Isogeny and symmetry properties for Barsotti–Tate groups

Ofer Gabber and Adrian Vasiu

March 11, 2015

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 $\dim(\text{Hom}(D[p^n], E[p^n]))$ is an isogeny invariant i.e., it does not change if $D$ and $E$ are 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 $p$-divisible 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 $\dim(\text{Hom}(G, H)) = \dim(\text{Hom}(H, G))$. 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 $\text{End}(G)_{\text{red}} \times_k \text{End}(H)^{\text{opp}}_{\text{red}}$.

KEY WORDS: Group schemes, Lie algebras, monoids, representations, (truncated) Barsotti–Tate groups, proalgebraic groups, and Dieudonné modules.

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

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

We recall that the \( a \)-number of \( G \) is \( a_G = \dim(\text{Hom} (\alpha_p, G)) \). Equivalently, \( a_G \) is the largest integer such that \( \alpha_p^{a_G} \) is a subgroup scheme of \( G \). In general, \( a_G \neq a_{G^*} \) (see Subsection 2.1) but it is well known that if \( G \) is a truncated Barsotti–Tate group, then we have \( a_G = a_{G^*} \) (for instance, see [GV, Subsect. 3.5]). The goal of the paper is to generalize this last identity in order to get several isogeny and symmetric 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 \( \dim(\text{Hom} (D[p^n], E[p^n])) = \dim(\text{Hom} (D[p^{n_{D,E}}], E[p^{n_{D,E}}])) \), cf. [GV, Subsect. 6.1]. Following [LNV, Def. 7.9] let \( s_{D,E} = \dim(\text{Hom} (D[p^{n_{D,E}}], E[p^{n_{D,E}}])) \). In Section 3 we will provide an elementary (group scheme theoretical) proof of the following isogeny property.

**Theorem 1** The dimension \( s_{D,E} \) is a symmetric isogeny 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 \( n_{D,E} = n_{E,D} \).

The case \( D = E \) and \( D' = E' \) of Theorem 1 (i.e., the equality \( s_{D,D} = s_{D',D'} \)) was first proved in [Va2, Thm. 1.2 (e)] (cf. also [GV, Rm. 4.5]). We have the following interpretation of \( n_{D,E} \) in terms of extensions (cf. [GV, Subsect. 6.1]): for \( n \in \mathbb{N} \), the homomorphism \( \text{Ext}^1(D, E) \to \text{Ext}^1(D[p^n], E[p^n]) \) 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 \( \text{Ext}^1(D, E) \to \text{Ext}^1(D[p^n], E[p^n]) \) and \( \text{Ext}^1(E, D) \to \text{Ext}^1(E[p^n], D[p^n]) \). 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 \( H \). If \( G \) is a truncated Barsotti–Tate group of level \( m \) over \( k \), then we have

\[
\dim(\text{Hom}(G, H)) = \dim(\text{Hom}(H, G)).
\]
Note that Theorem 2 also implies that $s_{D,E} = s_{E,D}$ and $n_{D,E} = n_{E,D}$ and, when combined with [Va2, Thm. 1.2 (e)], that $s_{D,E} = s_{D,E'}$ (cf. Remark 4.2 (b)). Theorem 2 does not hold in general if $m > 1$ and $G$ is a truncated Barsotti–Tate group of level strictly less than $m$ over $k$ (see Subsection 4.3).

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

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

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

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

Let $L_1$ and $L_2$ be the Lie algebras over $k$ of the reduced group schemes $\text{Hom}(G,H)_{\text{red}}$ and $\text{Hom}(H,G)_{\text{red}}$ (respectively). Let $L_1^\vee = \text{Hom}_k(L_1,k)$ be the dual $k$-vector space. Both $L_1^\vee$ and $L_2$ are naturally left $M$-modules. For instance, if $(g,h) \in M(k) = \text{End}(G)(k) \times \text{End}(H)^{\text{opp}}(k)$, then we have an endomorphism $c_{g,h} : \text{Hom}(H,G)_{\text{red}} \to \text{Hom}(H,G)_{\text{red}}$ which maps $l \in \text{Hom}(H,G)_{\text{red}}(k)$ to $g \circ l \circ h \in \text{Hom}(H,G)_{\text{red}}(k)$ and $(g,h)$ acts on $L_2$ via the Lie differential $\text{Lie}(c_{g,h}) : L_2 \to L_2$ 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 $[L_1^\vee]$ and $[L_2]$ in $K_0(M)/I_0(M)$ coincide.

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

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

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.

In Section 6 we present a generalization of the particular case of Theorem 1 in which $D$ and $E$ have the same dimension and codimension, to the relative contexts provided by quadruples of the form $(M, \phi, \vartheta, \mathcal{G})$ and $(M, g\phi, \vartheta g^{-1}, \mathcal{G})$, where $(M, \phi, \vartheta)$ and $(M, g\phi, \vartheta g^{-1})$ are the (contravariant) Dieudonné modules of two $p$-divisible groups over $k$, where $\mathcal{G}$ is a smooth integral closed subgroup scheme of $\text{GL}_M$ subject to the two axioms of [GV, Sect. 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 fibres of good integral models of Shimura varieties of Hodge type in unramified mixed characteristic $(0, p)$ (see [Va2, Sect. 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

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

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 $E = W(k)\{F, V\}$ as a subring of $\mathbb{D}$. For $m \in \mathbb{N}^*$, let $W_m(k) = W(k)/p^mW(k)$ and $E_m = E/p^mE$. The (contravariant) Dieudonné module of $G$ is a left $E$-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 $E_m$-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 $a_{G^*} = \dim_k(\text{Ker}(F : M \to M) \cap \text{Ker}(V : M \to M))$.

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

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 $Fv_1 = Fv_2 = Vv_1 = Vv_2 = 0$ and $Fv_3 = v_1$ and $Vv_3 = v_2$. Then $a_G = 1$ while $a_{G^*} = 2$. 

4
2.2 Brief review of quasi-algebraic groups over $k$

Following [Se1] 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 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 $k$.

Each quasi-algebraic group $Q$ over $k$ is the perfection $\tilde{Q}^{\text{perf}}$ of a group scheme $\tilde{Q}$ over $k$ of finite type (cf. [Se1, Prop. 10]; the proof of loc. cit. applies in the noncommutative case as well). Note that $Q = \tilde{Q}^{\text{perf}}$ is a proalgebraic group over $k$ (cf. also [Se1, Example 1) of p. 13] for the commutative case). Let $Q$ be the abelian category of commutative quasi-algebraic groups over $k$ (see [Se1, Prop 5]).

Fact 1 Let $f : U_1 \to U_2$ be a morphism of the category $Q$ 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 the two statements is equivalent to the statement that both Ker($f$) and Coker($f$) are trivial. □

2.3 The $\chi_p$ function on prounipotent groups

Until the end of Section 2 we will assume that $k$ is algebraically closed. Let $P$ be the abelian category of commutative proalgebraic groups over $k$ (see [Se1, Prop. 7]). Note that $Q$ is a full subcategory of $P$. We have a thick subcategory of $P$ 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 epimorphism $(p^n U)/(p^{n-1} U) \to (p^n U)/(p^{n+1} U)$.
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 which becomes constant for $n \geq n_0$ for some $n_0 \in \mathbb{N}^*$ and this gives that the kernel $\ker(p : p^nU \to p^{n_0}U)$ is zero dimensional and that the kernel $\ker(p : U \to U)$ is finite dimensional of dimension at most equal to $\dim(U/p^{n_0}U)$. 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 function

$$\chi_p(U) = \dim(U/pU) - \dim(\ker(p : U \to U))$$

is additive (cf. snake lemma). The proof of the following simple fact is left as an exercise.

**Fact 2** Let $U$ be a commutative prounipotent group $U$ such that $U/pU$ is finite dimensional. Then $\chi_p(U) \geq 0$. Moreover, we have $\chi_p(U) = 0$ if and only if $U$ is finite dimensional.

### 2.4 Pronipotent groups associated to $W(k)$-modules

Each finitely generated $W(k)$-module $N$ has the structure of a commutative prounipotent group $N$ with $N/pN$ finite dimensional and with $\chi_p(N) = \dim_{B(k)}(N[p])$. If $\chi_p(N) = 0$ (i.e., if $N$ has finite length), then $N$ 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 $W(A) \otimes_{W(k)} N$ and whose dimension is $\text{length}_{W(k)}(N)$.

If $X$ is a finite dimensional $B(k)$-vector space, then we view $X$ as an inductive limit $X$ of commutative proalgebraic groups $L$ given by lattices $L$ of $X$ (i.e., 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 $X$ is admissible if and only if there exist lattices $L_1$ and $L_2$ of $X$ such that $U$ is a proalgebraic subgroup of $L_1$ that contains $L_2$.

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

$$\chi(U_1, U_2) = \dim(U_1/U_3) - \dim(U_2/U_3)$$

for each admissible subgroup $U_3$ of $X$ 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 $X$ introduced in [Se2].
If $T : X \to X'$ is a homomorphism between the underlying abelian groups of two finite dimensional $B(k)$-vector spaces, then we say that $T$ is proalgebraic if and only if it comes from a proalgebraic homomorphism between lattices $T_0 : L \to L'$ i.e., we have

$$T : X \to X' = T_0 \otimes \mathbb{Z} \mathbb{Z}_{[\frac{1}{p}]} : L \otimes \mathbb{Z} \mathbb{Z}_{[\frac{1}{p}]} \to L' \otimes \mathbb{Z} \mathbb{Z}_{[\frac{1}{p}]}.$$ 

In this case we consider for each $n \in \mathbb{N}^*$ the kernel of $(T_0 \mod p^n) : L/p^nL \to L'/p^nL$. The images in $L/pL$ 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 $L/pL$ of $\text{Ker}(T_0)$ (we recall that filtered inverse limits are exact in our abelian category $P$ of commutative proalgebraic groups, cf. [Se1, Subsect. 2.3]). Then $p^{n_1-1}\text{Coker}(T_0)$ 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 $\text{Coker}(T_0)$ is killed by a power of $p$;

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

**Definition 2** We say that a proalgebraic homomorphism $\overline{T} : \overline{X} \to \overline{X}'$ is admissible if and only if it comes from a proalgebraic homomorphism between lattices $T_0 : L \to L'$ whose kernel $\text{Ker}(T_0)$ and cokernel $\text{Coker}(T_0)$ are finite dimensional (this is independent of the choice of lattices $L$ and $L'$).

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

If the $B(k)$-vector spaces $X$ and $X'$ have the same dimension, then the additivity of $\chi_p$ gives that the finite dimensionality of $\text{Ker}(T_0)$ is equivalent to the finite dimensionality of $\text{Coker}(T_0)$.

If $i$ and $j$ are distinct integers, $f : X \to X'$ is a $\sigma^i$-linear map and $g : X \to X'$ is a $\sigma^j$-linear map, then using the Dieudonné–Manin classification of $\sigma^a$-$F$-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, then for each lattice $L$ of $X$ the image $(f + g)(L)$ is an admissible subgroup of $\overline{X}$ and thus $f + g$ is admissible.
Lemma 1 Let $T : X \to X'$ be admissible. Let $U_1$ and $U_2$ (resp. $U'_1$ and $U'_2$) be admissible subgroups of $X$ (resp. of $X'$). Then the following two properties hold:

(a) we have $\chi(U'_2, T(U_2)) - \chi(U'_1, T(U_1)) = \chi(U'_2, U'_1) - \chi(U_2, U_1)$;

(b) if $T(U) \subset U'$, then for large $n$ the kernel of the induced map $U/p^nU \to U'/p^nU'$ is of dimension $\dim(U'/T(U))$.

Proof: As $T$ is admissible, there exists an admissible subgroup $U_3$ of $X$ contained in both $U_1$ and $U_2$ and such that $T(U_3)$ is an admissible subgroup of $X'$ contained in both $U'_1$ and $U'_2$. Then $\chi(U'_2, T(U_2)) - \chi(U'_1, T(U_1)) = \dim(U'_2/T(U_3)) - \dim(U'_1/T(U_3)) = \dim(U'/T(U_3))$ is equal to the difference $\dim(U'/T(U_3)) - \dim(U_1/T(U_3))$ and thus to the difference $\chi(U'_2, U'_1) - \chi(U_2, U_1)$. But as $T$ is admissible, it is surjective and Ker($T_0$) is a free finitely generated $\mathbb{Z}_p$-module and these imply that we have

$$\chi(T(U_2), T(U_1)) = \chi(U_2, U_1)$$

and thus that (a) holds. Part (b) is a standard application of the snake lemma. \(\square\)

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

Let $\text{Hom}_{W(k)}(N, L)^b$ be the sublattice of $\text{Hom}_{W(k)}(N, L)$ formed by $W(k)$-linear maps that send $VN$ to $VL$. We note that

$$\text{Hom}_{W(k)}(N, L)^b = \text{Hom}_{W(k)}(N, L) \cap \text{Hom}_{W(k)}(VN, VL)$$

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

$$\Psi_{N,L} : \text{Hom}_{W(k)}(N, L)^b \to \text{Hom}_{W(k)}(N, L)$$

(2)
defined by the abstract homomorphism

\[ \Psi_{N,L} : \text{Hom}_{W(k)}(N, L)^\# \to \text{Hom}_{W(k)}(N, L) \]

that maps \( h \in \text{Hom}_{W(k)}(N, L)^\# \) into \( h \mapsto h - \frac{1}{p} F h V \). It gives an admissible homomorphism of \( B(k) \)-vector spaces \( \Psi : X \to X \) in the sense of Section 2, where

\[ X = \text{Hom}_{B(k)}(N, L) \left[ \frac{1}{p} \right] = \text{Hom}_{W(k)}(N, L)^\# \left[ \frac{1}{p} \right] = \text{Hom}_{W(k)}(N, L) \left[ \frac{1}{p} \right]. \]

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

\[ \text{Hom}_{E}(N/p^n N, L/p^n L) = \text{Hom}(D[p^n], E[p^n]) = \text{Hom}(D[p^n], E[p^n])(k) \]

between Dieudonné modules modulo \( p^n \). The crystalline Dieudonné theory provides a natural evaluation homomorphism \( f \) from \( \text{Hom}(D[p^n], E[p^n]) \) to kernel of the reduction of \( \Psi_{N,L} \) modulo \( p^n \) (note that \( f \) is a morphism of the abelian category \( \mathcal{Q} \)). From [LNV, Lem. 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 \( N' \) be the (contravariant) Dieudonné modules of \( D' \) and \( E' \) (respectively). We have identifications \( L[p^{1/2}] = L'[p^{1/2}], N[p^{1/2}] = N'[p^{1/2}] \), and \( X = \text{Hom}_{W(k)}(N', L') \left[ \frac{1}{p} \right] = \text{Hom}_{W(k)}(N', L') \left[ \frac{1}{p} \right] \).

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

\[ s_{D,E} = \dim(\text{Hom}_{W(k)}(N, L)/\Psi_{N,L}(\text{Hom}_{W(k)}(N, L)^\#)) \]

and thus also

\[ s_{D,E} = \chi(\text{Hom}_{W(k)}(N, L), \Psi_{N,L}(\text{Hom}_{W(k)}(N, L)^\#)). \tag{3} \]

The dimension of \( \text{Hom}_{W(k)}(N, L)/\text{Hom}_{W(k)}(N, L)^\# \) is equal to the product of the dimension of \( E \) and of the codimension of \( D \). Thus the two \( k \)-vector
spaces $\text{Hom}_{W(k)}(N, L)/\text{Hom}_{W(k)}(N, L)^\flat$ and $\text{Hom}_{W(k)}(N', L')/\text{Hom}_{W(k)}(N', L')^\flat$ have the same dimension and therefore

$$\chi(\text{Hom}_{W(k)}(N', L'), \text{Hom}_{W(k)}(N, L)) = \chi(\text{Hom}_{W(k)}(N', L')^\flat, \text{Hom}_{W(k)}(N, L)^\flat).$$

(4)

From Formula (4) and Lemma 1 (a) applied with $(T, U_1, U_2, U'_1, U'_2) = (\Psi, \text{Hom}_{W(k)}(N, L)^\flat, \text{Hom}_{W(k)}(N', L')^\flat, \text{Hom}_{W(k)}(N, L), \text{Hom}_{W(k)}(N', L'))$ we get directly that $\chi(\text{Hom}_{W(k)}(N, L), \Psi_{N,L}(\text{Hom}_{W(k)}(N, L)^\flat))$ is equal to $\chi(\text{Hom}_{W(k)}(N', L'), \Psi(\text{Hom}_{W(k)}(N', L')^\flat))$. From this and Formula (3) 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 [Se1], [Be], and [BD, Sect. 3]). We recall that Serre duality is an involutory anti-equivalence 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 [Be, Prop. 1.2.1]).

We also recall that for a finitely generated $W_m(k)$-module $M$ and its dual $M^\vee = \text{Hom}_{W_m(k)}(M, W_m(k))$, the Serre dual of $M$ is $M^\vee$ in a functorial way with respect to all $\sigma^a$-linear maps with $a \in \mathbb{Z}$ (cf. [Se, Subsect. 8.4, Prop. 4 and Lem. 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 $0 \to \text{Ker}(f)^0 \to U_1 \to U_1/\text{Ker}(f)^0 \to 0$ and $0 \to \text{Im}(f) \to U_2 \to U_2/\text{Im}(f) \to 0$ as well as a natural isogeny $U_1/\text{Ker}(f)^0 \to \text{Im}(f)$. As $U_1$ and $U_2$ have the same dimension, we get that $\text{Ker}(f)^0$ and $U_2/\text{Im}(f)$ have the same dimensions. As Serre duality preserves short exact sequences, $(U_2/\text{Im}(f))^* \to \text{U}_2^*$ is a subgroup of $U_2^*$ contained in $\text{Ker}(f^*)$. As Serre duality preserves dimensions, we get that

$$\dim(\text{Ker}(f^*)) \geq \dim((U_2/\text{Im}(f))^*) = \dim(U_2/\text{Im}(f)) = \dim(\text{Ker}(f)^0).$$
Thus \(\dim(\ker(f^*)) \geq \dim(\ker(f))\). As the Serre duality is involuntary, we have \(f = (f^*)^*\) and therefore by replacing \(f\) with \(f^*\) in the last inequality we get that \(\dim(\ker(f)) \geq \dim(\ker(f^*))\). Thus \(\dim(\ker(f)) = \dim(\ker(f^*))\). □

We consider the lattice

\[
\text{Hom}_{W(k)}(N, L)^{\sharp} = \text{Hom}_{W(k)}(N, L) + \text{Hom}_{W(k)}(FN, FL)
\]

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

\[
\Psi_{N,L,+} : \text{Hom}_{W(k)}(N, L) \to \text{Hom}_{W(k)}(N, L)^{\sharp}
\]

(5)

of prounipotent groups.

The kernel of \(\Psi_{N,L,+}\) is the quasi-algebraic group \(\text{Hom}_E(N, L) = \text{Hom}(D, E)\) of Dieudonné module homomorphisms and thus is equal to the kernel of \(\Psi_{N,L}^{\sharp}\).

**Fact 3** The following two inclusions \(\text{Hom}_{W(k)}(N, L)^{\flat} \subset \text{Hom}_{W(k)}(N, L)\) and \(\text{Hom}_{W(k)}(N, L) \subset \text{Hom}_{W(k)}(N, L)^{\sharp}\) induce a quasi-isomorphism from (2) to (5) viewed as complexes of prounipotent groups and thus they also induce a quasi-isomorphism between the complexes (2) and (5) modulo \(p^m\) viewed as complexes of unipotent connected commutative quasi-algebraic groups. In particular, the kernels of the reductions modulo \(p^m\) of \(\Phi_{N,L}\) and \(\Psi_{N,L,+}\) have the same dimension.

**Proof:** If \(g, h \in \text{Hom}_{W(k)}(N, L)\) are such that \(g = h - \frac{1}{p}FhV\), then \(\frac{1}{p}FhV = g - h \in \text{Hom}_{W(k)}(N, L)\) and therefore we have \(h \in \text{Hom}_{W(k)}(N, L)^{\flat}\). If \(g \in \text{Hom}_{W(k)}(N, L)\) and \(l \in \text{Hom}_{W(k)}(FN, FL)\), then we have \(l = \frac{1}{p}FuV\) for some \(u \in \text{Hom}_{W(k)}(N, L)\) and therefore \(l - u = (g + l) - (g + u)\) belongs to the image of \(\Psi_{N,L,+}\). Based on the last three sentences we easily get that indeed the two inclusions mentioned induce a quasi-isomorphism from (2) to (5) viewed as complexes of prounipotent groups. From this the fact follows. □

We are now ready to proof Theorem 1. The Serre dual of (5) modulo \(p^m\) is isomorphic to the reduction modulo \(p^m\) of

\[
\Psi_{L,N} : \text{Hom}_{W(k)}(L, N)^{\flat} \to \text{Hom}_{W(k)}(L, N)
\]

(6)

(cf. the paragraph before Lemma 2); here (6) is the analogue of (2) but with the roles of \(N\) and \(L\) interchanged. Based on this and Lemma 2, we get
that $\text{Hom}(E[p^m], D[p^m])_{\text{red}}$ (i.e., the reduced algebraic group whose perfection is the kernel of $\Psi_{L,N}$ modulo $p^m$) has the same dimension as the kernel of the reduction modulo $p^m$ of $\Psi_{N,L}$. From this and Fact 3 we get that $\text{Hom}(E[p^m], D[p^m])_{\text{red}}$ has the same dimension as $\text{Hom}(E[p^m], D[p^m])_{\text{red}}$ (i.e., as the reduced algebraic group whose perfection is the kernel of $\Psi_{L,N}$ 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. □

4 Proof of Theorem 2

To prove Theorem 2, we will use some homological properties of left $E$-modules and some sort of noncommutative duality over the Cartier–Dieudonné ring $E$ which is analogous to the fact that for an affine connected smooth curve $\text{Spec} \ A$ 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 $\text{Spec} \ A$ via the functional “residue at infinity”.

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

**Proposition 1** (a) A left $E$-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 $E$-module $M$ of finite length corresponds to a truncated Barsotti–Tate group $G$ of level $m$ over $k$, then $M$ has a free resolution

$$0 \rightarrow E^r_m \rightarrow E^r_m \rightarrow M \rightarrow 0$$

with $r$ as the height of $G$.

**Proof:** We first prove (b). Let $D$ be a $p$-divisible 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 $E$-module which is the Dieudonné module of $D$. To prove (b) it suffices to show that we have a free resolution

$$0 \rightarrow E^r \rightarrow E^r \rightarrow L \rightarrow 0.$$

We consider a $W(k)$-basis $\{e_1, \ldots, e_r\}$ of $M$ for which there exist an element $g \in \text{Ker}(GL_L(W(k)) \rightarrow GL_L(k))$ and a permutation $\pi$ of the set
$J = \{1, 2, \ldots, r\}$ such that for each $i \in J$ we have $F e_i = p^{\varepsilon_i} g(e_{\pi(i)})$ where $\varepsilon_i \in \{0, 1\}$ is 1 if and only if $i \leq d$. The existence of such a $W(k)$-basis of $L$ follows from the classification of Barsotti–Tate groups of level 1 over $k$ obtained by Kraft and Ekedahl–Oort, to be compared with [Va2, Subsect. 2.3].

We consider two $W(k)$-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 $a_i = V b_{\pi(i)}$.

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

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

Let $h = (h_{i,j}, i, j \in J) \in GL_r(W(k))$ be the element such that for $i \in J$ we have $a_i = \sum_{j \in J} h_{i,j} b_j$. Due to the property (iii) and the fact that $g \in \text{Ker}(GL_L(W(k)) \to GL_L(k))$, we get that $h$ modulo $p$ is the identity $r \times r$ matrix with coefficients in $k$.

The left $E$-module

$$L_1 = (\oplus_{i,j} E a'_i \oplus \oplus_{i,j} b'_i) / (a'_i - \sum_{j \in J} h_{i,j} b'_j, i \in J)$$

is isomorphic to $E^r$. If $[a'_i]$ and $[b'_i]$ are the images of $a'_i$ and $b'_i$ in $L_1$, then the associations $[a'_i] \to a_i$ and $[b'_i] \to b_i$ define an $E$-linear surjection $\theta : L_1 \to L$.

Let $L_2 = E' = \oplus_{i \in J} E c_i$ and let $\eta : L_2 \to L_1$ be the $E$-linear map that maps $c_i$ to $[a'_i] - V [b'_{\pi(i)}]$ if $i \in \{1, \ldots, d\}$ and to $F[a'_i] - [b'_{\pi(i)}]$ if $i \in \{d + 1, \ldots, r\}$. The kernel of $\theta$ contains the image of $\eta$ and therefore we get a complex

$$L_2 \xrightarrow{\eta} L_1 \xrightarrow{\theta} L \to 0.$$  

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

$$0 \to L_2 \xrightarrow{\eta} L_1 \xrightarrow{\theta} L \to 0.$$  

Due to the very constructions, the left $E$-module $L_1/\eta(L_2)$ is the same as the $W(k)$-submodule $L'$ of $L_1/\eta(L_2)$ generated by $[a'_i] + \eta(L_2)$’s with $i \in J$. As the $W(k)$-linear map $L' = L_1/\eta(L_2) \to L$ 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 $L_2 \to L_1 \to L \to 0$ is exact at $L_1$. We are left to show that $\eta$ is injective. It suffices to show that the reduction $\eta_1 : L_2/pL_2 \to L_1/pL_1$ of $\eta$ modulo $p$ is injective. But as $h$ is congruent
modulo $p$ to the identity matrix, we have $L_1/pL_1 = E_1' = \oplus_{j \in J} E_1 \bar{a}_j'$, where $\bar{a}_j' = [a_j'] + pL_1$. To show that $\eta_1$ is injective, it suffices to show that the assumption that there exists a linear dependence relation with coefficients in $E_1$ of the form

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

leads to a contradiction.

We have a canonical identification $E_1 = \oplus_{i \in \mathbb{N}}^k F_i \oplus \oplus_{i \in \mathbb{N}^*} kV_i$ 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 $\alpha_i$ 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 (7) is a nonzero element of $k$, contradiction. Thus $\alpha_{d+1}, \ldots, \alpha_d \in \oplus_{i \in \mathbb{N}^*} kV_i$ and a similar argument shows that $\alpha_1, \ldots, \alpha_d \in \oplus_{i \in \mathbb{N}^*} kF_i$. From this and the equation (7) we easily get that in fact we have $\alpha_i = 0$ for all $i \in J$, contradiction. Thus $\eta_1$ is injective and this ends the proof of (b).

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

$$\cdots \xrightarrow{p^u} E_m \xrightarrow{p^{m-u}} E_m \xrightarrow{p^u} E_m/p^u E_m \rightarrow 0$$

of the right $E_m$-module $E_m/p^u E_m$. As $M$ has finite tor dimension, we have $\text{Tor}_n(E_m/p^u E_m, M) = 0$ 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 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, the left $E_1$-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

$$\cdots \xrightarrow{F} E_1 \xrightarrow{V} E_1 \xrightarrow{F} E_1/F E_1 \rightarrow 0$$

of the right $E_1$-module $E_1/F E_1$, shows that the complex

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

14
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.

We have an involutory antiautomorphism $\iota$ of $E_m$ that interchanges $F$ and $V$ and that fixes $W_m(k)$, and this allows us to transform right $E_m$-modules into left $E_m$-modules. If $L$ is a left $E_m$-module, let $L^\vee = \text{Hom}_{W_m(k)}(L, W_m(k))$ be endowed with the left $E_m$-module structure via the same rules as in the first paragraph of Section 3, and let $L^\# = \text{Hom}_{E_m}(L, E_m)$ with the left $E_m$-module structure given by the rule $(af)(x) = f(x)\iota(a)$ where $f \in L^\#$, $a \in E_m$, and $x \in L$. Similarly, the right multiplications of $E_m$ by elements $\iota(a)$ endow naturally $\text{Ext}^1_{E_m}(L, E_m)$ with the structure of a left $E_m$-module.

If $P$ is a finitely generated left $E_m$-module and $M$ a left $E_m$-module of finite length, then $\text{Hom}_{E_m}(P, M)$ has a natural structure of a commutative quasi-algebraic group $\text{Hom}_{E_m}(P, M)$. 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 $\text{Hom}_{E_m}(P, M)$ of $\text{Hom}_{E_m}(P, M)$ from the choices made.

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

**Proof:** The crystalline Dieudonné theory provides a natural evaluation morphism $f : \text{Hom}(G, H) \to \text{Hom}_{E_m}(P, M)$ of the abelian category $Q$. 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. 

**Fact 5** Let $P$ be a free left $E_m$-module of finite rank and let $M$ be a left $E_m$-module of finite length. Then the unipotent connected commutative quasi-algebraic groups $\text{Hom}_{E_m}(P, M)$ and $\text{Hom}_{E_m}(P^\#, M^\vee)$ 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 $\iota$ does.
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 2** 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 $\text{Hom}_{\mathbb{E}_m}(M,N)$ and $\text{Hom}_{\mathbb{E}_m}(M^\vee,N^\vee)$ have the same dimension.

**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 1 (b). Using Lemma 2 applied to the homomorphism

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

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

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

of $f$. Thus it suffices to show that $\text{Coker}(P_0^\# \to P_1^\#) = \text{Ext}_{\mathbb{E}_m}^1(M,\mathbb{E}_m)$ 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 $\text{Ext}_{\mathbb{E}_m}^1(N,\mathbb{E}_m)$ to $N^\vee$.

Before proving this lemma, we will need some preliminary material on left $\mathbb{E}_m$-modules. Let $S_m$ be the multiplicative subset of regular elements of $\mathbb{E}_m$ i.e., of elements $pf \mathbb{E}_m$ with nonzero images in $k[F]$ and $k[V]$. Note that $S_m$ admits calculus of left and right fractions (i.e., the left and right Ore conditions are satisfied). In other words, for each $s \in S_m$ and $x \in \mathbb{E}_m$, the intersection sets $sx \cap \mathbb{E}_m s$ and $xS \cap s\mathbb{E}_m$ are nonempty. Let $\mathbb{K}_m$ be the localization of $\mathbb{E}_m$ with respect to $S_m$ 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 $\text{Fin}(P)$ we mean the left $\mathbb{E}_m$-submodule
\[ \{x \in P | \text{$\mathbb{E}_m x$ is a finitely generated $W_m(k)$-module} \} = \ker(P \to \mathbb{K}_m \otimes_{\mathbb{E}_m} P). \]

We have the following elementary fact whose proof is left as an exercise.

**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 $\text{Ext}^1_{\mathbb{E}_m}(N, \mathbb{E}_m) = \text{Hom}_{\mathbb{E}_m}(N, \mathbb{K}_m/\mathbb{E}_m)$.

We have “development at infinity” homomorphisms to skew Laurent series rings
\[ e_{F,m} : \mathbb{K}_m \to W_m(k)((F^{-1})), \]
\[ e_{V,m} : \mathbb{K}_m \to W_m(k)((V^{-1})). \]

Let $\lambda_m : \mathbb{K}_m/\mathbb{E}_m \to W_m(k)$ be the $W_m(k)$-linear map
\[ \lambda_m([f + \mathbb{E}_m]) = (\text{constant term of } e_{F,m}(f)) - (\text{constant term of } e_{V,m}(f)). \]

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 $\text{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$ be endowed with the structure of a $(\mathbb{E}_m, W_m(k))$-bimodule by the rule $(abh)(x) = h(xa)b$ with $a \in \mathbb{E}_m$, $b \in W_m(k)$, $h \in \text{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k))$, and $x \in \mathbb{E}_m$. We define a map of $(\mathbb{E}_m, W_m(k))$-bimodules
\[ e_m : \mathbb{K}_m/\mathbb{E}_m \to \text{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k)) \]
by the rule $e_m(h + \mathbb{E}_m)(x) = \lambda_m(xh + \mathbb{E}_m)$ with $x, h \in \mathbb{E}_m$.

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

**Proof:** It suffices to show that for each $f \in S_m$, the restriction
\[ e_{f,m} : \{x \in \mathbb{K}_m/\mathbb{E}_m | fx = 0\} \to \{x \in \text{Hom}_{W_m(k)}(\mathbb{E}_m, W_m(k)) | fx = 0\} \]
of $e_m$ is a bijection of right $W_m(k)$-modules. As the domain and the codomain of $e_{f,m}$ are both free right $W_m(k)$-modules of the same finite rank equal to the rank of the right $W_m(k)$-module $\mathbb{E}_m/f\mathbb{E}_m$, it suffices to show that $e_{f,m}$ modulo $p$ is an injective $k$-linear map. Thus to prove the lemma it suffices to show that $e_1$ is injective. To check this, we can assume that $k$ is algebraically
closed and it suffices to show that the restriction of $e_1$ to each simple $E_1$-submodule $C$ of $K_1/E_1 = [k(F) \times k(V)]/E_1$ is injective.

In this and the next paragraph we will check that there exist precisely three simple left $E_1$-submodules of $K_1/E_1$: generated by $(F - 1)^{-1} + E_1$, by $(V - 1)^{-1} + E_1$, and by $(F + V)^{-1}V + E_1 = (0, 1) + E_1$. Let $x = (x_1, x_2) \in k(F) \times k(V)$ be such that $C$ is generated by $x + E_1$. If $x \in k\{F\} \times k\{V\}$, then $C = [k\{F\} \times k\{V\}]/E_1$ is a one dimensional $k$-vector space generated by $(F + V)^{-1}V + E_1$. Similarly, if either $x_1 = 0$ or $x_2 = 0$, then it is easy to see that $C = [k\{F\} \times k\{V\}]/E_1$.

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 $C$ is generated by $(F - 1)^{-1} + E_1$. 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 $x$ 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 $Fx = (1, 0) \in [k\{F\} \times k\{V\}] \setminus E_1$ and therefore $F(x + E_1)$ generates $C$ which implies that $x \in k\{F\} \times k\{V\}$ a contradiction. Thus $a \in k \setminus \{0\}$ and therefore $(F-a)x + E_1 = (0, -ax_2 - 1) + E_1$. Thus, if $-ax_2 - 1 \notin Vk\{V\}$, then from the end of the last paragraph we get that $C = [k\{F\} \times k\{V\}]/E_1$ and this contradicts the fact that $x_1 \notin k\{F\}$. Therefore $-ax_2 - 1 \in Vk\{V\}$ which implies that $x + E_1 = (F-a)^{-1} + E_1$. As $a \in k \setminus \{0\}$ and $k$ is algebraically closed, by multiplying $x$ with a nonzero element of $k$ we can assume that $x + E_1 = (F - 1)^{-1} + E_1$. As $F + VV = 1 = -\lambda_1((0, 1) + E_1) = \lambda_1((F - 1)^{-1} + E_1) = -\lambda_1((V - 1)^{-1} + E_1)$, we get that $e_1$ is nontrivial on these three simple left $E_1$-submodules of $K_1/E_1$. 

\[ \square \]

4.1 Proof of Lemma 3

As the left $E_m$-module $\text{Ext}^1_{E_m}(N, E_m)$ can be identified based on Fact 6 with $\text{Hom}_{E_m}(N, K_m/E_m)$, from Lemma 4 we get that it can be identified via $e_m$ with $\text{Hom}_{E_m}(N, \text{Hom}_{W_m}(k)(E_m, W_m(k)))$ and thus also with the left
\( \mathbb{E}_m \)-module \( N^\vee = \text{Hom}_{\mathbb{E}_m(k)}(N, W_m(k)) \) 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 2 and 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 \( \sigma_R \) be the Frobenius automorphism of \( R \), \( W(R) \), and \( B(R) = W(R)[\frac{1}{p}] \). Let

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

be defined similarly to \( D(k) = \mathbb{D} \) and \( E(k) = \mathbb{E} \) (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) Theorem 2 implies that \( s_{D,E} = s_{E,D} \). We recall from [Va2, Thm. 1.2 (e)] and [GV, Rm. 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 [Va2, Thm. 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. [Va2, Thm. 1.2 (c) and (f)]) and therefore we have

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

### 4.3 Example

Let \( n, m, q \) be positive integers such that \( m = n + \left\lceil \frac{q}{2} \right\rceil \). Let \( H \) be such that its Dieudonné module \( N \) is isomorphic to \( \mathbb{E}/(F, V)^{2n+q} \); thus \( p^m \) annihilates \( H \) but \( p^{m-1} \) does not annihilate \( H \). Let \( G = D[p^n] \), where \( D \) is a supersingular \( p \)-divisible group over \( k \) of height 2; thus the Dieudonné module \( M \) of \( G \) is
isomorphic to $E_m/(F-V)$. Then we have canonical identifications of abstract
groups $\text{Hom}_E(N,M) = M$ and $\text{Hom}_E(M,N) = (F,V)^{2n+q-1}/(F,V)^{2n+q}$. This implies that $2n + q = \dim(\text{Hom}(H,G)) > \dim(\text{Hom}(G,H)) = 2n$.

5 Proof of Theorem 3

Let $S(M)$ be the set (of representatives) of isomorphism classes of finite
dimensional simple left $M$-modules. The abelian group $K_0(M)$ is canonically
identified with the free abelian group on $S(M)$. The automorphism $\sigma$ acts
naturally on $S(M)$: the isomorphism class $[Z]$ is mapped to the isomorphism
class $[Z(\sigma)]$. Let $O(M)$ be the set of orbits of the action of $\sigma$ on $S(M)$; this
makes sense as it is easy to see that two simple left $M$-modules $Z_1$ and $Z_2$ of
finite dimension are isomorphic if and only if the two simple left $M$-modules
$Z_1^{(\sigma)}$ and $Z_2^{(\sigma)}$ are isomorphic. The abelian group $K_0(M)/I_0(M)$ is canonically
identified with the free abelian group on $O(M)$. For $i \in \{1,2\}$ we write
$[L^i] = \sum_{[Z] \in S(M)} n_{1,[Z]}[Z] \in K_0(M)$ and $[L_2] = \sum_{[Z] \in S(M)} n_{2,[Z]}[Z] \in K_0(M)$,
where each $n_{i,[Z]} \in \mathbb{N}$ and all but a finite number of the $n_{i,[Z]}$’s being 0.

Let $O(M,G,H)$ be the smallest finite subset of $O(M)$ such that for each
orbit $o \in O(M) \setminus O(M,G,H)$ 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 $o \in O(M,G,H)$ we have an identity

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

\(8\)

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
$M$-module $Z$ of finite dimension we have the following disjoint two possibil-
ities:

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

(b) If the image of $M(\bar{k})$ in $\text{End}(Z)(\bar{k})$ is infinite, then there exists a
    positive integer $n$ such that for each positive integer $m \geq n$ there exists no
    left $M$-module $W$ such that $Z$ and $W^{(\sigma^m)}$ are isomorphic.
Lemma 5 To prove that the identity (8) holds we can assume that for each $o \in O(M, G, H)$, every simple left $M$-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 $M_{k'}$-module $k' \otimes_k L_1$ or of the left $M_{k'}$-module $k' \otimes_k L_2$ is absolutely simple. To prove the lemma it suffices to show that if the Equation (8) holds in the case when the pair $(\sum \Hom, u)$ is replaced by the pair $(k, O(M, G, H))$ then for all $j$ is replaced by the pair $(k', O(M_{k'}, G_{k'}, H_{k'}))$, then the equation (8) holds as well.

If $[Z] \in o \in O(M, G, H)$, then $k' \otimes_k Z$ is a direct sum of absolutely simple left $M_{k'}$-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 $M_{k'}$-module that are not pairwise isomorphic and such that the Galois group $\text{Gal}(k'/k)$ acts transitively on the set $\{Z'_1, \ldots, Z'_{u_Z}\}$. We consider the orbit $o' \in O(M_{k'}, G_{k'}, H_{k'})$ 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 $u_Z, m_Z, s_Z$ depend only on the orbit $o$ and not on the choice of $Z$ with the property that $[Z] \in o$. Thus we can define $u_o = u_Z, m_o = m_Z, s_o = s_Z$.

We note that if $[Z_1] \in o' \in O(M, G, H)$ 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 $j \in \{1, \ldots, u_{Z_1}\}$ and $j_1 \in \{1, \ldots, u_{Z_1}\}$ the orbits in $O(M_{k'})$ 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 $\Hom_M(Z^{(a)}, Z_1^{(b)})$ is nonzero if and only if the $k'$-vector space $\Hom^{M_{k'}}((k' \otimes_k Z)^{(a)}, (k' \otimes_k Z_1)^{(b)})$ is nonzero.

We write $[(k' \otimes_k L_1)^{\gamma}] = \sum_{[Z'] \in S(M_{k'})} n_{1,[Z']} [Z'] \in K_0(M_{k'})$ and $[k' \otimes k L_2] = \sum_{[Z'] \in S(M_{k'})} n_{2,[Z']} [Z'] \in K_0(M_{k'})$, 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

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

(9)
As we have assumed that the Equation (8) holds in the case when the pair \((k, O(M, G, H))\) is replaced by the pair \((k', O(M_{k'}, G_{k'}, H_{k'}))\), we have 
\[
\sum_{Z' \in o} n_1(z') = \sum_{Z' \in o} n_2(z').
\]
From this and the equation (9) we get that the equation (8) holds.

\[\square\]

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

In this subsection we show that to prove (8) for all orbits \(o \in O(M, G, H)\) we can assume that \(k\) is a finite field. Based on Lemma 5 we can assume that each simple factor of a composition series of either \(L_1\) or \(L_2\) is absolutely simple.

Let \(R\) be a finitely generated \(F_p\)-subalgebra of \(k\) such that the following five properties hold for it:

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

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

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

(iv) The left \(\mathcal{M}\)-modules \(\mathcal{L}_1^\vee\) and \(\mathcal{L}_2\) have a composition series whose factors \(Z_{1,1}, \ldots, Z_{1,s_1}\) and \(Z_{2,1}, \ldots, Z_{1,s_2}\) (respectively) have absolutely simple fibres and are defined by free \(R\)-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 \(\mathcal{M}\)-modules \(Z_{j_1} \otimes_R k\) and \(Z_{j_2} \otimes_R k\) have different images in \(K_0(\mathcal{M})/I_0(\mathcal{M})\) (equivalently, if \([Z_{j_1} \otimes_R k]\) and \([Z_{j_2} \otimes_R k]\) do not belong to the same orbit of \(O(\mathcal{M})\)), then there exists a maximal ideal \(i\) of \(R\) such that the left \(\mathcal{M}/i\mathcal{M}\)-module \(Z_{j_1}/iZ_{j_1}\) is not isomorphic to \((Z_{j_2}/iZ_{j_2})^{(\sigma_i)}\) for all \(i \in \mathbb{N}\), where \(\sigma_i\) is the Frobenius automorphism of the finite field \(l = R/i\).

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

22
(v-) If \( j_1, j_2 \) are as in the property (v), then there exists a maximal ideal \( i \) of \( R \) such that the left \( \mathcal{M}/i\mathcal{M} \)-module \( Z_{j_1}/iZ_{j_1} \) is not isomorphic to \( (Z_{j_2}/iZ_{j_2})^{(\sigma_i)} \) for all \( i \in \{0, 1, \ldots, N\} \).

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

Due to the properties (iv) and (v), the pull back map \( O(M) \rightarrow O(M/iM) \) restricts to an injection \( O(M, G, H) \hookrightarrow O(M/iM) \). Thus to prove that (8) holds it suffices to show that Equation (8) holds in the case when the pair \((k, O(M, G, H))\) is replaced by the pair \((l, O(M/iM, G_l, H_l))\). Therefore to prove that the Equation (8) 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 \((R, L_1, L_2) = (k, L_1, L_2)\) and thus that \( L_1^o \) and \( L_2 \) have composition series whose factors are denoted as above by \( Z_{1,1}, \ldots, Z_{1,s_1} \) and \( Z_{2,1}, \ldots, Z_{1,s_2} \) (respectively).

To prove that the Equation (8) holds we can replace the finite field \( k \) by a finite field extension of it (cf. Lemma 5). Thus we can assume that the following two properties hold:

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

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

Let the groups \( K_0(M(k)), I_0(M(k)) \), and \( K_0(M(k))/I_0(M(k)) \) and the set \( O(M(k), G, H) \subset O(M(k)) \) be analogues to the groups \( K_0(M), I_0(M), \) and \( K_0(M)/I_0(M) \) and the set \( O(M, G, H) \subset O(M(k)) \) (respectively) but working in the category of finite dimensional \( k \)-vector spaces which are left modules over the abstract monoid \( M(k) \). From properties (i) and (ii) we get that the evaluation map \( O(M) \rightarrow O(M(k)) \) restricts to an injection \( O(M, G, H) \hookrightarrow O(M(k), G, H) \). Thus to prove that the Equation (8) holds it suffices to show that it holds in the case when the pair \((M, O(M, G, H))\) is replaced by the pair \((M(k), O(M(k), G, H))\). Therefore to prove that the Equation (8) holds we can assume that \( k \) is a finite field and we are viewing
$L_1^\gamma$ and $L_2$ as left modules over the abstract monoid $M(k) = \text{End}(G) \times \text{End}(H)^{\text{opp}} = \text{End}(G)_{\text{red}}(k) \times \text{End}(H)_{\text{red}}^{\text{opp}}(k)$; to emphasize the \(F_p\)-algebra structures we will denote $A_G = \text{End}(G)$ and $A_{H^\dagger} = \text{End}(H^\dagger)$ and $A = A_G \times A_{H^\dagger}$ viewed as finite dimensional \(F_p\)-algebras. For $\dagger \in \{G, H\}$, both $L_1^\gamma$ and $L_2$ are naturally left $A_{\dagger}$-modules and therefore each $Z_j$ with $j \in \{(1, 1), \ldots, (1, s_1), (2, 1), \ldots, (2, s_2)\}$ is a left $A_{\dagger}$-module.

### 5.3 Step 3: applying Theorem 2

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

$$A_G = \prod_{i=1}^s A_{G,i}$$

of \(F_p\)-algebras such that for each $i \in \{1, \ldots, s\}$ we have a canonical identification $S_{G,i} = A_{G,i}/J(A_{G,i})$. To the decomposition (10) corresponds product decompositions $G = \prod_{i=1}^s G_i$, $\text{Hom}(G, H) = \prod_{i=1}^s \text{Hom}(G_i, H)$, and $\text{Hom}(H, G) = \prod_{i=1}^s \text{Hom}(H, G_i)$. Thus to prove that Theorem 3 holds (equivalently that the Equation (8) holds in the case when the initial pair $(M, O(M, G, H))$ is replaced by the pair $(M(k), O(M(k), G, H))$) we can assume that $s = 1$ and therefore that $S_G$ is a simple \(F_p\)-algebra.

A similar argument shows that we can assume that $S_{H^\dagger} = A_{H^\dagger}/J(A_{H^\dagger})$ is a simple \(F_p\)-algebra. But in such a case, up to isomorphism there exists a unique simple left $M(k)$-module on which the identity elements of both $A_G$ and $A_{H^\dagger}$ act identically and therefore the analogue of the Equation (8) for the case when the pair $(M, O(M, G, H))$ is replaced by the pair $(M(k), O(M(k), G, H))$ becomes the identity $\dim_k(L_1^\gamma) = \dim_k(L_2)$ which is a particular case of Theorem 2 (note that $\dim_k(L_1^\gamma) = \dim_k(L_1) = \dim(\text{Hom}(G, H))$ and $\dim_k(L_2) = \dim(\text{Hom}(H, G))$). This ends the proof of Theorem 3. \(\square\)

### 5.4 Remark

The ring scheme $\text{End}(G)$ has $\text{End}(G)^0$ as a two-sided ideal subscheme and the quotient ring scheme $C_G = \text{End}(G)/\text{End}(G)^0 = \text{End}(G)_{\text{red}}/\text{End}(G)^0_{\text{red}}$
is étale. From [GV, Cor. 6 (b)] we get that \( \text{Aut}(G)^0(k) = 1_M + \text{End}(G)^0(k) \). From this and the fact that \( \text{Aut}(G)^0 \) is a unipotent group scheme (cf. [GV, Cor. 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 \( \text{End}(G)^0(k) \) and whose simple factors are one dimensional \( k \)-vector spaces annihilated by all crystalline realizations of elements of \( \text{End}(G)^0(k) \). Thus there exists \( u \in \mathbb{N}^* \) with the property that each product of arbitrary \( u \) endomorphisms of the Dieudonné module \( M \) that are crystalline realizations of elements of \( \text{End}(G)^0(k) \), 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 \( \text{End}(G)^0(k) \). We have 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 \( \text{End}(G)^0(k) \) whose factors are annihilated by all crystalline realizations of elements of \( \text{End}(G)^0(k) \). This implies that \( \text{End}(G)^0 \) acts trivially on each \( Z_j \) with \( j \in \{(1,1), \ldots, (1,s_1), (2,1), \ldots, (2,s_2)\} \). Therefore \( Z_j \) is a left \( C_G \)-module.

If \( H \) is also a truncated Barsotti–Tate group, then as in the previous paragraph we argue that \( \text{End}(G)^0 \times \text{End}(H^t)^0 \) acts trivially on each \( Z_j \) and therefore \( Z_j \) is a left \( C_G \)-module as well as a left \( C_{H^t} \)-module; thus in such a case the three steps above could be easily combined with the role of \( A = A_G \times A_{H^t} \) being replaced by the étale ring scheme \( C = C_G \times_k C_{H^t} \).

## 6 Isogeny and Symmetric Properties in the Relative Context

Let \( M \) be the (contravarint) Dieudonné module of a \( p \)-divisible group \( D \) over \( k \). In order to match our notations with the ones of [GV], let \( \phi : M \to M \) and \( \vartheta : M \to M \) be the \( \sigma \) and the \( \sigma^{-1} \)-linear maps (respectively) such that for \( x \in M \) we have \( \phi(X) = Fx \) and \( \vartheta(x) = Vx \). We denote also by \( \phi : \text{End}_{B(k)}(M[\frac{1}{p}]) \to \text{End}_{B(k)}(M[\frac{1}{p}]) \) the \( \sigma \)-linear automorphism induced naturally by \( \phi \); it maps \( h \in \text{End}_{B(k)}(M[\frac{1}{p}]) \) to \( \phi \circ h \circ \phi^{-1} \in \text{End}_{B(k)}(M[\frac{1}{p}]) \). Therefore \( \phi(h) = \frac{1}{p}FhV \).
Let $\mathcal{G}$ be a smooth closed subgroup scheme of $\text{GL}_M$ such that its generic fibre $\mathcal{G}_{B(k)}$ is connected. Thus the scheme $\mathcal{G}$ is integral. Let $\mathfrak{g} := \text{Lie}(\mathcal{G})$ be the Lie algebra of $\mathcal{G}$. Until the end we will assume that the following two axioms introduced in [GV, Sect. 6] hold for the triple $(M, \phi, \mathcal{G})$:

\begin{itemize}
  \item[(AX1)] the Lie subalgebra $\mathfrak{g}[\frac{1}{p}]$ of $\text{End}_{W(k)}(M)[\frac{1}{p}]$ is stable under $\phi$, i.e. we have $\phi(\mathfrak{g}[\frac{1}{p}]) = \mathfrak{g}[\frac{1}{p}]$;
  \item[(AX2)] there exist a direct sum decomposition $M = F^1 \oplus F^0$ such that the following two properties hold:
    \begin{enumerate}
      \item[(a)] the kernel $F^1$ of the reduction modulo $p$ of $\phi$ is $F^1/pF^1$;
      \item[(b)] the cocharacter $\mu : \mathbb{G}_m \to \text{GL}_M$ which acts trivially on $F^0$ and via the inverse of the identical character of $\mathbb{G}_m$ on $F^1$, normalizes $\mathcal{G}$.
    \end{enumerate}
\end{itemize}

The triple $(M, \phi, \mathcal{G})$ is called an $F$-crystal with a group over $k$, cf. [Va1, Def. 1.1 (a) and Subsect. 2.1]. Let $n^g_D$ be the smallest nonnegative integer that has the following property: for each element $\bar{g} \in \mathcal{G}(W(k))$ congruent to $1_M$ modulo $p^{n^g_D}$, there exists an inner isomorphism between $(M, \phi, \mathcal{G})$ and $(M, \bar{g}\phi, \mathcal{G})$. The existence of $n^g_D$ is implied by [Va1, Main Thm. A]. If $\mathcal{G} = \text{GL}_M$, then we have $n^g_D = n_D$ (see [GV, Subsect. 5.1]).

For $m \in \mathbb{N}^*$ let $\phi_m, \vartheta_m$ be the reductions modulo $p^m$ of $\phi$ and $\vartheta$ (respectively). Let $b^{(\sigma)}$ be the pull-back (or the tensorization) of some $W(k)$-linear map or $W(k)$-module $b$ with $\sigma$. Thus $M^{(\sigma)} := W(k) \otimes_{\sigma, W(k)} M$, etc.

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

(b) For $g_1, g_2 \in \mathcal{G}(W(k))$ we say that $(M, g_1\phi, \mathcal{G})$ and $(M, g_2\phi, \mathcal{G})$ 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 $p$-divisible group over $k$ whose Dieudonné module is $(M, g\phi, \vartheta g^{-1})$; it has the same dimension and codimension as $D$. Note that $D = D_{1_M}$. Moreover, if $\mathcal{G} = \text{GL}_M$, then each $p$-divisible 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

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

be the group scheme over $k$ of endomorphisms from $(M/p^mM, g_m\phi_m, \vartheta_m)$ to $(M/p^mM, \phi_m, \vartheta_m)$. Thus, if $R$ is a commutative $k$-algebra and if $\sigma_R$ is
Theorem 4 For each $g$ and $D, W$ are elements of $\textup{End}_D(M,\phi,\mathcal{G})$ that satisfy the identities (1) $\zeta$ of $W_m(R) \otimes_{W_m(k)} M/p^mM$ that satisfy the identities (1) $\zeta(W_m(R) \otimes \phi_m) \circ \hat{\zeta}(\sigma) = \hat{\zeta} \circ (1_W(R) \otimes g_m \phi_m)$ and $\hat{\zeta}(\sigma) \circ (1_W(R) \otimes \vartheta_m g_m^{-1}) = (1_W(R) \otimes \vartheta_m) \otimes \hat{\zeta}$; here $\phi_m$ and $\vartheta_m$ are viewed as $W_m(k)$-linear maps $(M/p^mM)^{(\sigma)} \to M/p^mM$ and $M/p^mM \to (M/p^mM)^{(\sigma)}$ (respectively).

We consider the closed subgroup scheme $\textup{End}_M(\mathbb{D},\phi,\mathcal{G})$ of $\textup{Hom}(D[p^m], D_g[p^m])$ such that for each commutative $k$-algebra $R$, the subgroup $\textup{Hom}(D[p^m], D_g[p^m])$ of $\textup{Hom}(D[p^m], D_g[p^m])$ is formed by all those $W_m(R)$-linear endomorphisms $\zeta$ of $W_m(R) \otimes_{W_m(k)} M/p^mM$ which are elements of $W_m(R) \otimes_{W_m(k)} M/p^mM$. 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 $n^g_{D,D_g}$ such that for all integers $n \geq n^g_{D,D_g}$ we have an equality

$$\dim(\textup{Hom}(D[p^n], D_g[p^n])) = \dim(\textup{Hom}(D[p^{n^g_{D,D_g}}], D_g[p^{n^g_{D,D_g}}]))$$

Moreover, if $n^g_{D,D_g} > 0$, then the finite sequence

$$(\dim(\textup{Hom}(D[p^n], D_g[p^n]))_{n \in \{1, \ldots, n^g_{D,D_g}\}}$$

is strictly increasing.

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

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

27
Proof: Let $M_1$ and $M_2$ be $M$. Let $E = D \oplus D_g$; it is a $p$-divisible group over $k$ whose Dieudonné module is $(M \oplus M, \phi \oplus g \phi) = (M_1 \oplus M_2, \phi \oplus g \phi)$. Let $\mathfrak{h}$ be the Lie subalgebra of $\text{End}_{W(k)}(M \oplus M) = \text{End}_{W(k)}(M_1 \oplus M_2)$ formed by all those $W(k)$-linear endomorphisms of $M \oplus M = M_1 \oplus M_2$ which annihilate $M_1$, which map $M_2$ into $M_1$, and for which the resulting $W(k)$-linear map from $M_2 = M$ to $M_1 = M$ is an element of $\mathfrak{g}$.

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

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

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

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

$$\textbf{Hom}(D[p^m], D_g[p^m])^\mathcal{H}_{\text{crys}} = \textbf{Aut}(D[p^m] \oplus D_g[p^m])^\mathcal{H}_{\text{crys}}$$

of affine group schemes over $k$, which for a commutative $k$-algebra $R$ maps $\zeta \in \textbf{Hom}(D[p^m], D_g[p^m])^\mathcal{H}_{\text{crys}}(R)$ to $1_{W(R) \otimes W(k)(M \oplus M)} + \zeta$, where $\zeta$ is identified with a $W_m(R)$-linear endomorphism of $W_m(R) \otimes W_m(k) (M \oplus M) = W_m(R) \otimes W_m(k) (M_1 \oplus M_2)$ which annihilates $W_m(R) \otimes W_m(k) M_1$ and which maps $W_m(R) \otimes W_m(k) M_2$ to $W_m(R) \otimes W_m(k) M_1$ in the same way as $\zeta$ does.

As the product of two elements of $\mathfrak{h}$ is 0, $W(k)1_M + \mathfrak{h}$ is a $W(k)$-subalgebra of $\text{End}_{W(k)}(M \oplus M)$ and therefore the hypothesis of [GV, Thm. 6] holds for the triple $(M \oplus M, \phi \oplus g \phi, \mathcal{H})$. Therefore the fact that (a) holds follows from [GV, Prop. 2 (c) and Thm. 6] and the Equation (11).

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

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

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

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

Thus the fact that $Tr_\mathfrak{g}$ is perfect implies that $Tr_\mathfrak{g}$ induces an isomorphism of latticed $F$-isocrystals from the dual of $(g, \phi_{D_g,D})$ to $(g, \phi_{D,D_g})$. 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 $N$ being replaced by $M = M_1$ and $M = M_2$ (respectively) and with the roles of $\Hom_{W(k)}(N, L)$ and $\Hom_{W(k)}(L, N)$ being replaced by the Lie subalgebra $g$ of $\End_{W(k)}(M) = \Hom_{W(k)}(M_2, M_1)$ and of $\End_{W(k)}(M) = \Hom_{W(k)}(M_1, M_2)$ (respectively). We would only like to add that, due to the axiom (AX1), with the notations $\Hom_{W(k)}(N, L)^\flat$ and $\Hom_{W(k)}(N, L)^\sharp$ of Subsections 3.1 and 3.2 used under the mentioned replacement of roles, for $\diamond \in \{\{D_g, D\}, \{D, D_g\}\}$ we take $g^{\diamond}_{\flat}$ to be
\[
g \cap \Hom_{W(k)}(M_2, M_1)^\flat = \{x \in g | \phi_\diamond(x) \in \Hom_{W(k)}(M_2, M_1)\} = g \cap \phi_\diamond^{-1}(g)
\]
and we take $g^{\diamond}_{\flat}$ to be
\[
g_{\frac{1}{p}} \cap \Hom_{W(k)}(M_2, M_1)^\sharp = g_{\frac{1}{p}} + (g_{\frac{1}{p}} \cap \phi_\diamond(\Hom_{W(k)}(M_2, M_1))) = g_{\frac{1}{p}} + \phi_\diamond(g).
\]
Note that the dual of $g^{\diamond}_{D,D_g}$ is $g^{\diamond}_{D_g,D}$.

\[\Box\]

**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**


Ofer Gabber, E-mail: gabber@ihes.fr

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.