Simple p-kernels of p-divisible groups

Frans Oort

Dedicated to Mike Artin, for his 70-th birthday

Introduction

In this paper we study p-divisible groups and their p-kernels over an algebraically closed field. We try to obtain insight in which way these two kind of objects depend on each other. In this paper p is a prime number.

The p-kernel of a p-divisible group is called a BT_1 group scheme; here BT stand for Barsotti-Tate group scheme (a synonym for a p-divisible group), and the index 1 stands for "truncated at level one". For such group schemes we defines notions of being "indecomposable" see (1.2), "minimal" see (1.9), and "simple" see (1.2); this last terminology is short for the notion "BT_1-simple". With these notions defined we show:

(0.1) Theorem A. *Let G be a BT_1 group scheme over an algebraically closed field k;*

$$G \textit{ is indecomposable and minimal} \quad \Longleftrightarrow \quad G \textit{ is simple.}$$

A proof will be given in Section 3 and in Section 5.

Starting from a p-divisible group X we obtain a BT_1 group scheme:

$$[p] : \{X \mid \text{a } \ p-\text{divisible group}\}/\cong_k \quad \longrightarrow \{G \mid \text{a } \ \mathrm{BT}_1\}/\cong_k; \quad X \mapsto G := X[p].$$

This map is known to be surjective; see [1], 1.7, see [6], 9.10; also see (2.5), where we define a section for this map. It is the main theorem of [8] that the fiber of this map over (G up to $\cong_k$) is precisely one p-divisible group X if G is minimal; however things are different if G is not minimal, as we will show here:

(0.2) Theorem B. *Let G be a* BT_1 *group scheme over an algebraically closed field k; suppose G is* not minimal; *then:*

$$\#(\{X \mid X[p] \cong G\}/\cong_k) \quad = \quad \infty.$$

A proof will be given in Sections 8, 9, 10.

We will see that there are subtle differences between numerical invariants attached to a p-divisible group X and to $X[p]$. This will make a proof of Theorem B not so easy. We illustrate this difficulty in an example in Section 6.

Throughout this paper we fix a prime number p. Base schemes will be over $\mathbb{F}_p$, and fields considered are of characteristic p. We use k and Ω for algebraically closed fields of characteristic $p > 0$.

We have gathered some information on notation in the first two sections; it seems best to start reading in Section 3, where proofs start, and refer back whenever information on notation is needed.

This paper was partly written during a visit to the ETH Zürich. I thank the Department of Mathematics of the ETH for hospitality and excellent working conditions. I thank the referee for valuable remarks on an earlier draft of this paper.

1 Group schemes annihilated by p

We review results obtained in [3], and we fix notations (slightly different from notation used in that reference). We only study "circular words" as we do not need the "linear words" as in [3]. As we mainly study Dieudonné modules, the action of a word is given on the covariant Dieudonné modules of groups schemes studied (we had to make choices).

(1.1) BT_1 **group schemes.** A finite locally free group scheme $G \to S$ is called a BT_1 group scheme, see [1], page 152, if $G[F] := \mathrm{Ker}F_G = \mathrm{Im}V_G =: V(G)$ and $G[V] = F(G)$. In particular this implies that G is annihilated by p. The abbreviation "BT_1" stands for "1-truncated Barsotti-Tate group"; the terms "p-divisible group" and "Barsotti-Tate group" indicate the same concept. We refer to [9], Exp. VII_A.4, for the definition of $F_T : T \to T^{(p)}$ for an S-scheme $T \to S$ and of $V_G : G^{(p)} \to G$ for a commutative S-group scheme $G \to S$.

(1.2) Definitions. *A* BT_1 *group scheme G over a field is said to be* decomposable *if there exist non-zero* BT_1 *group schemes G_1 and G_2 and an isomorphism $G \cong G_1 \times G_2$. We say that G is* indecomposable *if there is no isomorphism $G \cong G_1 \times G_2$ with non-zero* BT_1 *group schemes G_1 and G_2.*

A non-zero BT_1 *group scheme G over a field is said to be* simple (or: BT_1-simple) *if for any* BT_1 *subgroup scheme $G' \subset G$ we have either $0 = G'$ or $G' = G$.*

Remark. There are many examples of a group scheme which are BT_1-simple (i.e. simple in the category of BT_1 group schemes), but which are not simple as a finite group scheme. For example, for a supersingular elliptic curve E over a field $K \supset \mathbb{F}_p$ the group scheme $E[p]$ is a BT_1 group scheme, it is BT_1-simple; however $E[F] \subset E[p]$ is a proper, non-zero subgroup scheme, and we see that $E[p]$ is not simple as a group scheme.

Remark. If G is a BT_1 group scheme, and as a group scheme it is decomposable, $G \cong G' \times G''$, then G' and G'' are BT_1 group schemes. We see that "BT_1-indecomposable" and "indecomposable as group scheme" are equivalent notions for a BT_1 group scheme.

(1.3) If G is a BT_1 group scheme over a perfect field $K \supset \mathbb{F}_p$ its covariant Dieudonné module $\mathbb{D}(G) = M_1$ is a finite dimensional vector space over K on which $\mathcal{F}$ and $\mathcal{V}$ operate in a p-linear, respectively p^{-1}-linear way, such that $\mathcal{F}\mathcal{V} = [p]_{M_1} = 0 = \mathcal{V}\mathcal{F}$, with the property that $M_1[\mathcal{F}] = \mathcal{V}M_1$ and $M_1[\mathcal{V}] = \mathcal{F}M_1$. The Dieudonné module of a BT_1 is called a DM_1.

In [3] BT_1 group schemes over an algebraically closed field k are classified. Here is that classification.

(1.4) A circular word will be a finite, ordered set of the symbols $\mathcal{F}$ and $\mathcal{V}$:

$$w = L_1 \cdots L_h, \quad L_i \in \{\mathcal{F}, \mathcal{V}\};$$

this will be read in a cyclic way, in the sense that the letter L_1 is supposed to come directly after L_h; cyclic permutations give an equivalence relation, and the class of a word is given by: $\lceil L_1 \cdots L_h \rfloor = \lceil L_2 \cdots L_h, L_1 \rfloor = \cdots = \lceil L_i \cdots L_h L_1 \cdots L_{i-1} \rfloor = \cdots$. From now on we use the terminology "word" for the concept "circular word".

For a given word w and a perfect field K we construct a finite group scheme G_w over K defined by: the K-vector space

$$\mathbb{D}(G_w) = \sum_{1 \leq i \leq h} K \cdot z_i,$$

with structure of a Dieudonné module; the operation of $\mathcal{F}$ and of $\mathcal{V}$ will be described by the the combination $z_1 L_1 z_2 \cdots z_h L_h z_1$; this means:

$$L_i = \mathcal{F} \quad \Rightarrow \quad \mathcal{F} \cdot z_i := z_{i+1}, \quad \mathcal{V} \cdot z_{i+1} := 0,$$

$$L_i = \mathcal{V} \quad \Rightarrow \quad \mathcal{V} \cdot z_{i+1} := z_i, \quad \mathcal{F} \cdot z_i := 0.$$

One can visualize this by putting the symbols L_i in a circular graph, with the arrows $L_i = \mathcal{F}$ pointing clockwise, and the arrows equal to $\mathcal{V}$ anti-clockwise.

We will use the notation z_i for all $i \in \mathbb{Z}$, with the convention that $z_i = z_{i'}$ if $i \equiv i'$ (mod h), and the same convention for the notation L_i for all $i \in \mathbb{Z}$.

Comments. We see that the symbol $\mathcal{F}$ in a word indeed acts as $\mathcal{F}$ on the Dieudonné module, going clock-wise, but the symbol $\mathcal{V}$ act as "$\mathcal{V}^{-1}$", i.e. $\mathcal{V} z_{i+1} = z_i$. We have chosen not to incorporate that exponent "-1" in the notation of the word.

Definitions above show that a word w defines a DM_1 and hence defines a group scheme which is a BT_1 group scheme; this will be denoted denoted by G_w. Moreover equivalent words define isomorphic .

Notation. We see that G_w is defined over $\mathbb{F}_p$. We will use the notation G_w over any field and over any base scheme in characteristic p: instead of writing $G_w \otimes_{\mathbb{F}_p} K$, or $G \times_{\mathrm{Spec}(\mathbb{F}_p)} S$ we will just write G_w if it is clear from the context over what field, or base scheme we are working.

A word w is called *decomposable* if there exist $h, \mu \in \mathbb{Z}_{>0}$, with $\mu \cdot h' = h$ and $L_1, \cdots, L_{h'} \in \{\mathcal{F}, \mathcal{V}\}$, such that

$$\lceil L_1 \cdots L_h \rfloor = \lceil (L_1 \cdots L_{h'})^{\mu} \rfloor := \lceil (L_1 \cdots L_{h'}) \cdots (L_1 \cdots L_{h'}) \rfloor.$$

If such a way of writing with $\mu > 1$ is not possible we say the word w is *indecomposable.*

(1.5) **Theorem** (see [3], Section 5). *Let $k \supset \mathbb{F}_p$ be an algebraically closed field.*
(a) *A (circular) word w, by the formulas above, defines a* BT_1 *group scheme G_w, and w is indecomposable if and only if G_w is indecomposable.*
(b) *Any* BT_1 *group scheme over k is a direct sum of indecomposable* BT_1 *group schemes.*
(c) *For any indecomposable* BT_1 *group scheme G over k there exists an indecomposable word*

w such that $G \cong G_w$.
Hence: any BT_1 group scheme G over k can be written as

$$G \quad \cong \quad \prod_{1 \le j \le t} G_{w_j}$$

with indecomposable words $w_1, \cdots, w_t$. $\square$

Notation. For an indecomposable $G \cong G_w$, with $w = L_1 \cdots L_h$ we will say that w is the K-cycle, or the Kraft-cycle defining G. Notation: $\Gamma(G) = w$. Also see (1.9).

(1.6) The type of a simple p-divisible group. For a p-divisible we use the word "simple" meaning that every sub-p-divisible group is either zero or the whole group. We recall the definition of the "Type" of a simple p-divisible group, as it was given in [2].

We choose coprime positive integers $m, n \in \mathbb{Z}$. Write $h = m + n$.
Definition. *A* semi-module *for m and n is a subset $A \subset \mathbb{Z}$,*
bounded from below
such that $m + A \subset A$ and $n + A \subset A$.
If $A \subset \mathbb{Z}$ and $b \in \mathbb{Z}$ we write $b + A := \{b + a \mid a \in A\}$, and call this the *translation* of A over b. Once m and n are fixed we will say "semi-module" omitting "for m and n".

We consider all p-divisible groups X of dimension m, such that the dimension of X^t is n, and such that the Newton polygon $\mathcal{N}(X)$ is isoclinic, necessarily consisting of h slopes equal to $n/(m+n)$. Over an algebraically closed field k this gives just one isogeny class. For every such X we define a semi-module $A = \mathrm{Type}(X)$; here is a description of $X \mapsto \mathrm{Type}(X)$.

Define $H = H_{m,n}$ as in [2]; this means that H is in the isogeny class given above and $\mathrm{End}(H \otimes k)$ is the maximal order in $\mathrm{End}^0(H \otimes k)$; this is a (non-commutative) DVR; call its uniformizer π; we can see that $H_{m,n}$ is defined over $\mathbb{F}_p$, but we use the notation $H_{m,n}$ over any base scheme, if there is no danger for confusion. Over an algebraically closed field the conditions mentioned define $H = H_{m,n}$ up to isomorphism.

A p-divisible group X over k is in the isogeny class given above if and only if it is isogenous with $H_{m,n}$. An isogeny $X \to H = H_{m,n}$ gives an inclusion $\mathbb{D}(X) = M \subset Q = \mathbb{D}(H)$; there is a filtration $Q \supset \cdots \supset Q^{(i)} := \pi^i {\cdot} Q \supset \cdots$; we write

$$\mathrm{Type}(X) := \{i \in \mathbb{Z} \mid M \cap Q^{(i)} \neq M \cap Q^{(i+1)}\}.$$

Clearly this gives a semi-module. Any isogeny $X \to H = H_{m,n}$ defines in this way a semi-modules. It is not difficult to see that two such isogenies for X fixed give semi-modules which are equal up to translation.

We can make the choice of such a semi-module unique, once X is given, by a normalization. Here we will not follow the normalization for semi-modules as was done in [2]. In this paper we usually arrange things in such a way that zero is the smallest element in A, i.e. $A \subset \mathbb{Z}_{\geq 0}$ and $0 \in A$.

Note that $\mathrm{Type}(H_{m,n}) = \mathbb{Z}_{\geq 0} = [0, \infty)$, a semi-module for m and n.

(1.7) Let us fix coprime, positive integers m, and n; we write $h := m + n$. Let w be a word, in which $\mathcal{F}$ appears m times and $\mathcal{V}$ appears n times. We present another way of encoding the word w.

A subset $C \subset \mathbb{Z}$ is called the *beginning of a semi-module* if:

- for every $0 \leq i < h$ the set C contains precisely one element of the equivalence class $i + h{\cdot}\mathbb{Z}$;
- for every $i \in C$ either $i + n \in C$ or $i - m \in C$.

If $C \subset \mathbb{Z}$ is the beginning of a semi-module and $b \in \mathbb{Z}$ then also $b + C$ is the beginning of a semi-module.

From such a C we construct a word: choose $c_1 \in C$, and proceed inductively:
if $c_i + n \in C$, write $L_i = \mathcal{F}$ and $c_{i+1} = c_i + n$,
if $c_i - m \in C$, write $L_i = \mathcal{V}$ and $c_{i+1} = c_i - m$;
we obtain $C = \{c_1, \cdots, c_h\}$ with $c_{h+1} = c_1$. Write $z_i = e_{c_i}$. The class of the word w is given by $\lceil w \rfloor = \lceil L_1 \cdots L_h \rfloor$. The Dieudonné module of G_w is given by $\mathbb{D}(G_w) = \sum_{j \in C} \ K{\cdot}z_j$, where the action of $\mathcal{F}$ and of $\mathcal{V}$ on $\mathbb{D}(G_w)$ is given by $z_1 L_1 \cdots L_{h-1} z_h L_h z_1$.

Conversely from a word where the symbol $\mathcal{F}$ appears m times and $\mathcal{V}$ appears n times such a set $C \subset \mathbb{Z}$ (unique up to translation) can be reconstructed using the methods just explained; write this set as $C(w)$.

See (2.5) for another way to reconstruct $C(w)$ from w.

A word w gives rise to C, another way of encoding the word w. For $\mathbb{D}(G_w)$ we have the k- basis $\{e_j \mid j \in C\}$, we have a renumbering of $C = \{c_1, \cdots, c_h\}$, hence $\{e_j \mid j \in C\} = \{z_1, \cdots, z_h\}$ obtained by "following the cycle"; we obtain a k-basis $\{z_1, \cdots, z_h\}$, with $e_{c_i} = z_i$.

(1.8) Let $m, n \in \mathbb{Z}_{>0}$ be coprime, positive integers. Suppose $C = [0, h-1] := \{0, 1, \cdots, h-1\}$. This set C defines a word $w(C)$ of length $h = m + n$. This particular word is denoted by $w(m, n)$; it will be called a *minimal word*. From the construction of G_w and from properties of $H_{m,n}$ we see that $G_{w(m,n)} = H_{m,n}[p]$. We see that $w(m, n) = w(\{0, \cdots, h-1\})$.

We will also use the notation $w = w(\mathcal{V}, \mathcal{F})$ in order to remind the reader that a given word w is written with the letters $\mathcal{V}$ and $\mathcal{F}$; in Section 4 we will see the use of this notation. I hope these slightly inconsequent notations $w(m, n)$, $w(C)$ and $w(\mathcal{V}, \mathcal{F})$ will not cause confusion.

Example. Let $m = 3$, and $n = 2$. Write the set of base vectors $\{e_i \mid 0 \leq i \leq 4\} = \{e_i \mid i \in C\}$ according to the set of integers $\{0, 1, 2, 3, 4\} = C$. The circular word

$$(e_0 = z_1)\mathcal{F}(e_2 = z_2)\mathcal{F}(e_4 = z_3)\mathcal{V}(e_1 = z_4)\mathcal{F}(e_3 = z_5)\mathcal{V}(e_0 = z_1); \quad w(3, 2) = \mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}$$

is the minimal word associated with $(m, n) = (3, 2)$.

The set $C' = \{0, 2, 3, 4, 6\}$ defines the class of the word $w(C') = \mathcal{F}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{V}$; this class is not equal the class of the minimal word $\lceil w(3, 2) \rfloor = \lceil w(\{0, 1, 2, 3, 4\}) \rfloor = \lceil \mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V} \rfloor = \lceil C \rfloor$ associated with the ordered pair $(3, 2)$.

For $(m, n) = (1, 0)$ we write $w(1, 0) = \mathcal{F}$, and $G_{w(1,0)} = \mu_p$. For $(m, n) = (0, 1)$ we write $w(0, 1) = \mathcal{V}$, and $G_{w(0,1)} = \underline{\mathbb{Z}/p\mathbb{Z}}$.

A remark on notation. We use covariant Dieudonné module theory. Hence $\mathbb{D}(F) = \mathcal{V}$ and $\mathbb{D}(V) = \mathcal{F}$; see [6], 15.3. Note that $F = 0$ on μ_p; this explains why $\mathcal{V} = 0$ on $\mathbb{D}(\mu_p)$.

(1.9) Minimal BT_1 **group schemes: Definition.** *A* BT_1 *group scheme* G *is called* minimal *if there are pairs* (m_i, n_i) *and an isomorphism*

$$G \quad \cong \quad \prod_{1 \le j \le t} G_{w(m_j,n_j)}, \quad \gcd(m_j, n_j) = 1.$$

As $G_{w(m,n)} \cong H_{m,n}[p]$ we see that this definition is equivalent with the one given in [8]:
Definition. *A* BT_1 *group scheme is minimal if and only if it can be written as a direct sum of group schemes* $H_{m_j,n_j}[p]$.

In Section 4 we will describe how to recognize from a word whether it is minimal or not.

Notation. If $G \cong \prod_{1 \le j \le t} \ G_{w_j}$ we will write formally $\Gamma(G) = \sum_{1 \le j \le t} w_j$.

(1.10) The lowest index. Let w be an indecomposable word, $C = C(w)$, and $G = G_w$. We have $M = \mathbb{D}(G) = \sum_{j \in C} k{\cdot}e_j$. Let $d \in C$ be the largest element in C. The vector e_d will be called *the lowest generator*. Note that $\mathbb{D}(\alpha_p) = k{\cdot}z$ with $\mathcal{F}z = 0 = \mathcal{V}z$; by $z \mapsto e_d$ we obtain a homomorphism of group schemes

$$\iota : \alpha_p \quad \hookrightarrow \quad G_w,$$

which we will call *the lowest embedding* of α_p into $G = G_w$.

Note that the word w reads $\cdots \mathcal{F} e_d \mathcal{V} \cdots$. In general the condition $\cdots (\mathcal{F} = L_i) z_{i+1} (\mathcal{V} = L_{i+1}) \cdots$ is not sufficient to conclude that z_d is the lowest position, see Section 4.

2 Notations and definitions, preliminaries

We work over an algebraically closed field k.

(2.1) Definition. Let $w' = L'_1 \cdots L'_r$ and $w = L_1 \cdots L_h$ be indecomposable words. An *infinite slice* γ from w' to w is a subset of $(\mathbb{Z}/r) \times (\mathbb{Z}/h)$ given by an integer j and equalities

$$L'_i = L_{i+j}, \quad \forall i \in \mathbb{Z}.$$

We recall the convention $L_i = L_{i+th}$ for all $t \in \mathbb{Z}$ and $L'_i = L'_{i+th}$.

Note that if an infinite slice exists, then $\lceil w' \rfloor = \lceil w \rfloor$.

Remark. *Note that if a slice extends to the right in an infinite way, then it also extends to the left in an infinite way.* Indeed $L'_i = L'_{i+hr}$ for all $i \in \mathbb{Z}$ and $L_{i+j} = L_{i+j+hr}$.

Definition. A *finite slice* γ from w' to w is a subset of $(\mathbb{Z}/r) \times (\mathbb{Z}/h)$ given by the following properties:

there are given an integer j, integers $B < E$ (B = Beginning, E = End) such that:

$$L'_{B-1} \ne L_{B-1+j}, \quad L'_i = L_{i+j} \ \ \forall B \le i < E, \quad L'_E \ne L_{E+j}.$$

Moreover this finite slice is called a *zero finite slice* if moreover

$$L'_{B-1} = \mathcal{F} \ \ \& \ \ L_{B-1+j} = \mathcal{V}, \quad \text{or} \quad L'_E = \mathcal{V} \ \ \& \ \ L_{E+j} = \mathcal{F}.$$

We say that γ is a non-zero finite slice if moreover

$$L'_{B-1} = \mathcal{V} \;\;\&\;\; L_{B-1+j} = \mathcal{F}, \quad \text{and} \quad L'_E = \mathcal{F} \;\;\&\;\; L_{E+j} = \mathcal{V}.$$

We denote by $\mathcal{S}(w', w)$ the set of non-zero slices from w' to w.

(2.2) Definition. Consider words w, and w', as above and the indecomposable BT_1 group schemes $G = G_w$ and $G' = G_{w'}$ defined by these words. Let $\gamma = (j, B, E)$ be a finite slice. We say that $(\gamma, a_{B-1}, a_B, \cdots, a_E, a_{E+1})$ is a *finite string* if $a_i \in k$ and $a_{B-1} = 0$ and $a_{E+1} = 0$, and

$$B \le i \le E \Rightarrow a_i \neq 0; \quad B \le i < E, \;\; L'_i = \mathcal{F} \Rightarrow a_{i_1+1} = a_i^p, \quad L'_i = \mathcal{V} \Rightarrow a_{i_1+1} = a_i^{p^{-1}}.$$

A string ψ defines a homomorphism $\psi : G_{w'} \to G_w$.

Note that in one the following situations:

$$\begin{array}{ccc}
z'_i & \xrightarrow{\mathcal{F}} & z'_{i+1} \\
\downarrow & & \downarrow \\
 & & a{\cdot}z_{i+j+1} \\
z_{i+j} & \xleftarrow{\mathcal{V}} & z_{i+j+1}
\end{array}
\qquad \text{or} \qquad
\begin{array}{ccc}
z'_i & \xleftarrow{\mathcal{V}} & z'_{i+1} \\
\downarrow & & \downarrow \\
a{\cdot}z_{i+j} & & \\
z_{i+j} & \xrightarrow{\mathcal{F}} & z_{i+j+1}
\end{array}$$

we obtain $a = 0$. This shows that a non-zero string cannot be constructed upon a zero slice.

As k is algebraically closed, hence perfect, for any non-zero finite slice and any choice of $a_B \in k$ with $a_B \neq 0$ this can be completed to a finite string. We sum up the data for a non-zero finite string in the following diagram.

$$\begin{array}{ccccccccc}
z'_{B-1} & \xleftarrow{\mathcal{V}} & z'_B & \cdots & z'_E & \xrightarrow{\mathcal{F}} & z'_{E+1} & & w' \\
\downarrow & & \downarrow & || & \downarrow & & \downarrow & & \downarrow \\
0 & & \neq 0 & || & \neq 0 & & 0 & & \\
z_{B+j-1} & \xrightarrow{\mathcal{F}} & z_{B+j} & \cdots & z_{E+j} & \xleftarrow{\mathcal{V}} & z_{E+j+1} & & w,
\end{array}$$

$$\mathcal{V} = L_{B-1} \neq L_{B+j-1} = \mathcal{F}; \qquad B \le i < E \Rightarrow L'_i = L_{i+j}; \qquad \mathcal{F} = L_E \neq L_{E+j} = \mathcal{V}.$$

Remark. Suppose a non-zero finite slice γ from w' to w exists. Then there exist non-zero finite strings based on this slice. In fact we get a bijective map

$$\{\psi\}_\gamma \xrightarrow{\sim} k \qquad \psi \mapsto \psi(z'_E),$$

from the set of all strings ψ based on γ to k.

Slices and strings as defined here were already earlier considered in the context of group schemes with an additional structure, see [4], Section 4.

We say that ψ is in an *infinite string* if there exist an infinite slice γ and $a_i \in k$, non-zero for every i, coherent in the way explained before.

Suppose w and w' are indecomposable. Let m be the number of copies of $\mathcal{F}$ in w and n be the number of copies of $\mathcal{V}$ in w.

Claim. *If there exists an infinite slice γ from $G' = G_{w'}$ to $G = G_w$, then $w' = w$ and $G' \cong G$, and $a_i \in \mathbb{F}_{p^{|m-n|}}$. For any choice i we obtain a bijective map*

$$\{\psi\}_\gamma \xrightarrow{\sim} \mathbb{F}_{p^{|m-n|}} \qquad \psi \mapsto \psi(z'_i).$$

We see that $L'_i = L_{i+j}$ for all $i \in \mathbb{Z}$. This shows the indecomposable words are equivalent. Applying $L_1, \cdots, L_{m+n}$ we obtain $a_1 = a_1^{p^{|m-n|}}$. $\square$

Conversely, if G' and G are both powers of the same indecomposable BT_1, then there does exist an infinite string from G' to G.

(2.3) Let w' and w be indecomposable words of lengths r, respectively h. For every $j \in \mathbb{Z}$ consider in $(\mathbb{Z}/r) \times (\mathbb{Z}/h)$ a "diagonal line" given by all pairs $\{(i, i+j)\}$. Consider all pairs $(i, s) \in \mathbb{Z}$ with $L'_i \neq L_s$. These split up the diagonal lines into slices. We see that $(\mathbb{Z}/r) \times (\mathbb{Z}/h)$ is a disjoint union of slices.

(2.4) Proposition. *Let w' and w be indecomposable words. Every homomorphism $\varphi : G_{w'} \to G_w$ can be written as*

$$\varphi \quad = \quad \psi_1 + \cdots + \psi_t,$$

where each of the ψ_j belongs to a $\gamma_j \in \mathcal{S}(w', w)$, and $\psi_i \neq \psi_{i'}$ implies $\gamma_i \neq \gamma_{i'}$.
Proof. We obtain the Dieudonné module map

$$\mathbb{D}(\varphi): \quad \mathbb{D}(G_{w'}) = \sum_{i=1}^{i=r} k \cdot z'_i \quad \longrightarrow \quad \mathbb{D}(G_w) = \sum_{s=1}^{s=h} k \cdot z_s.$$

Write $\mathbb{D}(\varphi)(z_i) = \sum a_{i,s} z_s$. We have seen that if (i, s) belongs to a zero slice, then $a_{i,s} = 0$. All (i, s) belonging to one given non-zero slice γ_j indeed give a string ψ_j defined by those $a_{i,s}$ supported by γ_j. This proves the proposition. $\square$

(2.5) A lift. For every BT_1 group scheme G we define a p-divisible group $X = \mathcal{L}(G)$; moreover this has the property that $\mathcal{L}(G)[p] = G$.

We have seen that a BT_1 group scheme is direct sum of indecomposable group schemes. Let w be a (finite) word in the letters $\mathcal{F}$ and $\mathcal{V}$. This defines a BT_1 group scheme G_w. Writing

$$w = L_1 L_2 \cdots L_h, \quad L_i \in \{\mathcal{V}, \mathcal{F}\},$$

we define a Dieudonné module, free of rank h over W, with generators $Z_1, \cdots, Z_h$ (write $Z_{h+1} = Z_1$) and relations:

$$L_i = \mathcal{F} \quad \Rightarrow \quad \mathcal{F}Z_i = Z_{i+1}, \ \ \mathcal{V}Z_{i+1} = pZ_i,$$

and

$$L_i = \mathcal{V} \quad \Rightarrow \quad \mathcal{F}Z_i = pZ_{i+1}, \ \ \mathcal{V}Z_{i+1} = Z_i.$$

Clearly this defines a Dieudonné module M; we define X to be the p-divisible group such that $\mathbb{D}(X) = M$. This definition works over $\mathbb{F}_p$. However we will use the notation $\mathcal{L}(G_w)$ over any field, if there is no danger for confusion. Write $\mathcal{L}(\prod G_{w_i}) = \prod \mathcal{L}(G_{w_i})$. From the definition of $\mathcal{L}(G)$ we see that $\mathcal{L}(G)[p] = G$.

The lift $\mathcal{L}(G)$ could be called the "tautological lift". However note it is not functorial. For the words $w_1 = \mathcal{F}\mathcal{V}$ and $w_2 = \mathcal{F}^3\mathcal{V}^2$ there does exist an inclusion $G_{w_1} \hookrightarrow G_{w_2}$. However, we will see in (2.6) that the p-divisible groups $\mathcal{L}(G_{w_1})$ and $\mathcal{L}(G_{w_2})$ are isoclinic of different slopes, and hence the only homomorphism between them is the zero map.

For a word w we can construct $C(w)$ in the following way: choose $X = \mathcal{L}(G_w)$, and $A = \mathrm{Type}(X)$. Then $A_p =: A\backslash(h + A)$ equals $C(w)$, as can be easily seen.

Suppose w is a word consisting of precisely d letters $\mathcal{F}$ and precisely c letters $\mathcal{V}$; write $h = d+c$, the length of the word w. We write

$$\mu := \gcd(d, c), \quad d = \mu{\cdot}m, \quad c = \mu{\cdot}n.$$

(2.6) Lemma. *With the notation above, the tautological lift $\mathcal{L}(G_w)$ is isoclinic of slope*

$$n/(m + n): \quad \mathcal{L}(G_w) \sim (H_{m,n})^{\mu}.$$

Proof. For every i, with $1 \leq i \leq h := m + n$ we have $\mathcal{F}^h Z_i = p^c Z_i$; this proves the lemma. □

3 Simple finite group schemes

We work over an algebraically closed field k. In this section we will show:

(3.1) Lemma 1. *Let G be a* simple BT_1. *Then G is indecomposable:*

$$\text{indecomposable} \quad \Leftarrow \quad \text{simple}\ .$$

(3.2) Lemma 2. *Let G be an indecomposable* BT_1 *which is* not *minimal. Then G is not simple:*

$$\text{minimal} \quad \Leftarrow \quad \text{simple} + \text{indecomposable} \quad \Leftarrow \quad \text{simple}.$$

(3.3) Lemma 3. *Let G be an indecomposable, minimal* BT_1, *let $0 \neq G'$ be an indecomposable, minimal* BT_1 *and let*

$$G' \quad \hookrightarrow \quad G$$

be an immersion. Then

$$G' \quad \xrightarrow{\sim} \quad G$$

is an isomorphism:

$$\text{indecomposable} + \text{minimal} \quad \Rightarrow \quad \text{simple}.$$

A proof of Lemma 3 will be given in Section 5.

(3.4) Note that these three results imply Theorem A. Indeed, if G is simple, then it is indecomposable by (3.1), and then, by (3.2) we conclude it minimal.

Conversely, suppose G is indecomposable and minimal. Let $G'' \subset G$ be a non-zero BT_1 contained in G. Choose $G' \subset G''$ such that ($G' \neq 0$, and such that) G' is indecomposable and simple; by Lemma 2 we conclude that G' is minimal. By (3.3) we conclude that $G' = G$. Hence under the given conditions we conclude $G'' = G$. This implies that G is simple. This finishes the proof of Theorem A, granting (3.1), (3.2) and (3.3).

(3.5) Proof of (3.1). We know that every BT_1 can be written as a direct sum of indecomposables,

$$G = \prod_{1 \leq i \leq s} G_i.$$

If $s > 1$, we would have $G_1 \hookrightarrow G$ with $0 \neq G_1 \subsetneq G$. This is a contradiction with "G is simple". This proves (3.1) $\square$(3.1)

(3.6) Proof of (3.2). *We assume that G is an indecomposable* BT_1 *which is not minimal. We show that G is not simple.*

Step one. Let w be an indecomposable word; suppose the number of letters $\mathcal{F}$ in w equals d, the number of letters $\mathcal{V}$ in w equals c, and write

$$d = \mu{\cdot}m, \quad c = \mu{\cdot}n, \quad \gcd(m,n) = 1.$$

We show: if $\mu > 1$ then G_w is not simple. Indeed, $X := \mathcal{L}(G_w) \sim (G_{m,n})^{\mu}$, see (2.6). If $\mu > 1$ then X is not simple, there exists a proper sub-p-divisible group $X' \subset X$. Then $X'[p] \subset X[p] = G_w$ is a proper, non-zero BT_1 subgroup scheme; hence we see that in this case G_w is not simple.

Hence it suffices to show (3.2) under the extra condition $\mu = 1, \quad d = m, \quad c = n$. We write $h := m + n$.

Step two. Let w be as above, $G = G_w$, and $X = \mathcal{L}(X)$. Let $A = \mathrm{Type}(X)$. Suppose that this is normalized (translated) in such a way that $A \subset \mathbb{Z}_{\geq 0}$ and $0 \in A$. Note that $\Gamma(G) = A_p := A \backslash (h + A)$.

We assume that $m > n$: as G is non-minimal the case $m = 1 = n$ is excluded; proving the case where $m > n$, the other case follows by interchanging the role of $\mathcal{F}$ and $\mathcal{V}$. The word w is written as

$$w = L_1 L_2 \cdots L_{h-1} L_h.$$

Let $C = C(w)$ as defined in (1.7); we suppose C is normalized such that $0 \in C$ and $C \subset \mathbb{Z}_{\geq 0}$. As G is not minimal we know that $C \neq \{0, 1, \cdots, h-1\}$.

We have $\{e_j \mid j \in C\} = \{z_1, \cdots, z_h\}$; this renumbering we write as $z_i = e_{b_i}$; this means that

$$\{b_1, \cdots, b_h\} = C, \; b_1 = 0, \; L_i = \mathcal{F} \Rightarrow b_{i+1} = b_i + n, \quad L_i = \mathcal{V} \Rightarrow b_{i+1} = b_i - m.$$

The action of w is given by:

$$(z_1 = e_{b_1}) L_1 (z_2 = e_{b_2}) L_2 \cdots L_h (z_1 = e_{b_1}).$$

Assume $m > n$ and $z_1 = e_0$; we see that

$$L_1 = \mathcal{F} = L_2, \quad L_h = \mathcal{V}.$$

Note that $G = G_w$ is supposed to be non-minimal, hence $C \neq [0, h-1]$, hence C contains at least one element larger than h. We make the following choices:

- let $t + 1 < h$ be the largest index such that $b_{t+1} > h$;
- choose a new word w' of length t defined by:

$$L'_1 := \mathcal{V} \neq \mathcal{F} = L_1, L'_2 := L_2 = \mathcal{F}, \cdots, L'_i := L_i \quad (\text{for} \quad 1 < i \leq t), \cdots, L'_t := L_t.$$

- Consider $w' := L'_1 \cdots L'_t$ as a circular word of length t. In particular $L'_j = L'_{j+st}$ for all $s \in \mathbb{Z}$ and $1 \leq j \leq t$.
- Write $G_{w'}$ for the BT_1 group scheme defined by the word w'.
- Write E for the smallest integer with the property that $E > B := 2$ and such that $L'_E \neq L_E$.

We will show:

$$t < E < h, \quad L_E = \mathcal{V} \quad \text{and} \quad L'_E = \mathcal{F}. \qquad (*)$$

From $(*)$ we conclude

$$\mathcal{F} = L_1 \neq L'_1 = \mathcal{V}, L'_2 = L_2, \cdots, \quad L'_i = L_i \quad (2 =: B \leq i < E), \quad \text{and} \quad \mathcal{F} = L'_E \neq L_E = \mathcal{V};$$

this means that this is a slice, and from this we conclude that

$$\psi := (a_1 = 0, \quad a_2 = 1, \cdots, \quad a_i = 1 \quad (2 = B < i \leq E), \cdots, \quad a_E = 1, \quad a_{E+1} = 0) \qquad (**)$$

is a string which defines a homomorphism ψ; moreover, because $1 < B < E < h$ it follows that ψ is injective

$$0 \neq G_{w'} \xrightarrow{\sim} \psi(G_{w'}) \subsetneq G_w.$$

Once $(*)$ has been proved, we conclude that $G = G_w$ is not simple.

In order to prove $(*)$, we define $b'_1 = h, b'_2 = b_2, \cdots, b'_t = b_t$. These are positive integers. Moreover define $L'_{j+st} = L'_j$ for $1 \leq j \leq t$ and $s \in \mathbb{Z}$. Define

$$L'_i = \mathcal{F} \Rightarrow b'_{i+1} = b'_i + n, \quad i > 0,$$

$$L'_i = \mathcal{V} \Rightarrow b'_{i+1} = b'_i - m, \quad i > 0.$$

Note that $b'_1 = h$ and $b'_{t+1} > h$. For $1 \leq j \leq t$ we obtain $b'_{j+t} = b'_j + (b'_{t+1} - b'_1) > b'_j$. Repeating this argument we obtain $b'_{j+st} > b'_j > 0$ for $1 \leq j \leq t$ and $s \in \mathbb{Z}_{>0}$. This proves that $b'_i > 0$ for all $i \in \mathbb{Z}_{\geq 0}$. Note that the numbers $b_t, b_{t+1}, ..., b_h$ are all positive, and $b_{h+1} = b_1 = 0$; from this, and from the definition of E we conclude: $E < h$. By the choice of t moreover we conclude that $t < E$.
Warning: we do not claim that $C(w')$ and $\{b_1, \cdots, b_t\}$ are equal.

By our choice of E we have $b'_E = b_E$ and $b'_{E+1} \neq b_{E+1}$. By definition we have:
(i) either $b'_{E+1} = b_{E+1} + h$,
(ii) or $b'_{E+1} = b_{E+1} - h$.
Note that $t < E < h$; by the choice of t and by the fact that $b'_{E+1} > 0$ this shows that case (ii) is not possible. Hence we are in case (i); this shows

$$L_E = \mathcal{V}, \quad L'_E = \mathcal{F},$$

and we have proved $(*)$.

This proves $(**)$ is a string, defining an injective homomorphism $G' \hookrightarrow G$; this ends the proof of (3.2) $\square$(3.2)

4 The Euclidean type of a BT_1

We want to recognize whether a given word w defines a minimal BT_1. Starting from a minimal word w we define a "contraction". This process is based on the Euclidean algorithm. After a finite number of contractions the process stops. Keeping track of the steps tells us the shape the word we started with.

(4.1) We consider a circular word $w = w(P, Q)$ in the letters P and Q. We distinguish the following properties this word could have:

(1) a) There exists $s \in \mathbb{Z}_{\geq 0}$ such that PQ^sP and PQ^{s+2} appear in the circular word w;
b) There exists $s \in \mathbb{Z}_{\geq 0}$ such that QP^sQ and QP^{s+2} appear in the circular word w.

(2) a) There exists $s \in \mathbb{Z}_{\geq 0}$ and PQ^sP and $PQ^{s+1}P$ do appear in w and PQ^tP does not appear for $0 \leq t < s$ and does not appear for $t > s+1$.
b) There exists $s \in \mathbb{Z}_{\geq 0}$ and QP^sQ and $QP^{s+1}Q$ do appear in w and QP^tQ does not appear for $0 \leq t < s$ and does not appear for $t > s+1$.

(3) a) There exists $s \in \mathbb{Z}_{\geq 0}$ and $w = PQ^s$.
b) There exists $s \in \mathbb{Z}_{\geq 0}$ and $w = P^sQ$.

Remarks. These conditions are mutually exclusive: if (1a) or (1b) holds then none of (2) and (3) hold; the analogous statement if (2a) or (2b) holds; the analogous statement if (3a) or (3b) holds.

If w is a minimal word, then (1a) and (1b) do not hold.

If (3a) or (3b) holds then w is minimal.

If w is an indecomposable word then at least one of the five conditions hold.

Note that if (1a) and (1b) do not hold then it is not true that P^2 and Q^2 appear in w.

Remark. *If w is an indecomposable word then at least one of the five conditions hold.*
Proof. If P^2 and Q^2 occur in w, then (1a) and (1b) are satisfied with $s = 0$. If Q does occur, but Q^2 does not occur, we can write $w = QP^{n_1} \cdots QP^{n_t}$; if $t = 0$ we have $w = Q$, case (3b); if $t = 1$ we are in case (3b); if $t > 1$ we are either in case (1b) or in case (2b). If Q does not occur, then $w = P$, case (3a) with $s = 0$. If P does occur, but P^2 does not occur, an analogous reasoning as above can be used. $\square$

(4.2) Contraction. Suppose that $w_i = w_i(P_i, Q_i)$ satisfies (2a). We define new letters and a new word:

$$P_{i+1} := PQ^s, \quad Q_{i+1} := PQ^{s+1}, \quad w_{i+1}(P_{i+1}, Q_{i+1}) := w_i(P_i, Q_i).$$

The new word w_{i+1} is called the word obtained by *contraction* from the word w_i satisfying (2a).

Suppose that $w_i = w_i(P_i, Q_i)$ satisfies (2b). In this case we define new letters and a new word:

$$P_{i+1} := P^{s+1}Q, \quad Q_{i+1} := P^sQ, \quad w_{i+1}(P_{i+1}, Q_{i+1}) := w_i(P_i, Q_i).$$

The new word w_{i+1} is called the word obtained by *contraction* from the word w_i satisfying (2b).

Remark. Suppose w satisfies (2), and w_2 is the word obtained by contraction. Then w is indecomposable if and only if w_2 is indecomposable.

Remark. *Let w be an indecomposable word. After a finite number of contractions $w = w_1, w_2, \cdots, w_t$ we can achieve that w_t does not satisfy* (2a)*and does not satisfy* (2b) *and hence does satisfy* (1) *or* (3). Indeed, contraction gives a shorter word, hence this process of contractions stops and the last word in the sequence does not satisfy (2). Every indecomposable word satisfies one of the five conditions; w_t, not satisfying (2), does satisfy (1) or (3). □

(4.3) Suppose that $m \geq n > 0$. We characterize the fact that $m \geq n$ by the symbol $\varepsilon = +1$. In this case we define $\beta_1 = \beta := [m/n]$. We have:

$$\beta{\cdot}n \leq m < (\beta + 1){\cdot}n.$$

In case $m > n > 1$ we define

$$m_2 := m - \beta{\cdot}n, \quad \text{and} \quad n_2 := (\beta + 1){\cdot}n - m.$$

Claim. *If $m > n > 1$ in the minimal word $w = w(m, n)$ the combinations $\mathcal{VF}^\beta$ and $\mathcal{VF}^{\beta+1}$ do appear. Between two consecutive symbols $\mathcal{V}$ these are the only possibilities.* A minimal word with $m > n > 0$ satisfies (2a).

This follows from the description $C(w(m, n)) = [0, m + n - 1]$. □

Note that w minimal with $m > n > 1$ satisfies (2a) with $\beta = s$. In that case we define "contraction of w" as above: $P_1 := \mathcal{V}$, $Q_1 := \mathcal{F}$ and we write

$$P_2 = \mathcal{VF}^\beta \quad \text{and} \quad Q_2 = \mathcal{VF}^{\beta+1}.$$

This yields $w(\mathcal{V}, \mathcal{F}) = w_2(P_2, Q_2)$.

Claim. *If $w_1 = w(\mathcal{V}, \mathcal{F})$ satisfies* (2a) *, the word w_2 in the letters P_2, and Q_2 is a minimal word if and only if w is minimal, and w_2 is the word associated with the pair (m_2, n_2).*

A proof will be given in (4.7).

From (m, n) we have obtained $\{\varepsilon_1 = +1, \beta_1; (m_2, n_2)\}$. Conversely from these last data we can recover (m, n) by:

$$n = n_1 = m_2 + n_2, \quad \text{and} \quad m = m_1 = (\beta + 1)m_2 + \beta{\cdot}n_1.$$

(4.4) For $n > m > 1$ we write $\varepsilon = -1$, we write $\mathcal{V} = P_1, \quad \mathcal{F} = Q_1, \quad w = w_1(\mathcal{V},\mathcal{F}) = w_1(P_1,Q_1)$. We define

$$\beta = \beta_1 := \left[\frac{n}{m}\right], \quad \beta{\cdot}m < n < (\beta+1){\cdot}m.$$

We see that precisely $P_2 := \mathcal{V}^{\beta+1}\mathcal{F}$ and $Q_2 = \mathcal{V}^{\beta}\mathcal{F}$ appear in w. Define $n_1 = n$ and $m_1 = m$,

$$n_2 = n_1 - \beta{\cdot}m_1, \quad \text{and} \quad m_2 = (\beta+1){\cdot}m_1 - n_1.$$

The contracted word w_2, defined by

$$w =: w_1(P_1,Q_1) = w_2(P_2,Q_2),$$

belongs to the pair (m_2,n_2). We show: $w = w(\mathcal{V},\mathcal{F})$ is minimal, if and only if w_2 is minimal, see (4.7). We can reconstruct m and n by:

$$m = m_2 + n_2, \quad n = (\beta+1)n_2 + \beta m_2.$$

This ends the construction of the contraction step for $n > m > 1$.

(4.5) For a minimal word $w = w(m,n)$ we have $\gcd(m,n) = 1$. If $m > n > 1$ we are in case (2a); if $n > m > 1$ we are in case (2b); in these two cases contraction can be applied. If $m = 1$ or $n = 1$ we are in case (3), and no further contraction is possible. Starting with a minimal word w and continuing the Euclidean algorithm we obtain a sequence of ordered pairs of integers

$$(m,n) = (m_1,n_1),\ (m_2,n_2), \cdots,\ (m_r,n_r), \quad \text{with} \quad m_r = 1 \quad \text{or} \quad n_r = 1;$$

we call the *Euclidean type* of (m,n):

$$\mathrm{et}(m,n) = \{\varepsilon_1,\beta_1;\cdots;\varepsilon_i,\beta_i;\cdots;\varepsilon_r,\beta_r\},$$

with $r \geq 1, \quad \varepsilon_i \in \{+1,-1\}, \quad \beta_i \in \mathbb{Z}_{>0}$. We have seen that (m,n) determines this ordered set of integers, and that conversely from such a set $\{\varepsilon_1,\cdots,\beta_r\}$ we can reconstruct $w = w(m,n)$. This is not very deep or exiting, except from the possibility that we can recognize from the shape of a word whether it is minimal or not, see (4.7).

(4.6) **An easy example.** We illustrate the idea of the algorithm above by an example: take $(m,n) = (m_1,n_1) = (11,8)$. We see:

$$\varepsilon_1 = +1, \quad \beta_1 = 1, \quad (m_2,n_2) = (3,5); \quad \varepsilon_2 = -1, \quad \beta_2 = 1, \quad (m_3,n_3) = (1,2); \quad \varepsilon_3 = -1, \beta_3 = 2.$$

This is reflected in the contraction steps:

$$w_1 = (\mathcal{V}\mathcal{F})(\mathcal{V}\mathcal{F})(\mathcal{V}\mathcal{F}\mathcal{F})(\mathcal{V}\mathcal{F})(\mathcal{V}\mathcal{F})(\mathcal{V}\mathcal{F}\mathcal{F})(\mathcal{V}\mathcal{F})(\mathcal{V}\mathcal{F}\mathcal{F});$$

$$w_2 = (P_2P_2Q_2)(P_2P_2Q_2)(P_2Q_2);$$

$$w_3 = P_3P_3Q_3.$$

Note that w_1 starts at the lowest position e_{18}; we have

$$e_{18}(\mathcal{V}\mathcal{F})e_{15}(\mathcal{V}\mathcal{F})e_{12}(\mathcal{V}\mathcal{F}\mathcal{F})e_{17}(\mathcal{V}\mathcal{F})e_{14}(\mathcal{V}\mathcal{F})e_{11}(\mathcal{V}\mathcal{F}\mathcal{F})e_{16}(\mathcal{V}\mathcal{F})e_{13}(\mathcal{V}\mathcal{F}\mathcal{F})e_{18};$$

we see that w_2, using this presentation in $\lceil w_2 \rfloor$, also starts at the lowest position, and the same for w_3. This is a general phenomenon:

(4.7) Lemma. *Suppose w_i is an indecomposable word satisfying either* (2a) *or* (2b)*. Let w_{i+1} be the word obtained from w_i by contraction. Then:*

$$w_i \text{ is minimal} \quad \Longleftrightarrow \quad w_{i+1} \text{ is minimal.}$$

The place where w_i has the lowest position of an embedding of α_p is the same as the the lowest position of an embedding of α_p for the word w_{i+1}.

Proof. In order to simplify we write:

$$w = w_i, \quad \mathcal{V} = P_i, \quad \mathcal{F} = Q_i;$$

we write $m = m_i$ for the number of times $\mathcal{F}$ appears in w and $n = n_i$ for the number of times $\mathcal{V}$ appears; write $h = h_i = m + n$. We write $C = C(w)$; we normalize C by translation such that $h - 1 \in C$ is the largest element of C. If $m = 1$ or $n = 1$ we are not in case (2); hence we can assume $m > 1$ and $n > 1$. If $\gcd(m, n) > 1$ then w and w_{i+1} are not minimal; hence this case is settled; remaining cases: $\gcd(m, n) = 1$ and either $m > n > 1$ or $n > m > 1$.

Assume $m > n > 1$. Write

$$u = w_{i+1}, \quad P = P_{i+1} = \mathcal{V}\mathcal{F}^{\beta}, \quad Q = Q_{i+1} = \mathcal{V}\mathcal{F}^{\beta+1}, \quad m' = m_{i+1}, \quad n' = n_{i+1}, \quad h' = m' + n'.$$

Note that $m' + n' = n$. The operators P and Q act on C. We see that P "acts by $\beta{\cdot}n - m$" hence by $-m'$ and Q_2 "acts by $= (\beta + 1){\cdot}n - m$" hence by $+n'$. We see that $C(u) = C' \subset C$ is the subset under the normalization that $h - 1$ is the largest element. From this the last statement follows.

Assume w is minimal. Thus $C = [0, h - 1]$. Consider $C' \subset C$. Note that every element $b \in C'$ satisfies $b - m \geq 0$, because the words P and Q start with $\mathcal{V}$. As $n = m' + n' = h'$, hence $h - h' = m + n - h' = m$ it follows that $C' \subset [h - h_2, h - 1]$. Hence $C' = [h - h', h - 1]$, and we see that u is minimal.

Assume that u is minimal; with the normalization chosen we have hence $C(u) = C' = [h - h', h - 1]$. We show that every for b with $0 \leq b < m = h - h'$ we have $b \in C$; once this is proven, it follows that $C = [0, h - 1]$, hence w is minimal. For $0 \leq b < m$ choose $\rho \in \mathbb{Z}$ such that $m \leq b + \rho{\cdot}n =: y \leq h - 1$; this is possible (and ρ is unique), because $h' = n = h - m$. There are two cases to consider:

1) $m + m' \leq y + m' \leq h - 1$; in this case $u = \cdots (e_{y+m'}) P(e_y) \cdots$;

2) $m \leq y - n'$ and $y \leq h - 1$; in this case $u = \cdots (e_{y-n'}) Q(e_y) \cdots$.

In the first case $b + \rho{\cdot}n + m' < h = m + n$ gives $\rho{\cdot}n < (m - m') + n = (\beta + 1)n$, hence $\rho \leq \beta$; we see that $\mathcal{F}^{\beta-\rho}\mathcal{V}^{-1}e_{y+m'} = e_b$.

In the second case $\rho{\cdot}n < h - 1 = m + n - 1 < (\beta + 1)n + n - 1$ leads to $\rho \leq \beta + 1$; we see that $\mathcal{F}^{\beta+1-\rho}\mathcal{V}^{-1}e_{y-n'} = e_b$. In both cases we conclude $b \in C$. This shows w is minimal.

The case $n > m > 1$ is proved in an analogous way: $P := \mathcal{V}^{\beta+1}\mathcal{F}$ "acts by $-(\beta+1)m+n = -m'$" and $Q = \mathcal{V}^{\beta}\mathcal{F}$ "acts by $-\beta{\cdot}m + n = +n'$". This proves the proposition. □

(4.8) Conclusion. *Let w be an indecomposable word. Then at least one of the cases* (1a) - (3b) *holds. If* (3) *holds, or if after a finite number of contractions* (3) *holds, then w is minimal. If* (1) *holds, or if after a finite number of contractions* (1) *holds, then w is not minimal.*

5 A proof of Lemma 3

(5.1) In this section we fix notations: m, n are coprime positive integers, $m + n = h$, and f, g are coprime positive integers, $f + g = r$. We study the *indecomposable, minimal* words $w = w(m, n)$ and $w' = w(f, g)$, and the BT_1 group schemes $G' = G_{w'}$ and $G = G_w$.

(5.2) Lemma. *Keep notation as above. Suppose that $\psi : G' \to G$ is a homomorphism defined by a string (also called ψ). Suppose that ψ* is no-zero on the lowest embedding of α into G':

$$\left(\alpha_p \overset{\iota'}{\hookrightarrow} G' \xrightarrow{\psi} G\right) \quad \neq \quad 0.$$

Then the pairs (m,n) and (f,g) are equal.

(5.3) (5.2) $\Rightarrow$ Lemma 3. Indeed, suppose that $\varphi : G' \hookrightarrow G$ is an embedding, as in Lemma 3. By (2.4) we can write $\varphi = \psi_1 + \cdots \psi_r$ as finite sum of homomorphisms defined by strings. As φ is injective, we have $\iota' {\cdot} \varphi \neq 0$. This implies that for one of the ψ_i, say ψ_1, we have $\iota' {\cdot} \psi_1 \neq 0$. By (5.2) this implies $(m,n) = (f,g)$. Hence we have an embedding $\varphi : G' \hookrightarrow G$ of group schemes of the same rank; hence φ is an isomorphism; this proves Lemma 3, granting (5.2). $\square$

(5.4) If the string in (5.2) is infinite, we see that (m,n) and (f,g) are equal (use the fact that G' and G are indecomposable). From now on in the proof of (5.2) we suppose that *the string ψ is finite*, and we are going to obtain a contradiction.

(5.5) Where to start induction. *Suppose, in the notation above, that one of the four integers m, n, f, g equals to 1. Then the conclusion of* (5.2) *follows.*
Proof. We study a *finite* string ψ, and we use notation as in(2.2); for the definition of "lowest index" see (1.10); we shift indices in the words w and w' in such a way that a lowest index in w' is z_1', and such that in the string ψ the base vector z_1' is mapped in a non-zero way to z_1; hence $B \leq 0 < E$. Multiplying the homomorphism ψ by a constant we can suppose $\psi(z_1') = 1{\cdot}z_1$.

Suppose $g = 1$. Then $w' = \mathcal{V}\mathcal{F}^f$. We have

$$z_{-f}' \xrightarrow{\mathcal{F}} \cdots \xrightarrow{\mathcal{F}} z_{-1}' \xrightarrow{\mathcal{F}} z_0' \xleftarrow{\mathcal{V}}, \qquad L_{-f}' = \cdots = L_{-1}' = \mathcal{F}, \quad L_0' = \mathcal{V}.$$

Because $\psi(z_1') = z_1$ we conclude $L_{-1} = \mathcal{F}$ and $L_0 = \mathcal{V}$. If this were possible for a non-zero *finite* slice, going to the left, we would encounter $\mathcal{V}\mathcal{F}^t$ with $t > f$ as part of the word w; however, proceeding to the right, we would encounter $\mathcal{V}\mathcal{F}^u$ with $u < f$ as part of the word w. This is a contradiction with the fact that w is a minimal word. Hence in this case a *finite string which is non-zero on the lowest α_p* does not exist.

The case $f = 1$ is treated in the same way, with the roles of $\mathcal{F}$ and $\mathcal{V}$ interchanged.

Suppose $m \geq n = 1$. Then $L_{-m} = \mathcal{F} = \cdots = L_{-1}, \quad L_0 = \mathcal{V}$. Proceeding the string ψ to the left, we would conclude that we would encounter $\mathcal{V}\mathcal{F}^t$ with $t < m$ as part of the word w'; proceeding the string ψ to the right, we would conclude that we would encounter $\mathcal{V}\mathcal{F}^u$ with $u > m$ as part of the word w'. This is a contradiction with the fact that w' is minimal. In this case *a finite string which is non-zero on the lowest α_p does not exist.*

The case $n \geq m = 1$ is treated in the same way, with the roles of $\mathcal{F}$ and $\mathcal{V}$ interchanged.

This proves (5.2) in case that at least one of the four integers m, n, f, g equals to 1. $\square$

(5.6) The induction step in the proof of (5.2). We suppose that none of the integers m, n, f, g equals to 1. We assume there exists a finite ψ as in (5.2).
Induction hypothesis: (5.2) *has been proved for all cases where $f' + g' < f + g$.* The

induction step will be that (5.2) for (m,n) and (f,g) follows if we know (5.2) in the case (m_2,n_2) and (f_2,g_2).

This shows that (5.5) plus a proof of the induction step proves (5.2).

Let z'_1 be the position of the lowest embedding of α_p in G'.

Claim. *Then* $\beta(m,n)=\beta(f,g)$.

Suppose $f>g$. Write $\beta=\beta(f,g)$, i.e. $\beta=[f/g]$. This implies that

$$(\mathcal{VF}^{\beta+1})(z'_{-\beta-2})=z'_0, \quad \text{and} \quad (\mathcal{VF}^{\beta})(z'_0)=z'_{\beta+1}.$$

Following the string to the left, we see that only $(\mathcal{VF}^{\beta+1})$ and $(\mathcal{VF}^{\beta+2})$ can appear in the part of w left of z_0 covered by ψ. Following the string to the right we see that only $(\mathcal{VF}^t)$ with $t\le\beta+1$ can appear in the part of w right of z_0 covered by ψ. This proves $\beta(m,n)=\beta(f,g)$.

The case $g>f$ is treated in an analogous way. Hence the claim is proved. $\square$

Induction step. *Suppose a non-zero finite* $\psi: G'=G_{w'}\to G=G_w$ *as in* (5.2) *exists with all four integers* m,n,f,g *bigger than 1. Then there exists a finite* $\psi_2: G_{w'_2}\to G_{w_2}$ *which is non-zero on the lowest* $\iota'_2:\alpha_p\to G_{w'_2}$.

Indeed, we have seen that the lowest index in w' is between a letter Q'_2 and P'_2, and in the contracted word $w'_2(P'_2,Q'_2)$ this index again is the lowest position, see (4.7). Syllables P'_2 and Q'_2 in w' in the range of the finite string ψ are mapped to the same letter $P_2=P'_2$ and $Q_2=Q'_2$, while at the left end of string there is a P'_2 mapped by ψ to a Q_2 in w_2, and at the right end of the string there is a Q'_2 mapped by ψ to a P_2 in w_2. This proves that the finite string ψ as above, with all a_1 either equal to 1 or to 0, defines a string between w'_2 and w_2 non-zero at the lowest position.

This proves the induction step in case $f>g$. The case $g>f$ is treated in an analogous way.

Hence induction is proved. It can start by (5.5). Hence by the Euclidean algorithm every case of (5.2) follows. This proves (5.2), and hence it proves Lemma 3.

$\square$(5.2) $\square$Lemma 3 $\square$Theorem A

6 An example

The contents of this section is not needed for the proofs of the theorems. However we like to give the reader some background information.

(6.1) For a p-divisible group X over a field k we study its p-kernel $X[p]=G$. Can we deduce from numerical properties of X the possibilities for $\Gamma(G)$?

See (1.6) for the construction of a semi-module $A=\mathrm{Type}(X)$ attached to a simple p-divisible group X. A candidate for $\Gamma(G)$ is $A_p:=A\backslash(h+A)$: for every element γ in this set either $m+\gamma\in A'$ or $n+\gamma\in A'$ and every γ either is in $m+A'$ or in $n+A'$; writing $\mathcal{F}$ for $+n$ and $\mathcal{V}$ for $+m$ we see that we have a K-cycle.

In some cases, for a p-divisible group X it turns out that indeed $\Gamma(X[p])=A_p:=A\backslash(h+A)$. However we will see that there are cases where this is not the case. This is precisely the obstruction which makes it hard to compare properties of X, Type(X), $X[p]$ and $\Gamma(X[p])$. *We do not have a general formula which computes all possible* $\Gamma(X[p])$ *from* Type(X).

(6.2) We take $m = 7$ and $n = 4$. Let Q be the Dieudonné module of $H_{m,n}$. Hence Q is generated over W by $\{E_i \mid i \in \mathbb{Z}_{\geq 0}\}$. Moreover $\mathcal{F}\cdot E_i = E_{i+n}$ and $\mathcal{V}\cdot E_i = E_{i+m}$ and $pE_i = E_{i+m+n}$. Let M be the Dieudonné module generated by E_0 and E_5, Hence

$$\mathrm{Type}(M) =: A = \{0, 4, 5, 7, 8\} \cup [11, \infty);$$

equations are:

$$\mathcal{F}^3\cdot E_0 = E_{12} = \mathcal{V}\cdot E_5, \quad \mathcal{F}^4\cdot E_5 = E_{21} = \mathcal{V}^3\cdot E_0.$$

Conclusion.

$$\Gamma(M/pM) =: w = w(C) = \mathcal{F}^3\mathcal{V}\mathcal{F}^4\mathcal{V}^3, \quad C := A\backslash(11 + A).$$

(6.3) **A transfer.** Again we take $m = 7$ and $n = 4$. We choose an algebraically closed field k, and we take $a \in k$ with $a \neq 0$. We write $[a] \in W = W_\infty(k)$ for the Teichmüller lift of a. We define P as the Dieudonné submodule of Q generated by $q := E_0 + [a]\cdot E_1$ and E_5. We write A for the semi-module as defined in the previous subsection.

Claim.

$$\mathrm{Type}(P) = A := \{0, 4, 5, 7, 8\} \cup [11, \infty), \quad \text{but} \quad \Gamma(P/pP) = \mathcal{F}^5\mathcal{V}^3 + \mathcal{F}^2\mathcal{V}.$$

Note:

$$\mathrm{Type}(P) = \mathrm{Type}(M) \quad \text{and} \quad \Gamma(P/pP) \neq \Gamma(M/pM).$$

Proof. As $\mathcal{F}^2E_5 = E_{13} \in M$ we see that $\mathcal{F}^3q \equiv E_{12} \pmod{M \cap \pi^{13}Q}$; using a W-linear combination of p^2q and $\mathcal{F}pE_5$ we see that $E_{22} \in M$, hence $\mathcal{V}^3q \equiv E_{21} \pmod{M \cap \pi^{22}Q}$; we see that

$$\{q,\ \mathcal{F}q,\ \mathcal{F}^2q,\ E_{12},\ E_5,\ \mathcal{F}E_5,\ \mathcal{F}^2E_5,\ \mathcal{F}^3E_5,\ E_{21},\ \mathcal{V}^2q,\ \mathcal{V}q\}$$

is a W-basis for M. This proves the first claim.

Write $q' := E_4$. Hence $E_5 = (\mathcal{F}q - q')/[a^p]$; we see that q and q' generate the Dieudonné module M. Note that

$$0 \leq i \leq 4 \Rightarrow \mathcal{F}^i\cdot q \notin \mathcal{V}\cdot(P/pP); \quad 0 \leq i \leq 1 \Rightarrow \mathcal{F}^i\cdot q' \notin \mathcal{V}\cdot(P/pP).$$

Choose $\lambda \neq 0$ in k and $\mu \neq 0$ in k such that

$$\lambda^{p^5}a^{p^5} = \lambda^{p^{-3}}; \quad \mu^{p^2} = -a\cdot\mu^{p^{-1}}.$$

Note that:

$$p\cdot\mathcal{F}\cdot E_5 = E_{20} \in p\cdot M; \qquad p\cdot\mathcal{V}\cdot E_5 = E_{23}, \quad p^2\cdot q = E_{22} + [a]E_{23} \quad \Rightarrow \quad E_{22} \in p\cdot M;$$

$$p\cdot q = E_{11} + [a]E_{12} \quad \Rightarrow \quad E_{11} \equiv -[a]E_{12} \pmod{p\cdot M}.$$

With these notations we check:

$$\mathcal{F}^5\cdot[\lambda]\cdot q - \mathcal{V}^3\cdot[\lambda]\cdot q \in p\cdot M \quad \text{and} \quad \mathcal{F}^2\cdot[\mu]\cdot q' - \mathcal{V}\cdot[\mu]\cdot q' \in p\cdot M.$$

This proves the second part of the claim. $\square$

Note the subtle difference in determining $\mathrm{Type}(M)$ and $\Gamma(M/pM)$. In the fist case equations like $\mathcal{F}^3 \equiv E_{12} \pmod{M \cap \pi^{13}Q}$ should be satisfied, while in the second case equations should be satisfied modulo $p{\cdot}M$.

In the second case we see that in $E_{16} + [a^{p4}]{\cdot}E_{17}$ we have $E_{16} = p{\cdot}E_5$, and we get modulo pM a "transfer" (like in railway tracks) to E_{17} and then to E_{21} under $\mathcal{F}$:

$$E_0 + [a]{\cdot}E_1 = q \mapsto \mathcal{F}q \mapsto \mathcal{F}^2q \mapsto \mathcal{F}^3q \equiv E_{13} \mapsto E_{17} \mapsto E_{21} \leftarrow \mathcal{V}^2q \leftarrow \mathcal{V}q \leftarrow q,$$

and

$$E_4 = q' \mapsto \mathcal{F}q' \mapsto \mathcal{F}^2q' \equiv E_{11} \leftarrow q'$$

(up to units, in $M/p{\cdot}M$, and so on).

7 A catalogue of p-divisible groups

We produce a mild generalization of [2], Section 5. In this section we fix a Newton polygon β. If $\beta = \sum_i (m_i, n_i)$ we write $H = H(\beta) := \prod_i H_{m_i,n_i}$.

(7.1) From the proof of [7], (1.6), Step 1, we cite:
Given h there exists an integer $d(h)$ such that for every p-divisible group X of height h and Newton polygon $\mathcal{N}(X) = \beta$ there is an isogeny $\rho : H(\beta) \to X$ of degree $\deg(\rho) = d(h)$.

(7.2) We choose $\delta \in \mathbb{Z}_{\geq 0}$. We work over a field K. For every scheme S over K we write

$$T(S) = \{\rho : H \times S \to \mathcal{X} \mid \deg(\rho) = p^\delta\},$$

where $\mathcal{X} \to S$ is a p-divisible group, and ρ an isogeny of the degree indicated; equivalently one could give a finite flat subgroup scheme of the given rank inside H_S.

The functor $S \mapsto T(S)$ is representable: use the same, easy arguments as in [2], 5.9. The representing object will be denoted by $T = T_{\beta,\delta}$. This carries its universal family $\rho : H \times T \to \mathcal{X}$.

(7.3) If $\delta \geq d(h)$ the pair $(T = T_{\beta,\delta},\ \ \rho : H \times T \to \mathcal{X})$ is a *catalogue for all p-divisible groups isogenous with H*, by which we mean that for any algebraically closed field Ω containing K and for every p-divisible group Y over Ω with $\mathcal{N}(Y) = \beta$ there exists at least one point $t \in T_{\beta,\delta}(\Omega)$ such that $\mathcal{X}_t \cong Y$.

(7.4) **Lemma.** *For $\delta \geq 0$ and for any algebraically closed field Ω the map*

$$T_{\beta,\delta}(\Omega) \quad \longrightarrow \quad \{Y\}/\cong_\Omega, \quad (\rho_t : H \to \mathcal{X}_t)) = t \mapsto \mathcal{X}_t = Y$$

has finite fibers.

Proof. Suppose given Y. By [7], 1.10, the set of subgroup schemes $J \subset H_\Omega$ of given rank p^δ with the property that there exists some isomorphism $H_\Omega/J \cong Y$ is finite. This proves the lemma. $\square$

(7.5) **Remark.** In [7] we have developed a theory of "central leaves" and "isogeny leaves". Any catalogue as constructed above defines an image in the local deformation theory of any of its fibers, and such an image is contained in an isogeny leaf in the sense of [7].

8 Constructing a family

In order to conclude a proof of Theorem B we prove a stronger fact:

(8.1) Proposition. *Suppose given a* BT_1 *group scheme* G *over an algebraically closed field* k*. We choose the* p*-divisible group* X *by defining* $X := \mathcal{L}(G)$*. Let* $\beta = \mathcal{N}(X)$*, choose* $\delta \geq d(h)$ (as in Section 7), *and consider* $T_{\beta,\delta}$ *as before. Consider*

$$\mathcal{S}_G(T_{\beta,\delta}) := \{t \in T_{\beta,\delta} \mid \exists \Omega : \quad \mathcal{X}_t[p]_\Omega \cong G_\Omega\}.$$

If G *is* not minimal *then* $\mathcal{S}_G(T_{\beta,\delta})$ *has an irreducible component* S *of positive dimension containing* $(H \to X) = x \in T_{\beta,\delta}$*.*

Remark. By [6], Prop. 3.2 we know that $\mathcal{S}_G(T_{\beta,\delta}) \subset T_{\beta,\delta}$ is locally closed.

(8.2) Note: (8.1) $\Rightarrow$ Theorem B. *If this proposition holds, then theorem B follows.* Indeed, we apply Lemma (7.4) to the infinite set of points $S(k) \subset \mathcal{S}_G(T_{\beta,\delta})(k)$.

(8.3) First Step. *If for some positive integer* δ_1 *the set* $\mathcal{S}_G(T_{\beta,\delta_1})$ *contains a component of positive dimension then* (8.1) *is correct for every* $\delta \geq d(h)$*.*

Using (7.4) we conclude that

$$\#(\{X \mid X[p] \cong G\}/\cong_k) \quad = \quad \infty.$$

Again using (7.4), by $\delta \geq d(h)$ it follows that $\mathcal{S}_G(T_{\beta,\delta})(k)$ is non-finite. This proves the first step.

(8.4) Second Step. *The general case of Proposition* (8.1) *follows if we prove this statement for the case* $G = G_w$ *is indecomposable and non minimal.*

Suppose $G = \prod G_{w_i}$, a product of indecomposables; as before, $X = \mathcal{L}(G)$, $\beta = \mathcal{N}(X)$; write $\beta_i = \mathcal{N}(\mathcal{L}(G_{w_i}))$. Let us assume that an integer δ is chosen in such a way that $\delta = \prod \delta_i$ with $\delta_i \geq d(h(\beta_i))$. If G is not minimal, at least one of the words w_i is not minimal, say w_1. If we know the proposition for one factor G_{w_1}, we have a positive dimensional $S \subset \mathcal{S}_G(T_{\beta_1,\delta_1})$; over this S we multiply with fixed isogenies $H(\beta_i) \to \mathcal{L}(G_{w_i})$ for $i > 2$ each of degree p^{δ_i}. We obtain a positive dimensional family in $\mathcal{S}_G(T_{\beta,\delta})$.

We see that in order to prove (8.1), and hence to prove Theorem B, it suffices to prove (8.1) in case G is indecomposable. The rest of this section, Section 9 and Section 10 are devoted to proving that.

(8.5) We are going to prove (8.1) under the following assumptions:
We work over an algebraically closed field k*. We write* $w = L_1 L_2 \cdots L_h$*, a finite word,* $G = G_w$*; the number of letters equal to* $\mathcal{F}$ *in* w *is* d *and the number of letters equal to* $\mathcal{V}$ *is* c*,*

$$d = \mu{\cdot}m, \quad c = \mu{\cdot}n, \quad \gcd(m,n) = 1; \quad \beta = \mu{\cdot}(m,n).$$

We write $X = \mathcal{L}(G)$ *and* $M = \mathbb{D}(X)$*. We write* $H = H(\beta)$ *and* $Q = \mathbb{D}(H)$*.*

Note that $X \sim (H_{m,n})^\mu$, see (2.6).

(8.6) Lemma. *Among all embeddings $Q \hookrightarrow M$ there is a maximal one.*
Proof. Let $R := \mathrm{End}(H_{m,n} \otimes k)$. We know R is the maximal order in the endomorphism algebra $\mathrm{End}^0(H_{m,n} \otimes k)$, and it is (non-commutative) discrete valuation ring; a uniformizer was called π. If $M' \subset M$ and $M'' \subset M$ are Dieudonné submodules, so is their sum $M' + M'' \subset M$; if both are isomorphic with Q, then both are R-modules, and so is $M' + M''$. Hence the sup $M^{\max}$ of all submodules isomorphic with Q is a Dieudonné submodule, and it is an R-module.

Using $a, b \in \mathbb{Z}$ such that $am + bn = 1$ we see, as in [2], Lemma 5.4, that the action of π on $W(\mathbb{F}_{p^{m+n}})$ inside $\mathrm{End}(H_{m,n})$ is given by $\lambda{\cdot}\pi = \pi{\cdot}\sigma^{b-a}(\lambda)$; define $W_\infty(k)[\pi]$ by using this formula as the action of π on any $\lambda \in W_\infty(k)$. We see that this defines a discrete valuation ring $W_\infty(k)[\pi]$ and that the action of R on $M^{\max}$ extends to an action of $W_\infty(k)[\pi]$ on $M^{\max}$. We see that the $W_\infty(k)[\pi]$-module $M^{\max}$ is torsion-free and finitely generated. We conclude that $M^{\max}$ is free over $W_\infty(k)[\pi]$, i.e. $M^{\max} \cong Q$. This proves the lemma. $\square$

(8.7) We fix the maximal embedding $Q \subset M$. Choose the minimal $i \in \mathbb{Z}_{\geq 0}$ such that $M \subset \pi^{-i}Q =: Q'$. Note that M is supposed not to be a minimal p-divisible group, hence $Q \neq M$, and $M \neq Q'$. In this situation

$$Q \quad \subsetneq \quad M \quad \subsetneq \quad Q'$$

we distinguish two possibilities:

(8.7)**(1)** $\pi Q' \subset M$, hence $Q = \pi Q'$, or

(8.7)**(2)** $\pi Q' \not\subset M$, and $Q = \pi^i Q'$ with $i > 1$.

In both cases $Q' = (\mathbb{D}(H_{m,n}))^\mu$. We are going to prove the proposition in the two cases separately.

9 Case (1)

We analyze the structure of $X = \mathcal{L}(G)$ and $X[p] = G$ as in (8.7)(1). We write out "equations" for such situations and we conclude that any such case can be deformed in a positive dimensional family, in which $X[p]$ is geometrically constant.

We use assumptions and notations as in (8.5), and (8.7)(1). Write $a_{\mathrm{top}} = \dim_k(M/Q)$; note that $Q = \pi{\cdot}Q'$.

(9.1) Lemma. *In case* (8.7)(1) *it follows that* $m = 1 = n$ (i.e. X is supersingular), *the length of the word w is 2μ for some $\mu \in \mathbb{Z}_{\geq 2}$, and $Q' = (\mathbb{D}(G_{1,1}))^\mu$.*
Proof. As $M \neq Q'$ we have $a_{\mathrm{top}} < \mu$. Note that $\mathcal{F}{\cdot}Q' = \pi^m{\cdot}Q'$ and $\mathcal{V}{\cdot}Q' = \pi^n{\cdot}Q'$. Hence $a_{\mathrm{top}} < \mu$ and $Q = \pi Q' \subset M$ imply $m = 1 = n$. $\square$

The Dieudonné module $\mathbb{D}(H_{1,1})$ contains an element e with $\mathcal{F}e = \mathcal{V}e$, and such that $\mathbb{D}(H_{1,1}) = We \oplus W\mathcal{F}e$.

(9.2) Note that $a_{\mathrm{top}} \leq a := \dim_k(M/(\mathcal{F}{\cdot}M + \mathcal{V}{\cdot}M))$ (this last number equals the "usual a-number"). We define $v : Q'\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ by: $Z \in \pi^i Q'$ and $Z \notin \pi^{i+1}Q'$ then $v(Z) = i$.

We fix an isomorphism $Q' \cong (\mathbb{D}(H_{1,1}))^\mu$; we will write $\{e_1, \cdots, e_\mu\}$ for the set of generators which gives this isomorphism, where e_i is the Dieudonné module generator as above of the i-th factor.

We have $\mathbb{D}(G_w) = \sum_{1 \leq i \leq 2\mu} k \cdot z_i$, and the word w operates as $z_1 L_1 z_2 L_2 \cdots z_{2\mu} L_{2\mu} z_1$. We choose $Z_i \in M$ with $Z_i \bmod pM = z_i$. Define b to be the number of indices i, with $1 \leq i \leq 2\mu$ such that $v(Z_i) = 2$.

(9.3) Lemma. **(a)** *If $Z \in M$ and $Z \notin \mathcal{F}M + \mathcal{V}M$ then $v(Z) \leq 1$.*
(b) *For every i we have $0 \leq v(Z_i) \leq 2$. Hence $\mathcal{V}^3$ and $\mathcal{F}^3$ do not appear in w.*
(c) Define A as the number of times $\mathcal{V}^2$ appears in w. *We have $A \geq 1$.*
(d) *There exists a presentation $w = L_1 \cdots L_{2\mu}$ such that for every $0 \leq i < \mu$ the combination $L_{2i+1} L_{2i+2}$ is either $\mathcal{F}\mathcal{V}$ or $\mathcal{V}\mathcal{F}$.*
(e) *We have $a_{\rm top} > 0$ and $b > 0$ and $a_{\rm top} + b = \mu$.*
Proof. As $\pi^2 Q' \subset \mathcal{F}\pi Q' + \mathcal{V}\pi Q' \subset \mathcal{F}M + \mathcal{V}M$ part (a) follows.

Note that $\pi Q' \subset M$ implies $\pi^3 Q' \subset pM$; hence the first part of (b) follows; this implies the second part of (b).

As M is not isomorphic with Q the word w is not equal to $(\mathcal{F}\mathcal{V})^\mu$; hence (c) follows from (b).

Choose $L_{2\mu} = \mathcal{V} = L_1$, which is possible by (c). Then $v(Z_1) = 1$ by (b). By the previous results we see that for all $0 \leq i \leq \mu$ we have $v(Z_{2i+1}) = 1$; indeed, assume (induction hypothesis) that for some $0 \leq i \leq \mu$ we have $v(Z_{2i+1}) = 1$ (induction can start at $i = 0$); then $L_{2i+1} = \mathcal{F} = L_{2i+2}$ and $L_{2i+1} = \mathcal{V} = L_{2i+2}$ lead to a contradiction with $0 \leq v(Z_{2i+3}) \leq 2$; hence (d) follows.

As $\pi Q' \subsetneq M$ we have $a_{\rm top} > 0$. By (c) there is at least one index j with $v(Z_j) = 2$; hence $b > 0$. We see that $a_{\rm top} + b$ is the number of indices j with $v(Z_j) = 0$ or $v(Z_j) = 2$; as the number of j' with $v(Z_{j'}) = 1$ equals μ we have $a_{\rm top} + b = 2\mu - \mu = \mu$. This ends the proof of the lemma. $\square$

(9.4) We define a map $\rho : Q' \to Q'$, "taking the leading term", as follows. We write $\rho(0) = 0$. If $0 \neq Z \in Q'$, with $v(Z) = s$, we determine $x_j \in k$ such that

$$Z \bmod \pi^{s+1} Q' = \sum_j x_j (\pi^s \cdot e_j \bmod \pi^{s+1} Q') \in \pi^s Q' / \pi^{s+1} Q'$$

and we define

$$\rho(Z) = \sum_{1 \leq j \leq 2\mu} [x_j] \cdot \pi^s \cdot e_j.$$

Write $\rho(Z_i) =: Z'_i$, write M' for the Dieudonné module generated by $Z'_1, \cdots, Z'_{2\mu}$ and define $z'_j := Z_j \bmod pM'$.

Lemma. *We have $M = M'$, and $\{z'_1, \cdots, z'_{2\mu}\}$ is cyclic under the word w.*
Proof. We have $M/Q = M'/Q \subset Q'/Q$ and $(M \cap Q)/\pi Q = (M' \cap Q)/\pi Q \subset Q/\pi Q$; this implies the first statement. Note that $pM \subset \pi^2 Q'$; a congruence of the form $\mathcal{F}^s z_j \equiv \mathcal{V}^t z_{j+1} \pmod{pM}$ with $s, t \in \{1, 2\}$ implies $\mathcal{F}^s z'_j \equiv \mathcal{V}^t z'_{j+1} \pmod{pM}$. This proves the second statement. $\square$

Normalization. *From now on we suppose that the elements z_j and Z_j are chosen such that $\rho(Z_j) = Z_j$.*

(9.5) Notation. We have seen that $\mathcal{V}^2$ appears at least once in w. We choose a presentation of the circular word such that

$$\cdots(L_{2\mu} = \mathcal{V})z_1(L_1 = \mathcal{V})\cdots; \quad \text{note that} \quad v(Z_1) = 1.$$

The word w can be be written as

$$w = (\mathcal{V}\mathcal{F})^{t_1}(\mathcal{F}\mathcal{V})(\mathcal{V}\mathcal{F})^{t_2}(\mathcal{F}\mathcal{V})\cdots(\mathcal{V}\mathcal{F})^{t_u}(\mathcal{F}\mathcal{V}),$$

where we write $t_i = 0$ at places where we have $(\mathcal{F}\mathcal{V})(\mathcal{F}\mathcal{V}) = (\mathcal{F}\mathcal{V})(\mathcal{V}\mathcal{F})^0(\mathcal{F}\mathcal{V})$. We see that A is the number of times we have $t_i > 0$. Note that in this notation, if $\cdots(\mathcal{V}\mathcal{F})^{t_i}\mathcal{F}z_j\mathcal{V}\cdots$ then $v(Z_j) = 2$ and conversely all such letters are at such places; hence $u = b$. We write a_{bot} for the number of times that $v(Z_j) = 1$ and $\cdots(L_{j-1} = \mathcal{V})Z_j(L_j = \mathcal{F})\cdots$. We recall notation fixed up to now:

$$a' := a_{\text{top}} > 0, \quad a'' = a_{\text{bot}} \geq 0; \quad \text{it follows that} \quad a = a' + a''.$$

Note that

$$a' + b = \mu; \qquad A + a'' = b; \quad A > 0, \quad b > 0.$$

We write $2 = \varepsilon_1 < \cdots < \varepsilon_A < 2\mu$ for the indices immediately after $\mathcal{V}^2$ appears; i.e. these are all indices for which $w = \cdots\mathcal{V}\mathcal{V}z_{\varepsilon_j}\cdots$. Note that all ε_j are even. We write $\xi_j := Z_{\varepsilon_j}$.

We write $\gamma_1 < \cdots < \gamma_{a''}$ for those indices with $v(Z_j) = 1$ and $\cdots(L_{j-1} = \mathcal{V})z_j(L_j = \mathcal{F})\cdots$; not that $a'' \geq 0$; in case $a'' = 0$, there is no index γ_j. We write $\eta_j := Z_{\gamma_j}$.

We write $t = t(j)$ in the case that z_{ε_j} appears in the part $(\mathcal{V}\mathcal{F})^{(t(j))}$ in the word w; i.e. $w = \cdots(\mathcal{V} = L_{\varepsilon_j - 1})(\mathcal{V}\mathcal{F})^{(t(j))}\mathcal{F}\cdots$.

(9.6) Lemma. *Consider $\xi_j := Z_{\varepsilon_j}$ and suppose that we have*

$$\cdots(\mathcal{F}\mathcal{V})(\mathcal{V}Z'_{\varepsilon_j}\mathcal{F})(\mathcal{V}\mathcal{F})^{t-1}(\mathcal{F}\mathcal{V})\cdots, i.e. \quad t = t(j) \geq 0;$$

then

$$Z_{\varepsilon_j+1} = \mathcal{F}{\cdot}\xi_j, \quad Z_{\varepsilon_j+2} = \frac{1}{p}\mathcal{F}^2{\cdot}\xi_j, \cdots, \quad Z_{\varepsilon_j+2t+1} = \frac{1}{p^t}\mathcal{F}^{2t+1}{\cdot}\xi_j$$

are determined by Z_{ε_j}.

Proof. Keep in mind that we normalized all elements Z_s, see (9.4). Moreover $pM \subset \pi^2 Q'$. Equalities in the circular word $z_1 L_1 \cdots L_{2\mu}$ induce congruences for the elements Z_s; these congruences are equalities between the elements Z_s with $\varepsilon_j \leq s \leq \varepsilon_j + 2t + 1$, because for these indices we have $v(Z_s) \leq 1$. □

Remark. The elements $Z_{\varepsilon_j+2\ell}, \quad 1 \leq j \leq A, \quad 0 \leq \ell \leq t(j)$ and $\gamma_1, \cdots, \gamma_{a''}$ form a k-basis for $M/(\mathcal{F}M + \mathcal{V}M)$.

(9.7) We introduce variables

$$X_{j,s}, \quad 1 \leq j \leq A, \quad 1 \leq s \leq 2\mu; \quad Y_{j,s}, \quad 1 \leq j \leq a'', \quad 1 \leq s \leq 2\mu.$$

We write

$$\xi_j^{(X)} = \sum_{1 \leq s \leq 2\mu} [X_{j,s}]{\cdot}e_j, \qquad \eta_j^{(Y)} = \sum_{1 \leq s \leq 2\mu} [Y_{j,s}]{\cdot}\pi e_j.$$

From $\xi_j^{(X)} = Z_{\varepsilon_j}^{(X)}$ we determine $Z_{\varepsilon_j+1}^{(X)}, \cdots, \ Z_{\varepsilon_j+2t(j)+1}^{(X)}$ as in the lemma above by writing:

$$Z_{\varepsilon_j+1}^{(X)} = \mathcal{F}{\cdot}\xi_j^{(X)}, \cdots, \ Z_{\varepsilon_j+2t(j)+1}^{(X)} = \frac{1}{p^t(j)}\mathcal{F}^{2t(j)+1}{\cdot}\xi_j.$$

For every $1 \leq j \leq A$ we write $Z_{\varepsilon_j-1} = \mathcal{V}Z_{\varepsilon_j}$.

We determine under *which conditions the variables $X_{j,s}$ and $Y_{j,s}$ define elements (there are a elements):*

$$(*(X,Y)) \quad \xi_j^{(X)}, Z_{\varepsilon_j+2\ell}^{(X)}, \ \ 1 \leq j \leq A, \ 1 \leq \ell \leq t(j), \quad \eta_j^{(Y)}, \ \ 1 \leq j \leq a''$$

generating a Dieudonné module $M^{(X,Y)}$ whose "p-kernel" $\frac{1}{p}M^{(X,Y)}/M^{(X,Y)} \cong M^{(X,Y)}/p{\cdot}M^{(X,Y)}$ has geometric isomorphism type given by w.

(9.8) Here are those conditions/equations for $(*(X,Y))$:

$$\xi_j^{(X)}, Z_{\varepsilon_j+s}^{(X)}, \ \ 1 \leq j \leq A, \ 1 \leq s \leq t(j) \quad \text{are linearly independent in} \quad Q'/\pi{\cdot}Q'; \qquad (1)$$

$$Z_1, Z_3, \cdots, Z_{2\mu-1} \quad \text{generate} \quad Q/\pi Q; \qquad (2)$$

note that $\pi Q/\pi^2 Q \twoheadrightarrow \pi Q/pM$; we write $U = \pi Q/pM$;

$$\mathcal{F}^2 Z_{\varepsilon_j+2t(j)} \equiv \mathcal{V}Z_{\varepsilon_j+2t(j)+3} \pmod{pM^{(X)}}, \ \ 1 \leq j \leq A; \qquad (3)$$

$$\mathcal{F}Z\gamma_j \equiv \mathcal{V}Z_{\gamma_j+2} \pmod{pM^{(X)}}, \ \ 1 \leq j \leq a''. \qquad (4)$$

Note that (1) and (2) are open conditions on the variables; we see that (3) and (4) are equalities in U; *we see that the tuple (ξ_j, $\ 1 \leq j \leq A$; $\ \eta_j$, $\ 1 \leq j \leq a''$) gives a solution for these equations.* Note that if (x) and (y) satisfy (1), (2), (3) and (4) then $\xi^{(x)}$ and $\eta^{(y)}$ determine a Dieudonné module whose "p-kernel" is given by w.

We write $\mathbb{A}^{(X,Y)}$ for the affine space given by the variables $(*(X,Y))$; hence $\dim(\mathbb{A}^{(X,Y)}) = A{\cdot}2\mu{+}a''{\cdot}2\mu$. We write $\mathbb{A}^{(X)}$ for the affine space given by the variables $X_{j,s}$; hence $\dim(\mathbb{A}^{(X)}) = A{\cdot}2\mu$. We write $\mathcal{G}$ for the Grassmannian $\mathrm{Grass}(a_{top}, 2\mu)$ of linear spaces of dimension $a' = a_{top}$ in affine space of dimension 2μ. Note that $M^{(X,Y)}$ determines the point $[M^{(X,Y)}/Q] \in \mathcal{G}$.

(9.9) Proposition. *We construct a commutative diagram*

$$\begin{array}{ccccc} \mathbb{A}^{(X,Y)} & \longrightarrow & \mathbb{A}^{(X)} & \longrightarrow & \mathcal{G} \\ \uparrow & & \uparrow & & \uparrow \\ \mathcal{X} & \longrightarrow & \mathcal{Y} & \longrightarrow & \mathcal{Z}; \end{array}$$

for properties of $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ see below.

(a) The conditions/equations (1) – (4) above define a locally closed set of $\mathcal{X}' \subset \mathbb{A}^{(X,Y)}$; this set contains the point (ξ, η); we define $\mathcal{X} \subset \mathcal{X}' \subset \mathbb{A}^{(X,Y)}$ as an irreducible component containing this point. *Then:*

$$\dim(\mathcal{X}) \geq (A + a''){\cdot}\mu - b{\cdot}(\mu - a').$$

(b) Write $f : \mathbb{A}^{(X,Y)} \longrightarrow \mathbb{A}^{(X)}$ for the projection (forgetting Y); this induces $f_{\mathcal{X}} : \mathcal{X} \to \mathbb{A}^{(X)}$;

fibers of the morphism $f_{\mathcal{X}}$ have dimension at most $a''{\cdot}a'$.

(c) Let $\mathcal{Y}$ be the image $\mathcal{Y} = f_{\mathcal{X}}(\mathcal{X})$; *then*

$$\dim(\mathcal{Y}) \geq A{\cdot}a'.$$

(d) Write $g : \mathcal{Y} \to \mathcal{G}$ for the map which assigns to the given data the element $g(M^{(X,Y)}) := [M^{(X,Y)}/Q] \in \mathcal{G}$. Note that this depends only on the variables $X_{j,s}$.

Fibers of the morphism $g : \mathcal{Y} \to \mathcal{G}$ have dimension at most $A{\cdot}(a'-1)$.

(e) Consider the locally closed set $\mathcal{Z} \subset \mathcal{G}$ of points $[B/Q] \in \mathcal{G}$ such that $B+Q$ generates a Dieudonné module $M^{(B)}$ inside Q' where the geometric isomorphism type of $M^{(B)}/pM^{(B)}$ is given by w. *Then:*

$$\dim(\mathcal{Z}) \geq A \geq 1.$$

By this we mean that every component of $\mathcal{Z}$ has at least this dimension.
Proof. (a) There are $(A+a'')\mu$ unknowns, the dimension of $\mathbb{A}^{(X,Y)}$. By (3) and (4) we obtain $b{\cdot}(\mu - a')$ equations, as $\dim(U) = \mu - a'$. Hence

$$\dim(\mathcal{X}) \geq (A+a'')\mu - b{\cdot}(\mu - a') = ba'.$$

(b) There are a'' elements η_j^Y. Fixing $\mathcal{V}(\eta_j^Y) \in U$ we see that this image is equal to $\mathcal{V}(\eta_j^Y + C_j) \in U$ if and only if $\mathcal{V}C_j \in pM$. This proves (b).
(c) Hence

$$\dim(\mathcal{Y}) \geq ba' - a''a' = Aa'.$$

Discussion: note that $\mathcal{Y}$ is constructible; we can talk about $\dim(\mathcal{Y})$; we are eventually interested in $\mathcal{Z}$, and we know that this is a locally closed set in $\mathcal{G}$.
(d) Instead of $\xi_j^{(X)}$ we could choose $\lambda{\cdot}\xi_j^{(X)} + D_j$, with $0 \neq \lambda \in k$ and and D_j a linear combination of all base elements in M/Q not equal to $\xi_j^{(X)}$. Trying to satisfy the equations above and going through the word w we see that $\lambda \in \mathbb{F}_{p^{2\mu}}$. Hence all D_j, $1 \leq j \leq A$, give a "freedom" of dimension at most $A(a'-1)$.
Discussion: It may be that several choices for C_j and for D_j do not give a solution to the equations above.

Hence fibers of $\mathcal{Y} \to \mathcal{Z}$ have dimension at most $A(a'-1)$.
(e) We conclude:

$$\dim(\mathcal{Z}) \geq Aa' - A(a'-1) = A \geq 1.$$

This proves the proposition. $\square$

(9.10) Corollary. *Suppose G and $X = \mathcal{L}(G)$ are as in* (8.5), (8.7)(1). *There is a family of positive dimension in $\mathcal{S}_G(T_{\beta,\delta})$ with $\beta = \sigma = \mu{\cdot}(1,1)$ and $\delta = a'$ which contains the given X as closed fiber.*
By construction X determines a point in $\mathcal{S}_G(T_{\sigma,a'}) \subset \mathcal{Z}$ such that X is the closed fiber above this point. By the last part of the preceding proposition we see that this family in $\mathcal{G}$ has positive dimension. $\square$

By (8.3) this proves (8.1) in the case (8.7)(1). $\square$(8.1)(1)

10 Case (2)

We use assumptions and notations as in (8.5), and (8.7)(2). We construct

$$v : Q'\backslash\{0\} \to \mathbb{Z}_{\geq 0} \quad \text{by:} \qquad v(Z) = i \Leftrightarrow Z \in \pi^i{\cdot}Q', \quad Z \notin \pi^{i+1}{\cdot}Q'.$$

The word $w = L_1 \cdots L_h$ acts as $z_1 L_1 z_2 L_2 \cdots z_h L_h z_1$. Choose $Z_i \in M$ with $Z_i \bmod pM = z_i$. Assume the (circular) word to be presented in such a way that $v(Z_1) \leq v(Z_i)$ for all i. We write $v(z_i) = v(Z_i)$.

We focus on a subset of the elements z_i, the "top elements", and also on "bottom elements". We write

$$w = (\mathcal{F}^{d_1}\mathcal{V}^{c_1}) \cdots (\mathcal{F}^{d_a}\mathcal{V}^{c_a}), \quad d_i > 0, \quad c_i > 0,$$

and write

$$t_1 = z_1, \quad t_2 = z_{1+d_1+c_1}, \quad \cdots, \quad t_a = z_{1+d_1+c_1+\cdots+d_{a-1}+c_{a-1}},$$

and

$$b_1 = z_{1+d_1}, \quad b_2 = z_{1+d_1+c_1+d_2}, \quad \cdots, \quad b_a = z_{1+d_1+c_1+\cdots+c_{a-1}+d_a}.$$

The top elements are those where the word reads $\cdots \mathcal{V}t\mathcal{F}\cdots$, the bottom elements are those where the word reads $\cdots \mathcal{F}b\mathcal{V}\cdots$.

We pay special attention not only to a "highest top element": t_1, but also to a "lowest bottom element": we choose ε, with $1 \leq \varepsilon \leq a$ such that

$$v(b_\varepsilon) \quad \geq \quad v(b_j) \qquad \forall j.$$

This can be phrased as: $(d_1 + \cdot + d_i)n + (c_1 + \cdots + c_{i-1})m$ is maximal for $i = \varepsilon$. This implies

$$M \cap \pi^{v(b_\varepsilon)+1}{\cdot}Q' \subset p{\cdot}M. \qquad (*)$$

By definition the skeleton of Q' is the image of $\mathbb{D}(H \otimes \mathbb{F}_p)$ in $\mathbb{D}(H \otimes k) = Q'$. As we are in case (8.7)(2), there exists an element G in the skeleton of Q' such that $v(G) > 0$ and $G \notin M$, and such that

$$\pi^{v(G)+1}{\cdot}Q' \subset M. \qquad (**)$$

I.e. G is an element with maximal value having the property not being in M. Being in the skeleton implies that $\mathcal{F}^m G = \mathcal{V}^n G$ (this assumption is just made in order to make computations easier). We fix such a choice.

Remark. In fact we have $\pi^{v(G)+1}{\cdot}Q' = Q$, i.e. $v(G) + 1 = i$ in the notation in (8.7). Indeed, we know that Q is a π-power multiple of Q', we see that $G \notin M$ and we conclude by $(**)$.

For a choice of fields $k \subset K$ and an element $u \in K$ we are going to construct a Dieudonné module $M^{(u)}$ over the algebraic closure Ω of K (the choice of $M^{(u)}$ depends on M, on u, and on the particular choices of a highest top element t_1 and a lowest bottom element b_ε).

As before we define the top elements $T_i \in M$ by $T_1 = Z_1, \cdots$ and the bottom elements $B_1 = Z_{1+d_1} \cdots$. We write $U := [u] \in W_\infty(K)$, the Teichmüller lift of $u \in K$. For $1 \leq i \leq \varepsilon$ we define:

$$T_1^{(u)} = T_1 + U{\cdot}G, \quad T_2^{(u)} = p^{-c_1}\mathcal{F}^{d_1+c_1}(T_1 + U{\cdot}G), \cdots,$$

$$T_\varepsilon^{(u)} = p^{-(c_1+\cdots+c_{\varepsilon-1})}\mathcal{F}^{(d_1+c_1+d_2+\cdots+c_{\varepsilon-1})}(T_1+U{\cdot}G),$$

and

$$T_1^{(u)} = T_1+U{\cdot}G, \quad T_a^{(u)} = p^{-d_a}\mathcal{V}^{c_a+d_a}(T_1+U{\cdot}G), \cdots,$$
$$T_{\varepsilon+1}^{(u)} = p^{-(d_a+\cdots+d_{\varepsilon+1})}\mathcal{V}^{(c_a+d_a+c_{a-1}+\cdots+d_{\varepsilon+1})}(T_1+U{\cdot}G).$$

Note that for $u=0$ we have $T_i^{(u)} = T_i$ for all i.

We define $M^{(u)} \subset Q'$ as the Dieudonné module generated by $T_{\varepsilon+1}^{(u)}, \cdots, T_a^{(u)}, T_1^{(u)}, \cdots, T_\varepsilon^{(u)}$.

Remark on notation. We will use Q' for the Dieudonné module $\mathbb{D}(H)$, but also for the Dieudonné module $\mathbb{D}(H\otimes\Omega)$. In the latter case we should write $Q'\otimes W(\Omega)$, but we will not do that. We will study $M\subset Q'$ and $M^{(u)}\subset Q'\otimes W(\Omega)$, but we will simplify notation, e.g. write instead $M^{(u)}\subset Q'$, hoping that this will not cause confusion.

For a submodule $P\subset Q' = (\mathbb{D}(H_{1,1}))^\mu$ we write Type(P) for the subset of $\mathbb{Z}\times\{0,1,\cdots,\mu\}$ defined in the analogous way as we did this for $\mu=1$: we define Type(P) as the set of all pairs (i,D_i), where considering at place $i\in\mathbb{Z}$ we write $D_i\in\{0,1,\cdots,\mu\}$ as the dimension of $(\pi^i{\cdot}Q'\cap M)/(\pi^{i+1}{\cdot}Q'\cap M)$.

Crucial Lemma. *With notations introduced above:*
(a) *the isomorphism type of $M^{(u)}/p{\cdot}M^{(u)}$ is the same as the isomorphism type of $M/p{\cdot}M$, i.e.*

$$\Gamma\left(M^{(u)}/p{\cdot}M^{(u)}\right) = w;$$

(b) Type(M) = Type$(M^{(u)})$, *and $Q\subset M^{(u)}$ and the length of M/Q and of $M^{(u)}/Q$ are the same.*
Proof. We know $\mathcal{F}^{d_\varepsilon}{\cdot}t_\varepsilon = \mathcal{V}^{c_\varepsilon}t_{\varepsilon+1}$. By $(*)$ and $(**)$ we conclude that

$$\mathcal{F}^{d_\varepsilon}{\cdot}T_\varepsilon^{(u)} \equiv \mathcal{V}^{c_\varepsilon}T_{\varepsilon+1}^{(u)} \pmod{p{\cdot}M^{(u)}}.$$

This proves that the residue classes mod $p{\cdot}M^{(u)}$ of the elements $T_i^{(u)}$, $1\leq i\leq a$, in $M^{(u)}/p{\cdot}M^{(u)}$ are cyclic under the word w. This proves part (a) of the lemma.

This set of generators for $M^{(u)}$, cyclic modulo $p{\cdot}M^{(u)}$, is a W-basis for $M^{(u)}$. This proves Type(M) = Type$(M^{(u)})$. From this the other claims follow. This proves the lemma. □

(10.1) We come to a choice of a positive dimensional subspace of $\mathcal{S}_G(T_{\beta,\delta})$ containing x as in (8.1) in case (8.7)(2). We start with an algebraically closed field k. We choose a transcendental u over k, write $K=k(u)$, and we write Ω for an algebraic closure of K. Note that the Dieudonné module $M^{(u)}$ is defined over Ω. We have proved that $Q\subset M^{(u)}$ and that

the length δ of M/Q

(Dieudonné modules over k)

is the same as the length of $M^{(u)}/Q$

(Dieudonné modules over Ω). The Dieudonné module inclusions $Q\subset M^{(u)}\subset Q'$ gives rise to isogenies $H\to X^{(u)}\to H'$, and

$$N_u = \mathrm{Ker}(H\to X^{(u)}) \quad\subset\quad H[\pi^i] = \mathrm{Ker}(H\to H').$$

This subgroup scheme is a point in the Grassmannian considered, i.e. it corresponds with a point

$$(\rho_u : H \to X^{(u)} = H/N_u) \in T_{\beta,\delta};$$

this point is rational over some field L. Note that this field can be chosen within the perfect closure of K, and it can be chosen as a finite extension of K. We write B for the integral closure of $k[u]$ in L. Note that for any specialization $g : k[u] \to k$ the length of $M^{(g(u))}/Q$ equals δ; hence $\rho_u \in T_{\beta,\delta}(L)$ extends to $\rho \in T_{\beta,\delta}(B)$. Hence we have constructed a family $\mathrm{Spec}(B) =: S \subset T_{\beta,\delta}$ of positive dimension defined over k, containing $(\rho_0 : H \to X) = x$, where generic fiber and special fiber have the given w as K-cycle for the kernel by p. By (8.3) this proves (8.1) in case (8.7)(2). Hence the proof of (8.1) is finished; we have Theorem B as corollary.

$\square$(8.1), Theorem B

11 Some questions.

(11.1) Conjecture. Let X_0 be a p-divisible group, φ the isomorphism type of $X_0[p]$, and $D = \mathrm{Defo}(X_0)$ its equal-characteristic p universal deformation space. Inside D we have the "central leaf" $\mathcal{C}_{X_0}(D) \subset D$, the locus where the p-divisible group is geometrically isomorphic with X_0, and we have the "EO-stratum" $\mathcal{S}_\varphi(D) \subset D$, the locus where the p-kernel is geometrically isomorphic with $X_0[p]$. Clearly $\mathcal{C}_{X_0}(D) \subset \mathcal{S}_\varphi(D)$. We conjecture:

$$X_0 \quad \text{is not minimal} \quad \stackrel{?}{\Longrightarrow} \quad \mathcal{C}_{X_0}(D) \subsetneq \mathcal{S}_\varphi(D).$$

Remarks. By [8] we know that if X_0 is minimal, equality holds.

This conjecture holds if X_0 is isoclinic.

(11.2) Conjecture. Notation as in (11.1). Let $\gamma = \mathcal{N}(X_0)$. Denote by $\mathcal{W}^0_\gamma(D) \subset D$ the set where the Newton polygon is equal to γ; note that no Newton polygon strictly above γ appears on D. We conjecture:

$$X_0 \quad \text{is not minimal} \quad \stackrel{?}{\Longrightarrow} \quad \mathcal{C}_{X_0}(D) \subsetneq \left(\mathcal{W}^0_\gamma(D) \cap \mathcal{S}_\varphi(D)\right).$$

Remark. We showed above the special case of this conjecture, when $X_0 = \mathcal{L}(X_0[p])$. Note that (11.2) implies (11.1).

(11.3) Conjecture. Let (A_0, λ_0) be a principally polarized abelian variety. We conjecture:

$$X_0 := A_0[p^\infty] \quad \text{is not minimal} \quad \stackrel{?}{\Longrightarrow} \quad \mathcal{C}_{(X_0,\lambda_0)}(\mathcal{A}) \subsetneq \mathcal{S}_{(A_0,\lambda_0)[p]}(\mathcal{A}),$$

$$X_0 := A_0[p^\infty] \quad \text{is not minimal} \quad \stackrel{?}{\Longrightarrow} \quad \mathcal{C}_{(X_0,\lambda_0)}(\mathcal{A}) \subsetneq \left(\mathcal{W}^0_{\mathcal{N}(A_0)}(D) \cap \mathcal{S}_{(A_0,\lambda_0)[p]}(\mathcal{A})\right),$$

where $\mathcal{A} = \mathcal{A}_g \otimes \mathbb{F}_p$.

(11.4) Suppose given a semi-module A attached to m and n, see (1.6). *Can we describe all possibe* $\sum w_i$ *such that there exists* X *with* $\mathrm{Type}(X) = A$ and $\Gamma(X[p]) = \sum w_i$?

(11.5) An analogous question, phrased in slightly different terms: given a symmetric Newton polygon ξ. *Can we determine all possible isomorphisms types* φ *of a polarized* BT_1 *such that* $S_\varphi \cap W^0_\xi \neq \emptyset$?

References

[1] L. Illusie – *Déformations de groupes de Barsotti-Tate.* Exp.VI in: *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell* (Ed. L. Szpiro), Astérisque 127, Soc. Math. France 1985.

[2] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* Journ. Amer. Math. Soc. **13** (2000), 209 - 241. See: http://www.ams.org/jams

[3] H. Kraft – *Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten).* Sonderforsch. Bereich Bonn, September 1975. Ms. 86 pp.

[4] B. Moonen – *Group schemes with additional structures and Weyl group cosets.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 255-298 .

[5] F. Oort – *Commutative group schemes.* Lect. Notes Math. 15, Springer - Verlag 1966.

[6] F. Oort – *A stratification of a moduli space of polarized abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 345 - 416.

[7] F. Oort – *Foliations in moduli spaces of abelian varieties.* Journ. Amer. Math. Soc. **17** (2004), 267-296.

[8] F. Oort – *Minimal p-divisible groups.* [To appear in Ann. Math.]
See: http://www.math.uu.nl/people/oort/

[9] *Séminaire de géométrie algébrique,* SGA 3. *Schémas en groupes I.* M. Demazure and A. Grothendieck. Lect. Notes Math. 151, Springer - Verlag, 1970.

Frans Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: oort@math.uu.nl