Symmetry and isogeny properties for Barsotti–Tate groups

Ofer Gabber and Adrian Vasiu

August 27, 2018

ABSTRACT. Let k be a perfect field of characteristic $p > 0$. Let D and E be two Barsotti–Tate groups over k. We show that for $n >> 0$, the dimension $\dim(\boldsymbol{Hom}(D[p^n], E[p^n]))$ is a symmetric isogeneous invariant, i.e., it does not change if D and E are interchanged or replaced by Barsotti–Tate groups D' and E' isogenous to D and E (respectively). The case when D and E have the same dimension and codimension is generalized to the relative context provided by Barsotti–Tate groups over k endowed with a group in the sense of [GV]. Let G be a truncated Barsotti–Tate group of level m over k and let H be a finite commutative group scheme over k annihilated by p^m. We prove that $\dim(\boldsymbol{Hom}(G, H)) = \dim(\boldsymbol{Hom}(H, G))$. We also prove a stronger form of this identity that involves the Grothendieck group of the multiplicative monoid scheme over k associated to the reduced ring scheme $\boldsymbol{End}(G)_{\mathrm{red}} \times_k \boldsymbol{End}(H)^{\mathrm{opp}}_{\mathrm{red}}$.

KEY WORDS: Group schemes, Barsotti–Tate groups, monoids, representations, Lie algebras, rings, categories, Dieudonné modules, quasi-algebraic groups, and proalgebraic groups.

MSC 2010: 11F22, 11G10, 11G18, 14F30, 14G35, 14K10, 14L05, 14L15, 17B45, 20G15, 20M13, and 20M32.

1 Introduction

Let p be a prime and let k be a perfect field of characteristic p. Let G and H be two finite commutative group schemes over k of p power order. Let

$\boldsymbol{Hom}(G,H)$ be the affine group scheme over k of homomorphisms from G to H. Let G^{t} be the Cartier dual of G.

We recall that the a-number of G is $a_G = \dim(\boldsymbol{Hom}(\boldsymbol{\alpha}_p, G))$. Equivalently, a_G is the largest integer such that $\boldsymbol{\alpha}_p^{a_G}$ is a subgroup scheme of G. In general, $a_G \neq a_{G^{\mathrm{t}}}$ (see Subsection 2.1) but it is well known that if G is a truncated Barsotti–Tate group, then we have $a_G = a_{G^{\mathrm{t}}}$ (for instance, see [GV], Subsection 3.5). The goal of the paper is to generalize this last identity in order to get several symmetry and isogeny properties for (truncated) Barsotti–Tate groups over k.

We begin with the case of Barsotti–Tate groups over k. Let D and E be two Barsotti–Tate groups over k. It is known that there exists a smallest nonnegative integer $n_{D,E}$ such that for all integers $n \geq n_{D,E}$ we have

$$\dim(\boldsymbol{Hom}(D[p^n], E[p^n])) = \dim(\boldsymbol{Hom}(D[p^{n_{D,E}}], E[p^{n_{D,E}}])),$$

cf. [GV], Subsection 6.1. Following [LNV], Definition 7.9 we denote

$$s_{D,E} = \dim(\boldsymbol{Hom}(D[p^{n_{D,E}}], E[p^{n_{D,E}}])).$$

In Section 3 we will provide an elementary (group scheme theoretical) proof of the following symmetry and isogeny property.

Theorem 1 *The dimension $s_{D,E}$ is a symmetric isogenous invariant. In other words, if D' and E' are Barsotti–Tate groups over k isogenous to D and E (respectively), then we have $s_{D,E} = s_{E,D} = s_{D',E'}$. Moreover we have the symmetric property $n_{D,E} = n_{E,D}$.*

The case $D = E$ and $D' = E'$ of Theorem 1 (i.e., the equality $s_{D,D} = s_{D',D'}$) was first proved in [V2], Theorem 1.2 (e)] (cf. also [GV], Remark 4.5). We have the following interpretation of $n_{D,E}$ in terms of extensions (cf. [GV], Subsection 6.1]: for $n \in \mathbb{N}$, the homomorphism $\mathrm{Ext}^1(D,E) \to \mathrm{Ext}^1(D[p^n], E[p^n])$ is injective if and only if $n \geq n_{D,E}$. From this and the symmetric property $n_{D,E} = n_{E,D}$ we get:

Corollary 1 *For $n \in \mathbb{N}$ we consider the two homomorphisms of abstract groups $Ext^1(D,E) \to Ext^1(D[p^n], E[p^n])$ and $Ext^1(E,D) \to Ext^1(E[p^n], D[p^n])$. Then one is injective if and only if the other one is injective.*

In Section 4 we will prove the following general symmetric formula.

Theorem 2 *Let m be the smallest positive integer such that p^m annihilates both G and H. We assume that G is a truncated Barsotti–Tate group of level m over k. Then we have*

$$\dim(\boldsymbol{Hom}(G,H)) = \dim(\boldsymbol{Hom}(H,G)). \tag{1}$$

Note that Equation (1) also implies that $s_{D,E} = s_{E,D}$ and $n_{D,E} = n_{E,D}$ and, when combined with [V2], Theorem 1.2 (e), that $s_{D,E} = s_{D',E'}$ (cf. Remark 4.2 (b)). The following proposition (proved in Subsection 4.4 based on the examples of Subsection 4.3)) shows that for $m > 1$ the hypothesis of Theorem 2 is needed in general.

Proposition 1 *Let $m > n > 0$ be integers. Let G be a truncated Barsotti–Tate group of level n over k and let H be a finite commutative group scheme over k annihilated by p^m but not by p^{m-1}. Then the following optimal inequalities hold*

$$\frac{n}{m} \leq \frac{\dim(\boldsymbol{Hom}(G,H))}{\dim(\boldsymbol{Hom}(H,G))} \leq \frac{m}{n}. \tag{2}$$

Moreover, the difference $\dim(\boldsymbol{Hom}(G,H)) - \dim(\boldsymbol{Hom}(H,G))$ *when $m > n$ vary, can be an arbitrary integer.*

For a group scheme Γ over k, let Γ^0 and Γ_{red} be the identity component and the reduced group (respectively) of Γ. Let $\boldsymbol{M}$ be the multiplicative monoid scheme over k associated to the reduced ring scheme

$$\boldsymbol{End}(G)_{\mathrm{red}} \times_k \boldsymbol{End}(H)^{\mathrm{opp}}_{\mathrm{red}} = \boldsymbol{End}(G)_{\mathrm{red}} \times_k \boldsymbol{End}(H^{\mathrm{t}})_{\mathrm{red}}.$$

By a left $\boldsymbol{M}$-module Z (or a representation Z of $\boldsymbol{M}$) we mean a k-vector space Z equipped with a homomorphism ρ_Z from $\boldsymbol{M}$ to the multiplicative monoid scheme over k associated to the ring scheme $\boldsymbol{End}(Z)$. Let σ be the Frobenius automorphism of k. Let $Z^{(\sigma)}$ be the pullback of Z via σ viewed naturally as a left $\boldsymbol{M}$-module; thus $\rho_{Z^{(\sigma)}}$ is the composite of the Frobenius homomorphism $\boldsymbol{M} \to \boldsymbol{M}^{(\sigma)}$ with $(\rho_Z)^{(\sigma)}$.

Let $K_0(\boldsymbol{M})$ be the Grothendieck group of the abelian category of finite dimensional left $\boldsymbol{M}$-modules Z; let $[Z] \in K_0(\boldsymbol{M})$ be the element corresponding to Z. Let $I_0(\boldsymbol{M})$ be the subgroup of $K_0(\boldsymbol{M})$ generated by elements of the form $[Z^{(\sigma)}] - [Z]$ with Z an arbitrary finite dimensional left $\boldsymbol{M}$-module.

Let $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ be the Lie algebras over k of the reduced group schemes $\boldsymbol{Hom}(G,H)_{\mathrm{red}}$ and $\boldsymbol{Hom}(H,G)_{\mathrm{red}}$ (respectively). Let $\boldsymbol{L}_1^{\vee} = \mathrm{Hom}_k(\boldsymbol{L}_1, k)$ be the dual k-vector space. Both $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ are naturally left $\boldsymbol{M}$-modules. For instance, if $(g,h) \in \boldsymbol{M}(k) = \mathbf{End}(G)(k) \times \mathbf{End}(H)^{\mathrm{opp}}(k)$, then we have an endomorphism $c_{g,h} : \boldsymbol{Hom}(H,G)_{\mathrm{red}} \to \boldsymbol{Hom}(H,G)_{\mathrm{red}}$ which maps $l \in \boldsymbol{Hom}(H,G)_{\mathrm{red}}(k)$ to $g \circ l \circ h \in \boldsymbol{Hom}(H,G)_{\mathrm{red}}(k)$ and (g,h) acts on $\boldsymbol{L}_2$ via the Lie differential $\mathrm{Lie}(c_{g,h}) : \boldsymbol{L}_2 \to \boldsymbol{L}_2$ of $c_{g,h}$. We have the following stronger form of Theorem 2 which is proved in Section 5.

Theorem 3 *Let m be the smallest positive integer such that p^m annihilates both G and H. We assume that G is a truncated Barsotti–Tate group of level m over k. Then the images of $[\boldsymbol{L}_1^\vee]$ and $[\boldsymbol{L}_2]$ in $K_0(\boldsymbol{M})/I_0(\boldsymbol{M})$ coincide.*

The kernel of the dimension homomorphism $\dim : K_0(\boldsymbol{M}) \to \mathbb{Z}$ contains $I_0(\boldsymbol{M})$ and thus it induces a dimension homomorphism

$$\dim : K_0(\boldsymbol{M})/I_0(\boldsymbol{M}) \to \mathbb{Z}$$

denoted in the same way. Thus Theorem 3 implies Theorem 2. But we emphasize that the proof of Theorem 3 we present does rely on Theorem 2. Section 2 gathers some preliminary material required in the proofs of Theorems 1 to 3.

The particular case of Theorem 1 in which D and E have the same dimension and codimension is generalized in Section 6 to the relative contexts provided by quadruples of the form $(L,\phi,\vartheta,\mathcal{G})$ and $(L,g\phi,\vartheta g^{-1},\mathcal{G})$, where (L,ϕ,ϑ) and $(L,g\phi,\vartheta g^{-1})$ are the (contravariant) Dieudonné modules of two Barsotti–Tate groups over k, where $\mathcal{G}$ is a smooth integral closed subgroup scheme of $\boldsymbol{GL}_L$ subject to the two axioms of [GV], Section 5, and where $g \in \mathcal{G}(W(k))$. The motivation for all these generalizations stems out from applications to level m stratifications of special fibers of good integral models of Shimura varieties of Hodge type in unramified mixed characteristic $(0,p)$ (see [V2], Section 4).

2 Preliminaries

Let $W(k)$ be the ring of p-typical Witt vectors with coefficients in k. Let $B(k)$ be the field of fractions of $W(k)$. Let $B(k)\{F,F^{-1}\}$ be the noncommutative Laurent polynomial ring and let

$$\mathbb{D} = \mathbb{D}(k) = B(k)\{F,F^{-1}\}/I$$

where I is the two-sided ideal generated by all elements $Fa - \sigma(a)F$ with $a \in B(k)$. Let $V = pF^{-1} \in \mathbb{D}$ and let $\mathbb{E} = \mathbb{E}(k) = W(k)\{F, V\}$ as a subring of $\mathbb{D}$. For $m \in \mathbb{N}^*$, let $W_m(k) = W(k)/p^m W(k)$ and $\mathbb{E}_m = \mathbb{E}_m(k) = \mathbb{E}/p^m\mathbb{E}$. The (contravariant) Dieudonné module of G is a left $\mathbb{E}$-module M which as a $W(k)$-module is torsion and finitely generated. If G is annihilated by p^m, then M is as well a left $\mathbb{E}_m$-module. If G is a truncated Barsotti–Tate group of level m, then M is a free $W_m(k)$-module of finite rank. We have

$$a_G = \dim_k(M/(FM + VM))$$

and

$$a_{G^{\mathrm{t}}} = \dim_k(\mathrm{Ker}(F : M \to M) \cap \mathrm{Ker}(V : M \to M)).$$

2.1 Example with $a_G \neq a_{G^{\mathrm{t}}}$

Let G be such that M is a k-vector space of dimension 3 which has an ordered k-basis (v_1, v_2, v_3) with the properties that $Fv_1 = Fv_2 = Vv_1 = Vv_2 = 0$, $Fv_3 = v_1$, and $Vv_3 = v_2$. Then $a_G = 1$ while $a_{G^{\mathrm{t}}} = 2$.

2.2 Brief review of quasi-algebraic groups over k

Following [S1] we recall several ways to introduce a quasi-algebraic group Q over k. The simplest way is to define Q to be a group object of the category of perfect varieties over k, i.e., of the full subcategory of the category of schemes over k whose objects are perfections of schemes of finite type over k (equivalently are perfections of reduced schemes of finite type). Thus Q can be identified with a covariant functor from the category of commutative perfect k-algebras that are perfections of finitely generated k-algebras into the category of groups which is representable by a perfect variety over k. We also recall that a proalgebraic group over k is a projective limit of quasi-algebraic groups over k (to be compared with [S1], Definition 1 of Subsection 2.1).

Each quasi-algebraic group Q over k is the perfection $\tilde{Q}^{\mathrm{perf}}$ of a group scheme $\tilde{Q}$ over k of finite type (cf. [S1], Proposition 10; the proof of loc. cit. applies in the noncommutative case as well). Obviously $Q = \tilde{Q}^{\mathrm{perf}}$ is a proalgebraic group over k (in the language of [S1], Definition 1 of Subsection 2.1, see also [S1], Example 1) of Subsection 2.1 for the commutative case). Let $\mathcal{Q}$ be the abelian category of commutative quasi-algebraic groups over k (see [S1], Proposition 5).

Fact 1 *Let $f : U_1 \to U_2$ be a morphism of the category $\mathcal{Q}$ and let $\bar{k}$ be an algebraic closure of k. Then the following two statements are equivalent:*

(i) *f is an isomorphism;*

(ii) *the abstract homomorphism $f(\bar{k}) : U_1(\bar{k}) \to U_2(\bar{k})$ is an isomorphism.*

Proof: This follows from the fact that each one of these two statements is equivalent to the third statement that both $\mathrm{Ker}(f)$ and $\mathrm{Coker}(f)$ are trivial.$\Box$

2.3 The χ_p function on prounipotent groups

Until the end of Section 2 we will assume that k is algebraically closed. Let $\mathcal{P}$ be the abelian category of commutative proalgebraic groups over k (see [S1], Proposition 7). Note that $\mathcal{Q}$ is a full subcategory of $\mathcal{P}$. We have a thick (Serre) subcategory of $\mathcal{P}$ whose objects are finite dimensional proalgebraic groups (those which are projective limits of commutative quasi-algebraic groups of bounded dimension) and on it the dimension function dim (defined in the obvious way) is additive.

We now specialize to commutative prounipotent groups U over k. For each $n \in \mathbb{N}$ we have a natural multiplication by p epimorphism $(p^nU)/(p^{n+1}U) \to (p^{n+1}U)/(p^{n+2}U)$. Thus, if U/pU is finite dimensional, then we have a decreasing sequence $(\dim((p^nU)/(p^{n+1}U)))_{n\in\mathbb{N}}$ of nonnegative integers and therefore there exists a smallest invariant $n_U \in \mathbb{N}$ with the property that the subsequence $(\dim((p^nU)/(p^{n+1}U)))_{n\geq n_U}$ is constant. This gives that the kernel $\mathrm{Ker}(p : p^{n_U}U \to p^{n_U}U)$ is zero dimensional and by a decreasing induction on $i \in \{0, \ldots, n_U\}$ we get that that the kernel $\mathrm{Ker}(p : p^iU \to p^iU)$ is finite dimensional.

The full subcategory of $\mathcal{P}$ whose objects are those commutative prounipotent groups U for which U/pU is finite dimensional is thick and on it the integral valued function defined by the rule

$$\chi_p(U) = \dim(U/pU) - \dim(\mathrm{Ker}(p : U \to U))$$

is additive (cf. snake lemma).

Fact 2 *Let U be a commutative prounipotent group U such that U/pU is finite dimensional. Then $\chi_p(U) \geq 0$. Moreover, the following three statements are equivalent:*

(i) *we have $\chi_p(U) = 0$;*

(ii) *the commutative prounipotent group $p^{n_U}U$ is zero dimensional;*

(iii) *the commutative prounipotent group U is finite dimensional.*

Proof: If U is annihilated by p (i.e., $pU = 0$), then $\chi_p(U) = \dim(U) - \dim(U) = 0$. Based on the additivity of χ_p, a simple induction on $a \in \mathbb{N}^*$ shows that if U is annihilated by p^a (i.e., $p^aU = 0$), then $\chi_p(U) = 0$ and U is finite dimensional.

In general, from the additive equality $\chi_p(U) = \chi_p(U/p^{n_U}U) + \chi_p(p^{n_U}U)$ and from the facts that $\dim(\mathrm{Ker}(p : p^{n_U}U \to p^{n_U}U)) = 0$ (see above) and $\chi_p(U/p^{n_U}U) = 0$ (cf. previous paragraph), we get that

$$\chi_p(U) = \chi_p(p^{n_U}U) = \dim(p^{n_U}U/p^{n_U+1}U) \geq 0.$$

It is clear that (ii) implies (iii). If (iii) holds, then the constant sequence $(\dim((p^nU)/(p^{n+1}U)))_{n\geq n_U}$ has constant value 0 and therefore $\chi_p(U) = 0$, i.e., (i) holds. If (i) holds, then the endomorphism $p : p^{n_U}U \to p^{n_U}U$ has zero dimensional cokernel and it is easy to see that this implies that the identity component of $p^{n_U}U$ is trivial. Thus (ii) holds. We conclude that the statements (i) to (iii) are equivalent. $\square$

2.4 Prounipotent groups associated to $W(k)$-modules

Each finitely generated $W(k)$-module M has the structure of a commutative prounipotent group $\underline{M}$ with $\underline{M}/p\underline{M}$ finite dimensional and with

$$\chi_p(\underline{M}) = \dim_{B(k)}(M[\frac{1}{p}]).$$

If $\chi_p(\underline{M}) = 0$ (i.e., if M has finite length), then $\underline{M}$ is a commutative quasi-algebraic group over k which represents the functor that takes the perfection A of a finitely generated commutative k-algebra into the group $W(A)\otimes_{W(k)} M$ and whose dimension is $\mathrm{length}_{W(k)}(M)$.

If X is a finite dimensional $B(k)$-vector space, then we view X as an inductive limit $\underline{X}$ of commutative proalgebraic groups $\underline{L}$ given by lattices L of X (i.e., given by free $W(k)$-submodules L of X of rank equal to $\dim_{B(k)}(X)$).

Definition 1 *We say that a subgroup U of $\underline{X}$ is admissible if and only if there exist lattices L_1 and L_2 of X such that U is a proalgebraic subgroup of $\underline{L_1}$ that contains $\underline{L_2}$ (thus $\underline{L_2} \subset U \subset \underline{L_1}$).*

If U_1 and U_2 are admissible subgroups of $\underline{X}$, we can define the index

$$\chi(U_1, U_2) = \dim(U_1/U_3) - \dim(U_2/U_3) \in \mathbb{Z}$$

for each admissible subgroup U_3 of $\underline{X}$ contained in both U_1 and U_2; this generalizes the definition $\chi(L_1/L_2)$ for lattices L_1 and L_2 of X which was introduced in [S2] and which equals $\chi(\underline{L_1}, \underline{L_2})$. Note that $\chi(U_1, U_2) = -\chi(U_2, U_1)$. For four lattices L_1, L_2, L_3, and L_4 of X we also have the following interchanging identity

$$\chi(\underline{L_1}, \underline{L_2}) - \chi(\underline{L_3}, \underline{L_4}) = \chi(\underline{L_1}, \underline{L_3}) - \chi(\underline{L_2}, \underline{L_4}). \tag{3}$$

Example 1 *Let U be an admissible subgroup of $\underline{X}$, let L be a lattice of X, and let $n \in \mathbb{N}$. Then $\chi(U, \underline{L}) = \chi(p^n U, p^n \underline{L})$ and $\chi(U, p^n U) = n \dim_{B(k)}(X)$. To check this last formula, we note that as $\chi(p^n \underline{L}, p^n U) = -\chi(U, \underline{L})$ and $\chi(U, p^n U) = \chi(U, \underline{L}) + \chi(\underline{L}, p^n \underline{L}) + \chi(p^n \underline{L}, p^n U)$, we compute directly that $\chi(U, p^n U) = \chi(\underline{L}, p^n \underline{L}) = \dim(\underline{L}/p^n \underline{L}) = \mathit{length}_{W(k)}(L/p^n L) = n \dim_{B(k)}(X)$.*

Let $T : X \to X'$ be a homomorphism between the underlying abelian groups of two finite dimensional $B(k)$-vector spaces. We say that T is proalgebraic if and only if it comes from a proalgebraic homomorphism between lattices $T_0 : \underline{L} \to \underline{L'}$, i.e., we have

$$T = X \to X' = T_0(k) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}] : L \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}] \to L' \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}].$$

If T is proalgebraic, we get an inductive homomorphism

$$\underline{T} : \underline{X} \to \underline{X'} = T_0 \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}] : \underline{L} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}] \to \underline{L'} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}]$$

which will be also called proalgebraic.

If T is proalgebraic, we consider for each $n \in \mathbb{N}^*$ the kernel of $(T_0 \bmod p^n) : \underline{L}/p^n \underline{L} \to \underline{L'}/p^n \underline{L'}$. The images in $\underline{L}/p\underline{L}$ of such kernels form a decreasing sequence of quasi-algebraic subgroups, and thus they become constant for $n \geq n_1$ for some $n_1 \in \mathbb{N}^*$, with constant value equal to the image in $\underline{L}/p\underline{L}$ of $\mathrm{Ker}(T_0)$ (we recall that filtered inverse limits are exact in our abelian category $\mathcal{P}$ of commutative proalgebraic groups, cf. [S1], Subsection 2.3). Then $p^{n_1-1} \mathrm{Coker}(T_0)$ is torsion free. Based on this, it is easy to see that the following three statements are equivalent:

(i) the homomorphism T is surjective;

(ii) the cokernel $\mathrm{Coker}(T_0)$ is killed by a power of p;

(iii) the cokernel $\mathrm{Coker}(T_0)$ is finite dimensional.

Definition 2 *Let $T : X \to X'$ be a proalgebraic homomorphism between the underlying groups of two finite dimensional $B(k)$-vector spaces. We say that $T : X \to X'$ (or $\underline{T} : \underline{X} \to \underline{X'}$) is admissible if and only if it comes from a proalgebraic homomorphism between lattices $T_0 : \underline{L} \to \underline{L'}$ whose kernel $Ker(T_0)$ and cokernel $\mathrm{Coker}(T_0)$ are finite dimensional (this is independent of the choice of lattices L and L').*

We note that the finite dimensionality of $\mathrm{Ker}(T_0)$ means that $\mathrm{Ker}(T_0)$ is a free finitely generated $\mathbb{Z}_p$-module. Moreover, if T is admissible, then T is surjective.

The additivity of the function χ_p gives that

$$\chi_p(\mathrm{Ker}(T_0)) - \chi_p(\mathrm{Coker}(T_0)) = \chi_p(\underline{L}) - \chi_p(\underline{L'}) = \dim_{B(k)}(X) - \dim_{B(k)}(X').$$

Thus if the $B(k)$-vector spaces X and X' have the same dimension, then $\chi_p(\mathrm{Ker}(T_0)) = \chi_p(\mathrm{Coker}(T_0))$ and from Fact 2 we get that the finite dimensionality of $\mathrm{Ker}(T_0)$ is equivalent to the finite dimensionality of $\mathrm{Coker}(T_0)$.

Example 2 *If i and j are distinct integers, $f : X \to X'$ is a σ^i-linear map and $g : X \to X'$ is a σ^j-linear map, then using the Dieudonné–Manin classification of σ^a-F-isocrystals over k with $a \in \{i-j, j-i\} \subset \mathbb{Z} \setminus \{0\}$ we easily get that if either f or g is invertible (thus X and X' have the same dimension), then for each lattice L of X the image $(\underline{f+g})(\underline{L})$ is an admissible subgroup of $\underline{X'}$ and therefore $\underline{f+g}$ is admissible.*

Lemma 1 *Let $\underline{T} : \underline{X} \to \underline{X'}$ be admissible. Let U_1 and U_2 (resp. U_1' and U_2') be admissible subgroups of $\underline{X}$ (resp. of $\underline{X'}$). Then the following three properties hold:*

(a) *we have $\chi(U_2', \underline{T}(U_2)) - \chi(U_1', \underline{T}(U_1)) = \chi(U_2', U_1') - \chi(U_2, U_1)$ and therefore if $\chi(U_2', U_1') = \chi(U_2, U_1)$, then $\chi(U_2', \underline{T}(U_2)) = \chi(U_1', \underline{T}(U_1))$;*

(b) *we have $\dim_{B(k)}(X) = \dim_{B(k)}(X')$;*

(c) *if $\underline{T}(U) \subset U'$, then for large n the kernel of the induced map $U/p^nU \to U'/p^nU'$ has dimension equal to $\dim(U'/\underline{T}(U))$.*

Proof: As $\underline{T}$ is admissible, there exists an admissible subgroup U_3 of $\underline{X}$ contained in both U_1 and U_2 and such that $\underline{T}(U_3)$ is an admissible subgroup of $\underline{X'}$ contained in both U_1' and U_2'. Then $\chi(U_2', \underline{T}(U_2)) - \chi(U_1', \underline{T}(U_1)) = \dim(U_2'/\underline{T}(U_3)) - \dim(\underline{T}(U_2)/\underline{T}(U_3)) - \dim(U_1'/\underline{T}(U_3)) + \dim(\underline{T}(U_1)/\underline{T}(U_3))$ is equal to the difference between $\dim(U_2'/\underline{T}(U_3)) - \dim(U_1'/\underline{T}(U_3))$ and $\dim(\underline{T}(U_2)/\underline{T}(U_3)) - \dim(\underline{T}(U_1)/\underline{T}(U_3))$ and thus to the difference $\chi(U_2', U_1') - \chi(\underline{T}(U_2), \underline{T}(U_1))$. But as $\underline{T}$ is admissible, it is surjective and $\mathrm{Ker}(T_0)$ is a free finitely generated $\mathbb{Z}_p$-module and these two properties imply that we have

$$\chi(\underline{T}(U_2), \underline{T}(U_1)) = \chi(U_2, U_1) \tag{4}$$

and thus that (a) holds.

By taking $U_1 = pU_2$ in the Equation (4), from Example 1 applied with $n = 1$ we get that (b) holds.

To check (c), let $n_2 \in \mathbb{N}^*$ be such that p^{n_2} annihilates $U'/\underline{T}(U)$. Thus for $n \geq n_2$ we have $p^n U' \subset \underline{T}(U)$ as well as two short exact sequences

$$0 \to \mathrm{Ker}(U/p^nU \to U'/p^nU') \to U/p^nU \to \underline{T}(U)/p^nU' \to 0$$

and $0 \to \underline{T}(U)/p^nU' \to U'/p^nU' \to U'/\underline{T}(U) \to 0$. This implies that the dimension of $\mathrm{Ker}(U/p^nU \to U'/p^nU')$ is equal to the expression $\dim(U'/T(U)) + \dim(U/p^nU) - \dim(U'/p^nU')$. Based on (b) and Example 1, this expression is equal to $\dim(U'/T(U))$ and thus part (c) holds as well. $\square$

3 Proof of Theorem 1

To prove Theorem 1 we can assume that k is algebraically closed.

3.1 The isogeny invariance of $s_{D,E}$

Let L and J be the (contravariant) Dieudonné modules of D and E. We recall that the dual E^{t} of E has Dieudonné module $J^\vee = \mathrm{Hom}_{W(k)}(J, W(k))$ with F and V acting on $h \in J^\vee$ via the rules: $Fh(x) = \sigma(h(Vx))$ and $Vh(x) = \sigma^{-1}(h(Fx))$ for all $x \in J$.

Let $\mathrm{Hom}_{W(k)}(J, L)^\flat$ be the sublattice of $\mathrm{Hom}_{W(k)}(J, L)$ formed by $W(k)$-linear maps that send VJ to VL. We note that

$$\mathrm{Hom}_{W(k)}(J, L)^\flat = \mathrm{Hom}_{W(k)}(J, L) \cap \mathrm{Hom}_{W(k)}(VJ, VL)$$

is the largest sublattice of $\mathrm{Hom}_{W(k)}(J,L)$ for which we have a homomorphism of prounipotent groups

$$\underline{\Psi_{J,L}} : \underline{\mathrm{Hom}_{W(k)}(J,L)^\flat} \to \underline{\mathrm{Hom}_{W(k)}(J,L)} \tag{5}$$

defined by the abstract homomorphism

$$\Psi_{J,L} : \mathrm{Hom}_{W(k)}(J,L)^\flat \to \mathrm{Hom}_{W(k)}(J,L)$$

that maps $h \in \mathrm{Hom}_{W(k)}(J,L)^\flat$ to $h - \frac{1}{p}FhV$. It induces an admissible proalgebraic endomorphism $\underline{\Psi} : \underline{X} \to \underline{X}$ in the sense of Section 2, where

$$X = \mathrm{Hom}_{B(k)}(J[\frac{1}{p}], L[\frac{1}{p}]) = \mathrm{Hom}_{W(k)}(J,L)^\flat[\frac{1}{p}] = \mathrm{Hom}_{W(k)}(J,L)[\frac{1}{p}]$$

is a $B(k)$-vector space of finite dimension.

The kernel of $\underline{\Psi_{J,L}}$ is the quasi-algebraic group $\underline{\mathrm{Hom}_{\mathbb{E}}(J,L)} = \underline{\mathrm{Hom}(D,E)}$ of Dieudonné module homomorphisms. We check that the kernel of the reduction of $\underline{\Psi_{J,L}}$ modulo p^n is the quasi-algebraic group $\underline{\mathrm{Hom}(D[p^n],E[p^n])}$ of the abstract group

$$\mathrm{Hom}_{\mathbb{E}_n}(J/p^nJ, L/p^nL) = \mathrm{Hom}(D[p^n],E[p^n]) = \boldsymbol{Hom}(D[p^n],E[p^n])(k)$$

of homomorphisms between Dieudonné modules modulo p^n. The crystalline Dieudonné theory provides a natural evaluation homomorphism f from $\underline{\mathrm{Hom}(D[p^n],E[p^n])}$ to the kernel of the reduction of $\underline{\Psi_{J,L}}$ modulo p^n (note that f is a morphism of the abelian category $\mathcal{Q}$). From [LNV], Lemma 8.7 we get that the abstract homomorphism $f(k)$ is an isomorphism and therefore from Fact 1 we get that f itself is an isomorphism.

Let D' and E' be Barsotti–Tate groups over k isogenous to D and E (respectively). Let L' and J' be the (contravariant) Dieudonné modules of D' and E' (respectively). We have identifications $L[\frac{1}{p}] = L'[\frac{1}{p}]$, $J[\frac{1}{p}] = J'[\frac{1}{p}]$, and $X = \mathrm{Hom}_{W(k)}(J',L')[\frac{1}{p}] = \mathrm{Hom}_{W(k)}(J',L')^\flat[\frac{1}{p}]$. Moreover, $\underline{\Psi} : \underline{X} \to \underline{X}$ is also induced by a homomorphism of prounipotent groups

$$\underline{\Psi_{J',L'}} : \underline{\mathrm{Hom}_{W(k)}(J',L')^\flat} \to \underline{\mathrm{Hom}_{W(k)}(J',L')}$$

defined by the same rule as $\Psi_{J,L}$.

Lemma 1 (c) gives information on $\dim(\boldsymbol{Hom}(D[p^n],E[p^n]))$ for large n and thus for all $n \geq n_{D,E}$ we have

$$s_{D,E} = \dim(\underline{\mathrm{Hom}_{W(k)}(J,L)}/\underline{\Psi_{J,L}}(\underline{\mathrm{Hom}_{W(k)}(J,L)^\flat}))$$

and thus also

$$s_{D,E} = \chi(\underline{\mathrm{Hom}_{W(k)}(J,L)}, \underline{\Psi_{J,L}}(\underline{\mathrm{Hom}_{W(k)}(J,L)^\flat})). \tag{6}$$

The dimension of the k-vector space $\mathrm{Hom}_{W(k)}(J,L)/\mathrm{Hom}_{W(k)}(J,L)^\flat$ is the product of the dimension of E and of the codimension of D and thus it is equal to the dimension of the k-vector space $\mathrm{Hom}_{W(k)}(J',L')/\mathrm{Hom}_{W(k)}(J',L')^\flat$. From this equality and the Equation (3) applied with $(L_1, L_2, L_3, L_4) = (\underline{\mathrm{Hom}_{W(k)}(J',L')}, \underline{\mathrm{Hom}_{W(k)}(J,L)}, \underline{\mathrm{Hom}_{W(k)}(J',L')^\flat}, \underline{\mathrm{Hom}_{W(k)}(J,L)^\flat})$ we get that

$$\chi(\underline{\mathrm{Hom}_{W(k)}(J',L')}, \underline{\mathrm{Hom}_{W(k)}(J,L)}) = \chi(\underline{\mathrm{Hom}_{W(k)}(J',L')^\flat}, \underline{\mathrm{Hom}_{W(k)}(J,L)^\flat}). \tag{7}$$

From Formula (7) and Lemma 1 (a) applied with $(\underline{T}, U_1, U_2, U_1', U_2') = (\underline{\Psi}, \underline{\mathrm{Hom}_{W(k)}(J,L)^\flat}, \underline{\mathrm{Hom}_{W(k)}(J',L')^\flat}, \underline{\mathrm{Hom}_{W(k)}(J,L)}, \underline{\mathrm{Hom}_{W(k)}(J',L')})$ we get directly that $\chi(\underline{\mathrm{Hom}_{W(k)}(J',L')}, \underline{\Psi_{J',L'}}(\underline{\mathrm{Hom}_{W(k)}(J',L')^\flat}))$ is equal to $\chi(\underline{\mathrm{Hom}_{W(k)}(J,L)}, \underline{\Psi_{J,L}}(\underline{\mathrm{Hom}_{W(k)}(J,L)^\flat}))$. From this and Formula (6) and its analogue with (J,L) replaced by (J',L') we get that $s_{D,E} = s_{D',E'}$ is an isogeny invariant.

3.2 The symmetry of $s_{D,E}$

In this subsection we will prove that $s_{D,E} = s_{E,D}$ using Serre duality for unipotent connected commutative quasi-algebraic groups (see [S1], [B], and [BD], Section 3). We recall that Serre duality is an involutory antiequivalence of the category of unipotent connected commutative quasi-algebraic groups which preserves dimensions and short exact sequences and thus also finite direct sums (for instance, see [B], Proposition 1.2.1).

We also recall that for a finitely generated $W_m(k)$-module M and its dual $M^\vee = \mathrm{Hom}_{W_m(k)}(M, W_m(k))$, the Serre dual of $\underline{M}$ is $\underline{M^\vee}$ in a functorial way with respect to all σ^a-linear maps with $a \in \mathbb{Z}$ (cf. [S1], Subsection 8.4, Proposition 4 and Lemma 2).

Lemma 2 *Let $f : U_1 \to U_2$ be a homomorphism between unipotent connected commutative quasi-algebraic groups of the same finite dimension. Then the dimension of the kernel of f is equal to the dimension of the kernel of the Serre dual $f^* : U_2^* \to U_1^*$ of f. In particular, f is an isogeny if and only if f^* is an isogeny.*

Proof: We have short exact sequences $0 \to \operatorname{Ker}(f)^0 \to U_1 \to U_1/\operatorname{Ker}(f)^0 \to 0$ and $0 \to \operatorname{Im}(f) \to U_2 \to U_2/\operatorname{Im}(f) \to 0$ as well as a natural isogeny $U_1/\operatorname{Ker}(f)^0 \to \operatorname{Im}(f)$. As U_1 and U_2 have the same dimension, we get that $\operatorname{Ker}(f)^0$ and $U_2/\operatorname{Im}(f)$ have the same dimensions. As Serre duality preserves short exact sequences, $(U_2/\operatorname{Im}(f))^*$ is a subgroup of U_2^* contained in $\operatorname{Ker}(f^*)$. As Serre duality preserves dimensions, we get that

$$\dim(\operatorname{Ker}(f^*)) \geq \dim((U_2/\operatorname{Im}(f))^*) = \dim(U_2/\operatorname{Im}(f)) = \dim(\operatorname{Ker}(f)^0).$$

Thus $\dim(\operatorname{Ker}(f^*)) \geq \dim(\operatorname{Ker}(f))$. As the Serre duality is involuntary, we have $f = (f^*)^*$ and therefore by replacing f with f^* in the last inequality we get that $\dim(\operatorname{Ker}(f)) \geq \dim(\operatorname{Ker}(f^*))$. Thus $\dim(\operatorname{Ker}(f)) = \dim(\operatorname{Ker}(f^*))$.$\square$

We consider the lattice

$$\operatorname{Hom}_{W(k)}(J,L)^\sharp = \operatorname{Hom}_{W(k)}(J,L) + \operatorname{Hom}_{W(k)}(FJ,FL)$$

of the $B(k)$-vector space X. For an element $h \in \operatorname{Hom}_{W(k)}(J,L)$ we have $\frac{1}{p}FhV \in \operatorname{Hom}_{W(k)}(FJ,FL)$. Thus the admissible proalgebraic homomorphism of $B(k)$-vector spaces $\Psi : X \to X$ that maps h to $h - \frac{1}{p}FhV$ induces a homomorphism

$$\underline{\Psi_{J,L,+}} : \underline{\operatorname{Hom}_{W(k)}(J,L)} \to \underline{\operatorname{Hom}_{W(k)}(J,L)^\sharp} \tag{8}$$

of prounipotent groups.

The kernel of $\underline{\Psi_{J,L,+}}$ is the quasi-algebraic group $\underline{\operatorname{Hom}_{\mathbb{E}}(J,L)} = \underline{\operatorname{Hom}(D,E)}$ of Dieudonné module homomorphisms and thus is equal to the kernel of $\underline{\Psi_{J,L}}$.

Fact 3 *The following two inclusions* $\underline{\operatorname{Hom}_{W(k)}(J,L)^\flat} \subset \underline{\operatorname{Hom}_{W(k)}(J,L)}$ *and* $\underline{\operatorname{Hom}_{W(k)}(J,L)} \subset \underline{\operatorname{Hom}_{W(k)}(J,L)^\sharp}$ *induce a quasi-isomorphism from (5) to (8) viewed as complexes of prounipotent groups and thus they also induce a quasi-isomorphism between the complexes (5) and (8) modulo* p^m *viewed as complexes of unipotent connected commutative quasi-algebraic groups. In particular, the kernels of the reductions modulo* p^m *of* $\Phi_{J,L}$ *and* $\Psi_{J,L,+}$ *have the same dimension.*

Proof: The fact is equivalent to the following two identities

$$\operatorname{Im}(\Psi_{J,L}) = \operatorname{Hom}_{W(k)}(J,L) \cap \operatorname{Im}(\Psi_{J,L,+})$$

and

$$\mathrm{Hom}_{W(k)}(J,L) + \mathrm{Im}(\Psi_{J,L,+}) = \mathrm{Hom}_{W(k)}(J,L)^\sharp.$$

The inclusions "$\subseteq$" are obvious. We now check the reversed inclusions "$\supseteq$".

Let $g \in \mathrm{Hom}_{W(k)}(J,L) \cap \mathrm{Im}(\Psi_{J,L,+})$ and let $h \in \mathrm{Hom}_{W(k)}(J,L)$ be such that $g = \Psi_{J,L,+}(h) = h - \frac{1}{p}FhV$. Then $\frac{1}{p}FhV = g - h \in \mathrm{Hom}_{W(k)}(J,L)$ and therefore we have $h \in \mathrm{Hom}_{W(k)}(J,L)^\flat$. Thus $g = \Psi_{J,L}(h) \in \mathrm{Im}(\Psi_{J,L})$.

Let $v \in \mathrm{Hom}_{W(k)}(J,L)^\sharp$. Let $(g,l) \in \mathrm{Hom}_{W(k)}(J,L) \times \mathrm{Hom}_{W(k)}(FJ,FL)$ be such that $v = g + l$. Then we have $l = \frac{1}{p}FuV$ for some $u \in \mathrm{Hom}_{W(k)}(J,L)$ and therefore $l - u = v - (g+u)$ belongs to the image of $\Psi_{J,L,+}$. Thus $v = (g+u) + (l-u) \in \mathrm{Hom}_{W(k)}(J,L) + \mathrm{Im}(\Psi_{J,L,+})$.

The reversed inclusions "$\supseteq$" follow from the last two paragraphs. $\square$

We are now ready to complete the proof of Theorem 1. The Serre dual of (8) modulo p^m is isomorphic to the reduction modulo p^m of

$$\underline{\Psi_{L,J}} : \underline{\mathrm{Hom}_{W(k)}(L,J)^\flat} \to \underline{\mathrm{Hom}_{W(k)}(L,J)} \tag{9}$$

(cf. the paragraph before Lemma 2); here (9) is the analogue of (5) but with the roles of J and L interchanged. Based on this and Lemma 2, we get that $\mathbf{Hom}(E[p^m], D[p^m])_{\mathrm{red}}$ (i.e., the reduced algebraic group whose perfection is the kernel of $\underline{\Psi_{L,J}}$ modulo p^m) has the same dimension as the kernel of the reduction modulo p^m of $\Psi_{J,L,+}$. From this and Fact 3 we get that $\mathbf{Hom}(E[p^m], D[p^m])_{\mathrm{red}}$ has the same dimension as $\mathbf{Hom}(D[p^m], E[p^m])_{\mathrm{red}}$ (i.e., as the reduced algebraic group whose perfection is the kernel of $\Psi_{J,L}$ modulo p^m). As this holds for all $m \in \mathbb{N}^*$, we get that $n_{D,E} = n_{E,D}$ and that $s_{D,E} = s_{E,D}$. This ends the proof of Theorem 1. $\square$

4 Proof of Theorem 2

To prove Theorem 2 we will use homological properties of left $\mathbb{E}_m$-modules and some sort of a noncommutative duality over the Cartier–Dieudonné ring $\mathbb{E}_m$ which is analogous to the fact that for an affine connected smooth curve $\mathrm{Spec}\, A$ over k with field of rational functions K, the A-module K/A maps isomorphically to the A-torsion submodule in the k-dual of the space of one forms on $\mathrm{Spec}\, A$ via the functional "residue at infinity."

Let $m \in \mathbb{N}^*$. The left $\mathbb{E}_m$-modules of finite length are those that are finitely generated over $W_m(k)$.

Proposition 2 **(a)** *A left $\mathbb{E}_m$-module M of finite length corresponds to a truncated Barsotti–Tate group G of level m over k if and only if M is of finite tor dimension.*

(b) *If a left $\mathbb{E}_m$-module M of finite length corresponds to a truncated Barsotti–Tate group G of level m over k of height r, then M has a free resolution*

$$0 \to \mathbb{E}_m^r \to \mathbb{E}_m^r \to M \to 0.$$

Proof: We first prove (b). Let D be a Barsotti–Tate group over k such that $G = D[p^m]$; its height is r and we denote its dimension by d. Let L be the left $\mathbb{E}$-module which is the Dieudonné module of D. To prove (b) it suffices to show that we have a free resolution

$$0 \to \mathbb{E}^r \to \mathbb{E}^r \to L \to 0$$

in which the $\mathbb{E}$-linear map $\mathbb{E}^r \to L$ maps a (any) $\mathbb{E}$-basis of $\mathbb{E}^r$ into a $W(k)$-basis of M.

We consider epimorphisms $\kappa : \mathbb{E}^r \to L$ which map a $\mathbb{E}$-basis of $\mathbb{E}^r$ into a $W(k)$-basis of M. It suffices to show that the kernel $\mathrm{Ker}(\kappa)$ of one of them (and thus of each one of them) is a free left $\mathbb{E}$-module of rank r. Given a finite Galois extension k' of k, it is easy to see that the left $\mathbb{E}$-module $\mathrm{Ker}(\kappa)$ is free of rank r if and only if $\mathbb{E}(k') \otimes_{\mathbb{E}} \mathrm{Ker}(\kappa)$ is a free left $\mathbb{E}(k')$-module of rank r (cf. the notations of Section 2). We conclude that we can replace k by k' (i.e., we can perform a pullback of G to k').

By replacing k with a finite Galois extension k' of it, we can assume that there exists a $W(k)$-basis $\{e_1, \ldots, e_r\}$ of M for which there exist an element $g \in \mathrm{Ker}(\boldsymbol{GL}_L(W(k)) \to \boldsymbol{GL}_L(k))$ and a permutation π of the set $\Delta = \{1, 2, \ldots, r\}$ such that for each element $i \in \Delta$ we have $Fe_i = p^{\varepsilon_i} g(e_{\pi(i)})$, where $\varepsilon_i \in \{0, 1\}$ is 1 if and only if $i \leq d$. The existence of such a $W(k)$-basis of L after the mentioned replacement of k follows from the classification of Barsotti–Tate groups of level 1 over $\bar{k}$ obtained by Kraft and Ekedahl–Oort, to be compared with [V2], Subsection 2.3.

We consider two extra $W(k)$-bases $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_r\}$ of L that have the following three properties:

(i) For $i \in \{1, \ldots, d\}$ we have $a_i = Vb_{\pi(i)}$.

(ii) For $i \in \{d+1, \ldots, r\}$ we have $Fa_i = b_{\pi(i)}$.

(iii) For each $i \in \Delta$, a_i, b_i, and e_i are congruent modulo p.

Let $h = (h_{i,j})_{i,j\in\Delta} \in \boldsymbol{GL}_r(W(k))$ be the invertible matrix such that for each element $i \in \Delta$ we have an equality $a_i = \sum_{j\in\Delta} h_{ij} b_j$. Due to the property (iii) and the fact that $g \in \mathrm{Ker}(\boldsymbol{GL}_L(W(k)) \to \boldsymbol{GL}_L(k))$, we get that h modulo p is the identity $r \times r$ matrix with coefficients in k.

The left $\mathbb{E}$-module

$$P_0 = (\oplus_{i\in\Delta}\mathbb{E}a'_i \oplus_{i\in\Delta} \mathbb{E}b'_i)/(a'_i - \sum_{j\in\Delta} h_{ij} b'_j | i \in \Delta)$$

is isomorphic to $\mathbb{E}^r$. If $[a'_i]$ and $[b'_i]$ are the images of a'_i and b'_i in P_0, then the associations $[a'_i] \to a_i$ and $[b'_i] \to b_i$ define an $\mathbb{E}$-linear surjection $\theta : P_0 \to L$ which maps an $\mathbb{E}$-basis of P_0 into a $W(k)$-basis of L (thus, up to an identification of P_0 with $\mathbb{E}^r$, the search for κ will turn out to be θ).

Let $P_1 = \mathbb{E}^r = \oplus_{i\in\Delta}\mathbb{E}c_i$ and let $\eta : P_1 \to P_0$ be the $\mathbb{E}$-linear map that maps c_i to $[a'_i] - V[b'_{\pi(i)}]$ if $\in \{1, \ldots, d\}$ and to $F[a'_i] - [b'_{\pi(i)}]$ if $i \in \{d+1, \ldots, r\}$. The kernel of θ contains the image of η and therefore we get a complex

$$P_1 \xrightarrow{\eta} P_0 \xrightarrow{\theta} L \to 0.$$

To end the proof of (b), it suffices to show that in fact we have a short exact sequence

$$0 \to P_1 \xrightarrow{\eta} P_0 \xrightarrow{\theta} L \to 0.$$

Due to the very constructions, the left $\mathbb{E}$-module $P_0/\eta(P_1)$ is the same as the $W(k)$-submodule L' of $P_0/\eta(P_1)$ generated by $[a'_i] + \eta(P_1)$'s with $i \in \Delta$. As the $W(k)$-linear map $L' = P_0/\eta(P_1) \to L$ is a surjective map from a $W(k)$-module generated by r elements onto a free $W(k)$-module of rank r, it is an isomorphism and therefore the complex $P_1 \to P_0 \to L \to 0$ is exact at P_0. We are left to show that η is injective. It suffices to show that the reduction $\eta_1 : P_1/pP_1 \to P_0/pP_0$ of η modulo p is injective. But as h is congruent modulo p to the identity matrix, we have canonical identifications $P_0/pP_0 = \mathbb{E}_1^r = \oplus_{j\in\Delta}\mathbb{E}_1\bar{a}'_i$, where $\bar{a}'_i = [a'_i] + pP_0$. To show that η_1 is injective, it suffices to show that the assumption that there exists a linear dependence relation with coefficients α_i in $\mathbb{E}_1$ of the form

$$\sum_{i=1}^{d} \alpha_i(\bar{a}'_i - V\bar{a}'_{\pi(i)}) + \sum_{i=d+1}^{r} \alpha_i(F\bar{a}'_i - \bar{a}'_{\pi(i)}) = 0 \tag{10}$$

leads to a contradiction.

We have a canonical identification $\mathbb{E}_1 = \oplus_{i\in\mathbb{N}} kF^i \oplus_{i\in\mathbb{N}^*} kV^i$ of k-vector spaces. Suppose there exists $s \in \mathbb{N}$ such that for some $i \in \{d+1, \ldots, r\}$ the coefficient c_{i,F^s} of F^s in α_i is a nonzero element of k. But in such a case, it is easy to see that the coefficient of $F^{s+1}\bar{a}'_i$ in the left hand side of the Equation (10) is a nonzero element of k, contradiction. Thus $\alpha_{d+1}, \ldots, \alpha_r \in \oplus_{i\in\mathbb{N}^*} kV^i$ and a similar argument shows that $\alpha_1, \ldots, \alpha_d \in \oplus_{i\in\mathbb{N}^*} kF^i$. From this and the Equation (10) we easily get that in fact we have $\alpha_i = 0$ for all $i \in \Delta$, contradiction. Thus η_1 is injective and this ends the proof of (b).

The only if part of (a) follows from (b). We now proof the if part of (a). We assume that the left $\mathbb{E}_m$-module M of finite length has finite tor dimension. For $u \in \{1, \ldots, m\}$ we consider the following infinite free resolution

$$\cdots \xrightarrow{p^u} \mathbb{E}_m \xrightarrow{p^{m-u}} \mathbb{E}_m \xrightarrow{p^u} \mathbb{E}_m/p^u\mathbb{E}_m \to 0$$

of the right $\mathbb{E}_m$-module $\mathbb{E}_m/p^u\mathbb{E}_m$. As M has finite tor dimension, we have $\mathrm{Tor}_n(\mathbb{E}_m/p^u\mathbb{E}_m, M) = 0$ for $n >> 0$ and thus by tensoring this free resolution with M we get that the complex

$$M \xrightarrow{p^{m-u}} M \xrightarrow{p^u} M$$

is exact. By taking $u = 1$, we get that each cyclic $W(k)$-module which is a direct summand of M is isomorphic to $W_m(k)$. Thus the finitely generated $W_m(k)$-module M is free.

As M has finite tor dimension as a $\mathbb{E}_m$-module and is free as a $W_m(k)$-module, the left $\mathbb{E}_1$-module M/pM has also finite tor dimension. Based on this, an argument similar to the one of the previous paragraph but using the free resolution

$$\cdots \xrightarrow{F} \mathbb{E}_1 \xrightarrow{V} \mathbb{E}_1 \xrightarrow{F} \mathbb{E}_1/F\mathbb{E}_1 \to 0$$

of the right $\mathbb{E}_1$-module $\mathbb{E}_1/F\mathbb{E}_1$, shows that the complex

$$M/pM \xrightarrow{V} M/pM \xrightarrow{F} M/pM$$

is exact. Thus M/pM corresponds to a truncated Barsotti–Tate group of level 1 over k. From this and the previous paragraph we get that M corresponds to a truncated Barsotti–Tate group G of level m over k. Thus (a) holds as well. $\square$

We have an involutory antiautomorphism $\iota_m : \mathbb{E}_m \to \mathbb{E}_m$ that interchanges F and V and that fixes $W_m(k)$, and this allows us to transform right $\mathbb{E}_m$-modules into left $\mathbb{E}_m$-modules. If P is a left $\mathbb{E}_m$-module, let

$$P^\vee = \mathrm{Hom}_{W_m(k)}(P, W_m(k))$$

be endowed with the left $\mathbb{E}_m$-module structure via the same rules as in the first paragraph of Section 3, and let

$$P^{\#} = \mathrm{Hom}_{\mathbb{E}_m}(P, \mathbb{E}_m)$$

be endowed with the left $\mathbb{E}_m$-module structure given by the rule $(af)(x) = f(x)\iota_m(a)$ where $f \in P^{\#}$, $a \in \mathbb{E}_m$, and $x \in P$. Similarly, the right multiplications of $\mathbb{E}_m$ by elements $\iota_m(a)$ endow naturally $\mathrm{Ext}^1_{\mathbb{E}_m}(P, \mathbb{E}_m)$ with the structure of a left $\mathbb{E}_m$-module.

If P is a finitely generated left $\mathbb{E}_m$-module and M a left $\mathbb{E}_m$-module of finite length, then $\mathrm{Hom}_{\mathbb{E}_m}(P, M)$ has a natural structure of a commutative quasi-algebraic group $\underline{\mathrm{Hom}_{\mathbb{E}_m}(P, M)}$. This can be checked easily by choosing generators of P and an expression of M as a direct sum of cyclic $W_m(k)$-modules and by checking directly the independence of the resulting commutative quasi-algebraic group structure $\underline{\mathrm{Hom}_{\mathbb{E}_m}(P, M)}$ of $\mathrm{Hom}_{\mathbb{E}_m}(P, M)$ from the choices made.

Fact 4 *If M and N are both left $\mathbb{E}_m$-modules of finite length and thus the Dieudonné modules of commutative group schemes G and H (respectively), then this commutative quasi-algebraic group $\underline{\mathrm{Hom}_{\mathbb{E}_m}(N, M)}$ is isomorphic to the commutative quasi-algebraic group $\underline{\mathrm{Hom}(G, H)}$.*

Proof: The crystalline Dieudonné theory provides a natural evaluation morphism $f : \underline{\mathrm{Hom}(G, H)} \to \underline{\mathrm{Hom}_{\mathbb{E}_m}(P, M)}$ of the abelian category $\mathcal{Q}$. If $\bar{k}$ is an algebraic closure of k, then from the classical (contravariant) Dieudonné theory we get that $f(\bar{k})$ is an isomorphism. Thus the fact follows from Fact 1. $\square$

Fact 5 *Let P be a free left $\mathbb{E}_m$-module of finite rank and let M be a left $\mathbb{E}_m$-module of finite length. Then the unipotent connected commutative quasi-algebraic groups $\underline{\mathrm{Hom}_{\mathbb{E}_m}(P, M)}$ and $\underline{\mathrm{Hom}_{\mathbb{E}_m}(P^{\#}, M^{\vee})}$ are naturally Serre dual.*

Proof: This follows from the fact that Serre duality commutes with finite direct sums and interchanges F and V in the same way as ι_m does. $\square$

Now Theorem 2 follows from the following proposition applied to the Dieudonné modules M and N of G and H (respectively) and from the Fact 4:

Proposition 3 *Let M, N be two left $\mathbb{E}_m$-modules of finite length. We assume that M is the Dieudonné module of a truncated Barsotti–Tate group G of level m over k. Then $\underline{\mathrm{Hom}_{\mathbb{E}_m}(M,N)}$ has the same dimension as $\underline{\mathrm{Hom}_{\mathbb{E}_m}(M^\vee,N^\vee)}$ and thus also as $\underline{\mathrm{Hom}_{\mathbb{E}_m}(N,M)}$.*

Proof: We consider a free resolution

$$0 \to P_1 \to P_0 \to M \to 0$$

with P_1 and P_0 left $\mathbb{E}_m$-modules isomorphic to $\mathbb{E}_m^r$ and with r as the height of G, cf. Proposition 2 (b). Using Lemma 2 applied to the homomorphism

$$f : \underline{\mathrm{Hom}_{\mathbb{E}_m}(P_0,N)} \to \underline{\mathrm{Hom}_{\mathbb{E}_m}(P_1,N)}$$

and the Fact 5, the kernel $\underline{\mathrm{Hom}_{\mathbb{E}_m}(M,N)}$ of f has the same dimension as the kernel $\underline{\mathrm{Hom}_{\mathbb{E}_m}(\mathrm{Coker}(P_0^\# \to P_1^\#),N^\vee)}$ of the Serre dual

$$f^* : \underline{\mathrm{Hom}_{\mathbb{E}_m}(P_1^\#,N^\vee)} \to \underline{\mathrm{Hom}_{\mathbb{E}_m}(P_0^\#,N^\vee)}$$

of f. Thus it suffices to show that $\mathrm{Coker}(P_0^\# \to P_1^\#) = \mathrm{Ext}^1_{\mathbb{E}_m}(M,\mathbb{E}_m)$ is isomorphic to $M^\vee$. But this is a particular case of the following lemma. $\square$

Lemma 3 *If N is a left $\mathbb{E}_m$-module of finite length, then we have a natural isomorphism of left $\mathbb{E}_m$-modules from $\mathrm{Ext}^1_{\mathbb{E}_m}(N,\mathbb{E}_m)$ to $N^\vee$.*

Before proving this lemma, we will need some preliminary material on left $\mathbb{E}_m$-modules. Let $\mathbb{S}_m$ be the multiplicative subset of regular elements of $\mathbb{E}_m$, i.e., of elements of $\mathbb{E}_m$ with nonzero images in both $k[F] = \mathbb{E}_m/(p,V)$ and $k[V] = \mathbb{E}_m/(p,F)$. Note that $\mathbb{S}_m$ admits calculus of left and right fractions (i.e., the left and right Ore conditions are satisfied). In other words, for each $s \in \mathbb{S}_m$ and $x \in \mathbb{E}_m$, the intersection sets $\mathbb{S}_m x \cap \mathbb{E}_m s$ and $x\mathbb{S}_m \cap s\mathbb{E}_m$ are nonempty. Let $\mathbb{K}_m$ be the localization of $\mathbb{E}_m$ with respect to $\mathbb{S}_m$ and let $\mathbb{E}_m \to \mathbb{K}_m$ be the natural inclusion of rings. The multiplicative set of powers of $F+V$ also satisfies the left and right Ore conditions, and inverting $F+V$ in $\mathbb{E}_m$ we get the product of skew Laurent polynomial rings $W_m(k)\{F,F^{-1}\} \times W_m(k)\{V,V^{-1}\}$. This gives a product description of $\mathbb{K}_m$: it is flat over $\mathbb{Z}/p^m\mathbb{Z}$ and modulo p it is the product $k(F) \times k(V)$ of two (skew) division rings.

Definition 3 *Let P be a left $\mathbb{E}_m$-module. By its finite part $Fin(P)$ we mean the left $\mathbb{E}_m$-submodule*

$$\{x \in P \mid \mathbb{E}_m x \textit{ is a finitely generated } W_m(k)\textit{-module}\} = \mathrm{Ker}(P \to \mathbb{K}_m \otimes_{\mathbb{E}_m} P).$$

We have the following elementary fact.

Fact 6 *The short exact sequence* $0 \to \mathbb{E}_m \to \mathbb{K}_m \to \mathbb{K}_m/\mathbb{E}_m \to 0$ *is an injective resolution of* $\mathbb{E}_m$ *and therefore we have an identity* $Ext^1_{\mathbb{E}_m}(N, \mathbb{E}_m) = \mathrm{Hom}_{\mathbb{E}_m}(N, \mathbb{K}_m/\mathbb{E}_m)$ *of left* $\mathbb{E}_m$*-modules.*

Proof: Based on the Baer Criterion, it suffices to show that for each nonzero element $a \in \mathbb{E}_m$, every $\mathbb{E}_m$-linear map l from $\mathbb{E}_m a$ to $\mathbb{K}_m$ or to $\mathbb{K}_m/\mathbb{E}_m$ extends to a $\mathbb{E}_m$-linear map l' from $\mathbb{E}_m$ to $\mathbb{K}_m$ or to $\mathbb{K}_m/\mathbb{E}_m$ (respectively). Using induction on $m \in \mathbb{N}^*$, it suffices to check the existence of l' in the case when $m = 1$.

We first consider the case when the codomain of l is $\mathbb{K}_1$. By replacing a with a left multiple of it by an element of $\mathbb{S}_1$, we can assume that either $a = 1$ or $a = V$. If $a = 1$, then $l' = l$ exists. If $a = V$, then $l(f) = (0, b) \in \mathbb{K}_1 = k(F) \times k(V)$ with $b \in k(V)$ and therefore we can define l' via the rule $l'(1) = (0, V^{-1}b) \in \mathbb{K}_1 = k(F) \times k(V)$.

Next we consider the case when the codomain of l is $\mathbb{K}_1/\mathbb{E}_1$. If $a \in \mathbb{S}_1$, then $\mathbb{E}_m a$ is a free $\mathbb{E}_m$-module and therefore l lifts to a $\mathbb{E}_m$-linear map $f : \mathbb{E}_m a \to \mathbb{K}_1$. If $f' : \mathbb{E}_m \to \mathbb{K}_1$ is a $\mathbb{E}_m$-linear map which extends f (cf. previous paragraph), then we can take l' to be the composite of f' with the epimorphism $\mathbb{K}_1 \to \mathbb{K}_1/\mathbb{E}_1$. We now assume that $a \notin \mathbb{S}_1$. Thus either $a = V^t c$ with $c \in k\{V\} \setminus \{0\} \subset \mathbb{E}_1$ and $t \in \mathbb{N}^*$ or $a = F^t c$ with $c \in k\{F\} \setminus \{0\} \subset \mathbb{E}_1$ and $t \in \mathbb{N}^*$. The two situations are similar and thus to fix the ideas we will assume that $a = V^t c$. We write $l(a) = (0, b) + \mathbb{E}_1$ with $b \in k(V)$. Thus we can define l' via the rule $l'(1) = (0, c^{-1}V^{-t}b) + \mathbb{E}_1 \in \mathbb{K}_1/\mathbb{E}_1$.

Therefore l' always exists. $\square$

We have "development at infinity" homomorphisms to skew Laurent series rings

$$e_{m,F} : \mathbb{K}_m \to W_m(k)((F^{-1}))$$

and

$$e_{m,V} : \mathbb{K}_m \to W_m(k)((V^{-1}))$$

obtained by mapping V to pF^{-1} and F to pV^{-1} (respectively).

Let $\lambda_m : \mathbb{K}_m/\mathbb{E}_m \to W_m(k)$ be the $W_m(k)$-linear map

$$\lambda_m([f + \mathbb{E}_m]) = (\text{constant term of } e_{m,F}(f)) - (\text{constant term of } e_{m,V}(f)).$$

We view $\mathbb{K}_m/\mathbb{E}_m$ as a $(\mathbb{E}_m, W_m(k))$-bimodule ($\mathbb{E}_m$ on left, $W_m(k)$ on right). Let $\mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$ be endowed with the structure of a $(\mathbb{E}_m, W_m(k))$-bimodule by the rule $(ahb)(x) = h(xa)b$ with $a \in \mathbb{E}_m$, $b \in W_m(k)$, $h \in$

$\mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$, and $x \in \mathbb{E}_m$. We define a map of $(\mathbb{E}_m, W_m(k))$-bimodules

$$\tau_m : \mathbb{K}_m/\mathbb{E}_m \to \mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$$

by the rule $\tau_m(h+\mathbb{E}_m)(x) = \lambda_m(xh+\mathbb{E}_m)$ with $x, h \in \mathbb{E}_m$.

Lemma 4 *The map τ_m of $(\mathbb{E}_m, W_m(k))$-bimodules is injective and its image is the finite part $Fin(\mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k)))$ of $\mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$ (viewed as a left $\mathbb{E}_m$-module).*

Proof: It suffices to show that for each $f \in \mathbb{S}_m$, the restriction

$$\tau_{m,f} : \{x \in \mathbb{K}_m/\mathbb{E}_m | fx = 0\} \to \{x \in \mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k)) | fx = 0\}$$

of τ_m is a bijection of right $W_m(k)$-modules. As f is a regular element of $\mathbb{E}_m$, the short exact sequence of left $\mathbb{E}_m$-modules $0 \to \mathbb{E}_m f \to \mathbb{E}_m \to \mathbb{E}_m/\mathbb{E}_m f \to 0$ is a free resolution of the left $\mathbb{E}_m$-module $\mathbb{E}_m/\mathbb{E}_m f$ and it is easy to see that $\mathbb{E}_m/\mathbb{E}_m f$ is a left $W_m(k)$-module of finite length. From this and Proposition 2 (a) we get that $\mathbb{E}_m/\mathbb{E}_m f$ corresponds to a truncated Barsotti–Tate group of level m and in particular that the left $W_m(k)$-module $\mathbb{E}_m/\mathbb{E}_m f$ is free of finite rank. Via the involutory antiautomorphism ι_m, we get that the right $\mathbb{E}_m$-module $\mathbb{E}_m/f\mathbb{E}_m$ is a right free $W_m(k)$-module of finite rank.

As the domain and the codomain of $\tau_{m,f}$ are both free right $W_m(k)$-modules of the same finite rank equal to the rank of the free right $W_m(k)$-module $\mathbb{E}_m/f\mathbb{E}_m$, it suffices to show that $\tau_{m,f}$ modulo p is an injective k-linear map. Thus to prove the lemma it suffices to show that τ_1 is injective. To check this, we can assume that k is algebraically closed and it suffices to show that the restriction of τ_1 to each simple $\mathbb{E}_1$-submodule S of $\mathbb{K}_1/\mathbb{E}_1 = [k(F) \times k(V)]/\mathbb{E}_1$ is injective.

In this and the next paragraph we will check that there exist precisely three simple left $\mathbb{E}_1$-submodules of $\mathbb{K}_1/\mathbb{E}_1$: generated by $(F-1)^{-1}+\mathbb{E}_1$, by $(V-1)^{-1}+\mathbb{E}_1$, and by $(F+V)^{-1}V+\mathbb{E}_1 = (0,1)+\mathbb{E}_1$. Let $x = (x_1, x_2) \in k(F) \times k(V)$ be such that S is generated by $x+\mathbb{E}_1$. If $x \in k\{F\} \times k\{V\}$, then $S = [k\{F\} \times k\{V\}]/\mathbb{E}_1$ is a one dimensional k-vector space generated by $(F+V)^{-1}V+\mathbb{E}_1$. Similarly, if either $x_1 = 0$ or $x_2 = 0$, then it is easy to see that $S = [k\{F\} \times k\{V\}]/\mathbb{E}_1$.

Thus we can assume that $x \notin k\{F\} \times k\{V\}$ and that neither x_1 nor x_2 is 0. To fix the ideas we can assume that $x_1 \notin k\{F\}$ and $x_2 \neq 0$ and we want to show that S is generated by $(F-1)^{-1}+\mathbb{E}_1$. Writing $x_1 = f_1(F)^{-1}f_2(F)$

with $f_1(F), f_2(F) \in k\{F\} \setminus \{0\}$, we can assume that $x \in S - \{0\}$ is such that $f_1(F)$ has the smallest possible degree $d_1 \in \mathbb{N}^*$ in F. As k is algebraically closed, there exists $a \in k$ such that we can write $f_1(F) = f_1'(F)(F-a)$ with $f_1'(F) \in k\{F\}$. Based on the smallest possible degree d_1 property we easily get that we can assume that $f_1'(F) = 1$. Moreover, modulo elements in $F\mathbb{E}_1 = \mathbb{E}_1 F$ and modulo a multiplication by a nonzero element of k and thus modulo the replacement of a by another element in k, we can assume that $f_2(F) = 1$ and thus that $x_1 = (F-a)^{-1}$. If $a = 0$, then $Fx = (1,0) \in [k\{F\} \times k\{V\}] \setminus \mathbb{E}_1$ and therefore $Fx + \mathbb{E}_1$ generates S which implies that $x \in k\{F\} \times k\{V\}$ a contradiction. Thus $a \in k \setminus \{0\}$ and therefore $(F-a)x + \mathbb{E}_1 = (0, -ax_2 - 1) + \mathbb{E}_1$. Thus, if $-ax_2 - 1 \notin Vk\{V\}$, then from the end of the last paragraph we get that $S = [k\{F\} \times k\{V\}]/\mathbb{E}_1$ and this contradicts the fact that $x_1 \notin k\{F\}$. Therefore $-ax_2 - 1 \in Vk\{V\}$ which implies that $x + \mathbb{E}_1 = (F-a)^{-1} + \mathbb{E}_1$. As $a \in k \setminus \{0\}$ and k is algebraically closed, by multiplying x with a nonzero element of k we can assume that $x + \mathbb{E}_1 = (F-1)^{-1} + \mathbb{E}_1$.

The identities

$$1 = -\lambda_1((0,1) + \mathbb{E}_1) = \lambda_1((F-1)^{-1} + \mathbb{E}_1) = -\lambda_1((V-1)^{-1} + \mathbb{E}_1),$$

imply that τ_1 is nontrivial on these three simple left $\mathbb{E}_1$-submodules of $\mathbb{K}_1/\mathbb{E}_1$.$\square$

4.1 Proof of Lemma 3

As the left $\mathbb{E}_m$-module $\mathrm{Ext}^1_{\mathbb{E}_m}(N, \mathbb{E}_m)$ can be identified based on Fact 6 with $\mathrm{Hom}_{\mathbb{E}_m}(N, \mathbb{K}_m/\mathbb{E}_m)$, from Lemma 4 we get that it can be identified via τ_m with $\mathrm{Hom}_{\mathbb{E}_m}(N, \mathrm{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k)))$ and thus also with the left $\mathbb{E}_m$-module $N^\vee = \mathrm{Hom}_{W_m(k)}(N, W_m(k))$ as one can easily check using a presentation of the left $\mathbb{E}_m$-module N of finite length. This ends the proof of Lemma 3 and thus also the proofs of Proposition 3 and of Theorem 2. $\square$

4.2 Remarks

(a) Let R be a perfect ring of characteristic p, let $W(R)$ be the ring of p-typical Witt vectors with coefficients in R, and let σ_R be the Frobenius automorphism of R, $W(R)$, and $B(R) = W(R)[\frac{1}{p}]$. Let

$$\mathbb{D}(R) = B(R)\{F, F^{-1}\}/I(R) \quad \text{and} \quad \mathbb{E}(R) = W(R)\{F, V\} \subset \mathbb{D}(R)$$

be defined similarly to $\mathbb{D}(k) = \mathbb{D}$ and $\mathbb{E}(k) = \mathbb{E}$ (thus $I(R)$ is the two-sided ideal generated by all elements $Fa - \sigma_R(a)F$ with $a \in B(R)$). Let $\mathbb{E}_m(R) = \mathbb{E}(R)/p^m\mathbb{E}(R)$ and $W_m(R) = W(R)/p^mW(R)$. Then Lemma 3 continues to hold in the context of $\mathbb{E}_m(R)$ and $W_m(R)$ provided the role of N is replaced by the one of a left $\mathbb{E}_m(R)$-module whose projective dimension as a $W_m(R)$-module is at most one (however, the proof is more complicated in this generality provided by R).

(b) Equation (1) implies that $s_{D,E} = s_{E,D}$. We recall from [V2], Theorem 1.2 (e) and [GV], Remark 4.5 that $s_D = s_{D,D}$ is an isogeny invariant. From the last two sentences we get directly that $s_{D,E} = \frac{1}{2}(s_{D\oplus E} - s_D - s_E)$ is an isogeny invariant. Based on this and [V2], Theorem 1.2 (c) and (f), one gets that $s_{D,E}$ can be easily computed in terms of the Newton polygons of D and E. For instance, if D is isoclinic of dimension d and codimension c and E is isoclinic of dimension f and codimension e, then $s_D = cd$, $s_E = ef$, and

$$s_{D\oplus E} = (c+e)(d+f) - |cf - de|$$

(cf. [V2], Theorem 1.2 (c) and (f)) and therefore we have

$$s_{D,E} = \min\{cf, de\}.$$

4.3 Example

Let n, m, t be positive integers such that $m = n + t$. Let $q \in \{2t-1, 2t\}$. Let H be such that its Dieudonné module N is isomorphic to $\mathbb{E}/(F,V)^{2n+q}$. Then p^m annihilates H but p^{m-1} does not annihilate H. Let $G = D[p^n]$, where D is a supersingular Barsotti–Tate group over k of height 2; thus the Dieudonné module M of G is isomorphic to $\mathbb{E}_n/(F-V)$. We have canonical identifications of quasi-algebraic groups $\underline{\mathrm{Hom}_{\mathbb{E}}(M,N)} = \underline{(F,V)^{2n+q-1}/(F,V)^{2n+q}}$ and $\underline{\mathrm{Hom}_{\mathbb{E}}(N,M)} = \underline{M}$ (cf. the notations of Subsection 2.4 and of the proof of Theorem 2). From this and Fact 4 we get that

$$\dim(\boldsymbol{Hom}(H,G)) = \mathrm{length}_{W(k)}((F,V)^{2n+q-1}/(F,V)^{2n+q}) = 2n+q$$

and that

$$\dim(\boldsymbol{Hom}(G,H)) = \mathrm{length}_{W(k)}(M) = 2n.$$

Thus $\dim(\boldsymbol{Hom}(G,H)) - \dim(\boldsymbol{Hom}(H,G)) = -q$. From this via Cartier duality we get that $\dim(\boldsymbol{Hom}(G^{\mathrm{t}},H^{\mathrm{t}})) - \dim(\boldsymbol{Hom}(H^{\mathrm{t}},G^{\mathrm{t}})) = q$.

If $q = 2t$, then we have $\dim(\boldsymbol{Hom}(H,G)) = \frac{m}{n}\dim(\boldsymbol{Hom}(G,H))$ and $\dim(\boldsymbol{Hom}(H^{\mathrm{t}},G^{\mathrm{t}})) = \frac{n}{m}\dim(\boldsymbol{Hom}(G^{\mathrm{t}},H^{\mathrm{t}}))$.

4.4 Proof of Proposition 1

The last part and the optimality part of Proposition 1 follow from Subsection 4.3. If the inequality $\dim(\boldsymbol{Hom}(G,H)) \leq \frac{m}{n}\dim(\boldsymbol{Hom}(H,G))$ always holds, then by replacing in this inequality the pair (G,H) by the pair $(G^{\mathrm{t}}, H^{\mathrm{t}})$ and by using the Cartier duality we easily get that the other inequality $\frac{n}{m}\dim(\boldsymbol{Hom}(H,G)) \leq \dim(\boldsymbol{Hom}(G,H))$ also holds. Thus it suffices to show that the inequality $\dim(\boldsymbol{Hom}(G,H)) \leq \frac{m}{n}\dim(\boldsymbol{Hom}(H,G))$ holds.

Let D be a Barsotti–Tate group over k such that $G = D[p^n]$, cf. [I], Theorem 4.4 e). Let $C = \boldsymbol{Hom}(H, D[p^m])$; it is a commutative group scheme of finite type over k annihilated by p^m. From the short exact sequences $0 \to G \to D[p^n] \to D[p^{m-n}] \to 0$ and $0 \to D[p^m - n] \to D[p^n] \to G \to 0$, we get an exact complex $0 \to \boldsymbol{Hom}(G,H) \to \boldsymbol{Hom}(D[p^m], H)$ as well as an identity $\boldsymbol{Hom}(H,G) = C[p^n]$. Thus $\dim(\boldsymbol{Hom}(G,H)) \leq \dim(\boldsymbol{Hom}(D[p^m],H))$ and $\dim(\boldsymbol{Hom}(H,G)) = \dim(C[p^n])$. We have $\dim(\boldsymbol{Hom}(D[p^m],H)) = \dim(C)$ and $\dim(C) \leq \frac{m}{n}\dim(C]p^n])$, cf. Equation (1) and Lemma 5 below (respectively). From the last two sentences we get that $\dim(\boldsymbol{Hom}(G,H)) \leq \frac{m}{n}\dim(\boldsymbol{Hom}(H,G))$. Thus Inequalities (2) hold. $\square$

Lemma 5 *Let $m > n > 0$ be integers. Let C be a commutative group scheme of finite type over k annihilated by p^m. Then the dimension of its subgroup scheme $C[p^n] = Ker(p^n : C \to C)$ is at least equal to $\frac{n}{m}\dim(C)$.*

Proof: For $i \in \{0, \ldots, m-1\}$ let $a_i = \dim(C[p^{i+1}]/C[p^i])$. Then we have $\dim(C[p^n]) = \sum_{j=0}^{n-1} a_j$ and $\dim(C) = \sum_{i=0}^{m-1} a_i$. Thus the difference

$$m\dim(C[p^n]) - n\dim(C) = (m-n)\sum_{j=0}^{n-1} a_j - n\sum_{i=n}^{m-1} a_i$$

is the sum of $n(m-n)$ expressions of the form $a_j - a_i$ with $0 \leq j < n \leq i \leq m-1$. But for $0 \leq j < i \leq m-1$ the multiplication by p^{i-j} induces a monomorphism $C[p^{i+1}]/C[p^i] \to C[p^{j+1}]/C[p^j]$ and therefore the inequality $a_j - a_i \geq 0$ holds. The lemma follows from the last two sentences. $\square$

5 Proof of Theorem 3

Let $S(\boldsymbol{M})$ be the set (of representatives) of isomorphism classes of finite dimensional simple left $\boldsymbol{M}$-modules. The abelian group $K_0(\boldsymbol{M})$ is canonically identified with the free abelian group on $S(\boldsymbol{M})$.

Two left $\boldsymbol{M}$-modules Z_1 and Z_2 of finite dimension are isomorphic if and only if the two left $\boldsymbol{M}^{(\sigma)}$-modules $Z_1^{(\sigma)}$ and $Z_2^{(\sigma)}$ are isomorphic. As the Frobenius homomorphism $\boldsymbol{M} \to \boldsymbol{M}^{(\sigma)}$ is a dominant morphism between reduced schemes of finite type over k, the two left $\boldsymbol{M}^{(\sigma)}$-modules $Z_1^{(\sigma)}$ and $Z_2^{(\sigma)}$ are isomorphic if and only if the two left $\boldsymbol{M}$-modules $Z_1^{(\sigma)}$ and $Z_2^{(\sigma)}$ are isomorphic. From the last two sentences we get that:

(i) the automorphism σ acts naturally on $S(\boldsymbol{M})$: the isomorphism class $[Z]$ is mapped to the isomorphism class $[Z^{(\sigma)}]$;

(ii) it makes sense to speak about the partition of $S(\boldsymbol{M})$ into orbits of the action of σ on $S(\boldsymbol{M})$: $[Z_1], [Z_2] \in S(\boldsymbol{M})$ belong to the same orbit if and only if there exists $n \in \mathbb{N}$ such that either $[Z_1] = [Z_2^{(\sigma^n)}]$ or $[Z_1^{(\sigma^n)}] = [Z_2]$.

Let $O(\boldsymbol{M})$ be the set of orbits of the action of σ on $S(\boldsymbol{M})$. Based on (ii), the abelian group $K_0(\boldsymbol{M})/I_0(\boldsymbol{M})$ is canonically identified with the free abelian group on $O(\boldsymbol{M})$. For $i \in \{1, 2\}$ we write

$$[\boldsymbol{L}_1^\vee] = \sum_{[Z] \in S(\boldsymbol{M})} n_{1,[Z]}[Z] \in K_0(\boldsymbol{M})$$

and

$$[\boldsymbol{L}_2] = \sum_{[Z] \in S(\boldsymbol{M})} n_{2,[Z]}[Z] \in K_0(\boldsymbol{M}),$$

where each $n_{i,[Z]} \in \mathbb{N}$ and all but a finite number of the $n_{i,[Z]}$'s being 0. Let $O(\boldsymbol{M}, G, H)$ be the smallest finite subset of $O(\boldsymbol{M})$ such that for each $o \in O(\boldsymbol{M}) \setminus O(\boldsymbol{M}, G, H)$ and for every $[Z] \in o$ we have $n_{1,[Z]} = n_{2,[Z]} = 0$.

Theorem 3 is equivalent to the following statement: for each orbit $o \in O(\boldsymbol{M}, G, H)$ we have an identity

$$\sum_{[Z] \in o} n_{1,[Z]} = \sum_{[Z] \in o} n_{2,[Z]}. \tag{11}$$

Below we will need the following elementary fact whose proof is left as an exercise.

Fact 7 *Let $\bar{k}$ be an algebraic closure of k. Then for an absolutely simple left $\boldsymbol{M}$-module Z of finite dimension we have the following disjoint two possibilities:*

(a) *If the image of $\boldsymbol{M}(\bar{k})$ in $\mathbf{End}(Z)(\bar{k})$ is finite, then there exists $n \in \mathbb{N}^*$ such that the left $\boldsymbol{M}$-modules Z and $Z^{(\sigma^n)}$ are isomorphic.*

(b) *If the image of $\boldsymbol{M}(\bar{k})$ in $\mathbf{End}(Z)(\bar{k})$ is infinite, then there exists $n \in \mathbb{N}^*$ such that for each integer $m \geq n$ there exists no left $\boldsymbol{M}$-module W such that Z and $W^{(\sigma^m)}$ are isomorphic.*

Lemma 6 *To prove that the identity (11) holds we can assume that for each $o \in O(\boldsymbol{M}, G, H)$, every simple left $\boldsymbol{M}$-module Z with $[Z] \in o$ is absolutely simple.*

Proof: Let k' be a finite Galois extension of k such that each simple factor of a composition series of either the left $\boldsymbol{M}_{k'}$-module $k' \otimes_k \boldsymbol{L}_1$ or of the left $\boldsymbol{M}_{k'}$-module $k' \otimes_k \boldsymbol{L}_2$ is absolutely simple. To prove the lemma it suffices to show that if the Equation (11) holds in the case when the pair $(k, O(\boldsymbol{M}, G, H))$ is replaced by the pair $(k', O(\boldsymbol{M}_{k'}, G_{k'}, H_{k'}))$, then the Equation (11) holds as well.

If $[Z] \in o \in O(\boldsymbol{M}, G, H)$, then $k' \otimes_k Z$ is a direct sum of absolutely simple left $\boldsymbol{M}_{k'}$-modules. It is well known that we can write

$$k' \otimes_k Z = \oplus_{j=1}^{u_Z} m_Z Z'_j,$$

where $u_Z, m_Z \in \mathbb{N}^*$ and where the Z'_j's are absolutely simple left $\boldsymbol{M}_{k'}$-module that are not pairwise isomorphic and such that the Galois group $\mathrm{Gal}(k'/k)$ acts transitively on the set $\{Z'_1, \ldots, Z'_{u_Z}\}$. We consider the orbit $o' \in O(\boldsymbol{M}_{k'}, G_{k'}, H_{k'})$ such that $[Z'_1] \in o'$. Let $I_{Z'_1}$ be the nonempty subset of $\{1, \ldots, u_Z\}$ formed by all those elements j such that $[Z'_j] \in o'$ and let $s_Z \in \mathbb{N}^*$ be the number of elements of $I_{Z'_1}$. It is easy to see that u_Z, m_Z, and s_Z depend only on the orbit o and not on the choice of Z with the property that $[Z] \in o$. Thus we can define $u_o = u_Z$, $m_o = m_Z$, and $s_o = s_Z$.

We note that if $[Z_1] \in o' \in O(\boldsymbol{M}, G, H)$ and $o' \neq o$ and if we similarly write

$$k' \otimes_k Z_1 = \oplus_{j=1}^{u_{Z_1}} m_{Z_1} Z'_{1,j},$$

then for all $j \in \{1, \ldots, u_Z\}$ and $j_1 \in \{1, \ldots, u_{Z_1}\}$ the orbits in $O(\boldsymbol{M}_{k'})$ to which Z'_j and Z'_{1,j_1} belong are distinct. This is so as for all $a, b \in \mathbb{Z}$, the k-vector space $\mathrm{Hom}_{\boldsymbol{M}}(Z^{(\sigma^a)}, Z_1^{(\sigma^b)})$ is nonzero if and only if the k'-vector space $\mathrm{Hom}_{\boldsymbol{M}'_k}((k' \otimes_k Z)^{(\sigma^a)}, (k' \otimes_k Z_1)^{(\sigma^b)})$ is nonzero.

We write $[(k' \otimes_k \boldsymbol{L}_1)^\vee] = \sum_{[Z'] \in S(\boldsymbol{M}_{k'})} n_{1,[Z']}[Z'] \in K_0(\boldsymbol{M}_{k'})$ and $[k' \otimes_k \boldsymbol{L}_2] = \sum_{[Z'] \in S(\boldsymbol{M}_{k'})} n_{2,[Z']}[Z'] \in K_0(\boldsymbol{M}_{k'})$, where each $n_{i,[Z']} \in \mathbb{N}$ and all but a finite number of the $n_{i,[Z']}$'s being zero. Based on the last two paragraphs we get that for $i \in \{1,2\}$ we have

$$\sum_{[Z']\in o'} n_{i,[Z']} = m_o s_o \sum_{[Z]\in o} n_{i,[Z]}. \tag{12}$$

As we have assumed that the Equation (11) holds in the case when the pair $(k, O(\boldsymbol{M}, G, H))$ is replaced by the pair $(k', O(\boldsymbol{M}_{k'}, G_{k'}, H_{k'}))$, we have $\sum_{[Z']\in o'} n_{1,[Z']} = \sum_{[Z']\in o'} n_{2,[Z']}$. From this and the Equation (12) we get that the Equation (11) holds. $\square$

5.1 Step 1: reduction to the case of a finite field

In this subsection we show that to prove (11) for all orbits $o \in O(\boldsymbol{M}, G, H)$ we can assume that k is a finite field. Based on Lemma 6 we can assume that each simple factor of a composition series of either $\boldsymbol{L}_1$ or $\boldsymbol{L}_2$ is absolutely simple. Let $\mathcal{R}$ be a finitely generated $\mathbb{F}_p$-subalgebra of k such that the following five properties hold for it:

(i) There exist a truncated Barsotti–Tate group $\mathcal{G}$ of level m over $\mathcal{R}$ and a finite flat commutative group scheme $\mathcal{H}$ over $\mathcal{R}$ annihilated by p^m such that $G = \mathcal{G}_k$ and $H = \mathcal{H}_k$.

(ii) The reduced scheme $\mathbf{End}(\mathcal{G})_{\text{red}} \times_{\mathcal{R}} \mathbf{End}(\mathcal{H})^{\text{opp}}_{\text{red}}$ is a smooth subgroup scheme of $\mathbf{End}(\mathcal{G}) \times_{\mathcal{R}} \mathbf{End}(\mathcal{H})^{\text{opp}}$; let $\boldsymbol{\mathcal{M}}$ be the multiplicative monoid scheme over $\mathcal{R}$ associated to the reduced ring scheme $\mathbf{End}(\mathcal{G})_{\text{red}} \times_{\mathcal{R}} \mathbf{End}(\mathcal{H})^{\text{opp}}_{\text{red}}$.

(iii) The reduced scheme $\mathbf{Hom}(\mathcal{G}, \mathcal{H})_{\text{red}} \times_{\mathcal{R}} \mathbf{Hom}(\mathcal{H}, \mathcal{G})_{\text{red}}$ is a smooth subgroup scheme of $\mathbf{Hom}(\mathcal{G}, \mathcal{H}) \times_{\mathcal{R}} \mathbf{Hom}(\mathcal{H}, \mathcal{G})$; let $\boldsymbol{\mathcal{L}}_1$ and $\boldsymbol{\mathcal{L}}_2$ be the Lie algebras over $\mathcal{R}$ of $\mathbf{Hom}(\mathcal{G}, \mathcal{H})_{\text{red}}$ and $\mathbf{Hom}(\mathcal{H}, \mathcal{G})_{\text{red}}$ (respectively) and let $\boldsymbol{\mathcal{L}}_1^\vee = \mathrm{Hom}_{\mathcal{R}}(\boldsymbol{\mathcal{L}}_1, \mathcal{R})$ be the $\mathcal{R}$-dual of the $\mathcal{R}$-module $\boldsymbol{\mathcal{L}}_1$.

(iv) The left $\boldsymbol{\mathcal{M}}$-modules $\boldsymbol{\mathcal{L}}_1^\vee$ and $\boldsymbol{\mathcal{L}}_2$ have a composition series whose factors $\mathcal{Z}_{1,1}, \ldots, \mathcal{Z}_{1,s_1}$ and $\mathcal{Z}_{2,1}, \ldots, \mathcal{Z}_{1,s_2}$ (respectively) have absolutely simple fibers and are defined by free $\mathcal{R}$-modules.

(v) If $j_1, j_2 \in \{(1,1), \ldots, (1,s_1), (2,1), \ldots, (2,s_2)\}$ are distinct elements such that the simple left $\boldsymbol{M}$-modules $\mathcal{Z}_{j_1} \otimes_{\mathcal{R}} k$ and $\mathcal{Z}_{j_2} \otimes_{\mathcal{R}} k$ have different images in $K_0(\boldsymbol{M})/I_0(\boldsymbol{M})$ (equivalently, if $[\mathcal{Z}_{j_1} \otimes_{\mathcal{R}} k]$ and $[\mathcal{Z}_{j_2} \otimes_{\mathcal{R}} k]$ do not belong to the same orbit of $O(\boldsymbol{M})$), then there exists a maximal ideal $\mathfrak{i}$ of $\mathcal{R}$ such that the absolutely simple left $\boldsymbol{\mathcal{M}}/\mathfrak{i}\boldsymbol{\mathcal{M}}$-module $\mathcal{Z}_{j_1}/\mathfrak{i}\mathcal{Z}_{j_1}$ is not isomorphic to $(\mathcal{Z}_{j_2}/\mathfrak{i}\mathcal{Z}_{j_2})^{(\sigma_l^i)}$ for all $i \in \mathbb{N}$, where σ_l is the Frobenius automorphism of the finite field $l = \mathcal{R}/\mathfrak{i}$.

The existence of $\mathcal{R}$ such that properties (i) to (iv) hold is a standard piece of algebraic geometry. Based on the Fact 7, there exists $n_{G,H} \in \mathbb{N}^*$ such that the property (v) holds if and only if the following property holds:

(v-) If j_1, j_2 are as in the property (v), then there exists a maximal ideal $\mathfrak{i}$ of $\mathcal{R}$ such that the left $\boldsymbol{\mathcal{M}}/\mathfrak{i}\boldsymbol{\mathcal{M}}$-module $\mathcal{Z}_{j_1}/\mathfrak{i}\mathcal{Z}_{j_1}$ is not isomorphic to $(\mathcal{Z}_{j_2}/\mathfrak{i}\mathcal{Z}_{j_2})^{(\sigma_{\mathfrak{i}}^i)}$ for all $i \in \{0, 1, \ldots, n_{G,H}\}$.

But by localizing $\mathcal{R}$ we can assume that the property (v-) holds for all maximal ideals of $\mathcal{R}$ and therefore we can indeed choose $\mathcal{R}$ such that the properties (i) to (v) hold.

We have an inective pullback map $O(\boldsymbol{M}, G, H) \hookrightarrow O(\boldsymbol{\mathcal{M}}/\mathfrak{i}\boldsymbol{\mathcal{M}})$, cf. properties (iv) and (v). Thus to prove that (11) holds it suffices to show that Equation (11) holds in the case when the pair $(k, O(\boldsymbol{M}, G, H))$ is replaced by the pair $(l, O(\boldsymbol{\mathcal{M}}/\mathfrak{i}\boldsymbol{\mathcal{M}}, \mathcal{G}_l, \mathcal{H}_l))$. Therefore to prove that the Equation (11) holds we can assume that $k = l$ is a finite field.

5.2 Step 2: reduction to the case of abstract monoids

As k is finite, we can assume that $(\mathcal{R}, \boldsymbol{\mathcal{L}}_1, \boldsymbol{\mathcal{L}}_2) = (k, \boldsymbol{L}_1, \boldsymbol{L}_2)$ and thus that $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ have composition series whose factors are denoted as above by $\mathcal{Z}_{1,1}, \ldots, \mathcal{Z}_{1,s_1}$ and $\mathcal{Z}_{2,1}, \ldots, \mathcal{Z}_{1,s_2}$ (respectively).

To prove that the Equation (11) holds we can replace the finite field k by a finite field extension of it (cf. Lemma 6). Thus we can assume that the following two properties also hold:

(i) for each element $j \in \{(1,1), \ldots, (1, s_1), (2,1), \ldots, (2, s_2)\}$, $\mathcal{Z}_j$ is an absolutely simple left $\boldsymbol{M}(k)$-module;

(ii) for each distinct elements $j_1, j_2 \in \{(1,1), \ldots, (1, s_1), (2,1), \ldots, (2, s_2)\}$, $[\mathcal{Z}_{j_1}]$ and $[\mathcal{Z}_{j_2}]$ belong to the same orbit $o \in O(\boldsymbol{M}, G, H)$ if and only if $\mathcal{Z}_{j_1}$ and $\mathcal{Z}_{j_2}$ belong to the same orbit of the natural (analogous) action of σ on the set of isomorphism classes of finite dimensional simple left $\boldsymbol{M}(k)$-modules.

Let the groups $K_0(\boldsymbol{M}(k))$, $I_0(\boldsymbol{M}(k))$, $K_0(\boldsymbol{M}(k))/I_0(\boldsymbol{M}(k))$ and the set $O(\boldsymbol{M}(k), G, H) \subset O(\boldsymbol{M}(k))$ be analogues to the groups $K_0(\boldsymbol{M})$, $I_0(\boldsymbol{M})$, $K_0(\boldsymbol{M})/I_0(\boldsymbol{M})$ and the set $O(\boldsymbol{M}, G, H) \subset O(\boldsymbol{M}(k))$ (respectively) but working in the category of finite dimensional k-vector spaces which are left modules over the abstract monoid $\boldsymbol{M}(k)$. We have an injective pullback map $O(\boldsymbol{M}, G, H) \hookrightarrow O(\boldsymbol{M}(k), G, H)$, cf. properties (i) and (ii). Thus to prove that the Equation (11) holds it suffices to show that it holds in the case when the pair $(\boldsymbol{M}, O(\boldsymbol{M}, G, H))$ is replaced by the pair $(\boldsymbol{M}(k), O(\boldsymbol{M}(k), G, H))$. Therefore to prove that the Equation (11) holds we can assume that k is a finite field and we are viewing $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ as left modules over the abstract monoid $\boldsymbol{M}(k) = \mathrm{End}(G) \times \mathrm{End}(H)^{\mathrm{opp}} = \mathrm{End}(G) \times \mathrm{End}(H^{\mathrm{t}}) = \mathbf{End}(G)_{\mathrm{red}}(k) \times \mathbf{End}(H)^{\mathrm{opp}}_{\mathrm{red}}(k) = \mathbf{End}(G)_{\mathrm{red}}(k) \times \mathbf{End}(H^{\mathrm{t}})_{\mathrm{red}}(k)$; to emphasize the $\mathbb{F}_p$-algebra structures we will denote $\boldsymbol{A}_G = \mathrm{End}(G)$ and $\boldsymbol{A}_{H^{\mathrm{t}}} = \mathrm{End}(H^{\mathrm{t}})$ viewed as finite dimensional $\mathbb{F}_p$-algebras.

The left modules $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ over the abstract monoid $\mathrm{End}(G) \times \{1_{H^{\mathrm{t}}}\}$ are actually left $\boldsymbol{A}_G$-modules and for each $h \in \mathrm{End}(H)^{\mathrm{opp}} = \mathrm{End}(H^{\mathrm{t}})$ the multiplication by $(1_G, h)$ on $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ are $\boldsymbol{A}_G$-linear transformations. Similarly, the left modules $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ over the abstract monoid $\{1_G\} \times \mathrm{End}(H^{\mathrm{t}})$ are actually left $\boldsymbol{A}_{H^{\mathrm{t}}}$-modules and for each $g \in \mathrm{End}(G)$ the multiplication by $(g, 1_{H^{\mathrm{t}}})$ on $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ are $\boldsymbol{A}_{H^{\mathrm{t}}}$-linear transformations. From the last two we get that $\boldsymbol{L}_1^\vee$ and $\boldsymbol{L}_2$ have composition series which are also series of left $\boldsymbol{A}_G$-modules and left $\boldsymbol{A}_{H^{\mathrm{t}}}$-modules, and therefore we can assume that $\mathcal{Z}_j$ with $j \in \{(1,1), \ldots, (1, s_1), (2,1), \ldots, (2, s_2)\}$ are left $\boldsymbol{A}_G$-modules and left $\boldsymbol{A}_{H^{\mathrm{t}}}$-modules with the property that the identity elements of $\boldsymbol{A}_G$ and $\boldsymbol{A}_{H^{\mathrm{t}}}$ act identically on them.

5.3 Step 3: applying Theorem 2

We consider the Jacobson radical $J(\boldsymbol{A}_G)$ of $\boldsymbol{A}_G$. The quotient ring $\boldsymbol{S}_G = \boldsymbol{A}_G/J(\boldsymbol{A}_G)$ is semisimple and thus a finite product $\boldsymbol{S}_G = \prod_{i=1}^s \boldsymbol{S}_{G,i}$ of simple rings. Each idempotent of $\boldsymbol{A}_G/J(\boldsymbol{A}_G)$ lifts to an idempotent of $\boldsymbol{A}_G$ and thus we can assume that we have a product decomposition

$$\boldsymbol{A}_G = \prod_{i=1}^{s} \boldsymbol{A}_{G,i} \tag{13}$$

of $\mathbb{F}_p$-algebras such that for each $i \in \{1, \ldots, s\}$ we have a canonical identification $\boldsymbol{S}_{G,i} = \boldsymbol{A}_{G,i}/J(\boldsymbol{A}_{G,i})$. To the decomposition (13) corresponds product decompositions $G = \prod_{i=1}^s G_i$, $\boldsymbol{Hom}(G, H) = \prod_{i=1}^s \boldsymbol{Hom}(G_i, H)$, and $\boldsymbol{Hom}(H, G) = \prod_{i=1}^s \boldsymbol{Hom}(H, G_i)$. Thus to prove that Theorem 3 holds (equivalently that the Equation (11) holds in the case when the initial pair $(\boldsymbol{M}, O(\boldsymbol{M}, H, G))$ is replaced by the pair $(\boldsymbol{M}(k), O(\boldsymbol{M}(k), G, H)))$ we can assume that $s = 1$ and therefore that $\boldsymbol{S}_G$ is a simple $\mathbb{F}_p$-algebra.

A similar argument shows that we can assume that $\boldsymbol{S}_{H^{\mathrm{t}}} = \boldsymbol{A}_{H^{\mathrm{t}}}/J(\boldsymbol{A}_{H^{\mathrm{t}}})$ is also a simple $\mathbb{F}_p$-algebra. But in such a case, up to isomorphism there exists a unique simple left $\boldsymbol{M}(k)$-module on which the identity elements of both $\boldsymbol{A}_G$ and $\boldsymbol{A}_{H^{\mathrm{t}}}$ act identically and therefore the analogue of the Equation (11) for the case when the pair $(\boldsymbol{M}, O(\boldsymbol{M}, G, H))$ is replaced by the pair $(\boldsymbol{M}(k), O(\boldsymbol{M}(k), G, H))$ becomes the identity $\dim_k(\boldsymbol{L}_1^\vee) = \dim_k(\boldsymbol{L}_2)$ which is equivalent to the Equation (1) as $\dim_k(\boldsymbol{L}_1^\vee) = \dim_k(\boldsymbol{L}_1) = \dim(\mathbf{Hom}(G, H))$ and $\dim_k(\boldsymbol{L}_2) = \dim(\mathbf{Hom}(H, G))$. This ends the proof of Theorem 3. $\square$

5.4 Remark

The ring scheme $\boldsymbol{End}(G)$ has $\boldsymbol{End}(G)^0$ as a two-sided ideal subscheme and the quotient ring scheme $\boldsymbol{C}_G = \boldsymbol{End}(G)/\boldsymbol{End}(G)^0 = \boldsymbol{End}(G)_{\mathrm{red}}/\boldsymbol{End}(G)^0_{\mathrm{red}}$ is étale. From [GV], Corollary 6 (b) we get that $\boldsymbol{Aut}(G)^0(k) = 1_M + \boldsymbol{End}(G)^0(k)$. From this and the fact that $\boldsymbol{Aut}(G)^0_{\mathrm{red}}$ is a unipotent group scheme (cf. [GV], Corollary 5), we get that there exists a composition series of the $W_m(k)$-module M which is left invariant by all crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$ and whose simple factors are one dimensional k-vector spaces annihilated by all crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$. Thus there exists $u \in \mathbb{N}^*$ with the property that each product of arbitrary u endomorphisms of the Dieudonné module M of G that are crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$, is zero. For $v \in \{1, \ldots, u\}$, let M_v be the $W_m(k)$-submodule of M generated by all $(f_1 f_2 \cdots f_v)(M)$ with $f_1, \ldots, f_v$ as $W_m(k)$-endomorphisms of M that are crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$. We obtain a filtration

$$0 = M_u \subset M_{u_1} \subset \cdots \subset M_1 \subset M$$

by $W_m(k)$-submodules left invariant by all crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$ whose factors are annihilated by all crystalline realizations of elements of $\boldsymbol{End}(G)^0(k)$. This implies that $\boldsymbol{End}(G)^0_{\mathrm{red}}$ acts trivially on each $\mathcal{Z}_j$ with $j \in \{(1,1), \ldots, (1, s_1), (2,1), \ldots, (2, s_2)\}$. Therefore $\mathcal{Z}_j$ is a left $\boldsymbol{C}_G$-module.

If H is also a truncated Barsotti–Tate group, then as in the previous paragraph we argue that $\boldsymbol{End}(G)^0_{\mathrm{red}} \times \boldsymbol{End}(H^{\mathrm{t}})^0_{\mathrm{red}}$ acts trivially on each $\mathcal{Z}_j$ and therefore $\mathcal{Z}_j$ is a left $\boldsymbol{C}_G$-module as well as a left $\boldsymbol{C}_{H^{\mathrm{t}}}$-module; thus in such a case the three steps above could be easily combined with $\boldsymbol{A}_G$ and $\boldsymbol{A}_{H^{\mathrm{t}}}$ being replaced by the étale ring schemes $\boldsymbol{C}_G$ and $\boldsymbol{C}_{H^{\mathrm{t}}}$.

6 Isogeny and Symmetry Properties in the Relative Context

Let L be the (contravarint) Dieudonné module of a Barsotti–Tate group D over k. In order to match our notations with the ones of [GV] (modulo the replacement of M by L), let $\phi : L \to L$ and $\vartheta : L \to L$ be the σ-linear map and the σ^{-1}-linear map (respectively) such that for each $x \in L$ we have $\phi(x) = Fx$ and $\vartheta(x) = Vx$. We denote also by $\phi : \mathrm{End}_{B(k)}(L[\frac{1}{p}]) \to \mathrm{End}_{B(k)}(L[\frac{1}{p}])$ the σ-linear automorphism induced naturally by ϕ: it maps $h \in \mathrm{End}_{B(k)}(L[\frac{1}{p}])$ to $\phi \circ h \circ \phi^{-1} \in \mathrm{End}_{B(k)}(L[\frac{1}{p}])$. Therefore $\phi(h) = \frac{1}{p}FhV$.

Let $\mathcal{G}$ be a smooth closed subgroup scheme of $\boldsymbol{GL}_L$ such that its generic fiber $\mathcal{G}_{B(k)}$ is connected. Thus the scheme $\mathcal{G}$ is integral. Let $\mathfrak{g} := \mathrm{Lie}(\mathcal{G})$ be the Lie algebra of $\mathcal{G}$. Until the end we will assume that the following two axioms introduced in [GV], Section 6 hold for the triple $(L, \phi, \mathcal{G})$:

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

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

(a) the kernel $\bar{F}^1$ of the reduction modulo p of ϕ is F^1/pF^1;

(b) the cocharacter $\mu : \mathbb{G}_m \to \boldsymbol{GL}_L$ which acts trivially on F^0 and via the inverse of the identical character of $\mathbb{G}_m$ on F^1, normalizes $\mathcal{G}$.

The triple $(L, \phi, \mathcal{G})$ is called an *F-crystal with a group* over k, cf. [V1], Definition 1.1 (a) and Subsection 2.1. Let $n_D^{\mathcal{G}}$ be the smallest nonnegative integer that has the following property: for each element $\tilde{g} \in \mathcal{G}(W(k))$ congruent to 1_L modulo $p^{n_D^{\mathcal{G}}}$, there exists an inner isomorphism between $(L, \phi, \mathcal{G})$ and $(L, \tilde{g}\phi, \mathcal{G})$. The existence of $n_D^{\mathcal{G}}$ is implied by [V1], Main Theorem A. If $\mathcal{G} = \boldsymbol{GL}_L$, then we have $n_D^{\mathcal{G}} = n_D$ (see [GV], Subsection 5.1).

For $m \in \mathbb{N}^*$ let ϕ_m, ϑ_m be the reductions modulo p^m of ϕ and ϑ (respectively). Let $\flat^{(\sigma)}$ be the pullback (or the tensorization) of some $W(k)$-linear map or $W(k)$-module $\flat$ with σ. Thus $L^{(\sigma)} := W(k) \otimes_{\sigma, W(k)} L$, etc.

Definition 4 **(a)** *By the family of F-crystals with a group over k associated to $(L, \phi, \mathcal{G})$ we mean the set $\mathcal{F}$ of all F-crystals with a group over k of the form $(L, g\phi, \mathcal{G})$ with $g \in \mathcal{G}(W(k))$.*

(b) *For $g_1, g_2 \in \mathcal{G}(W(k))$ we say that $(L, g_1\phi, \mathcal{G})$ and $(L, g_2\phi, \mathcal{G})$ are $\mathcal{G}$-isogeneous if there exists an element $h \in \mathcal{G}(B(k))$ such that $hg_1\phi = g_2\phi h$.*

For $g \in \mathcal{G}(W(k))$ let D_g be the Barsotti–Tate group over k whose Dieudonné module is $(L, g\phi, \vartheta g^{-1})$; it has the same dimension and codimension as D. Note that $D = D_{1_L}$. Moreover, if $\mathcal{G} = \boldsymbol{GL}_L$, then each Barsotti–Tate group over k of the same dimension and codimension as D is isomorphic to D_g for some $g \in \mathcal{G}(W(k))$.

Let $g_m \in \mathcal{G}(W_m(k))$ be the reduction modulo p^m of g. Let

$$\boldsymbol{Hom}(D[p^m], D_g[p^m])_{\mathrm{crys}}$$

be the group scheme over k of endomorphisms from $(L/p^mL, g_m\phi_m, \vartheta_m g_m^{-1})$ to $(L/p^mL, \phi_m, \vartheta_m)$. Thus, if R is a commutative k-algebra and if σ_R is the Frobenius endomorphism of the ring $W_m(R)$ of p-typical Witt vectors of length m with coefficients in R, then $\boldsymbol{Hom}(D[p^m], D_g[p^m])_{\mathrm{crys}}(R)$ is the group of those $W_m(R)$-linear endomorphisms $\natural$ of $W_m(R) \otimes_{W_m(k)} L/p^mL$ that satisfy the identities $(1_{W_m(R)} \otimes \phi_m) \circ \natural^{(\sigma)} = \natural \circ (1_{W_m(R)} \otimes g_m\phi_m)$ and $\natural^{(\sigma)} \circ (1_{W_m(R)} \otimes \vartheta_m g_m^{-1}) = (1_{W_m(R)} \otimes \vartheta_m) \otimes \natural$; here ϕ_m and ϑ_m are viewed as $W_m(k)$-linear maps $(L/p^mL)^{(\sigma)} \to L/p^mL$ and $L/p^mL \to (L/p^mL)^{(\sigma)}$ (respectively).

We consider the closed subgroup scheme

$$\boldsymbol{Hom}(D[p^m], D_g[p^m])^{\mathcal{G}}_{\mathrm{crys}}$$

of $\boldsymbol{Hom}(D[p^m], D_g[p^m])_{\mathrm{crys}}$ such that for each commutative k-algebra R, the subgroup $\boldsymbol{Hom}(D[p^m], D_g[p^m])^{\mathcal{G}}_{\mathrm{crys}}(R)$ of $\boldsymbol{Hom}(D[p^m], D_g[p^m])_{\mathrm{crys}}(R)$ consists of all those $W_m(R)$-linear endomorphisms $\natural$ of $W_m(R) \otimes_{W_m(k)} L/p^mL$ which in fact are elements of $W_m(R) \otimes_{W_m(k)} \mathfrak{g}/p^m\mathfrak{g}$. The goal of this section is to prove the following theorem that generalizes the particular case of Theorem 1 in which D and E have the same dimension and codimension.

Theorem 4 *For each $g \in \mathcal{G}(W(k))$ the following three properties hold:*

(a) *There exists a smallest nonnegative integer $n^{\mathcal{G}}_{D,D_g}$ such that for all integers $n \geq n^{\mathcal{G}}_{D,D_g}$ we have an equality*

$$\dim(\boldsymbol{Hom}(D[p^n], D_g[p^n])^{\mathcal{G}}_{crys}) = \dim(\boldsymbol{Hom}(D[p^{n^{\mathcal{G}}_{D,D_g}}], D_g[p^{n^{\mathcal{G}}_{D,D_g}}])^{\mathcal{G}}_{crys}).$$

Moreover, if $n^{\mathcal{G}}_{D,D_g} > 0$, then the finite sequence

$$(\dim(\boldsymbol{Hom}(D[p^n], D_g[p^n])^{\mathcal{G}}_{crys}))_{n \in \{1,\ldots,n^{\mathcal{G}}_{D,D_g}\}}$$

is strictly increasing.

(b) *If* $s^{\mathcal{G}}_{D,D_g} = \dim(\boldsymbol{Hom}(D[p^{n^{\mathcal{G}}_{D,D_g}}], D_g[p^{n^{\mathcal{G}}_{D,D_g}}])^{\mathcal{G}}_{crys})$*, then* $s^{\mathcal{G}}_{D,D_g}$ *is an isogeny invariant. In other words, for all elements* $g_1, g_2 \in \mathcal{G}(W(k))$ *such that* $(L, g_1\phi, \mathcal{G})$ *and* $(L, g_2\phi, \mathcal{G})$ *are* $\mathcal{G}$*-isogeneous to* $(L, \phi, \mathcal{G})$ *and* $(L, g\phi, \mathcal{G})$ *(respectively), we have* $s^{\mathcal{G}}_{D,D_g} = s^{\mathcal{G}}_{D_{g_1},D_{g_2}}$.

(c) *Let* $Tr : \mathrm{End}_{W(k)}(L) \times \mathrm{End}_{W(k)}(L) \to W(k)$ *be the trace bilinear map that maps a pair* $(a, b) \in \mathrm{End}_{W(k)}(L) \times \mathrm{End}_{W(k)}(L)$ *to the trace of the* $W(k)$*-linear endomorphism* $a \circ b : L \to L$*. We assume that* Tr *restricts to a perfect bilinear map* $Tr_{\mathfrak{g}} : \mathfrak{g} \times \mathfrak{g} \to W(k)$ *(this forces* $\mathcal{G}$ *to be a reductive group scheme over* $W(k)$*). Then we have the following symmetry properties* $s^{\mathcal{G}}_{D,D_g} = s^{\mathcal{G}}_{D_g,D}$ *and* $n^{\mathcal{G}}_{D,D_g} = n^{\mathcal{G}}_{D_g,D}$.

Proof: Let L_1 and L_2 be L. Let $E = D \oplus D_g$; it is a Barsotti–Tate group over k whose Dieudonné module is $(L \oplus L, \phi \oplus g\phi) = (L_1 \oplus L_2, \phi \oplus g\phi)$. Let $\mathfrak{h}$ be the Lie subalgebra of $\mathrm{End}_{W(k)}(L \oplus L) = \mathrm{End}_{W(k)}(L_1 \oplus L_2)$ formed by all those $W(k)$-linear endomorphisms of $L \oplus L = L_1 \oplus L_2$ which annihilate L_1, which map L_2 into L_1, and for which the resulting $W(k)$-linear map from $L_2 = L$ to $L_1 = L$ is an element of $\mathfrak{g}$.

Let $\mathcal{H}$ be the closed subgroup scheme of $\boldsymbol{GL}_{L\oplus L}$ with the property that for each commutative k-algebra R, we have

$$\mathcal{H}(R) = 1_{W(R)\otimes_{W(k)}(L\oplus L)} + W(R) \otimes_{W(k)} \mathfrak{h}.$$

The Lie algebra of $\mathcal{H}$ is $\mathfrak{h}$ and the triple $(L \oplus L, \phi \oplus g\phi, \mathcal{H})$ is an F-crystal with a group over k.

For $m \in \mathbb{N}^*$ let $\boldsymbol{Aut}(D[p^m] \oplus D_g[p^m])^{\mathcal{H}}_{\mathrm{crys}}$ be the group scheme over k defined in [GV], Definition 2 (a). We have a canonical identification

$$\boldsymbol{Hom}(D[p^m], D_g[p^m])^{\mathcal{G}}_{\mathrm{crys}} = \boldsymbol{Aut}(D[p^m] \oplus D_g[p^m])^{\mathcal{H}}_{\mathrm{crys}} \tag{14}$$

of affine group schemes over k, which for a commutative k-algebra R maps $\natural \in \boldsymbol{Hom}(D[p^m], D_g[p^m])^{\mathcal{G}}_{\mathrm{crys}}(R)$ to $1_{W(R)\otimes_{W(k)}(L\oplus L)} + \natural$, where $\natural$ is identified with a $W_m(R)$-linear endomorphism of $W_m(R)\otimes_{W_m(k)}(L\oplus L) = W_m(R)\otimes_{W_m(k)}(L_1\oplus L_2)$ which annihilates $W_m(R) \otimes_{W_m(k)} L_1$ and which maps $W_m(R) \otimes_{W_m(k)} L_2$ to $W_m(R) \otimes_{W_m(k)} L_1$ in the same way as $\natural$ does.

As the product of two elements of $\mathfrak{h}$ is 0, $W(k)1_L + \mathfrak{h}$ is a $W(k)$-subalgebra of $\mathrm{End}_{W(k)}(L\oplus L)$ and therefore the hypothesis of [GV], Theorem 6 holds for the triple $(L \oplus L, \phi \oplus g\phi, \mathcal{H})$. Therefore the fact that (a) holds follows from [GV], Proposition 2 (c) and Theorem 6 and the Equation (14).

In order to prove (b) and (c), we can assume that k is algebraically closed and we first consider the σ-linear isomorphisms

$$\phi_{D,D_g}, \phi_{D_g,D} : \mathfrak{g}[\frac{1}{p}] \to \mathfrak{g}[\frac{1}{p}]$$

which map $h \in \mathfrak{g}[\frac{1}{p}]$ to $\phi \circ h \circ \phi^{-1} g^{-1}$ and $g\phi \circ h \circ \phi^{-1}$ (respectively). For all $x, y \in \mathrm{End}_{W(k)}(L)$ we have an identity

$$\sigma(Tr(x, y)) = Tr(\phi_{D,D_g}(x), \phi_{D_g,D}(y)). \tag{15}$$

Thus the fact that $\mathrm{Tr}_{\mathfrak{g}}$ is perfect implies that $\mathrm{Tr}_{\mathfrak{g}}$ induces an isomorphism of latticed F-isocrystals from the dual of $(\mathfrak{g}, \phi_{D_g,D})$ to $(\mathfrak{g}, \phi_{D,D_g})$. Based on this, the proofs of (b) and (c) are entirely analogous to the proofs of Subsections 3.1 and 3.2, with the roles of L and J being replaced by $L = L_1$ and $L = L_2$ (respectively) and with the roles of $\mathrm{Hom}_{W(k)}(J, L)$ and $\mathrm{Hom}_{W(k)}(L, J)$ being replaced by the Lie subalgebra $\mathfrak{g}$ of $\mathrm{End}_{W(k)}(L) = \mathrm{Hom}_{W(k)}(L_2, L_1)$ and of $\mathrm{End}_{W(k)}(L) = \mathrm{Hom}_{W(k)}(L_1, L_2)$ (respectively). We would only like to add that, due to the axiom (AX1), with the notations $\mathrm{Hom}_{W(k)}(J, L)^\flat$ and $\mathrm{Hom}_{W(k)}(J, L)^\sharp$ of Subsections 3.1 and 3.2 but used under the mentioned replacement of roles, for $\diamond \in \{\{D_g, D\}, \{D, D_g\}\}$ we take $\mathfrak{g}_\diamond^\flat$ to be

$$\mathfrak{g} \cap \mathrm{Hom}_{W(k)}(L_2, L_1)^\flat = \{x \in \mathfrak{g} | \phi_\diamond(x) \in \mathrm{Hom}_{W(k)}(L_2, L_1)\} = \mathfrak{g} \cap \phi_\diamond^{-1}(\mathfrak{g})$$

and we take $\mathfrak{g}_\diamond^\sharp$ to be

$$\mathfrak{g}[\frac{1}{p}] \cap \mathrm{Hom}_{W(k)}(L_2, L_1)^\sharp = \mathfrak{g} + (\mathfrak{g}[\frac{1}{p}] \cap \phi_\diamond(\mathrm{Hom}_{W(k)}(L_2, L_1))) = \mathfrak{g} + \phi_\diamond(\mathfrak{g}).$$

Note that the dual of $\mathfrak{g}^\sharp_{D,D_g}$ is $\mathfrak{g}^\flat_{D_g,D}$. $\square$

Acknowledgement. The second author would like to thank Binghamton University, U.S.A., Mathematisches Forschungsinstitut Oberwolfach, Germany, I.H.E.S., Bures-sur-Yvette, France, and I.I.S.E.R., Thiruvananthapuram, India for good working conditions.

References

[B] L. Begueri, *Dualité sur un corps local à corps résiduel algébriquement clos*, Mém. Soc. Math. France (N.S.) 1980/81, no. 4

[BD] M. Boyarchenko and V. Drinfeld, *Character sheaves on unipotent groups in positive characteristic: foundations,* Selecta Math. (N.S.) **20** (2014), no. 1, 125–235

[GV] O. Gabber and A. Vasiu, *Dimensions of group schemes of automorphisms of truncated Barsotti–Tate groups,* Int. Math. Res. Not. IMRN **2013**, no. 18, 4285–4333

[I] L. Illusie, *Déformations de groupes de Barsotti–Tate (d'apès A. Grothendieck),* Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (Paris, 1983/84), 151–198, Astérisque **127**, Soc. Math. de France, Paris, 1985

[LNV] E. Lau, M.-H. Nicole, and A. Vasiu, *Stratifications of Newton polygon strata and Traverso's conjectures for p-divisible groups,* Ann. of Math. (2) **178** (2013), no. 3, 789–834

[S1] J.-P. Serre, *Groupes proalgébriques,* Inst. Hautes Études Sci. Publ. Math. No. **7**, 1960

[S2] J.-P. Serre, *Trees,* Springer-Verlag, Berlin-New York, 1980

[V1] A. Vasiu, *Crystalline boundedness principle,* Ann. Sci. École Norm. Sup. **39** (2006), no. 2, 245–300

[V2] A. Vasiu, *Level m stratifications of versal deformations of p-divisible groups,* J. Alg. Geom. **17** (2008), no. 4, 599–641

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

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