CRYSTALLINE BOUNDEDNESS PRINCIPLE

BY ADRIAN VASIU

ABSTRACT. – We prove that an F-crystal (M, φ) over an algebraically closed field k of characteristic $p > 0$ is determined by $(M, \varphi) \bmod p^n$, where $n \geqslant 1$ depends only on the rank of M and on the greatest Hodge slope of (M, φ). We also extend this result to triples (M, φ, G), where G is a flat, closed subgroup scheme of $\mathbf{GL}_M$ whose generic fibre is connected and has a Lie algebra normalized by φ. We get two purity results. If $\mathfrak{C}$ is an F-crystal over a reduced $\mathbf{F}_p$-scheme S, then each stratum of the Newton polygon stratification of S defined by $\mathfrak{C}$, is an affine S-scheme (a weaker result was known before for S noetherian). The locally closed subscheme of the Mumford scheme $\mathcal{A}_{d,1,N_k}$ defined by the isomorphism class of a principally quasi-polarized p-divisible group over k of height $2d$, is an affine $\mathcal{A}_{d,1,N_k}$-scheme.
© 2006 Elsevier SAS

RÉSUMÉ. – Nous prouvons qu'un F-cristal (M, φ) défini sur un corps k algébriquement clos de caractéristique $p > 0$ est déterminé par $(M, \varphi) \bmod p^n$, où $n \geqslant 1$ dépend seulement du rang de M et de la plus grande pente de Hodge de (M, φ). On étend ce résultat aux triplets (M, φ, G), où G est un sous-groupe fermé et plat de $\mathbf{GL}_M$ dont la fibre générique est connexe et a une algèbre de Lie normalisée par φ. Nous obtenons deux résultats de pureté. Si $\mathfrak{C}$ est un F-cristal sur un $\mathbf{F}_p$-schéma réduit S, alors chaque strate de la stratification du polygone de Newton de S défini par $\mathfrak{C}$ est un S-schéma affine (un résultat moins général était déjà connu pour S noethérien). Le sous-schéma localement fermé du schéma de Mumford $\mathcal{A}_{d,1,N_k}$ défini par la classe d'isomorphisme d'un groupe p-divisible principalement quasi polarisé sur k de hauteur $2d$ est un $\mathcal{A}_{d,1,N_k}$-schéma affine.
© 2006 Elsevier SAS

1. Introduction

Let $p \in \mathbf{N}$ be a prime. Let k be a perfect field of characteristic p. Let $\bar{k}$ be an algebraic closure of k. Let $W(k)$ be the Witt ring of k. Let $B(k) := W(k)[\frac{1}{p}]$ be the field of fractions of $W(k)$. Let $\sigma := \sigma_k$ be the Frobenius automorphism of k, $W(k)$, and $B(k)$. A group scheme H over $\mathrm{Spec}(W(k))$ is called integral if H is flat over $\mathrm{Spec}(W(k))$ and $H_{B(k)}$ is connected (i.e. if the scheme H is integral). Let $\mathrm{Lie}(H_{B(k)})$ be the Lie algebra over $B(k)$ of $H_{B(k)}$. If H is smooth over $\mathrm{Spec}(W(k))$, let $\mathrm{Lie}(H)$ be the Lie algebra over $W(k)$ of H. If O is a free module of finite rank over some commutative $\mathbf{Z}$-algebra R, let $\mathbf{GL}_O$ be the group scheme over $\mathrm{Spec}(R)$ of linear automorphisms of O.

Let $(r, d) \in \mathbf{N} \times (\mathbf{N} \cup \{0\})$, with $r \geqslant d$. Let D be a p-divisible group over $\mathrm{Spec}(\bar{k})$ of height r and dimension d. It is well known that if $d \in \{0, 1, r-1, r\}$, then:

(∗) D is uniquely determined up to isomorphism by its p-torsion subgroup scheme $D[p]$.

But (∗) does not hold if $2 \leqslant d \leqslant r - 2$. In 1963 Manin published an analogue of (∗) for $2 \leqslant d \leqslant r - 2$ but unfortunately he separated it into three parts (see [28, p. 44, 3.6, and 3.8] and below). Only recently, this paper and [36] contain explicit analogues of (∗) for $2 \leqslant d \leqslant r - 2$. The two main reasons for this delay in the literature are: (i) the widely spread opinion, which

goes back more than 40 years, that p-divisible groups involve an infinite process, and (ii) the classification results of [28, p. 44] were rarely used. Our point of view is that F-crystals in locally free sheaves of finite rank over many $\mathrm{Spec}(k)$-schemes Y involve a *bounded infinite process*. In this paper we give meaning to this point of view for the case $Y = \mathrm{Spec}(\bar{k})$. We start with few definitions.

1.1. DEFINITIONS. –

(a) By a *latticed F-isocrystal with a group* over k we mean a triple (M, φ, G), where M is a free $W(k)$-module of finite rank, where φ is a σ-linear automorphism of $M[\frac{1}{p}]$, and where G is an integral, closed subgroup scheme of $\mathbf{GL}_M$, such that the Lie subalgebra $\mathrm{Lie}(G_{B(k)})$ of $\mathrm{End}(M[\frac{1}{p}])$ is normalized by φ. Here we denote also by φ the σ-linear (algebra) automorphism of $\mathrm{End}(M[\frac{1}{p}])$ that takes $e \in \mathrm{End}(M[\frac{1}{p}])$ into $\varphi \circ e \circ \varphi^{-1} \in \mathrm{End}(M[\frac{1}{p}])$. If $G = \mathbf{GL}_M$, then often we do not mention G and we omit "with a group".

(b) By an isomorphism between two latticed F-isocrystals with a group (M_1, φ_1, G_1) and (M_2, φ_2, G_2) over k we mean a $W(k)$-linear isomorphism $f : M_1 \xrightarrow{\sim} M_2$ such that $\varphi_2 \circ f = f \circ \varphi_1$ and the isomorphism $\mathbf{GL}_{M_1} \xrightarrow{\sim} \mathbf{GL}_{M_2}$ induced by f, takes G_1 onto G_2.

The pair $(M[\frac{1}{p}], \varphi)$ is called an F-isocrystal over k. If we have $pM \subseteq \varphi(M) \subseteq M$, then the pair (M, φ) is called a Dieudonné module over k. For $g' \in G(B(k))$ let $g'\varphi$ be the σ-linear automorphism of $M[\frac{1}{p}]$ that takes $x \in M[\frac{1}{p}]$ into $g'(\varphi(x)) \in M[\frac{1}{p}]$. The triple $(M, g'\varphi, G)$ is also a latticed F-isocrystal with a group over k.

Often there exists a "good" class $\mathbf{M}$ of motives over k that has the following property. The crystalline realization of any motive $\mathcal{M}$ in $\mathbf{M}$ is naturally identified with $(M, g_{\mathcal{M}}\varphi)$ for some $g_{\mathcal{M}} \in G(W(k))$ and moreover $G_{B(k)}$ is the identity component of the subgroup of $\mathbf{GL}_{M[\frac{1}{p}]}$ that fixes some tensors of the tensor algebra of $M[\frac{1}{p}] \oplus \mathrm{Hom}(M[\frac{1}{p}], B(k))$ which do not depend on $\mathcal{M}$ and which are (expected to be) crystalline realizations of motives over k that are intrinsically associated to $\mathcal{M}$. For instance, see [40, §5 and §6] for contexts that pertain to classes of H^1 motives of abelian varieties over $\mathrm{Spec}(k)$ which are associated to k-valued points of a (fixed) good integral model of a Shimura variety of Hodge type. The paper [40] and many previous ones (like [25]) deal with particular cases of such triples (M, φ, G)'s: the pair (M, φ) is a Dieudonné module over k, the group scheme G is reductive, and there exists a semisimple element $s_\varphi \in G(B(k))$ whose eigenvalues are 1 and p and such that φs_φ^{-1} is a σ-linear automorphism of M. Any good classification of the triples $(M, g_{\mathcal{M}}\varphi, G)$ up to isomorphisms defined by elements of $G(W(k))$, is often an important tool toward the classification of motives in $\mathbf{M}$.

Classically, one approaches the classification of all triples $(M, g\varphi, G)$ with $g \in G(W(k))$, up to isomorphisms defined by elements of $G(W(k))$, in two steps. The first step aims to classify $(M[\frac{1}{p}], g\varphi, G_{B(k)})$'s up to isomorphisms defined by elements of $G(B(k))$. The second step aims to use the first step in order to study $(M, g\varphi, G)$'s.

A systematic and general approach to the first step was started in [24], which works in the context in which the group $G_{B(k)}$ is reductive, $k = \bar{k}$, and the pair $(M[\frac{1}{p}], G_{B(k)})$ has a $\mathbf{Q}_p$ structure $(M_{\mathbf{Q}_p}, G_{\mathbf{Q}_p})$ with respect to which φ becomes $g_\varphi(1_{M_{\mathbf{Q}_p}} \otimes \sigma)$ for some $g_\varphi \in G(B(k))$; thus, in order to classify $(M[\frac{1}{p}], g\varphi, G_{B(k)})$'s up to isomorphisms defined by elements of $G(B(k))$, one only has to describe the image G_φ of the set $\{gg_\varphi \mid g \in G(W(k))\}$ in the set $B(G_{\mathbf{Q}_p})$ of σ-conjugacy classes of elements of $G_{\mathbf{Q}_p}(B(k)) = G(B(k))$. Even if $k = \bar{k}$, in general such $\mathbf{Q}_p$ structures do not exist (for instance, they do not exist if the group $G_{B(k)}$ is commutative and $(\mathrm{Lie}(G_{B(k)}), \varphi)$ has non-zero slopes).

One can define two natural equivalence relations I_φ and R_φ on the set underlying the group $G(W(k))$ as follows. A pair $(g_1, g_2) \in G(W(k))^2$ belongs to I_φ (respectively to R_φ) if and only

if there exists $g_{12} \in G(W(k))$ (respectively $g_{12} \in G(B(k))$) such that $g_{12}g_1\varphi = g_2\varphi g_{12}$. The set of isomorphism classes of $(M, g\varphi, G)$'s (up to isomorphisms defined by elements of $G(W(k))$) is in natural bijection to the quotient set $G(W(k))/I_\varphi$. The quotient set $G(W(k))/R_\varphi$ is a more general version of the above type of sets G_φ. In general, the natural surjective map $G(W(k))/I_\varphi \twoheadrightarrow G(W(k))/R_\varphi$ is not an injection and some of its fibres have the same cardinality as k. In general, one can not "recover" $(M, g\varphi, G)$ and its reductions modulo powers of p from the equivalence class $[g] \in G(W(k))/I_\varphi$ and from the triple $(M[\frac{1}{p}], g\varphi, G_{B(k)})$. The last two sentences explain why in this paper, for the study of the quotient set $G(W(k))/I_\varphi$ and of (reductions modulo powers of p of) $(M, g\varphi, G)$'s, we can not appeal to the results of [24,37], etc. In addition, the language of latticed F-isocrystals is more general and more suited for reductions modulo powers of p, for endomorphisms, for deformations, and for functorial purposes than the language of either σ-conjugacy classes or equivalence classes of I_φ.

If $g_1, g_2, g_{12} \in G(W(k))$ satisfy $g_{12}g_1\varphi = g_2\varphi g_{12}$, it is of interest to keep track of the greatest number $n_{12} \in \mathbf{N} \cup \{0\}$ such that g_{12} and 1_M are congruent $\mod p^{n_{12}}$. As the relation I_φ is not suitable for this purpose, it will not be used outside this introduction.

The set $\{(M, g\varphi, G) \mid g \in G(W(k))\}$ is in natural bijection to $G(W(k))$. Any set of the form $\{(M, g\varphi, G) \mid g \in G(W(k))\}$ will be called a *family* of latticed F-isocrystals with a group over k. This paper is a starting point for general classifications of families of latticed F-isocrystals with a group over $\bar{k}$. The fact that such classifications are achievable is supported by the following universal principle.

1.2. MAIN THEOREM A (Crystalline Boundedness Principle). – *Suppose $k = \bar{k}$. Let (M, φ, G) be a latticed F-isocrystal with a group over k. Then there exists a number $n_{\mathrm{fam}} \in \mathbf{N} \cup \{0\}$ that is effectively bounded from above and that has the property that for any pair $(g, g_{n_{\mathrm{fam}}}) \in G(W(k))^2$ such that $g_{n_{\mathrm{fam}}}$ is congruent $\mod p^{n_{\mathrm{fam}}}$ to 1_M, there exist isomorphisms between $(M, g\varphi, G)$ and $(M, g_{n_{\mathrm{fam}}}g\varphi, G)$ which are elements of $G(W(k))$.*

Thus the equivalence class $[g] \in G(W(k))/I_\varphi$ depends only on $g \mod p^{n_{\mathrm{fam}}}$; this supports our *bounded infinite process* point of view. If $G = \mathbf{GL}_M$ and (M, φ) is a Dieudonné module over k, then Main Theorem A is a direct consequence of [28, p. 44, 3.6, and 3.8]. By a classical theorem of Dieudonné (see [7, Thms. 3 and 5], [28, §2], [5, Ch. IV, §4], or [14, Ch. III, §6]), the category of p-divisible groups over $\mathrm{Spec}(k)$ is anti-equivalent to the category of Dieudonné modules over k. Thus we get a new proof of the following result which in essence is due to Manin and which is also contained in [36].

1.3. COROLLARY. – *There exists a smallest number $T(r,d) \in \mathbf{N} \cup \{0\}$ such that any p-divisible group D over $\mathrm{Spec}(\bar{k})$ of height r and dimension d, is uniquely determined up to isomorphism by its $p^{T(r,d)}$-torsion subgroup scheme $D[p^{T(r,d)}]$. Upper bounds of $T(r,d)$ are effectively computable in terms of r.*

1.4. On the proof of Main Theorem A

The proof of Main Theorem A (see 3.1) relies on what we call the *stairs method*. The method is rooted on the simple fact that for any $t \in \mathbf{N}$ and every $y, z \in \mathrm{End}(M)$, the two automorphisms $1_M + p^t y$ and $1_M + p^t z$ of M commute $\mod p^{2t}$. To outline the method, we assume in this paragraph that G is smooth over $\mathrm{Spec}(W(k))$. Let $m \in \mathbf{N} \cup \{0\}$ be the smallest number for which there exists a $W(k)$-submodule E of $\mathrm{Lie}(G)$ that contains $p^m(\mathrm{Lie}(G))$ and that has a $W(k)$-basis $\{e_1, e_2, \ldots, e_v\}$ such that for $l \in \{1, \ldots, v\}$ we have $\varphi(e_l) = p^{n_l}e_{\pi(l)}$, where π is a permutation of the set $\{1, \ldots, v\}$ and where n_l's are integers that have the following *stairs property*. For any cycle $(l_1, \ldots, l_q)$ of π, the integers $n_{l_1}, \ldots, n_{l_q}$ are either all non-negative or all non-positive. The existence of m is implied by Dieudonné's classification of F-isocrystals

over k (see [28, §2]). In general, the $W(k)$-submodule E is not a Lie subalgebra of $\mathrm{Lie}(G)$. For any $\tilde{g} \in G(W(k))$ congruent mod p^{2m+t} to 1_M, there exists $\tilde{e} \in E$ such that the elements $\tilde{g}$ and $1_M + p^{m+t}\tilde{e}$ of $\mathbf{GL}_M(W(k))$ are congruent mod p^{2m+1+t}. Due to this and the stairs property, for $p \geqslant 3$ there exists an isomorphism between $(M, \tilde{g}\varphi, G)$ and (M, φ, G) which is an element $\tilde{g}_0 \in G(W(k))$ congruent mod p^{m+t} to 1_M (see 3.1.1). If $p = 2$, then a slight variant of this holds. Exponential maps (see 2.6) substitute from many points of view the classical Verschiebung maps of Dieudonné modules; for instance, one can choose $\tilde{g}_0$ to be an infinite product of exponential elements of the form $\sum_{i=0}^{\infty} \frac{p^{i(m+1)}}{i!} e^i$, where $e \in E$. See 2.2 to 2.4 for the σ-linear preliminaries that are necessary for the estimates which give us the effectiveness part of Main Theorem A. These estimates provide inductively upper bounds of m in terms of $\dim(G_{B(k)})$ and of the s-number and the h-number of the latticed F-isocrystal $(\mathrm{Lie}(G), \varphi)$ over k (see 2.2.1(e) for these two non-negative integers which do not change if φ is replaced by $g\varphi$).

1.5. Complements, examples, and applications

See 3.2 for interpretations and variants of Main Theorem A in terms of reductions modulo powers of p; in particular, see 3.2.4 for the passage from Main Theorem A to Corollary 1.3. In 3.3 we improve (in many cases of interest) the upper bounds (of n_{fam}, etc.) we obtain in 3.1.1 to 3.1.5.

In Section 4 we include four examples. It is well known that if the p-divisible group D is ordinary, then D is uniquely determined up to isomorphism by $D[p]$ and moreover D has a unique lift to $\mathrm{Spec}(W(\bar{k}))$ (called the canonical lift) that has the property that any endomorphism of D lifts to it. Example 2 identifies the type of latticed F-isocrystals with a group over $\bar{k}$ to which the last two facts generalize naturally (see 4.3.1 and 4.3.2). Example 4 shows that if $r = 2d$, $d \geqslant 3$, and the slopes of the Newton polygon of D are $\frac{1}{d}$ and $\frac{d-1}{d}$, then D is uniquely determined up to isomorphism by $D[p^3]$ (see 4.5).

In Section 5 we list four direct applications of Main Theorem A and of 3.2. First we present the homomorphism form of Main Theorem A (see 5.1.1). Second we define *transcendental degrees of definition* for many classes of latticed F-isocrystals with a group over $\bar{k}$ (see 5.2). When the transcendental degrees of definition are 0, we also define (finite) *fields of definition*. In particular, Theorem 5.2.3 (when combined with Lemma 3.2.2) implies that it is possible to build up an *atlas* and a *list of tables* of isomorphism classes of p-divisible groups (endowed with certain extra structures) over $\mathrm{Spec}(\bar{k})$ that are definable over the spectrum of a fixed finite field $\mathbf{F}_{p^q}$, which are similar in nature to the atlas of finite groups (see [3]) and to the list of tables of elliptic curves over $\mathrm{Spec}(\mathbf{Q})$ (see [4]).

Let $N \in \mathbf{N} \setminus \{1, 2\}$ be relatively prime to p. Let $\mathcal{A}_{d,1,N}$ be the smooth, quasi-projective Mumford moduli scheme over $\mathrm{Spec}(\mathbf{F}_p)$ that parametrizes isomorphism classes of principally polarized abelian schemes with level-N structure and of relative dimension d over $\mathrm{Spec}(\mathbf{F}_p)$-schemes (see [33, Thms. 7.9 and 7.10]). Third we apply the principally quasi-polarized version of Corollary 1.3 (see 3.2.5) to get a new type of stratification of $\mathcal{A}_{d,1,N}$. Here the word stratification is used in a wide sense (see 2.1.1) which allows the number of strata to be infinite. The strata we get are defined by isomorphism classes of principally quasi-polarized p-divisible groups of height $2d$ over spectra of algebraically closed fields of characteristic p; they are regular and equidimensional (see 5.3.1 and 5.3.2). Moreover, this new type of stratification of $\mathcal{A}_{d,1,N}$ satisfies the *purity property* we define in 2.1.1, i.e. its strata are affine $\mathcal{A}_{d,1,N}$-schemes (see 5.3.1 and 5.3.2). Variants of 1.3, 3.2.5, 3.2.6, and 5.3.2 but without its purity property part, are also contained in [36].

Fourth we get a new proof (see 5.4) of the "Katz open part" of the Grothendieck–Katz specialization theorem for Newton polygons (see [22, 2.3.1 and 2.3.2]).

The main goal of Section 6 is to prove the following result (see 6.1 and 6.2).

1.6. MAIN THEOREM B. – *Let $\mathfrak{C}$ be an F-crystal in locally free sheaves of finite rank over a reduced* $\mathrm{Spec}(\mathbf{F}_p)$*-scheme S. Then the Newton polygon stratification of S defined by $\mathfrak{C}$ satisfies the purity property* (*i.e. each stratum of it is an affine S-scheme*).

A variant of Main Theorem B was obtained first in [10, 4.1], for the particular case when S is locally noetherian. The fact that the variant is a weaker form of Main Theorem B is explained in 6.3(a). The main new idea of Section 6 is: Newton polygons are encoded in the existence of suitable morphisms between different evaluations of F-crystals (viewed without connections) at Witt schemes of (effectively computable) finite lengths. The proof of Main Theorem B combines this new idea with the results of Katz (see [22, 2.6 and 2.7]) on isogenies between F-crystals of constant Newton polygons over spectra of (perfections of) complete, discrete valuation rings that are of the form $\bar{k}[[x]]$.

2. Preliminaries

See 2.1 for our main notations and conventions. See 2.2 for few definitions and simple properties that pertain to latticed F-isocrystals with a group over k. In particular, in 2.2.2 we define Dieudonné–Fontaine torsions and volumes of latticed F-isocrystals. Inequalities and estimates on such torsions are gathered in 2.3 and 2.4 (respectively); they are essential for examples and for the effectiveness part of 1.2. In 2.5 we apply [42] to get $\mathbf{Z}_p$ structures for many classes of latticed F-isocrystals with a group over $\bar{k}$. In 2.6 and 2.7 we include group scheme theoretical properties that are needed in Sections 3 and 4. In 2.8 we present complements on the categories $\mathcal{M}(W_q(S))$ we will introduce in 2.1. In 2.9 we recall two results of commutative algebra. Sections 2.8 and 2.9 are not used before 5.4. For Newton polygons of F-isocrystals over k we refer to [22, 1.3].

2.1. Notations and conventions

By w we denote an arbitrary variable. If $q \in \mathbf{N}$, let $\mathbf{F}_{p^q}$ be the field with p^q elements. If R is a commutative $\mathbf{F}_p$-algebra, let $W(R)$ be the Witt ring of R and let $W_q(R)$ be the ring of Witt vectors of length q with coefficients in R. We identify $R = W_1(R)$. Let Φ_R be the canonical Frobenius endomorphism of either $W(R)$ or $W_q(R)$; we have $\Phi_k = \sigma_k = \sigma$. Let $R^{(p^q)}$ be R but viewed as an R-algebra via the q-th power Frobenius endomorphism $\Phi_R^q : R \to R$. If R is reduced, let $R^{\mathrm{perf}} := \mathrm{ind} \lim_{q \in \mathbf{N}} R^{(p^q)}$ be the perfection of R.

Let $\mathcal{M}(W_q(R))$ be the abelian category whose objects are $W_q(R)$-modules endowed with Φ_R-linear endomorphisms and whose morphisms are $W_q(R)$-linear maps that respect the Φ_R-linear endomorphisms. We identify $\mathcal{M}(W_q(R))$ with a full subcategory of $\mathcal{M}(W_{q+1}(R))$ and thus we can define $\mathcal{M}(W(R)) := \bigcup_{q \in \mathbf{N}} \mathcal{M}(W_q(R))$.

If S is a $\mathrm{Spec}(\mathbf{F}_p)$-scheme, in a similar way we define $W_q(S)$, Φ_S, $\mathcal{M}(W_q(S))$, and $\mathcal{M}(W(S))$. We view $W_q(S)$ as a scheme and by a $W_q(S)$-module we mean a quasi-coherent module over the structure ring sheaf $\mathcal{O}_{W_q(S)}$ of $W_q(S)$. The formal scheme $W(S)$ is used only as a notation. If $S = \mathrm{Spec}(R)$, then we identify canonically $\mathcal{M}(W_q(R)) = \mathcal{M}(W_q(S))$ and $\mathcal{M}(W(R)) = \mathcal{M}(W(S))$. If $t \in \{1, \ldots, q\}$ and $*(q)$ is a morphism of $\mathcal{M}(W_q(S))$, let $*(t)$ be the morphism of $\mathcal{M}(W_t(S))$ that is the tensorization of $*(q)$ with $W_t(S)$. Let S^{top} be the topological space underlying S. All crystals over S (i.e. all crystals on Berthelot's crystalline site $\mathrm{CRIS}(S/\mathrm{Spec}(\mathbf{Z}_p))$) are in locally free sheaves of finite rank. An F-crystal $\mathfrak{C}$ over S comprises from a crystal $\mathfrak{M}$ over S and an isogeny $\Phi_S^*(\mathfrak{M}) \to \mathfrak{M}$ of crystals over S; let $h_{\mathfrak{C}} \in \mathbf{N} \cup \{0\}$ be the smallest number such that $p^{h_{\mathfrak{C}}}$ annihilates the cokernel of this isogeny. We

identify an F-crystal (respectively an F-isocrystal) over $\mathrm{Spec}(k)$ with a latticed F-isocrystal (M, φ) over k that has the property that $\varphi(M) \subseteq M$ (respectively with an F-isocrystal over k as defined in Section 1). The pulls back of F-crystals $\mathfrak{C}$ and $\mathfrak{C}_*$ over S to an S-scheme S_1 (respectively to an affine S-scheme $\mathrm{Spec}(R_1)$) are denoted by $\mathfrak{C}_{S_1}$ and $\mathfrak{C}_{*S_1}$ (respectively by $\mathfrak{C}_{R_1}$ and $\mathfrak{C}_{*R_1}$).

Let (M, φ, G) be a latticed F-isocrystal with a group over k. We refer to M as its $W(k)$-module. Let $r_M \in \mathbf{N} \cup \{0\}$ be the rank of M. If f_1 and f_2 are two $\mathbf{Z}$-endomorphisms of either M or $M[\frac{1}{p}]$, let $f_1 f_2 := f_1 \circ f_2$. Two $\mathbf{Z}$-endomorphisms of M are said to be congruent mod p^q if their reductions mod p^q coincide. Let $M^* := \mathrm{Hom}(M, W(k))$. Let

$$\mathcal{T}(M) := \bigoplus_{t, u \in \mathbf{N} \cup \{0\}} M^{\otimes t} \otimes_{W(k)} M^{* \otimes u}.$$

We denote also by φ the σ-linear automorphism of $\mathcal{T}(M)[\frac{1}{p}]$ that takes $f \in M^*[\frac{1}{p}]$ into $\sigma f \varphi^{-1} \in M^*[\frac{1}{p}]$ and that acts on $\mathcal{T}(M)[\frac{1}{p}]$ in the natural tensor product way. The canonical identification $\mathrm{End}(M[\frac{1}{p}]) = M[\frac{1}{p}] \otimes_{B(k)} M^*[\frac{1}{p}]$ is compatible with the φ actions (see 1.1(a) for the action of φ on $\mathrm{End}(M[\frac{1}{p}])$). If O is either a free $W(k)$-submodule or a $B(k)$-vector subspace of $\mathcal{T}(M)[\frac{1}{p}]$ such that $\varphi(M) \subseteq M$, then we denote also by φ the σ-linear endomorphism of O induced by φ. The $W(k)$-span of tensors $v_1, \ldots, v_n \in \mathcal{T}(M)[\frac{1}{p}]$ is denoted by $\langle v_1, \ldots, v_n \rangle$. The latticed F-isocrystal (M^*, φ) over k is called the dual of (M, φ). We emphasize that the pair (M^*, φ) involves no Tate twist. A bilinear form on M is called perfect if it defines naturally a $W(k)$-linear isomorphism $M \xrightarrow{\sim} M^*$.

Let $\widetilde{G}_{B(k)}$ be a connected subgroup of $\mathbf{GL}_{M[\frac{1}{p}]}$. As φ is a σ-linear automorphism of $M[\frac{1}{p}]$, the group $\{\varphi \tilde{g} \varphi^{-1} \mid \tilde{g} \in \widetilde{G}_{B(k)}(B(k))\}$ is the group of $B(k)$-valued points of the unique connected subgroup of $\mathbf{GL}_{M[\frac{1}{p}]}$ that has $\varphi(\mathrm{Lie}(\widetilde{G}_{B(k)}))$ as its Lie algebra (see [1, Ch. II, 7.1] for the uniqueness part). So as φ normalizes $\mathrm{Lie}(G_{B(k)})$, for $g \in G(B(k))$ we have $\varphi g \varphi^{-1} \in G(B(k))$; in what follows this fact is used without any extra comment.

In this paragraph we assume $\varphi(M) \subseteq M$. We also refer to (M, φ, G) as an F-crystal with a group over k. The Hodge slopes of (M, φ) (see [22, 1.2]) are the non-negative integers $h_1, \ldots, h_{r_M}$ such that the torsion $W(k)$-module $M/\varphi(M)$ is isomorphic to $\bigoplus_{i=1}^{r_M} W(k)/(p^{h_i})$. If O is a $W(k)$-submodule of M such that $\varphi(O) \subseteq O$, we denote also by φ the σ-linear endomorphism of M/O induced by φ. We refer to the triple $(M/p^q M, \varphi, G_{W_q(k)})$ as the reduction mod p^q of (M, φ, G). If $G = \mathbf{GL}_M$, then often we do not mention G and $G_{W_q(k)}$ and we omit "with a group". The reduction $(M/p^q M, \varphi) \bmod p^q$ of (M, φ) is an object of $\mathcal{M}(W_q(k))$.

If $a, b \in \mathbf{Z}$ with $b \geqslant a$, let $S(a, b) := \{a, a+1, \ldots, b\}$. If $l \in \mathbf{N}$, if $*$ is a small letter, and if $(*_1, \ldots, *_l)$ is an l-tuple which is either an element of $\mathbf{Z}^l$ or an ordered $W(k)$-basis of some $W(k)$-module, then we define $*_t$ for any $t \in \mathbf{Z}$ via the rule: $*_t := *_u$, where $u \in \{1, \ldots, l\} \cap (t + l\mathbf{Z})$. If $x \in \mathbf{R}$, let $[x]$ be the greatest integer of the interval $(-\infty, x]$.

2.1.1. Conventions on stratifications

Let K be a field. By a *stratification* $\mathcal{S}$ of a reduced $\mathrm{Spec}(K)$-scheme X (*in potentially an infinite number of strata*), we mean that:

(i) for any field L that is either K or an algebraically closed field that contains K, a set $\mathcal{S}_L$ of disjoint reduced, locally closed subschemes of X_L is given such that each point of X_L with values in an algebraic closure of L factors through some element of $\mathcal{S}_L$;

(ii) if $i_{12} : L_1 \hookrightarrow L_2$ is an embedding between two fields as in (a), then the reduced scheme of the pull back to L_2 of any member of $\mathcal{S}_{L_1}$, is an element of $\mathcal{S}_{L_2}$; so we have a natural pull back injective map $\mathcal{S}(i_{12}) : \mathcal{S}_{L_1} \hookrightarrow \mathcal{S}_{L_2}$.

If the inductive limit of all maps $\mathcal{S}(i_{12})$ exists (respectively does not exist) in the category of sets, then we say that the stratification $\mathcal{S}$ has a *class* which is (respectively is not) a set. Each element of some set $\mathcal{S}_L$ is referred as a *stratum* of $\mathcal{S}$. We say $\mathcal{S}$ satisfies the *purity property* if for any field L as in (a), every element of $\mathcal{S}_L$ is an affine X_L-scheme.[1] Thus $\mathcal{S}$ satisfies the purity property if and only if each stratum of it is an affine X-scheme. If all maps $\mathcal{S}(i_{12})$'s are bijections, then we identify $\mathcal{S}$ with $\mathcal{S}_K$ and we say $\mathcal{S}$ is *of finite type*.

2.2. Definitions and simple properties

In this section we introduce few notions and simple properties that pertain naturally to latticed F-isocrystals.

2.2.1. Complements to 1.1

(a) A morphism (respectively an isogeny) between two latticed F-isocrystals (M_1, φ_1) and (M_2, φ_2) over k is a $W(k)$-linear map (respectively isomorphism) $f : M_1[\frac{1}{p}] \to M_2[\frac{1}{p}]$ such that $f\varphi_1 = \varphi_2 f$ and $f(M_1) \subseteq M_2$. If f is an isogeny, then by its degree we mean p^l, where l is the length of the artinian $W(k)$-module $M_2/f(M_1)$.

(b) By a *latticed F-isocrystal with a group and an emphasized family of tensors* over k we mean a quadruple

$$\left(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}} \right),$$

where (M, φ, G) is a latticed F-isocrystal with a group over k, where $\mathcal{J}$ is a set of indices, and where $t_\alpha \in \mathcal{T}(M)$ is a tensor that is fixed by both φ and G, such that $G_{B(k)}$ is the subgroup of $\mathbf{GL}_{M[\frac{1}{p}]}$ that fixes t_α for all $\alpha \in \mathcal{J}$. If $(M_1, \varphi_1, G_1, (t_{1\alpha})_{\alpha \in \mathcal{J}})$ and $(M_2, \varphi_2, G_2, (t_{2\alpha})_{\alpha \in \mathcal{J}})$ are two latticed F-isocrystals with a group and an emphasized family of tensors (indexed by the same set $\mathcal{J}$) over k, by an isomorphism between them we mean an isomorphism $f : (M_1, \varphi_1, G_1) \xrightarrow{\sim} (M_2, \varphi_2, G_2)$ such that the $W(k)$-linear isomorphism $\mathcal{T}(M_1) \xrightarrow{\sim} \mathcal{T}(M_2)$ induced by f, takes $t_{1\alpha}$ into $t_{2\alpha}$ for all $\alpha \in \mathcal{J}$.

(c) By a *principal bilinear quasi-polarized latticed F-isocrystal with a group* over k we mean a quadruple $(M, \varphi, G, \lambda_M)$, where (M, φ, G) is a latticed F-isocrystal with a group over k and where $\lambda_M : M \otimes_{W(k)} M \to W(k)$ is a perfect bilinear form with the properties that the $W(k)$-span of λ_M is normalized by G and that there exists $c \in \mathbf{Z}$ such that we have $\lambda_M(\varphi(x), \varphi(y)) = p^c \sigma(\lambda_M(x, y))$ for all $x, y \in M$. We refer to λ_M as a principal bilinear quasi-polarization of (M, φ, G), (M, φ), and $(M[\frac{1}{p}], \varphi)$. Let G^0 be the Zariski closure in $\mathbf{GL}_M$ of the identity component of the subgroup of $G_{B(k)}$ that fixes λ_M. We refer to (M, φ, G^0) as the latticed F-isocrystal with a group over k of $(M, \varphi, G, \lambda_M)$. The quotient group $G_{B(k)}/G^0_{B(k)}$ is either trivial or isomorphic to $\mathbf{G}_m$.

By an isomorphism between two principal bilinear quasi-polarized latticed F-isocrystals with a group $(M_1, \varphi_1, G_1, \lambda_{M_1})$ and $(M_2, \varphi_2, G_2, \lambda_{M_2})$ over k we mean an isomorphism $f : (M_1, \varphi_1, G_1) \xrightarrow{\sim} (M_2, \varphi_2, G_2)$ such that we have $\lambda_{M_1}(x, y) = \lambda_{M_2}(f(x), f(y))$ for all $x, y \in M_1$. We speak also about principal bilinear quasi-polarized latticed F-isocrystals with a group and an emphasized family of tensors over k and about isomorphisms between them; notation $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}}, \lambda_M)$.

---

[1] This is a more practical, refined, and general definition than any other one that relies on codimension 1 statements on complements. See Remark 6.3(a) below.

If the form λ_M is alternating, we drop the word bilinear (i.e. we speak about *principal quasi-polarized latticed F-isocrystals with a group* over k, etc.).

(d) We say the *W-condition* holds for the latticed F-isocrystal with a group (M,φ,G) over k if there exists a direct sum decomposition $M = \bigoplus_{i=a}^{b} \widetilde{F}^i(M)$, where $a, b \in \mathbf{Z}$ with $b \geqslant a$, such that $M = \bigoplus_{i=a}^{b} \varphi(p^{-i}\widetilde{F}^i(M))$ and the cocharacter $\mu\colon \mathbf{G}_m \to \mathbf{GL}_M$ defined by the property that $\beta \in \mathbf{G}_m(W(k))$ acts on $\widetilde{F}^i(M)$ through μ as the multiplication by β^{-i}, factors through G. In such a case we also refer to (M,φ,G) as a *p-divisible object with a group* over k. We refer to the factorization $\mu\colon \mathbf{G}_m \to G$ of μ as a *Hodge cocharacter* of (M,φ,G). For $i \in S(a,b)$ let $F^i(M) := \bigoplus_{j=b}^{i} \widetilde{F}^j(M)$. We refer to the decreasing and exhaustive filtration $(F^i(M))_{i \in S(a,b)}$ of M as a *lift* of (M,φ,G). If $G = \mathbf{GL}_M$, we also refer to (M,φ) as a *p-divisible object* over k.

Here "W" stands to honor [42, p. 512] while the notion "p-divisible object" is a natural extrapolation of the terminology "object" introduced in [11, §2].

(e) By the *shifting number* (to be abbreviated as the *s-number*) of a latticed F-isocrystal (M,φ) over k we mean the smallest number $s \in \mathbf{N} \cup \{0\}$ such that $\varphi(p^s M) \subseteq M$ (equivalently such that $\varphi(M) \subseteq p^{-s}M$). By the *greatest Hodge slope* (to be abbreviated as the *h-number*) of (M,φ) we mean the greatest Hodge slope h of $(M,p^s\varphi)$, i.e. the unique number $h \in \mathbf{N} \cup \{0\}$ such that we have $p^{h-s}M \subseteq \varphi(M)$ and $p^{h-s-1}M \not\subseteq \varphi(M)$.

We have $s = 0$ if and only if (M,φ) is an F-crystal over k; in this case h is the number $h_{(M,\varphi)}$ defined in 2.1. We have $s = 0$ and $h \in \{0,1\}$ if and only if (M,φ) is a Dieudonné module over k.

Let s^* and h^* be the s-number and the h-number (respectively) of (M^*,φ). We have $\varphi(M^*) = \varphi(M)^* \subseteq p^{s-h}M^*$ but $\varphi(M^*) \not\subseteq p^{s-h+1}M^*$. Thus $s^* = \max\{0, h-s\}$. As (M,φ) is the dual of (M^*,φ), we also have $s = \max\{0, h^*-s^*\}$. So if $s = 0$, then $s^* = h$ and $h^* \in S(0,h)$. If $s > 0$, then $s = h^* - s^*$ and thus $h^* = s + s^* = \max(s,h)$.

If $s = 0$, then the s-number and the h-number of $(\mathrm{End}(M),\varphi) = (M,\varphi) \otimes (M^*,\varphi)$ are at most $s + s^* = h$ and $h + h^* \leqslant 2h$ (respectively).

2.2.2. DEFINITIONS. –

(a) Let (M,φ) be a p-divisible object (M,φ) over k. We say (M,φ) is a *cyclic Dieudonné–Fontaine p-divisible object* over k if there exists a $W(k)$-basis $\{e_1,\ldots,e_{r_M}\}$ of M such that for $i \in S(1,r_M)$ we have an identity $\varphi(e_i) = p^{n_i}e_{i+1}$, where $n_1,\ldots,n_{r_M}$ are integers that are either all non-negative or all non-positive. We refer to $\{e_1,\ldots,e_{r_M}\}$ as a *standard $W(k)$-basis* of (M,φ).

We say (M,φ) is an *elementary Dieudonné–Fontaine p-divisible object* over k if it is a cyclic Dieudonné–Fontaine p-divisible object over k that is not the direct sum of two or more non-trivial cyclic Dieudonné–Fontaine p-divisible objects over k.

We say (M,φ) is an *elementary Dieudonné p-divisible object* over k if there exists a $W(k)$-basis $\{e_1,\ldots,e_{r_M}\}$ of M such that for $i \in S(2,r_M)$ we have an identity $\varphi(e_i) = e_{i+1}$ and moreover $\varphi(e_1) = p^{n_1}e_2$ for some integer n_1 that is relatively prime to r_M.

We say (M,φ) is a *Dieudonné–Fontaine* (respectively *a Dieudonné*) *p-divisible object* over k if it is a direct sum of elementary Dieudonné–Fontaine (respectively of elementary Dieudonné) p-divisible objects over k.

(b) By the *Dieudonné–Fontaine torsion* (respectively *volume*) of a latticed F-isocrystal (M,φ) over k we mean the smallest number

$$\mathbf{T}(M,\varphi) \in \mathbf{N} \cup \{0\}$$

(respectively $\mathbf{V}(M,\varphi) \in \mathbf{N} \cup \{0\}$) such that there exists a Dieudonné–Fontaine p-divisible object (M_1,φ_1) over $\bar{k}$ for which we have an isogeny

$f : (M_1, \varphi_1) \hookrightarrow (M \otimes_{W(k)} W(\bar{k}), \varphi \otimes \sigma_{\bar{k}})$ with the property that $p^{\mathbf{T}(M,\varphi)} M \subseteq f(M_1)$ (respectively that $M/f(M_1)$ has length $\mathbf{V}(M, \varphi)$). By replacing Dieudonné–Fontaine with Dieudonné, in a similar way we define the *Dieudonné torsion* $\mathbf{T}_+(M, \varphi) \in \mathbf{N} \cup \{0\}$ and the *Dieudonné volume* $\mathbf{V}_+(M, \varphi) \in \mathbf{N} \cup \{0\}$ of (M, φ).

2.2.2.1. *Remarks.* – (a) Any (elementary) Dieudonné p-divisible object over k is also an (elementary) Dieudonné–Fontaine p-divisible object over k. Moreover, any Dieudonné–Fontaine p-divisible object over k is definable over $\mathbf{F}_p$.

(b) The existence of $\mathbf{V}_+(M, \varphi)$ (and thus also of $\mathbf{V}(M, \varphi)$, $\mathbf{T}_+(M, \varphi)$, and $\mathbf{T}(M, \varphi)$) is equivalent to Dieudonné's classification of F-isocrystals over $\bar{k}$. This and the fact that suitable reductions (modulo powers of p) of p-divisible objects over k are studied systematically for the first time in [14,15], explains our terminology.

(c) Classically one works only with Dieudonné p-divisible objects (as they are uniquely determined by their Newton polygons) and with Dieudonné volumes (as they keep track of degrees of isogenies); see [7,28,6,10], etc. But working with Dieudonné–Fontaine p-divisible objects and torsions one can get considerable improvements for many practical calculations or upper bounds (like the ones we will encounter in Section 3).

2.2.3. LEMMA. – *Let K be an algebraically closed field that contains k. Let (M, φ) be a Dieudonné–Fontaine p-divisible object over k with the property that $\varphi(M) \subseteq M$. Let h be the h-number of (M, φ), let $e_M := \max\{r_M, [\frac{r_M^2}{4}]\}$, let k_1 be the composite field of k and $\mathbf{F}_{p^{r_M!}}$, and let $m \in \mathbf{N}$. We have the following two properties:*
  (a) *For any endomorphism $f_{he_M + m}$ of $(M \otimes_{W(k)} W_{he_M + m}(K), \varphi \otimes \sigma_K)$, the reduction $f_m \mod p^m$ of $f_{he_M + m}$ is the scalar extension of an endomorphism of $(M \otimes_{W(k)} W_m(k_1), \varphi \otimes \sigma_{k_1})$. If (M, φ) is a Dieudonné p-divisible object over k, then the previous sentence holds with e_M being substituted by r_M.*
  (b) *Each endomorphism of $(M \otimes_{W(k)} W(K), \varphi \otimes \sigma_K)$ is the scalar extension of an endomorphism of $(M \otimes_{W(k)} W(k_1), \varphi \otimes \sigma_{k_1})$.*

Proof. – We write $(M, \varphi) = \bigoplus_{i=1}^s (M_i, \varphi)$ as a direct sum of elementary Dieudonné–Fontaine p-divisible objects over k. Let $\{e_1^{(i)}, \ldots, e_{r_{M_i}}^{(i)}\}$ be a standard $W(k)$-basis of (M_i, φ). We check that (a) holds. Let $i_0 \in S(1, s)$ and let $j_0 \in S(1, r_{M_{i_0}})$. We write $f_{he_M + m}(e_{j_0}^{(i_0)} \otimes 1) = \sum_{i=1}^s \sum_{j=1}^{r_{M_i}} e_j^{(i)} \otimes \beta_{j_0 j}^{(i_0 i)}$, where all $\beta_{j_0 j}^{(i_0 i)}$'s belong to $W_{he_M + m}(K)$. Let $r_{M_{i_0 i}} := l.c.m.\{r_{M_{i_0}}, r_{M_i}\}$; it is a divisor of $r_M!$. If $i = i_0$, then $r_{M_{i_0 i}} = r_{M_{i_0}} \leqslant r_M \leqslant e_M$. If $i \neq i_0$, then $r_{M_{i_0}} + r_{M_i} \leqslant r_M$ and thus we have $r_{M_{i_0 i}} \leqslant r_{M_{i_0}} r_{M_i} \leqslant [\frac{r_M^2}{4}] \leqslant e_M$.

As $f_{he_M + m}(\varphi^{r_{M_{i_0 i}}}(e_{j_0}^{(i_0)}) \otimes 1) = (\varphi \otimes \sigma_K)^{r_{M_{i_0 i}}}(f_{he_M + m}(e_{j_0}^{(i_0)} \otimes 1))$, we have an equality

(1) $$p^{m_{j_0}^{(i_0 i)}} \beta_{j_0 j}^{(i_0 i)} = p^{q_j^{(i_0 i)}} \sigma_K^{r_{M_{i_0 i}}} \left(\beta_{j_0 j}^{(i_0 i)} \right) \in W_{he_M + m}(K),$$

where $m_{j_0}^{(i_0 i)} \in \mathbf{N} \cup \{0\}$ is such that $\varphi^{r_{M_{i_0 i}}}(e_{j_0}^{(i_0)}) = p^{m_{j_0}^{(i_0 i)}} e_{j_0}^{(i_0)}$ and where $q_j^{(i_0 i)} \in \mathbf{N} \cup \{0\}$ is such that $\varphi^{r_{M_{i_0 i}}}(e_j^{(i)}) = p^{q_j^{(i_0 i)}} e_j^{(i)}$. The numbers $m_{j_0}^{(i_0 i)}$ and $q_j^{(i_0 i)}$ are at most $h r_{M_{i_0 i}}$ and so at most $h e_M$. Let $s_{j_0 j}^{(i_0 i)} \in S(0, he_M + m)$ be the unique number such that we can write $\beta_{j_0 j}^{(i_0 i)} = p^{s_{j_0 j}^{(i_0 i)}} \tilde{\beta}_{j_0 j}^{(i_0 i)}$, with $\tilde{\beta}_{j_0 j}^{(i_0 i)} \in \mathbf{G}_m(W_{he_M + m}(K))$. From (1) we easily get that

$$t_{j_0 j}^{(i_0 i)} := \min\{he_M + m, m_{j_0}^{(i_0 i)} + s_{j_0 j}^{(i_0 i)}\} \quad \text{equals to} \quad \min\{he_M + m, q_j^{(i_0 i)} + s_{j_0 j}^{(i_0 i)}\}$$

and that $\sigma_K^{r_{M_{i_0 i}}}(\tilde{\beta}_{j_0 j}^{(i_0 i)})$ and $\tilde{\beta}_{j_0 j}^{(i_0 i)}$ coincide mod $p^{he_M + m - t_{j_0 j}^{(i_0 i)}}$. Thus $\tilde{\beta}_{j_0 j}^{(i_0 i)}$ mod $p^{he_M + m - t_{j_0 j}^{(i_0 i)}}$

belongs to $W_{he_M + m - t_{j_0 j}^{(i_0 i)}}(\mathbf{F}_p{}^{r_{M_{i_0 i}}})$ and therefore $\beta_{j_0 j}^{(i_0 i)}$ mod $p^{he_M + m - t_{j_0 j}^{(i_0 i)} + s_{j_0 j}^{(i_0 i)}}$ belongs to

$W_{he_M + m - t_{j_0 j}^{(i_0 i)} + s_{j_0 j}^{(i_0 i)}}(\mathbf{F}_p{}^{r_{M_{i_0 i}}})$. As $-m_{j_0}^{(i_0 i)} \leqslant -t_{j_0 j}^{(i_0 i)} + s_{j_0 j}^{(i_0 i)}$, we get that

$\beta_{j_0 j}^{(i_0 i)}$ mod $p^{he_M + m - m_{j_0}^{(i_0 i)}}$ belongs to $W_{he_M + m - m_{j_0}^{(i_0 i)}}(\mathbf{F}_p{}^{r_{M_{i_0 i}}})$ and thus also to

$W_{he_M + m - m_{j_0}^{(i_0 i)}}(k_1)$. So due to the inequality $m \leqslant he_M + m - m_{j_0}^{(i_0 i)}$, we have $f_m(e_{j_0}^{(i_0)} \otimes 1) \in$
$M \otimes_{W(k)} W_m(k_1)$ for any pair $(i_0, j_0) \in S(1, s) \times S(1, r_{M_{i_0}})$. Thus f_m is the scalar extension of an endomorphism of $(M \otimes_{W(k)} W_m(k_1), \varphi \otimes \sigma_{k_1})$.

If (M, φ) is a Dieudonné p-divisible object over k, then the Hodge slopes of (M_{i_0}, φ) are $0, \ldots, 0$, and some integer in $S(0, h)$; thus $m_{j_0}^{(i_0 i)} \leqslant h \frac{r_{M_{i_0 i}}}{r_{M_{i_0}}} \leqslant hr_{M_i} \leqslant hr_M$. A similar argument shows that $q_j^{(i_0 i)} \leqslant hr_M$. Thus in the previous paragraph we can substitute e_M by r_M. So (a) holds.

Part (b) follows from (a) by taking $m \to \infty$. $\square$

2.2.4. Deviations of tuples

Let $l \in \mathbf{N}$. Let $\tau = (n_1, \ldots, n_l) \in \mathbf{Z}^l$.

(a) Suppose $\sum_{i=1}^l n_i$ is non-negative (respectively is non-positive). Let $P(\tau)$ be the set of pairs (t, u), where $t \in S(1, l)$ and $u \in S(t, l + t - 1)$ have the property that all sums $\sum_{i=v}^u n_i$ with $v \in S(t, u)$ are non-positive (respectively are non-negative). By the non-negative (respectively the non-positive) sign deviation of τ we mean the non-negative integer $\max\{0, -\sum_{i=t}^u n_i \mid (t, u) \in P(\tau)\}$ (respectively $\max\{0, \sum_{i=t}^u n_i \mid (t, u) \in P(\tau)\}$).

(b) If $\sum_{i=1}^l n_i$ is non-negative (respectively is non-positive), then by the non-negative (respectively the non-positive) value deviation of τ we mean the absolute value of the sum of all non-positive (respectively of all non-negative) entries of τ. As a convention, this sum is 0 if τ has no non-positive (respectively no non-negative) entries.

(c) If $\sum_{i=1}^l n_i$ is positive (respectively is negative), then by the sign deviation $\mathbf{S}\tau$ of τ we mean its non-negative (respectively its non-positive) sign deviation. If $\sum_{i=1}^l n_i = 0$, then by the sign deviation $\mathbf{S}\tau$ of τ we mean the smaller of its non-negative and non-positive sign deviations. We also use this definition with (sign, $\mathbf{S}$) replaced by (value, $\mathbf{W}$).

Samples: $\mathbf{S}(-1, 1, -1, -1, 1, 1, 0, -1) = 1 + 1 = 2$, $\mathbf{W}(-1, 1, -1, -1, 1, 1, 0, -1) = 3$, $\mathbf{S}(1, 1, -2, 1, 3) = \mathbf{W}(1, 1, -2, 1, 3) = 2$, and $\mathbf{S}(-1, 1, -1) = \mathbf{W}(-1, 1, -1) = 1$.

2.3. Inequalities

Let (M, φ) be a latticed F-isocrystal over k. Obviously $\mathbf{V}(M, \varphi) \leqslant \mathbf{V}_+(M, \varphi)$ and $\mathbf{T}(M, \varphi) \leqslant \mathbf{T}_+(M, \varphi)$. Moreover we have

$$\mathbf{T}(M, \varphi) \leqslant \mathbf{V}(M, \varphi) \leqslant \mathbf{T}(M, \varphi) r_M$$

and the same inequalities hold with $(\mathbf{T}, \mathbf{V})$ being replaced with $(\mathbf{T}_+, \mathbf{V}_+)$.

2.3.1. LEMMA. – *Let $\tau = (n_1, \ldots, n_{r_M}) \in \mathbf{Z}^{r_M}$. Suppose there exists a $W(k)$-basis $\{e_1, \ldots, e_{r_M}\}$ of M such that for $i \in S(1, r_M)$ we have $\varphi(e_i) = p^{n_i} e_{i+1}$. Then we have the following sequence of three inequalities*

$$(2) \qquad \mathbf{T}(M, \varphi) \leqslant \mathbf{S}\tau \leqslant \mathbf{W}\tau \leqslant |n_1| + |n_2| + \cdots + |n_{r_M}|.$$

Proof. – The second and the third inequalities follow from their very definitions.

We check the first inequality of (2) only in the case when $\sum_{i=1}^{r_M} n_i > 0$ and at least one entry n_i is negative, as in all other cases the first inequality of (2) is checked in the same way. We perform the following type of operation.

Let $u \in \mathbf{N} \cup \{0\}$ be the greatest number such that there exists $t \in S(1, r_M)$ with the property that $n_{t-v,t} := \sum_{i=t-v}^{t} n_i$ is non-positive for all $v \in S(0, u)$; we have $n_{t+1} > 0$, $n_{t-u-1} > 0$, and $\sum_{i=t-u-1}^{t} n_i > 0$. For $v \in S(0, u)$ we replace e_{t-v} by $\tilde{e}_{t-v} := p^{-n_{t-v,t}} e_{t-v}$. Up to a cyclic rearrangement of τ, we can assume $t - u = 1$; so $t = 1 + u$ and $n_{r_M} = n_0 = n_{t-u-1} > 0$. The r_M-tuple $(\tilde{e}_1, \ldots, \tilde{e}_{u+1}, e_{u+2}, \ldots, e_{r_M})$ is mapped by φ into the r_M-tuple $(\tilde{e}_2, \ldots, \tilde{e}_{u+1}, e_{u+2}, p^{n_{u+2}} e_{u+3}, \ldots, p^{n_{r_M}-1} e_{r_M}, p^{\sum_{i=0}^{u+1} n_i} \tilde{e}_1)$. We have $\sum_{i=0}^{u+1} n_i = \sum_{i=t-u-1}^{t} n_i > 0$. So if for all $i \in S(u+2, r_M - 1)$ we have $n_i \geqslant 0$, then the pair $(\langle \tilde{e}_1, \ldots, \tilde{e}_{u+1}, e_{u+2}, \ldots, e_{r_M} \rangle, \varphi)$ is a cyclic Dieudonné–Fontaine p-divisible object over k and we are done as by their very definitions, we have $-n_{t-v,t} \in S(0, \mathbf{S}\tau)$ and thus $p^{\mathbf{S}\tau}$ annihilates the quotient $W(k)$-module $M/\langle \tilde{e}_1, \ldots, \tilde{e}_{u+1}, e_{u+2}, \ldots, e_{r_M} \rangle$; if this is not the case, we next deal with the inoperated entries $n_{u+2}, \ldots, n_{r_M}$.

We repeat the operation as follows. Let $u_1 \in \mathbf{N} \cup \{0\}$ be the greatest number such that there exists $t_1 \in S(u+2, r_M)$ with the property that $n_{t_1-v_1,t_1} := \sum_{i=t_1-v_1}^{t_1} n_i$ is non-positive for all $v_1 \in S(0, u_1)$; we have $n_{t_1+1} > 0$, $n_{t_1-u_1-1} > 0$, and $\sum_{i=t_1-u_1-1}^{t_1} n_i > 0$. Due to the "greatest" property of u we have $t_1 - u_1 > u + 2$. For $v_1 \in S(0, u_1)$ we replace $e_{t_1-v_1}$ by $\tilde{e}_{t_1-v_1} := p^{-n_{t_1-v_1,t_1}} e_{t_1-v_1}$ and we repeat the operation for the inoperated entries $n_{u+2}, n_{u+3}, \ldots, n_{t_1-u_1-1}, n_{t_1+1}, n_{t_1+2}, \ldots, n_{r_M}$. By induction on the number of remaining inoperated entries (they do not have to be indexed by a set of consecutive numbers in $S(1, r_M)$), we get that the first inequality of (2) holds. $\square$

2.3.2. *Example.* – If for $i \in S(1, r_M)$ we have $n_i \in \{-1, 0, 1\}$, then from (2) we get

$$(3) \qquad\qquad \mathbf{T}(M, \varphi) \leqslant \mathbf{W}\tau = \min\{n^-, n^+\},$$

where n^- (respectively n^+) is the number of i's such that $n_i = -1$ (respectively such that $n_i = 1$).

We now consider the case when $r_M \geqslant 3$ and $(n_1, n_2, \ldots, n_{r_M}) = (1, 1, \ldots, 1, -1)$. So (M, φ) has a unique slope $\frac{r_M - 2}{r_M}$ that is positive. As $\varphi(M) \not\subseteq M$, we have $\mathbf{T}(M, \varphi) \geqslant 1$. But $\mathbf{T}(M, \varphi) \leqslant 1$, cf. (3). Thus $\mathbf{T}(M, \varphi) = 1$. In fact $(\langle e_1, \ldots, p e_{r_M} \rangle, \varphi)$ is an elementary Dieudonné–Fontaine p-divisible object over k whose Hodge slopes are $0, 0, 1, \ldots, 1$. It is easy to see that $\mathbf{T}_+(M, \varphi) = r_M - 2$; so $\mathbf{T}_+(M, \varphi) > \mathbf{T}(M, \varphi)$ for $r_M > 3$.

2.4. Estimates

Let (M, φ) be a latticed F-isocrystal over k. Let s and h be the s-number and the h-number (respectively) of (M, φ). Let $\mathcal{H}$ be the set of slopes of $(M[\frac{1}{p}], \varphi)$. If $\alpha \in \mathcal{H}$, we write $\alpha = \frac{a_\alpha}{b_\alpha}$, where $(a_\alpha, b_\alpha) \in \mathbf{Z} \times \mathbf{N}$ with $g.c.d.(a_\alpha, b_\alpha) = 1$.

2.4.1. LEMMA. – *Suppose $k = \bar{k}$. Let $(a, b, c) \in \mathbf{N} \times (\mathbf{N} \cup \{0\}) \times (\mathbf{N} \cup \{0\})$. There exists a smallest number*

$$d(a, b, c) \in \mathbf{N} \cup \{0\}$$

(respectively $d_+(a, b, c) \in \mathbf{N} \cup \{0\}$) such that for any latticed F-isocrystal $\mathfrak{C}$ over k of rank a, s-number b, and h-number c, we have an inequality $\mathbf{T}(\mathfrak{C}) \leqslant d(a, b, c)$ (respectively $\mathbf{T}_+(\mathfrak{C}) \leqslant d_+(a, b, c)$). In particular, for any element $g \in \mathbf{GL}_M(W(k))$ we have $\mathbf{T}(M, g\varphi) \leqslant d(r_M, s, h)$.

Moreover upper bounds of $d(a,b,c)$ (respectively of $d_+(a,b,c)$) are effectively computable in terms of a, b, and c.

Proof. – As $\mathbf{T}(\mathfrak{C}) \leqslant \mathbf{T}_+(\mathfrak{C})$, it suffices to prove the lemma for $d_+(a,b,c)$. To ease the notations, we will assume that $(r_M, s, h) = (a, b, c)$ and that $(M, \varphi) = \mathfrak{C}$. We have

$$(4) \qquad \mathbf{T}_+(M, \varphi) \leqslant s\big(\max\{b_\alpha \mid \alpha \in \mathcal{H}\} - 1\big) + \mathbf{T}_+\big(M, p^s\varphi\big).$$

To check this inequality we first remark that if O is a $W(k)$-submodule of M such that the pair $(O, p^s\varphi)$ is an elementary Dieudonné p-divisible object over k and if $\{e_1, \ldots, e_{r_O}\}$ is a standard $W(k)$-basis of $(O, p^s\varphi)$ such that we have $(p^s\varphi)(e_i) = e_{i+1}$ for all $i \in S(1, r_O - 1)$, then the following pair $(O', \varphi) := (\langle p^{r_O s - s} e_1, p^{r_O s - 2s} e_2, \ldots, p^s e_{r_O - 1}, e_{r_O}\rangle, \varphi)$ is an elementary Dieudonné p-divisible object over k. As $(O[\frac{1}{p}], \varphi)$ is a simple F-isocrystal over k whose unique slope belongs to $\mathcal{H}$, we have $r_O \leqslant \max\{b_\alpha \mid \alpha \in \mathcal{H}\}$. From this and the fact that O/O' is annihilated by $p^{s(r_O - 1)}$, we easily get that (4) holds.

Thus it suffices to prove the existence of a number $d_+(a,b,c)$ that has all the required properties under the extra assumption $b = s = 0$; as $s = 0$, we have $\mathcal{H} \subseteq [0, h]$. We will use an induction on $a = r_M$. The case $a = 1$ is trivial. To accomplish for $a \geqslant 2$ the inductive passage from $a - 1 = r_M - 1$ to $a = r_M$, we consider two disjoint cases.

Case 1. Suppose the F-isocrystal $(M[\frac{1}{p}], \varphi)$ over k is not simple. Let $\alpha \in \mathcal{H}$. We consider a short exact sequence $0 \to (M_1, \varphi) \to (M, \varphi) \to (M_2, \varphi) \to 0$ such that the F-isocrystal $(M_2[\frac{1}{p}], \varphi)$ over k is simple of α. For $i \in S(1, 2)$, the h-number of (M_i, φ) is at most h and we have $r_{M_i} < a = r_M$. By induction, there exists $d_i \in \mathbf{N} \cup \{0\}$ that has upper bounds effectively computable in terms of r_{M_i} and $c = h$ and such that there exists a $W(k)$-submodule O_i of M_i with the properties that $r_{O_i} = r_{M_i}$, that $p^{d_i} M_i \subseteq O_i$, and that (O_i, φ) is a Dieudonné p-divisible object over k. The map $\sigma^{b_\alpha} - 1_{W(k)} : W(k) \to W(k)$ is onto. This implies that $p^{a_\alpha} M_1 \subseteq (\varphi^{b_\alpha} - p^{a_\alpha} 1_{M_1})(M_1)$. Let $x \in O_2$ be such that $\varphi^{b_\alpha}(x) = p^{a_\alpha} x$ and $\varphi^{b_\alpha - 1}(x) \in O_2 \setminus pO_2$. If $\tilde{x} \in M$ maps into x, then there exists $y \in M_1$ such that $\varphi^{b_\alpha}(y) - p^{a_\alpha}(y)$ is $p^{a_\alpha}[\varphi^{b_\alpha}(\tilde{x}) - p^{a_\alpha}(\tilde{x})] \in p^{a_\alpha} M_1$. Thus $z := -y + p^{a_\alpha}\tilde{x} \in M$ maps into $p^{a_\alpha} x$ and we have $\varphi^{b_\alpha}(z) = p^{a_\alpha}(z)$. By choosing x to belong to a standard $W(k)$-basis of (O_2, φ), we get that the monomorphism $i_2 : (p^{a_\alpha} O_2, \varphi) \hookrightarrow (M_2, \varphi)$ lifts to a monomorphism $j_2 : (p^{a_\alpha} O_2, \varphi) \hookrightarrow (M, \varphi)$. As $(O_1 + j_2(p^{a_\alpha} O_2), \varphi)$ is a Dieudonné p-divisible object over k and as $p^{d_1 + d_2 + a_\alpha}$ annihilates $M/O_1 + j_2(p^{a_\alpha} O_2)$, we get

$$(5) \qquad \mathbf{T}_+(M, \varphi) \leqslant d_1 + d_2 + a_\alpha \leqslant d_1 + d_2 + hb_\alpha \leqslant d_1 + d_2 + hr_M.$$

Case 2. Suppose the F-isocrystal $(M[\frac{1}{p}], \varphi)$ over k is simple of slope α. Thus $a = r_M = b_\alpha$. Let $\{e_1, \ldots, e_a\} \subseteq M$ be a $B(k)$-basis of $M[\frac{1}{p}]$ such that $e_1 \in M \setminus pM$, for $i \in S(1, a-1)$ we have $\varphi(e_i) = e_{i+1}$, and $\varphi(e_a) = p^{a_\alpha} e_1$. For $t \in S(1, a)$, let $M_t := \langle e_1, \ldots, e_t \rangle$ and $\widetilde{M}_t := M_t[\frac{1}{p}] \cap M$. We have $M_1 = \widetilde{M}_1$ and $\widetilde{M}_a = M$.

2.4.1.1. CLAIM. – *There exists a strictly increasing sequence $(c_t)_{t \in S(1,a)}$ of non-negative integers that depends only on $a = r_M$ and $c = h$, that is effectively computable, and that has the property that for any $t \in S(1, a)$ we have inclusions*

$$(6) \qquad p^{c_t}(\widetilde{M}_t) \subseteq M_t \subseteq \widetilde{M}_t.$$

To check this claim we use induction on $t \in S(1, a)$. Taking $c_1 := 0$, (6) holds for $t = 1$. Suppose there exists a number $r \in S(1, a-1)$ such that (6) holds for $t \in S(1, r)$. We now check

that (6) holds for $t = r + 1$. Thus we have to show that there exists an effectively computable natural number c_{r+1} which is at least $c_r + 1$ and for which we have

$$(7) \qquad\qquad e_{r+1} = \varphi(e_r) \notin p^{1+c_{r+1}} M + \widetilde{M}_r.$$

We write $e_{r+1} = \varphi(e_r) = p^{n_r} x_r + y_r$, where $x_r \in M \setminus pM$, $n_r \in \mathbf{N} \cup \{0\}$, and $y_r \in \widetilde{M}_r$. By our initial induction (on ranks), we can speak about an effectively computable number $d_r \in \mathbf{N}$ that is at least $\max\{d_+(r, 0, l) \mid l \in S(0, h)\}$. Let

$$(8) \qquad\qquad c_{r+1} := c_r + d_r + r!ah.$$

We show that the assumption $n_r > c_{r+1}$ leads to a contradiction. Let $\widetilde{M}_0 := 0$. Let $\tilde{e}_r \in \widetilde{M}_r$ be such that we have a direct sum decomposition $\widetilde{M}_r = \widetilde{M}_{r-1} \oplus \langle \tilde{e}_r \rangle$. Based on (6) (applied with $t = r$), we can write $e_r = y_{r-1} + l_r \tilde{e}_r$, where $y_{r-1} \in \widetilde{M}_{r-1}$ and $l_r \in W(k) \setminus p^{c_r+1} W(k)$. Let $w_r := \sigma(l_r)^{-1}(y_r - \varphi(y_{r-1})) \in \widetilde{M}_r[\frac{1}{p}]$. We have $\varphi(\tilde{e}_r) = w_r + \sigma(l_r)^{-1} p^{n_r} x_r \in M$. As $n_r > c_{r+1} > c_r$, we have $\sigma(l_r)^{-1} p^{n_r} x_r \in p^{n_r - c_r} M \subseteq M$; thus $w_r \in \widetilde{M}_r = \widetilde{M}_r[\frac{1}{p}] \cap M$. Let η_r be the σ-linear endomorphism of $\widetilde{M}_r$ that acts on $\widetilde{M}_{r-1}$ as φ does and that takes $\tilde{e}_r$ into w_r; thus $\eta_r(e_r) = y_r$. The difference $\varphi(\tilde{e}_r) - \eta_r(\tilde{e}_r)$ is $\sigma(l_r)^{-1} p^{n_r} x_r \in p^{n_r - c_r} M$. Thus φ restricted to $\widetilde{M}_r$ and η_r, when viewed as maps from $\widetilde{M}_r$ to M, coincide mod $p^{n_r - c_r}$. From this and the inequality $n_r - c_r \geqslant h + 1$, we get that the pair $(\widetilde{M}_r, \eta_r)$ is an F-crystal over k whose h-number is at most h.

Let O_r be a $W(k)$-submodule of $\widetilde{M}_r$ such that $p^{\mathbf{T}_+(\widetilde{M}_r, \eta_r)} \widetilde{M}_r \subseteq O_r$ and (O_r, η_r) is a Dieudonné p-divisible object over k. Let $t_r \in S(0, \mathbf{T}_+(\widetilde{M}_r, \eta_r))$ be the smallest number such that $p^{t_r} e_1 \in O_r \setminus pO_r$. We consider a direct sum decomposition $(O_r, \eta_r) = (O_{r,1}, \eta_r) \oplus \cdots \oplus (O_{r,s_r}, \eta_r)$ into elementary Dieudonné p-divisible objects over k; we can assume that the indices are such that the component $e_{1,1} \in O_{r,1}$ of $p^{t_r} e_1 \in O_r$ with respect to this direct sum decomposition of O_r, is not divisible inside $O_{r,1}$ by p (i.e. we have $e_{1,1} \notin pO_{r,1}$). Let $u_r \in [0, h]$ be the unique slope of $(O_{r,1}, \eta_r)$.

The element $p^{r!a\alpha} e_1 = \varphi^{r!a}(e_1)$ is congruent mod $p^{n_r - c_r}$ to $\eta_r^{r!a}(e_1)$. As we have $p^{\mathbf{T}_+(\widetilde{M}_r, \eta_r)} \widetilde{M}_r \subseteq O_r$, we get that $\eta_r^{r!a}(e_{1,1}) - p^{r!a\alpha} e_1 \in p^{t_r + n_r - c_r - \mathbf{T}_+(\widetilde{M}_r, \eta_r)} O_{r,1}$; thus $\eta_r^{r!a}(e_{1,1}) - p^{r!a\alpha} e_1 \in p^{n_r - c_r - \mathbf{T}_+(\widetilde{M}_r, \eta_r)} O_{r,1}$. As $(O_{r,1}, \eta_r)$ is an elementary Dieudonné p-divisible object over k whose rank divides $r!a$ and as $e_{1,1} \in O_{r,1} \setminus pO_{r,1}$, there exists $z_r \in O_{r,1} \setminus pO_{r,1}$ such that $\eta_r^{r!a}(e_{1,1}) = p^{r!au_r} z_r$. Thus $p^{r!au_r} z_r - p^{r!a\alpha} e_{1,1} \in p^{n_r - c_r - \mathbf{T}_+(\widetilde{M}_r, \eta_r)} O_{r,1}$. As $d_r \geqslant \mathbf{T}_+(\widetilde{M}_r, \eta_r)$ and $n_r > c_{r+1}$, from (8) we get $n_r - c_r - \mathbf{T}_+(\widetilde{M}_r, \eta_r) \geqslant r!ha + 1$. As $h \geqslant \max\{u_r, \alpha\}$, we have $r!ah + 1 > \max\{r!au_r, r!a\alpha\}$. Thus

$$(9) \qquad\qquad n_r - c_r - \mathbf{T}_+(\widetilde{M}_r, \eta_r) > \max\{r!au_r, r!a\alpha\}.$$

From (9) and the relations $p^{r!au_r} z_r - p^{r!a\alpha} e_{1,1} \in p^{n_r - c_r - \mathbf{T}_+(M_r, \eta_r)} O_{r,1}$ and $z_r, e_{1,1} \in O_{r,1} \setminus pO_{r,1}$, we get that $r!au_r = r!a\alpha$. Thus $\alpha = u_r$ and therefore $a = r_{O_{r,1}} \leqslant r$. This contradicts the fact that $r \in S(1, a-1)$. Thus $n_r \leqslant c_{r+1}$ and so (7) holds. Thus (6) holds for $t = r + 1$. As c_{r+1} depends only on r, a, h, c_r, and d_r and as (by induction) c_r and d_r depend only on r, a, and h, we get that c_{r+1} depends only on a and $c = h$. This ends our second induction on $t \in S(1, a)$. Thus the claim holds.

We have $p^{c_a} M = p^{c_a} \widetilde{M}_a \subseteq M_a \subseteq M$, cf. (6). As (M_a, φ) is an elementary Dieudonné p-divisible object over k, we get $\mathbf{T}_+(M, \varphi) \leqslant c_a$. This ends case 2.

The above two cases imply that $\mathbf{T}_+(M,\varphi)$ has upper bounds that are effectively computable in terms of $a = r_M$ and $c = h$. Thus the number $d_+(a,0,c)$ exists and has effectively computable upper bounds in terms of a and c. This ends the initial induction (on ranks a) and so it also ends the proof of Lemma 2.4.1. $\square$

2.4.2. An interpretation

The estimates of the proof of 2.4.1.1 are different from the ones of [22, §I]. It seems to us that loc. cit. can be used in order to improve these estimates. Accordingly, we now make the connection between loc. cit. [10, §2], and 2.4.1.1. We situate ourselves in the context of case 2 of 2.4.1. Let $O(\alpha)$ be the $\mathbf{Z}_p$-algebra of endomorphisms of the unique elementary Dieudonné p-divisible object over k of slope α. It is known that $O(\alpha)$ is an order of the central division algebra over $\mathbf{Q}_p$ whose invariant is the image of the non-negative rational number α in $\mathbf{Q}/\mathbf{Z}$, cf. [5, Ch. IV, §3]. There exists a $W(k)$-submodule $\widetilde{M}$ of M that contains $p^{-[(r_M-1)\alpha]}M$ and such that the pair $(\widetilde{M},\varphi)$ is an α-divisible F-crystal over k (i.e. for all $n \in \mathbf{N}$ we can write φ^n as $p^{[n\alpha]}$ times a σ^n-linear endomorphism φ_n of $\widetilde{M}$), cf. [22, pp. 151–152]. As we have $r_M\alpha \in \mathbf{N} \cup \{0\}$, all slopes of (M,φ_{r_M}) are 0. Thus $\varphi_{r_M}(\widetilde{M}) = \widetilde{M}$. Triples of the form $(\widetilde{M},\varphi,\varphi_{r_M})$ are easily classified. Their isomorphism classes are in one-to-one correspondence to isomorphism classes of torsion free $O(\alpha)$-modules which by inverting p become free $O(\alpha)[\frac{1}{p}]$-modules of rank 1, see [10, 2.4 and 2.5]. It is easy to see that under this correspondence, Claim 2.4.1.1 is equivalent to the following well known result.

2.4.2.1. CLAIM. – *There exists a smallest number $N(\alpha) \in \mathbf{N}$ which has effectively computable upper bounds and for which the following property holds: for any element $x \in O(\alpha) \setminus pO(\alpha)$, the length of the artinian $\mathbf{Z}_p$-module $O(\alpha)/O(\alpha)x$ is at most $N(\alpha)$.*

2.5. Standard $\mathbf{Z}_p$ structures

Let $(M,\varphi,G,(t_\alpha)_{\alpha\in\mathcal{J}})$ be a latticed F-isocrystal with a group and an emphasized family of tensors over k such that the W-condition holds for (M,φ,G) (see 2.2.1(b) and (d)). Let $M = \bigoplus_{i=a}^b \widetilde{F}^i(M)$, $(F^i(M))_{i\in S(a,b)}$, and $\mu:\mathbf{G}_m \to G$ be as in 2.2.1(d). Each tensor $t_\alpha \in \mathcal{T}(M)$ is fixed by both μ and φ. Let $\mu_{\mathrm{can}}:\mathbf{G}_m \to \mathbf{GL}_M$ be the inverse of the canonical split cocharacter of $(M,(F^i(M))_{i\in S(a,b)},\varphi)$ defined in [42, p. 512]. Let $M = \bigoplus_{i=a}^b \widetilde{F}^i_{\mathrm{can}}(M)$ be the direct sum decomposition such that the cocharacter μ_{can} acts on $\widetilde{F}^i_{\mathrm{can}}(M)$ via the $-i$-th power of the identity character of $\mathbf{G}_m$. We have $F^i(M) = \bigoplus_{j=b}^i \widetilde{F}^j_{\mathrm{can}}(M)$ for all $i \in S(a,b)$ and $M = \bigoplus_{i=a}^b \varphi(p^{-i}\widetilde{F}^i_{\mathrm{can}}(M))$, cf. loc. cit. The cocharacter μ_{can} fixes each t_α (cf. the functorial aspects of [42, p. 513]) and so it factors through G. As $M = \bigoplus_{i=a}^b \varphi(p^{-i}\widetilde{F}^i_{\mathrm{can}}(M))$, the resulting cocharacter $\mu_{\mathrm{can}}:\mathbf{G}_m \to G$ is also a Hodge cocharacter of (M,φ,G) in the sense of 2.2.1(d).

Let $\sigma_0 := \varphi\mu(p)$. We have $\sigma_0(M) = \varphi(\bigoplus_{i=a}^b p^{-i}\widetilde{F}^i(M)) = M$. Thus σ_0 is a σ-linear automorphism of M and so also of $\mathcal{T}(M)$. For $\alpha \in \mathcal{J}$ we have $\sigma_0(t_\alpha) = t_\alpha$. Let $M_{\mathbf{Z}_p} := \{m \in M \mid \sigma_0(m) = m\}$. We now assume $k = \bar{k}$. So $M_{\mathbf{Z}_p}$ is a free $\mathbf{Z}_p$-module such that we have $M = M_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} W(k)$ and $t_\alpha \in \mathcal{T}(M_{\mathbf{Z}_p})$ for all $\alpha \in \mathcal{J}$. Let $G_{\mathbf{Q}_p}$ be the subgroup of $\mathbf{GL}_{M_{\mathbf{Z}_p}[\frac{1}{p}]}$ that fixes t_α for all $\alpha \in \mathcal{J}$; its pullback to $\mathrm{Spec}(B(k))$ is $G_{B(k)}$. Let $G_{\mathbf{Z}_p}$ be the Zariski closure of $G_{\mathbf{Q}_p}$ in $\mathbf{GL}_{M_{\mathbf{Z}_p}}$. As G is the Zariski closure of $G_{B(k)}$ in $\mathbf{GL}_M$, we get that G is the pullback to $\mathrm{Spec}(W(k))$ of $G_{\mathbf{Z}_p}$. If moreover we have a principal bilinear quasi-polarization $\lambda_M:M\otimes_{W(k)}M \to W(k)$ of (M,φ,G), then λ_M is also the extension to $W(k)$ of a perfect bilinear form $\lambda_{M_{\mathbf{Z}_p}}$ on $M_{\mathbf{Z}_p}$.

2.6. Exponentials

Let $H = \mathrm{Spec}(A)$ be an integral, affine group scheme of finite type over $\mathrm{Spec}(W(k))$. Let O be a free $W(k)$-module of finite rank such that we have a closed embedding homomorphism $H \hookrightarrow \mathbf{GL}_O$; one constructs O as a $W(k)$-submodule of A (cf. [6, vol. I, Exp. VI$_B$, 11.11.1]). If $p \geqslant 3$, let $E_O := p\,\mathrm{End}(O)$. If $p = 2$, let E_O be the sum of $p^2\,\mathrm{End}(O)$ and of the set of nilpotent elements of $p\,\mathrm{End}(O)$. Let

$$\exp : E_O \to \mathbf{GL}_O\big(W(k)\big)$$

be the exponential map that takes $x \in E_O$ into $\sum_{i=0}^{\infty} \frac{x^i}{i!}$; here $x^0 := 1_O$.

Let $l \in \mathbf{N}$. Here are the well known properties of the map $\exp$ we will often use.

(a) If $p \geqslant 3$ and $x \in p^l\,\mathrm{End}(O)$, then $\exp(x)$ is congruent mod p^{2l} to $1_O + x$.

(b) If $p = 2$, $l \geqslant 2$, and $x \in p^l\,\mathrm{End}(O)$, then $\exp(x)$ is congruent mod p^{2l} to $1_O + x + \frac{x^2}{2}$ and is congruent mod p^{2l-1} to $1_O + x$.

(c) If $x \in \mathrm{Lie}(H_{B(k)}) \cap E_O$, then $\exp(x) \in H(W(k))$.

To check (c) it is enough to show that $\exp(x) \in H(B(k))$. It suffices to check this under the extra assumption that the transcendental degree of k is countable. Fixing an embedding $W(k) \hookrightarrow \mathbf{C}$, we can view $H(\mathbf{C})$ as a Lie subgroup of $\mathbf{GL}_O(\mathbf{C})$; so the relation $\exp(x) \in H(B(k))$ follows easily from [20, Ch. II, §1, 3].

2.6.1. LEMMA. – *Suppose H is smooth over $\mathrm{Spec}(W(k))$. Let $l \in \mathbf{N}$. Let $g_l \in H(W(k))$ be congruent* mod p^l *to 1_O. Then for any $i \in S(1,l)$ there exists $z_{i,l} \in \mathrm{Lie}(H)$ such that g_l is congruent* mod p^{i+l} *to $1_O + p^l z_{i,l}$.*

Proof. – We use induction on i. The case $i = 1$ is trivial. Let $\bar{z}_{1,l}$ be the reduction mod p of $z_{1,l}$. The passage from i to $i+1$ goes as follows. We first consider the case when either $p \geqslant 3$ or $p = 2$ and $i + 1 < l$. Let $g_{l+1} := g_l \exp(-p^l z_{1,l}) \in H(W(k))$; it is congruent mod p^{l+1} to $(1_O + p^l z_{1,l})(1_O - p^l z_{1,l})$ (cf. 2.6(a) and (b)) and so also to 1_O. By replacing g_l with g_{l+1}, the role of the pair $(i+1, l)$ is replaced by the one of the pair $(i, l+1)$. As $1_O + p^l z_{1,l}$ and $\exp(p^l z_{1,l})$ are congruent mod p^{i+1+l} (cf. 2.6(a) and (b)), by induction we get that $g_l = g_{l+1} \exp(p^l z_{1,l})$ is congruent mod p^{i+1+l} to $(1_O + p^{l+1} z_{i,l+1})(1_O + p^l z_{1,l})$ and so also to $1_O + p^l(z_{1,l} + p z_{i,l+1})$. Thus as $z_{i+1,l}$ we can take the sum $z_{1,l} + p z_{i,l+1}$.

Let now $p = 2$ and $i + 1 = l \geqslant 2$. We have $\bar{z}_{1,l}^2 \in \mathrm{Lie}(H_k)$, cf. [1, Ch. II, 3.1, 3.5, Lemma 3 of 3.19]. Thus there exists $\tilde{z}_{1,l} \in \mathrm{Lie}(H)$ that is congruent mod 2 to $z_{1,l}^2$. But $1_O - 2^l z_{1,l}$ is congruent mod 2^{2l} to $\exp(-2^l z_{1,l}) \exp(-2^{2l-1} \tilde{z}_{1,l})$, cf. 2.6(b). The existence of $z_{i+1,l}$ is now argued as in the previous paragraph but working with $g_{l+1} := g_l \exp(-2^l z_{1,l}) \exp(-2^{2l-1} \tilde{z}_{1,l}) \in H(W(k))$. This ends the induction. $\square$

2.6.2. LEMMA. – *Suppose H is smooth over $\mathrm{Spec}(W(k))$. Let $l \in \mathbf{N}$. If $z_l \in \mathrm{Lie}(H)$, then the reduction* mod p^{2l} *of $1_O + p^l z_l$ belongs to $H(W_{2l}(k))$.*

Proof. – We can assume $p = 2$ (cf. 2.6(a) and (c) applied with $x = p^l z_l$) and $l \geqslant 2$ (as H is smooth). By replacing $1_O + 2^l z_l$ with $(1_O + 2^l z_l) \exp(-2^l z_l)$, we can assume (cf. 2.6(b)) that $z_l \in 2^{l-1} \mathrm{Lie}(H)$. But this case is obvious (as H is smooth). $\square$

2.7. Dilatations

In this section we study an arbitrary integral, closed subgroup scheme $G = \mathrm{Spec}(R_G)$ of $\mathbf{GL}_M$. Let $W(k)^{\mathrm{sh}}$ be the strict henselization of $W(k)$. If $a : \mathrm{Spec}(W(k)^{\mathrm{sh}}) \to G$ is a morphism, then the Néron measure of the defect of smoothness $\delta(a) \in \mathbf{N} \cup \{0\}$ of G at a is the length of the torsion part of the coherent $\mathcal{O}_{\mathrm{Spec}(W(k)^{\mathrm{sh}})}$-module $a^*(\Omega_{G/\mathrm{Spec}(W(k))})$. Here $\Omega_{G/\mathrm{Spec}(W(k))}$

is the coherent $\mathcal{O}_G$-module of relative differentials of G with respect to $\mathrm{Spec}(W(k))$. As G is a group scheme, the value of $\delta(a)$ does not depend on a and so we denote it by $\delta(G)$. We have $\delta(G) \in \mathbf{N}$ if and only if G is not smooth over $\mathrm{Spec}(W(k))$, cf. [2, 3.3, Lemma 1]. Let $S(G)$ be the Zariski closure in G_k of all special fibres of $W(k)^{\mathrm{sh}}$-valued points of G. It is a reduced subgroup of G_k. We write $S(G) = \mathrm{Spec}(R_G/J_G)$, where J_G is the ideal of R_G that defines $S(G)$.

By the *canonical dilatation* of G we mean the affine G-scheme $G_1 = \mathrm{Spec}(R_{G_1})$, where R_{G_1} is the R_G-subalgebra of $R_G[\frac{1}{p}]$ generated by $\frac{x}{p}$, with $x \in J_G$. The $\mathrm{Spec}(W(k))$-scheme G_1 is integral and has a canonical group scheme structure with respect to which the morphism $G_1 \to G$ is a homomorphism of group schemes over $\mathrm{Spec}(W(k))$, cf. [2, 3.2, p. 63 and (d) of p. 64]. The morphism $G_1 \to G$ has the following universal property (cf. [2, 3.2, Prop. 1]): any morphism $Y \to G$ of flat $\mathrm{Spec}(W(k))$-schemes whose special fibre factors through the closed embedding $S(G) \hookrightarrow G_k$, factors uniquely through $G_1 \to G$. Either $\delta(G_1) = 0$ (i.e. G_1 is smooth over $\mathrm{Spec}(W(k))$) or (cf. [2, 3.3, Prop. 5]) we have $0 < \delta(G_1) < \delta(G)$.

By using at most $\delta(G)$ canonical dilatations, we get the existence of a unique smooth, affine group scheme G' over $\mathrm{Spec}(W(k))$ that is endowed with a homomorphism $G' \to G$ whose fibre over $\mathrm{Spec}(B(k))$ is an isomorphism and that has the following universal property (cf. [2, 7.1, Thm. 5]): any morphism $Y \to G$ of $\mathrm{Spec}(W(k))$-schemes with Y smooth, factors uniquely through $G' \to G$. In particular, we can identify $G'(W(k)^{\mathrm{sh}})$ with $G(W(k)^{\mathrm{sh}})$. The homomorphism $G' \to G$ is called the *group smoothening* of G. Let

$$n(G) \in S\big(0, \delta(G)\big)$$

be the smallest number of canonical dilatations one has to perform in order to construct G'. We have $n(G) = 0$ if and only if G is smooth over $\mathrm{Spec}(W(k))$.

The closed embedding $i_G : G \hookrightarrow \mathbf{GL}_M$ gets replaced by a canonical homomorphism $i_{G'} : G' \to \mathbf{GL}_M$ that factors through i_G. We identify $\mathrm{Lie}(G')$ with a $W(k)$-lattice of $\mathrm{Lie}(G_{B(k)})$ contained in $\mathrm{End}(M)$. Let $d_{\mathrm{sm}} \in \mathbf{N} \cup \{0\}$ be the smallest number such that we have $p^{d_{\mathrm{sm}}}(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)) \subseteq \mathrm{Lie}(G') \subseteq \mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)$.

We fix a closed embedding homomorphism $G' \hookrightarrow \mathbf{GL}_{M'}$, where M' is a free $W(k)$-module of finite rank (see beginning of 2.6). Let $g \in G'(W(k)) = G(W(k))$.

2.7.1. DEFINITION. – Let $n \in \mathbf{N}$. We say g is congruent $\mathrm{mod}\ p^n$ to $1_{M'}$ (respectively to 1_M) if and only if the image of g in $G'(W_n(k))$ (respectively in $G(W_n(k))$) is the identity element.

2.7.2. LEMMA. – *We have the following three properties*:
(a) *If g is congruent $\mathrm{mod}\ p^n$ to $1_{M'}$, then g is also congruent $\mathrm{mod}\ p^n$ to 1_M.*
(b) *If g is congruent $\mathrm{mod}\ p^{n+n(G)}$ to 1_M, then g is also congruent $\mathrm{mod}\ p^n$ to $1_{M'}$.*
(c) *We have an inequality $d_{\mathrm{sm}} \leqslant n(G)$.*

Proof. – Part (a) is trivial. We write $G' = \mathrm{Spec}(R_{G'})$ and $\mathbf{GL}_M = \mathrm{Spec}(R_M)$. Let I_G, I_{G_1}, $I_{G'}$, and I_M be the ideals of R_G, R_{G_1}, $R_{G'}$, and R_M (respectively) that define the identity sections. We have $I_{G_1} = I_G[\frac{1}{p}] \cap R_{G_1}$ and $I_{G'} = I_G[\frac{1}{p}] \cap R_{G'}$.

We check (b). Let $m_g : R_G \to W(k)$ be the homomorphism that defines g; we have $m_g(I_G) \subseteq p^{n+n(G)}W(k)$. Let $m_{1g} : R_{G_1} \to W(k)$ be the homomorphism through which m_g factors. We have $m_{1g}(I_{G_1}) \subseteq p^{n+n(G)-1}W(k)$, cf. the very definition of R_{G_1}. Part (b) follows from a repeated application of this fact to the sequence of $n(G)$ dilatations performed to construct G'. The cokernel of the cotangent map (computed at $W(k)$-valued identity elements) $I_G/I_G^2 \to I_{G_1}/I_{G_1}^2$ is annihilated by p, cf. the very definition of R_{G_1}. By applying this repeatedly, we get that the cokernel of the cotangent map $I_M/I_M^2 \to I_{G'}/I_{G'}^2$ is annihilated

by $p^{n(G)}$. Taking duals we get that the cokernel of the $W(k)$-linear Lie monomorphism $\mathrm{Lie}(G') \hookrightarrow \mathrm{Lie}(G_{B(k)}) \cap \mathrm{Lie}(\mathbf{GL}_M)$ is also annihilated by $p^{n(G)}$. As $\mathrm{Lie}(\mathbf{GL}_M)$ is the Lie algebra associated to $\mathrm{End}(M)$, we get that (c) holds. $\quad\square$

2.8. Complements on $\mathcal{M}(W_q(S))$

Let $q \in \mathbf{N}$ and let $l \in S(0,q)$. Let $f : S_1 \to S$ be a morphism of $\mathrm{Spec}(\mathbf{F}_p)$-schemes. Let $f_q : W_q(S_1) \to W_q(S)$ be the natural morphism of $\mathrm{Spec}(\mathbf{Z}/p^q\mathbf{Z})$-schemes defined by f. Let $\mathfrak{C}$ be an F-crystal over S. In this section we include four complements on the category $\mathcal{M}(W_q(S))$.

2.8.1. Pullbacks
Let $f_q^* : \mathcal{M}(W_q(S)) \to \mathcal{M}(W_q(S_1))$ be the natural pullback functor. So if $S = \mathrm{Spec}(R)$ and $S_1 = \mathrm{Spec}(R_1)$ are affine and if $h : (O, \varphi_O) \to (O', \varphi_{O'})$ is a morphism of $\mathcal{M}(W_q(S))$, then $f_q^*(h)$ is the morphism

$$ h \otimes 1_{W_q(R_1)} : \big(O \otimes_{W_q(R)} W_q(R_1), \varphi_O \otimes \Phi_{R_1}\big) \to \big(O' \otimes_{W_q(R)} W_q(R_1), \varphi_{O'} \otimes \Phi_{R_1}\big). $$

In general $W_q(S) \times_{W_{q+1}(S)} W_{q+1}(S_1)$ is not $W_q(S_1)$. Thus, in general the restriction of f_{q+1}^* to $\mathcal{M}(W_q(S))$ and f_q^* do not coincide as functors from $\mathcal{M}(W_q(S))$ to $\mathcal{M}(W_q(S_1))$ and therefore the sequence of functors $(f_q^*)_{q\in\mathbf{N}}$ does not define a pullback functor from $\mathcal{M}(W(S))$ to $\mathcal{M}(W(S_1))$. If the Frobenius endomorphism of $\mathcal{O}_{S_1}$ is surjective, then regardless of what S is we have $W_q(S) \times_{W_{q+1}(S)} W_{q+1}(S_1) = W_q(S_1)$ and thus the sequence of functors $(f_q^*)_{q\in\mathbf{N}}$ does define a pullback functor $f^* : \mathcal{M}(W(S)) \to \mathcal{M}(W(S_1))$.

If u is an object (or a morphism) of $\mathcal{M}(W_q(S))$, then by its pullback to an object (or a morphism) of $\mathcal{M}(W_q(S_1))$ we mean $f_q^*(u)$. If $t \in \mathbf{N}$ and if $f_{q+t}^*(u)$ is an object (or a morphism) of $\mathcal{M}(W_q(S_1))$, then we have $f_{q+t}^*(u) = f_q^*(u)$. If S_1 is the spectrum of a perfect field, we also speak simply of the pullback of u via f, to be often denoted as $f^*(u)$ (instead of either $f_q^*(u)$ or $f_{q+t}^*(u)$).

If S is integral, if k_S is the field of fractions of S, and if u is a morphism of $\mathcal{M}(W_q(S))$, then we say $\mathrm{Coker}(u)$ is *generically annihilated by* p^l if the pullback of u to a morphism of $\mathcal{M}(W_q(k_S)) = \mathcal{M}(W_q(\mathrm{Spec}(k_S)))$ has a cokernel annihilated by p^l.

2.8.2. The evaluation functor E
Let $\delta_q(S)$ be the canonical divided power structure of the ideal sheaf of $\mathcal{O}_{W_q(S)}$ that defines the closed embedding $S \hookrightarrow W_q(S)$. The evaluation of the F-crystal $\mathfrak{C}$ at the thickening $(S \hookrightarrow W_q(S), \delta_q(S))$ is a triple $(\mathcal{F}_q, \varphi_{\mathcal{F}_q}, \nabla_{\mathcal{F}_q})$, where $\mathcal{F}_q$ is a locally free $\mathcal{O}_{W_q(S)}$-module of finite rank, where $\varphi_{\mathcal{F}_q} : \mathcal{F}_q \to \mathcal{F}_q$ is a Φ_S-linear endomorphism, and where $\nabla_{\mathcal{F}_q}$ is an integrable and topologically nilpotent connection on $\mathcal{F}_q$, that satisfies certain axioms. In this paper, connections as $\nabla_{\mathcal{F}_q}$ will play no role; on the other hand, we will often use the following object

$$ \mathbf{E}\big(\mathfrak{C}; W_q(S)\big) := (\mathcal{F}_q, \varphi_{\mathcal{F}_q}) $$

of $\mathcal{M}(W_q(S))$. A morphism $v : \mathfrak{C} \to \mathfrak{C}_1$ of F-crystals over S defines naturally a morphism

$$ \mathbf{E}\big(v; W_q(S)\big) : \mathbf{E}\big(\mathfrak{C}; W_q(S)\big) \to \mathbf{E}\big(\mathfrak{C}_1; W_q(S)\big). $$

The association $v \to \mathbf{E}(v; W_q(S))$ defines a $\mathbf{Z}_p$-linear (evaluation) functor from the category of F-crystals over S into the category $\mathcal{M}(W_q(S))$.

To ease notations, let $\mathbf{E}(\mathfrak{C}; W_q(S_1)) := \mathbf{E}(\mathfrak{C}_{S_1}; W_q(S_1))$ and, in the case when $S_1 = \mathrm{Spec}(R_1)$ is affine, let $\mathbf{E}(\mathfrak{C}; W_q(R_1)) := \mathbf{E}(\mathfrak{C}; W_q(S_1))$.

The functorial morphism $f_q : (S_1 \hookrightarrow W_q(S_1), \delta_q(S_1)) \to (S \hookrightarrow W_q(S), \delta_q(S))$ gives birth to a canonical isomorphism (to be viewed as an identity)

$$(10) \qquad\qquad c_{f;q} : f_q^*\big(\mathbf{E}\big(\mathfrak{C}; W_q(S)\big)\big) \xrightarrow{\sim} \mathbf{E}\big(\mathfrak{C}; W_q(S_1)\big).$$

If $e : S_2 \to S_1$ is another morphism of $\mathrm{Spec}(\mathbf{F}_p)$-schemes, then we have identities

$$(11) \qquad\qquad (f \circ e)_q^* = e_q^* \circ f_q^* \quad \text{and} \quad c_{e;q} \circ e_q^*(c_{f;q}) = c_{f \circ e;q}.$$

In what follows we will use without any extra comment the identities (10) and (11).

2.8.3. Inductive limits

Let $V \hookrightarrow V_1$ be a monomorphism of commutative $\mathbf{F}_p$-algebras. Suppose we have an inductive limit $V_1 = \mathrm{ind}\lim_{\alpha \in \Lambda} V_\alpha$ of commutative V-subalgebras of V_1 indexed by the set of objects Λ of a filtered, small category. For $\alpha \in \Lambda$, let $f^\alpha : \mathrm{Spec}(V_\alpha) \to \mathrm{Spec}(V)$ be the natural morphism.

Let (O, φ_O) and $(O', \varphi_{O'})$ be objects of $\mathcal{M}(W_q(V))$ such that O and O' are free $W_q(V)$-modules of finite rank. Let (O_1, φ_{O_1}) and $(O_1', \varphi_{O_1'})$ be the pullbacks of (O, φ_O) and $(O', \varphi_{O'})$ (respectively) to objects of $\mathcal{M}(W_q(V_1))$. We consider a morphism

$$u_1 : (O_1, \varphi_{O_1}) \to (O_1', \varphi_{O_1'})$$

of $\mathcal{M}(W_q(V_1))$ whose cokernel is annihilated by p^l. We fix ordered $W_q(V)$-bases $\mathcal{B}_O$ and $\mathcal{B}_{O'}$ of O and O' (respectively). Let B_1 be the matrix representation of u_1 with respect to the ordered $W_q(V_1)$-basis of O_1 and O_1' defined naturally by $\mathcal{B}_O$ and $\mathcal{B}_{O'}$ (respectively). As $p^l \mathrm{Coker}(u_1) = 0$, for $x' \in \mathcal{B}_{O'}$ we can write $p^l x' \otimes 1 = u_1(\sum_{x \in \mathcal{B}_O} x \otimes \beta_{xx'})$, where each $\beta_{xx'} \in W_q(V_1)$. Let V_{u_1} be the V-subalgebra of V_1 generated by the components of the Witt vectors of length q with coefficients in V_1 that are either entries of B_1 or $\beta_{xx'}$ for some pair $(x, x') \in \mathcal{B}_O \times \mathcal{B}_{O'}$. As V_{u_1} is a finitely generated V-algebra, there exists $\alpha_0 \in \Lambda$ such that $V_{u_1} \hookrightarrow V_{\alpha_0}$. This implies that u_1 is the pullback of a morphism

$$u_{\alpha_0} : f_q^{\alpha_0 *}(O, \varphi_O) \to f_q^{\alpha_0 *}(O', \varphi_{O'})$$

of $\mathcal{M}(W_q(V_{\alpha_0}))$ whose cokernel is annihilated by p^l. Here are four special cases of interest.

(a) If V is a field and V_1 is an algebraic closure of V, then as V_α's we can take the finite field extensions of V that are contained in V_1.

(b) If V_1 is a local ring of an integral domain V, then as V_α's we can take the V-algebras of global functions of open, affine subschemes of $\mathrm{Spec}(V)$ that contain $\mathrm{Spec}(V_1)$.

(c) We consider the case when V is a discrete valuation ring that is an N-2 ring in the sense of [29, (31.A)], when V_1 is a faithfully flat V-algebra that is also a discrete valuation ring, and when each V_α is a V-algebra of finite type. The flat morphism $f^{\alpha_0} : \mathrm{Spec}(V_{\alpha_0}) \to \mathrm{Spec}(V)$ has quasi-sections, cf. [18, Ch. IV, Cor. (17.16.2)]. In other words, there exist a finite field extension $\tilde{k}$ of k and a V-subalgebra $\tilde{V}$ of $\tilde{k}$ such that: (i) $\tilde{V}$ is a local, faithfully flat V-algebra of finite type whose field of fractions is $\tilde{k}$, and (ii) we have a morphism $\tilde{f}^{\alpha_0} : \mathrm{Spec}(\tilde{V}) \to \mathrm{Spec}(V_{\alpha_0})$ such that $\tilde{f} := f^{\alpha_0} \circ \tilde{f}^{\alpha_0}$ is the natural morphism $\mathrm{Spec}(\tilde{V}) \to \mathrm{Spec}(V)$. As V is an N-2 ring, its normalization in $\tilde{k}$ is a finite V-algebra and so a Dedekind domain. This implies that we can assume $\tilde{V}$ is a discrete valuation ring. For future use, we recall that any excellent ring is a Nagata ring (cf. [29, (34.A)]) and so also an N-2 ring (cf. [29, (31.A)]). Let

$$\tilde{u} : \tilde{f}_q^*(O, \varphi_O) = \tilde{f}_q^{\alpha_0 *}\big(f_q^{\alpha_0 *}(O, \varphi_O)\big) \to \tilde{f}_q^*(O', \varphi_{O'}) = \tilde{f}_q^{\alpha_0 *}\big(f_q^{\alpha_0 *}(O', \varphi_{O'})\big)$$

be the pullback of u_{α_0} to a morphism of $\mathcal{M}(W_q(\widetilde{V}))$; its cokernel is annihilated by p^l.

If V is the local ring of an integral $\mathrm{Spec}(\mathbf{F}_p)$-scheme U, then $\widetilde{V}$ is a local ring of the normalization of U in $\tilde{k}$. So from (b) we get that there exists an open subscheme $\widetilde{U}$ of this last normalization that has $\widetilde{V}$ as a local ring and that has the property that $\tilde{u}$ extends to a morphism of $\mathcal{M}(W_q(\widetilde{U}))$ whose cokernel is annihilated by p^l.

(d) If V is reduced and $V_1 = V^{\mathrm{perf}}$, we can take $\Lambda = \mathbf{N}$ and $V_n = V^{(p^n)}$ ($n \in \mathbf{N}$).

2.8.4. Hom schemes

Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two objects of $\mathcal{M}(W_q(S))$ such that their underlying $\mathcal{O}_{W_q}(S)$-modules are locally free of finite ranks. We consider the functor

$$\mathbf{Hom}(\mathcal{O}_1, \mathcal{O}_2) \colon \mathrm{Sch}^S \to \mathrm{SET}$$

from the category Sch^S of S-schemes to the category SET of sets, with the property that $\mathbf{Hom}(\mathcal{O}_1, \mathcal{O}_2)(S_1)$ is the set underlying the $\mathbf{Z}/p^q\mathbf{Z}$-module of morphisms of $\mathcal{M}(W_q(S_1))$ that are between $f_q^*(\mathcal{O}_1)$ and $f_q^*(\mathcal{O}_2)$; here $f \colon S_1 \to S$ is as in the beginning of 2.8.

2.8.4.1. LEMMA. – *The functor* $\mathbf{Hom}(\mathcal{O}_1, \mathcal{O}_2)$ *is representable by an affine S-scheme which locally is of finite presentation.*

Proof. – Localizing, we can assume that $S = \mathrm{Spec}(R)$ is affine and that $\mathcal{O}_1 = (O_1, \varphi_{O_1})$ and $\mathcal{O}_2 = (O_2, \varphi_{O_2})$ are such that O_1 and O_2 are free $W_q(R)$-modules. For $i \in \{1, 2\}$ let r_i be the rank of O_i. Let $\mathbf{Hom}(O_1, O_2)$ be the affine space (of relative dimension qr_1r_2) over $\mathrm{Spec}(R)$ with the property that for any commutative R-algebra R_1, $\mathbf{Hom}(O_1, O_2)(R_1)$ is the set of $W_q(R_1)$-linear maps $x \colon O_1 \otimes_{W_q(R)} W_q(R_1) \to O_2 \otimes_{W_q(R)} W_q(R_1)$. We have an identity $(\varphi_{O_2} \otimes \Phi_{R_1}) \circ x = x \circ (\varphi_{O_1} \otimes \Phi_{R_1})$ if and only if x belongs to the subset of $\mathbf{Hom}(O_1, O_2)(R_1)$ that is naturally identified with $\mathbf{Hom}(\mathcal{O}_1, \mathcal{O}_2)(\mathrm{Spec}(R_1))$. As the relation $(\varphi_{O_2} \otimes \Phi_{R_1}) \circ x = x \circ (\varphi_{O_1} \otimes \Phi_{R_1})$ defines a closed subscheme of $\mathbf{Hom}(O_1, O_2)$ that is of finite presentation, the lemma follows. $\square$

2.9. On two results of commutative algebra

In 5.4 and Section 6 we will use the following two geometric variations of well known results of commutative algebra.

2.9.1. LEMMA. – *Let X and Y be two integral, normal, locally noetherian schemes. Let $u \colon X \to Y$ be an affine morphism that is birational; let K be the field of fractions of either X or Y. Let $D(X)$ and $D(Y)$ be the sets of local rings of X and Y (respectively) that are discrete valuation rings (of K). If $D(Y) \subseteq D(X)$, then u is an isomorphism.*

Proof. – Working locally in the Zariski topology of Y, we can assume $X = \mathrm{Spec}(R_X)$ and $Y = \mathrm{Spec}(R_Y)$ are also affine and noetherian. Thus (inside K) we have

$$R_Y \hookrightarrow R_X = \bigcap_{V \in D(X)} V \hookrightarrow \bigcap_{V \in D(Y)} V = R_Y$$

(cf. [29, (17.H)] for the two identities). So $R_Y = R_X$. Thus u is an isomorphism. $\square$

2.9.2. LEMMA. – *Let $X' = \mathrm{Spec}(R') \to X = \mathrm{Spec}(R)$ be a morphism between affine schemes which at the level of rings is defined by an integral (i.e. an ind-finite) monomorphism $R \hookrightarrow R'$. Then an open subscheme U of X is affine if and only if its pullback $U' := U \times_X X'$ to X' is affine.*

Proof. – It is enough to show that U is affine if U' is affine. The morphism $U' \to U$ is surjective (see [29, (5.E)]). So as U' is quasi-compact (being affine), U is also quasi-compact. Thus $X^{\mathrm{top}} \setminus U^{\mathrm{top}}$ is the zero locus in X^{top} of a finite number of elements of R. So there exists a finitely generated $\mathbf{Z}$-subalgebra R_0 of R such that U is the pullback of an open subscheme U_0 of $\mathrm{Spec}(R_0)$ through the natural morphism $\mathrm{Spec}(R) \to \mathrm{Spec}(R_0)$.

Let Λ (respectively Λ') be the set of finite subsets of R (respectively of R'). For $\alpha \in \Lambda$ (respectively $\alpha' \in \Lambda'$), let R_α (respectively $R'_{\alpha'}$) be the R_0-subalgebra of R (respectively of R') generated by α (respectively by α'). Let $X_\alpha := \mathrm{Spec}(R_\alpha)$ and $X'_{\alpha'} := \mathrm{Spec}(R'_{\alpha'})$. Let U_α and $U'_{\alpha'}$ be the pullbacks of U_0 to X_α and $X'_{\alpha'}$ (respectively). As $U'_{\alpha'}$ is a quasi-compact, open subscheme of $X'_{\alpha'}$, it is an $X'_{\alpha'}$-scheme of finite presentation. As the scheme U' is affine, by applying [18, Ch. IV, (8.10.5)] to the projective limit $U' \hookrightarrow X' = \mathrm{proj}\lim_{\alpha' \in \Lambda'} U'_{\alpha'} \hookrightarrow X'_{\alpha'}$ of open embeddings of finite presentation, we get that there exists $\beta' \in \Lambda'$ such that $U'_{\beta'}$ is affine. Let $\beta \in \Lambda$ be such that $R'_{\beta' \cup \beta}$ is a finite R_β-algebra. As $U'_{\beta' \cup \beta} = U'_{\beta'} \times_{X'_{\beta'}} X'_{\beta' \cup \beta}$ is affine, the scheme U_β is also affine (cf. Chevalley theorem of [16, Ch. II, (6.7.1)] applied to the finite, surjective morphism $U'_{\beta' \cup \beta} \to U_\beta$). Thus $U = U_\beta \times_{X_\beta} X$ is affine. $\square$

3. Proof of Main Theorem A and complements

In 3.1 we prove Main Theorem A stated in 1.2. See formula (18) of 3.1.3 for a concrete expression of the number n_{fam} mentioned in 1.2. In 3.2 we include interpretations and variants of 1.2 in terms of reductions modulo powers of p; in particular, see 3.2.4 for the passage from 1.2 to 1.3. See 3.3 for improvements of the estimates of 3.1.1 to 3.1.5 in many particular cases of interest. If $p \geqslant 3$ let $\varepsilon_p := 1$. Let $\varepsilon_2 := 2$.

3.1. Proof of 1.2

We start the proof of 1.2. Until 3.1.4 we will assume $k = \bar{k}$. Let $v := \dim(G_{B(k)})$. It suffices to prove 1.2 under the extra hypothesis $v \geqslant 1$. Let $\delta(G)$, $n(G) \in \mathbf{N} \cup \{0\}$, the group smoothening $G' \to G$ of G, and the closed embedding homomorphism $G' \hookrightarrow \mathbf{GL}_{M'}$ be as in 2.7. We have $G'(W(k)) = G(W(k))$.

Let $m := \mathbf{T}(\mathrm{Lie}(G'), \varphi) \in \mathbf{N} \cup \{0\}$. Based on Definitions 2.2.2(a) and (b), there exists a $B(k)$-basis $\mathcal{B} = \{e_1, \dots, e_v\}$ of $\mathrm{Lie}(G_{B(k)})$ formed by elements of $\mathrm{Lie}(G')$ and there exists a permutation π of $S(1, v)$, such that the following three things hold:

(a) denoting $E := \langle e_1, \dots, e_v \rangle$, we have $p^m \mathrm{Lie}(G') \subseteq E \subseteq \mathrm{Lie}(G')$;

(b) if $l \in S(1, v)$, then we have $\varphi(e_l) = p^{n_l} e_{\pi(l)}$ for some $n_l \in \mathbf{Z}$;

(c) for any cycle $\pi_0 = (l_1, \dots, l_q)$ of π, the integers $n_{l_1}, \dots, n_{l_q}$ are either all non-negative or all non-positive.

If we have $n_{l_j} \geqslant 0$ for all $j \in S(1, q)$, let $\tau(\pi_0) := 1$. If there exists $j \in S(1, q)$ such that $n_{l_j} < 0$, let $\tau(\pi_0) := -1$. Let $n \in \mathbf{N}$ be such that

$$(12) \qquad\qquad n \geqslant 2m + \varepsilon_p + n(G).$$

Let $g_n \in G(W(k))$ be congruent $\mathrm{mod}\ p^n$ to 1_M. So $g_n \in G'(W(k))$ is congruent $\mathrm{mod}\ p^{n-n(G)}$ to $1_{M'}$ (cf. 2.7.2(b)) and below we will only use this congruence.

3.1.1. CLAIM. – *For any* $t \in \mathbf{N}$ *there exists* $\tilde{g}_t \in G'(W(k)) = G(W(k))$ *congruent* $\mathrm{mod}\ p^{n-n(G)+t-1-m}$ *to* $1_{M'}$ *and such that* $\tilde{g}_t g_n \varphi \tilde{g}_t^{-1} \varphi^{-1} \in G'(W(k)) = G(W(k))$ *is congruent* $\mathrm{mod}\ p^{n-n(G)+t}$ *to* $1_{M'}$. *Thus there exists* $\tilde{g}_0 \in G'(W(k)) = G(W(k))$ *congruent* $\mathrm{mod}\ p^{n-n(G)-m}$ *to* $1_{M'}$ *and such that* $\tilde{g}_0 g_n \varphi = \varphi \tilde{g}_0$.

If $t \geqslant 2$ and if the element $\tilde{g}_{t-1}$ exists, then we can replace the triple (n, t, g_n) by the triple $(n + t - 1, 1, \tilde{g}_{t-1} g_n \varphi \tilde{g}_{t-1}^{-1} \varphi^{-1})$. Thus using induction on $t \in \mathbf{N}$, to prove the first part of the claim we can assume that $t = 1$. As $W(k)$ is p-adically complete, the second part of the claim follows from its first part; this is so as we can take $\tilde{g}_0$ to be an infinite product of the form $\cdots \tilde{h}_3 \tilde{h}_2 \tilde{h}_1$ that has the property that for all $c \in \mathbf{N}$ the element $\tilde{h}_c \in G'(W(k)) = G(W(k))$ is congruent mod $p^{n-n(G)+c-1-m}$ to $1_{M'}$ and moreover $\tilde{h}_c \tilde{h}_{c-1} \cdots \tilde{h}_1 g_n \varphi \tilde{h}_1^{-1} \cdots \tilde{h}_c^{-1} \varphi^{-1} \in G'(W(k)) = G(W(k))$ is congruent mod $p^{n-n(G)+c}$ to $1_{M'}$. Thus to prove the claim, it suffices to prove its first part for $t = 1$.

For $t = 1$ we will use what we call the *stairs method* for E. Let $z_n \in \mathrm{Lie}(G')$ be such that g_n is congruent mod $p^{n-n(G)+1}$ to $1_{M'} + p^{n-n(G)} z_n$. As $n - n(G) \geqslant m + 1$, based on 3.1(a) we can write

$$p^{n-n(G)} z_n = \sum_{l \in S(1,v)} p^{u_l} c_l e_l,$$

where $u_l \in \mathbf{N}$ depends only on the cycle of π to which l belongs and where $c_l \in W(k)$. We take the u_l's to be the maximal possible values subject to the last sentence. Thus

(13a) $$u_l \geqslant n - n(G) - m \geqslant m + \varepsilon_p \geqslant \varepsilon_p \geqslant 1.$$

From (13a) and (12) we get

(13b) $$\min\{u_l + u_{l'} \mid l, l' \in S(1,v)\} \geqslant 2(n - n(G) - m) \geqslant n - n(G) + \varepsilon_p \geqslant n - n(G) + 1.$$

Due to (13b), the product $\tilde{g}_n^{(1)} := \prod_{l \in S(1,v)}(1_{M'} + p^{u_l} c_l e_l) \in \mathbf{GL}_{M'}(W(k))$ is congruent mod $p^{2(n-n(G)-m)}$ and so also mod $p^{n-n(G)+1}$ to $1_{M'} + \sum_{l \in S(1,v)} p^{u_l} c_l e_l = 1_{M'} + p^{n-n(G)} z_n$. The element $\tilde{g}_n^{(2)} := (\tilde{g}_n^{(1)})^{-1} g_n \in \mathbf{GL}_{M'}(W(k))$ is congruent mod $p^{n-n(G)+1}$ to $(1_{M'} + p^{n-n(G)} z_n)^{-1}(1_{M'} + p^{n-n(G)} z_n) = 1_{M'}$. We have $g_n = \tilde{g}_n^{(1)} \tilde{g}_n^{(2)}$. For $l \in S(1,v)$ let $q_l := -\min\{0, n_l\} \in \mathbf{N} \cup \{0\}$. We will choose $\tilde{g}_1 \in G'(W(k))$ to be a product $\prod_{l \in S(1,v)} \exp(p^{u_l + q_l} x_l e_l)$, with all x_l's in $W(k)$. This last product makes sense, cf. 2.6(a) and (b) and the fact that for $p = 2$ we have $u_l + q_l \geqslant u_l \geqslant m + \varepsilon_2 \geqslant \varepsilon_2 = 2$.

For $l \in S(1,v)$ we have $u_l = u_{\pi(l)}$. Thus

(14) $$\varphi \tilde{g}_1^{-1} \varphi^{-1} = \prod_{l \in S(1,v)} \exp\big(-p^{u_l + q_l} \sigma(x_l) \varphi(e_l)\big)$$

$$= \prod_{l \in S(1,v)} \exp\big(-p^{u_l + q_{\pi^{-1}(l)} + n_{\pi^{-1}(l)}} \sigma(x_{\pi^{-1}(l)}) e_l\big).$$

These exponential elements are well defined even if $p = 2$, as for $p = 2$ we have inequalities $u_l + q_{\pi^{-1}(l)} + n_{\pi^{-1}(l)} \geqslant u_l \geqslant \varepsilon_2 \geqslant 2$. Thus $\varphi \tilde{g}_1^{-1} \varphi^{-1} \in G'(W(k)) = G(W(k))$, cf. 2.6(c).

We have $\varphi \tilde{g}_1^{-1} \varphi^{-1} \in G'(W(k)) = G(W(k))$, cf. 2.6(c). We have to show that we can choose the x_l's such that $\tilde{g}_1 g_n \varphi \tilde{g}_1^{-1} \varphi^{-1} \in G'(W(k))$ is congruent mod $p^{n-n(G)+1}$ to $1_{M'}$. It suffices to show that if g_n is not congruent mod $p^{n-n(G)+1}$ to $1_{M'}$, then we can choose the x_l's such that by replacing g_n with $g_{n+1} \tilde{g}_1 g_n \varphi \tilde{g}_1^{-1} \varphi^{-1} \in G'(W(k))$, where $g_{n+1} \in G'(W(k))$ is congruent mod $p^{n-n(G)+1}$ to $1_{M'}$, we can also replace each u_l by $u_l + t_l$, where $t_l \in \mathbf{N}$ depends only on the cycle of π to which l belongs.

The element $\tilde{g}_1 g_n \varphi \tilde{g}_1^{-1} \varphi^{-1} \in G'(W(k))$ is congruent mod $p^{n-n(G)+1}$ to the product $\tilde{g}_1 \tilde{g}_n^{(1)} \varphi \tilde{g}_1^{-1} \varphi^{-1}$. From (13a), (13b), (14), and 2.6(a) and (b), we get that $\varphi \tilde{g}_1^{-1} \varphi^{-1}$ is congruent mod $p^{n-n(G)+1}$ to $\prod_{l \in S(1,v)} [1_{M'} - p^{u_l + q_{\pi^{-1}(l)} + n_{\pi^{-1}(l)}} \sigma(x_{\pi^{-1}(l)}) e_l]$. A similar argument

shows that $\tilde{g}_1$ is congruent mod $p^{n-n(G)+1}$ to $\prod_{l \in S(1,v)}(1_{M'} + p^{u_l+q_l}x_l e_l)$. Thus the product $\tilde{g}_1 \tilde{g}_n^{(1)} \varphi \tilde{g}_1^{-1} \varphi^{-1}$ of the three elements $\tilde{g}_1$, $\tilde{g}_n^{(1)}$, and $\varphi \tilde{g}_1^{-1} \varphi^{-1}$, is congruent mod $p^{n-n(G)+1}$ to the following product of three elements

$$\prod_{l \in S(1,v)} \left(1_{M'} + p^{u_l+q_l}x_l e_l\right) \prod_{l \in S(1,v)} \left(1_{M'} + p^{u_l}c_l e_l\right)$$

$$\times \prod_{l \in S(1,v)} \left[1_{M'} - p^{u_l+q_{\pi^{-1}(l)}+n_{\pi^{-1}(l)}}\sigma(x_{\pi^{-1}(l)})e_l\right]$$

and so (cf. (13b)) also to $1_{M'} + \sum_{l \in S(1,v)} p^{u_l}[p^{q_l}x_l + c_l - p^{q_{\pi^{-1}(l)}+n_{\pi^{-1}(l)}}\sigma(x_{\pi^{-1}(l)})]e_l$.

To show that we can take each t_l to be at least 1, it suffices to show that we can choose the x_l's such that we have

$$(15) \qquad p^{q_l}x_l + c_l - p^{q_{\pi^{-1}(l)}+n_{\pi^{-1}(l)}}\sigma(x_{\pi^{-1}(l)}) \in pW(k) \quad \forall l \in S(1,v).$$

In other words, by denoting with $\bar{x} \in k$ the reduction mod p of an arbitrary element $x \in W(k)$, it suffices to show that for each cycle $\pi_0 = (l_1, \ldots, l_q)$ of π there exist solutions in k of the following circular system of equations over k

$$(16) \qquad \bar{b}_{l_j}\bar{x}_{l_j} + \bar{c}_{l_j} - \bar{d}_{l_j}\bar{x}_{l_{j-1}}^p = 0 \quad \text{with } j \in S(1,q),$$

where $b_{l_j} := p^{q_{l_j}}$ and $d_{l_j} := p^{q_{l_{j-1}}+n_{l_{j-1}}}$ (here we have $l_0 = l_q$, cf. end of 2.1).

If $\tau(\pi_0) = 1$, then $q_{l_j} = q_{l_{j-1}} = 0$ and $n_{l_{j-1}} \geqslant 0$; so $p^{q_{l_j}}x_{l_j} + c_{l_j} - p^{q_{l_{j-1}}+n_{l_{j-1}}}\sigma(x_{l_{j-1}})$ is $x_{l_j} + c_{l_j} - p^{n_{l_{j-1}}}\sigma(x_{l_{j-1}})$. If $\tau(\pi_0) = -1$, then $q_{l_{j-1}} = -n_{l_{j-1}} \geqslant 0$ and so we have $p^{q_{l_j}}x_{l_j} + c_{l_j} - p^{q_{l_{j-1}}+n_{l_{j-1}}}\sigma(x_{l_{j-1}}) = p^{q_{l_j}}x_{l_j} + c_{l_j} - \sigma(x_{l_{j-1}})$; moreover, there exists $j_0 \in S(1,j)$ such that $q_{l_{j_0}} = -n_{l_{j_0}} > 0$. Thus depending on the value of $\tau(\pi_0)$ we have:

(+) $\bar{b}_{l_j} = 1$ and $\bar{d}_{l_j} \in \{0,1\}$ for all $j \in S(1,q)$, if $\tau(\pi_0) = 1$;

(−) $\bar{d}_{l_j} = 1$ and $\bar{b}_{l_j} \in \{0,1\}$ for all $j \in S(1,q)$ and moreover there exists $j_0 \in S(1,q)$ such that $\bar{b}_{l_{j_0}} = 0$, if $\tau(\pi_0) = -1$.

If $\tau(\pi_0) = 1$, then based on (+) we can eliminate the variables $\bar{x}_{l_q}, \bar{x}_{l_{q-1}}, \ldots, \bar{x}_{l_3}$, and $\bar{x}_{l_2}$ one by one from the system (16). The resulting equation in the variable $\bar{x}_{l_1}$ is of the form $\bar{x}_{l_1} = \bar{u}_{l_1} + \bar{v}_{l_1}\bar{x}_{l_1}^{p^q}$, where $\bar{u}_{l_1}$ and $\bar{v}_{l_1} \in k$. This equation defines an étale k-algebra. Thus (as k is separably closed) the system (16) has solutions in k if $\tau(\pi_0) = 1$.

If $\tau(\pi_0) = -1$, then based on (−) (and on the fact that k is perfect) the values of $\bar{x}_{l_{j_0-1}}$, $\bar{x}_{l_{j_0-2}}, \ldots, \bar{x}_{l_1}, \bar{x}_{l_q}, \bar{x}_{l_{q-1}}, \ldots, \bar{x}_{l_{j_0}}$ are one by one uniquely determined and so the system (16) has a unique solution.

This ends the proof of the first part of the claim for $t = 1$ and so it also ends the proof of the claim.

3.1.2. Inequalities involving s- and h-numbers

Let s'_L and h'_L be the s-number and the h-number (respectively) of $(\mathrm{Lie}(G'), \varphi)$. Let s_L and h_L be the s-number and the h-number (respectively) of $(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M), \varphi)$. We recall from 2.7 that $d_{\mathrm{sm}} \in \mathbf{N} \cup \{0\}$ is the smallest number such that we have inclusions

$$(17a) \qquad p^{d_{\mathrm{sm}}}\left(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)\right) \subseteq \mathrm{Lie}(G') \subseteq \mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M).$$

We have $p^{s_L}\varphi(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)) \subseteq \mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)$. Thus $p^{s_L+d_{\mathrm{sm}}}\varphi(\mathrm{Lie}(G')) \subseteq p^{s_L+d_{\mathrm{sm}}}\varphi(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)) \subseteq p^{d_{\mathrm{sm}}}(\mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)) \subseteq \mathrm{Lie}(G')$. From the very

definition of s'_L we get

$$(17b) \qquad\qquad\qquad s'_L \leqslant s_L + d_{\text{sm}}.$$

The h-numbers of $(\text{Lie}(G_{B(k)}) \cap \text{End}(M), p^{\max\{s_L,s'_L\}}\varphi)$ and $(\text{Lie}(G'), p^{\max\{s_L,s'_L\}}\varphi)$ are $h_L + \max\{s_L,s'_L\} - s_L$ and $h'_L + \max\{s_L,s'_L\} - s'_L$ (respectively). From this and (17a) we easily get that

$$(17c) \qquad\qquad h'_L + \max\{s_L,s'_L\} - s'_L \leqslant d_{\text{sm}} + h_L + \max\{s_L,s'_L\} - s_L.$$

From (17b), (17c), and the inequalities $d_{\text{sm}} \leqslant n(G) \leqslant \delta(G)$ (see 2.7.2(c) and 2.7), we get

$$(17d) \qquad\qquad h'_L \leqslant h_L + d_{\text{sm}} + s'_L - s_L \leqslant h_L + d_{\text{sm}} + d_{\text{sm}} \leqslant h_L + 2\delta(G).$$

3.1.3. End of the proof of 1.2

As $v = \dim(G_{B(k)})$, G', and $n(G)$ depend only on G and as s'_L and h'_L depend only on the family $\{(M, g\varphi, G) \mid g \in G(W(k)) = G'(W(k))\}$ of latticed F-isocrystals with a group over k, the number

$$(18) \qquad\qquad\qquad n_{\text{fam}} := 2d(v, s'_L, h'_L) + \varepsilon_p + n(G)$$

is not changed if φ gets replaced by $g\varphi$ for some $g \in G(W(k))$. As $m \leqslant d(v, s'_L, h'_L)$ (cf. 2.4.1), we have $n_{\text{fam}} \geqslant 2m + \varepsilon_p + n(G)$. So from (12) applied with $n = n_{\text{fam}}$ and from 3.1.1, we get that for any $g_{n_{\text{fam}}} \in G(W(k))$ congruent mod $p^{n_{\text{fam}}}$ to 1_M, there exists an isomorphism between (M, φ, G) and $(M, g_{n_{\text{fam}}}\varphi, G)$ defined by an element of $G'(W(k)) = G(W(k))$. This property holds even if φ gets replaced by $g\varphi$. As $n(G) \leqslant \delta(G)$, we have

$$(19) \qquad\qquad\qquad n_{\text{fam}} \leqslant 2d(v, s'_L, h'_L) + \varepsilon_p + \delta(G).$$

So based on the effectiveness part of 2.4.1 and on (17b) and (17d), to end the proof of 1.2 it is enough to show that $\delta(G)$, s_L, and h_L are effectively bounded from above. But $\delta(G)$ is effectively computable in terms of the ideal sheaf of $\mathcal{O}_{\mathbf{GL}_M}$ that defines the closed embedding homomorphism $G \hookrightarrow \mathbf{GL}_M$, cf. [2, 3.3, Lemma 2]. As the numbers s_L and h_L are effectively computable in terms of $(\text{Lie}(G_{B(k)}), \varphi)$ and $\text{End}(M)$ and as the connected group $G_{B(k)}$ is uniquely determined by its Lie algebra (cf. [1, Ch. II, 7.1]), the numbers s_L and h_L are also effectively computable in terms of the closed embedding homomorphism $G \hookrightarrow \mathbf{GL}_M$. This ends the proof of 1.2.

3.1.4. DEFINITION. – Let (M, φ, G) be a latticed F-isocrystal with a group over k. By the *isomorphism number* (to be abbreviated as the *i-number*) of (M, φ, G) we mean the smallest number $n \in \mathbf{N} \cup \{0\}$ such that for any $g_n \in G(W(\bar{k}))$ congruent mod p^n to $1_{M \otimes_{W(k)} W(\bar{k})}$, there exists an isomorphism between $(M \otimes_{W(k)} W(\bar{k}), \varphi \otimes \sigma_{\bar{k}}, G_{W(\bar{k})})$ and $(M \otimes_{W(k)} W(\bar{k}), g_n(\varphi \otimes \sigma_{\bar{k}}), G_{W(\bar{k})})$ which is an element of $G(W(\bar{k}))$. If $G = \mathbf{GL}_M$, we also refer to n as the i-number of (M, φ).

If $(M, \varphi, G, \lambda_M)$ and G^0 are as in 2.2.1(c), then by the i-number of $(M, \varphi, G, \lambda_M)$ we mean the i-number of its latticed F-isocrystal with a group (M, φ, G^0) over k.

3.1.5. *Example*. – Suppose G is smooth over $\text{Spec}(W(k))$ and $k = \bar{k}$. Thus $n(G) = d_{\text{sm}} = 0$, $s'_L = s_L$, $h'_L = h_L$, and $n_{\text{fam}} = 2d(v, s_L, h_L) + \varepsilon_p$. Let $m := \mathbf{T}(\text{Lie}(G'), \varphi)$. If n is as in 3.1.4, then we have $0 \leqslant n \leqslant 2m + \varepsilon_p \leqslant 2d(v, s_L, h_L) + \varepsilon_p$ (cf. 3.1.1 and 3.1.3).

3.2. Truncations

In 3.2.1 to 3.2.7 we work in a context that pertains to Dieudonné modules and to p-divisible groups. In particular, in 3.2.1 and 3.2.2 we define and study D-truncations that are the crystalline analogues (with a group) over k of truncated Barsotti–Tate groups over $\mathrm{Spec}(k)$. In 3.2.8 we consider reductions modulo powers of p of those F-crystals with a group (M, φ, G) over k for which G is smooth over $\mathrm{Spec}(W(k))$. In 3.2.9 we introduce the F-truncations that generalize the D-truncations.

3.2.1. On D-truncations

Let $(r, d) \in \mathbf{N} \times (\mathbf{N} \cup \{0\})$. Let (M, φ, G) be an F-crystal with a group over k. Until 3.2.8 we assume that (M, φ) is a Dieudonné module over k, that $r_M = r$, that d is the dimension of the kernel of $\varphi \mod p$, that G is smooth over $\mathrm{Spec}(W(k))$, and that the W-condition holds for (M, φ, G). Let $M = \widetilde{F}^0(M) \oplus \widetilde{F}^1(M)$ be a direct sum decomposition such that $M = \varphi(\widetilde{F}^0(M) \oplus \frac{1}{p}\widetilde{F}^1(M))$ and the cocharacter $\mu : \mathbf{G}_m \to \mathbf{GL}_M$ that fixes $\widetilde{F}^0(M)$ and that acts via the inverse of the identical character of $\mathbf{G}_m$ on $\widetilde{F}^1(M)$, factors through G (cf. 2.2.1(d)). The rank of $\widetilde{F}^1(M)$ is d. Let $\sigma_0 := \varphi\mu(p)$; it is a σ-linear automorphism of either M and $\mathcal{T}(M)$ (cf. 2.5). As σ_0 normalizes $\mathrm{Lie}(G_{B(k)})$ and $\mathrm{End}(M)$, it also normalizes $\mathrm{Lie}(G) = \mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M)$. As $G(W(k)) = G(B(k)) \cap \mathbf{GL}_M(W(k))$, we have $\sigma_0 G(W(k))\sigma_0^{-1} = G(W(k))$.

Let $q \in \mathbf{N}$. Let $\vartheta : M \to M$ be the σ^{-1}-linear endomorphism that is the Verschiebung map of (M, φ); we have $\vartheta\varphi = \varphi\vartheta = p1_M$. We denote also by ϑ its reduction $\mod p^q$. By the D-truncation $\mod p^q$ of (M, φ, G) we mean the quadruple

$$\left(M/p^q M, \varphi, \vartheta, G_{W_q(k)}\right).$$

This quadruple determines (respectively is determined by) the reduction $\mod p^q$ (respectively $\mod p^{q+1}$) of (M, φ, G). We also refer to $(M/p^q M, \varphi, \vartheta)$ as the D-truncation $\mod p^q$ of (M, φ). If $(M_1/p^q M_1, \varphi_1, \vartheta_1, G_{1W_q(k)})$ is a similar D-truncation $\mod p^q$, then by an isomorphism $f : (M/p^q M, \varphi, \vartheta, G_{W_q(k)}) \xrightarrow{\sim} (M_1/p^q M_1, \varphi_1, \vartheta_1, G_{1W_q(k)})$ we mean a $W_q(k)$-linear isomorphism $f : M/p^q M \xrightarrow{\sim} M_1/p^q M_1$ such that we have identities $f\varphi = \varphi_1 f$ and $f\vartheta = \vartheta_1 f$ and the isomorphism $\mathbf{GL}_{M/p^q M} \xrightarrow{\sim} \mathbf{GL}_{M_1/p^q M_1}$ induced by f, takes $G_{W_q(k)}$ onto $G_{1W_q(k)}$.

If (M_1, φ_1, G_1) is $(M, g\varphi, G)$ with $g \in G(W(k))$ and if $f \in G(W_q(k))$, then we say f is an *inner isomorphism* between the D-truncation $\mod p^q$ of (M, φ, G) and $(M, g\varphi, G)$.

3.2.2. LEMMA. – *For $g \in G(W(k))$ the following two statements are equivalent*:
(a) *the D-truncations $\mod p^q$ of (M, φ, G) and $(M, g\varphi, G)$ are inner isomorphic*;
(b) *there exists an element $\tilde{g} \in G(W(k))$ such that $\tilde{g}g\varphi\tilde{g}^{-1} = g_q\varphi$, where $g_q \in G(W(k))$ is congruent $\mod p^q$ to 1_M.*

Proof. – As G is smooth over $\mathrm{Spec}(W(k))$, the reduction homomorphism $G(W(k)) \to G(W_q(k))$ is onto. Thus it suffices to check that (a) implies (b) under the extra assumptions that the σ-linear endomorphisms φ and $g\varphi$ coincide $\mod p^q$ and that the σ^{-1}-linear endomorphisms ϑ and ϑg^{-1} coincide $\mod p^q$. Let $g_0 := \sigma_0^{-1} g \sigma_0 \in G(W(k))$. Let $g_{0,q} \in G(W_q(k))$ be $g_0 \mod p^q$. We have $\varphi = \sigma_0\mu(p^{-1})$ and $g\varphi = \sigma_0 g_0 \mu(p^{-1})$. We get that the two endomorphisms $\mu(p^{-1})$ and $g_0\mu(p^{-1})$ of M coincide $\mod p^q$. Thus

(i) the element $g_{0,q}$ fixes $\widetilde{F}^0(M)/p^q\widetilde{F}^0(M)$ and is congruent $\mod p^{q-1}$ to $1_{M/p^q M}$.

We have $\vartheta = p\mu(p)\sigma_0^{-1}$ and $\vartheta g^{-1} = p\mu(p)g_0^{-1}\sigma_0^{-1}$. We get that the two endomorphisms $p\mu(p)$ and $p\mu(p)g_0^{-1}$ of M coincide $\mod p^q$. Thus $p\mu(p)$ and $p\mu(p)g_0$ also coincide $\mod p^q$ and therefore we have an inclusion

(ii) $(1_{M/p^q M} - g_{0,q})(\widetilde{F}^1(M)/p^q \widetilde{F}^1(M)) \subseteq p^{q-1} \widetilde{F}^0(M)/p^q \widetilde{F}^0(M)$.

Let $\widetilde{F}^{-1}(\mathrm{End}(M))$ be the maximal direct summand of $\mathrm{End}(M)$ on which μ acts via the identity cocharacter of $\mathbf{G}_m$. Thus $\widetilde{F}^{-1}(\mathrm{End}(M))$ is the $\mathrm{Hom}(\widetilde{F}^1(M), \widetilde{F}^0(M))$ factor of the following direct sum decomposition $\mathrm{End}(M) = \mathrm{End}(\widetilde{F}^1(M)) \oplus \mathrm{End}(\widetilde{F}^0(M)) \oplus \mathrm{Hom}(\widetilde{F}^1(M), \widetilde{F}^0(M)) \oplus \mathrm{Hom}(\widetilde{F}^0(M), \widetilde{F}^1(M))$ into $W(k)$-submodules.

Let U_{-1}^{big} be the closed subgroup scheme of $\mathbf{GL}_M$ defined by the rule: if A is a commutative $W(k)$-algebra, then $U_{-1}^{\mathrm{big}}(A) := 1_{M \otimes_{W(k)} A} + \widetilde{F}^{-1}(\mathrm{End}(M)) \otimes_{W(k)} A \leqslant \mathbf{GL}_M(A)$. So U_{-1}^{big} is the maximal subgroup scheme of $\mathbf{GL}_M$ that fixes both $\widetilde{F}^0(M)$ and $M/\widetilde{F}^0(M)$; it is smooth over $\mathrm{Spec}(W(k))$. We have $\mathrm{Lie}(U_{-1}^{\mathrm{big}}) = \widetilde{F}^{-1}(\mathrm{End}(M))$. Let U_{-1} be the closed subgroup scheme of U_{-1}^{big} defined by the rule:

$$U_{-1}(A) := 1_{M \otimes_{W(k)} A} + \big(\mathrm{Lie}(G) \cap \widetilde{F}^{-1}\big(\mathrm{End}(M)\big)\big) \otimes_{W(k)} A.$$

The group scheme U_{-1} is smooth, unipotent, has connected fibres and its Lie algebra is the direct summand $\mathrm{Lie}(G) \cap \widetilde{F}^{-1}(\mathrm{End}(M))$ of $\widetilde{F}^{-1}(\mathrm{End}(M))$. As $U_{-1B(k)}$ is connected and $\mathrm{Lie}(U_{-1}) \subseteq \mathrm{Lie}(G)$, the group $U_{-1B(k)}$ is a closed subgroup of $G_{B(k)}$ (cf. [1, Ch. II, 7.1]). Thus U_{-1} is a closed subgroup scheme of G. As μ factors through G, we have two identities $\mathrm{Lie}(G) \cap \mathrm{Lie}(U_{-1}^{\mathrm{big}}) = \mathrm{Lie}(U_{-1})$ and $\mathrm{Lie}(G_k) \cap \mathrm{Lie}(U_{-1k}^{\mathrm{big}}) = \mathrm{Lie}(U_{-1k})$. Thus the intersection $U'_{-1} := G \cap U_{-1}^{\mathrm{big}}$ has smooth fibres and has U_{-1} as its identity component. As the group $U_{-1B(k)}^{\mathrm{big}}/U_{-1B(k)}$ has no non-trivial finite subgroups, we have $U_{-1B(k)} = U'_{-1B(k)}$. As U_{-1}^{big} is a complete intersection in $\mathbf{GL}_M$, U'_{-1} has dimension at least equal to $1 + \dim(U_{-1k})$ at each k-valued point. So as $\dim(U'_{-1k}) = \dim(U_k)$, the group $U'_{-1B(k)} = U_{-1B(k)}$ is Zariski dense in U'_{-1}. Thus $U_{-1} = U'_{-1} = G \cap U_{-1}^{\mathrm{big}}$.

We have $g_{0,q} \in \mathrm{Ker}(U_{-1}^{\mathrm{big}}(W_q(k)) \to U_{-1}^{\mathrm{big}}(W_{q-1}(k)))$, cf. (i) and (ii). As $U_{-1} = G \cap U_{-1}^{\mathrm{big}}$, in fact we have $g_{0,q} \in \mathrm{Ker}(U_{-1}(W_q(k)) \to U_{-1}(W_{q-1}(k)))$. Thus, up to a replacement of g by a $\mathrm{Ker}(G(W(k)) \to G(W_q(k)))$-multiple of it, we can assume that $g_0 \in U_{-1}(W(k))$. We write $g_0 = 1_M + p^{q-1} u_{-1}$, where $u_{-1} \in \mathrm{Lie}(U_{-1})$.

Let $\tilde{g} := 1_M + p^q u_{-1} \in U_{-1}(W(k)) \leqslant G(W(k))$. As we have $\tilde{g}^{-1} = 1_M - p^q u_{-1}$ and $g_0^{-1} = 1_M - p^{q-1} u_{-1}$, we get $\mu(p^{-1}) \tilde{g}^{-1} \mu(p) = g_0^{-1}$. Thus we compute that $\tilde{g} g \varphi \tilde{g}^{-1}$ is $\tilde{g} g \sigma_0 \mu(p^{-1}) \tilde{g}^{-1} \mu(p) \sigma_0^{-1} \varphi = \tilde{g} g \sigma_0 g_0^{-1} \sigma_0^{-1} \varphi = \tilde{g} g (\sigma_0 g_0 \sigma_0^{-1})^{-1} \varphi = \tilde{g} g g^{-1} \varphi = \tilde{g} \varphi$. So as g_q we can take $\tilde{g}$. Thus (a) implies (b). Obviously (b) implies (a). □

3.2.3. COROLLARY. – *Suppose $k = \bar{k}$ and (M, φ) is the Dieudonné module of a p-divisible group D over $\mathrm{Spec}(k)$ of height $r = r_M$ and dimension d. Let $n \in \mathbf{N} \cup \{0\}$ be the i-number of (M, φ). Then n is the smallest number $t \in \mathbf{N} \cup \{0, \infty\}$ for which the following statement holds:*

(∗) *if D_1 is a p-divisible group over $\mathrm{Spec}(k)$ of height r and dimension d and if $D_1[p^t]$ is isomorphic to $D[p^t]$, then D_1 is isomorphic to D.*

Proof. – The Dieudonné module of D_1 is isomorphic to $(M, g\varphi)$ for some $g \in \mathbf{GL}_M(W(k))$; moreover any such pair $(M, g\varphi)$ is isomorphic to the Dieudonné module of some p-divisible group over $\mathrm{Spec}(k)$ of height r and dimension d. For $q \in \mathbf{N}$, the classical Dieudonné theory achieves also a natural one-to-one and onto correspondence between the isomorphism classes of truncated Barsotti–Tate groups of level q over k and the isomorphism classes of D-truncations mod p^q of Dieudonné modules over k (see [14, pp. 153 and 160]). So (∗) holds if and only if for any $g \in \mathbf{GL}_M(W(k))$, the fact that the D-truncations mod p^t of (M, φ) and $(M, g\varphi)$ are isomorphic implies that (M, φ) and $(M, g\varphi)$ are isomorphic. From this and 3.2.2 (applied with $G = \mathbf{GL}_M$ and $q = t$), we get that (∗) holds if and only if (M, φ) and $(M, g\varphi)$ are isomorphic for all elements $g \in \mathbf{GL}_M(W(k))$ congruent mod p^t to 1_M. Thus (∗) holds if and only if $t \geqslant n$. □

3.2.4. Proof of 1.3

To prove 1.3, we can assume that $k = \bar{k}$ and that (M, φ) is the Dieudonné module of D. Let n be the i-number of (M, φ). Let n_{fam} be as in 3.1.5 for $G = \mathbf{GL}_M$. We have $n \leqslant n_{\mathrm{fam}}$, cf. 3.1.5. From 3.2.3 we get that D is uniquely determined up to isomorphism by $D[p^n]$ and so also by $D[p^{n_{\mathrm{fam}}}]$. Thus the number $T(r, d)$ exists and we have $T(r, d) \leqslant n_{\mathrm{fam}}$. From 3.2.3 we also get that $T(r, d) \geqslant n$. If $d \in \{0, r\}$, then $T(r, d) = n_{\mathrm{fam}} = n = 0$. If $d \notin \{0, r\}$, then the s-number and the h-number of $(\mathrm{End}(M), \varphi)$ are 1 and 2 (respectively) and $\mathrm{End}(M)$ has rank r^2. Thus for $d \in S(1, r - 1)$ we have (cf. 3.1.5)

$$n \leqslant T(r, d) \leqslant n_{\mathrm{fam}} \leqslant 2d\big(r^2, 1, 2\big) + \varepsilon_p.$$

So $T(r, d)$ is effectively bounded from above in terms of r, cf. 2.4.1. This proves 1.3.

3.2.5. Principal quasi-polarizations

Suppose $r = 2d = r_M$, $k = \bar{k}$, and we have a principal quasi-polarization λ_M of (M, φ). We refer to the triple (M, φ, λ_M) as a principally quasi-polarized Dieudonné module over k. Let $G := \mathbf{Sp}(M, \lambda_M)$. Let $n \in \mathbf{N} \cup \{0\}$ be the i-number of (M, φ, G). Let (D, λ_D) be a principally quasi-polarized p-divisible group over $\mathrm{Spec}(k)$ whose principally quasi-polarized Dieudonné module is isomorphic to (M, φ, λ_M). The principally quasi-polarized Dieudonné module of any other principally quasi-polarized p-divisible group over $\mathrm{Spec}(k)$ of height $r = r_M$ is of the form $(M, g\varphi, \lambda_M)$ for some $g \in G(W(k))$. So as in the proof of 3.2.3 we argue that n is the smallest number $t \in \mathbf{N} \cup \{0, \infty\}$ for which the following statement holds:

(∗) *if (D_1, λ_{D_1}) is a principally quasi-polarized p-divisible group over $\mathrm{Spec}(k)$ of height $r = 2d$ and if the principally quasi-polarized truncated Barsotti–Tate groups of level t of (D_1, λ_{D_1}) and (D, λ_D) are isomorphic, then (D_1, λ_{D_1}) is isomorphic to (D, λ_D).*

As in 3.2.4 we argue that there exists a smallest number $T(d) \in \mathbf{N}$ such that any principally quasi-polarized p-divisible group over $\mathrm{Spec}(k)$ of height $r = 2d$ is uniquely determined up to isomorphism by its principally quasi-polarized truncated Barsotti–Tate group of level $T(d)$. The number $T(d)$ is effectively bounded from above in terms of the relative dimension $2d^2 + d$ of $G = \mathbf{Sp}(M, \lambda_M)$ over $\mathrm{Spec}(W(k))$ and so also of d itself.

From the very definition of $T(d)$ we get:

3.2.6. COROLLARY. – *Suppose $k = \bar{k}$. Let D be a p-divisible group over $\mathrm{Spec}(k)$ of height $r = 2d$ and dimension d. Let D^{t} be the Cartier dual of D. Then the number of isomorphism classes of principally quasi-polarized p-divisible groups of the form (D, λ_D) is bounded from above by the finite number of distinct truncations of level $T(d)$ of isomorphisms $D \xrightarrow{\sim} D^{\mathrm{t}}$, i.e. by the number of elements of the following finite set of isomorphisms $\mathrm{Im}(\mathrm{Isom}(D, D^{\mathrm{t}}) \to \mathrm{Isom}(D[p^{T(d)}], D^{\mathrm{t}}[p^{T(d)}]))$.*

3.2.7. PROPOSITION. – *Suppose $k = \bar{k}$. Let R be the normalization of $k[[w]]$ in an algebraic closure K of $k((w))$. For $* \in \{k, K\}$ let D_* be a p-divisible group over $\mathrm{Spec}(*)$ of height r and dimension d. Then D_k is the specialization (via $\mathrm{Spec}(R)$) of a p-divisible group over $\mathrm{Spec}(K)$ which is isomorphic to D_K if and only if $D_k[p^{T(r,d)}]$ is the specialization (via $\mathrm{Spec}(R)$) of a truncated Barsotti–Tate group of level $T(r, d)$ over $\mathrm{Spec}(K)$ which is isomorphic to $D_K[p^{T(r,d)}]$.*

Proof. – It suffices to check the if part. Let $\mathcal{G}_R$ be a truncated Barsotti–Tate group of level $T(r, d)$ over $\mathrm{Spec}(R)$ that lifts $D_k[p^{T(r,d)}]$ and that has the property that its fibre over $\mathrm{Spec}(K)$ is isomorphic to $D_K[p^{T(r,d)}]$. Let R_0 be a finite $k[[w]]$-subalgebra of R such that $\mathcal{G}_R$ is the pullback of a truncated Barsotti–Tate group $\mathcal{G}_{R_0}$ of level $T(r, d)$ over $\mathrm{Spec}(R_0)$. As R_0 is a complete discrete valuation ring, there exists a p-divisible group D'_{R_0} over $\mathrm{Spec}(R_0)$ that lifts

both D_k and $\mathcal{G}_{R_0}$ (cf. [21, 4.4(f)]). The pullback of D'_{R_0} to $\operatorname{Spec}(K)$ is isomorphic to D_K (cf. 1.3) and it specializes (via $\operatorname{Spec}(R)$) to D_k. $\square$

We have a logical variant of 3.2.7 in the principally quasi-polarized context. We next consider F-crystals with a group over k.

3.2.8. THEOREM. – *Suppose $k = \bar{k}$. Let (M, φ, G) be an F-crystal with a group over k; so $\varphi(M) \subseteq M$. Let h be the h-number of (M, φ). Let $m := \mathbf{T}(\operatorname{Lie}(G), \varphi)$ and let $n := 2m + \varepsilon_p$. Let $g \in G(W(k))$. Let $t \in \mathbf{N} \cup \{0\}$.*
   (a) *Suppose G is smooth over $\operatorname{Spec}(W(k))$ and there exists $\tilde{g}_{h+n+t} \in G(W_{h+n+t}(k))$ which is an isomorphism between the reductions $\mod p^{h+n+t}$ of $(M, g\varphi)$ and (M, φ). Then there exists $\tilde{g}_0 \in G(W(k))$ which is an isomorphism between $(M, g\varphi, G)$ and (M, φ, G) and whose image in $G(W_{h+n+t}(k))$ is congruent $\mod p^{n-m+t}$ to $\tilde{g}_{h+n+t}$.*
   (b) *If $G = \mathbf{GL}_M$, then the images of the two reduction homomorphisms $\operatorname{Aut}(M, \varphi) \to \operatorname{Aut}(M/p^{n-m+t}M, \varphi)$ and $\operatorname{Aut}(M/p^{n+h+t}M, \varphi) \to \operatorname{Aut}(M/p^{n-m+t}M, \varphi)$ are the same.*

Proof. – Part (b) is a practical application of (a) for the case when $G = \mathbf{GL}_M$. As $G(W(k))$ surjects onto $G(W_{h+n+t}(k))$, it suffices to prove (a) under the extra assumption that $\tilde{g}_{h+n+t} = 1_{M/p^{h+n+t}M}$. So $g \mod p^{h+n+t}$ fixes $\operatorname{Im}(\varphi(M) \to M/p^{h+n+t}M)$. But $p^h M \subseteq \varphi(M)$ and so $g \mod p^{h+n+t}$ fixes also the $W_{h+n+t}(k)$-submodule $p^h M/p^{h+n+t}M$ of $M/p^{h+n+t}M$. Thus g is congruent $\mod p^{n+t}$ to 1_M. So the element $\tilde{g}_0$ exists, cf. 3.1.1 (applied with $G = G'$, $M = M'$, and $n(G) = 0$). $\square$

3.2.9. On F-truncations

One can generalize the D-truncations of 3.2.1 as follows. Let (M, φ, G) be a p-divisible object with a group over k and let $(F^i(M))_{i \in S(a,b)}$ be a lift of it (see 2.2.1(b) and (d)). Let $\varphi_i : F^i(M) \to M$ be the σ-linear map defined by the rule $\varphi_i(x) = p^{-i}\varphi(x)$, where $x \in F^i(M)$. We denote also by φ_i its reduction $\mod p^q$. By an *inner isomorphism* between $(M/p^q M, (F^i(M)/p^q F^i(M))_{i \in S(a,b)}, (\varphi_i)_{i \in S(a,b)}, G_{W_q(k)})$ and a similar quadruple $(M/p^q M, (F^i_1(M)/p^q F^i_1(M))_{i \in S(a,b)}, ((g\varphi)_i)_{i \in S(a,b)}, G_{W_q(k)})$ defined by some lift $(F^i_1(M))_{i \in S(a,b)}$ of $(M, g\varphi, G)$ (with $g \in G(W(k))$), we mean an arbitrary element $f \in \operatorname{Im}(G(W(k)) \to G(W_q(k)))$ that has the following two properties:
   (i) it takes $F^i(M)/p^q F^i(M)$ onto $F^i_1(M)/p^q F^i_1(M)$ for all $i \in S(a,b)$;
   (ii) we have $f\varphi_i = (g\varphi)_i f$ for all $i \in S(a,b)$.

By the *F-truncation* $\mod p^q$ of (M, φ, G) we mean the set $F_q(M, \varphi, G)$ of inner isomorphism classes of quadruples $(M/p^q M, (F^i(M)/p^q F^i(M))_{i \in S(a,b)}, (\varphi_i)_{i \in S(a,b)}, G_{W_q(k)})$ we obtain by allowing $(F^i(M))_{i \in S(a,b)}$ to run through all lifts of (M, φ, G).

If (M, φ) is a Dieudonné module over k and if G is smooth, then it is easy to see that the D-truncations $\mod p^q$ of (M, φ, G) and $(M, g\varphi, G)$ are inner isomorphic if and only if the F-truncations $\mod p^q$ of (M, φ, G) and $(M, g\varphi, G)$ are inner isomorphic.

3.3. Refinements of 3.1.1

In many particular cases we can choose the $W(k)$-span E of 3.1.1(a) to be stable under products and this can lead to significant improvements of the inequalities we obtained in 3.1.1 to 3.1.5. For the sake of generality, we now formalize such improvements in a relative context.

Let (M, φ, G) be a latticed F-isocrystal with a group over k. Until Section 4 we assume $k = \bar{k}$. Until Section 4 we also assume that there exists an integral, closed subgroup scheme G_1 of $\mathbf{GL}_M$ which contains G and for which the following two conditions hold:

(i) the triple (M, φ, G_1) is a latticed F-isocrystal with a group over k;
(ii) there exist a $B(k)$-basis $\mathcal{B}_1 := \{e_1, \ldots, e_{v_1}\}$ of $\mathrm{Lie}(G_{1B(k)})$ and a permutation π_1 of $S(1, v_1)$, that have the following four properties:
  (ii.a) $E_1 := \langle e_1, \ldots, e_{v_1} \rangle$ is a $W(k)$-submodule of $\mathrm{End}(M)$ such that $E_1 E_1 \subseteq E_1$;
  (ii.b) each cycle $(l_1, \ldots, l_q)$ of π_1 has the property that for $j \in S(1, q)$ we have $\varphi(e_{l_j}) = p^{n_{l_j}} e_{l_{j+1}}$, where the integers n_{l_j}'s are either all non-negative or all non-positive;
  (ii.c) if $v := \dim(G_{B(k)})$ (so $v \in S(1, v_1)$), then the intersection $E := E_1 \cap \mathrm{Lie}(G_{B(k)})$ has $\{e_1, \ldots, e_v\}$ as a $W(k)$-basis and moreover the permutation π_1 normalizes $S(1, v)$;
  (ii.d) for any $t \in \mathbf{N}$ and every element of $G(W(k))$ that has the form $1_M + \sum_{l \in S(1,v_1)} p^t x_l e_l$, where all x_l's belong to $W(k)$, we have $x_l \in pW(k)$ for all $l \in S(v+1, v_1)$.

Let
$$E_2 := E_1\left[\frac{1}{p}\right] \cap \mathrm{End}(M) = \mathrm{Lie}(G_{1B(k)}) \cap \mathrm{End}(M).$$

From (ii.a) we get that $1_M + E_2$ is a semigroup with identity contained in $\mathrm{End}(M)$.

3.3.1. LEMMA. – *There exists a closed subgroup scheme G_2 of $\mathbf{GL}_M$ that is defined by the rule*: *if A is a commutative $W(k)$-algebra, then $G_2(A)$ is the group of invertible elements of the semigroup with identity $1_{M \otimes_{W(k)} A} + E_2 \otimes_{W(k)} A$. We have $G_1 = G_2$.*

Proof. – We show that G_2 is an integral, closed subgroup scheme of $\mathbf{GL}_M$ and that $\mathrm{Lie}(G_{2B(k)}) \subseteq E_2[\frac{1}{p}] = E_1[\frac{1}{p}]$. If $1_M \in E_2$, then $1_M + E_2 = E_2$ is a $W(k)$-subalgebra of $\mathrm{End}(M)$ which as a $W(k)$-submodule is a direct summand; so obviously G_2 is an integral, closed subgroup scheme of $\mathbf{GL}_M$ and we have $\mathrm{Lie}(G_{2B(k)}) \subseteq E_2[\frac{1}{p}] = E_1[\frac{1}{p}]$.

We now consider the case when $1_M \notin E_2$. Let $E_3 := \mathrm{End}(M) \cap (E_2[\frac{1}{p}] + B(k)1_M)$; it is a $W(k)$-subalgebra of $\mathrm{End}(M)$ that has E_2 as a two-sided ideal. The finite $W(k)$-algebra E_3/E_2 is isomorphic to a $W(k)$-subalgebra of $B(k)1_M$ and so to $W(k)1_M$. So as $W(k)$-modules, we have a direct sum decomposition $E_3 = E_2 \oplus W(k)1_M$. Let G_3 be the integral, closed subgroup scheme of $\mathbf{GL}_M$ of invertible elements of E_3. Let $x \in 1_{M \otimes_{W(k)} A} + E_2 \otimes_{W(k)} A$ be an element that has an invertible determinant. The inverse $x^{-1} \in \mathrm{End}(M)$ of x belongs to $G_3(A)$ and moreover modulo the ideal $E_2 \otimes_{W(k)} A$ of $E_3 \otimes_{W(k)} A$ it is $1_{M \otimes_{W(k)} A}$. Thus $x^{-1} \in 1_{M \otimes_{W(k)} A} + E_2 \otimes_{W(k)} A$. This implies that the group $G_2(A)$ is the group of all elements of $1_{M \otimes_{W(k)} A} + E_2 \otimes_{W(k)} A$ that have an invertible determinant. From this description of points of G_2, we get that G_2 is an integral, closed subgroup scheme of either $\mathbf{GL}_M$ or G_3 and that we have $\mathrm{Lie}(G_{2B(k)}) \subseteq E_2[\frac{1}{p}] = E_1[\frac{1}{p}]$.

If $x \in E_1$, then we have $1_M + p^t x \in G_2(W(k))$ for all $t \gg 0$. Thus $E_1[\frac{1}{p}] \subseteq \mathrm{Lie}(G_{2B(k)})$ and therefore we have identities $\mathrm{Lie}(G_{1B(k)}) = E_1[\frac{1}{p}] = E_2[\frac{1}{p}] = \mathrm{Lie}(G_{2B(k)})$. So $G_{1B(k)} = G_{2B(k)}$, cf. [1, Ch. II, 7.1]. Thus $G_1 = G_2$. □

3.3.2. THEOREM. – *We recall that conditions 3.3(i) and (ii) hold. Let $m_1 \in \mathbf{N} \cup \{0\}$ be the smallest number such that $p^{m_1}(E_2) \subseteq E_1 \subseteq E_2$. Let $g \in G(W(k)) \cap (1_M + p^j E_1)$ with $j \in \mathbf{N}$. If $p = 2$ we assume that either $G = G_1$ or $j \geqslant 2$. We have*:
  (a) *There exists $\tilde{g} \in G(W(k)) \cap (1_M + p^j E_1)$ which is an isomorphism between $(M, g\varphi, G)$ and (M, φ, G).*
  (b) *The i-number of (M, φ, G) is at most $m_1 + 1$.*

Proof. – To prove (a), we write $g = 1_M + \sum_{l \in S(1,v_1)} p^j x_l(j) e_l$, where all $x_l(j)$'s belong to $W(k)$. By induction on $t \in \{j, j+1, \ldots\}$ we construct an element $\tilde{g}_t \in G(W(k))$ such that there

exist elements $x_l(t)$'s in $W(k)$ that satisfy the identity

$$(20a) \qquad \tilde{g}_t \tilde{g}_{t-1} \cdots \tilde{g}_j g \varphi \tilde{g}_j^{-1} \cdots \tilde{g}_{t-1}^{-1} \tilde{g}_t^{-1} \varphi^{-1} = 1_M + \sum_{l \in S(1,v_1)} p^t x_l(t) e_l.$$

If $t = j$ let $\tilde{g}_t := 1_M$. The passage from t to $t+1$ goes as follows. For $l \in S(1,v_1)$ let $q_l := -\min\{0, n_l\}$; we recall that $n_l \in \mathbf{Z}$ is such that $\varphi(e_l) = p^{n_l} e_{\pi_1(l)}$ (cf. 3.3(ii.b)).

We first consider the case $p \geqslant 3$. Let

$$(20b) \qquad \tilde{g}_{t+1} := \prod_{l \in S(1,v)} \exp\big(p^{t+q_l} \tilde{x}_l(t+1) e_l\big) \in G\big(W(k)\big),$$

where all $\tilde{x}_l(t+1)$'s belong to $W(k)$. As π_1 normalizes $S(1,v)$, we have

$$(20c) \qquad \varphi \tilde{g}_{t+1}^{-1} \varphi^{-1} = \prod_{l \in S(1,v)} \exp\big(-p^{t+q_l+n_l} \sigma\big(\tilde{x}_l(t+1)\big) e_{\pi_1(l)}\big) \in G\big(W(k)\big)$$

(to be compared with (14)). As $E_1 E_1 \subseteq E_1$ and $p \geqslant 3$, for any $e \in E_1$ the element $\exp(p^t e) = 1_M + \sum_{i=1}^{\infty} \frac{p^{ti}}{i!} e^i$ belongs to $1_M + p^t E_1$. From this and the inequalities $q_l \geqslant 0$ and $q_l + n_l \geqslant 0$, we get that any exponential element of either (20b) or (20c) belongs to $1_M + p^t E_1$. Thus, as $1_M + p^t E_1$ is a semigroup contained in $\mathrm{End}(M)$, we get that $\tilde{g}_{t+1} \in 1_M + p^t E_1$ and that (cf. also (20a)) we can write

$$(20d) \qquad \tilde{g}_{t+1}\big(\tilde{g}_t \cdots \tilde{g}_j g \varphi \tilde{g}_j^{-1} \cdots \tilde{g}_t^{-1} \varphi^{-1}\big) \varphi \tilde{g}_{t+1}^{-1} \varphi^{-1} = 1_M + \sum_{l \in S(1,v_1)} p^t x_l'(t+1) e_l,$$

where all $x_l'(t+1)$'s belong to $W(k)$. If $i > v$, then $x_l'(t+1) \in pW(k)$ (cf. 3.3(ii.d)).

Based on 2.6(a), from (20b), (20c), and (20d) we get that for any $l \in S(1,v)$ the Witt vector $x_l'(t+1) \in W(k)$ is congruent $\mathrm{mod}\ p$ to the sum (to be compared with (15))

$$p^{q_l} \tilde{x}_l(t+1) + x_l(t) - p^{n_{\pi_1^{-1}(l)} + q_{\pi_1^{-1}(l)}} \sigma\big(\tilde{x}_{\pi_1^{-1}(l)}(t+1)\big).$$

As in the part of the proof of 3.1.1 that pertains to $(+)$ and $(-)$, we argue that we can choose the $\tilde{x}_l(t+1)$'s with $l \in S(1,v)$ such that we have $x_l'(t+1) \in pW(k)$ for all $l \in S(1,v)$. Thus for all $l \in S(1,v_1)$ we can write $p^t x_l'(t+1) = p^{t+1} x_l(t+1)$, where $x_l(t+1) \in W(k)$. This ends the induction for $p \geqslant 3$.

Let now $p = 2$. For $t \geqslant 2$, we have $2t - 1 \geqslant t + 1$. So the above passage from t to $t+1$ has to be modified only if $t = j = 1$, cf. 2.6(b). As $E_1 E_1 \subseteq E_1$, for any $e \in E_1$ the element $1_M + pe$ has an inverse in $1_M + pE_1$ and thus (cf. 3.3.1) it is an element of $G_2(W(k)) = G_1(W(k))$. Thus, if $t = j = 1$ and $G = G_1$, we can take

$$(20e) \qquad \tilde{g}_2 := 1_M + \sum_{l \in S(1,v)} p^{1+q_l} \tilde{x}_l(2) e_l \in G_2\big(W(k)\big) = G_1\big(W(k)\big) = G\big(W(k)\big)$$

and we can proceed as above. This ends the induction.

The infinite product $\tilde{g} := \cdots \tilde{g}_{j+2} \tilde{g}_{j+1} \tilde{g}_j \in G(W(k)) \cap (1_M + p^j E_1)$ is well defined (as $W(k)$ is p-adically complete). Passing to limit $t \to \infty$ in (20a), we get $\tilde{g} g \varphi \tilde{g}^{-1} \varphi^{-1} = 1_M$. Thus $\tilde{g}$ is an isomorphism between $(M, g\varphi, G)$ and (M, φ, G). So (a) holds.

We prove (b). For $g \in G(W(k)) \leqslant G_1(W(k))$, we have $g - 1_M \in E_2$ (cf. 3.3.1). If g is congruent mod p^{m_1+1} to 1_M, then $g - 1_M \in p^{m_1+1}E_2 \subseteq pE_1$. Thus $g \in G(W(k)) \cap (1_M + pE_1)$. So there exists an isomorphism between $(M, g\varphi, G)$ and (M, φ, G) which is an element of $G(W(k))$, cf. (a) applied with $j = 1$. So (b) follows from Definition 3.1.4.   □

3.3.3. Variant

Suppose $G = G_1$ and $E_1 E_1 = 0$. Then 3.3.2(a) holds even if $j = 0$, i.e. even if we only have $g \in G(W(k)) \cap (1_M + E)$. This is so as we have $\exp(x) = 1 + x$ for any $x \in E = E_1$. Thus the proof of 3.3.2(a) holds even if $j = 0$ and so the proof of 3.3.2(b) can be adapted to get that the i-number of (M, φ, G) is at most m_1.

3.3.4. COROLLARY. – *Let m_1 be as in 3.3.2. We assume that $G = G_1$ and that all slopes of $(\mathrm{Lie}(G_{B(k)}), \varphi)$ are 0. Then the i-number of (M, φ, G) is at most m_1.*

Proof. – Let $E_{\mathbf{Z}_p} := \{x \in \mathrm{Lie}(G_{B(k)}) \cap \mathrm{End}(M) \mid \varphi(x) = x\}$. We can assume $E = E_1$ is the $W(k)$-span of $E_{\mathbf{Z}_p}$. We have $E_{\mathbf{Z}_p} E_{\mathbf{Z}_p} \subseteq E_{\mathbf{Z}_p}$, cf. 3.3(ii.a). Let $g_{m_1} \in G(W(k))$ be congruent mod p^{m_1} to 1_M. We write $g_{m_1} = 1_M + e$, with $e \in E$ (to be compared with the proof of 3.3.2(b)). Based on 3.3.2(a), to prove the corollary it suffices to check that there exists $\tilde{g} \in G(W(k))$ such that $\tilde{g} g_{m_1} \varphi \tilde{g}^{-1} \varphi^{-1} \in G(W(k)) \cap (1_M + pE)$.

The element $1 + e = g_{m_1} \in G(W(k))$ normalizes E_2. Thus $(1_M + e)E \subseteq E \subseteq E_2 = (1_M + e)E_2$. So by reasons of length of artinian modules we get that $(1_M + e)E = E$. Let $e' \in E$ be such that $(1_M + e)e' = -e$. Thus $(1_M + e)(1_M + e') = 1_M + e - e = 1_M$. So $(1_M + e)^{-1} = 1_M + e' \in 1_M + E = 1_M + E_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} W(k)$.

Let H be the group scheme over $\mathrm{Spec}(\mathbf{Z}_p)$ defined by the rule: if A is a commutative $\mathbf{Z}_p$-algebra, then $H(A)$ is the group of invertible elements of the semigroup with identity $1_{M \otimes_{W(k)} A} + E_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} A$ contained in $\mathrm{End}(M) \otimes_{W(k)} A$. The automorphism σ of $W(k)$ acts naturally on $H(W(k))$. If $u \in H(W(k))$, then $u \in G(W(k))$ (cf. 3.3.1) and $\sigma(u) = \sigma u \sigma^{-1}$ is $\varphi u \varphi^{-1} \in H(W(k))$. Moreover we have $g_{m_1} \in H(W(k))$, cf. previous paragraph.

Let $\bar{g}_{m_1}$ be the image of g_{m_1} in $H(k)$. The scheme H is an open subscheme of the affine space over $\mathrm{Spec}(\mathbf{Z}_p)$ that is of relative dimension v and that is defined naturally by $E_{\mathbf{Z}_p}$. Thus the group scheme H over $\mathrm{Spec}(\mathbf{Z}_p)$ has connected fibres and is smooth. Moreover, the special fibre $H_{\mathbf{F}_p}$ is a quasi-affine group and thus also an affine group over $\mathrm{Spec}(\mathbf{F}_p)$ (cf. [6, vol. I, Exp. VI$_B$, 11.11]). Let $\bar{\tilde{g}} \in H(k)$ be such that $\bar{\tilde{g}} \bar{g}_{m_1} \sigma(\bar{\tilde{g}})^{-1}$ is the identity element of $H(k)$, cf. Lang theorem (see [1, Ch. V, 16.4]). Let $\tilde{g} \in H(W(k))$ be an element that lifts $\bar{\tilde{g}}$. The element $\tilde{g} g_{m_1} \varphi \tilde{g}^{-1} \varphi^{-1} = \tilde{g} g_{m_1} \sigma(\tilde{g}^{-1}) \in H(W(k)) \leqslant G(W(k))$ has a trivial image in $H(k)$ and thus it belongs to $1_M + pE$.   □

3.3.5. *Example.* – Let $c \in \mathbf{N}$ be such that $g.c.d.(c, r_M - c) = 1$. We assume (M, φ) is the Dieudonné module of a p-divisible group D over $\mathrm{Spec}(k)$ of height $r := r_M$, dimension $d := r - c = r_M - c$, and (unique) slope $\frac{d}{r}$. Let $m := \mathbf{T}(\mathrm{End}(M), \varphi)$. Let E be the $W(k)$-subalgebra of $\mathrm{End}(M)$ generated by elements of $\mathrm{End}(M)$ fixed by φ. As all slopes of $(\mathrm{End}(M[\frac{1}{p}]), \varphi)$ are 0, any $W(k)$-submodule O of $\mathrm{End}(M)$ with the property that (O, φ) is a Dieudonné–Fontaine p-divisible object over k, is $W(k)$-generated by elements fixed by φ and so is contained in E. Thus $m \in \mathbf{N} \cup \{0\}$ is the smallest number such that $p^m \mathrm{End}(M) \subseteq E$. As $c \in \mathbf{N}$, we have $E \neq \mathrm{End}(M)$ and so $m \geqslant 1$. The i-number n of (M, φ) is at most m, cf. 3.3.4. But D is uniquely determined up to isomorphism by $D[p^n]$ (cf. 3.2.3) and thus also by $D[p^m]$. Using direct sums of $t \in \mathbf{N}$ copies of (M, φ), a similar argument shows that D^t is uniquely determined up to isomorphism by $D^t[p^m]$.

3.3.6. *Example.* – The case $m = 1$ of 3.3.5 also solves positively the isoclinic case of [35, Conjecture 5.7] as one can easily check this starting from [10, 5.3 and 5.4]. For the reader's

convenience here is the version of the last sentence in the spirit of this paper. In this section, we use the notations of 3.3.5 and we moreover assume that D is such that there exists a $W(k)$-basis $\{e_0, e_1, \ldots, e_{r-1}\}$ of M with the property that $\varphi(e_i)$ is e_{i+d} if $i \in S(0, c-1)$ and is pe_{i+d} if $i \in S(c, r-1)$. Here and below, all the lower right indices of the form $_i$ and $_{i,j}$ are mod r. For $i, j \in S(0, r-1)$ let $e_{i,j} \in \mathrm{End}(M)$ be such that it annihilates $e_{j'}$ if $j' \neq j$ and takes e_j into e_i. We have $\varphi(e_{i,j}) = p^{n_{i,j}} e_{i+d,j+d}$, where the integer $n_{i,j}$ is defined by the rule:

($*$) *it is 0 if $(i,j) \in S(0, c-1)^2 \cup S(c, r-1)^2$, it is 1 if $(i,j) \in S(c, r-1) \times S(0, c-1)$, and it is -1 if $(i,j) \in S(0, c-1) \times S(c, r-1)$.*

We check that $m = 1$. Replacing D by D^{t} if necessary, we can assume $c > d = r - c$; so $c > \frac{r}{2}$. Based on (2) and the inequality $m \geqslant 1$, to show that $m = 1$ it is enough to show that for all pairs $(i,j) \in S(0, r-1)^2$ we have an equality $\mathbf{S}\tau_{i,j} = 1$, where $\tau_{i,j} := (n_{i,j}, n_{i+d,j+d}, n_{i+2d,j+2d}, \ldots, n_{i+(r-1)d,j+(r-1)d})$.

So it suffices to show that none of the $\tau_{i,j}$'s is of the form $(-1, 0, 0, \ldots, 0, -1, \ldots)$, cf. Definitions 2.2.4(b) and (c). Thus it suffices to show that for any pair $(i_0, j_0) \in S(0, c-1) \times S(c, r-1)$, the first non-zero number of the sequence $n_{i_0+d,j_0+d}, \ldots, n_{i_0+rd,j_0+rd}$ is 1. We write $j_0 = c + d_0$, with $d_0 \in S(0, d-1)$. As $d_0 \in S(0, c-1)$, we can assume $n_{i_0+d,j_0+d} = n_{i_0+d,d_0}$ is 0. Thus $(i_1, j_1) := (i_0 + d, d_0) \in S(0, c-1)^2$ and we have $i_1 \geqslant j_1$.

We have to show that the first non-zero number of the sequence $n_{i_1,j_1}, n_{i_1+d,j_1+d}, \ldots, n_{i_1+(r-1)d,j_1+(r-1)d}$ is 1. We can assume $n_{i_1+d,j_1+d} \neq 1$. As $i_1 \geqslant j_1$ we have $n_{i_1+d,j_1+d} \neq -1$. Thus $n_{i_1+d,j_1+d} = 0$. If $i_1 + d \leqslant c - 1$, let $(i_2, j_2) := (i_1 + d, j_1 + d) \in S(0, c-1)^2$; if $i_1 + d \geqslant c$, then from ($*$) and the equality $n_{i_1+d,j_1+d} = 0$ we get $j_1 + d \geqslant c$ and thus we have $(i_2, j_2) := (i_1 + 2d - r, j_1 + 2d - r) \in S(0, c-1)^2$. We conclude that $(i_2, j_2) \in S(0, c-1)^2$ and $i_2 \geqslant j_2$. We have $n_{i_2,j_2} = 0$. We have to show that the first non-zero number of the sequence $n_{i_2,j_2}, \ldots, n_{i_2+(r-1)d,j_2+(r-1)d}$ is 1. As in this way we cannot construct indefinitely pairs $(i_u, j_u) \in S(0, c-1)^2$ with $i_u \geqslant j_u$ (here $u \in \mathbf{N}$), we get that the first non-zero number of the sequence $n_{i_2,j_2}, \ldots, n_{i_2+(r-1)d,j_2+(r-1)d}$ is 1.

So $\mathbf{S}\tau_{i,j} = 1$ and $m = 1$. Thus for $t \in \mathbf{N}$, D^{t} is uniquely determined up to isomorphism by $D^{\mathrm{t}}[p]$ (cf. end of 3.3.5). This was predicted by [35, Conjecture 5.7].

3.3.7. *Example*. – We assume that all slopes of $(\mathrm{End}(M), \varphi)$ are 0 and that $G_1 = \mathbf{GL}_M$. Thus 3.3(i) holds. Let $E_{1\mathbf{Z}_p}$ be the $\mathbf{Z}_p$-subalgebra of $\mathrm{End}(M)$ formed by elements fixed by φ. Let $E_1 := E_{1\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} W(k) \subseteq \mathrm{End}(M)$; we have $v_1 = r_M^2$ and $E_2 = \mathrm{End}(M)$. We also assume that $p \geqslant 3$ and that $G = \mathbf{Sp}(M, \lambda_M)$ (respectively and that $G = \mathbf{SO}(M, \lambda_M)$), where λ_M is a perfect alternating (respectively perfect symmetric) bilinear form on M which is a principal (respectively a principal bilinear) quasi-polarization of (M, φ). As $p \geqslant 3$, we have a direct sum decomposition $\mathrm{End}(M) = \mathrm{Lie}(G) \oplus \mathrm{Lie}(G)^\perp$, where $\mathrm{Lie}(G)^\perp$ is the perpendicular of $\mathrm{Lie}(G)$ with respect to the trace form on $\mathrm{End}(M)$. As φ normalizes $\mathrm{Lie}(G)[\frac{1}{p}]$, it also normalizes $\mathrm{Lie}(G)^\perp[\frac{1}{p}]$. Thus E_1 has a $W(k)$-basis $\mathcal{B}_1 = \{e_1, \ldots, e_{v_1}\}$ that is the disjoint union of a $\mathbf{Z}_p$-basis $\{e_1, \ldots, e_v\}$ of $E_{1\mathbf{Z}_p} \cap \mathrm{Lie}(G)$ and of a $\mathbf{Z}_p$-basis $\{e_{v+1}, \ldots, e_{v_1}\}$ of $E_{1\mathbf{Z}_p} \cap \mathrm{Lie}(G)^\perp$. Let $\pi_1 := 1_{S(1,v_1)}$.

Properties 3.3(ii.a) to (ii.c) hold, cf. constructions. We check that 3.3(ii.d) holds. Let $g \in G(W(k))$ be of the form $1_M + \sum_{l \in S(1,v_1)} p^t x_l e_l$, where all x_l's belong to $W(k)$. The involution of $\mathrm{End}(M)$ defined by λ_M fixes $\mathrm{Lie}(G)^\perp$ and acts as -1 on $\mathrm{Lie}(G)$. Thus the product $(1_M - \sum_{l=1}^v p^t x_l e_l + \sum_{l=v+1}^{v_1} p^t x_l e_l)(1_M + \sum_{l \in S(1,v_1)} p^t x_l e_l)$ is 1_M (as $g \in G(W(k))$) and belongs to $1_M + 2(\sum_{l=v+1}^{v_1} p^t x_l e_l) + p^{t+1} E_1$. As $p \geqslant 3$, for $l \in S(v+1, v_1)$ we have $x_l \in pW(k)$. So 3.3(ii.d) holds. Thus 3.3(ii) holds. So 3.3.2 applies. In particular, the i-number of (M, φ, G) is at most $m_1 + 1$, where $m_1 \in \mathbf{N} \cup \{0\}$ is the smallest number such that we have $p^{m_1} \mathrm{End}(M) \subseteq E_1 = E_{1\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} W(k)$ (cf. 3.3.2(b)).

4. Four examples

In this section we include four examples that pertain to Sections 3.1 to 3.3. Let $\varepsilon_p \in \{1, 2\}$ be as before 3.1. Let (M, φ, G) be a p-divisible object with a group over k. Let $n \in \mathbf{N} \cup \{0\}$ be the i-number of (M, φ, G), cf. 3.1.4. In this section we will assume that $k = \bar{k}$ and that G is a reductive group scheme over $\mathrm{Spec}(W(k))$. Thus the group scheme G is smooth over $\mathrm{Spec}(W(k))$ and its fibres are connected and have trivial unipotent radicals. As G is smooth over $\mathrm{Spec}(W(k))$, with the notations of 2.7 we have $G = G'$ and $n(G) = 0$. Let $M = \bigoplus_{i=a}^{b} \widetilde{F}^i(M)$, $(F^i(M))_{i \in S(a,b)}$, and $\mu \colon \mathbf{G}_m \to G$ be as in 2.2.1(d). Let $b_L \in S(0, b-a)$ be the smallest number such that we have a direct sum decomposition

$$\mathrm{Lie}(G) := \bigoplus_{i=-b_L}^{b_L} \widetilde{F}^i\big(\mathrm{Lie}(G)\big)$$

with the property that $\beta \in \mathbf{G}_m(W(k))$ acts on $\widetilde{F}^i(\mathrm{Lie}(G))$ through μ as the multiplication with β^{-i}. As the group scheme G is reductive, both $W(k)$-modules $\widetilde{F}^{b_L}(\mathrm{Lie}(G))$ and $\widetilde{F}^{-b_L}(\mathrm{Lie}(G))$ are non-zero. As in 2.5, we have a σ-linear automorphism $\sigma_0 := \varphi\mu(p)$ of M. As $\varphi = \sigma_0\mu(p^{-1})$, the s-number of $(\mathrm{Lie}(G), \varphi)$ is b_L. If $b_L \leqslant 1$, we say (M, φ, G) is a *Shimura p-divisible object* over k. Let $f_{-1} \in \mathbf{N} \cup \{0\}$ be the rank of $\widetilde{F}^{-1}(\mathrm{Lie}(G))$.

In Sections 4.1–4.5 we will consider four unrelated situations.

4.1. Example 1

In this section we assume that $b_L = 1$ and that all slopes of $(\mathrm{Lie}(G), \varphi)$ are 0. Let $f \in \mathbf{N}$ be the smallest number such that there exists a filtration

$$0 = \mathcal{E}_0 \subseteq \mathcal{E}_1 \subseteq \cdots \subseteq \mathcal{E}_f := \mathrm{Lie}(G)$$

by $W(k)$-submodules that are direct summands, with the property that for any number $i \in S(1, f)$, the quotient $W(k)$-module $\mathcal{E}_i/\mathcal{E}_{i-1}$ is a maximal direct summand of $\mathrm{Lie}(G)/\mathcal{E}_{i-1}$ normalized by φ. For $i \in S(2, f)$ we choose $x_i \in \mathcal{E}_i \setminus (\mathcal{E}_{i-1} + p\mathcal{E}_i)$ such that we have $p\varphi(x_i) - px_i \in \mathcal{E}_{i-1} \setminus p\mathcal{E}_{i-1}$ and the images of $x_1, \ldots, x_{i-1}$, and x_i in

$$\mathrm{Lie}(G)/\big(\widetilde{F}^0\big(\mathrm{Lie}(G)\big) + \widetilde{F}^1\big(\mathrm{Lie}(G)\big) + p\,\mathrm{Lie}(G)\big) \xrightarrow{\sim} \widetilde{F}^{-1}\big(\mathrm{Lie}(G)\big)/p\widetilde{F}^{-1}\big(\mathrm{Lie}(G)\big)$$

are k-linearly independent. The possibility of making such choices is implied by the maximal property of $\mathcal{E}_i/\mathcal{E}_{i-1}$. By reasons of ranks we get $f - 1 \leqslant f_{-1}$. By induction on $j \in S(1, f)$ we get φ normalizes $\mathcal{E}_1 + p\mathcal{E}_2 + \cdots + p^{j-1}\mathcal{E}_j$. Taking $j = f$, we get that $E := \mathcal{E}_1 + p\mathcal{E}_2 + \cdots + p^{f-1}\mathcal{E}_f$ has a $W(k)$-basis formed by elements fixed by φ. Thus (E, φ) is a Dieudonné p-divisible object over k. As p^{f-1} annihilates $\mathrm{Lie}(G)/E$ we get $\mathbf{T}(\mathrm{Lie}(G), \varphi) \leqslant f - 1$. Thus (cf. 3.1.5 for the first inequality)

$$n \leqslant 2\mathbf{T}\big(\mathrm{Lie}(G), \varphi\big) + \varepsilon_p \leqslant 2(f-1) + \varepsilon_p \leqslant 2f_{-1} + \varepsilon_p.$$

Often 3.3.4 provides (respectively 3.3.2(b) and 3.3.7 applied with $G_1 = \mathbf{GL}_M$ provide) better upper bounds of n. For instance, if $G = \mathbf{GL}_M$ (respectively if $p \geqslant 3$ and $G = \mathbf{Sp}(M, \lambda_M)$ with λ_M as a principal quasi-polarization of (M, φ)) we get $n \leqslant \mathbf{T}(\mathrm{Lie}(G), \varphi) \leqslant f_{-1}$ (respectively $n \leqslant \mathbf{T}(\mathrm{Lie}(G), \varphi) + 1 \leqslant f_{-1} + 1$). If (M, φ) is the Dieudonné module of a supersingular p-divisible group over $\mathrm{Spec}(k)$ of height $2d$ and if $G = \mathbf{GL}_M$ (respectively and if $p \geqslant 3$ and $G = \mathbf{Sp}(M, \lambda_M)$), then f_{-1} is d^2 (respectively is $\frac{d^2+d}{2}$). Thus we have the following concrete application of 3.2.3 (respectively of 3.2.5):

4.1.1. PROPOSITION. – *Let $d \in \mathbf{N}$. If $p \geqslant 2$ (respectively if $p \geqslant 3$), then any (respectively any principally quasi-polarized) supersingular p-divisible group of height $r = 2d$ over $\mathrm{Spec}(k)$ is uniquely determined up to isomorphism by its truncated (respectively its principally quasi-polarized truncated) Barsotti–Tate group of level d^2 (respectively of level $\frac{d^2+d}{2} + 1$).*

4.2. Root decompositions

The image of μ is either trivial or a closed $\mathbf{G}_m$ subgroup of G and thus its centralizer in G is a reductive group scheme which has a maximal torus (cf. [6, vol. III, Exp. XIX, 2.8 and 6.1]). Thus there exists a maximal torus T of G through which μ factors. We have $\mathrm{Lie}(T) \subseteq \widetilde{F}^0(\mathrm{Lie}(G))$. It is easy to check that there exists $g \in G(W(k))$ such that $g\varphi$ normalizes $\mathrm{Lie}(T)$. Accordingly, for the next three examples (i.e. until Section 5) we will assume that we have $\varphi(\mathrm{Lie}(T)) = \mathrm{Lie}(T)$. Let

$$\mathrm{Lie}(G) = \mathrm{Lie}(T) \bigoplus_{\gamma \in \Phi} \mathfrak{g}_\gamma$$

be the root decomposition relative to T. So Φ is a root system of characters of T and each $\mathfrak{g}_\gamma$ is a free $W(k)$-module of rank 1 on which T acts via the character γ.

Let Δ be a basis of Φ such that $\bigoplus_{\gamma \in \Delta} \mathfrak{g}_\gamma \subseteq \bigoplus_{i=0}^{b_L} \widetilde{F}^i(\mathrm{Lie}(G))$. Let Φ^+ and Φ^- be the sets of positive and negative (respectively) roots of Φ with respect to Δ. Let C be the unique Borel subgroup scheme of G which contains T and for which we have $\mathrm{Lie}(C) = \mathrm{Lie}(T) \bigoplus_{\gamma \in \Phi^+} \mathfrak{g}_\gamma$, cf. [6, vol. III, Exp. XXII, 5.5.1]. As $\mathrm{Lie}(C)[\frac{1}{p}]$ is generated by the $B(k)$-vector subspace $\bigoplus_{\gamma \in \Delta} \mathfrak{g}_\gamma[\frac{1}{p}]$ of the Lie algebra $\bigoplus_{i=0}^{b_L} \widetilde{F}^i(\mathrm{Lie}(G))[\frac{1}{p}]$, we have an inclusion $\mathrm{Lie}(C) \subseteq \bigoplus_{i=0}^{b_L} \widetilde{F}^i(\mathrm{Lie}(G))$.

As μ factors through T, for any root $\gamma \in \Phi$ there exists an integer $n(\gamma) \in S(-b_L, b_L)$ such that we have $\mathfrak{g}_\gamma \subseteq \widetilde{F}^{n(\gamma)}(\mathrm{Lie}(G))$. As $\varphi = \sigma_0 \mu(p^{-1})$ and $\sigma_0(\mathrm{Lie}(T)) = \varphi(\mathrm{Lie}(T)) = \mathrm{Lie}(T)$, there exists a permutation Π of Φ such that we have

$$(21) \qquad \sigma_0(\mathfrak{g}_\gamma) = \mathfrak{g}_{\Pi(\gamma)} \quad \text{and} \quad \varphi(\mathfrak{g}_\gamma) = p^{n(\gamma)} \mathfrak{g}_{\Pi(\gamma)}, \quad \forall \gamma \in \Phi.$$

If $\gamma \in \Phi^+$ (respectively if $\gamma \in \Phi^-$), then $n(\gamma) \in S(0, b_L)$ (respectively then $n(\gamma) \in S(-b_L, 0)$); this is a consequence of the inclusion $\mathrm{Lie}(C) \subseteq \bigoplus_{i=0}^{b_L} \widetilde{F}^i(\mathrm{Lie}(G))$.

As $\mathrm{Lie}(T)$ is normalized by φ, it has a $W(k)$-basis formed by elements fixed by φ. Let $\Pi_0 := (\gamma_1, \ldots, \gamma_l)$ be a cycle of Π. For $j \in S(1, l)$ let $y_{\gamma_j} \in \mathfrak{g}_{\gamma_j} \setminus \{0\}$ be such that (cf. (21)) we have $\varphi(y_{\gamma_j}) = p^{m(\gamma_j)} y_{\gamma_{j+1}}$ (with $\gamma_{l+1} := \gamma_1$), where $m(\gamma_1), \ldots, m(\gamma_l)$ are integers that are either all positive or all negative. Let $\mathcal{B}_0 := \{y_{\gamma_1}, \ldots, y_{\gamma_l}\}$.

Let E be a $W(k)$-submodule of $\mathrm{Lie}(G)$ that contains $\mathrm{Lie}(T)$, that satisfies the identity $E[\frac{1}{p}] = \mathrm{Lie}(G)[\frac{1}{p}]$, and that is maximal subject to the property that it has a $W(k)$-basis $\mathcal{B}$ which is the union of a $\mathbf{Z}_p$-basis of $\{x \in \mathrm{Lie}(T) \mid \varphi(x) = x\}$ and of subsets $\mathcal{B}_0$ that are associated as above to some cycle Π_0 of Π. Let π be the permutation of $\mathcal{B}$ which fixes $\mathcal{B} \cap \mathrm{Lie}(T)$ and which for $\gamma \in \Phi$ takes the element of $\mathfrak{g}_\gamma \cap \mathcal{B}$ into the element of $\mathfrak{g}_{\Pi(\gamma)} \cap \mathcal{B}$.

4.3. Example 2

It is not difficult to check that there exists an element $g \in G(W(k))$ which normalizes T and which has the property that $g\varphi$ takes $\mathrm{Lie}(C)$ into $\mathrm{Lie}(C)$. Accordingly, in this section we assume that there exists a Borel subgroup $\widetilde{C}$ of G which contains T and which has the property that $\varphi(\mathrm{Lie}(\widetilde{C})) \subseteq \mathrm{Lie}(\widetilde{C})$. So if we have $\mathfrak{g}_\gamma \subseteq \mathrm{Lie}(\widetilde{C})$, then $n(\gamma) \geqslant 0$. Thus we have

$\mathrm{Lie}(\widetilde{C}) \subseteq \bigoplus_{i=0}^{b_L} \widetilde{F}^i(\mathrm{Lie}(G))$. Thus, not to introduce extra notations, we can assume that $C = \widetilde{C}$; so $\varphi(\mathrm{Lie}(C)) \subseteq \mathrm{Lie}(C)$.

The last inclusion implies that Π normalizes both Φ^+ and Φ^-. As we have $n(\gamma) \geqslant 0$ if $\gamma \in \Phi^+$ and $n(\gamma) \leqslant 0$ if $\gamma \in \Phi^-$, for any cycle $\Pi_0 = (\gamma_1, \ldots, \gamma_l)$ of Π we can choose the above elements $y_{\gamma_j} \in \mathfrak{g}_{\gamma_j}$ to be generators of $\mathfrak{g}_{\gamma_j}$. Thus, due to the maximal property of E, we have $E = \mathrm{Lie}(G)$ (i.e. for any $\gamma \in \Phi$ the intersection $\mathcal{B} \cap \mathfrak{g}_\gamma$ is a $W(k)$-basis of $\mathfrak{g}_\gamma$). Thus $\mathbf{T}(\mathrm{Lie}(G), \varphi) = 0$, i.e. $(\mathrm{Lie}(G), \varphi) = (E, \varphi)$ is a Dieudonné–Fontaine p-divisible object over k. We have $n \leqslant \varepsilon_p$, cf. 3.1.5. Thus $n \leqslant 1$ if $p \geqslant 3$ and $n \leqslant 2$ if $p = 2$.

4.3.1. PROPOSITION. – *We recall that G is a reductive group scheme, that T is a maximal torus of G through which $\mu : \mathbf{G}_m \to G$ factors and whose Lie algebra is normalized by φ, and that we have $\varphi(\mathrm{Lie}(C)) \subseteq \mathrm{Lie}(C)$ for some Borel subgroup scheme C of G that contains T. Then the i-number n of (M, φ, G) is at most 1.*

Proof. – We know that $n \leqslant 1$ if $p \geqslant 3$. Thus we can assume $p = 2$ (but as the below arguments work for all primes, we will keep the notation p instead of 2). Let $\Phi(0) := \Phi \cup \{0\}$, $n(0) := 0$, and $G(0) := T$. For $\gamma \in \Phi$ let $G(\gamma)$ be the unique $\mathbf{G}_a$ subgroup scheme of G that is normalized by T and such that $\mathrm{Lie}(G(\gamma)) = \mathfrak{g}_\gamma$, cf. [6, vol. III, Exp. XXII, 1.1]. If $x \in \mathfrak{g}_\gamma$ is such that $x^p \neq 0$, then the torus T acts on $\langle x^p \rangle$ via the p-th power of the character γ. The reduction $\bar{x}^p \bmod p$ of x^p belongs to $\mathfrak{g}_\gamma \bmod p$, cf. [1, Ch. II, 3.1, 3.5, Lemma 3 of 3.19]. From the last two sentences we get that $\bar{x}^p = 0$. This implies that for each $\gamma \in \Phi$ we have a bijection $\exp_\gamma : \mathfrak{g}_\gamma \xrightarrow{\sim} G(\gamma)(W(k))$ which maps $x \in \mathfrak{g}_\gamma$ into $\exp_\gamma(x) = \sum_{i=0}^\infty \frac{x^i}{i!}$ (we emphasize that $\mathfrak{g}_\gamma$ is not included in the domain of the exponential map of 2.6 defined for $O = M$).

Let $g_1 \in G(W(k))$ be congruent $\bmod\ p$ to 1_M. Let $l_1 \in \mathrm{Lie}(G)$ be such that g_1 is congruent $\bmod\ p^2$ to $1_M + pl_1$. We show that there exists $g \in G(W(k))$ congruent $\bmod\ p$ to 1_M and such that $gg_1\varphi g^{-1}\varphi^{-1} \in G(W(k))$ is congruent $\bmod\ p^2$ to 1_M.

We take g to be a product $\prod_{\gamma \in \Phi(0)} g_1^\gamma$ (taken in any order), where $g_1^\gamma \in G(\gamma)(W(k))$ is congruent $\bmod\ p^{1+\max\{0,-n(\gamma)\}}$ to 1_M. Let $l_1^0 \in \mathrm{Lie}(T)$ be such that $g_1^0 \in G(0)(W(k))$ is congruent $\bmod\ p^2$ to $1_M + pl_1^0$. The element $\varphi g_1^0 \varphi^{-1} = \sigma_0 g_1^0 \sigma_0^{-1} \in G(0)(B(k)) \cap \mathbf{GL}_M(W(k)) = G(0)(W(k))$ is congruent $\bmod\ p^2$ to $1_M + p\sigma_0(l_1^0)$. For $\gamma \in \Phi$ let $x_1^\gamma \in p^{1+\max\{0,-n(\gamma)\}}\mathfrak{g}_\gamma$ and $l_1^\gamma \in \mathfrak{g}_\gamma$ be such that $g_1^\gamma = \exp_\gamma(x_1^\gamma)$ is congruent $\bmod\ p^{2+\max\{0,-n(\gamma)\}}$ to $1_M + p^{1+\max\{0,-n(\gamma)\}}l_1^\gamma$, cf. 2.6.1 and 2.6.2. Based on (21) we have

$$\varphi g_1^\gamma \varphi^{-1} = \exp_{\Pi(\gamma)}\big(p^{1+\max\{0,n(\gamma)\}}\sigma_0(x_1^\gamma)\big) \in G\big(\Pi(\gamma)\big)\big(W(k)\big).$$

So if $n(\gamma) > 0$ (respectively if $n(\gamma) \leqslant 0$), then from 2.6(b) (respectively from the very definition of l_1^γ) we get that $\varphi g_1^\gamma \varphi^{-1} = \exp_{\Pi(\gamma)}(p^{1+\max\{0,n(\gamma)\}}\sigma_0(x_1^\gamma))$ is congruent $\bmod\ p^2$ to 1_M (respectively to $1_M + p\sigma_0(l_1^\gamma)$). Thus by replacing g_1 with the following product

$$gg_1\varphi g^{-1}\varphi^{-1} = \bigg(\prod_{\gamma \in \Phi(0)} g_1^\gamma\bigg)g_1\bigg(\prod_{\gamma \in \Phi(0)} \varphi g_1^\gamma \varphi^{-1}\bigg)^{-1} \in G\big(W(k)\big)$$

of elements congruent $\bmod\ p$ to 1_M, the role of l_1 gets replaced by the one of

$$\tilde{l}_1 := l_1 + \sum_{\gamma \in \Phi, n(\gamma) > 0} l_1^\gamma + \sum_{\gamma \in \Phi(0), n(\gamma) = 0} \big[l_1^\gamma - \sigma_0(l_1^\gamma)\big] + \sum_{\gamma \in \Phi, n(\gamma) < 0} -\sigma_0(l_1^\gamma).$$

By writing all elements defining $\tilde{l}_1$ as linear combinations of elements of the $W(k)$-basis $\mathcal{B}$ of $E = \mathrm{Lie}(G)$, as in the part of 3.1.1 that involves (+) and (−) we argue that we can choose the

l_1^γ's and so also the g_1^γ's, such that we have $\tilde{l}_1 \in p\,\mathrm{Lie}(G)$; here $\gamma \in \Phi(0)$. Thus $gg_1\varphi g^{-1}\varphi^{-1}$ is congruent mod p^2 to 1_M. So if $n = 2$, then the i-number of (M, φ, G) is at most 1 and this contradicts the definition of n. As $n \leqslant 2$, we get $n \leqslant 1$. $\square$

4.3.2. PROPOSITION. – *We continue to work under the hypotheses of* 4.3.1. *Let* $E_0 := \{e \in \mathrm{Lie}(G) \mid \varphi(e) = e\}$. *We have*:
  (a) *The cocharacter* $\mu : \mathbf{G}_m \to G$ *is the unique Hodge cocharacter of* (M, φ, G) *that centralizes* E_0.
  (b) *The lift* $(F^i(M))_{i \in S(a,b)}$ *is the unique lift of* (M, φ, G) *such that for any* $e \in E_0$ *and every* $i \in S(a,b)$ *we have* $e(F^i(M)) \subseteq F^i(M)$.

Proof. – As $\varphi = \sigma_0\mu(p^{-1})$, we have $n(\gamma) = 0$ if and only if $\mathfrak{g}_\gamma \subseteq \widetilde{F}^0(\mathrm{Lie}(G))$. So as Π normalizes Φ^+ and Φ^- and as $n(\gamma) \geqslant 0$ (respectively $n(\gamma) \leqslant 0$) if $\gamma \in \Phi^+$ (respectively if $\gamma \in \Phi^-$), we easily get that $E_0 \subseteq \widetilde{F}^0(\mathrm{Lie}(G))$. Thus μ centralizes E_0 and for $e \in E_0$ we have $e(\widetilde{F}^i(M)) \subseteq \widetilde{F}^i(M)$ for all $i \in S(a,b)$; thus $e(F^i(M)) \subseteq F^i(M)$ for all $i \in S(a,b)$.

Let μ_1 be another Hodge cocharacter of (M, φ, G) that centralizes E_0. As $\varphi(\mathrm{Lie}(T)) = \mathrm{Lie}(T)$, $\mathrm{Lie}(T)$ is $W(k)$-generated by elements of $E_0 \cap \mathrm{Lie}(T)$. Thus μ_1 centralizes $\mathrm{Lie}(T)$ and therefore it factors through T. So μ and μ_1 commute. So to show that $\mu = \mu_1$ it is enough to show that $\mu_k = \mu_{1k}$. As $\varphi^{-1}(M) = (\sigma_0\mu(p^{-1}))^{-1}(M) = \bigoplus_{i=a}^b p^{-i}\widetilde{F}^i(M)$, for $i \in S(a,b)$ we have $((p^{-i}\varphi)^{-1}(M)) \cap M = \sum_{t=0}^{i-a} p^t F^{i-t}(M)$. This identity implies that the filtration $(F^i(M)/pF^i(M))_{i \in S(a,b)}$ of M/pM is uniquely determined by (M, φ). Thus both cocharacters μ_k and μ_{1k} act on $F^i(M)/F^{i+1}(M) + pF^i(M) \xrightarrow{\sim} \widetilde{F}^i(M)/p\widetilde{F}^i(M)$ via the $-i$-th power of the identity character of $\mathbf{G}_m$. So as μ_k and μ_{1k} commute, by decreasing induction on $i \in S(a,b)$ we get that $\widetilde{F}^i(M)/p\widetilde{F}^i(M)$ is the maximal k-vector subspace of M/pM on which both μ_k and μ_{1k} act via the $-i$-th power of the identity character of $\mathbf{G}_m$. This implies $\mu_k = \mu_{1k}$. Thus $\mu = \mu_1$. So (a) holds.

Let $(F_1^i(M))_{i \in S(a,b)}$ be another lift of (M, φ, G) such that for any $e \in E_0$ and $i \in S(a,b)$, we have $e(F_1^i(M)) \subseteq F_1^i(M)$. The inverse of the canonical split cocharacter of $(M, (F_1^i(M))_{i \in S(a,b)}, \varphi)$ fixes all elements of E_0 (cf. the functorial aspects of [42, p. 513]), factors through G (cf. 2.5), and thus it is μ (cf. (a)). Thus for $i \in S(a,b)$ we have $F^i(M) = \bigoplus_{j=i}^b \widetilde{F}^j(M) = F_1^i(M)$. So (b) holds. $\square$

If $g \in G(W(k))$, then the Newton polygon of $(M, g\varphi)$ is above the Newton polygon of (M, φ) (cf. [37, Thm. 4.2]). Thus Proposition 4.3.1 generalizes the well known fact that an ordinary p-divisible group D over $\mathrm{Spec}(k)$ is uniquely determined up to isomorphism by $D[p]$. Proposition 4.3.2 generalizes the well known fact that the canonical lift of D is the unique lift of D to $\mathrm{Spec}(W(k))$ with the property that any endomorphism of D lifts to it. The last two sentences motivate the next definition.

4.3.3. DEFINITION. – *We refer to* (M, φ, G) *of* 4.3.1 *as an* ordinary p-divisible object with a reductive group *over* k *and to either* $(F^i(M))_{i \in S(a,b)}$ *or* $(M, (F^i(M))_{i \in S(a,b)}, \varphi, G)$ *as the* canonical lift *of* (M, φ, G).

4.4. Example 3

Let $c \in \mathbf{N}$. We assume that $b_L = 1$ and that there exists a direct sum decomposition $M = \bigoplus_{i=1}^c M_i$ in $W(k)$-modules of rank 2 such that $G = \prod_{i=1}^c \mathbf{GL}_{M_i}$ and we have $\varphi(M_i[\frac{1}{p}]) = M_{i+1}[\frac{1}{p}]$ for $i \in S(1,c)$, where $M_{c+1} := M_1$. We have $r_M = 2c$. As $b_L = 1$ and $G \xrightarrow{\sim} \mathbf{GL}_2^c$, we have $f_{-1} \in S(1,c)$. For $i \in S(1,c)$ we have $\varphi(\mathrm{End}(M_i)[\frac{1}{p}]) = \mathrm{End}(M_{i+1})[\frac{1}{p}]$. Thus the permutation π of $\mathcal{B}$ has at most two cycles formed by elements of $\mathcal{B} \setminus \mathrm{Lie}(T)$ (equivalently the

permutation Π of Φ has at most two cycles). If we have one such cycle, then its length is $2c$. If we have two such cycles, then their length is c.

Let $\varepsilon \in \{1, 2\}$. Let $l = \varepsilon c$ be such that we have a cycle $(y_1, \ldots, y_l)$ of π formed by elements of $\mathcal{B} \setminus \mathrm{Lie}(T)$. For $i \in S(1, l)$ let $s_i \in \mathbf{N} \cup \{0\}$ be such that $e_i := p^{-s_i} y_i$ generates $\mathfrak{g}_{\gamma_i}$ for some $\gamma_i \in \Phi$. Let $(n_1, \ldots, n_l) := (n(\gamma_1), \ldots, n(\gamma_l)) \in \mathbf{Z}^l$; we have $\varphi(e_i) = p^{n_i} e_{i+1}$ (cf. (21)). As $b_L = 1$, for $i \in S(1, l)$ we have $n_i \in \{-1, 0, 1\}$. The number n_+ (respectively n_-) of those $i \in S(1, l)$ such that $n_i = 1$ (respectively $n_i = -1$), is at most f_{-1}. Moreover $n_+ + n_- = \varepsilon f_{-1} \leqslant \varepsilon c = l$. Thus $n_0 := \min\{n_+, n_-\} \leqslant \frac{\varepsilon}{2} f_{-1}$.

We have $\mathbf{T}(\langle e_1, \ldots, e_l \rangle, \varphi) \leqslant n_0$ and there exist numbers $a_i \in S(0, n_0)$ such that $(\langle p^{a_1} e_1, \ldots, p^{a_l} e_l \rangle, \varphi)$ is a Dieudonné–Fontaine p-divisible object over k, cf. (3) and the proof of (2). Based on the maximal property of E, we can assume $\langle p^{a_1} e_1, \ldots, p^{a_l} e_l \rangle \subseteq \langle y_1, \ldots, y_l \rangle$ (i.e. $s_i \leqslant a_i$ for all $i \in S(1, l)$). If $l = c$, then the set $\{n_+, n_-\}$ (and so also n_0) does not depend on the choice of the cycle $(y_1, \ldots, y_l)$. Thus we can choose E such that $p^{n_0} \mathrm{Lie}(G) \subseteq E$. So any element of $G(W(k))$ congruent mod p^{n_0+1} to 1_M belongs to $1_M + pE$. As $\mathrm{Lie}(T) \subseteq E$, E is a $W(k)$-subalgebra of $\prod_{i=1}^c \mathrm{End}(M_i)$ and so also of $\mathrm{End}(M)$. Thus (cf. 3.3.2(b) applied with $G = G_1$ and with $m_1 \in S(0, n_0)$) we have

$$n \leqslant n_0 + 1 = \min\{n_+, n_-\} + 1 \leqslant \frac{\varepsilon}{2} f_{-1} + 1 \leqslant c + 1.$$

4.5. Example 4

Let $d \in \mathbf{N} \setminus \{1, 2\}$. Let D be a p-divisible group over $\mathrm{Spec}(k)$ of height $r = 2d$, dimension d, and slopes $\frac{1}{d}$ and $\frac{d-1}{d}$. Let (M, φ_0) be the Dieudonné module of D; we have $r_M = r$. It is easy to see that we have a short exact sequence

$$0 \to D_2 \to D \to D_1 \to 0$$

of p-divisible groups over $\mathrm{Spec}(k)$, where the slopes of D_1 and D_2 are $\frac{d-1}{d}$ and $\frac{1}{d}$ (respectively). This short exact sequence is different from the classical slope filtration of D (see [41, §3]) which is a short exact sequence $0 \to D_1 \to D \to D_2 \to 0$. As D_1 and D_2 are uniquely determined up to isomorphisms (see [5, Ch. IV, §8]), there exist a $W(k)$-basis $\{e_1, \ldots, e_r\}$ of M and elements $x_1, \ldots, x_d \in \langle e_1, \ldots, e_d \rangle$ such that φ_0 takes the r-tuple $(e_1, \ldots, e_r)$ into $(e_2, pe_3, \ldots, pe_d, pe_1, e_{d+2} + x_2, \ldots, e_r + x_d, pe_{d+1} + px_1)$. Let

$$M_1 := \langle e_1, \ldots, e_d \rangle \quad \text{and} \quad M_2 := \langle e_{d+1}, \ldots, e_r \rangle.$$

The pairs (M_1, φ_0) and $(M/M_1, \varphi_0)$ are the Dieudonné modules of D_1 and D_2 (respectively). Let φ be the σ-linear endomorphism of M that takes $(e_1, \ldots, e_r)$ into $(e_2, pe_3, \ldots, pe_d, pe_1, e_{d+2}, \ldots, e_r, pe_{d+1})$. Let $G := \mathbf{GL}_M$.

Let P_1 and P_2 be the maximal parabolic subgroup schemes of G that normalize M_1 and M_2 (respectively). Let U_1 and U_2 be the unipotent radicals of P_1 and P_2 (respectively). Let $u_0 \in U_1(W(k))$ be the unique element such that $\varphi_0 = u_0 \varphi$. As T we take the maximal torus of G that normalizes $\langle e_i \rangle$ for all $i \in S(1, r)$. Let $L_1 = \mathbf{GL}_{M_1} \times_{\mathrm{Spec}(W(k))} \mathbf{GL}_{M_2}$ be the unique Levi subgroup scheme of either P_1 or P_2 such that $T \leqslant L_1$, cf. [6, vol. III, Exp. XXVI, 1.12(ii)]. We have natural identifications $\mathrm{Lie}(L_1) = \mathrm{End}(M_1) \oplus \mathrm{End}(M_2)$, $\mathrm{Lie}(U_1) = \mathrm{Hom}(M_2, M_1)$, and $\mathrm{Lie}(U_2) = \mathrm{Hom}(M_1, M_2)$. The triples (M, φ_0, P_1) and (M, φ_0, U_1) are latticed F-isocrystals with a group over k.

As U_1 is commutative we have $(\mathrm{Lie}(U_1), \varphi) = (\mathrm{Lie}(U_1), \varphi_0)$. We easily get that $\mathrm{Lie}(U_1)$ has a $W(k)$-basis $\{e_i^{(j)} \mid 1 \leqslant i, j \leqslant d\}$ such that $\varphi_0(e_i^{(j)}) = p^{n_i^{(j)}} e_{i+1}^{(j)}$, where each d-tuple

$(n_1^{(j)}, n_2^{(j)}, \ldots, n_d^{(j)})$ is either $(1, 1, \ldots, 1, 1, -1)$ or some d-tuple of the form $(1, 1, \ldots, 1, 0, 1, \ldots, 1, 0)$. As $\mathbf{S}(1, 1, \ldots, 1, -1) = 1$ and $\mathbf{S}(1, 1, \ldots, 1, 0, 1, \ldots, 1, 0) = 0$, from (2) applied to all pairs $(\langle e_1^{(j)}, \ldots, e_d^{(j)}\rangle, \varphi)$ we get $\mathbf{T}(\mathrm{Lie}(U_1), \varphi_0) \leqslant 1$. As $\mathrm{Lie}(U_1)$ is a $W(k)$-submodule of $\mathrm{End}(M)$ whose product with itself is the zero $W(k)$-submodule, the i-numbers of (M, φ_0, U_1) and (M, φ, U_1) are at most 1 (cf. 3.3.3). A similar argument shows that both $\mathbf{T}(\mathrm{Lie}(U_2), \varphi)$ and the i-number of (M, φ, U_2) are at most 1.

4.5.1. PROPOSITION. – *The p-divisible group D is uniquely determined up to isomorphism by $D[p^3]$.*

Proof. – Let $t \in \mathbf{N} \setminus \{1\}$. Let $g_t \in G$ be congruent mod p^t to 1_M. We will show that if $t \geqslant 3$, then there exists $g \in G(W(k))$ such that $gg_t\varphi_0 g^{-1}\varphi_0^{-1} \in G(W(k))$ is congruent mod p^{t+1} to 1_M. The product morphism $U_2 \times_{\mathrm{Spec}(W(k))} L_1 \times_{\mathrm{Spec}(W(k))} U_1 \to G$ is an open embedding around the identity section, cf. [6, vol. III, Exp. XXII, 4.1.2]. Thus we can write $g_t = u_2 l_1 u_1$, where the elements $u_1 \in U_1(W(k))$, $l_1 \in L_1(W(k))$, and $u_2 \in U_2(W(k))$ are all congruent mod p^t to 1_M. As the i-number of (M, φ_0, U_1) is at most 1, to show the existence of g we can replace u_0 by any other element of $U_1(W(k))$ that is congruent mod p to u_0. Thus we can assume $u_1 = 1_M$.

For $i \in \{1, 2\}$ let E_i be the $W(k)$-span of the $\mathbf{Z}_p$-algebra of endomorphisms of (M_i, φ). Let $E := E_1 \oplus E_2$. We have $p\,\mathrm{Lie}(L_1) \subseteq E$ (cf. 3.3.6 applied to both D_1 and D_2) and thus $l_1 \in L_1(W(k)) \cap (1_M + p^{t-1}E)$. There exists $\tilde{l}_1 \in L_1(W(k))$ congruent mod p^{t-1} to 1_M and such that $\tilde{l}_1 l_1 \varphi \tilde{l}_1^{-1} = \varphi$, cf. 3.3.2(a) applied with $j = t - 1$ to (M, φ, L_1) and E. So, as L_1 normalizes both U_1 and U_2, by replacing $g_t\varphi_0$ with $\tilde{l}_1 g_t \varphi_0 \tilde{l}_1^{-1}$, u_2 with $\tilde{l}_1 u_2 \tilde{l}_1^{-1}$, and u_0 with the element $\tilde{l}_1 l_1 u_0 l_1^{-1} \tilde{l}_1^{-1} \in U_1(W(k))$ congruent mod p^{t-1} to u_0, we can assume l_1 is congruent mod p^{t+1} to 1_M. This implies that g_t and u_2 are congruent mod p^{t+1}.

As $\mathbf{T}(\mathrm{Lie}(U_2), \varphi) \leqslant 1$, from 3.3.2(a) applied in a way similar to the one of the previous paragraph we deduce the existence of $\tilde{u}_2 \in U_2(W(k))$ congruent mod p^{t-1} to 1_M and such that $\tilde{u}_2 u_2 \varphi \tilde{u}_2^{-1} = \varphi$. As g_t and u_2 are congruent mod p^{t+1}, the element

$$g_t' := \tilde{u}_2 g_t \varphi_0 \tilde{u}_2^{-1}\varphi_0^{-1} = \tilde{u}_2 g_t u_0 \varphi \tilde{u}_2^{-1}\varphi^{-1}u_0^{-1} = \tilde{u}_2 g_t u_0 u_2^{-1} \tilde{u}_2^{-1} u_0^{-1} \in G(W(k))$$

is congruent mod p^{t+1} to the commutator of $\tilde{u}_2 u_2$ and u_0. A simple matrix computation of this commutator shows that for $t \geqslant 3$ we can write $g_t' = u_2' l_2' u_1'$, where $u_1' \in U_1(W(k))$ and $l_1' \in L_1(W(k))$ are congruent mod p^{t-1} to 1_M and where $u_2' \in U_2(W(k))$ is congruent mod p^{2t-2} and so also mod p^{t+1} to 1_M (here is the only place where we need $t \neq 2$).

Repeating twice the above part that allowed us to assume that u_1 and l_1 are congruent mod p^{t+1} to 1_M, we get that for $t \geqslant 3$ we can assume g_t' is congruent mod p^{t+1} to u_2' and thus also to 1_M. This ends the argument for the existence of g.

Thus for $t \geqslant 3$ we have $t + 1 \neq n$; so $n \leqslant 3$. So the proposition follows from 3.2.3. $\square$

4.5.2. Notations for $d = 3$

Let d be 3. For $\alpha \in W(k)$ let φ_α be the σ-linear endomorphism of M that takes $(e_1, \ldots, e_6)$ into $(e_2, pe_3, pe_1, e_5, e_6 + \alpha e_1, pe_4)$. The slopes of (M, φ_α) are $\frac{1}{3}$ and $\frac{2}{3}$. For $(i, j) \in \{1, 2, 3\} \times \{4, 5, 6\}$ let U_{ij} be the unique $\mathbf{G}_a$ subgroup scheme of U_1 that is normalized by T, that fixes $e_{j'}$ for $j' \in \{4, 5, 6\} \setminus \{j\}$, and that takes e_j into $e_j + \langle e_i \rangle$. Let $n_\alpha \in U_{16}(W(k))$ be the unique element such that $\varphi_\alpha = n_\alpha \varphi$.

4.5.3. PROPOSITION. – *Suppose $d = 3$. Let $\alpha_1, \alpha_2 \in W(k) \setminus \{0\}$ be such that the $\mathbf{F}_{p^3}$-vector subspace of k generated by α_1 mod p is different from the $\mathbf{F}_{p^3}$-vector subspace of k generated by α_2 mod p. Then (M, φ_{α_1}) and (M, φ_{α_2}) are not isomorphic.*

Proof. – We show that the assumption that there exists $g_1 \in G(W(k))$ which is an isomorphism between (M, φ_{α_1}) and (M, φ_{α_2}) leads to a contradiction. As $\mathrm{Lie}(P_1)[\frac{1}{p}]$ is the maximal direct summand of $\mathrm{End}(M[\frac{1}{p}])$ normalized by φ_α and such that all slopes of $(\mathrm{Lie}(P_1)[\frac{1}{p}], \varphi_\alpha)$ are non-negative, the element $g_1 \in G(W(k))$ normalizes $\mathrm{Lie}(P_1)$ and so also P_1. Thus $g_1 \in P_1(W(k))$. We write $g_1 = u_1 l_1$, where $u_1 \in U_1(W(k))$ and $l_1 \in L_1(W(k))$. We have $u_1 l_1 n_{\alpha_1} l_1^{-1} l_1 \varphi = n_{\alpha_2} \varphi u_1 \varphi^{-1} \varphi l_1$. As $u_1 l_1 n_{\alpha_1} l_1^{-1}$ and $n_{\alpha_2} \varphi u_1 \varphi^{-1}$ belong to $U_1(W(k))$, the actions of $l_1 \varphi$ and φl_1 on both M_1 and M/M_1 are equal. So as $l_1 \varphi$ and φl_1 both normalize the direct supplement $M_2[\frac{1}{p}]$ of $M_1[\frac{1}{p}]$ in $M[\frac{1}{p}]$, we get $l_1 \varphi = \varphi l_1$; so we also have $u_1 l_1 n_{\alpha_1} l_1^{-1} = n_{\alpha_2} \varphi u_1 \varphi^{-1}$. As $l_1 \varphi = \varphi l_1$, a simple computation shows that l_1 takes e_1 (respectively e_6) into $a_1 e_1 + b_1 e_2 + c_1 e_3$ (respectively $pa_6 e_4 + pb_6 e_5 + c_6 e_6$), where $a_1, b_1, c_1 \in W(\mathbf{F}_{p^3})$ (respectively a_6, $b_6 \in W(\mathbf{F}_{p^3})$ and $c_6 \in \mathbf{G}_m(W(\mathbf{F}_{p^3}))$). As $U_1 = \prod_{i=1}^3 \prod_{j=4}^6 U_{ij}$, there exist unique elements $u_{ij} \in U_{ij}(W(k))$ such that we have $u_1 = \prod_{i=1}^3 \prod_{j=4}^6 u_{ij}$. We call u_{ij} as the component of u_1 in $U_{ij}(W(k))$. Both $g_1 \bmod p$ and $l_1 \bmod p$ normalize the kernel of φ_α's mod p, i.e. they normalize $\langle e_2, e_3, e_6 \rangle \bmod p$. So $u_1 \bmod p$ also normalizes $\langle e_2, e_3, e_6 \rangle \bmod p$. If $(i, j) \neq (1, 6)$, then $u_{ij} \bmod p$ normalizes $\langle e_2, e_3, e_6 \rangle \bmod p$. Thus $u_{16} \bmod p$ normalizes $\langle e_2, e_3, e_6 \rangle \bmod p$ and therefore it is $1_{M/pM}$. As U_{35} fixes both $\langle e_2, e_3, e_6 \rangle$ and $M/\langle e_2, e_3, e_6 \rangle$, $\varphi(u_{35}) \bmod p$ is $1_{M/pM}$. Thus the component of $n_{\alpha_2} \varphi u_1 \varphi^{-1}$ in $U_{16}(W(k))$ is congruent mod p to n_{α_2}. The component of $l_1 n_{\alpha_1} l_1^{-1}$ in $U_{16}(W(k))$ is n_{α_3}, where $\alpha_3 := a_1 \alpha_1 c_6^{-1} \in W(k)$. So $\alpha_3 \bmod p$ belongs to the $\mathbf{F}_{p^3}$-vector subspace of k generated by $\alpha_1 \bmod p$. The component of $u_1 l_1 n_{\alpha_1} l_1^{-1}$ in $U_{16}(W(k))$ is congruent mod p to n_{α_3}. As $u_1 l_1 n_{\alpha_1} l_1^{-1} = n_{\alpha_2} \varphi u_1 \varphi^{-1}$, we get that n_{α_2} and n_{α_3} are congruent mod p. So $\alpha_2 \bmod p$ belongs to the $\mathbf{F}_{p^3}$-vector subspace of k generated by $\alpha_1 \bmod p$. This contradicts our hypothesis. Thus g_1 does not exist. $\square$

4.5.4. *Remark.* – The set of isomorphism classes of p-divisible groups over $\mathrm{Spec}(k)$ of height 6 and dimension 3 has the same cardinality as k, cf. 4.5.3, 1.3, and the classical Dieudonné theory. But the set of isomorphism classes of p-torsion subgroup schemes of such p-divisible groups over $\mathrm{Spec}(k)$ is finite (see [26]; to be compared with [34, §1]). Based on this, 4.5.1, and 3.2.3, we get that the set of those elements $\alpha \in \mathbf{G}_m(W(k))$ for which the i-number of (M, φ_α) is either 2 or 3, has the same cardinality as k. Let λ_M be the perfect alternating form on M defined by the rule: if $1 \leqslant i < j \leqslant 6$, then $\lambda_M(e_i, e_j) \in \{0, 1\}$ and we have $\lambda_M(e_i, e_j) = 1$ if and only if $(i, j) \in \{(1, 6), (3, 5), (2, 4)\}$. The form λ_M is a principal quasi-polarization of any (M, φ_α).

From 4.1.1 and 4.5.1 we easily get that $T(6, 3) \leqslant 9$.

5. Four direct applications

In this section we continue to assume that $k = \bar{k}$.

5.1. The homomorphism form of 1.2

Let (M_1, φ_1) and (M_2, φ_2) be two F-crystals over k. Let $(M, \varphi) := (M_1, \varphi_1) \oplus (M_2, \varphi_2)$. For $i \in \{1, 2\}$, let h_i be the h-number of (M_i, φ_i). Let $h_{12} := \max\{h_1, h_2\}$, let $m_{12} := \mathbf{T}(\mathrm{End}(M), \varphi)$, let $v_{12} := m_{12} + h_{12}$, let $\varepsilon_p \in \{1, 2\}$ be as before 3.1, and let $n_{12} := m_{12} + \varepsilon_p$. The h-number of (M, φ) is h_{12}.

5.1.1. THEOREM. – *We endow $(\mathbf{N} \cup \{0\})^2$ with the lexicographic order. We have*:
(a) *For all $t \in \mathbf{N} \cup \{0\}$, the images defined via restrictions of the two groups* $\mathrm{Hom}((M_1, \varphi_1), (M_2, \varphi_2))$ *and* $\mathrm{Hom}((M_1/p^{n_{12}+v_{12}+t}M_1, \varphi_1), (M_2/p^{n_{12}+v_{12}+t}M_2, \varphi_2))$ *in the group* $\mathrm{Hom}((M_1/p^{n_{12}+t}M_1, \varphi_1), (M_2/p^{n_{12}+t}M_2, \varphi_2))$, *coincide.*

(b) *We fix a quadruple $(r_1, r_2, c_1, c_2) \in (\mathbf{N} \cup \{0\})^4$. There exists a smallest pair*

$$(v, n) := \big(v(r_1, r_2, c_1, c_2), n(r_1, r_2, c_1, c_2)\big) \in \big(\mathbf{N} \cup \{0\}\big)^2$$

with the properties that $n \in S(0, v + \varepsilon_p - \max\{c_1, c_2\})$ and that for any $t \in \mathbf{N} \cup \{0\}$ and for every two F-crystals (M_1, φ_1) and (M_2, φ_2) over k which satisfy $(r_{M_1}, r_{M_2}, h_1, h_2) = (r_1, r_2, c_1, c_2)$, the images defined via restrictions of the two groups $\mathrm{Hom}((M_1, \varphi_1), (M_2, \varphi_2))$ and $\mathrm{Hom}((M_1/p^{n+v+t}M_1, \varphi_1), (M_2/p^{n+v+t}M_2, \varphi_2))$ in the group $\mathrm{Hom}((M_1/p^{n+t}M_1, \varphi_1), (M_2/p^{n+t}M_2, \varphi_2))$, coincide. The number v (and so also n) has upper bounds that depend only on r_1, r_2, and $\max\{c_1, c_2\}$.

(c) *Let r_1, $r_2 \in \mathbf{N}$. There exists a smallest pair*

$$(v, n) := \big(v(r_1, r_2), n(r_1, r_2)\big) \in \big(\mathbf{N} \cup \{0\}\big)^2$$

with the properties that $n \in S(0, v + \varepsilon_p - 1)$ and that for any $t \in \mathbf{N} \cup \{0\}$ and for every two p-divisible groups D_1 and D_2 over $\mathrm{Spec}(k)$ of heights r_1 and r_2, a homomorphism $D_1[p^{n+t}] \to D_2[p^{n+t}]$ lifts to a homomorphism $D_1 \to D_2$ if and only if it lifts to a homomorphism $D_1[p^{n+v+t}] \to D_2[p^{n+v+t}]$. The number v (and so also n) has upper bounds that depend only on r_1 and r_2.

Proof. – Let $e_{12} \in \mathrm{Hom}((M_1/p^{n_{12}+v_{12}+t}M_1, \varphi_1), (M_2/p^{n_{12}+v_{12}+t}M_2, \varphi_2))$. Let $g \in \mathrm{Aut}(M/p^{n_{12}+v_{12}+t}M, \varphi)$ be such that it takes $x_2 \in M_2/p^{n_{12}+v_{12}+t}M_2$ into x_2 and it takes $x_1 \in M_1/p^{n_{12}+v_{12}+t}M_1$ into $x_1 + e_{12}(x_1)$. Let $\tilde{g} \in \mathrm{Aut}(M, \varphi)$ be such that it lifts the reduction mod $p^{n_{12}+t}$ of g, cf. 3.2.8(b). Let $\tilde{e}_{12} : M_1 \to M_2$ be the $W(k)$-linear map such that we have $\tilde{g}(x_1) - \tilde{e}_{12}(x_1) \in M_1$ for all $x_1 \in M_1$. We have $\tilde{e}_{12} \in \mathrm{Hom}((M_1, \varphi_1), (M_2, \varphi_2))$ and moreover e_{12} and $\tilde{e}_{12}$ have the same image in $\mathrm{Hom}((M_1/p^{n_{12}+t}M_1, \varphi_1), (M_2/p^{n_{12}+t}M_2, \varphi_2))$. This proves (a).

We know that m_{12} has an upper bound $b_{12} \in \mathbf{N}$ which is effectively computable in terms of $2h_{12} = 2\max\{c_1, c_2\}$ and $r_M^2 = (r_{M_1} + r_{M_2})^2 = (r_1 + r_2)^2$ (cf. 2.4.1 and end of 2.2.1(e)) and that we have $v \leqslant m_{12} + h_{12}$ (cf. (a)). From this (b) follows.

To prove (c), for $i \in \{1, 2\}$ we take (M_i, φ_i) to be the Dieudonné module of D_i. We have $h_{12} \in \{0, 1\}$. If $h_{12} = 0$, then $h_1 = h_2 = 0$ and so both D_1 and D_2 are étale p-divisible groups; in such a case any homomorphism $D_1[p^{n+t}] \to D_2[p^{n+t}]$ lifts to a homomorphism $D_1 \to D_2$. Thus we can assume that $h_{12} = 1$. Based on 3.2.3, the proofs of (a) and (b) can be adapted to the context of p-divisible groups; thus (c) follows from the particular case of (b) when $\max\{c_1, c_2\}$ is $h_{12} = 1$. $\square$

5.1.2. Remark. – If $v_1, n_1 \in \mathbf{N}$ are such that $v_1 \geqslant v$ and $n_1 \geqslant n$, then the homomorphisms parts of 5.1.1(b) and (c) continue to hold if we replace (v, n) with (v_1, n_1).

5.2. Transcendental degrees of definition

For simplicity, in this section we work in a context without principal bilinear quasi-polarizations (but we emphasize that all of 5.2 can be adapted to the context of 2.2.1(c)). Let $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ be a latticed F-isocrystal with a group and an emphasized family of tensors over k such that the W-condition holds for (M, φ, G). Let $(F^i(M))_{i \in S(a,b)}$ be a lift of (M, φ, G).

Let $\mu := \mu_{\mathrm{can}} : \mathbf{G}_m \to G$ be the inverse of the canonical split cocharacter of $(M, (F^i(M))_{i \in S(a,b)}, \varphi)$ (see 2.5). Let $(M_{\mathbf{Z}_p}, G_{\mathbf{Z}_p})$ be the $\mathbf{Z}_p$ structure of (M, G) that is defined as in 2.5 by the σ-linear automorphism $\sigma_0 := \varphi\mu(p) : M \xrightarrow{\sim} M$; thus σ_0 fixes $M_{\mathbf{Z}_p}$ and

normalizes $G(W(k))$ and moreover we have $t_\alpha \in \mathcal{T}(M_{\mathbf{Z}_p})$ for all $\alpha \in \mathcal{J}$. Let $n \in \mathbf{N} \cup \{0\}$ be the i-number of (M, φ, G).

5.2.1. FACT. – *Let k_1 be the smallest subfield of k with the property that $\mu_{W_n(k)}$ is the pullback of a cocharacter $\mu_{1W_n(k_1)} \colon \mathbf{G}_m \to G_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(W_n(k_1))$. Then the field k_1 is finitely generated and its transcendental degree $t(k_1)$ is at most $n r_M^2$. Thus if $t(k_1) = 0$, then k_1 is a finite field.*

Proof. – Let $\mathcal{B}$ be a $W(k)$-basis of M such that μ normalizes the $W(k)$-spans of elements of $\mathcal{B}$. Let $\mathcal{B}_1$ be a $\mathbf{Z}_p$-basis of $M_{\mathbf{Z}_p}$; we also view it as a $W(k)$-basis of M. Let $B \in M_{r_M \times r_M}(W(k))$ be the change of coordinates matrix that changes $\mathcal{B}_1$-coordinates into $\mathcal{B}$-coordinates. Let R_1 be the $\mathbf{F}_p$-subalgebra of k generated by the coordinates of the Witt vectors of length n with coefficients in k that are entries of B mod p^n. Obviously k_1 is a subfield of the field of fractions of R_1. As R_1 is generated by $n r_M^2$ elements, k_1 is finitely generated and we have $\dim(\mathrm{Spec}(R_1)) \leqslant n r_M^2$. Thus $t(k_1) \leqslant n r_M^2$. $\square$

Until 5.3 we take G to be smooth over $\mathrm{Spec}(W(k))$. Thus for any $l \in \mathbf{N}$ there exists a cocharacter $\mu_{1,n+l}$ of $G_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(W_{n+l}(k_1^{\mathrm{perf}}))$ that lifts the pullback $\mu_{1W_n(k_1^{\mathrm{perf}})}$ to $\mathrm{Spec}(W_n(k_1^{\mathrm{perf}}))$ of $\mu_{1W_n(k_1)}$, cf. [6, vol. II, Exp. IX, 3.6]. We can assume that $\mu_{1,n+l+1}$ lifts $\mu_{1,n+l}$, cf. loc. cit. From [6, vol. II, Exp. IX, 7.1] we get that there exists a unique cocharacter $\mu_1 \colon \mathbf{G}_m \to G_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(W(k_1^{\mathrm{perf}}))$ that lifts all $\mu_{1,n+l}$'s.

The cocharacter $\mu_{1W(k)} \colon \mathbf{G}_m \to G$ is of the form $g_n \mu g_n^{-1}$ for some $g_n \in G(W(k))$ congruent mod p^n to 1_M, cf. [6, vol. II, Exp. IX, 3.6] and the fact that we have $G(W(k)) = \mathrm{proj\,lim}_{l \in \mathbf{N}} G(W_{n+l}(k))$. Let $\tilde{g}_n := g_n^{-1} \sigma_0 g_n \sigma_0^{-1} \in G(W(k))$; it is congruent mod p^n to 1_M. The element $g_n^{-1} \in G(W(k))$ defines an isomorphism between $(M, \sigma_0 \mu_{1W(k)}(\frac{1}{p}), G, (t_\alpha)_{\alpha \in \mathcal{J}})$ and $(M, \tilde{g}_n \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$. Moreover $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ and $(M, \tilde{g}_n \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ are isomorphic under an isomorphism defined by an element of $G(W(k))$, cf. the very definition of n. We conclude that:

(∗) *the quadruple $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ is isomorphic to $(M, \sigma_0 \mu_{1W(k)}(\frac{1}{p}), G, (t_\alpha)_{\alpha \in \mathcal{J}})$; thus $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ is definable over k_1^{perf} and moreover its isomorphism class is uniquely determined by the triple $(M_{\mathbf{Z}_p}, (t_\alpha)_{\alpha \in \mathcal{J}}, \mu_{1W_n(k_1)})$.*

This motivates the following definitions.

5.2.2. DEFINITIONS. –

(a) We say k_1 (respectively $t(k_1)$) is the field (respectively the transcendental degree) of definition of (M, φ, G) or of $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ with respect to the lift $(F^i(M))_{i \in S(a,b)}$ of (M, φ, G). By the *transcendental degree of definition $td \in \mathbf{N} \cup \{0\}$* of (M, φ, G) or of $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ we mean the smallest number we get by considering transcendental degrees of definition of (M, φ, G) with respect to (arbitrary) lifts of it.

(b) If $td = 0$, then by the *field of definition* of (M, φ, G) or of $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ we mean the finite field that has the smallest number of elements and that is the field of definition of (M, φ, G) with respect to some lift of it.

If $td = 0$ we do not stop to study when the field of definition of (M, φ, G) is contained in all fields of definition of (M, φ, G) with respect to (arbitrary) lifts of (M, φ, G).

5.2.3. THEOREM (*Atlas Principle*). – *We recall that $k = \bar{k}$, that G is smooth over $\mathrm{Spec}(W(k))$, and that the W-condition holds for (M, φ, G). Let $q \in \mathbf{N}$. Let $\mathcal{I}(q) \in \mathbf{N} \cup \{0, \infty\}$ be the number of isomorphism classes of latticed F-isocrystals with a group and an emphasized family of tensors over k that have the form $(M, g\varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ for some $g \in G(W(k))$, that have tran-*

scendental degrees of definition 0, *and that have* $\mathbf{F}_{p^q}$ *as their fields of definition. Then we have* $\mathcal{I}(q) \in \mathbf{N} \cup \{0\}$.

Proof. – We check that the number $N_{\mathrm{tor}} \in \mathbf{N} \cup \{\infty\}$ of isomorphism classes of pairs of the form $(M_{\mathbf{Z}_p}, (t_\alpha)_{\alpha \in \mathcal{J}})$ that are obtained by replacing φ with some $g\varphi$ and by considering some lift of $(M, g\varphi, G)$, is finite. The "difference" between two such pairs is measured by a torsor Θ of $G_{\mathbf{Z}_p}$ in the flat topology of $\mathrm{Spec}(\mathbf{Z}_p)$. So Θ is smooth over $\mathrm{Spec}(\mathbf{Z}_p)$. Thus Θ is a trivial torsor if and only if $\Theta_{\mathbf{F}_p}$ is a trivial torsor. As the set $H^1(\mathbf{F}_p, G_{\mathbf{F}_p})$ is finite (cf. [38, Ch. III, §4, 4.2 and 4.3]), the number of isomorphism classes of torsors of $G_{\mathbf{F}_p}$ is finite. From the last two sentences we get that $N_{\mathrm{tor}} \in \mathbf{N}$.

Let $m \in \mathbf{N}$. We check that the number $N(\mu, m, q, G_{\mathbf{Z}_p}) \in \mathbf{N} \cup \{0, \infty\}$ of cocharacters of $G_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(W_m(\mathbf{F}_{p^q}))$ that over $\mathrm{Spec}(W_m(k))$ are $G(W_m(k))$-conjugate to $\mu_{W_m(k)}$, is also finite. Based on the infinitesimal liftings of [6, vol. II, Exp. IX, 3.6] and on the fact that the group $G_{\mathbf{Z}_p}(W_m(\mathbf{F}_{p^q}))$ is finite, it is enough to prove that the number $N(\mu, 1, q, G_{\mathbf{Z}_p})$ is finite. It suffices to prove that $N(\mu, 1, q, \mathbf{GL}_{M_{\mathbf{Z}_p}}) \in \mathbf{N}$. The number of maximal split tori of $\mathbf{GL}_{M_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} \mathbf{F}_{p^q}}$ is finite and each such torus has precisely $(b - a + 1)^{r_M}$ cocharacters that act on $M_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} \mathbf{F}_{p^q}$ via those $-i$-th powers of the identity character of $\mathbf{G}_m$ that satisfy $i \in S(a, b)$. Thus $N(\mu, 1, q, \mathbf{GL}_{M_{\mathbf{Z}_p}}) \in \mathbf{N}$.

Let n_{fam} be as in 3.1.5; we have $n_{\mathrm{fam}} \geqslant n$. Based on 5.2 (∗), we get that $\mathcal{I}(q)$ is bounded from above by a sum of N_{tor} numbers of the form $N(\mu, n_{\mathrm{fam}}, q, G_{\mathbf{Z}_p})$ and in particular that $\mathcal{I}(q) \leqslant N_{\mathrm{tor}} N(\mu, n_{\mathrm{fam}}, q, \mathbf{GL}_{M_{\mathbf{Z}_p}})$. Thus $\mathcal{I}(q) \in \mathbf{N} \cup \{0\}$. □

5.3. Groupoids and stratifications

Main Theorem A has many reformulations in terms of (stacks of) groupoids. Not to increase the length of the paper, we postpone to future work the introduction of Shimura (stacks of) groupoids that parametrize isomorphism classes of Shimura p-divisible objects we defined in the beginning of Section 4. Presently, this Shimura context is the most general context to which we can extend the classical deformation theories of p-divisible groups (see [30, Chs. 4 and 5], [21, Chs. 3 and 4], [11, 7.1], [8, Main Thm. of Introd.], [9, Main Thm. 1], and [12, §7]). Here, as an anticipation of the numerous possibilities offered by 1.2, we work only with (principally quasi-polarized) p-divisible groups. However, we point out that based on 3.2.2, by using [40, 5.4] as a substitute for the deformation theory of [21, 4.8], the below proof of 5.3.1 can be adapted to contexts that involve arbitrary Shimura varieties of Hodge type and thus involve (principally quasi-polarized) Dieudonné modules equipped with smooth groups as in 3.2 (like the context of [40, §5]).

Let S be a reduced $\mathrm{Spec}(\mathbf{F}_p)$-scheme. Let $\mathcal{D}$ be a p-divisible group over S of height r and relative dimension d. For $i \in \{1, 2\}$ let $\mathcal{D}_i$ be the pullback of $\mathcal{D}$ to $S_{12} := S \times_{\mathrm{Spec}(\mathbf{F}_p)} S$ via the i-th projection $p_i : S_{12} \to S$. For $l \in \mathbf{N}$, let I_l be the affine S_{12}-scheme that parametrizes isomorphisms between $\mathcal{D}_1[p^l]$ and $\mathcal{D}_2[p^l]$; it is of finite presentation. The morphism $i_l : I_l \to S_{12}$ of S-schemes is a $\mathrm{Spec}(\mathbf{F}_p)$-groupoid that acts on S in the sense of [6, vol. I, Exp. V] and [31, Appendix A].

5.3.1. BASIC THEOREM. –
(a) *There exists a number $l \in \mathbf{N}$ effectively bounded from above only in terms of r and such that for any algebraically closed field K of characteristic p, the pullbacks of $\mathcal{D}$ through two K-valued points y_1 and y_2 of S are isomorphic if and only if the K-valued point of S_{12} defined by the pair (y_1, y_2) factors through $i_l : I_l \to S_{12}$.*
(b) *Suppose S is smooth over $\mathrm{Spec}(\mathbf{F}_p)$ of dimension $d(r - d)$ and $\mathcal{D}$ is a versal deformation at each maximal point of S. Then there exists a stratification $\mathcal{S}(\mathcal{D})$ of S in reduced,*

locally closed subschemes such that two points y_1 and y_2 as in (a) *factor through the same stratum if and only if $y_1^*(\mathcal{D})$ is isomorphic to $y_2^*(\mathcal{D})$. The strata of $\mathcal{S}(\mathcal{D})$ are regular and equidimensional.*

(c) *The stratification $\mathcal{S}(\mathcal{D})$ of* (b) *satisfies the purity property.*

(d) *Let $q \in \mathbf{N}$ and let K be as in* (a). *Then for any stratum S_0 of the stratification $\mathcal{S}(\mathcal{D})$ of* (b) *that is a subscheme of S_K, there exists a regular scheme $S_0[q]$ that is finite, flat over S_0 and such that the pullback of $\mathcal{D}[p^q]$ to $S_0[q]$ is constant, i.e. is the pullback to $S_0[q]$ of a truncated Barsotti–Tate group of level q over* $\mathrm{Spec}(K)$.

Proof. – Part (a) follows from 1.3: as l we can take any integer greater that $T(r,d)$. For the rest of the proof we will assume that S is smooth over $\mathrm{Spec}(\mathbf{F}_p)$ of dimension $d(r-d)$ and that $\mathcal{D}$ is a versal deformation at each maximal point of S. We first construct the strata of $\mathcal{S}(\mathcal{D})$ that are subschemes of S_K. Let $y_1 \in S(K) = S_K(K)$. Let

$$S(y_1)^{\mathrm{top}} := (p_2 \circ i_l)_K\big((p_1 \circ i_l)_K^{-1}(y_1)\big) \subseteq S_K^{\mathrm{top}}.$$

As I_l is a $\mathrm{Spec}(\mathbf{F}_p)$-scheme of finite type, $S(y_1)^{\mathrm{top}}$ is a constructible subset of S_K^{top} (cf. [18, Ch. IV, (1.8.4) and (1.8.5)]). Let $\overline{S}(y_1)$ be the Zariski closure of $S(y_1)^{\mathrm{top}}$ in S_K; it is a reduced, closed subscheme of S_K. We identify a maximal point of $S(y_1)^{\mathrm{top}}$ with a K-valued point of S_K. We say $S(y_1)^{\mathrm{top}}$ is regular at a maximal point of it, if there exists a regular, open subscheme of $\overline{S}(y_1)$ which contains this point and whose topological space is contained in $S(y_1)^{\mathrm{top}}$. As $S(y_1)^{\mathrm{top}}$ is a dense, constructible subset of $\overline{S}(y_1)^{\mathrm{top}}$, there exists a regular, open, dense subscheme $W(y_1)$ of $\overline{S}(y_1)$ such that $W(y_1)^{\mathrm{top}} \subseteq S(y_1)^{\mathrm{top}}$.

A point $y_3 \in S(K) = S_K(K)$ belongs to $S(y_1)^{\mathrm{top}}$ if and only if $y_1^*(\mathcal{D})$ and $y_3^*(\mathcal{D})$ are isomorphic. Let now $y_2 \in S(K) = S_K(K)$ be a maximal point of $S(y_1)^{\mathrm{top}}$. Let $i_{12} : y_2^*(\mathcal{D}) \to y_1^*(\mathcal{D})$ be an isomorphism, cf. (a). We have $S(y_2)^{\mathrm{top}} = S(y_1)^{\mathrm{top}}$. For $i \in \{1,2\}$ let I_{y_i} be the spectrum of the completion of the local ring of S_K at y_i. We denote also by y_i the factorization of y_i through I_{y_i}. Let $I_{y_i} \times_{S_K} S(y_1)^{\mathrm{top}}$ be the pullback of $S(y_1)^{\mathrm{top}}$ to a constructible subset of $I_{y_i}^{\mathrm{top}}$. Due to the versal property of $\mathcal{D}$ and the fact that S is smooth over $\mathrm{Spec}(\mathbf{F}_p)$ of dimension $d(r-d)$, the local schemes I_{y_1} and I_{y_2} have dimension $d(r-d)$ and moreover there exists a unique isomorphism

$$I_{12} : I_{y_1} \xrightarrow{\sim} I_{y_2}$$

such that the following two things hold (cf. [21, 4.8]; see [9, 2.4.4] for the equivalence of the categories of p-divisible groups over I_i and over the formal completion of I_i along y_i):

(i) we have $I_{12} \circ y_1 = y_2 : \mathrm{Spec}(K) \to I_{y_2}$;

(ii) there exists an isomorphism $I_{12}^*(\mathcal{D}_{I_{y_2}}) \xrightarrow{\sim} \mathcal{D}_{I_{y_1}}$ that lifts i_{12}.

Due to (ii) the local geometries of $S(y_1)^{\mathrm{top}}$ at y_1 and y_2 are the same. In other words, I_{12} induces via restriction an isomorphism $J_{12}^{\mathrm{top}} : I_{y_1} \times_{S_K} S(y_1)^{\mathrm{top}} \xrightarrow{\sim} I_{y_2} \times_{S_K} S(y_1)^{\mathrm{top}}$ between constructible subsets. Any commutative $\mathbf{F}_p$-algebra of finite type is excellent, cf. [29, (34.A) and (34.B)]. So the morphism $I_{y_i} \to S_K$ is regular. From the last two sentences we get (cf. [29, (33)] for the regular part of (iv)) that:

(iii) the dimensions of $S(y_1)^{\mathrm{top}}$ at y_1 and y_2 are the same;

(iv) if $S(y_1)^{\mathrm{top}}$ is regular at y_2, then $S(y_1)^{\mathrm{top}}$ is also regular at y_1.

By taking y_2 to be a maximal point of $W(y_1)^{\mathrm{top}}$ and y_1 to be an arbitrary maximal point of $S(y_1)^{\mathrm{top}}$, from (iii) we get that $S(y_1)^{\mathrm{top}}$ is equidimensional and from (iv) we get that $S(y_1)^{\mathrm{top}}$ is regular at all its maximal points. So $\overline{S}(y_1)$ is also equidimensional. As $S(y_1)^{\mathrm{top}}$ is a constructible subset of $\overline{S}(y_1)^{\mathrm{top}}$, from the last two sentences we get that $S(y_1)^{\mathrm{top}}$ is the underlying topological space of an equidimensional, regular, open subscheme $S(y_1)$ of $\overline{S}(y_1)$. Thus $S(y_1)$ is a reduced,

locally closed subscheme of S_K. Let

$$J_{12} : I_{y_1} \times_{S_K} S(y_1) \xrightarrow{\sim} I_{y_2} \times_{S_K} S(y_1)$$

be the isomorphism of reduced schemes defined by I_{12} (or J_{12}^{top}).

Let $\mathcal{S}_K(\mathcal{D})$ be the set of reduced, locally closed subschemes of S_K that are of the form $S(y_1)$ for some $y_1 \in S(K) = S_K(K)$. Standard Galois descent shows that there exists a set $\mathcal{S}_{\mathbf{F}_p}(\mathcal{D})$ of reduced, locally closed subschemes of S whose pullbacks to $S_{\overline{\mathbf{F}_p}}$ are the elements of $\mathcal{S}_{\overline{\mathbf{F}_p}}(\mathcal{D})$. If L is an algebraically closed field that contains K and if y_1^L is the L-valued point of S defined by y_1, then by the very definitions $S(y_1^L) = S(y_1)_L$. So we have natural pullback injective maps $\mathcal{S}_K(\mathcal{D}) \hookrightarrow \mathcal{S}_L(\mathcal{D})$ and $\mathcal{S}_{\mathbf{F}_p}(\mathcal{D}) \hookrightarrow \mathcal{S}_L(\mathcal{D})$. So $\mathcal{S}_{\mathbf{F}_p}(\mathcal{D})$ and $\mathcal{S}_K(\mathcal{D})$'s define a stratification $\mathcal{S}(\mathcal{D})$ of S in the sense of 2.1.1. So as each $S(y_1)$ is a regular and equidimensional $\mathrm{Spec}(K)$-scheme, (b) holds.

Let $v, n \in \mathbf{N}$ be as in 5.1.1(c) for $r_1 = r_2 := r$. Let $\tilde{n} := \max\{q, l, n\}$. For $m \in \{\tilde{n}, \tilde{n} + v\}$ let $\mathbf{I}_m(y_1)$ be the $\overline{S}(y_1)$-scheme that parametrizes isomorphisms between $\mathcal{D}_{\overline{S}(y_1)}$ and the pullback of $y_1^*(\mathcal{D})$ through the natural morphism $\overline{S}(y_1) \to \mathrm{Spec}(K)$. We consider the natural truncation morphism $\mathbf{T}_{\tilde{n},v} : \mathbf{I}_{\tilde{n}+v}(y_1) \to \mathbf{I}_{\tilde{n}}(y_1)$ of $\overline{S}(y_1)$-schemes.

Let $\mathbf{I}_{\tilde{n},v}(y_1)$ be the minimal reduced, closed subscheme of $\mathbf{I}_{\tilde{n}}(y_1)_{\mathrm{red}}$ through which the reduced morphism defined by $\mathbf{T}_{\tilde{n},v}$ factors. As $\tilde{n} \geqslant l$, from (a) we get that $\mathbf{I}_{\tilde{n},v}(y_1)$ is in fact an $S(y_1)$-scheme. The resulting morphism

$$m_{\tilde{n},v}(y_1) : \mathbf{I}_{\tilde{n},v}(y_1) \to S(y_1)$$

is surjective, cf. the definition of $S(y_1)$. To prove (c) and (d), it suffices to show that $S(y_1)$ is an affine $\overline{S}(y_1)$-scheme and that $\mathbf{I}_{\tilde{n},v}(y_1)$ is a regular scheme that is finite, flat over $S(y_1)$. It suffices to check this under the extra assumption that S is affine. So the schemes S_K, $\overline{S}(y_1)$, $\mathbf{I}_{\tilde{n}}(y_1)$, and $\mathbf{I}_{\tilde{n},v}(y_1)$ are also affine.

We check that the surjective morphism $m_{\tilde{n},v}(y_1) : \mathbf{I}_{\tilde{n},v}(y_1) \to S(y_1)$ is quasi-finite above any point y_{gen} of $S(y_1)$ of codimension 0. Let F_{gen} and I_{gen} be the fibres over y_{gen} of $\mathbf{I}_{\tilde{n},v}(y_1)$ and $\mathbf{I}_{\tilde{n}+v}(y_1)$ (respectively). We show that the assumption that F_{gen} is not of dimension 0 leads to a contradiction. This assumption implies that the image of I_{gen} in F_{gen} contains an open, dense subscheme of F_{gen} of positive dimension. We get the existence of an algebraically closed field L that contains the residue field of y_{gen} and such that the number of automorphisms of $y_1^*(\mathcal{D})_L[p^{\tilde{n}}]$ that lift to automorphisms of $y_1^*(\mathcal{D})_L[p^{\tilde{n}+v}]$ is infinite. From this and 5.1.1(c) we get that the image of $\mathrm{Aut}(y_1^*(\mathcal{D})_L) = \mathrm{Aut}(y_1^*(\mathcal{D}))$ in $\mathrm{Aut}(y_1^*(\mathcal{D})_L[p^{\tilde{n}}])$ is infinite. But $\mathrm{Aut}(y_1^*(\mathcal{D}))$ is a $\mathbf{Z}_p$-algebra of finite rank and so this image is finite. Contradiction.

So F_{gen} has dimension 0. Thus there exists an open, dense subscheme $U(y_1)$ of $S(y_1)$ such that the reduced $\mathrm{Spec}(K)$-scheme of finite type $\mathbf{I}_{\tilde{n},v}(y_1) \times_{\overline{S}(y_1)} U(y_1)$ is regular as well as (cf. [18, Ch. IV, (9.6.1) and (11.1.1)] and the surjectivity of $m_{\tilde{n},v}$) finite, flat over $U(y_1)$. From (ii) and constructions we get the existence of an isomorphism of S_K-schemes

$$K_{12} : I_{y_1} \times_{S_K} \mathbf{I}_{\tilde{n},v}(y_1) \xrightarrow{\sim} I_{y_2} \times_{S_K} \mathbf{I}_{\tilde{n},v}(y_1)$$

such that we have $(1_{I_{y_2}} \times_{S_K} m_{\tilde{n},v}(y_1)) \circ K_{12} = J_{12} \times_{S(y_1)} m_{\tilde{n},v}(y_1)$. In particular, we get:

(v) the morphism $m_{\tilde{n},v}(y_1)$ is finite and flat above an open subscheme of $S(y_1)$ that contains y_1 if and only if it is so above an open subscheme of $S(y_1)$ that contains y_2.

As in the above part that pertains to local geometries, the existence of such isomorphisms K_{12} of S_K-schemes implies that $\mathbf{I}_{\tilde{n},v}(y_1)$ is regular and equidimensional. From (v) and the existence of $U(y_1)$ we get that $\mathbf{I}_{\tilde{n},v}(y_1)$ is a finite, flat $S(y_1)$-scheme. From this and the fact that $\mathbf{I}_{\tilde{n},v}(y_1)$

is a regular subscheme of $\mathbf{I}_{\tilde{n}}(y_1)$, we get that (d) holds for $\tilde{n}$ (and so also for $q \leqslant \tilde{n}$) and that $\mathbf{I}_{\tilde{n},v}(y_1)$ is the normalization of $S(y_1)$ in the ring of fractions of $\mathbf{I}_{\tilde{n},v}(y_1)$. As $\mathbf{I}_{\tilde{n},v}(y_1)$ is affine and $m_{\tilde{n},v}(y_1)$ is a finite, surjective morphism, from the Chevalley theorem of [16, Ch. II, (6.7.1)] we get that $S(y_1)$ is affine. So (c) holds. $\square$

5.3.2. Ultimate stratifications

Let $N \geqslant 3$ and $\mathcal{A}_{d,1,N}$ be as in 1.5. Let $(\mathcal{A}, \lambda_\mathcal{A})$ be the universal principally polarized abelian scheme over $\mathcal{A}_{d,1,N}$. We have:

(a) *There exists a stratification $\mathcal{S}_{d,N}$ of $\mathcal{A}_{d,1,N}$ defined by the following property: two geometric points y_1 and y_2 of $\mathcal{A}_{d,1,N}$ with values in the same algebraically closed field K, factor through the same stratum of $\mathcal{S}_{d,N}$ if and only if the principally quasi-polarized p-divisible groups of $y_1^*(\mathcal{A}, \lambda_\mathcal{A})$ and $y_2^*(\mathcal{A}, \lambda_\mathcal{A})$, are isomorphic.*

(b) *The stratification $\mathcal{S}_{d,N}$ of $\mathcal{A}_{d,1,N}$ satisfies the purity property and its strata are regular and equidimensional.*

(c) *Let $q \in \mathbf{N}$. Let K be as in* (i). *Then for any stratum S_0 of the stratification $\mathcal{S}_{d,N}$ that is a subscheme of $\mathcal{A}_{d,1,N_K}$, there exists a regular scheme $S_0[q]$ that is finite, flat over S_0 and such that the pullback to $S_0[q]$ of the principally quasi-polarized truncated Barsotti–Tate group of level q of $(\mathcal{A}, \lambda_\mathcal{A})$ is constant, i.e. it is the pullback to $S_0[q]$ of a principally quasi-polarized truncated Barsotti–Tate group of level q over* $\mathrm{Spec}(K)$.

The proofs of (a) to (c) are the same as those of 5.3.1(b) to (d), cf. 3.2.5. We only have to add that the use of [21, 4.8] in the proof of 5.3.1(b) has to be substituted by the well known fact that the formal deformation spaces of a principally polarized abelian variety over $\mathrm{Spec}(K)$ and of its principally quasi-polarized p-divisible group, are naturally identified (cf. the Serre–Tate deformation theory of [23, Ch. 1]).

Let $\mathrm{Sch}_{\mathrm{red}}^{\mathbf{F}_p}$ be the category of reduced $\mathrm{Spec}(\mathbf{F}_p)$-schemes endowed with the étale topology. Let $\mathcal{A}_{d,1}$ be the moduli stack over $\mathrm{Sch}_{\mathrm{red}}^{\mathbf{F}_p}$ of principally polarized abelian schemes of relative dimension d (see [13, Ch. I, §4, p. 17 and 4.3]). The stratification $\mathcal{S}_{d,N}$ descends to a stratification $\mathcal{S}_d$ of $\mathcal{A}_{d,1}$. As we did not formalize stratifications of stacks, we describe $\mathcal{S}_d$ directly as follows.

We fix a principally quasi-polarized p-divisible group $\mathcal{T} := (D, \lambda_D)$ over $\mathrm{Spec}(k)$ of height $r = 2d$. The objects of $\mathcal{A}_{d,1}$ are principally polarized abelian schemes over reduced $\mathrm{Spec}(\mathbf{F}_p)$-schemes. The substack $\mathcal{A}_{d,1}(\mathcal{T})$ of $\mathcal{A}_{d,1}$ associated to $\mathcal{T}$ is the full subcategory of $\mathcal{A}_{d,1}$ whose objects are principally polarized abelian schemes over reduced $\mathrm{Spec}(\mathbf{F}_p)$-schemes with the property that all principally quasi-polarized p-divisible groups obtained from them via pullbacks through points with values in the same algebraically closed field K that contains k, are isomorphic to $\mathcal{T} \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K)$.

We refer to $\mathcal{S}_d$ (respectively to $\mathcal{S}_{d,N}$) as the *ultimate stratification* of $\mathcal{A}_{d,1}$ (respectively of $\mathcal{A}_{d,1,N}$).

Let $\mathcal{A}_{d,1}(\mathcal{T})_k := \mathcal{A}_{d,1}(\mathcal{T}) \times_{\mathrm{Sch}_{\mathrm{red}}^{\mathbf{F}_p}} \mathrm{Sch}_{\mathrm{red}}^k$ and $\mathcal{A}_{d,1_k} := \mathcal{A}_{d,1} \times_{\mathrm{Sch}_{\mathrm{red}}^{\mathbf{F}_p}} \mathrm{Sch}_{\mathrm{red}}^k$, where $\mathrm{Sch}_{\mathrm{red}}^k$ is the full subcategory of $\mathrm{Sch}_{\mathrm{red}}^{\mathbf{F}_p}$ formed by reduced $\mathrm{Spec}(k)$-schemes. The pullback of $\mathcal{A}_{d,1}(\mathcal{T})_k$ via the 1-morphism $\mathcal{A}_{d,1,N_k} \to \mathcal{A}_{d,1_k}$ is the stratum of $\mathcal{S}_{d,N}$ that is a subscheme of $\mathcal{A}_{d,1,N_k}$ and that corresponds naturally to $\mathcal{T}$. Using this it can be easily checked that $\mathcal{A}_{d,1}(\mathcal{T})_k$ is a separated, algebraic stack over $\mathrm{Sch}_{\mathrm{red}}^k$ in the similar sense as of [13, Ch. I, §4, 4.6 and 4.8] but worked out using only reduced $\mathrm{Spec}(k)$-schemes.

The following proposition, to which we refer as the *integral Manin problem* for Siegel modular varieties (see [28, p. 76] and [39, p. 98] for the original Manin problem), implies that $\mathcal{A}_{d,1}(\mathcal{T})$ is a non-empty category.

5.3.3. PROPOSITION. – *Let* $\mathrm{Spec}(C)$ *be a local, complete scheme whose residue field is* $k = \bar{k}$. *Then any principally quasi-polarized* p-*divisible group* $\mathcal{T}'_C$ *over* $\mathrm{Spec}(C)$ *that lifts* $\mathcal{T}$, *is the one of a principally polarized abelian scheme over* $\mathrm{Spec}(C)$.

Proof. – We first show that $\mathcal{T}$ is associated to a principally polarized abelian variety (A, λ_A) over $\mathrm{Spec}(k)$. Let (M, φ, λ_M) be the principally quasi-polarized Dieudonné module of $\mathcal{T}$. Let $\widetilde{A}$ be an abelian variety $\widetilde{A}$ over $\mathrm{Spec}(k)$ whose F-isocrystal is $(M[\frac{1}{p}], \varphi)$, cf. [39, p. 98]. Based on [32, §23, Cor. 1], up to an isogeny, we can choose $\widetilde{A}$ such that it has a principal polarization $\lambda_{\widetilde{A}}$. The principally quasi-polarized Dieudonné module of $(\widetilde{A}, \lambda_{\widetilde{A}})$ is of the form $(\widetilde{M}, \varphi, \lambda_{\widetilde{M}})$, where $\widetilde{M}$ is a certain $W(k)$-lattice of $M[\frac{1}{p}]$.

5.3.3.1. LEMMA. – *If* λ_1 *and* λ_2 *are two principal quasi-polarizations of* $(M[\frac{1}{p}], \varphi)$, *then the triples* $(M[\frac{1}{p}], \varphi, \lambda_1)$ *and* $(M[\frac{1}{p}], \varphi, \lambda_2)$ *are isomorphic.*

Proof. – It suffices to prove the lemma under the assumption that there exists $\alpha \in [0, \frac{1}{2}] \cap \mathbf{Q}$ such that all slopes of $(M[\frac{1}{p}], \varphi)$ are α and $1 - \alpha$, cf. Dieudonné's classification of F-isocrystals over k (see [28, §2]) and [39, p. 98]. Let $i \in \{1, 2\}$.

We first consider the case when $\alpha \neq \frac{1}{2}$; so $\alpha \neq 1 - \alpha$. Let $M[\frac{1}{p}] = M_\alpha \oplus M_{1-\alpha}$ be the direct sum decomposition that is normalized by φ and such that for $\beta \in \{\alpha, 1 - \alpha\}$ all slopes of (M_β, φ) are β. We have $\lambda_i(M_\beta, M_\beta) = 0$ and the bilinear form $\lambda_{i,\beta} : M_\beta \otimes_{B(k)} M_{1-\beta} \to B(k)$ induced naturally by λ_i, is non-degenerate. But $\lambda_{i,1-\alpha}$ is determined by $\lambda_{i,\alpha}$. Thus λ_i is uniquely determined by the isomorphism $j_i : (M_\alpha, \varphi) \xrightarrow{\sim} (M_{1-\alpha}^*, p1_{M_{1-\alpha}^*}\varphi)$ defined naturally by $\lambda_{i,\alpha}$ via the rule $j_i(x)(y) = \lambda_i(x, y) = \lambda_{i,\alpha}(x, y)$, where $x \in M_\alpha$ and $y \in M_{1-\alpha}$. Let $f_{12} := j_1^{-1} j_2 : (M_\alpha, \varphi) \xrightarrow{\sim} (M_\alpha, \varphi)$. The automorphism $e_{12} := f_{12} \oplus 1_{M_{1-\alpha}}$ of $(M[\frac{1}{p}], \varphi) = (M_\alpha, \varphi) \oplus (M_{1-\alpha}, \varphi)$ takes λ_2 into λ_1, i.e. for $x, y \in M[\frac{1}{p}]$ we have an identity $\lambda_2(x, y) = \lambda_1(e_{12}(x), e_{12}(y))$.

Let now α be $\frac{1}{2}$. As $\alpha = \frac{1}{2}$, the F-isocrystal $(M[\frac{1}{p}], \varphi)$ over k is a direct sum of simple F-isocrystals over k of rank 2. Using the standard argument that shows that any two non-degenerate, symmetric, bilinear forms on an even dimensional complex vector space are isomorphic, we get that both $(M[\frac{1}{p}], \varphi, \lambda_1)$ and $(M[\frac{1}{p}], \varphi, \lambda_2)$ are direct sums of principally quasi-polarized F-isocrystals over k of rank 2. Thus we can assume $r_M = 2$ (i.e. $d = 1$). But in this case the lemma is trivial (for instance, cf. [27, pp. 35–36]). $\square$

Based on the lemma, it suffices to prove the proposition under the extra hypothesis that $\lambda_M = \lambda_{\widetilde{M}}$. From the classical Dieudonné theory we get directly the next property.

5.3.3.2. THE ISOGENY PROPERTY. – *There exists a unique principally polarized abelian variety* (A, λ_A) *over* $\mathrm{Spec}(k)$ *that is* $\mathbf{Z}[\frac{1}{p}]$-*isogenous to* $(\widetilde{A}, \lambda_{\widetilde{A}})$ *and whose principally quasi-polarized Dieudonné module is identifiable under this* $\mathbf{Z}[\frac{1}{p}]$-*isogeny with* (M, φ, λ_M).

So $\mathcal{T}$ is the principally quasi-polarized p-divisible group of (A, λ_A). From the Serre–Tate deformation theory (see [23, Ch. 1]) and the Grothendieck algebraization theorem (see [17, Ch. III, Thm. (5.4.5)]), we easily get the existence of a principally polarized abelian scheme over $\mathrm{Spec}(C)$ whose principally quasi-polarized p-divisible group is $\mathcal{T}'_C$. $\square$

5.3.4. *Remarks.* – (a) If $d \geqslant 2$, then the stratification $\mathcal{S}_{d,N}$ has a class which is not a set (for $d \geqslant 3$ this follows from 4.5.4).

(b) Let $q \in \mathbf{N}$. Let $\mathcal{S}_{d,N,q}$ be the stratification of $\mathcal{A}_{d,1,N}$ defined by the rule: two geometric points y_1 and y_2 of $\mathcal{A}_{d,1,N}$ with values in the same algebraically closed field, factor through the same stratum of $\mathcal{S}_{d,N,q}$ if and only if the principally quasi-polarized truncated Barsotti–Tate

groups of level q of $y_1^*(\mathcal{A}, \lambda_{\mathcal{A}})$ and $y_2^*(\mathcal{A}, \lambda_{\mathcal{A}})$, are isomorphic. The strata of $\mathcal{S}_{d,N,q}$ are regular and equidimensional (one argues this in a way similar to the proof of 5.3.1; instead of [21, 4.8] one has to use a principal quasi-polarized version of [21, 4.7 and 4.8] and the Serre–Tate deformation theory). For $q \geqslant T(d)$ we have $\mathcal{S}_{d,N,q} = \mathcal{S}_{d,N}$, cf. 3.2.5. The case $q = 1$ was first studied by Ekedahl and Oort, cf. [34, §1]. The strata of $\mathcal{S}_{d,N,1}$ are quasi-affine, cf. [34, 1.2]. As each stratum of $\mathcal{S}_{d,N,q}$ is a locally closed subscheme of a stratum of $\mathcal{S}_{d,N,1}$, the strata of $\mathcal{S}_{d,N,q}$ are also quasi-affine. For $1 \leqslant q < T(d)$, we do not know when the stratification $\mathcal{S}_{d,N,q}$ satisfies the purity property.

(c) The existence of the ultimate stratifications $\mathcal{S}_d$ and $\mathcal{S}_{d,N}$, though of foundation, is only a first step toward the solution of the below Main Problem. Due to the importance of Main Problem, we will state a general form of it, even if in this paper we do not formalize specializations of latticed F-isocrystals with a group (such specializations are standard for p-divisible groups; see also 3.2.7). To be short, we state Main Problem only in a context that involves tensors but no principal bilinear quasi-polarizations.

MAIN PROBLEM. – Let $(M, \varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$ be a latticed F-isocrystal with a group and an emphasized family of tensors over k such that the W-condition holds for (M, φ, G) (see 2.2.1(b) and (d)). List using families all isomorphism classes of $(M, g\varphi, G, (t_\alpha)_{\alpha \in \mathcal{J}})$'s (where $g \in G(W(k))$) and decide which such classes specialize to which other.

5.4. On the specialization theorem

Let S be an integral $\mathrm{Spec}(\mathbf{F}_p)$-scheme. We take k to be an algebraic closure of the field of fractions k_S of S. Let $\mathfrak{C}$ be an F-crystal over S. Let $h_{\mathfrak{C}} \in \mathbf{N} \cup \{0\}$ be as in 2.1; the h-number of any pullback of $\mathfrak{C}$ via a geometric point of S is at most $h_{\mathfrak{C}}$. Let $\mathcal{N}$ be the Newton polygon of $\mathfrak{C}_k$. Let

$$U^{\mathrm{top}} := \big\{ x \in S^{\mathrm{top}} \mid x^*(\mathfrak{C}) \text{ has Newton polygon } \mathcal{N} \big\}.$$

We recall that Grothendieck proved that for any geometric point y of S the Newton polygon of $y^*(\mathfrak{C})$ is above $\mathcal{N}$ (see [19, Appendice]) and that Katz added that moreover there exists an open subscheme U of S such that the notations match, i.e. U^{top} is the topological space underlying U (see [22, 2.3.1 and 2.3.2]).

We give another proof of the existence of U using Grothendieck's result. This result implies that if $x \in U^{\mathrm{top}}$, then all points of the spectrum of the local ring of x in S belong to U^{top}. To show the existence of U, it is enough to show that there exists a non-empty open subscheme U' of S such that $U'^{\mathrm{top}} \subseteq U^{\mathrm{top}}$. The argument for this goes as follows. The existence of such open subschemes U' implies that U^{top} is an ind-constructible subset of S^{top}, cf. [18, Ch. IV, (9.2.1) and (9.2.3)]. Based on this and the above part that pertains to $x \in U^{\mathrm{top}}$, from [18, Ch. IV, Thm. (1.10.1)] we get that each point of U^{top} is an interior point of U^{top}. Thus U^{top} is an open subset of S^{top} and therefore U exists.

Let $\mathfrak{C}_0$ be a Dieudonné–Fontaine p-divisible object over $\mathbf{F}_p$ of Newton polygon $\mathcal{N}$. Let h_0 be the h-number of $\mathfrak{C}_0$ and let r_0 be the rank of $\mathfrak{C}_0$. Let $i \colon \mathfrak{C}_{0k} \to \mathfrak{C}_k$ be an isogeny. Let $l \in \mathbf{N}$ be such that p^l annihilates $\mathrm{Coker}(i)$. Let $v := \max\{v(r_0, r_0, h_0, b) \mid b \in S(0, h_{\mathfrak{C}})\}$ and $n := \max\{1, n(r_0, r_0, h_0, b) \mid b \in S(0, h_{\mathfrak{C}})\}$ be defined using the numbers of 5.1.1(b).

Let $i(n + v + l)$ be the reduction of $i \bmod p^{n+v+l}$; it is a morphism of $\mathcal{M}(W_{n+v+l}(k))$ whose cokernel is annihilated by p^l. From 2.8.3 (see 2.8.3(a) applied with $(V_1, V, q) = (k, k_S, n + v + l)$), we get that there exists a finite field extension $k_{\widetilde{S}}$ of k_S such that $i(n + v + l)$ is the pullback of a morphism $i(n + v + l)_{k_{\widetilde{S}}}$ of $\mathcal{M}(W_{n+v+l}(k_{\widetilde{S}}))$ whose cokernel is annihilated by p^l. Let $\widetilde{S}$ be the normalization of S in $k_{\widetilde{S}}$ (the notations match, i.e. $k_{\widetilde{S}}$ is the field of fractions

of $\widetilde{S}$). The continuous map $\widetilde{S}^{\mathrm{top}} \to S^{\mathrm{top}}$ is proper, cf. the going-up theorem of [29, (5.E)]. So if there exists an open, dense subscheme $\widetilde{U}'$ of $\widetilde{S}$ with the property that $\widetilde{U}'^{\mathrm{top}}$ maps into U^{top}, then we can take U' to be the complement in S of the image of $\widetilde{S}^{\mathrm{top}} \setminus \widetilde{U}'^{\mathrm{top}}$ in S^{top}. Thus it suffices to consider the case when $k_{\widetilde{S}} = k_S$. Let U' be an open subscheme of S such that we have a morphism

$$i_{U'}(n+v+l) \colon \mathbf{E}\big(\mathfrak{C}_0; W_{n+v+l}(U')\big) \to \mathbf{E}\big(\mathfrak{C}; W_{n+v+l}(U')\big)$$

of $\mathcal{M}(W_{n+v+l}(U'))$ that extends $i(n+v+l)_{k_S}$ and that has a cokernel annihilated by p^l, cf. 2.8.3(b). For an arbitrary geometric point $z \colon \mathrm{Spec}(K) \to U'$, the reduction $\mathrm{mod}\ p^{n+l}$ of the pullback morphism $z^*(i_{U'}(n+v+l))$ lifts to a morphism $i_z \colon \mathfrak{C}_{0K} \to z^*(\mathfrak{C})$ of F-crystals over K (cf. 5.1.1(b), 5.1.2, and the definitions of v and n). As the cokernel of the reduction $\mathrm{mod}\ p^{n+l}$ of i_z is annihilated by p^l and as $n \geqslant 1$ (by reasons of ranks) the morphism i_z is injective and thus an isogeny. Thus $z^*(\mathfrak{C})$ has Newton polygon $\mathcal{N}$. So $U'^{\mathrm{top}} \subseteq U^{\mathrm{top}}$. This ends the argument for the existence of U' and so also of U.

6. Proof of Main Theorem B

Let S be a reduced $\mathrm{Spec}(\mathbf{F}_p)$-scheme. Let $\mathfrak{C}$ be an F-crystal over S. Let $\mathcal{S}(\mathfrak{C})$ be the Newton polygon stratification of S defined by $\mathfrak{C}$, cf. [22, 2.3.1 and 2.3.2]. The stratification $\mathcal{S}(\mathfrak{C})$ is of finite type and locally in the Zariski topology of S has a finite number of strata. The main goal of this Section is to prove Main Theorem B stated in 1.6, i.e. to prove that $\mathcal{S}(\mathfrak{C})$ satisfies the purity property (see 6.2). In 6.1 we capture the very essence of Main Theorem B for the case when S is an integral, locally noetherian scheme. In 6.3 we include two remarks on the connection between 6.1 and a result of de Jong and Oort and on Newton polygon stratifications defined by certain reductions modulo powers of p of F-crystals. We will use the notations of 2.8.2.

6.1. THEOREM. – *Suppose S is integral and locally noetherian. Let U be the maximal open subscheme of S with the property that the Newton polygons of pullbacks of $\mathfrak{C}$ through geometric points of U are all equal* (*see* 5.4). *Then U is an affine S-scheme.*

Proof. – It suffices to prove this under the extra assumptions that $S = \mathrm{Spec}(R)$ is affine and that the underlying R-module of $\mathbf{E}(\mathfrak{C}; W_1(S))$ is free. Let R_U be the R-algebra of global functions of U. We have to show that U is affine, i.e. the natural and functorial morphism $f_U \colon U \to \mathrm{Spec}(R_U)$ is an isomorphism. This statement is local in the faithfully flat topology of S and thus we can assume that S is local. Let $\widehat{R}$ be the completion of R and let $\widehat{S} := \mathrm{Spec}(\widehat{R})$. As $\widehat{S}$ is a faithfully flat S-scheme, to show that U is affine (i.e. f_U is an isomorphism) it suffices to show that $U \times_S \widehat{S}$ is affine (i.e. $f_U \times_S \widehat{S} = f_{U \times_S \widehat{S}}$ is an isomorphism). Let $\widehat{S}_1 = \mathrm{Spec}(\widehat{R}_1), \ldots, \widehat{S}_j = \mathrm{Spec}(\widehat{R}_j)$ be the irreducible components of the reduced scheme of $\widehat{S}$ (here $j \in \mathbf{N}$); they are spectra of local, complete, integral, noetherian $\mathbf{F}_p$-algebras. The scheme $U \times_S \widehat{S}$ is affine if and only if the irreducible components $U \times_S \widehat{S}_1, \ldots, U \times_S \widehat{S}_j$ of the reduced scheme of $U \times_S \widehat{S}$ are all affine (cf. [16, Ch. II, Cor. (6.7.3)]). So to prove the theorem we can assume $R = \widehat{R} = \widehat{R}_1$. As R is a local, complete ring, it is also excellent (cf. [29, (34.B)]). Thus the normalization S^{n} of S is a finite S-scheme. So S^{n} is a semilocal, complete, integral, normal scheme. This implies that S^{n} is local. But U is affine if and only if $U \times_S S^{\mathrm{n}}$ is affine, cf. 2.9.2. Thus to prove the Theorem, we can also assume S is normal; so $S = S^{\mathrm{n}}$.

We emphasize that for the rest of the proof we will only use the fact that S is an integral, normal, excellent, affine scheme (but not necessarily local and thus not necessarily complete). We group the main steps into distinct (and numbered) sections.

6.1.1. Notations and two operations

Let k_S, k, $h_{\mathfrak{C}}$, $\mathcal{N}$, $\mathfrak{C}_0$, h_0, r_0, v, and n be as in 5.4. So $\mathcal{N}$ is the Newton polygon of pullbacks of $\mathfrak{C}_U$ via geometric points of U, $\mathfrak{C}_0$ is a Dieudonné–Fontaine p-divisible object over $\mathbf{F}_p$ that has Newton polygon $\mathcal{N}$, r_0 is the rank of $\mathfrak{C}_0$, etc. Let $q_0 := r_0!$. Below all pullbacks to $\mathrm{Spec}(k)$ of F-crystals are via the natural dominant morphisms $\mathrm{Spec}(k) \to \mathrm{Spec}(\mathbf{F}_p)$ and $\mathrm{Spec}(k) \to S$.

We consider the following two replacement operations $(\mathcal{R}1)$ and $(\mathcal{R}2)$ of the triple $(S, U, \mathfrak{C})$ by a new triple $(\widetilde{S}, \widetilde{U}, \widetilde{\mathfrak{C}})$. For both operations $\widetilde{S}$ is an integral, normal, affine S-scheme of finite type, $\widetilde{\mathfrak{C}}$ is $\mathfrak{C}_{\widetilde{S}}$, and

  $(\mathcal{R}1)$ *either $(\widetilde{S}, \widetilde{U})$ is the normalization of (S, U) in a finite field extension of k_S*

  $(\mathcal{R}2)$ *or U is an open subscheme of $\widetilde{S}$ and $\widetilde{U} := U$ is $U \times_S \widetilde{S}$.*

The scheme $\widetilde{S}$ is also excellent, cf. [29, (34.B)]. Moreover, U is affine if and only if $\widetilde{U}$ is affine (in connection with $(\mathcal{R}1)$, cf. 2.9.2). So in what follows we will often perform one of these two operations in order to simplify the setting and to eventually end up with a situation where in fact we have $U = S$. By performing $(\mathcal{R}1)$, we can assume that R is an $\mathbf{F}_{p^{q_0}}$-algebra (i.e. $\mathbf{F}_{p^{q_0}} \hookrightarrow R$).

Let V be a local ring of U that is a discrete valuation ring. Let V_2 be a complete discrete valuation ring that is a faithfully flat V-algebra, and that has an algebraically closed residue field k_2. Let $V_1 := V_2^{\mathrm{perf}}$. We fix an isomorphism $V_2 \xrightarrow{\sim} k_2[[w]]$ and we view it as an identification under which V_2 and V_1 become k_2-algebras. Let Φ_2 be the Frobenius endomorphism of $W(k_2)[[w]]$ that takes w into w^p and is compatible with σ_{k_2}.

6.1.2. KEY LEMMA. – *There exists a number $l \in \mathbf{N}$ that is greater than $\max\{h_0 r_0^2, h_{\mathfrak{C}}\}$, that depends only on $\mathfrak{C}_0$ and $h_{\mathfrak{C}}$ but not on V, and such that there exists an isogeny $i_{V_1} : \mathfrak{C}_{0V_1} \to \mathfrak{C}_{V_1}$ of F-crystals over $\mathrm{Spec}(V_1)$ whose cokernel is annihilated by p^l.*

Proof. – We first show by induction on $r_0 \in \mathbf{N}$ that there exists a number $\tilde{l}_C \in \mathbf{N}$ that does not depend on V but only on $\mathfrak{C}_0$ and $h_{\mathfrak{C}}$ and such that we have an isogeny $i_1 : \mathfrak{C}_{CV_1} \to \mathfrak{C}_{V_1}$ whose cokernel is annihilated by $p^{\tilde{l}_C}$, where $\mathfrak{C}_C$ is an F-crystal over $\mathrm{Spec}(k_2)$ and where the role of $\mathfrak{C}_{V_1}$ is that of the pullback to $\mathrm{Spec}(V_1)$ of an arbitrary F-crystal over $\mathrm{Spec}(V_2)$ of constant Newton polygon which depends only on $\mathcal{N}$.

Let α_1 be the smallest slope of $\mathcal{N}$. Let $\tilde{l}_1 := -[-\alpha_1(r_0 - 1)]$. Theorem [22, 2.6.1] says that there exists an isogeny $i_1' : \mathfrak{C}' \to \mathfrak{C}_{V_2}$, where $\mathfrak{C}'$ is an α_1-divisible F-crystal over $\mathrm{Spec}(V_2)$. The α_1-divisibility means that if (M', φ', ∇') is the evaluation of $\mathfrak{C}'$ at the thickening defined by the closed embedding $\mathrm{Spec}(V_2) \hookrightarrow \mathrm{Spec}(W(k_2)[[w]])$, then for all $u \in \mathbf{N}$ the Φ_2^u-linear endomorphism $(\varphi')^u$ of M' is divisible by $p^{[u\alpha_1]}$. We can choose $\mathfrak{C}'$ and i_1' such that $\mathrm{Coker}(i_1')$ is annihilated by $p^{\tilde{l}_1}$, cf. [22, p. 153]. If α_1 is the only slope of $\mathcal{N}$, then $\mathfrak{C}'$ is the pullback of an F-crystal over $\mathrm{Spec}(k_2)$ (cf. [22, proof of 2.7.1]); so we can take $\tilde{l}_C$ to be $\tilde{l}_1$ and i_1 to be i_1'. In particular, $\tilde{l}_C$ exists if $r_0 = 1$.

We now consider the case when $\mathcal{N}$ has at least two slopes. From [22, proof of 2.6.2] we get that we have a unique short exact sequence

$$0 \to \mathfrak{C}_1' \to \mathfrak{C}' \to \mathfrak{C}_2' \to 0$$

of F-crystals over $\mathrm{Spec}(V_2)$ with the property that the Newton polygons of the pullbacks of $\mathfrak{C}_1'$ (respectively of $\mathfrak{C}_2'$) via geometric points of $\mathrm{Spec}(V_2)$ have all slopes equal to α_1 (respectively have all slopes greater than α_1). As V_1 is perfect, loc. cit. also proves that this short exact sequence has a unique splitting after we pull it back to $\mathrm{Spec}(V_1)$. Thus we have a unique direct sum decomposition $\mathfrak{C}_{V_1}' = \mathfrak{C}_{1V_1}' \oplus \mathfrak{C}_{2V_1}'$ of F-crystals over $\mathrm{Spec}(V_1)$. Using this decomposition and the fact that both F-crystals $\mathfrak{C}_1'$ and $\mathfrak{C}_2'$ over $\mathrm{Spec}(V_2)$ have ranks smaller than r_0, by induction we get the existence of $\tilde{l}_C$. This ends the induction.

Let $\tilde{l}_f := \max\{d(r_0,0,c) \mid c \in S(0, h_{\mathfrak{C}} + \tilde{l}_C)\}$ with $d(r_0,0,c)$'s as in 2.4.1. The h-number of $\mathfrak{C}_C$ is at most $h_{\mathfrak{C}} + \tilde{l}_C$. So from 2.4.1 (applied over k_2) we get that there exists a Dieudonné–Fontaine p-divisible object $\mathfrak{C}'_0$ over $\mathbf{F}_p$ for which we have an isogeny $i_2 : \mathfrak{C}'_{0V_1} \to \mathfrak{C}_{CV_1}$ whose cokernel is annihilated by $p^{\tilde{l}_f}$. As the number of isomorphism classes of Dieudonné–Fontaine p-divisible objects over $\mathbf{F}_p$ that have $\mathcal{N}$ as their Newton polygons is finite, there exists a number $\tilde{l}_{\mathcal{N}} \in \mathbf{N}$ such that we have an isogeny $i_3 : \mathfrak{C}_{0V_1} \to \mathfrak{C}'_{0V_1}$ whose cokernel is annihilated by $p^{\tilde{l}_{\mathcal{N}}}$.

As i_{V_1} we can take the composite isogeny $i_1 \circ i_2 \circ i_3$. Thus as l we can take any integer greater than $\max\{h_0 r_0^2, h_{\mathfrak{C}}, \tilde{l}_C + \tilde{l}_f + \tilde{l}_{\mathcal{N}}\}$. $\square$

6.1.3. The open subscheme U_0

With l as in 6.1.2, let $m := 8l + n + v + 1$. We continue the proof of Theorem 6.1 by considering (see 2.8.2) the evaluation morphism

$$\mathbf{E}\big(i_{V_1}; W_{m+2v}(V_1)\big) : \mathbf{E}\big(\mathfrak{C}_0; W_{m+2v}(V_1)\big) \to \mathbf{E}\big(\mathfrak{C}; W_{m+2v}(V_1)\big)$$

of $\mathcal{M}(W_{m+2v}(V_1))$. We apply 2.8.3(c) (with $q = m + 2v$) to this morphism. We get that there exist a finite field extension $k_{S,V}$ of k_S and an open, affine subscheme $U_{\widetilde{V}}$ of the normalization of U in $k_{S,V}$, such that $U_{\widetilde{V}}$ has a local ring $\widetilde{V}$ which is a discrete valuation ring and which dominates V and moreover we have a morphism

$$i_{U_{\widetilde{V}}}(m+2v) : \mathbf{E}\big(\mathfrak{C}_0; W_{m+2v}(U_{\widetilde{V}})\big) \to \mathbf{E}\big(\mathfrak{C}; W_{m+2v}(U_{\widetilde{V}})\big)$$

of $\mathcal{M}(W_{m+2v}(U_{\widetilde{V}}))$ whose cokernel is annihilated by p^l. See 2.1 for $i_{U_{\widetilde{V}}}(m+v)$.

Let $\tilde{m} \in \{m, m+v\}$. Let $I_{\tilde{m}}$ be the set of morphisms $\mathfrak{C}_{0k}/p^{\tilde{m}}\mathfrak{C}_{0k} \to \mathfrak{C}_k/p^{\tilde{m}}\mathfrak{C}_k$ that are reductions $\bmod\ p^{\tilde{m}}$ of morphisms $\mathfrak{C}_{0k}/p^{\tilde{m}+v}\mathfrak{C}_{0k} \to \mathfrak{C}_k/p^{\tilde{m}+v}\mathfrak{C}_k$. Any morphism in $I_{\tilde{m}}$ lifts to a morphism $\mathfrak{C}_{0k} \to \mathfrak{C}_k$, cf. 5.1.1(b), 5.1.2, and the definitions of v and $n < m$; thus $I_{\tilde{m}}$ is a finite set. Let $J_{\tilde{m}} := \{i \in I_{\tilde{m}} \mid p^l \operatorname{Coker}(i) = 0\}$. Based on the case 2.8.3(a) of 2.8.3, by performing $(\mathcal{R}1)$ we can assume that $J_{\tilde{m}}$ is the set of pullbacks of a set of morphisms $L_{\tilde{m}}$ of $\mathcal{M}(W_{\tilde{m}}(k_S))$ whose cokernels are annihilated by p^l. The pullback of $i_{U_{\widetilde{V}}}(m+v)$ to a morphism of $\mathcal{M}(W_{m+v}(k_{S,V}))$ is also the pullback of a morphism in L_{m+v}. As $V = \widetilde{V} \cap k_S$, inside $W_{m+v}(k_{S,V})$ we have $W_{m+v}(V) = W_{m+v}(\widetilde{V}) \cap W_{m+v}(k_S)$. This implies that the pullback of $i_{U_{\widetilde{V}}}(m+v)$ to a morphism of $\mathcal{M}(W_{m+v}(\widetilde{V}))$ is in fact the pullback of a morphism of $\mathcal{M}(W_{m+v}(V))$ whose cokernel is generically annihilated by p^l (in the sense of 2.8.1). From the case 2.8.3(b) of 2.8.3 (applied with (V_1, V) replaced by (V, R)), we get the existence of an open subscheme U_V of U that has V as a local ring and such that we have a morphism

$$i_{U_V}(m+v) : \mathbf{E}\big(\mathfrak{C}_0; W_{m+v}(U_V)\big) \to \mathbf{E}\big(\mathfrak{C}; W_{m+v}(U_V)\big)$$

of $\mathcal{M}(W_{m+v}(U_V))$ whose cokernel is generically annihilated by p^l.

For $i \in J_m$ let $\mathcal{V}(i)$ be the set of all those discrete valuation rings V of U such that the pullback of $i_{U_V}(m)$ to a morphism of $\mathcal{M}(W_m(k))$ is i. Let $U_i := \bigcup_{V \in \mathcal{V}(i)} U_V$. Let

$$i_{U_i}(m) : \mathbf{E}\big(\mathfrak{C}_0; W_m(U_i)\big) \to \mathbf{E}\big(\mathfrak{C}; W_m(U_i)\big)$$

be the morphism of $\mathcal{M}(W_m(U_i))$ which is obtained by gluing together the morphisms $i_{U_V}(m)$'s with $V \in \mathcal{V}(i)$. We have:
(a) if $U_0 := \bigcup_{i \in J_m} U_i$, then $U^{\mathrm{top}} \setminus U_0^{\mathrm{top}}$ has codimension at least 2 in U^{top};
(b) for any $i \in J_m$, the cokernel of $i_{U_i}(m)$ is generically annihilated by p^l.

6.1.4. Gluing morphisms

We now modify the morphisms $i_{U_i}(m)$'s ($i \in J_m$) so that they glue together to define a morphism

$$i_{U_0}(m) : \mathbf{E}\big(\mathfrak{C}_0 ; W_m(U_0)\big) \to \mathbf{E}\big(\mathfrak{C} ; W_m(U_0)\big)$$

of $\mathcal{M}(W_m(U_0))$ whose cokernel is generically annihilated by p^{3l}. If there exists $i \in J_m$ such that $U_i = U_0$, then $i_{U_0}(m) = i_{U_i}(m)$ has a cokernel generically annihilated by p^l.

We now assume that for all $i \in J_m$ we have $U_0 \neq U_i$. The pullback of $i_{U_i}(m)$ to a morphism of $\mathcal{M}(W_m(k))$ is $i \in J_m$. Let $f_i : \mathfrak{C}_{0k} \to \mathfrak{C}_k$ be a morphism such that its reduction mod p^m is i, cf. 5.1.1(b), 5.1.2, and the fact that $J_m \subseteq I_m$. As $m > l$ and $i \in J_m$, the cokernel of f_i is annihilated by p^l and so f_i is an isogeny.

Let $f_0 \in \{p^l f_i \mid i \in J_m\}$. We have:
(a) the image of f_0 lies inside the intersection of the images of all f_i's ($i \in J_m$);
(b) the cokernel of f_0 is annihilated by p^{2l}.

Let $s_i : \mathfrak{C}_{0k} \to \mathfrak{C}_{0k}$ be the isogeny such that we have $f_0 = f_i \circ s_i$, cf. (a). So $\mathrm{Coker}(s_i)$ is annihilated by p^{2l}, cf. (b). We know that s_i is the pullback of an isogeny $\mathfrak{C}_{0\mathbf{F}_{p^{q_0}}} \to \mathfrak{C}_{0\mathbf{F}_{p^{q_0}}}$, cf. 2.2.3(b) applied to $\mathfrak{C}_0$. So as $\mathbf{F}_{p^{q_0}} \hookrightarrow R$, we get that the reduction mod p^m of s_i is the pullback of a (constant) morphism

$$s_{U_i}(m) : \mathbf{E}\big(\mathfrak{C}_0 ; W_m(U_i)\big) \to \mathbf{E}\big(\mathfrak{C}_0 ; W_m(U_i)\big)$$

of $\mathcal{M}(W_m(U_i))$ whose cokernel is annihilated by p^{2l}. If $i_1, i_2 \in J_m$, then the pullbacks of $i_{U_{i_1}}(m) \circ s_{U_{i_1}}(m)$ and $i_{U_{i_2}}(m) \circ s_{U_{i_2}}(m)$ to morphisms of $\mathcal{M}(W_m(k))$ are the reduction of f_0 mod p^m and thus they coincide. This implies that the pullbacks of $i_{U_{i_1}}(m) \circ s_{U_{i_1}}(m)$ and $i_{U_{i_2}}(m) \circ s_{U_{i_2}}(m)$ to morphisms of $\mathcal{M}(W_m(U_{i_1} \cap U_{i_2}))$ coincide. Thus the morphisms $i_{U_i}(m) \circ s_{U_i}(m)$ indexed by $i \in J_m$ glue together to define a morphism $i_{U_0}(m) : \mathbf{E}(\mathfrak{C}_0 ; W_m(U_0)) \to \mathbf{E}(\mathfrak{C} ; W_m(U_0))$ of $\mathcal{M}(W_m(U_0))$ whose cokernel is generically annihilated by $p^{3l} = p^l p^{2l}$, cf. 6.1.3(b) and the fact that p^{2l} annihilates $\mathrm{Coker}(s_{U_i}(m))$.

It is easy to see that by performing $(\mathcal{R}1)$ we can assume p^{3l} annihilates $\mathrm{Coker}(i_{U_0}(m))$ but this will not be used in what follows.

6.1.5. LEMMA. – *By performing $(\mathcal{R}2)$, we can assume that $i_{U_0}(m)$ extends to a morphism $i_S(m) : \mathbf{E}(\mathfrak{C}_0 ; W_m(S)) \to \mathbf{E}(\mathfrak{C} ; W_m(S))$ of $\mathcal{M}(W_m(S))$.*

Proof. – Let S' be the affine S-scheme of finite type that parametrizes morphisms between the two objects $\mathbf{E}(\mathfrak{C}_0 ; W_m(S))$ and $\mathbf{E}(\mathfrak{C} ; W_m(S))$ of $\mathcal{M}(W_m(S))$, cf. 2.8.4.1. Let $U_0 \hookrightarrow S'$ be the open embedding of S-schemes that defines $i_{U_0}(m)$. Let U' be the normalization of the Zariski closure of U_0 in S'. As S is an excellent scheme, the S-scheme U' is integral, normal, affine, and of finite type. As U_0 is an open subscheme of both U and U' and due to 6.1.3(a), the affine morphism $U' \times_S U \to U$ between integral, normal, noetherian schemes is birational and has the property that any discrete valuation ring of U is also a local ring of $U' \times_S U$. Thus the morphism $U' \times_S U \to U$ is an isomorphism, cf. 2.9.1. So U is an open subscheme of U'. So by performing $(\mathcal{R}2)$ (with $\widetilde{S} = U'$), we can assume $U' = S$. Thus we can speak about the morphism $i_S(m) : \mathbf{E}(\mathfrak{C}_0 ; W_m(S)) \to \mathbf{E}(\mathfrak{C} ; W_m(S))$ of $\mathcal{M}(W_m(S))$ that extends $i_{U_0}(m)$. $\square$

6.1.6. Duals

Let $\mathfrak{C}(l)$ be the Tate twist of $\mathfrak{C}$ by (l), i.e. $\mathfrak{C}$ tensored with the pullback to S of the F-crystal $(\mathbf{Z}_p, p^l 1_{\mathbf{Z}_p})$ over $\mathbf{F}_p$. As for modules, let $\mathfrak{C}^*$ be the dual of $\mathfrak{C}$ (one could call it a latticed F-isocrystal over S). We also define the Tate twist $\mathfrak{C}^*(l)$ of $\mathfrak{C}^*$ by (l); it is an F-crystal over S (as $l > h_{\mathfrak{C}}$). In a similar way we define $\mathfrak{C}_0^*(l)$. As $l > h_0$, $\mathfrak{C}_0^*(l)$ is a Dieudonné–Fontaine p-divisible object over $\mathbf{F}_p$ with non-negative slopes.

We repeat the constructions we performed for $\mathfrak{C}_0$ and $\mathfrak{C}$ (like the ones through which we got l, U_0, $i_S(m)$, etc.) in the context of $\mathfrak{C}_0^*(l)$ and $\mathfrak{C}^*(l)$. So by enlarging l and by performing $(\mathcal{R}1)$ and $(\mathcal{R}2)$, we can assume there exists a morphism

$$i_S^*(m) : \mathbf{E}\big(\mathfrak{C}_0^*(l); W_m(S)\big) \to \mathbf{E}\big(\mathfrak{C}^*(l); W_m(S)\big)$$

of $\mathcal{M}(W_m(S))$ whose cokernel is generically annihilated by p^{3l} and which is the analogue of $i_S(m)$. As $l > h_{\mathfrak{C}}$, we think of $\mathbf{E}(\mathfrak{C}^*(l); W_m(S))$ to be a "twisted dual" of $\mathbf{E}(\mathfrak{C}; W_m(S))$ in the sense that there exists a morphism

$$j_S(m-l) : \mathbf{E}\big(\mathfrak{C}; W_{m-l}(S)\big) \to \mathbf{E}\big(\mathfrak{C}_0; W_{m-l}(S)\big)$$

which at the level of $\mathcal{O}_{W_{m-l}(S)}$-modules is the dual of $i_S^*(m-l)$. Thus the pullback of $j_S(m-l)$ to an object of $\mathcal{M}(W_{m-l}(k))$ has a cokernel annihilated by p^{3l}. By performing $(\mathcal{R}_1)$ we can assume $\mathrm{Coker}(j_S(m-l))$ is generically annihilated by p^{3l}, cf. 2.8.3(a).

6.1.7. End of the proof of Theorem 6.1

We will use the existence of the morphisms $i_S(m)$ and $i_S^*(m)$ to show that the assumption $U \neq S$ leads to a contradiction. Let $y : \mathrm{Spec}(k_1) \to S$ be a geometric point that does not factor through U. Let

$$c_S(m-l) := j_S(m-l) \circ i_S(m-l) : \mathbf{E}\big(\mathfrak{C}_0; W_{m-l}(S)\big) \to \mathbf{E}\big(\mathfrak{C}_0; W_{m-l}(S)\big).$$

We check that $\mathrm{Coker}(c_S(m-l))$ is annihilated by p^{7l}. Let $c_S(m-l)_{\mathrm{gen}}$ and $c_S(m-2l)_{\mathrm{gen}}$ be the morphisms of $\mathcal{M}(W_{m-l}(k))$ and $\mathcal{M}(W_{m-2l}(k))$ (respectively) that are the natural pullbacks of $c_S(m-l)$ and $c_S(m-2l)$ (respectively). As $c_S(m-2l)_{\mathrm{gen}}$ is the composite of two morphisms of $\mathcal{M}(W_{m-2l}(k))$ whose cokernels are annihilated by p^{3l}, $\mathrm{Coker}(c_S(m-2l)_{\mathrm{gen}})$ is annihilated by p^{6l}. As $c_S(m-2l)_{\mathrm{gen}}$ lifts to $c_S(m-l)_{\mathrm{gen}}$ and as $l > h_0 r_0^2$, $c_S(m-2l)_{\mathrm{gen}}$ is the pullback of a morphism of $\mathcal{M}(W_{m-2l}(\mathbf{F}_{p^{q_0}}))$ (cf. 2.2.3(a) applied with (K,k) replaced by $(k, \mathbf{F}_p)$). So as $\mathbf{F}_{p^{q_0}} \hookrightarrow R$, we get that $\mathrm{Coker}(c_S(m-2l))$ itself is annihilated by p^{6l}. Thus p^{7l} annihilates $\mathrm{Coker}(c_S(m-l))$.

As the endomorphism $y^*(c_S(m-l)) = y^*(j_S(m-l)) \circ y^*(i_S(m-l))$ of $\mathcal{M}(W_{m-l}(k))$ has a cokernel annihilated by p^{7l}, we get that p^{7l} annihilates $\mathrm{Coker}(y^*(i_S(m-l)))$. Let $f_y : \mathfrak{C}_{0k_1} \to y^*(\mathfrak{C})$ be a morphism that lifts $y^*(i_S(m-l-v))$, cf. 5.1.1(b) and 5.1.2. As $m-v-l = 7l+n+1 \geqslant 7l+1$ (cf. the definition of m in 6.1.3) and as p^{7l} annihilates $\mathrm{Coker}(y^*(i_S(m-l-v)))$ (by reasons of ranks) the morphism f_y is injective and so an isogeny. So $y^*(\mathfrak{C})$ has Newton polygon $\mathcal{N}$. So y factors through U. This contradicts the choice of y. Thus the existence of the morphisms $i_S(m)$ and $i_S^*(m)$ implies that $U = S$. As $U = S$, U is affine. This ends the proof of Theorem 6.1. $\square$

6.2. Proof of Main Theorem B

We prove 1.6. Let U be a reduced, locally closed subscheme of S that is a stratum of $\mathcal{S}(\mathfrak{C})$. We have to show that U is an affine S-scheme. It suffices to check this under the extra assumptions that $S = \mathrm{Spec}(R)$ is affine, that U is an open, dense subscheme of S, and that the underlying R-module of $\mathbf{E}(\mathfrak{C}; W_1(S))$ is free. We will show that U is an affine scheme. It suffices to check this under the extra assumption that R is normal and perfect, cf. 2.9.2 applied with X and X' replaced by S and by the normalization of $\mathrm{Spec}(R^{\mathrm{perf}})$ (respectively).

Let $\mathcal{N}$ be the Newton polygon of pullbacks of $\mathfrak{C}_U$ via geometric points of U. Let $\mathfrak{C}_0, h_0, r_0, v$, and n be associated to $\mathcal{N}$ and $h_{\mathfrak{C}}$ as in 5.4 (this makes sense even if R is not an integral domain;

see 2.1 for $h_{\mathfrak{C}}$). So $\mathfrak{C}_0 = (M_0, \varphi_0)$ is a Dieudonné–Fontaine p-divisible object over $\mathbf{F}_p$ that has rank r_0, has h-number h_0, and has Newton polygon $\mathcal{N}$.

Let $\tilde{n}$ be the maximum between $2 + h_{\mathfrak{C}} + 2\max\{d(r_0^2, s, c) \mid s \in S(0, h_{\mathfrak{C}}),\ c \in S(0, 2h_{\mathfrak{C}})\}$ and n. If (M, φ) is an F-crystal over an algebraically closed field K of characteristic p of rank r_0 and h-number at most $h_{\mathfrak{C}}$, then $(\mathrm{End}(M), \varphi)$ is a latticed F-isocrystal over K whose rank is r_0^2, whose s-number is at most $h_{\mathfrak{C}}$, and whose h-number is at most $2h_{\mathfrak{C}}$ (see end of 2.2.1(e)). Thus from 3.2.8(a) (applied with $G = \mathbf{GL}_M$) and 2.4.1 we get:

(i) any F-crystal over K whose rank is r_0 and whose h-number is at most $h_{\mathfrak{C}}$, is uniquely determined up to isomorphism by its reduction mod $p^{\tilde{n}}$.

We consider quadruples of the form $(\tilde{k}, \widetilde{\Phi}, \widetilde{M}, \tilde{\varphi})$, where:

- $\tilde{k}$ is an algebraically closed field of characteristic p,
- $\widetilde{\Phi}$ is the Frobenius endomorphism of $W(\tilde{k})[[w]]$ that is compatible with $\sigma_{\tilde{k}}$ and that takes w into w^p,
- $\widetilde{M}$ is a free $W(\tilde{k})[[w]]$-module of rank r_0 equipped with a $\widetilde{\Phi}$-linear endomorphism $\tilde{\varphi}$,

which have the property that the Newton polygons and the h-numbers of extensions of $(\widetilde{M}, \tilde{\varphi})$ via $W(\tilde{k})$-homomorphisms $W(\tilde{k})[[w]] \to W(K)$ that are compatible with the Frobenius endomorphisms and that involve algebraically closed fields K of characteristic p, are $\mathcal{N}$ and respectively are at most $h_{\mathfrak{C}}$.

We consider the unique $W(\tilde{k})$-monomorphism $W(\tilde{k})[[w]] \hookrightarrow W(\tilde{k}[[w]]^{\mathrm{perf}})$ that lifts the natural inclusion $\tilde{k}[[w]] \hookrightarrow \tilde{k}[[w]]^{\mathrm{perf}}$ and that is compatible with the Frobenius endomorphisms $\widetilde{\Phi}$ and $\Phi_{\tilde{k}[[w]]^{\mathrm{perf}}}$, cf. [22, p. 145]; it maps w into $(w, 0, 0, \ldots) \in W(\tilde{k}[[w]]^{\mathrm{perf}})$.

The results [22, 2.6.1, 2.6.2, 2.7.1, and 2.7.4] hold as well in the context of pairs of the form $(\widetilde{M}, \tilde{\varphi})$ that are not endowed with connections (one only has to disregard all details of loc. cit. that pertain to connections). So as in the proof of 6.1.2 we argue that there exists a number $l \in \mathbf{N}$ which has the properties that $l \geqslant \max\{h_0 r_0^2, h_{\mathfrak{C}}\}$ and that for any quadruple $(\tilde{k}, \widetilde{\Phi}, \widetilde{M}, \tilde{\varphi})$ as above, there exists a monomorphism

$$\left(M_0 \otimes_{\mathbf{Z}_p} W(\tilde{k}[[w]]^{\mathrm{perf}}), \varphi_0 \otimes \Phi_{\tilde{k}[[w]]^{\mathrm{perf}}}\right) \hookrightarrow \left(\widetilde{M} \otimes_{W(\tilde{k})[[w]]} W(\tilde{k}[[w]]^{\mathrm{perf}}), \tilde{\varphi} \otimes \Phi_{\tilde{k}[[w]]^{\mathrm{perf}}}\right)$$

whose cokernel is annihilated by p^l. Let $m := 8l + \tilde{n} + v + 1$ and $\tilde{m} := m + 2v$.

Let $(O, \varphi_O) := \mathrm{proj}\lim_{t \in \mathbf{N}} \mathbf{E}(\mathfrak{C}; W_t(S))$. As the underlying R-module of the object $\mathbf{E}(\mathfrak{C}; W_1(S))$ is free, O is a free $W(R)$-module of rank r_0. Moreover φ_O is a Φ_R-linear endomorphism of O. As R is perfect, the $W_t(R)$-module of differentials $\Omega_{W_t(R)}$ is trivial. So the connection on O induced by $\mathfrak{C}$ is trivial. From this and [22, p. 145] we get that the pair (O, φ_O) determines $\mathfrak{C}$ up to isomorphism. Let $\mathcal{B} = \{e_1, \ldots, e_{r_0}\}$ be a $W(R)$-basis of O. Let $B \in M_{r_0 \times r_0}(W(R))$ be the matrix representation of φ_O with respect to $\mathcal{B}$. Let $B_{\tilde{m}} \in M_{r_0 \times r_0}(W_{\tilde{m}}(R))$ be B mod $p^{\tilde{m}}$. Let R^0 be a finitely generated $\mathbf{F}_p$-subalgebra of R which contains the components of the Witt vectors of length $\tilde{m}$ with coefficients in R that are entries of $B_{\tilde{m}}$; so $B_{\tilde{m}} \in M_{r_0 \times r_0}(W_{\tilde{m}}(R^0))$. Let $S^0 := \mathrm{Spec}(R^0)$.

Let φ'_O be a Φ_R-linear endomorphism of O whose matrix representation with respect to $\mathcal{B}$ is a matrix $B' \in M_{r_0 \times r_0}(W(R^0)) \subseteq M_{r_0 \times r_0}(W(R))$ that lifts $B_{\tilde{m}}$. Let $\mathfrak{C}'_S$ be the F-crystal over S that corresponds to the pair (O, φ'_O), cf. the above part that refers to [22, p. 145]. As $B' \in M_{r_0 \times r_0}(W(R^0))$, loc. cit. also implies that $\mathfrak{C}'_S$ is the pullback to S of an F-crystal $\mathfrak{C}'$ over $\mathrm{Spec}(R^{0\,\mathrm{perf}})$. As B and B' are congruent mod $p^{\tilde{m}}$, we can identify $\mathfrak{C}/p^{\tilde{m}}\mathfrak{C}$ with $\mathfrak{C}'_S/p^{\tilde{m}}\mathfrak{C}'_S$. It is easy to see that due to this identification and to (i), the two Newton polygon stratifications $\mathcal{S}(\mathfrak{C})$ and $\mathcal{S}(\mathfrak{C}'_S)$ of S coincide. Thus to prove that U is affine we can assume that $B = B'$, $R = R^{0\,\mathrm{perf}}$, and $\mathfrak{C} = \mathfrak{C}'$. As $R = R^{0\,\mathrm{perf}}$, there exists a unique open subscheme U^0 of S^0 such that we have $U = U^0 \times_{S^0} S$.

To prove that U is affine, it suffices to show that U^0 is affine. The scheme U^0 is affine if and only if its intersection with any irreducible component C^0 of S^0 is affine, cf. [16, Ch. II, Cor. (6.7.3)]. Thus by replacing (S^0, S) with $(C^0, C^{0\mathrm{perf}})$, we can assume that both S^0 and S are integral schemes. By replacing S^0 and S with their normalizations (cf. 2.9.2), we can also assume that S^0 is a normal $\mathrm{Spec}(\mathbf{F}_p)$-scheme of finite type.

As $B_{\tilde{m}} \in M_{r_0 \times r_0}(W_{\tilde{m}}(R^0))$, for any $j \in S(1, \tilde{m})$ and for every S^0-scheme S_1 we can speak about the object $\mathbf{E}(\mathfrak{C}; W_j(S_1))$ of $\mathcal{M}(W_j(S_1))$ whose underlying $\mathcal{O}_{W_j(S_1)}$-module is the free $\mathcal{O}_{W_j(S_1)}$-module that has $\mathcal{B}$ as an $\mathcal{O}_{W_j(S_1)}$-basis and whose underlying Frobenius endomorphism has a matrix representation with respect to $\mathcal{B}$ which is the natural image of $B_{\tilde{m}}$ in $M_{r_0 \times r_0}(\mathcal{O}_{W_j(S_1)})$. If S_1 is an S-scheme, then $\mathbf{E}(\mathfrak{C}; W_j(S_1))$ is precisely the object of $\mathcal{M}(W_j(S_1))$ defined in 2.8.2.

Let V^0 be an arbitrary local ring of U^0 that is a discrete valuation ring. Let w_0 be a uniformizer of it. Let V_3^0 be a V^0-algebra that is a complete discrete valuation ring, that has w_0 as a uniformizer, and that has an algebraically closed residue field k_3. So V_3^0 is isomorphic to $k_3[[w_0]]$, with w_0 viewed as a variable. We identify $w_0^{p^{-\tilde{m}}}$ with a uniformizer of $V_2^0 := V_3^{0(p^{\tilde{m}})}$. So $k_2 := k_3^{(p^{\tilde{m}})}$ is the residue field of V_2^0. Let $V_1^0 := k_2[[w_0^{p^{-\tilde{m}}}]]^{\mathrm{perf}} = V_2^{0\,\mathrm{perf}}$. For $j \in S(1, \tilde{m})$ let $W_j^0 := W(k_2)[[w_0^{p^{-j}}]]$ be endowed with the Frobenius endomorphism $\Phi_{W_j^0}$ that is compatible with σ_{k_2} and that takes $w_0^{p^{-j}}$ into $w_0^{p^{-j+1}}$. Let $f_j^0 : W_j^0 \hookrightarrow W(k_2[[w_0^{p^{-j}}]])$ be the $W(k_2)$-monomorphism that lifts the canonical identification $k_2[[w_0^{p^{-j}}]] = W_1(k_2[[w_0^{p^{-j}}]])$ and that takes $w_0^{p^{-j}}$ into the Witt vector $(w_0^{p^{-j}}, 0, 0, \ldots) \in W(k_2[[w_0^{p^{-j}}]])$. The following two properties hold:

(ii) each f_j^0 is compatible with Frobenius endomorphisms, and

(iii) if $j < \tilde{m}$, the restriction of f_{j+1}^0 to the $W(k_0)$-subalgebra W_j^0 of W_{j+1}^0 is f_j^0.

We recall that if $x = (x_0, x_1, \ldots, x_{\tilde{m}})$ is a Witt vector of length $\tilde{m}$, then $px = (0, x_0^p, x_1^p, \ldots, x_{\tilde{m}-1}^p)$. Based on this and (ii) and (iii), by induction on $j \in S(1, \tilde{m})$ we get that the image (via the natural monomorphism $R^0 \hookrightarrow k_2[[w_0^{p^{-j}}]]$) of the matrix $B = B' \in M_{r_0 \times r_0}(W(R^0))$ in $M_{r_0 \times r_0}(W_j(k_2[[w_0^{p^{-j}}]]))$, belongs to $M_{r_0 \times r_0}(W_j^0/p^j W_j^0)$. Thus the image of $B = B'$ in $M_{r_0 \times r_0}(W_{\tilde{m}}(k_2[[w_0^{p^{-\tilde{m}}}]]))$, belongs to $M_{r_0 \times r_0}(W_{\tilde{m}}^0/p^{\tilde{m}} W_{\tilde{m}}^0)$ and so it lifts to a matrix $\widetilde{B} \in M_{r_0 \times r_0}(W_{\tilde{m}}^0)$.

Let $\widetilde{M} := \bigoplus_{i=1}^{r_0} W_{\tilde{m}}^0 e_i$. Let $\tilde{\varphi}$ be the $\Phi_{W_{\tilde{m}}^0}$-linear endomorphism of $\widetilde{M}$ whose matrix representation with respect to $\mathcal{B}$ is $\widetilde{B}$. The extension of $(\widetilde{M}, \tilde{\varphi})$ via a $W(k_2)$-homomorphism $W_{\tilde{m}}^0 \to W(K)$ compatible with Frobenius endomorphisms, has the h-number at most $h_{\mathfrak{C}}$ (as $\tilde{m} > h_{\mathfrak{C}}$) and has Newton polygon $\mathcal{N}$ (cf. (i) and the fact that V^0 is a local ring of U^0). So there exists a monomorphism

$$\left(M_0 \otimes_{\mathbf{Z}_p} W(V_1^0), \varphi_0 \otimes \Phi_{V_1^0}\right) \hookrightarrow \left(\widetilde{M} \otimes_{W_{\tilde{m}}^0} W(V_1^0), \tilde{\varphi} \otimes \Phi_{V_1^0}\right)$$

whose cokernel is annihilated by p^l, cf. the choice of l (applied with $k_2[[w_0^{p^{-\tilde{m}}}]]$ instead of $\tilde{k}[[w]]$). Thus there exists a morphism $\mathbf{E}(\mathfrak{C}_0; W_{\tilde{m}}(V_1^0)) \to \mathbf{E}(\mathfrak{C}; W_{\tilde{m}}(V_1^0))$ of $\mathcal{M}(W_{\tilde{m}}(V_1^0))$ whose cokernel is annihilated by p^l.

As in Sections 6.1.3 to 6.1.7 we only used evaluation functors $\mathbf{E}$ and pullbacks of F-crystals over S via geometric points of S and as for any algebraically closed field K the map $S(K) \to S^0(K)$ is bijective, the rest of the proof that U^0 is affine is the same as in Sections 6.1.3 to 6.1.7 (but with the role of (n, m) being replaced with the one of $(\tilde{n}, \tilde{m})$). We will only add two extra sentences.

From 2.8.3(c) (applied with q replaced by $\tilde{m}$) we get that there exist:

(iv) an open subscheme $U^0_{\widetilde{V}^0}$ of the normalization of U^0 in a finite field extension k_{S^0,V^0} of the field of fractions k_{S^0} of S^0, a local ring $\widetilde{V}^0$ of $U^0_{\widetilde{V}^0}$ which dominates V^0, and a morphism $i_{U^0_{\widetilde{V}^0}}(\tilde{m})\colon \mathbf{E}(\mathfrak{C}_0; W_{\tilde{m}}(U^0_{\widetilde{V}^0})) \to \mathbf{E}(\mathfrak{C}; W_{\tilde{m}}(U^0_{\widetilde{V}^0}))$ of $\mathcal{M}(W_{\tilde{m}}(U^0_{\widetilde{V}^0}))$ whose cokernel is annihilated by p^l.

In connection with the last two paragraphs of 6.1.3 and with Sections 6.1.4 to 6.1.7, we only have to add an upper right index 0 to all schemes that (modulo the two operations of 6.1.1) are about to be introduced; thus we get open subschemes $U^0_{V^0}$, U^0_i, and U^0_0 of U^0, etc. This ends the proof of 1.6.

6.3. *Remarks*. – (a) Let S be an integral, locally noetherian scheme. Let $\mathfrak{C}$ and $\mathcal{S}(\mathfrak{C})$ be as in the beginning of Section 6. Let U be the unique stratum of $\mathcal{S}(\mathfrak{C})$ which is an open subscheme of S. The open embedding $U \hookrightarrow S$ is an affine morphism, cf. 6.1. This implies that either $U = S$ or $S^{\text{top}} \setminus U^{\text{top}}$ is of pure codimension 1 in S^{top}. It suffices to check this statement under the extra assumptions that (to be compared with the first paragraph of the proof of 6.1) S is also local, complete, and normal and that $S^{\text{top}} \setminus U^{\text{top}}$ has pure codimension $c \in \mathbf{N}$ in S^{top}. If $c > 1$, then by applying 2.9.1 to the affine, birational open embedding $U \hookrightarrow S$ we get that $U = S$. Thus c must be 1.

Thus 6.1 implies the following result of de Jong and Oort (see [10, 4.1]): if S is a local, integral, noetherian ring and if U contains the complement in S of the closed point of S, then either the dimension of S is at most 1 or $S = U$. The converse of this implication holds, provided our scheme S is locally factorial. But in general the result of de Jong and Oort does not imply 6.1. This is so as there exist integral, normal, noetherian, affine schemes $S = \text{Spec}(R)$ that have a prime Weil divisor C such that the open subscheme $S \setminus C$ of S is not an affine scheme. Here is one classical example.

Let $R := k[x_1, x_2, x_3, x_4]/(x_1 x_4 - x_2 x_3)$. Let $C := \text{Spec}(k[x_1, x_3])$ be the irreducible divisor of S defined by the equations $x_4 = x_2 = 0$. The open subscheme $S \setminus C$ of S is the union of $\text{Spec}(R[\frac{1}{x_2}])$ and $\text{Spec}(R[\frac{1}{x_4}])$ and thus its R-algebra of global functions is $R[\frac{1}{x_2}] \cap R[\frac{1}{x_4}]$. But $W := \text{Spec}(R[\frac{1}{x_2}] \cap R[\frac{1}{x_4}])$ is an affine S-scheme whose fibre over the point of S defined by $x_1 = x_2 = x_3 = x_4 = 0$ is non-empty. Thus the natural morphism $S \setminus C \to W$ is not an isomorphism and so the scheme $S \setminus C$ is not affine.

(b) Let (M, φ) be an F-crystal over a perfect field k of characteristic p. It is easy to see that [22, 1.4 and 1.5] implies the existence of a number $n_0 \in \mathbf{N}$ such that for any $g \in \mathbf{GL}_M(W(k))$ the Newton polygon of $(M, g\varphi)$ depends only on $g \bmod p^{n_0}$. For instance, if $k = \bar{k}$ we can take n_0 to be the number n_{fam} of 3.1.5 for $G = \mathbf{GL}_M$. One can use this (in a way similar to the first part of 6.2) to define Newton polygon stratifications for reductions modulo adequate powers of p of F-crystals over reduced $\text{Spec}(\mathbf{F}_p)$-schemes.

For instance, it can be easily checked starting from 1.3 and [21, 4.4(e)] that any truncated Barsotti–Tate group $\mathcal{G}_S$ of level $T(r, d)$ over a reduced $\text{Spec}(\mathbf{F}_p)$-scheme S which has height r and relative dimension d, defines a stratification $\mathcal{S}(\mathcal{G}_S)$ of S as follows. The association $\mathcal{G}_S \to \mathcal{S}(\mathcal{G}_S)$ is uniquely determined by the following two properties:

(i) it is functorial with respect to pullbacks, and

(ii) if there exists a p-divisible group $\mathcal{D}_S$ over S such that $\mathcal{D}_S[p^{T(r,d)}]$ is isomorphic to $\mathcal{G}_S$, then $\mathcal{S}(\mathcal{G}_S)$ is the Newton polygon stratification of S defined by the F-crystal over S that is associated naturally to $\mathcal{D}_S$.

REFERENCES

[1] BOREL A., Linear Algebraic Groups, Graduate Texts in Math., vol. **126**, Springer, Berlin, 1991.

[2] BOSCH S., LÜTKEBOHMERT W., RAYNAUD M., Néron Models, Ergeb. Math. Grenzgeb. (3), vol. **21**, Springer, Berlin, 1990.

[3] CONWAY J.H., CURTIS R.T., NORTON S.P., PARKER R.A., WILSON R.A., Atlas of Finite Groups, Oxford University Press, Eynsham, 1985, xxxiv+252 pp.

[4] CREMONA J.E., Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1992.

[5] DEMAZURE M., Lectures on p-Divisible Groups, Lecture Notes in Math., vol. **302**, Springer, Berlin, 1972.

[6] DEMAZURE M., GROTHENDIECK A., et al., Schémas en groupes, vols. I–III, Lecture Notes in Math., vols. **151–153**, Springer, Berlin, 1970.

[7] DIEUDONNÉ J., Groupes de Lie et hyperalgèbres de Lie sur un corps de caractérisque $p > 0$ (IV), *Amer. J. Math.* **77** (1955) 429–452.

[8] DE JONG J., Finite locally free group schemes in characteristic p and Dieudonné modules, *Invent. Math.* **114** (1) (1993) 89–137.

[9] DE JONG J., Crystalline Dieudonné module theory via formal and rigid geometry, *Inst. Hautes Études Sci. Publ. Math.* **82** (1995) 5–96.

[10] DE JONG J., OORT F., Purity of the stratification by Newton polygons, *J. Amer. Math. Soc.* **13** (1) (2000) 209–241.

[11] FALTINGS G., Crystalline cohomology and p-adic Galois representations, in: *Algebraic Analysis, Geometry, and Number Theory, Baltimore, MD, 1988*, Johns Hopkins University Press, Baltimore, MD, 1989, pp. 25–80.

[12] FALTINGS G., Integral crystalline cohomology over very ramified valuation rings, *J. Amer. Math. Soc.* **12** (1) (1999) 117–144.

[13] FALTINGS G., CHAI C.-L., Degeneration of Abelian Varieties, Ergeb. Math. Grenzgeb. (3), vol. **22**, Springer, Berlin, 1990.

[14] FONTAINE J.-M., Groupes p-divisibles sur les corps locaux, J. Astérisque, vol. **47/48**, Soc. Math. de France, Paris, 1977.

[15] FONTAINE J.-M., LAFFAILLE G., Construction de représentations p-adiques, *Ann. Sci. École Norm. Sup.* **15** (4) (1982) 547–608.

[16] GROTHENDIECK A., Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphisms, Inst. Hautes Études Sci. Publ. Math., vol. **11**, 1961.

[17] GROTHENDIECK A., Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents, Première partie, Inst. Hautes Études Sci. Publ. Math., vol. **11**, 1963.

[18] GROTHENDIECK A., Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schéma, Inst. Hautes Études Sci. Publ. Math., vol. **20**, 1964, vol. **24**, 1965, vol. **28**, 1996, and vol. **32**, 1967.

[19] GROTHENDIECK A., Groupes de Barsotti–Tate et cristaux de Dieudonné, Sém. Math. Sup., vol. **45**, (1970), Les presses de l'Université de Montréal, Montréal, Quebec, 1974.

[20] HELGASON S., Differential Geometry, Lie Groups, and Symmetric Spaces, Academic Press, New York, 1978.

[21] ILLUSIE L., Déformations des groupes de Barsotti–Tate (d'après A. Grothendieck), in: *Seminar on Arithmetic Bundles: The Mordell Conjecture, Paris, 1983/84*, in: J. Astérisque, vol. **127**, Soc. Math. de France, Paris, 1985, pp. 151–198.

[22] KATZ N., Slope filtration of F-crystals, in: *Journées de Géométrie Algébrique de Rennes, Rennes, 1978, vol. I*, in: J. Astérisque, vol. **63**, Soc. Math. de France, Paris, 1979, pp. 113–163.

[23] KATZ N., Serre–Tate local moduli, in: *Algebraic Surfaces Orsay, 1976–1978*, in: Lecture Notes in Math., vol. **868**, Springer, Berlin, 1981, pp. 138–202.

[24] KOTTWITZ R.E., Isocrystals with additional structure, *Comp. Math.* **56** (2) (1985) 201–220.

[25] KOTTWITZ R.E., Points on some Shimura varieties over finite fields, *J. Amer. Math. Soc.* **5** (2) (1992) 373–444.

[26] KRAFT, H., Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten), *Manuscript*, Univ. Bonn, 1975, 86 p.

[27] LI K.-Z., OORT F., Moduli of Supersingular Abelian Varieties, Lecture Notes in Math., vol. **1680**, Springer, Berlin, 1998.

[28] MANIN J.I., The theory of formal commutative groups in finite characteristic, *Russian Math. Surveys* **18** (6) (1963) 1–83.

[29] MATSUMURA H., Commutative Algebra, second ed., Benjamin/Cummings, Reading, MA, 1980.

[30] MESSING W., The Crystals Associated to Barsotti–Tate Groups, with Applications to Abelian Schemes, Lecture Notes in Math., vol. **264**, Springer, Berlin, 1972.

[31] MILNE J.S., The points on a Shimura variety modulo a prime of good reduction, in: *The Zeta Functions of Picard Modular Surfaces*, Univ. Montréal Press, Montréal, Quebec, 1992, pp. 153–255.

[32] MUMFORD D., Abelian Varieties, Tata Inst. of Fund. Research Studies in Math., vol. **5**, Tata Institute of Fundamental Research, Oxford University Press, Bombay, London, 1970, viii+242 pp. (Reprinted 1988).

[33] MUMFORD D., FOGARTY J., KIRWAN F., Geometric Invariant Theory, third ed., Ergeb. Math. Grenzgeb. (2), vol. **34**, Springer, Berlin, 1994.

[34] OORT F., A stratification of a moduli space of abelian varieties, in: *Moduli of Abelian Varieties, Texel Island, 1999*, in: Progr. Math., vol. **195**, Birkhäuser, Basel, 2001, pp. 345–416.

[35] OORT F., Newton polygon strata in the moduli space of abelian varieties, in: *Moduli of Abelian Varieties, Texel Island, 1999*, in: Progr. Math., vol. **195**, Birkhäuser, Basel, 2001, pp. 417–440.

[36] OORT F., Foliations in moduli spaces of abelian varieties, *J. Amer. Math. Soc.* **17** (2) (2004) 267–296.

[37] RAPOPORT M., RICHARTZ M., On the classification and specialization of F-isocrystals with additional structure, *Comp. Math.* **103** (2) (1996) 153–181.

[38] SERRE J.-P., Galois Cohomology, Springer, Berlin, 1997.

[39] TATE J., Classes d'isogénie des variétés sur un corps fini (d'après J. Honda), in: *Sém. Bourbaki 1968/69, Exp. 352*, in: Lecture Notes in Math., vol. **179**, Springer, Berlin, 1971, pp. 95–110.

[40] VASIU A., Integral canonical models of Shimura varieties of preabelian type, *Asian J. Math.* **3** (2) (1999) 401–518.

[41] ZINK T., On the slope filtration, *Duke Math. J.* **109** (1) (2001) 79–95.

[42] WINTENBERGER J.-P., Un scindage de la filtration de Hodge pour certaines variétés algebriques sur les corps locaux, *Ann. of Math. (2)* **119** (3) (1984) 511–548.

Adrian VASIU
University of Arizona,
Department of Mathematics,
617 N. Santa Rita, PO Box 210089,
Tucson, AZ 85721-0089, USA
E-mail: adrian@math.arizona.edu