a_D \geq 1$ and thus we have

$$(4) \quad n_D \leq s_D + 1 - a_D^2 \leq s_D.$$

We recall that $B(k)$ is the field of fractions of $W(k)$. Dieudonné's classification of F -isocrystals over k implies that we have a direct sum decomposition

$(M[\frac{1}{p}], \phi) = \oplus_{s=1}^v (W_s, \phi)$ into simple F -isocrystals over k (here v is a positive integer). More precisely, for $s \in \{1, \dots, v\}$ there exist $c_s, d_s \in \mathbb{N}$ such that $r_s := c_s + d_s > 0$, $\text{g.c.d.}\{c_s, d_s\} = 1$, $\dim_{B(k)}(W_s) = r_s$, and moreover there exists a $B(k)$ -basis for W_s formed by elements fixed by $p^{-d_s}\phi^{r_s}$; the unique Newton polygon slope of (W_s, ϕ) is $\alpha_s := \frac{d_s}{r_s} \in \mathbb{Q} \cap [0, 1]$. We have

$$(5) \quad s_D = cd - \frac{1}{2} \sum_{s=1}^v \sum_{t=1}^v r_s r_t |\alpha_s - \alpha_t| = cd - \frac{1}{2} \sum_{s=1}^v \sum_{t=1}^v |c_s d_t - c_t d_s|,$$

cf. [Va2, Thm. 1.2 (c), (d), (e), and (f)]. From (4) and (5) we get

$$(6) \quad n_D \leq 1 + cd - a_D^2 - \frac{1}{2} \sum_{s=1}^v \sum_{t=1}^v |c_s d_t - c_t d_s| \leq cd - \frac{1}{2} \sum_{s=1}^v \sum_{t=1}^v |c_s d_t - c_t d_s|.$$

5.5 Remark

In the proof of [Va2, Thm. 1.2 (e)] (see [Va2, Subsect. 3.5]) one needs to take m slightly bigger (it would suffice to take $m \geq \max\{2\kappa + n_{\tilde{D}}, n_D\}$ instead of $m \geq \max\{\kappa + n_{\tilde{D}}, n_D\}$) in order to get that the pull-back $\mathcal{D}_{\tilde{Y}}$ of \mathcal{D} to \tilde{Y} of [Va2, Subsect. 3.5] is a constant p -divisible group isomorphic to $D \times_k \tilde{Y}$. The p -divisible group $\mathcal{D}_{\tilde{Y}}$ is isomorphic to \mathcal{C}/\mathcal{L} , where the p -divisible group $\mathcal{C} := \tilde{\mathcal{D}}_{m,m} \times_{i_D(m)} \tilde{Y}$ is equipped with an isomorphism $\theta_1 : \mathcal{C} \rightarrow \tilde{D} \times_k \tilde{Y}$ and where \mathcal{L} is the pull-back of $(D[p^\kappa]/\mathcal{K}) \times_k \tilde{Y} \subset \tilde{D}[p^\kappa]$ via an isomorphism $\theta_2 : \mathcal{C}[p^{m-\kappa}] \rightarrow \tilde{D}[p^{m-\kappa}] \times_k \tilde{Y}$. Let $\omega := \theta_1[p^{m-\kappa}] \circ \theta_2^{-1} \in \mathbf{Aut}(\tilde{D}[p^{m-\kappa}])(\tilde{Y})$. We can assume that the restriction of ω to the closed point $\text{Spec } k$ of \tilde{Y} is the identity. The reduced group \mathfrak{E} of the image of the restriction homomorphism $\mathbf{Aut}(\tilde{D}[p^{m-\kappa}]) \rightarrow \mathbf{Aut}(\tilde{D}[p^\kappa])$ is a finite, étale group over k (cf. either Corollary 2 (a) for $m \geq 2\kappa + n_{\tilde{D}}$ or [Va1, Thm. 5.1.1 (c)] for $m \gg 0$). As the k -scheme \tilde{Y} is connected and reduced (being integral), the restriction of ω to an automorphism of $\tilde{D}[p^\kappa]_{\tilde{Y}}$ is a \tilde{Y} -valued point of \mathfrak{E} which is the identity as its restriction to the closed point $\text{Spec } k$ of \tilde{Y} is so. From this we easily get that the p -divisible group $\mathcal{D}_{\tilde{Y}}$ is isomorphic to $D \times_k \tilde{Y}$.

6 Generalizations to relative contexts

We recall that (M, ϕ, ϑ) is the contravariant Dieudonné module of D and that we denote also by $\phi : \text{End}(M)[\frac{1}{p}] \rightarrow \text{End}(M)[\frac{1}{p}]$ the σ -linear automorphism

induced naturally by ϕ . Let G be a smooth closed subgroup scheme of \mathbf{GL}_M such that its generic fibre $G_{B(k)}$ is connected. Thus the scheme G is integral. Let $\mathfrak{g} := \text{Lie}(G)$ be the Lie algebra of G . Until the end we will assume that the following two axioms hold for the triple (M, ϕ, G) :

(**AX1**) the Lie subalgebra $\mathfrak{g}[\frac{1}{p}]$ of $\text{End}(M)[\frac{1}{p}]$ is stable under ϕ , i.e. we have $\phi(\mathfrak{g}[\frac{1}{p}]) = \mathfrak{g}[\frac{1}{p}]$;

(**AX2**) there exist a direct sum decomposition $M = F^1 \oplus F^0$ such that the following two properties hold:

- (a) the kernel \bar{F}^1 of the reduction modulo p of ϕ is F^1/pF^1 ;
- (b) the cocharacter $\mu : \mathbb{G}_m \rightarrow \mathbf{GL}_M$ which acts trivially on F^0 and via the inverse of the identical character of \mathbb{G}_m on F^1 , normalizes G .

The triple (M, ϕ, G) is called an *F-crystal with a group* over k , cf. [Va1, Def. 1.1 (a) and Subsect. 2.1]. If μ factors through G , then the *W-condition* of [Va1, Subsubsect. 2.2.1 (d)] holds for (M, ϕ, G) . Axioms (AX1) and (AX2) are a weakening of the two axioms used in [Va2, Subsect. 4.1]. Until the end, we will use the notations of Subsubsection 3.1.1 and Subsection 3.2.

Definition 1 (a) Let $g_1, g_2 \in G(W(k))$. An inner isomorphism between the two triples $(M, g_1\phi, G)$ and $(M, g_2\phi, G)$ is an element $g_3 \in G(W(k))$ that defines an isomorphism between the Dieudonné modules $(M, g_1\phi, \vartheta g_1^{-1})$ and $(M, g_2\phi, \vartheta g_2^{-1})$ (i.e. we have $g_3 g_1 \phi = g_2 \phi g_3$).

(b) An inner isomorphism between $(M/p^m M, g_1[m]\phi_m, \vartheta_m g_1[m]^{-1}, G_{W_m(k)})$ and $(M/p^m M, g_2[m]\phi_m, \vartheta_m g_2[m]^{-1}, G_{W_m(k)})$ is an element $g_3[m] \in G(W_m(k))$ which defines an isomorphism between the following two Dieudonné modules $(M/p^m M, g_1[m]\phi_m, \vartheta_m g_1[m]^{-1})$ and $(M/p^m M, g_2[m]\phi_m, \vartheta_m g_2[m]^{-1})$.

(c) Let $\mathbf{Aut}(D[p^m])_{\text{crys}}$ and $\zeta_m : \mathbf{Aut}(D[p^m]) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}$ be as in the proof of Theorem 5. Let $\mathbf{Aut}(D[p^m])_{\text{crys}}^G := \mathcal{D}_m^G \cap \mathbf{Aut}(D[p^m])_{\text{crys}}$ (the intersection being taken inside \mathcal{D}_m). Let $\mathbf{Aut}(D[p^m])^G := \zeta_m^{-1}(\mathbf{Aut}(D[p^m])_{\text{crys}}^G)$. Thus $\mathbf{Aut}(D[p^m])^G(k)$ is the subgroup of $\mathbf{Aut}(D[p^m])(k)$ formed by those elements that define (via ζ_m) elements of $G(W_m(k))$.

(d) For $i \in \mathbb{N}^*$ let $\gamma_D^G(i) := \dim(\mathbf{Aut}(D[p^i])^G) = \dim(\mathbf{Aut}(D[p^i])_{\text{crys}}^G)$. Let $\gamma_D^G(0) := 0$. We call $(\gamma_D^G(i))_{i \in \mathbb{N}}$ the centralizing G -sequence of D .

Lemma 4 The intersection $\mathcal{W}^G := G_k \cap \mathcal{W}$ is a smooth group over k .

Proof: This is a particular case of [CGP, Prop. 2.1.8 (3) and Rm. 2.1.11] applied to the smooth affine group G_k over k and the \mathbb{G}_m action on it induced by the special fibre λ of the inverse μ^{-1} of the cocharacter μ of the axiom (AX2) (our pair (G_k, \mathcal{W}^G) is $(G, P_G(\lambda) = Z_G(\lambda) \times_k U_G(\lambda))$ of loc. cit.). \square

6.1 Relative notations and basic properties

Let $\tilde{\mathcal{H}}^G$ be the dilatation of G centered on \mathcal{W}^G . As in Subsubsection 3.1.1, based on the axiom (AX1) and Lemma 4 we get that $\tilde{\mathcal{H}}^G$ is a smooth affine group scheme over $\text{Spec } W(k)$ equipped with a homomorphism $\tilde{\mathcal{P}}^G : \tilde{\mathcal{H}}^G \rightarrow G$ whose generic fibre is an isomorphism of groups over $\text{Spec } B(k)$. Moreover, $\tilde{\mathcal{H}}^G$ is a closed subgroup scheme of $\tilde{\mathcal{H}}$ (cf. [BLR, Ch. 3, Sect. 3.2, Prop. 2 (a)]) and $\tilde{\mathcal{P}}^G$ is the natural restriction of $\tilde{\mathcal{P}}$. Another way to define $\tilde{\mathcal{P}}^G$ is as follows (cf. Example 2 of Appendix A). We can identify $\tilde{\mathcal{H}}^G$ with the schematic closure $G_{B(k),M,\phi^{-1}(M)}$ in $G \times_{W(k)} \phi^{-1}G\phi$ of $G_{B(k)}$ embedded diagonally in $G \times_{W(k)} \phi^{-1}G\phi$ (here $\phi^{-1}G\phi$ is the schematic closure of $G_{B(k)}$ in $\mathbf{GL}_{\phi^{-1}(M)}$). Under this identification, $\tilde{\mathcal{P}}^G$ gets identified with the first projection homomorphism $G_{B(k),M,\phi^{-1}(M)} \rightarrow G$.

Let d_G be the relative dimension of G over $\text{Spec } W(k)$; thus $d_G = \dim(G_k)$. Let $m \in \mathbb{N}^*$. Let $\mathcal{H}_m^G := \mathbb{W}_m(\tilde{\mathcal{H}}^G)$; it is a smooth subgroup of \mathcal{H}_m of dimension md_G . Let $\mathcal{D}_m^G := \mathbb{W}_m(G)$; it is a smooth closed subvariety of \mathcal{D}_m of dimension md_G . As in Subsection 3.2 we argue that we have an action

$$\mathbb{T}_m^G : \mathcal{H}_m^G \times_k \mathcal{D}_m^G \rightarrow \mathcal{D}_m^G$$

which is the natural restriction of the action \mathbb{T}_m . Thus, if $\tilde{h} \in \tilde{\mathcal{H}}^G(W(k))$ and $g \in G(W(k))$, then the product of $\tilde{h}[m] \in \mathcal{H}_m^G(k) = \tilde{\mathcal{H}}^G(W_m(k))$ and $g[m] \in \mathcal{D}_m^G(k) = G(W_m(k))$ is $\mathbb{T}_m(\tilde{h}[m], g[m]) := (hg\phi(h^{-1}))[m]$, where $h := \tilde{\mathcal{P}}^G(W(k))(\tilde{h}) \in G(W(k))$ has the same meaning as in Subsubsection 3.1.1.

Let n_D^G be the smallest non-negative integer that has the following property: for each element $\tilde{g} \in G(W(k))$ congruent to 1_M modulo $p^{n_D^G}$, there exists an inner isomorphism between (M, ϕ, G) and $(M, \tilde{g}\phi, G)$. The existence of n_D^G is implied by [Va1, Main Thm. A]. If $G = \mathbf{GL}_M$, then $n_D^G = n_D$ (cf. either [Va1, Lemma 3.2.2 and Cor. 3.2.3] or [NV1, Thm. 2.2 (a)]).

Let $\rho_{m+1}^G := \text{Red}_{m+1, \tilde{\mathcal{H}}^G}$ and $\tau_{m+1}^G := \text{Red}_{m+1, G}$ (see Subsubsection 3.1.3 for notations). Thus $\rho_{m+1}^G : \mathcal{H}_{m+1}^G \rightarrow \mathcal{H}_m^G$ is the natural reduction epimorphism of smooth affine groups over k and $\tau_{m+1}^G : \mathcal{D}_{m+1}^G \rightarrow \mathcal{D}_m^G$ is the natural reduction epimorphism of affine (group) varieties over k . The action \mathbb{T}_m^G is also a natural reduction of the action \mathbb{T}_{m+1}^G . The projective limits

$$\mathcal{H}_\infty^G := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{H}_m^G \quad \text{and} \quad \mathcal{D}_\infty^G := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{D}_m^G$$

in the category of ringed spaces are also projective limits in the category of k -schemes, \mathcal{H}_∞^G is an affine group scheme over k , and \mathcal{D}_∞^G is an affine (group)

scheme over k . Moreover, we have a limit action

$$\mathbb{T}_\infty^G : \mathcal{H}_\infty^G \times_k \mathcal{D}_\infty^G \rightarrow \mathcal{D}_\infty^G.$$

Let \mathcal{O}_m^G be the orbit of $1_M[m] \in \mathcal{D}_m^G(k)$ under the action \mathbb{T}_m^G . Let \mathcal{S}_m^G be the subgroup scheme of \mathcal{H}_m^G which is the stabilizer of $1_M[m]$. Inside \mathcal{H}_m , we have $\mathcal{S}_m^G = \mathcal{S}_m \cap \mathcal{H}_m^G$. Let $\mathcal{C}_m^G := \mathcal{S}_{m,\text{red}}^G$. We have $\dim(\mathcal{S}_m^G) = \dim(\mathcal{C}_m^G) = \dim(\mathcal{H}_m^G) - \dim(\mathcal{O}_m^G) = md_G - \dim(\mathcal{O}_m^G)$. The orbits of \mathbb{T}_∞^G are defined similarly to the orbits of \mathbb{T}_∞ (see Subsubsection 3.2.1).

Lemma 5 *The set of orbits of \mathbb{T}_m^G is in natural bijection to the set of (representatives of) inner isomorphism classes of quadruples of the form $(M/p^m M, g[m]\phi_m, \vartheta_m g[m]^{-1}, G_{W_m(k)})$ with $g \in G(W(k))$.*

Proof: The rule that maps the orbit of $g[m]$ under \mathbb{T}_m^G to the inner isomorphism class of $(M/p^m M, g[m]\phi_m, \vartheta_m g[m]^{-1}, G_{W_m(k)})$ is well defined (cf. definition of \mathbb{T}_m^G) and we are left to check that the resulting map is a bijection. It suffices to show that if $g_1, g_2, g_3 \in G(W(k))$ are as in Definition 1 (b), then there exists $\tilde{h} \in \tilde{\mathcal{H}}^G(W(k))$ such that $\mathbb{T}_m^G(\tilde{h}[m], g_1[m]) = g_2[m]$. The pair $(g_3[m], (g_2^{-1}g_3g_1)[m])$ is an automorphism of the pair of maps $M/p^m M \xrightleftharpoons[\vartheta_m]{\phi_m} M/p^m M$. Thus the pair $(g_3[m], \phi^{-1}(g_2^{-1}g_3g_1)[m]\phi)$ is an isomor-

phism of the pair of $W_m(k)$ -linear maps $M/p^m M \xrightleftharpoons[p]{j_m} \phi^{-1}(M)/p^m \phi^{-1}(M)$, where j_m is the reduction modulo p^m of the inclusion $M \hookrightarrow \phi^{-1}(M)$.

Based on the axiom (AX2), the group $G_{B(k)}$ is well positioned with respect to $(M, \phi^{-1}(M))$ in the sense of Definition 2 of Appendix A (cf. Proposition 4 of Appendix A applied to $(W(k), p, G, \mu_{B(k)}, \phi^{-1}(M))$ instead of $(R, \pi, G_M, \lambda, M')$). For the remaining part of the proof we will only use this well positioned property which asserts the existence of an isomorphism $\Theta : \tilde{\mathcal{H}}^G = G_{B(k), M, \phi^{-1}(M)} \rightarrow G_{B(k), M, \phi^{-1}(M)}^* := (G \times_{W(k)} \phi^{-1} G \phi) \cap \mathbf{GL}_{M, \phi^{-1}(M)}$.

We have $(g_3[m], \phi^{-1}(g_2^{-1}g_3g_1)[m]\phi) \in G_{B(k), M, \phi^{-1}(M)}^*(W_m(k))$, cf. first before last paragraph and axiom (AX1) which implies that $\phi^{-1}g_2^{-1}g_3g_1\phi \in G(B(k))$. Let $\tilde{h} \in \tilde{\mathcal{H}}^G(W(k))$ be the unique element such that we have $\Theta(\tilde{h}[m]) = (g_3[m], \phi^{-1}(g_2^{-1}g_3g_1)[m]\phi)$ (cf. previous paragraph). Therefore $\tilde{\mathcal{P}}^G(\tilde{h}[m]) = g_3[m]$ and the linear automorphisms of $\phi^{-1}(M)/p^m \phi^{-1}(M)$ induced by \tilde{h} and $\phi^{-1}(g_2^{-1}g_3g_1)[m]\phi$ coincide (i.e. $\phi(\tilde{h}[m]) = (g_2^{-1}g_3g_1)[m]$). Thus we compute $\mathbb{T}_m^G(\tilde{h}[m], g_1[m]) = g_3[m]g_1[m]((g_2^{-1}g_3g_1)[m])^{-1} = g_2[m]$. \square

There exist upper bounds of n_D^G which depend only on r and on the closed embedding homomorphism $G \hookrightarrow \mathbf{GL}_M$, cf. [Va1, Main Thm. A and Example 3.1.5]. The following consequences of Lemma 5 and of the existence of such upper bounds of n_D^G are shown similarly to Corollary 4 (a) to (c).

Corollary 7 (a) *The projective limit $\mathcal{O}_\infty^G := \text{proj.lim.}_{m \rightarrow \infty} \mathcal{O}_m^G$ in the category of ringed spaces is also a projective limit in the category of k -schemes and it is a reduced, quasi-compact, locally closed subscheme of \mathcal{D}_∞^G whose k -valued points form one orbit of the action $\mathbb{T}_\infty^G(k) : \mathcal{H}_\infty^G(k) \times \mathcal{D}_\infty^G(k) \rightarrow \mathcal{D}_\infty^G(k)$ in the category of sets. Thus \mathcal{O}_∞^G is the orbit of $1_M \in \mathcal{D}_\infty^G(k)$ under the action \mathbb{T}_∞^G .*

(b) *The set of orbits of \mathbb{T}_∞^G is in natural bijection to the set of (representatives of) inner isomorphism classes of triples of the form $(M, g\phi, \vartheta g, G)$ with $g \in G(W(k))$.*

(c) *If K is an algebraically closed field that contains k , then we have $n_{D^K}^{G_{W(K)}} = n_D^G$.*

We note that the proof of Corollary 7 (b) does not require the use of the well positioned property mentioned in the proof of Lemma 5.

The generalizations of Theorems 2, 3, and 4 to the relative context provided by (M, ϕ, G) is automatic. For instance, if \mathcal{T}_{m+1}^G is the reduced group of $(\rho_{m+1}^G)^{-1}(\mathcal{S}_m^G)$ and if \mathcal{V}_{m+1}^G is the inverse image of the point $1_M[m] \in \mathcal{O}_m^G(k)$ under the epimorphism $\tau_{m+1}^G : \mathcal{D}_{m+1}^G \twoheadrightarrow \mathcal{D}_m^G$, then the set of orbits of the action \mathbb{T}_{m+1}^G that map onto \mathcal{O}_m^G is in a natural bijection to the set of orbits of the action $\mathcal{T}_{m+1}^G \times_k \mathcal{V}_{m+1}^G \rightarrow \mathcal{V}_{m+1}^G$ induced via restriction by \mathbb{T}_{m+1}^G . Moreover, \mathcal{V}_{m+1}^G is isomorphic to $\mathbb{A}_k^{d_G}$, $\mathcal{T}_{m+1}^{G,0}$ is unipotent, we have a short exact sequence $1 \rightarrow \mathbb{G}_a^{d_G} \rightarrow \mathcal{T}_{m+1}^G \rightarrow \mathcal{C}_{m+1}^G \rightarrow 1$, etc. Thus in all that follows we will concentrate on the generalization of Theorem 1 and of its corollaries.

Lemma 6 *We assume that $n_D = 0$ (i.e. D is either étale or of multiplicative type). Then we have $n_D^G \in \{0, 1\}$. If moreover the special fibre G_k is connected, then we have $n_D^G = 0$.*

Proof: As $n_D = 0$, the image of μ is either trivial or equal to the center of \mathbf{GL}_M . Thus $\mathcal{W} = \mathbf{GL}_{M/pM}$, μ centralizes G , and we have $\mathcal{W}^G = G_k$. Let $\sigma_\phi := \phi\mu(p) : M \rightarrow M$; it is a σ -linear automorphism of M which normalizes G and which acts on $G(B(k))$ in the same way as ϕ . The \mathbb{Z}_p -module $M_{\mathbb{Z}_p} := \{x \in M \mid \sigma_\phi(x) = x\}$ is a \mathbb{Z}_p structure of M (i.e. we have

$M = W(k) \otimes_{\mathbb{Z}_p} M_{\mathbb{Z}_p}$) and $\mathfrak{g}_{\mathbb{Z}_p} := \{x \in \mathfrak{g} \mid \sigma_\phi(x) = x\} = \mathfrak{g} \cap \text{End}(M_{\mathbb{Z}_p})$ is a \mathbb{Z}_p structure of \mathfrak{g} . Thus G is the pull-back to $\text{Spec } W(k)$ of a smooth closed subgroup scheme $G_{\mathbb{Z}_p}$ of $\mathbf{GL}_{M_{\mathbb{Z}_p}}$, cf. [Va4, Prop. 3.2].

If G_k is (resp. is not) connected, let $g \in G(W(k))$ (resp. let $g \in \text{Ker}(G(W(k)) \rightarrow G(k))$). We will show that there exist an inner isomorphism between $(M, g\phi, G)$ and (M, ϕ, G) . For this let s be a positive integer such that $s \geq \max\{2, n_D^G\}$. The affine group $\mathbb{K}_s := \mathbb{W}_s(G)$ (resp. the kernel \mathbb{K}_s of the natural restriction homomorphism $\mathbb{W}_s(G) \rightarrow \mathbb{W}_1(G)$) over k is connected and smooth, cf. Subsubsection 3.1.3. The endomorphism of \mathbb{K}_s induced naturally by σ_ϕ is the usual Frobenius endomorphism σ_s of \mathbb{K}_s with respect to the \mathbb{F}_p -form $\mathbb{K}_{s, \mathbb{F}_p}$ of \mathbb{K}_s defined by $\mathbb{W}_s(G_{\mathbb{Z}_p})$ (resp. by the kernel of the natural restriction homomorphism $\mathbb{W}_s(G_{\mathbb{Z}_p}) \rightarrow \mathbb{W}_1(G_{\mathbb{Z}_p})$); here the \mathbb{W}_s and \mathbb{W}_1 functors are applied over \mathbb{Z}_p . A classical theorem of Lang implies that there exists an element $h[s] \in \mathbb{K}_s(k) \subset G(W_s(k))$ such that $g[s] = h[s]^{-1} \sigma_s(h[s])$. If $h \in G(W(k))$ lifts $h[s]$, then we get that $g_1 := hg\phi(h^{-1}) \in G(W(k))$ is such that $g_1[s] = 1_M[s]$ and $hg\phi = hg\phi(h^{-1})\phi h = g_1\phi h$. From this and the very definition of $n_D^G \leq s$, we get that there exists $h_1 \in G(W(k))$ such that $h_1 g_1 \phi = \phi h_1$. We conclude that $h_1 h$ is an inner isomorphism between $(M, g\phi, G)$ and (M, ϕ, G) . Thus we have $n_D^G = 0$ (resp. $n_D^G \leq 1$). \square

Proposition 2 *The following five properties hold:*

- (a) *The natural homomorphism $\iota_m^G : \mathcal{S}_m^G \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}^G$ induced by ι_m gives an isomorphism $\iota_m^G(k) : \mathcal{S}_m^G(k) \rightarrow \mathbf{Aut}(D[p^m])_{\text{crys}}^G(k)$.*
- (b) *The sequence $(\gamma_D^G(i))_{i \in \mathbb{N}}$ is increasing.*
- (c) *The subsequence $(\gamma_D^G(i))_{i \geq n_D^G}$ is constant.*
- (d) *We assume that $n_D^G \geq 2$. Then we have $\gamma_D^G(n_D^G - 1) < \gamma_D^G(n_D^G)$.*
- (e) *The connected smooth affine groups $\mathbf{Aut}(D[p^m])_{\text{red}}^{G,0}$ and $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^{G,0}$ are unipotent.*

Proof: Due to the axiom (AX2), $\sigma_\phi := \phi\mu(p) : M \rightarrow M$ is a σ -linear automorphism of M which normalizes G . Based on this, the argument for (a) is the same as the one in the proof of [Va2, Cor. 4.3 (b)] (see second paragraph of [Va2, p. 635]). As a second proof of (a), we first remark that $\iota_m^G(k)$ is injective as $\iota_m(k)$ is so; the fact that $\iota_m^G(k)$ is onto follows directly from the proof of Lemma 5 applied with $g_1[m] = g_2[m] = 1_M[m]$.

Based on (a) we get:

$$\gamma_D^G(m) = \dim(\mathbf{Aut}(D[p^m])_{\text{crys}}^G) = \dim(\mathcal{C}_m^G) = md_G - \dim(\mathcal{O}_m^G).$$

Thus $\gamma_D^G(m+1) - \gamma_D^G(m) = d_G - \dim(\mathcal{O}_{m+1}^G) + \dim(\mathcal{O}_m^G)$. As the fibres of τ_{m+1}^G are isomorphic to $\mathbb{A}_k^{d_G}$, the faithfully flat morphism $\mathcal{O}_{m+1}^G \rightarrow \mathcal{O}_m^G$ induced by τ_{m+1}^G has fibres of dimension at most d_G . Thus $\dim(\mathcal{O}_{m+1}^G) - \dim(\mathcal{O}_m^G) \leq d_G$, i.e. $\gamma_D^G(m+1) - \gamma_D^G(m) \geq 0$. As $\gamma_D^G(1) \geq 0 = \gamma_D^G(0)$, we get that (b) holds.

If $n_D^G = 0$, then $\mathcal{O}_m^G = \mathcal{D}_m^G$ has dimension md_G and thus $\gamma_D^G(m) = 0$. As $\gamma_D^G(0) = 0$, we conclude that (c) holds if $n_D^G = 0$. Thus to prove (c) we can assume that $n_D^G \geq 1$. If $m \geq n_D^G$, then from the very definition of n_D^G we get that $\mathcal{O}_{m+1}^G = (\tau_{m+1}^G)^{-1}(\mathcal{O}_m^G)$. This implies that $\dim(\mathcal{O}_{m+1}^G) = \dim(\mathcal{O}_m^G) + d_G$, i.e. $\gamma_D^G(m+1) - \gamma_D^G(m) = 0$. Thus (c) holds.

To prove (d), it suffices to show that the equality $\gamma_D^G(n_D^G - 1) = \gamma_D^G(n_D^G)$ leads to a contradiction. This equality implies that $\dim(\mathcal{O}_{n_D^G}^G) = d_G + \dim(\mathcal{O}_{n_D^G - 1}^G)$. Therefore all fibres of the faithfully flat morphism $\mathcal{O}_{n_D^G}^G \rightarrow \mathcal{O}_{n_D^G - 1}^G$ have dimension d_G and thus, being closed subschemes of $\mathbb{A}_k^{d_G}$, are isomorphic to $\mathbb{A}_k^{d_G}$. Thus $\mathcal{O}_{n_D^G}^G = (\tau_{n_D^G}^G)^{-1}(\mathcal{O}_{n_D^G - 1}^G)$. This means that if $\tilde{g} \in \text{Ker}(G(W(k)) \rightarrow G(W_{n_D^G - 1}(k)))$, then $(M, \tilde{g}\phi, G)$ is inner isomorphic to a triple of the form $(M, \tilde{g}_1\phi, G)$ with $\tilde{g}_1 \in \text{Ker}(G(W(k)) \rightarrow G(W_{n_D^G}(k)))$ and therefore (cf. definition of n_D^G) it is inner isomorphic to (M, ϕ, G) . Thus we have $n_D^G \leq n_D^G - 1$. Contradiction. Therefore (d) holds.

Part (e) follows from the fact that $\mathbf{Aut}(D[p^m])_{\text{red}}^{G,0}$ and $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^{G,0}$ are subgroups of the unipotent groups $\mathbf{Aut}(D[p^m])_{\text{red}}^0$ and $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^0$ (respectively), cf. Theorem 5 (b) and (c) and very definitions. \square

6.2 Lie algebra group schemes of endomorphisms

For all that follows, it is convenient to also introduce the Lie algebra version of $\mathbf{Aut}(D[p^m])_{\text{crys}}^G$. Let $l, i \in \mathbb{N}$ be such that $l \geq i$. Let \sharp be the vector group scheme over $\text{Spec } W(k)$ (resp. $\text{Spec } W_m(k)$) associated to a free $W(k)$ -module (resp. $W_m(k)$ -module) \sharp of finite rank. Let $\mathbb{W}_0(\mathfrak{g}) := \text{Spec } k$.

We recall that $\mathbf{End}(D[p^l])_{\text{crys}}$ is a closed subgroup scheme of $\mathbb{W}_l(\text{End}(M))$, cf. Corollary 6. Let $\mathbf{End}(D[p^l])_{\text{crys}}^{\mathfrak{g}} := \mathbf{End}(D[p^l])_{\text{crys}} \cap \mathbb{W}_l(\mathfrak{g})$, the intersection being taken inside $\mathbb{W}_l(\text{End}(M))$. The crystalline Dieudonné functor defines a homomorphism $\mathbb{D} : \mathbf{End}(D[p^l]) \rightarrow \mathbf{End}(D[p^l])_{\text{crys}}$ which induces a bijection at the level of k -valued points. Let $\mathbf{End}(D[p^l])^{\mathfrak{g}} := \mathbb{D}^{-1}(\mathbf{End}(D[p^l])_{\text{crys}}^{\mathfrak{g}})$. The k -valued points of $\mathbf{End}(D[p^l])^{\mathfrak{g}}$ are those endomorphisms of $D[p^l]$ whose crystalline realizations belong to $\mathfrak{g}/p^l\mathfrak{g} \subset \text{End}(M/p^lM)$.

The homomorphism $\mathbf{End}(D[p^l])^{\mathfrak{g}} \rightarrow \mathbf{End}(D[p^l])_{\text{crys}}^{\mathfrak{g}}$ which is the natural

restriction of \mathbb{D} , induces a bijection at the level of k -valued points. Thus let

$$\gamma_D^{\mathfrak{g}}(l) := \dim(\mathbf{End}(D[p^l])^{\mathfrak{g}}) = \dim(\mathbf{End}(D[p^l]_{\text{crys}})^{\mathfrak{g}}).$$

We have $\gamma_D^{\mathfrak{g}}(0) = 0$.

Next we will use the notations of Subsection 2.1. Let

$$\kappa_{i,l}^{\mathfrak{g}} : \mathbf{End}(D[p^i])^{\mathfrak{g}} \hookrightarrow \mathbf{End}(D[p^l])^{\mathfrak{g}}$$

be the monomorphism induced naturally by $\kappa_{i,l}$. Let

$$r_{l,i}^{\mathfrak{g}} : \mathbf{End}(D[p^l])^{\mathfrak{g}} \rightarrow \mathbf{End}(D[p^i])^{\mathfrak{g}}$$

be the restriction homomorphism induced naturally by $r_{l,i}$. As in Subsection 2.1 we argue that we have a complex of commutative group schemes

$$0 \rightarrow \mathbf{End}(D[p^i])^{\mathfrak{g}} \xrightarrow{\kappa_{i,l}^{\mathfrak{g}}} \mathbf{End}(D[p^l])^{\mathfrak{g}} \xrightarrow{r_{l,i}^{\mathfrak{g}}} \mathbf{End}(D[p^{l-i}])^{\mathfrak{g}}$$

whose complex of groups of k -valued points is exact. This implies that:

(i) The image $\text{Im}(r_{l,i}^{\mathfrak{g}})$ has dimension $\gamma_D^{\mathfrak{g}}(l) - \gamma_D^{\mathfrak{g}}(i)$.

If $l \geq n_D$, then $\text{Im}(r_{l+1,1})$ and thus also $\text{Im}(r_{l+1,1}^{\mathfrak{g}})$ has dimension 0 (cf. Corollary 2 (a)). From this and (i) we get that:

(ii) If $l \geq n_D$, then $\gamma_D^{\mathfrak{g}}(l+1) = \gamma_D^{\mathfrak{g}}(l)$.

Theorem 6 *We assume that one of the following two conditions holds:*

(i) *The subset \mathfrak{g} of $\text{End}(M)$ is stable under products (therefore $W(k)1_M + \mathfrak{g}$ is a $W(k)$ -subalgebra of $\text{End}(M)$) and G is the group scheme of invertible elements of $1_M + \mathfrak{g}$.*

(ii) *We have $p > 2$ and G admits a Cayley transform \mathcal{U} of the form $g \mapsto (1_M - g)(1_M + g)^{-1}$ (i.e. the rule $g \mapsto (1_M - g)(1_M + g)^{-1}$ defines an isomorphism \mathcal{U} between the non-empty open subscheme of G formed by points which do not have the eigenvalue -1 and the non-empty open subscheme of \mathfrak{g} formed by points which do not have the eigenvalue -1). If $n_D = 0$, then moreover G_k is connected.*

Then the following seven properties hold:

(a) *For all $l \in \mathbb{N}$ we have $\gamma_D^G(l) = \gamma_D^{\mathfrak{g}}(l)$.*

(b) *The sequence $(\gamma_D^G(i+1) - \gamma_D^G(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} .*

(c) If $n_D^G > 0$, then we have $\gamma_D^G(1) < \gamma_D^G(2) < \cdots < \gamma_D^G(n_D^G)$.

(d) We have $n_D^G \leq n_D$.

(e) Let $l > i > 0$ be integers. Then the image of the restriction homomorphism $r_{l,i}^g : \mathbf{End}(D[p^l])^g \rightarrow \mathbf{End}(D[p^i])^g$ (or $r_{l,i,\text{crys}}^g : \mathbf{End}(D[p^l])_{\text{crys}}^g \rightarrow \mathbf{End}(D[p^i])_{\text{crys}}^g$) is finite if and only if $l - i \geq n_D^G$.

(f) Let l and i be as in (e). Then the image of the restriction homomorphism $s_{l,i}^G : \mathbf{Aut}(D[p^l])^G \rightarrow \mathbf{Aut}(D[p^i])^G$ (or $s_{l,i,\text{crys}}^G : \mathbf{Aut}(D[p^l])_{\text{crys}}^G \rightarrow \mathbf{Aut}(D[p^i])_{\text{crys}}^G$) is finite if and only if $l - i \geq n_D^G$.

(g) If $i \geq 2n_D^G$ is a positive integer, then the unipotent groups $\mathbf{Aut}(D[p^i])_{\text{red}}^{G,0}$ and $\mathbf{Aut}(D[p^i])_{\text{crys,red}}^{G,0}$ are commutative.

Proof: To prove (a) we distinguish three cases as follows.

We assume that (i) holds and $1_M \in \mathfrak{g}$ (i.e. \mathfrak{g} is a $W(k)$ -subalgebra of $\text{End}(M)$). In this case $\mathbf{Aut}(D[p^m])_{\text{crys}}^G$ is an open subscheme of $\mathbf{End}(D[p^m])_{\text{crys}}^g$ and thus (a) holds.

We assume that (i) holds and $1_M \notin \mathfrak{g}$. Then $\mathbf{Aut}(D[p^m])_{\text{crys}}^G$ is isomorphic to an open subscheme of $\mathbf{End}(D[p^m])_{\text{crys}}^g$ via the morphism which at the level of k -valued points maps an automorphism $g[m]$ to the endomorphism $g[m] - 1_M[m]$. Thus (a) holds.

We assume that (ii) holds. To check that (a) holds, we can assume $l > 0$. The isomorphism \mathcal{U} induces naturally a Cayley transform $\mathcal{U}_l : OG_l \rightarrow O\mathfrak{g}_l$ which is an isomorphism between the non-empty open subscheme OG_l of $G_{W_l(k)}$ formed by points which do not have the eigenvalue -1 and the non-empty open subscheme $O\mathfrak{g}_l$ of $\underline{\mathfrak{g}/p^l\mathfrak{g}}$ formed by points which do not have the eigenvalue -1 .

The association $\diamond \mapsto (1 - \diamond)(1 + \diamond)^{-1}$ maps endomorphisms of some pull-back of $D[p^l]$ or of some scalar extension of $(M/p^lM, \phi_l, \vartheta_l)$ to endomorphisms of the same pull-back of $D[p^l]$ or of the same scalar extension of $(M/p^lM, \phi_l, \vartheta_l)$. Therefore \mathcal{U}_l induces an isomorphism

$$\mathcal{U}_l : \mathbf{OAut}(D[p^l])_{\text{crys}}^G \rightarrow \mathbf{OEnd}(D[p^l])_{\text{crys}}^g$$

from a suitable non-empty open subscheme $\mathbf{OAut}(D[p^l])_{\text{crys}}^G$ of $\mathbf{Aut}(D[p^l])_{\text{crys}}^G$ to a suitable non-empty open subscheme $\mathbf{OEnd}(D[p^l])_{\text{crys}}^g$ of $\mathbf{End}(D[p^l])_{\text{crys}}^g$. Thus $\dim(\mathbf{Aut}(D[p^l])_{\text{crys}}^G) = \dim(\mathbf{End}(D[p^l])_{\text{crys}}^g)$. Therefore (a) holds.

Based on the property 6.2 (i) and on (a), the proofs of (b) and (c) are the same as the proofs of Theorem 1 (a) and (b) (the roles of $\mathbf{End}(D[p^m])$, $\mathbf{Aut}(D[p^m])$, and \mathbb{T}_m being replaced by $\mathbf{End}(D[p^m])^g$, $\mathbf{Aut}(D[p^m])^G$, and \mathbb{T}_m^G).

If (i) holds, then G_k is the group scheme of invertible elements of $1_{M/pM} + \mathfrak{g}/p\mathfrak{g}$ and thus it is connected. Thus to prove (d) we can use the fact that if $n_D = 0$, then G_k is connected. If $n_D = 0$, then $n_D^G = 0 = n_D$ (cf. Lemma 6 and the connectedness of G_k). Thus to prove (d) we can assume that $\min\{n_D, n_D^G\} > 0$. Let $l := n_D + 1 \geq 2$. We have $\gamma_D^{\mathfrak{g}}(l) = \gamma_D^{\mathfrak{g}}(l-1)$, cf. property 6.2 (ii). From this and (a) we get $\gamma_D^G(l) = \gamma_D^G(l-1)$. From this and (b) we get that $l = n_D + 1 \geq n_D^G + 1$. Thus (d) holds.

Based on (a) to (c), part (e) follows from the property 6.2 (i).

Part (f) follows from (e) via the three cases considered in the proof of (a). For instance, if the condition (ii) holds, then the existence of $\mathcal{U}_l : \mathbf{OAut}(D[p^l]_{\text{crys}}^G \rightarrow \mathbf{OEnd}(D[p^l]_{\text{crys}}^{\mathfrak{g}}))$ implies that $r_{l,i,\text{crys}}^{\mathfrak{g}}$ has finite image if and only if $s_{l,i,\text{crys}}^G$ has finite image. Thus indeed (e) implies (f).

The argument that $\mathbf{Aut}(D[p^i]_{\text{red}}^{G,0})$ (and thus also $\mathbf{Aut}(D[p^i]_{\text{crys,red}}^{G,0})$) is commutative if $i \geq \max\{1, 2n_D^G\}$ is the same as the one for Corollary 3 (d). Thus (g) holds. \square

6.3 The invariant v_D , exponentials, and logarithms

In order to obtain some variants of Theorem 6, we will introduce new invariants v_D and v_D^G . The connected smooth affine group $\mathbf{Aut}(D[p]_{\text{crys,red}}^0)$ is unipotent, cf. Theorem 5 (a) and (b). Thus $\mathbf{Aut}(D[p]_{\text{crys,red}}^0)$ is a subgroup of the unipotent radical of some Borel subgroup of $\mathbf{GL}_{M/pM}$. This implies that there exists a smallest non-negative integer v_D with the property that for each $g[1] \in \mathbf{Aut}(D[p]_{\text{crys}}^0(k))$, we have $(g[1] - 1_M[1])^{v_D} = 0$. We call v_D as the *unipotent number* of D . We recall that r is the height of D (i.e. the rank of M). We have $v_D \in \{0, \dots, r\}$. From Corollary 6 (b) we get:

(i) For each element $e[1] \in \mathbf{End}(D[p]_{\text{crys}}^0(k))$ we have $e[1]^{v_D} = 0$.

Let v_D^G be the smallest non-negative integer with the property that for each $g[1] \in \mathbf{Aut}(D[p]_{\text{crys}}^{G,0}(k))$ and each $e[1] \in \mathbf{End}(D[p]_{\text{crys}}^{\mathfrak{g},0}(k))$ we have $(g[1] - 1_M[1])^{v_D^G} = 0$ and $e[1]^{v_D^G} = 0$ as elements of $\text{End}(M/pM)$. We call v_D^G as the *unipotent G -number* of D . Obviously:

(ii) We have inequalities $0 \leq v_D^G \leq v_D \leq r$.

For $x \in \text{End}(M)$, let $\bar{x} \in \text{End}(M/pM)$ be its reduction modulo p . For $t \in \{1, \dots, r\}$ let $\Sigma_{1,t}(M) := p\{x \in \text{End}(M) | \bar{x}^t = 0\}$. For $p > 2$ and $s \in \{1, \dots, \min\{r, \frac{p-1}{2}\}\}$, let $\Sigma_s(M) := \{x \in \text{End}(M) | \bar{x}^s = 0\}$. Let Σ denote

either $\Sigma_{1,t}$ or Σ_s . The exponential rule $z \mapsto \sum_{i=0}^{\infty} \frac{z^i}{i!}$ defines a bijection

$$\exp : \Sigma(M) \rightarrow 1_M + \Sigma(M)$$

whose inverse

$$\log : 1_M + \Sigma(M) \rightarrow \Sigma(M)$$

is defined by the logarithmic rule $1_M + z \mapsto \sum_{i=1}^{\infty} \frac{(-1)^{i-1} z^i}{i}$, cf. Proposition 6 (b) or 7 (a) of Appendix B. Let $\Sigma^{\mathfrak{g}} := \Sigma(M) \cap \mathfrak{g}$ and $\Sigma^G := \{g \in G(W(k)) \mid g - 1_M \in \Sigma(M)\}$. Let $\Sigma^{\mathfrak{g}}[m]$ (resp. $\Sigma^G[m]$) be the image of $\Sigma^{\mathfrak{g}}$ (resp. of Σ^G) in $\mathfrak{g}/p^m \mathfrak{g}$ (resp. in $G(W_m(k))$). From Proposition 7 (a) of Appendix B we get:

(iii) Restricting \exp to $\Sigma^{\mathfrak{g}}$ and \log to Σ^G we get inverse bijections $\Sigma^{\mathfrak{g}} \xrightleftharpoons[\log]{\exp} \Sigma^G$

which induce inverse bijections $\Sigma^{\mathfrak{g}}[m] \xrightleftharpoons[\log_m]{\exp_m} \Sigma^G[m]$.

Let $\mathcal{D}_{m,\Sigma}^G$ be the reduced closed subgroup scheme of \mathcal{D}_m^G whose k -valued points are $\Sigma^G[m]$. Let $\mathbb{W}_{m,\Sigma}(\mathfrak{g})$ be the reduced closed subgroup scheme of $\mathbb{W}_m(\mathfrak{g})$ whose k -valued points are $\Sigma^{\mathfrak{g}}[m]$. Let $\Omega_m^G := \text{Ker}(s_{m,1,\text{crys}}^G)_{\text{red}}^0$, where $s_{m,1,\text{crys}}^G : \mathbf{Aut}(D[p^m])_{\text{crys}}^G \rightarrow \mathbf{Aut}(D[p])_{\text{crys}}^G$ is the natural restriction homomorphism; it is a closed subgroup of $\mathcal{D}_{m,1}^G := \text{Ker}(\tau_2^G \circ \dots \circ \tau_m^G : \mathcal{D}_m^G \rightarrow \mathcal{D}_1^G)$. Let $\Omega_m^{\mathfrak{g}} := \text{Ker}(r_{m,1,\text{crys}}^{\mathfrak{g}})_{\text{red}}^0$, where $r_{m,1,\text{crys}}^{\mathfrak{g}} : \mathbf{End}(D[p^m])_{\text{crys}}^{\mathfrak{g}} \rightarrow \mathbf{End}(D[p])_{\text{crys}}^{\mathfrak{g}}$ is the natural restriction homomorphism; it is a closed subgroup scheme of $\mathbb{W}_{m,1}(\mathfrak{g}) := \text{Ker}(\mathbb{W}_m(\mathfrak{g}) \rightarrow \mathbb{W}_1(\mathfrak{g}))$.

If $e_m \in \Sigma^{\mathfrak{g}}[m]$ (resp. $e_m \in \Sigma^G[m]$) is the crystalline realization of an endomorphism (resp. automorphism) of $D[p^m]$, i.e. is a k -valued point of $\mathbf{End}(D[p^m])_{\text{crys}}^{\mathfrak{g}}$ (resp. of $\mathbf{Aut}(D[p^m])_{\text{crys}}^G$), then $\exp_m(e_m) \in \Sigma^G[m]$ (resp. $\log_m(e_m) \in \Sigma^{\mathfrak{g}}[m]$) is the crystalline realization of an automorphism (resp. endomorphism) of $D[p^m]$ (cf. Proposition 7 (b) of Appendix B). From this, the property (iii), and the Proposition 6 (c) of Appendix B we get the following two properties.

(iv) If p is arbitrary and $\Sigma = \Sigma_{1,t}$, then there exists an isomorphism $\mathcal{D}_{m,\Sigma}^G \rightarrow \mathbb{W}_{m,\Sigma}(\mathfrak{g})$ which on k -valued points is induced by \log_m and whose inverse is induced on k -valued points by \exp_m . For $t \geq v_D$ the isomorphism $\mathcal{D}_{m,\Sigma}^G \rightarrow \mathbb{W}_{m,\Sigma}(\mathfrak{g})$ restricts to an isomorphism $\Omega_m^G \rightarrow \Omega_m^{\mathfrak{g}}$. If $p > 2$, then the isomorphism $\mathcal{D}_{m,\Sigma}^G \rightarrow \mathbb{W}_{m,\Sigma}(\mathfrak{g})$ is the restriction of an isomorphism $\mathcal{D}_{m,1}^G \rightarrow \mathbb{W}_{m,1}(\mathfrak{g})$ which on k -valued points is induced by \log_m and whose inverse is induced on k -valued points by \exp_m .

(v) If $p > 2$ and $\Sigma = \Sigma_s$ with $s \in \{1, \dots, \min\{r, \frac{p-1}{2}\}\}$, then there exists an isomorphism $\mathcal{D}_{m,\Sigma}^G \rightarrow \mathbb{W}_{m,\Sigma}(\mathfrak{g})$ which on k -valued points is induced by \log_m and whose inverse is induced on k -valued points by \exp_m . If $v_D^G \leq \frac{p-1}{2}$, then for $s \geq v_D^G$ the mentioned isomorphism restricts to an isomorphism $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^{G,0} \rightarrow \mathbf{End}(D[p^m])_{\text{crys,red}}^{\mathfrak{g},0}$.

Proposition 3 *The following two properties hold:*

- (a) *If $l \geq n_D + 1$, then $\gamma_D^G(l) = \gamma_D^{\mathfrak{g}}(l)$.*
- (b) *We have $n_D^G \leq n_D + 1$.*

Proof: If $l \geq n_D + 1$, then from Corollary 2 (a) we get that we have identities $\Omega_l^G = \mathbf{Aut}(D[p^l])_{\text{crys,red}}^{G,0}$ and $\Omega_l^{\mathfrak{g}} = \mathbf{End}(D[p^l])_{\text{crys,red}}^{\mathfrak{g},0}$. Thus (a) follows from the property 6.3 (iv).

From (a) and the property 6.2 (ii) we get that the sequence $(\gamma_D^G(l))_{l \geq n_D + 1}$ is constant. To prove (b) we can assume $n_D^G \geq 2$. From the last two sentences and Proposition 2 (d), we get that $n_D^G \leq n_D + 1$ (i.e. (b) holds). \square

Theorem 7 *We assume that p is odd and that $v_D^G \leq \frac{p-1}{2}$ (for instance, these hold if $2 \leq 2r < p$). If $n_D = 0$, then we assume that G_k is connected. Then the seven properties of Theorem 6 hold.*

Proof: As in the proof of Theorem 6, it suffices to show that the statement (a) of Theorem 6 holds. We take $\Sigma := \Sigma_{v_D^G}$. Thus we have an isomorphism $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^{G,0} \rightarrow \mathbf{End}(D[p^m])_{\text{crys,red}}^{\mathfrak{g},0}$, cf. property 6.3 (v). Therefore the statement (a) of Theorem 6 holds. \square

6.4 Remarks

We end this section with three remarks.

(a) Subsubsections 3.1.2 and 3.2.4 can be as well adapted to the relative context provided by G . For instance, the group scheme over $\text{Spec } W(k)$ defined by the intersection $\mathbf{Aut}(\phi, \vartheta)^G := \mathbf{Aut}(\phi, \vartheta) \cap (G^{(\sigma)} \times_{W(k)} G)$ taken inside $\mathbf{GL}_{M(\sigma)} \times_{W(k)} \mathbf{GL}_M$, is naturally isomorphic to $(\tilde{\mathcal{H}}^G)^{(\sigma)}$. One ends up with an action $\mathbb{T}_m^{G,\sigma} \mathcal{H}_m^{G,\sigma} \times_k \mathcal{D}_m^{G,\sigma} \rightarrow \mathcal{D}_m^{G,\sigma}$ isomorphic to the action $\mathbb{T}_m^{G,(\sigma)}$.

(b) Referring to properties 6.3 (iv) and (v), their isomorphisms $\Omega_m^G \rightarrow \Omega_m^{\mathfrak{g}}$ and $\mathbf{Aut}(D[p^m])_{\text{crys,red}}^{G,0} \rightarrow \mathbf{End}(D[p^m])_{\text{crys,red}}^{\mathfrak{g},0}$ are based on the closed subgroup scheme G of \mathbf{GL}_M . One gets variants of these isomorphisms working with

either the closed subgroup scheme $\phi^{-1}G\phi$ of $\mathbf{GL}_{\phi^{-1}(M)}$ or the closed subgroup scheme $\tilde{\mathcal{H}}^G$ of $\mathbf{GL}_{M, \phi^{-1}(M)}$ or the closed subgroup scheme $\mathbf{Aut}(\phi, \vartheta)^G$ of $\mathbf{GL}_{M(\sigma)} \times_{W(k)} \mathbf{GL}_M$. For instance, working with $\tilde{\mathcal{H}}^G$, the role played by $\mathbf{Aut}(D[p^m])_{\text{crys, red}}$ is played by \mathcal{C}_m^G and the role played by $\mathbf{End}(D[p^m])_{\text{crys, red}}$ is played by the reduced closed subgroup scheme of $\mathbb{W}_m(\underline{\text{Lie}}(\tilde{\mathcal{H}}^G))$ whose k -valued points are elements $e_m \in \text{Lie}(\tilde{\mathcal{H}}^G)/p^m \text{Lie}(\tilde{\mathcal{H}}^G)$ which have a lift $e \in \text{Lie}(\tilde{\mathcal{H}}^G)$ such that we have $\phi(e) - e \in p^m \mathfrak{g}$ (here we view $\text{Lie}(\tilde{\mathcal{H}}^G)$ as a Lie subalgebra of \mathfrak{g} via the differential map $d\tilde{\mathcal{P}}^G$ of $\tilde{\mathcal{P}}^G$). Moreover, all these isomorphisms are compatible with the different isomorphisms and homomorphisms between the four groups G , $\phi^{-1}G\phi$, $\tilde{\mathcal{H}}^G$, $\mathbf{Aut}(\phi, \vartheta)^G$, and their pull-backs via σ , as one can easily check based on Fact 4 of Appendix B.

(c) Axiom (AX2) was used only in the proofs of Lemmas 4 and 5 and Proposition 2 (a). Thus all the results of this section continue to hold even if the axiom (AX2) is replaced by the following weaker version of it.

(AX2') The intersection $\mathcal{W}^G = G_k \cap \mathcal{W}$ is a smooth subgroup of G_k and $G_{B(k)}$ is well positioned with respect to $(M, \phi^{-1}(M))$.

7 Examples

In this section we exemplify the results of Section 6 through three simple situations that are of special interest. Expressions of the form ϕ_1 and ϑ_1 will have a meaning different from the one before Subsection 3.1.

7.1 The homomorphism context

Let D_1 and D_2 be two p -divisible groups over k . For $j \in \{1, 2\}$ let $(M_j, \phi_j, \vartheta_j)$ be the contravariant Dieudonné module of D_j . We take $D := D_1 \oplus D_2$. We have $(M, \phi, \vartheta) = (M_1, \phi_1, \vartheta_1) \oplus (M_2, \phi_2, \vartheta_2)$ and a direct sum decomposition $\text{End}(M) = \text{End}(M_1) \oplus \text{End}(M_2) \oplus \text{Hom}(M_1, M_2) \oplus \text{Hom}(M_2, M_1)$ into $W(k)$ -modules. Let G be the smooth integral closed subgroup scheme of \mathbf{GL}_M whose group of valued points in a commutative $W(k)$ -algebra R is

$$G(R) = 1_{R \otimes_{W(k)} M} + R \otimes_{W(k)} \text{Hom}(M_2, M_1).$$

We have $\mathfrak{g} := \text{Lie}(G) = \text{Hom}(M_2, M_1)$. It is easy to see that axioms (AX1) and (AX2) hold for the triple (M, ϕ, G) (in connection to (AX2) one has to

take $M = F^1 \oplus F^0$ such that we have $F^j = (F^j \cap M_1) \oplus (F^j \cap M_2)$ for each $j \in \{1, 2\}$. Moreover, the condition (i) of Theorem 6 holds.

Let n_{D_1, D_2} be the smallest non-negative integer for which the following statement holds. If E is a p -divisible group over k equipped with a short exact sequence $0 \rightarrow D_2 \rightarrow E \rightarrow D_1 \rightarrow 0$ whose truncation of level n_{D_1, D_2} splits, then the short exact sequence $0 \rightarrow D_2 \rightarrow E \rightarrow D_1 \rightarrow 0$ splits. The contravariant Dieudonné module of every p -divisible group \tilde{E} over k equipped with a short exact sequence $0 \rightarrow D_2 \rightarrow \tilde{E} \rightarrow D_1 \rightarrow 0$ is isomorphic to $(M, g\phi, \vartheta g^{-1})$ for some arbitrary element $g \in G(W(k))$. Based on this one easily checks that $n_{D_1, D_2} = n_D^G$ (to be compared with [Va1, Lemma 3.2.2]).

For $i \in \mathbb{N}$ let $\mathbf{Hom}(D_1[p^i], D_2[p^i])$ be the group scheme over k of homomorphisms from $D_1[p^i]$ to $D_2[p^i]$. Let $\gamma_{D_1, D_2}(i) := \dim(\mathbf{Hom}(D_1[p^i], D_2[p^i]))$. One can naturally identify $\mathbf{Hom}(D_1[p^i], D_2[p^i])_{\text{red}}$ with $\mathbf{End}(D)_{\text{red}}^g$ as well as $\mathbf{Aut}(D[p^i])_{\text{red}}^G$ with $1_{D[p^i]} + \mathbf{Hom}(D_1[p^i], D_2[p^i])_{\text{red}}$. Therefore $\gamma_D^G(i) = \gamma_{D_1, D_2}(i)$. Thus from Theorem 6 and Proposition 2 (c) we get that:

- (i) If $n_{D_1, D_2} > 0$, then $\gamma_{D_1, D_2}(1) < \gamma_{D_1, D_2}(2) < \cdots < \gamma_{D_1, D_2}(n_{D_1, D_2})$.
- (ii) The sequence $(\gamma_{D_1, D_2}(i+1) - \gamma_{D_1, D_2}(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} and for $i \geq n_{D_1, D_2}$ we have $\gamma_{D_1, D_2}(i) = \gamma_{D_1, D_2}(n_{D_1, D_2})$. Moreover we have $n_{D_1, D_2} \leq n_{D_1 \oplus D_2}$.
- (iii) For integers $l > i > 0$, the image of the restriction homomorphism $\mathbf{Hom}(D_1[p^l], D_2[p^l]) \rightarrow \mathbf{Hom}(D_1[p^i], D_2[p^i])$ is finite if and only if $l - i \geq n_{D_1, D_2}$.

7.2 The filtered context

We assume that D has an increasing filtration \mathcal{F} of the form

$$0 = D_0 \subset D_1 \subset \cdots \subset D_{s-1} \subset D_s = D.$$

Let M_i be the direct summand of M such that M/M_i defines the contravariant Dieudonné module of D_i . We have a decreasing filtration

$$0 = M_s \subset \cdots \subset M_1 \subset M_0 = M.$$

Let G be the parabolic subgroup scheme of \mathbf{GL}_M that normalizes each M_j with $j \in \{0, \dots, s\}$. We have $\mathfrak{g} := \text{Lie}(G) = \{e \in \text{End}(M) \mid e(M_j) \subset M_j \forall j \in \{0, \dots, s\}\}$. It is easy to see that axioms (AX1) and (AX2) hold for the triple (M, ϕ, G) . Moreover, the condition (i) of Theorem 6 holds.

Let $n_{\mathcal{F}}$ be the smallest non-negative integer for which the following statement holds. If D' is a p -divisible group over k equipped with an increasing filtration \mathcal{F}' of the form $0 = D'_0 \subset D'_1 \subset \cdots \subset D'_{s-1} \subset D'_s = D'$ whose truncation of level $n_{\mathcal{F}}$ is isomorphic to the truncation of level $n_{\mathcal{F}}$ of \mathcal{F} and whose factors D'_{j+1}/D'_j have the same dimension and codimension as D_{j+1}/D_j for all $j \in \{0, \dots, s-1\}$, then \mathcal{F}' is isomorphic to \mathcal{F} . The contravariant Dieudonné module of each p -divisible group D' equipped with an increasing filtration \mathcal{F}' of the form $0 = D'_0 \subset D'_1 \subset \cdots \subset D'_{s-1} \subset D'_s = D'$ whose factors D'_{j+1}/D'_j have the same dimension and codimension as D_{j+1}/D_j for all $j \in \{0, \dots, s-1\}$, is isomorphic to $(M, g\phi, \vartheta g^{-1})$ for some arbitrary element $g \in G(W(k))$. Based on this one easily checks that $n_{\mathcal{F}} = n_D^G$ (to be compared with [Val, Lemma 3.2.2]).

For $i \in \mathbb{N}$, let $\mathbf{Aut}_{\mathcal{F}}(D[p^i])$ (resp. $\mathbf{End}_{\mathcal{F}}(D[p^i])$) be the group scheme of automorphisms (resp. endomorphisms) of the filtered truncated Barsotti–Tate group $0 = D_0[p^i] \subset D_1[p^i] \subset \cdots \subset D_{s-1}[p^i] \subset D_s[p^i] = D[p^i]$. Thus $\mathbf{Aut}_{\mathcal{F}}(D[p^i])$ (resp. $\mathbf{End}_{\mathcal{F}}(D[p^i])$) is a closed subgroup scheme of $\mathbf{Aut}(D[p^i])$ (resp. $\mathbf{End}(D[p^i])$) with the property for a commutative k -algebra R and for $e_R \in \mathbf{Aut}(D[p^i])(R)$ (resp. $e_R \in \mathbf{End}(D[p^i])(R)$) we have $e_R \in \mathbf{Aut}_{\mathcal{F}}(D[p^i])(R)$ (resp. $e_R \in \mathbf{End}_{\mathcal{F}}(D[p^i])(R)$) if and only if e_R maps $D_j[p^i]_R$ into itself for all $j \in \{0, \dots, s\}$. Each $\mathbf{Aut}_{\mathcal{F}}(D[p^i])$ is an open (as well as closed) subscheme of $\mathbf{End}_{\mathcal{F}}(D[p^i])$ and thus we can define $\gamma_{\mathcal{F}}(i) := \dim(\mathbf{Aut}_{\mathcal{F}}(D[p^i])) = \dim(\mathbf{End}_{\mathcal{F}}(D[p^i]))$. It is easy to see that $\mathbf{Aut}_{\mathcal{F}}(D[p^i])_{\text{red}} = \mathbf{Aut}(D[p^i])_{\text{red}}^G$ and $\mathbf{End}_{\mathcal{F}}(D[p^i])_{\text{red}} = \mathbf{End}(D[p^i])_{\text{red}}^{\mathfrak{g}}$. Thus $\gamma_{\mathcal{F}}(i) = \gamma_D^G(i)$. From Theorem 6 and Proposition 2 (c) we get that:

- (i) If $n_{\mathcal{F}} > 0$, then we have $\gamma_{\mathcal{F}}(1) < \gamma_{\mathcal{F}}(2) < \cdots < \gamma_{\mathcal{F}}(n_{\mathcal{F}})$.
- (ii) The sequence $(\gamma_{\mathcal{F}}(i+1) - \gamma_{\mathcal{F}}(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} and for $i \geq n_{\mathcal{F}}$ we have $\gamma_{\mathcal{F}}(i) = \gamma_{\mathcal{F}}(n_{\mathcal{F}})$. Moreover we have $n_{\mathcal{F}} \leq n_D$.
- (iii) For integers $l > i > 0$, the image of the restriction homomorphism $\mathbf{End}_{\mathcal{F}}(D[p^l]) \rightarrow \mathbf{End}_{\mathcal{F}}(D[p^i])$ is finite if and only if $l - i \geq n_{\mathcal{F}}$.
- (iv) If $i \geq 2n_{\mathcal{F}}$ is an integer, then the unipotent group $\mathbf{Aut}_{\mathcal{F}}(D[p^i])_{\text{red}}^0$ is commutative.

7.3 The principally quasi-polarized context

Let D^{\natural} be the Cartier dual of D . We assume that there exists an isomorphism $\lambda : D \rightarrow D^{\natural}$ such that the perfect bilinear form $\psi : M \times M \rightarrow W(k)$ associated naturally to λ is symmetric (resp. is alternating). If $p = 2$ and ψ

is symmetric, we also assume that ψ modulo 2 is alternating. We refer to λ as a symmetric principal (resp. a principal) quasi-polarization of D .

We have $c = d > 0$. Let $G := \mathbf{SO}(q)$, where $q : M \rightarrow W(k)$ is the quadratic form defined by the rule $q(x) = \frac{1}{2}\psi(x, x)$ (resp. let $G := \mathbf{Sp}(M, \psi)$). The group scheme G is \mathbb{G}_m (resp. is \mathbf{SL}_2) if $d = 1$ and it is semisimple if $d > 1$ (see [Va5, Subsect. 3.1 and Prop. 3.4] for the case when $p = 2$ and ψ is symmetric). It is easy to see that axioms (AX1) and (AX2) hold for the triple (M, ϕ, G) .

Let $n_{D,\lambda}$ be the smallest non-negative integer n for which the following statement holds: if (D', λ') is another p -divisible group of dimension d over k equipped with a symmetric principal (resp. with a principal) quasi-polarization such that $(D'[p^n], \lambda'[p^n])$ is inner isomorphic (resp. is isomorphic) to $(D[p^n], \lambda[p^n])$, then (D', λ') is isomorphic to (D, λ) . Here, in the case when ψ is symmetric, by an inner isomorphism $(D'[p^n], \lambda'[p^n]) \rightarrow (D[p^n], \lambda[p^n])$ we mean an isomorphism defined at the level of Dieudonné modules by an isomorphism $(M/p^n M, \phi_n, \vartheta_n, q_n) \rightarrow (M'/p^n M', \phi'_n, \vartheta_n, q'_n)$, where the left lower indexes n mean reduction modulo p^n .

We always have $n_{D,\lambda} \geq 1$. We have $n_D^G = 0$ if and only if $d = 1$ and ψ is symmetric. If $n_D^G \geq 1$, it is well known that $n_{D,\lambda} = n_D^G$ (if ψ is alternating, see [Va2, Example 4.5]; the symmetric case is similar). For $i \in \mathbb{N}$, let $\gamma_{D,\lambda}(i)$ be the dimension of the group scheme $\mathbf{Inn}(D[p^i], \lambda[p^i])$ (resp. $\mathbf{Aut}(D[p^i], \lambda[p^i])$) of inner automorphisms (resp. of automorphisms) of $(D[p^i], \lambda[p^i])$. It is easy to see that $\mathbf{Inn}(D[p^i], \lambda[p^i])_{\text{red}} = \mathbf{Aut}(D[p^i])_{\text{red}}^G$ (resp. $\mathbf{Aut}(D[p^i], \lambda[p^i])_{\text{red}} = \mathbf{Aut}(D[p^i])_{\text{red}}^G$). Thus $\gamma_{D,\lambda}(i) = \gamma_D^G(i)$.

If $p > 2$, then G admits a Cayley transform of the form $g \mapsto (1_M - g)(1_M + g)^{-1}$ and thus Theorem 6 applies. In particular, for $p > 2$ and $d > 1$ (resp. for $p > 2$) we have $n_{D,\lambda} = n_D^G \leq n_D$. If $p = 2$ and $d > 1$ (resp. if $p = 2$), then from Proposition 3 (b) we get the weaker fact that $n_{D,\lambda} = n_D^G \leq n_D + 1$.

If $p > 2$ and $d > 1$ (resp. if $p > 2$), then from Theorem 6 we also get that:

- (i) We have $\gamma_{D,\lambda}(1) < \gamma_{D,\lambda}(2) < \cdots < \gamma_{D,\lambda}(n_{D,\lambda})$.
- (ii) The sequence $(\gamma_{D,\lambda}(i+1) - \gamma_{D,\lambda}(i))_{i \in \mathbb{N}}$ is a decreasing sequence in \mathbb{N} and for $i \geq n_{D,\lambda}$ we have $\gamma_{D,\lambda}(i) = \gamma_{D,\lambda}(n_{D,\lambda})$.
- (iii) For integers $l > i > 0$, the restriction homomorphism $\mathbf{Inn}(D[p^l], \lambda[p^l]) \rightarrow \mathbf{Inn}(D[p^i], \lambda[p^i])$ (resp. $\mathbf{Aut}(D[p^l], \lambda[p^l]) \rightarrow \mathbf{Aut}(D[p^i], \lambda[p^i])$) has a finite image if and only if $l - i \geq n_{D,\lambda}$.
- (iv) If $i \geq 2n_{D,\lambda}$ is an integer, then the unipotent group $\mathbf{Inn}(D[p^i], \lambda[p^i])_{\text{red}}^0$ (resp. $\mathbf{Aut}(D[p^i], \lambda[p^i])_{\text{red}}^0$) is commutative.

The notations of the below appendices will be independent from the previous notations of the paper.

8 Appendix A: affine group schemes over discrete valuation rings

Let R be an arbitrary discrete valuation ring. Let K be the field of fractions of R and let π be a uniformizer of R . Let $k := R/(\pi)$ be the residue field of R . Let $H = \text{Spec } Q$ be a flat, affine group scheme over $\text{Spec } R$. Let $J = \text{Spec } Q/I$ be a closed subgroup scheme of H_k ; thus I is an ideal of Q which contains $Q\pi$. Let Q' be the R -subalgebra of $Q[\frac{1}{\pi}]$ generated by all elements of the form $\frac{x}{\pi}$ with $x \in I$; it contains Q . See [BLR, Ch. 3, Sect. 3.2] for dilatations. The dilatation of H centered on J is the flat, affine group scheme $H' = \text{Spec } Q'$ over $\text{Spec } R$ which is uniquely determined by the following two properties (they follow directly from the very description of Q' ; see [BLR, Ch. 3, Sect. 3.2, Props. 1, 2, and 3]):

- (i) there exists a homomorphism $f : H' \rightarrow H$ that corresponds to the R -monomorphism $Q \hookrightarrow Q'$;
- (ii) a morphism $g : X \rightarrow H$ of flat $\text{Spec } R$ -schemes factors (uniquely) through H' if and only if the morphism $g_k : X_k \rightarrow H_k$ factors through J .

By applying (ii) with X a $\text{Spec } K$ -scheme, we get that f_K is an isomorphism of $\text{Spec } K$ -schemes that corresponds to the identity $Q[\frac{1}{\pi}] = Q'[\frac{1}{\pi}]$. If H and J are smooth, then H' is also smooth (cf. loc. cit.). If \tilde{H} is a flat, closed subgroup scheme of H and if $\tilde{J} := J \cap \tilde{H}_k$, then the dilatation \tilde{H}' of \tilde{H} centered on \tilde{J} comes equipped with a homomorphism $\tilde{H}' \rightarrow H'$ (cf. (ii)). It is easy to see (cf. loc. cit.) that:

- (iii) the homomorphism $\tilde{H}' \rightarrow H'$ is a closed embedding.

Let V be a finite dimensional K -vector space. By an R -lattice of V we mean an R -submodule of V generated by a K -basis of V . Let M and M' be two lattices of V such that we have $\pi M' \subset M \subset M'$. We consider a direct sum decomposition $M = F^1 \oplus F^0$ into free R -modules such that we have $M' = \pi^{-1}F^1 \oplus F^0$. Let $\lambda : \mathbb{G}_m \rightarrow \mathbf{GL}_V$ be the cocharacter defined by the rule: $t \in \mathbb{G}_m(K)$ fixes $F^0[\frac{1}{\pi}]$ and acts as the multiplication by t^{-1} on $F^1[\frac{1}{\pi}]$.

Let G be a closed subgroup scheme of \mathbf{GL}_V . Let G_M and $G_{M'}$ be the schematic closures of G in \mathbf{GL}_M and $\mathbf{GL}_{M'}$ (respectively); they are flat,

affine group schemes over $\text{Spec } R$. Let $G_{M,M'}$ be the schematic closure of G in $\mathbf{GL}_M \times_R \mathbf{GL}_{M'}$ embedded diagonally into the generic fibre of $\mathbf{GL}_M \times_R \mathbf{GL}_{M'}$.

Example 1 Suppose $G = \mathbf{GL}_V$. Then $G_M = \mathbf{GL}_M$, $G_{M'} = \mathbf{GL}_{M'}$, and we claim that $G_{M,M'}$ is the group scheme H over $\text{Spec } R$ that represents the functor of automorphisms of the pair of R -linear maps $M \xrightleftharpoons[\pi]{\iota} M'$, where $\iota : M \hookrightarrow M'$ is the inclusion. As $\lambda(\pi^{-1})$ maps M' isomorphically onto M , H is isomorphic to the group scheme $\mathbf{Aut}(\iota_1, \iota_2)$ over $\text{Spec } R$ that represents the functor of automorphisms of the pair of R -linear maps $M \xrightleftharpoons[\iota_2]{\iota_1} M$, where $\iota_1 : M \hookrightarrow M$ and $\iota_2 : M \hookrightarrow M$ map $(x, y) \in F^1 \oplus F^0 = M$ to $(\pi x, y)$ and $(x, \pi y)$ (respectively). For a commutative R -algebra S , we write an S -linear endomorphism of $S \otimes_R (F^1 \oplus F^0)$ in the form $\begin{pmatrix} s & t \\ u & v \end{pmatrix}$, where $s \in \text{End}(S \otimes_R F^1)$, $t \in \text{Hom}(S \otimes_R F^0, S \otimes_R F^1)$, $u \in \text{Hom}(S \otimes_R F^1, S \otimes_R F^0)$, and $v \in \text{End}(S \otimes_R F^0)$. The subgroup $\mathbf{Aut}(\iota_1, \iota_2)(S)$ of $\mathbf{GL}_M(S) \times \mathbf{GL}_M(S)$ is formed by all pairs of the form $\left(\begin{pmatrix} s & t \\ \pi u & v \end{pmatrix}, \begin{pmatrix} s & \pi t \\ u & v \end{pmatrix} \right)$ which are invertible. From this it follows that H is flat (in fact even smooth) and thus it is $G_{M,M'}$. The description of the subgroups $\mathbf{Aut}(\iota_1, \iota_2)(S)$ also implies that the following three properties hold:

(a) the first projection homomorphism $\mathbf{Aut}(\iota_1, \iota_2) \rightarrow \mathbf{GL}_M$ and thus also $\mathbf{GL}_{M,M'} \rightarrow \mathbf{GL}_M$ is the dilatation of \mathbf{GL}_M centered on the parabolic subgroup P_k of $\mathbf{GL}_{M/\pi M}$ that normalizes the k -vector subspace $\pi M'/\pi M = F^1/\pi F^1$ of $M/\pi M$;

(b) similarly, the second projection homomorphism $\mathbf{Aut}(\iota_1, \iota_2) \rightarrow \mathbf{GL}_M$ (resp. $\mathbf{GL}_{M,M'} \rightarrow \mathbf{GL}_{M'}$) is the dilatation of \mathbf{GL}_M (resp. of $\mathbf{GL}_{M'}$) centered on the parabolic subgroup P'_k of $\mathbf{GL}_{M/\pi M}$ (resp. of $\mathbf{GL}_{M'/\pi M'}$) that normalizes the k -vector subspace $F^0/\pi F^0$ of $M/\pi M$ (resp. of $M'/\pi M'$);

(c) the special fibre $\mathbf{Aut}(\iota_1, \iota_2)_k$ (and thus also H_k) is connected.

Example 2 In general, the homomorphism $G_{M,M'} \rightarrow G_M$ is the dilatation of G_M centered on $G_{M,k} \cap P_k$ and the homomorphism $G_{M,M'} \rightarrow G_{M'}$ is the dilatation of $G_{M'}$ centered on $G_{M',k} \cap P'_k$ (cf. Example 1 and property (iii)).

We also consider the intersection $G_{M,M'}^* := (G_M \times_R G_{M'}) \cap \mathbf{GL}_{M,M'}$ taken inside $\mathbf{GL}_M \times_R \mathbf{GL}_{M'}$. We have a closed embedding homomorphism $h : G_{M,M'} \rightarrow G_{M,M'}^*$ whose generic fibre is an isomorphism.

Definition 2 We say that G is well positioned with respect to (M, M') if $G_{M,M'} = G_{M,M'}^*$, i.e. h is an isomorphism (equivalently, $G_{M,M'}^*$ is flat).

For $n \in \mathbb{N}^*$ let $h_n := h(R/(\pi^n)) : G_{M,M'}(R/(\pi^n)) \rightarrow G_{M,M'}^*(R/(\pi^n))$. If G is well positioned with respect to (M, M') , then each h_n is an isomorphism.

Fact 3 *We assume that k is algebraically closed and $G_{M,M'}$ is smooth. If h_1 and h_2 are isomorphisms, then G is well positioned with respect to (M, M') .*

Proof: By the fiberwise criterion of flatness, it suffices to check that the special fibre $h_k : G_{M,M',k} \rightarrow G_{M,M',k}^*$ of h is an isomorphism. But h_k is a bijection (as h_1 is an isomorphism), it induces an isomorphism dh_k at the level of Lie algebras (as h_2 is an isomorphism), it is a closed embedding, and has a smooth domain. Thus h_k is an isomorphism. \square

Proposition 4 *If G is normalized by λ , then G is well positioned with respect to (M, M') .*

Proof: We will use the theory of dynamically defined (see [CGP, Sect. 2.1]) closed subgroup schemes $U_*(-\lambda)$, $Z_*(\lambda)$, and $U_*(\lambda)$ of $*$, where $*$ stands for an affine group schemes over either $\text{Spec } K$ or $\text{Spec } R$ normalized by λ or by some extension of λ to a cocharacter over $\text{Spec } R$. Like $Z_*(\lambda)$ is the scheme theoretic centralizer of λ (or of some extension of it over $\text{Spec } R$) in $*$, while $U_*(\lambda)$ and $U_*(-\lambda)$ are unipotent subgroup schemes of $*$ obtained naturally from the K -vector spaces $\text{Hom}(F^1[\frac{1}{\pi}], F^0[\frac{1}{\pi}])$ and $\text{Hom}(F^0[\frac{1}{\pi}], F^1[\frac{1}{\pi}])$ (respectively).

The product open embedding $U_{GL_V}(-\lambda) \times_K Z_{GL_V}(\lambda) \times_K U_{GL_V}(\lambda) \hookrightarrow GL_V$ defines the “big cell” of GL_V . Its intersection with G is the “big cell” $\mathfrak{C}_G := U_G(-\lambda) \times_K Z_G(\lambda) \times_K U_G(\lambda)$ of G , cf. [CGP, Prop. 2.1.8 and Rm. 2.1.11]. The “big cell” notion extends to smooth affine group schemes over R (cf. loc. cit.) and the special fibre of $GL_{M,M'}$ lies in the big cell. When we consider the big cell $\mathfrak{C}_M \times_R \mathfrak{C}_{M'}$ of $GL_M \times_R GL_{M'}$, it is easy to see that we have corresponding decompositions for G_M , $G_{M'}$, and $G_{M,M'}$ and thus also for $G_{M,M'}^* = (G_M \times_R G_{M'}) \cap GL_{M,M'}$. For instance for G_M , if \mathfrak{C}_{G_M} is the schematic closure of \mathfrak{C}_G in \mathfrak{C}_M , then the closed embedding morphism $j : \mathfrak{C}_{G_M} \hookrightarrow G_M \cap \mathfrak{C}_M$ between flat $\text{Spec } R$ -schemes is an isomorphism as j_K is an isomorphism; but \mathfrak{C}_{G_M} is a product $U_{G_M}(-\lambda) \times_R Z_{G_M}(\lambda) \times_R U_{G_M}(\lambda)$ (as its generic fibre \mathfrak{C}_G and \mathfrak{C}_M are such products) and thus we get the product decomposition $G_M \cap \mathfrak{C}_M = U_{G_M}(-\lambda) \times_R Z_{G_M}(\lambda) \times_R U_{G_M}(\lambda)$ into $\text{Spec } R$ -schemes which are flat as G_M is so. Thus it suffices to check the flatness of $G_{M,M'}^*$ for each one of the three factors of its open subscheme big cell.

The $Z(\lambda)$ factor. We have $Z_G(\lambda) \subset \mathbf{GL}_{F^0[\frac{1}{\pi}]} \times_K \mathbf{GL}_{F^1[\frac{1}{\pi}]}$. Its schematic closures in G_M and $G_{M'}$ are $Z_{G_M}(\lambda)$ and $Z_{G_{M'}}(\lambda)$ (respectively) and can be identified with the schematic closures of $Z_G(\lambda)$ in $Z_{\mathbf{GL}_M}(\lambda) = \mathbf{GL}_{F^1} \times_R \mathbf{GL}_{F^0}$ and $Z_{\mathbf{GL}_{M'}}(\lambda) = \mathbf{GL}_{\pi^{-1}F^1} \times_R \mathbf{GL}_{F^0}$ (respectively). As $\mathbf{GL}_{F^1} = \mathbf{GL}_{\pi^{-1}F^1}$, $Z_{G_{M,M'}}^*(\lambda)$ is the intersection of the product of these last schematic closures with the diagonal of $Z_{\mathbf{GL}_M}(\lambda) \times_R Z_{\mathbf{GL}_{M'}}(\lambda)$ and this intersection is flat and can be identified with both $Z_{G_M}(\lambda)$ and $Z_{G_{M'}}(\lambda)$.

The $U(\lambda)$ factor. We have $U_{\mathbf{GL}_M}(\lambda) = \underline{\text{Hom}}(F^1, F^0)$ and $U_{\mathbf{GL}_{M'}}(\lambda) = \underline{\text{Hom}}(\pi^{-1}F^1, F^0)$ (here underlying means the group scheme functor associated to a module). Moreover $U_{\mathbf{GL}_{M,M'}}(\lambda)$ is the graph of the restriction homomorphism $\phi : \underline{\text{Hom}}(\pi^{-1}F^1, F^0) \rightarrow \underline{\text{Hom}}(F^1, F^0)$. But ϕ sends the schematic closure $U_{G_{M'}}(\lambda)$ of $U_G(\lambda)$ in $\underline{\text{Hom}}(\pi^{-1}F^1, F^0)$ to the schematic closure $U_{G_M}(\lambda)$ of $U_G(\lambda)$ in $\underline{\text{Hom}}(F^1, F^0)$. Thus again the intersection $U_{G_{M,M'}}^*(\lambda)$ of the product of these schematic closures with the graph of ϕ is flat and in fact it is isomorphic to $U_{G_{M'}}(\lambda)$.

The $U(-\lambda)$ factor. The argument for this is similar to the one in the previous paragraph and in fact we have $U_{G_{M,M'}}^*(-\lambda) = U_{G_M}(-\lambda)$. \square

9 Appendix B: properties of exp and log maps for matrices in p -adic contexts

Let p be a prime. Let K be a field of characteristic 0 complete with respect to an ultrametric absolute value $|\cdot| \rightarrow \mathbb{R}$. We extend $|\cdot|$ to an absolute value on an algebraic closure \bar{K} of K , denoted also by $|\cdot|$. We assume that the residue characteristic of K is p and let $q := |p|^{\frac{1}{p-1}} \in (0, 1)$. Let $n \in \mathbb{N}^*$ and let I_n be the identity matrix of $M_n(K)$ or $M_n(\bar{K})$. By the norm of a matrix $X = (x_{i,j})_{1 \leq i,j \leq n} \in M_n(\bar{K})$ we mean

$$\|X\| := \max\{|x_{i,j}| \mid 1 \leq i, j \leq n\} \in [0, \infty).$$

Let $\rho(X)$ (denoted $\|x\|_{\text{sp}}$ in some papers) be the *spectral radius* of X , i.e. the maximum of the absolute values of the eigenvalues of X in \bar{K} . We can conjugate X to an upper triangular matrix whose entries off the main diagonal have arbitrarily small absolute values. Thus if $\rho(X) > 0$, then we can conjugate X so that we have $\|X\| = \rho(X)$ and if $\rho(X) = 0$, then we can conjugate X so that its norm is arbitrarily small. The series $e_1(X) =$

$\sum_{n=1}^{\infty} \frac{X^n}{n!}$ and $\exp(X) = I_n + e_1(X)$ converge if $\rho(X) < q$ and the series $l_1(X) = \log(I_n + X) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n$ converges if $\rho(X) < 1$. From [Bo, Ch. II, Sect. 8, Prop. 4] and our conjugation statements, we get that e_1 and l_1 define inverse bijections on $\mathbb{B}_n := \{X \in M_n(K) | \rho(X) < q\}$.

Proposition 5 *Let G be an algebraic subgroup of $\mathbf{GL}_{n,K}$. Then we have inverse bijections $\{\zeta \in \text{Lie}(G) | \rho(\zeta) < q\} \xrightleftharpoons[\log]{\exp} \{g \in G(K) | \rho(g - I_n) < q\}$.*

Proof: For $\zeta \in M_n(K)$ with $\rho(\zeta) < q$ we have to check that $\zeta \in \text{Lie}(G)$ if and only if $\exp(\zeta) \in G(K)$.

To check the only if part, we recall that we have a formal exponential $\exp(T\zeta)$ in $G(K[[T]])$ (cf. [DGa, Ch. II, Sect. 6, Subsect. 3]). By Subsubsection 3.3 of loc. cit., it is given by the usual exponential series for $\mathbf{GL}_{n,K}$, hence the spectral radius condition gives that $\exp(T\zeta)$ and $\exp(-T\zeta)$ are matrices with coefficients in the ring $K\{T\}$ of restricted formal power series. Thus $\exp(T\zeta) \in G(K[[T]]) \cap \mathbf{GL}_n(K\{T\}) = G(K\{T\})$ and by evaluating at $T = 1$ we get that $\exp(\zeta) \in G(K)$.

We now check the if part. We have $\exp(T\zeta) \in \mathbf{GL}_n(K\{T\})$ and it belongs to $G(K)$ when evaluated at $T = 1$ and thus at each $T \in \mathbb{Z}$. Hence every equation for G in $\mathbf{GL}_{n,K}$ evaluated at $\exp(T\zeta)$ is an element in $K\{T\}$ with infinitely many zeros in K and thus it is 0, cf. Weierstraß preparation theorem for $K\{T\}$. Thus $\exp(T\zeta) \in G(K\{T\}) \subset G(K[[T]])$ and by evaluating its derivative at $T = 0$ we get that $\zeta \in \text{Lie}(G)$. \square

Remark Proposition 5 and its proof extend to the case when the residue field of K has characteristic 0 provided we take $q = 1$.

9.1 Applications to rings of Witt vectors

Let A be a reduced \mathbb{F}_p -algebra. Let $W(A)$ be the ring of Witt vectors with coefficients in A . Let F and V be the Frobenius and the Verschiebung maps of $W(A)$. Let $m \in \mathbb{N}^*$. Let $W_m(A) := W(A)/V^m(W(A))$. For $X = (x_{i,j})_{1 \leq i,j \leq n} \in M_n(W(A))$ and $l \in \mathbb{N}$, let $\pi_l(X) = (x_{l,i,j})_{1 \leq i,j \leq n} \in M_n(A)$ be the matrix of the l -th Witt components of the entries of X ; thus $x_{i,j} = (x_{0,i,j}, x_{1,i,j}, \dots) \in W(A)$. For $s \in \mathbb{N}^*$, let

$$\Sigma_s = \{X \in M_n(W(A)) | \pi_0(X)^s = 0\} \text{ and } \Sigma_{1,s} = V(\Sigma_s).$$

For $a \in \mathbb{N}^*$ we have $\Sigma_{1,1} \subset \cdots \subset \Sigma_{1,n} = \Sigma_{1,n+a} \subset \Sigma_1 \subset \cdots \subset \Sigma_n = \Sigma_{n+a}$. Moreover, $\Sigma_1 = V(M_n(W(A)))$ and $\Sigma_{1,1} = V^2(M_n(W(A)))$.

As A is reduced, $W(A)$ is torsion free and thus expressions of the form $\frac{y}{d}$ are uniquely determined if they make sense (here $y \in W(A)$ and $d \in \mathbb{N}^*$). The V -adic filtration is compatible with the multiplication, i.e. we have $V^a(W(A))V^b(W(A)) \subset V^{a+b}(W(A))$ for all $a, b \in \mathbb{N}$. Also we recall that $V(x_1) \cdots V(x_d) = p^{d-1}V(x_1 \cdots x_d)$ for all $d \in \mathbb{N}^*$ and $x_1, \dots, x_d \in W(A)$. Moreover, as V is additive, these properties extend to matrices in $M_n(W(A))$.

Proposition 6 *Let Σ be either Σ_s for $p > 2$ and $1 \leq s \leq \frac{p-1}{2}$ or $\Sigma_{1,t}$ for p arbitrary and $t \in \mathbb{N}^*$. Then the following three properties hold:*

(a) *For $v \in \mathbb{N}^*$ the rule $X \mapsto \frac{X^v}{v!}$ sends Σ to Σ .*

(b) *The partial sums of the series $e_1(b) = \sum_{v=1}^{\infty} \frac{b^v}{v!}$ and $l_1(b) = \sum_{v=1}^{\infty} \frac{(-1)^{v-1}}{v} b^v$ send Σ to Σ and converge V -adically to maps $e_1 : \Sigma \rightarrow \Sigma$ and $l_1 : \Sigma \rightarrow \Sigma$ which are inverse to each other.*

(c) *For $l \in \mathbb{N}$ the entries of $\pi_l(e_1(X))$ and $\pi_l(l_1(X))$ are polynomials with coefficients in \mathbb{F}_p in the entries of $\pi_{\tilde{l}}(X)$ with $\tilde{l} \in \{0, \dots, l\}$. Thus if $\Sigma[m] := \text{Im}(\Sigma \rightarrow M_n(W_m(A)))$, then e_1 and l_1 induce inverse bijections $\Sigma[m] \xrightleftharpoons[l_1]{e_1} \Sigma[m]$ which commute with the conjugation by $\mathbf{GL}_n(W_m(A))$.*

Proof: We have $\frac{V(X)^v}{v!} = \frac{p^{v-1}}{v!}V(X^v)$ and $\text{ord}_p(v!) \leq \frac{v-1}{p-1}$ and thus the rule $X \mapsto \frac{X^v}{v!}$ sends Σ_1 to Σ_1 and $\Sigma_{1,t}$ is preserved. If $v \geq td$ (resp. $v \geq td + 1$), then the rule $X \mapsto \frac{X^v}{v!}$ sends $\Sigma_{1,t}$ to $V^d(\Sigma_1)$ (resp. to $V^d(\Sigma_{1,t})$).

If $p > 2$ and $X \in \Sigma_s$ with $s \leq \frac{p-1}{2}$, we can write $X^{\frac{p-1}{2}} = V(Y)$ and thus $\frac{X^{p-1}}{p} = V(Y^2) \in \Sigma_s$; as $\frac{T^v}{v!}$ is $cT^a(\frac{T^{p-1}}{p})^b$ for some $c \in \mathbb{Z}_{(p)}$, $a \in \{0, \dots, p-1\}$, and $b \in \mathbb{N}$, we get that $\frac{X^v}{v!} \in \Sigma_s$. If $v \geq (p-1)(d+1)$, then the rule $X \mapsto \frac{X^v}{v!}$ sends Σ_s to $V^d(\Sigma_1)$. Thus (a) and the first part of (b) hold.

The fact that e_1 is inverse to l_1 can be reduced to the case when A is a perfect field k in which case Proposition 5 applies with $K = W(k)[\frac{1}{p}]$, $\Sigma_s \subset \{X \in M_n(K) = \text{Lie}(\mathbf{GL}_{n,K}) \mid \rho(X) \leq |p|^{\frac{1}{s}}\} \subset \mathbb{B}_n$, and $\Sigma_{1,t} \subset \{X \in M_n(K) = \text{Lie}(\mathbf{GL}_{n,K}) \mid \rho(X) \leq |p|^{\frac{t+1}{t}}\} \subset \mathbb{B}_n$. Thus the second part of (b) also holds. Part (c) follows directly from the above facts on $X \mapsto \frac{X^v}{v!}$. \square

Let P be a finitely generated, projective $W_m(A)$ -module. If P is free of rank n , we can speak about $\Sigma_P \subset \text{End}(P)$ and about inverse bijections

$\Sigma_P \xrightleftharpoons[l_1]{e_1} \Sigma_P$ which can be identified with $\Sigma[m] \xrightleftharpoons[l_1]{e_1} \Sigma[m]$ with respect to each isomorphism $P \rightarrow W_m(A)^n$ of $W_m(A)$ -modules. These inverse bijections make sense for all P (without assuming their freeness) via a natural sheafification process (there exists a finite open cover $\text{Spec } A = \cup_{i=1}^u \text{Spec } A_{f_i}$ such that $W_m(A_{f_i}) \otimes_{W_m(A)} P$ is free for all $i \in \{1, \dots, u\}$; here each $f_i \in A$).

Fact 4 (a) *If P is a finitely generated, projective $W_m(A)$ -module and Q is a direct summand of P and if $x \in \Sigma_P$ is such that $x(Q) \subset Q$, then we have $e_1(x)(Q) \subset Q$ and $l_1(x)(Q) \subset Q$.*

(b) *If $\phi : P_1 \rightarrow P_2$ is a $W_m(A)$ -linear map between finitely generated, projective $W_m(A)$ -modules and if $x_1 \in \Sigma_{P_1}$ and $x_2 \in \Sigma_{P_2}$ are such that $x_2 \circ \phi = \phi \circ x_1$, then we have $e_1(x_2) \circ \phi = \phi \circ e_1(x_1)$ and $l_1(x_2) \circ \phi = \phi \circ l_1(x_1)$.*

Proof: Locally in the Zariski topology of $\text{Spec } A$, to prove (a) we can assume that P is free and Q is generated by a subset of a $W_m(A)$ -basis for P . It is clear from very definitions that e_1 and l_1 preserve block upper triangular matrices of the form $\begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix}$ and therefore (a) holds. Part (b) follows from (a) applied to the direct summand of $P_1 \oplus P_2$ which is the graph of ϕ . \square

9.2 The perfect field case

Let now A be a perfect field k of characteristic p . Let $B(k) := W(k) \left[\frac{1}{p} \right]$. Let M be a free $W(k)$ -module of finite rank. For $x \in \text{End}(M)$, let $\bar{x} \in \text{End}(M/pM)$ be its reduction modulo p . Let G be a flat, closed subgroup scheme of \mathbf{GL}_M . Let $\mathfrak{g} := \text{Lie}(G_{B(k)}) \cap \text{End}(M)$; thus $\mathfrak{g}/p^m \mathfrak{g}$ embeds in $\text{End}(M/p^m M)$ for every $m \in \mathbb{N}^*$. We define Σ subsets $\Sigma(M)$ of $\text{End}(M)$ via the rules: if $\Sigma = \Sigma_s$, then $\Sigma(M) := \{x \in \text{End}(M) | \bar{x}^s = 0\}$ and if $\Sigma = \Sigma_{1,t}$, then $\Sigma(M) := p\{x \in \text{End}(M) | \bar{x}^t = 0\}$.

Proposition 7 (a) *For every Σ as in Proposition 6, the \exp and \log induce inverse bijections $\mathfrak{g} \cap \Sigma(M) \rightleftharpoons \{g \in G(W(k)) | g - 1_M \in \Sigma(M)\}$ which at their own turns induce for each $m \in \mathbb{N}^*$ inverse bijections between the image $\Sigma^{\mathfrak{g}}[m]$ of $\mathfrak{g} \cap \Sigma(M)$ in $\mathfrak{g}/p^m \mathfrak{g}$ and the image $\Sigma^G[m]$ of $\{g \in G(W(k)) | g - 1_M \in \Sigma(M)\}$ in $G(W_m(k))$.*

(b) *If (M, ϕ, ϑ) is the Dieudonné module of a p -divisible group D over k (thus $\phi : W(k) \otimes_{F, W(k)} M \rightarrow M$ and $\vartheta : M \rightarrow W(k) \otimes_{F, W(k)} M$ are $W(k)$ -linear maps such that $\phi \circ \vartheta$ and $\vartheta \circ \phi$ are the multiplication by p) and if $e_m \in$*

$\Sigma^g[m]$ is the crystalline realization of an endomorphism of $D[p^m]$ (i.e. is an endomorphism of (M, ϕ, ϑ) modulo p^m), then $\exp(e_m)$ and $\log(1_{M/p^m M} + e_m)$ are crystalline realizations of endomorphisms of $D[p^m]$.

Proof: As $V(W(k)) = pW(k)$, part (a) follows from Propositions 5 and 6. Part (b) follows from Fact 4 (b) applied to the reductions modulo p^m of ϕ and ϑ . \square

Acknowledgments. The second author would like to thank Binghamton University, IHES, Bures-sur-Yvette, and IAS, Princeton for good work conditions and J. E. Humphreys for the reference to [Sp] used in the proof of Proposition 1. He was partially supported by the NSF grant DMS #0900967.

References

- [Bo] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1-3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989.
- [BBM] P. Berthelot, L. Breen, and W. Messing, *Théorie de Dieudonné cristalline II*, Lecture Notes in Math., Vol. **930**, Springer-Verlag, Berlin, 1982.
- [BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. **21**, Springer-Verlag, Berlin, 1990.
- [BM] P. Berthelot and W. Messing, *Théorie de Dieudonné cristalline III*, The Grothendieck Festschrift, Vol. I, Progr. Math., Vol. **86**, 173–247, Birkhäuser Boston, Boston, MA, 1990.
- [CGP] B. Conrad, O. Gabber, and G. Prasad, *Pseudo-reductive groups*, New Mathematical Monographs, Vol. **17**, Cambridge University Press, Cambridge, 2010.
- [DGa] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Avec un appendice *Corps de classes local* par Michiel Hazewinkel, Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.

- [DGr] M. Demazure, A. Grothendieck, et al. *Schémas en groupes*, Vol. **II**, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Lecture Notes in Math., Vol. **152**, Springer-Verlag, Berlin-New York, 1970.
- [Fo] J.-M. Fontaine, *Groupes p -divisibles sur les corps locaux*, Astérisque **47/48**, Soc. Math. de France, Paris, 1977.
- [Gre] M. Greenberg, *Schemata over local rings*, Ann. of Math. (2) **73** (1961), no. 3, 624–648.
- [Gro] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*. Inst. Hautes Études Sci. Publ. Math. No. **28** (1966) 255 pp.
- [GV] O. Gabber and A. Vasiu, *Projective limits of algebraic group actions and applications to Tannakian categories*, work in progress.
- [Il] L. Illusie, *Déformations de groupes de Barsotti–Tate (d’après A. Grothendieck)*, Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (Paris, 1983/84), 151–198, Astérisque **127**, Soc. Math. de France, Paris, 1985.
- [IR] L. Illusie and M. Raynaud, *Les suites spectrales associées au complexe de de Rham–Witt*, Inst. Hautes Études Sci. Publ. Math. No. **57** (1983), 73–212.
- [Ka] N. Katz, *Slope filtration of F -crystals*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, 113–163, Astérisque **63**, Soc. Math. de France, Paris, 1979.
- [Kr] H. Kraft, *Kommutative algebraische p -Gruppen (mit Anwendungen auf p -divisible Gruppen und abelsche Varietäten)*, manuscript 86 pages, Univ. Bonn, 1975.
- [LNV] E. Lau, M.-H. Nicole, and A. Vasiu, *Stratifications of Newton polygon strata and Traverso’s conjectures for p -divisible groups*, manuscript 48 pages, 2009, <http://arxiv.org/abs/0912.0506>.

- [Ma] J. I. Manin, *The theory of formal commutative groups in finite characteristic*, Russian Math. Surv. **18** (1963), no. 6, 1–83.
- [Mo] B. Moonen, *Group schemes with additional structures and Weyl group cosets*, Moduli of abelian varieties (Texel Island, 1999), 255–298, Progr. Math., Vol. **195**, Birkhäuser, Basel, 2001.
- [MW] B. Moonen and T. Wedhorn, *Discrete invariants of varieties in positive characteristic*, Int. Math. Res. Not. **72** (2004), 3855–3903.
- [NV1] M.-H. Nicole and A. Vasiu, *Minimal truncations of supersingular p -divisible groups*, Indiana Univ. Math. J. **56** (2007), no. 6, 2887–2897.
- [NV2] M.-H. Nicole and A. Vasiu, *Traverso’s isogeny conjecture for p -divisible groups*, Rend. Semin. Mat. U. Padova **118** (2008), 73–83.
- [Oo1] F. Oort, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), 345–416, Progr. Math., Vol. **195**, Birkhäuser, Basel, 2001.
- [Oo2] F. Oort, *Foliations in moduli spaces of abelian varieties*, J. Amer. Math. Soc. **17** (2004), no. 2, 267–296.
- [Oo3] F. Oort, *Simple p -kernels of p -divisible groups*, Adv. Math. **198** (2005), no. 1, 275–310.
- [PWZ] R. Pink, T. Wedhorn, and T. Zigler, *Algebraic zip data*, Doc. Math. **16** (2011), 253–300.
- [Se] J.-P. Serre, *Groupes proalgébriques*, Inst. Hautes Études Sci. Publ. Math. No. **7**, 1960.
- [Sp] T. A. Springer, *Linear algebraic groups. Second edition*, Progr. Math., Vol. **9**, Birkhäuser Boston, Inc., Boston, MA, 1998.

- [Tr1] C. Traverso, *Sulla classificazione dei gruppi analitici commutativi di caratteristica positiva*, Ann. Scuola Norm. Sup. Pisa (3) **23** (1969), no. 3, 481–507.
- [Tr2] C. Traverso, *p -divisible groups over fields*, Symposia Mathematica, Vol. **XI** (Convegno di Algebra Commutativa, INDAM, Rome, 1971), 45–65, Academic Press, London, 1973.
- [Tr3] C. Traverso, *Specializations of Barsotti–Tate groups*, Symposia Mathematica, Vol. **XXIV** (Sympos., INDAM, Rome, 1979), 1–21, Acad. Press, London-New York, 1981.
- [Va1] A. Vasiu, *Crystalline boundedness principle*, Ann. Sci. École Norm. Sup. **39** (2006), no. 2, 245–300.
- [Va2] A. Vasiu, *Level m stratifications of versal deformations of p -divisible groups*, J. Alg. Geom. **17** (2008), no. 4, 599–641.
- [Va3] A. Vasiu, *Reconstructing p -divisible groups from their truncations of small level*, Comment. Math. Helv. **85** (2010), no. 1, 165–202.
- [Va4] A. Vasiu, *Mod p classification of Shimura F -crystals*, Math. Nachr. **283** (2010), no. 8, 1068–1113.
- [Va5] A. Vasiu, *Integral models in unramified mixed characteristic $(0, 2)$ of hermitian orthogonal Shimura varieties of PEL type, Part I*, manuscript 40 pages, 2011, available at <http://www.math.binghamton.edu/adrian>.
- [We] T. Wedhorn, *Specialization of F -zips*, manuscript 23 pages, 2007, available at <http://www2.math.uni-paderborn.de/people/torsten-wedhorn.html>.

Ofer Gabber, Email: gabber@ihes.fr
 Address: IHÉS, Le Bois-Marie, 35, Route de Chartres,
 F-91440 Bures-sur-Yvette, France.

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