Workshop on Hopf Algebras
Hanoi, October-November 2023
Lectures by Frans Oort:

I Finite commutative group schemes annihilated by p

II Is a finite group scheme annihilated by its rank?

1 Introduction. We focus on the concept of a finite group scheme. Although basic concepts are formulated for schemes, eventually the core of our considerations can be formulated for base fields or base rings and algebras over base rings. We do not need deep basic concepts of algebraic geometry, although in remarks indicating geometric motivation and consequences more knowledge is needed for understanding.
Warning. My mini-course is not meant as a complete course in finite group schemes. Some results will be taken as **BB** (black box: the statement should be clear and understandable, but no proof is given here). More extensive description of the theory of finite group schemes are given in [24], [44], [36], [32], [35].

We have two main themes:

(I) A classification of finite *commutative* group schemes annihilated by p over a perfect field as announced by Hanspeter Kraft in [15]. This implies that the set of isomorphisms classes of such group schemes of a fixed rank over an algebraically closed field is *finite*, Section 8, see (1.1), with important geometric applications. In the preprint by Kraft this result is stated. Complete proofs can be found in [26], [18], [3].

- It this interesting, is this a useful mathematical idea to study? In Section 20 we see that this theorem is crucial in understanding moduli spaces of polarized abelian varieties in positive characteristic.

Dieudonné theory translates properties of commutative group schemes over perfect fields into properties of modules over a certain ring. By the Krull-Remak-Schmidt Theorem, see (2.3), a module of finite length is a direct sum of indecomposable modules. The idea of a proof of a proof of (I) is

- construct candidates for indecomposable finite group schemes, see (3.2), (3.3).
- then show these are indeed indecomposable,
- and prove these are all possible indecomposable modules.

The classification of finite commutative group schemes annihilated by p over an algebraically closed field k as described in Theorem (8.3) has a corollary:

(1.1) Corollary. *Let k be an algebraically closed field of characteristic p. For any $n \in \mathbb{Z}_{>0}$ the set of k-isomorphism classes of finite commutative group schemes of rank p^n annihilated by p is* finite. See (8.4).

We see three condition: (1) k is algebraically closed, (2) work with *commutative* group schemes, (3) annihilated by p. In Section 10 we show all three conditions are necessary in order to conclude finiteness in (1.1).

The idea of this classification can be found in a preprint [15] in 1975.
Proofs of this can be found in [26], [18], [19], [20], [3], [21]. In order to state this theorem we will first develop notations and ideas, especially the concepts of *circular words* (3.3) and *linear words* (3.2), as for the first time given by Kraft, in order to be able to formulate precise results.

Of independent interests are two tools we use in the proof: the Krull-Remak-Schmidt Theorem, see (2.3), and a theorem originally proved by Hasse and Witt in 1936, now known as the Lang-Seidenberg Theorem (5.3).

(II) We study the question whether a finite group scheme of constant rank over an arbitrary base scheme is annihilated by its rank (the scheme theoretic analogue of a theorem of Legendre for abstract finite groups).

Open Question. In the second talk for a finite group scheme $G \to S$ of rank m we study the morphism $[m]_G : G \to G$ and we ask the question whether this factors through the trivial element of G/S:

$$([m]_G : G \to G) \quad \overset{?}{=} \quad \left(G \to S \overset{e}{\hookrightarrow} G\right), \quad \mathrm{rank}(G/S) = m.$$

We collect all kind of examples in a separate section. These will be of crucial importance for understanding material discussed.

The following concepts will be assumed to be known to the audience: basic algebra and basic algebraic geometry; the definition of a group scheme; the morphism $F_S : S \to S^{(p)}$ for a (group) scheme in characteristic p; the notion of the morphism $V_G : G^{(p)} \to G$ of a commutative group scheme in characteristic p. The theory of the Dieudonné module of a commutative group scheme in over a perfect field of characteristic p.

2 Strategy for proof of the classification of finite commutative group schemes annihilated by p

(2.1) In this topic we fix a prime number p, and all group schemes considered will be over an algebraically closed field $k \supset \mathbb{F}_p$. We study commutative group schemes, apply the Dieudonné module functor, shifting the problem to a classification of certain modules. We assume moreover that group schemes considered, and hence Dieudonné modules considered, are annihilated by p. We write $\Lambda = \Lambda_k$ for the ring of infinite Witt vectors over k, and $R = \Lambda\{\mathcal{F}, \mathcal{V}\}$ with the well know relations, in particular

$$R^{(1)} = R/pR = k\{\mathcal{F}, \mathcal{V}\}$$

for the Dieudonné ring modulo p, i.e. with relations

$$\mathcal{F}\mathcal{V} = 0 = \mathcal{V}\mathcal{F}, \quad \mathcal{F}x = x^p\mathcal{F}, \quad x\mathcal{V} = \mathcal{V}x^p.$$

Write $\mathcal{M} = \mathcal{M}_k$ for the category of left modules over $R^{(1)}$, finite as a k-vector space (i.e. of finite length). We are going to classify all isomorphism classes in $\mathcal{M}_k$.

This category $\mathcal{M}$ is an abelian category, kernels and cokernels exist, direct sums exist, and every object is artinian and noetherian (descending and ascending chains are stationary.)

Covariant Dieudonné module theory translates $F : G \to G^{(p)}$ into multiplication by $\mathcal{V} : \mathbb{D}(G) \to \mathbb{D}(G)$, and (for commutative group schemes) translates $V : G^{(p)} \to G$ in multiplication by $\mathcal{F} : \mathbb{D}(G) \to \mathbb{D}(G)$. If G is finite and local, then F is nilpotent, hence $\mathcal{V}$ is nilpotent. If G^D is finite and local, then V is nilpotent on G, hence $\mathcal{F}$ is nilpotent.

(2.2) Definition. An object M in an additive category is said to be *indecomposable* if $M \neq 0$ and $M \cong M_1 \oplus M_2$ implies either $M_1 = 0$ or $M_2 = 0$.

An object M is called *simple* if $0 \subset M_1 \subsetneq M$ implies $0 = M_1$.

Example. A finite abelian group G is indecomposable if and only G is cyclic of prime power order. A finite abelian group G is a simple object in that category if and only G is cyclic of prime order.

Example. Up to isomorphism there are three simple finite group schemes of rank p over $k = \overline{k} \supset \mathbb{F}_p$ in the category of finite commutative group schemes over k:

$$\underline{\mathbb{Z}/p}_k; \quad \alpha_{p,k}; \quad \mu_{p,k};$$

their (covariant) Dieudonné modules are k-vector spacs of dimension one with respectively:

$\mathcal{F} = 0$, and $\mathcal{V}$ bijective; $\quad \mathcal{F} = 0$, and $\mathcal{V} = 0$; $\quad \mathcal{F} = 0$ bijective, and $\mathcal{V} = 0$.

The splitting of finite commutative group schemes (over a perfect field) into etale-local, local-local, local etale summands translates into properties of their Dieudonné modules. In particular

$$(G \text{ is local-local}) \quad \Longleftrightarrow \quad (\mathcal{V} \text{ and } \mathcal{F} \text{ are nilpotent on } M = \mathbb{D}(G)).$$

The category of finite dimensional Dieudonné modules annihilated by p is an abelian category, kernels and cokernels exist, direct sums exist, and every object is artinian and noetherian (descending and ascending chains are stationary.)

Remark / Definition. For a module over $k\{\mathcal{F}, \mathcal{V}\}$ we have

$$\mathcal{V}(M) \subset \mathrm{Ker}(\mathcal{F}) \text{ and } \mathcal{F}(M) \subset \mathrm{Ker}(\mathcal{V}).$$

Suppose $\dim_k(M) < \infty$. Note that $\dim(\mathrm{Ker}(\mathcal{F})) + \dim(\mathcal{F}(M)) = \dim(M)$ and the same for $\mathcal{V}$. Hence:

$$(\mathcal{V}(M) = \mathrm{Ker}(\mathcal{F})) \Longleftrightarrow (\mathcal{F}(M) = \mathrm{Ker}(\mathcal{V})).$$

We say M is a BT_1-module (explanation of this terminology later) if this condition holds.

Remark. Consider $\mathcal{M}^{\mathrm{BT}}$, the category of BT_1-modules over k; note that $\mathbb{D}(\alpha_{p,k})$ is not in this category; we know a (non-trivial) classification of all simple objects in $\mathcal{M}^{\mathrm{BT}}$, see [27]; for more information see Section 20; note that any simple object in $\mathcal{M}^{\mathrm{BT}}$ on which $\mathcal{F}$ and $\mathcal{V}$ are nilpotent is not simple in $\mathcal{M}$. We use the terminology "simple" and "indecomposable" for objects considered in $\mathcal{M}$. Note that not every morphism in $\mathcal{M}^{\mathrm{BT}}$ has a kernel or a cokernel in this category $\mathcal{M}^{\mathrm{BT}}$.

We recall the following result for an arbitrary ring, and later we will apply this for the Dieudonné ring.

(2.3) Theorem (Krull-Remak-Schmidt).
See [1], § 2.5; see [33] Chap 5;
see [16], Proposition X.7.4 and Theorem X.7 5.
Just a reminder: for $R = \mathbb{Z}$, classifying finite abelian groups, we see that every simple object is $\mathbb{Z}/\ell$ where ℓ is a prime number, and every indecomposable object is of the form $\mathbb{Z}/\ell^n$, with $n \in \mathbb{Z}_{>0}$. (Do not get into confusion: "simple finite groups" is a much wider concept than "simple object" in the category of finite abelian groups.)

Hence the classification theorem we are looking for translates into:
Question. *Classify all isomorphism classes in $\mathcal{M} = \mathcal{M}_k$: describe all indecomposable objects in $\mathcal{M}$.*

A little warning. In the theorem above the indecomposable modules and their multiplicities are determined by a module M considered; however the decomposition-isomorphism in the theorem in general is far from unique. This will be the most serious obstacle in the proof discussed below.

This idea indicates what kind of facts we have to show in order to answer the question: *find all indecomposable objects in $\mathcal{M}$.*

The proof we are going to give as an answer to this question will consists of the following steps.

(A) In the category $\mathcal{M}$, following Kraft, we construct objects M'_u and $M_{\lfloor w \rceil}$. The goal is to show these are indecomposable and that these are the only indecomposable modules in $\mathcal{M}$.

- *How do we prove these are indecomposable,*
- *how do we show there are no other idecomposable modules in $\mathcal{M}$, and*
- *how do we find which appear in a decomposition of a given $M \in \mathcal{M}$?*

(B) For any $M \in \mathcal{M}$ we construct the canonical filtration (canonical flag)

$$\text{can.flag}(M) = Q_* = (0 = Q_0 \subsetneqq \cdots \subsetneqq Q_i \subsetneqq Q_{i+1} \subsetneqq \cdots \subsetneqq Q_m = M)$$

and we prove various properties. In particular we show this flag is *saturated*, see (4.2), (4.4). A *flag* is a filtration were the numbering is chosen such that $Q_i \subsetneqq Q_{i+1}$ for every i.

(C) The associated graded

$$\mathcal{G}(M) = \mathcal{G}(\text{can.flag}(M)) := \sum_{0 \leq i < m} \quad Q_{i+1}/Q_i$$

turns out to be a Dieudonné module, steps in the canonical filtration are vertices of a directed graph $\Gamma = \Gamma(M)$ and
(AHA) *this defines a set of words and a decomposition of $\mathcal{G}(M)$ into the indecomposables constructed in* (A).
Note that we still have to show these are all indecomposable modules.
Notation. We write $\sum$ or $\times$ for a direct sum of k-vector spaces and $\oplus$ and $\bigoplus$ for a direct sums of Dieudonné modules.

(D) Using this filtration we show every M'_u is indecomposable and for an indecomposable cyclic word w the object $M_{\lfloor w \rceil}$ is indecomposable.
Remark. We give a proof using filtrations; is is plausible that a (complicated) direct proof can be given of the fact that these modules are indecomposable.

(E) The canonical maps $Q_{i+1} \to Q_{i+1}/Q_i$ can be lifted (choices involved) to an isomorphism of Dieudonné modules

$$M \quad \overset{\sim}{\longleftarrow} \quad \mathcal{G}(M) \quad \cong \quad (\oplus_{i \in L} \;\; M'_{u_i}) \bigoplus \left(\oplus_{j \in C} \;\; M_{\lfloor w_j \rceil}\right),$$

where L is a finite set of linear words and C is a finite a set of indecomposable circular words.

3 A: Construction of M'_u and $M_{\lfloor w \rceil}$

(3.1) We explain a notation we are going to use. For a module $M \in \mathcal{M}$ and a non-zero element $x \in M$ we use the following shorthands.

$\mathcal{V}x$	$\mathcal{V}x \neq 0$	$x \notin \mathrm{Ker}(\mathcal{V})$	$(\mathcal{V}(x) \neq 0) \overset{\mathcal{V}}{\mapsfrom} x$
$\mathcal{F}x$	$\exists y \in M \quad \text{with} \quad \mathcal{F}y = x$	$x \in \mathcal{F}(M)$	$y \overset{\mathcal{F}}{\mapsto} x, \quad \mathcal{V}(x) = 0$
$\emptyset x$	$x \in \mathrm{Ker}(\mathcal{V}) \quad \text{and} \quad x \notin \mathcal{F}(M)$		
$x\mathcal{F}$	$\mathcal{F}x \neq 0$	$x \notin \mathrm{Ker}(\mathcal{F})$	$x \overset{\mathcal{F}}{\mapsto} (\mathcal{F}(x) \neq 0)$
$x\mathcal{V}$	$\exists y \in M \quad \text{with} \quad \mathcal{V}y = x$		$x \overset{\mathcal{V}}{\mapsfrom} y, \quad \mathcal{F}(x) = 0$
$x\emptyset$	$x \in \mathrm{Ker}(\mathcal{F}) \quad \text{and} \quad x \notin \mathcal{V}(M)$		

Note the direction of the arrows. Moreover, as $\mathcal{F}\mathcal{V} = 0 = \mathcal{V}\mathcal{F}$ we have $\mathrm{Ker}(\mathcal{V}) \subset \mathcal{F}(M)$ and $\mathrm{Ker}(\mathcal{F}) \subset \mathcal{V}(M)$; check that al possibilities appear in the table above.
Note:
$\mathcal{V}(x) = z \quad \Rightarrow \quad \mathcal{F}(z) = 0;$
$\mathcal{F}(y) = x \quad \Rightarrow \quad \mathcal{V}(x) = 0.$

(3.2) Linear words: construction of M'_u.
Let $h \in \mathbb{Z}_{\geq 0}$, let $L_1, \cdots, L_h \in \{\mathcal{F}, \mathcal{V}\}$; write $u = \emptyset$ if $h = 0$, and otherwise $u = (L_1 \cdots L_h)$; we say u is a *linear word*. We choose a k-vector space of dimension $h + 1$

$$M'_u = \sum_{1 \leq i \leq h+1} k \cdot z_i$$

and we define $\mathcal{F}$ and $\mathcal{V}$ on M'_u by

$$\emptyset z_1 L_1 z_2 \cdots z_h L_h z_{h+1} \emptyset;$$

sometimes we write $L_0 = \emptyset$, and $L_{h+1} = \emptyset$. For every index i the notation $L_{i-1} z_i L_i$ defines $\mathcal{F}(z_i)$ and $\mathcal{V}(z_i)$. Moreover $\mathcal{F}\mathcal{V} = 0 = \mathcal{V}\mathcal{F}$ for every base vector.

Conclusion. We have defined a Dieudonné module $M'_u \in \mathcal{M}$.
Moreover $\mathcal{F}^{h+1}$ and $\mathcal{V}^{h+1}$ are zero on M'_u (give a proof); hence $M'_u \in \mathcal{M}$ is local-local.
A particular case. For the emptyword, $h = 0$ we see $M'_\emptyset$ has dimension one, and $\mathcal{F}$ and $\mathcal{V}$ are zero on this module. We see $\mathbb{D}(\alpha_p) = M'_\emptyset$.

Claim. *Suppose $\mathcal{F}$ and $\mathcal{V}$ are nilpotent on M For every $0 \neq M \in \mathcal{M}$ there exists an inclusion $M'_{\emptyset} \hookrightarrow M$;*

$M'_{\emptyset}$ is the only simple local-local object in $\mathcal{M}$.

Proof. For every $0 \neq x \in M$ either $\mathcal{F}(x) = 0 = \mathcal{V}(x)$, and we are done,

or there exists $j \in \mathbb{Z}_{>0}$ with $\mathcal{F}^j(x) \neq 0$ and $\mathcal{F}^{j+1}(x) = 0$, and $M'_{\emptyset} \cong k{\cdot}\mathcal{F}^j(x)$,

or there exists $j \in \mathbb{Z}_{>0}$ with $\mathcal{V}^j(x) \neq 0$ and $\mathcal{V}^{j+1}(x) = 0$, and $M'_{\emptyset} \cong k{\cdot}\mathcal{V}^j(x)$. □

Claim. *For every word u, $M \in M'_u$, we have*

$$\mathcal{V}(M) \subsetneqq \mathrm{Ker}(\mathcal{F}) \quad \text{and} \quad \mathcal{F}(M) \subsetneqq \mathrm{Ker}(\mathcal{V}).$$

Proof.
For $\emptyset z_1?$ we see $z_1 \notin \mathcal{F}(M)$ and $z_1 \in \mathrm{Ker}(\mathcal{V})$;
For $?z_h\emptyset$ we see $z_h \notin \mathcal{V}(M)$ and $z_1 \in \mathrm{Ker}(\mathcal{F})$. □

(3.3) Circular words: construction of $M_{\lfloor w \rceil}$.
Let $h \in \mathbb{Z}_{\geq 1}$, let $L_1, \cdots, L_h \in \{\mathcal{F}, \mathcal{V}\}$. We write $w = [L_1 \cdots L_h]$, call this a *circular word*; define L_j for every $j \in \mathbb{Z}$: write $L_{j+mh} = L_j$ for every $m \in \mathbb{Z}$; circular permutations (shift of indices) give an equivalence between circular word; its equivalence class is indicated by $\lfloor w \rceil$. We choose a k-vector space of dimension h

$$M_{\lfloor w \rceil} = \sum_{1 \leq i \leq h} k{\cdot}z_i$$

and we define $\mathcal{F}$ and $\mathcal{V}$ on $M_{\lfloor w \rceil}$ by

$$z_1 L_1 z_2 \cdots z_h L_h z_1.$$

For every index i the notation $L_{1-i} z_i L_i$ defines $\mathcal{F}(z_i)$ and $\mathcal{V}(z_i)$. Moreover $\mathcal{F}\mathcal{V} = 0 = \mathcal{V}\mathcal{F}$ for every base vector.
Conclusion. We have defined a Dieudonné module $M_{\lfloor w \rceil}$.

Consider $M = M_{\lfloor w \rceil}$ with $w = [L_1 \cdots L_h]$ over $k = \overline{k} \supset \mathbb{F}_p$.

- For every w and every $d \in \mathbb{Z}_{>0}$, there is an isomorphism $M_{\lfloor w^d \rceil} \cong (M_{\lfloor w \rceil})^d$; here we write $w^d = [L_1 \cdots L_h, \cdots, L_1 \cdots L_h]$, the word w repeated d times. In a proof of this fact we use $\mathbb{F}_{p^d} \subset k$.

- **Definition.** A circular word w' is said to be *indecomposable* if there does not exists a circular word w and $d \in \mathbb{Z}_{>1}$ with $w' = w^d$.

- We going to show that an indecomposable circular word w defines an indecomposable module $M = M_{\lfloor w \rceil}$.
- On $M_{\lfloor [\mathcal{F}] \rceil}$ the map $\mathcal{V}$ is zero and $\mathcal{F}$ is bijective. Note that $M_{\lfloor [\mathcal{F}] \rceil} \cong \mathbb{D}(\underline{\mathbb{Z}/p})$. Recall that $M_{\lfloor \mathcal{F} \rceil^d} \cong (M_{\mathcal{F}})^d$.
- On $M_{\lfloor [\mathcal{V}] \rceil}$ the map $\mathcal{F}$ is zero and $\mathcal{V}$ is bijective. Note that $M_{\lfloor [\mathcal{V}] \rceil} \cong \mathbb{D}(\mu_p)$. Recall that $M_{\lfloor \mathcal{V} \rceil^d} \cong (M_{\mathcal{V}})^d$.
- Any $M = M_{\lfloor w \rceil}$ is a BT_1-module. (Give a proof.)
- If both $\mathcal{F}$ and $\mathcal{V}$ do appear in w, then $M_{\lfloor w \rceil}$ is local-local (give a proof).
- We see: over k the classification of indecomposable modules $M_w \in \mathcal{M}$ is easy if only $\mathcal{F}$ or only $\mathcal{V}$ appear in w, and we are left with the case both $\mathcal{F}$ and $\mathcal{V}$ do appear in w.
- We will write M_w instead of $M_{\lfloor w \rceil}$ if no confusion is possible.

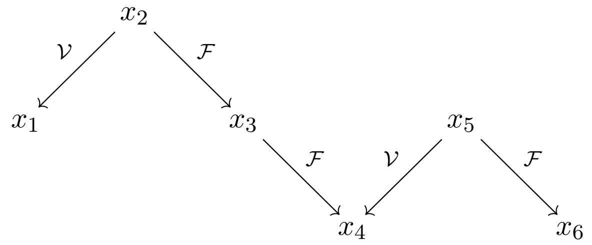
Remark.

- Maps between BT_1-module can have a a kernel and/or a cokernel that is not a BT_1-module.
- A map $M'_{u_1} \to M'_{u_2}$ can have a a kernel and/or a cokernel that is a BT_1-module.
- In general an automorphism of $M'_u \oplus M_{\lfloor w \rceil}$ does not preserve the summands.
- There are many extensions of the form $M/P' \cong P''$ that are not split, even in the case P' and P'' are indecomposable.

These facts are serious obstacles for a proof we are going to present: we are going to write any M as a decomposition of indecomposables, but even the splitting in circular-linear ones is not canonical in general.

(3.4) Exercise. If $M/P' = P''$ is an extension in $\mathcal{M}$ and $P', P'' \in \mathcal{M}^{\mathrm{BT}}$ then also M is a BT_1-module.

(3.5) It is convenient to visualize linear and circular words by graphs. Here are examples



Note : $\mathcal{F}$ from left to right,

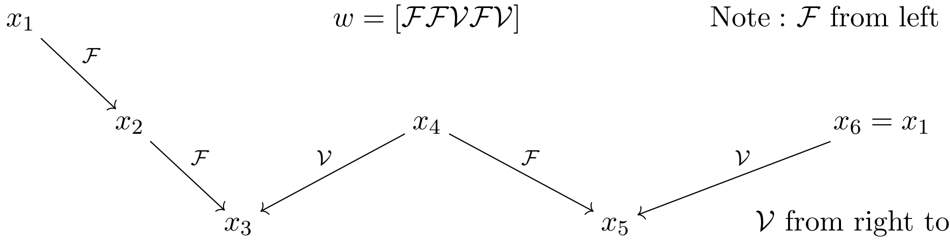
$u = (\mathcal{V}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F})$;

$\mathcal{V}$ from right to left.

Note: $\mathcal{F}(x_1) = 0 = \mathcal{V}(x_1)$, $\mathcal{F}(x_4) = 0 = \mathcal{V}(x_4)$ and $\mathcal{F}(x_6) = 0 = \mathcal{V}(x_6)$.

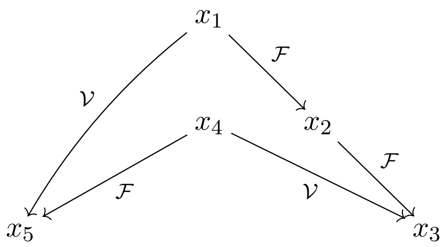
$w = [\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}]$

Note : $\mathcal{F}$ from left to right,



$\mathcal{V}$ from right to left.

or



Note : clockwise $\mathcal{F}$

$w = [\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}]$.

anti – clockwise : $\mathcal{V}$.

4 B: The canonical filtration

(4.1) In this section we develop the basic idea used in proofs below. We consider *filtrations* of M by Dieudonné submodules. A *flag* in M is a filtration $S_* = (0 = S_0 \subset \cdots \subset S_m = M)$ with proper inclusions: for every $0 \leq i < m$ we have $S_i \subsetneqq S_{i+1}$.

(4.2) Definition. A flag S_* is called *saturated* if the following two properties hold:
(F) For every index $0 \leq i < m$ either $\mathcal{F}(S_i) = \mathcal{F}(S_{i+1})$ or there exists a (unique) index $j \leq i$ with

$$\mathcal{F}(S_i) \subset S_j, \quad \mathcal{F}(S_{i+1}) \subset S_{j+1},$$

$$\mathcal{F}(S_{i+1}) \cap S_j = \mathcal{F}(S_i), \; S_j + \mathcal{F}(S_{i+1}) = S_{j+1},$$

(V) For every index $0 \leq i < m$ either $\mathcal{V}(S_i) = \mathcal{V}(S_{i+1})$ or there exists a (unique) index $j \leq i$ with

$$\mathcal{V}(S_i) \subset S_j, \quad \mathcal{V}(S_{i+1}) \subset S_{j+1},$$

$$\mathcal{V}(S_{i+1}) \cap S_j = \mathcal{V}(S_i), \; S_j + \mathcal{V}(S_{i+1}) = S_{j+1}.$$

The conditions (F) and (V) can be rephrased as:
for every index $0 \leq i < m$ either the map induced by $\mathcal{F}$ on S_{i+1}/S_i is zero, or there exists j and a bijective map

$$\mathcal{F} \bmod \mathcal{F}(S_i) : \frac{S_{i+1}}{S_i} \quad \xrightarrow{\sim} \quad \frac{S_{j+1}}{S_j}.$$

For every index $0 \leq i < m$ either the map induced by $\mathcal{V}$ on S_{i+1}/S_i is zero, or there exists j and a bijective map

$$\mathcal{V} \bmod \mathcal{V}(S_i) : \frac{S_{i+1}}{S_i} \quad \xrightarrow{\sim} \quad \frac{S_{j+1}}{S_j}.$$

(4.3) Construction. For a filtration S_* we use the following operations:

- $(F)(S_*)$: add all $S_i + (\mathcal{F}(S_j) \cap Si + 1)$ and $((F))(S_*) := (F)^{\gg 0}(S_*)$; analogous notation for $((V^{-1}))$, $((V))$, $((F^{-1}))$; each of these operations refines the previous filtration;
- $(V^{-1}\text{-}F)(S_*) := \left(((V^{-1}))((F))\right)^{\gg 0}(S_*)$; analogous notation for $(F^{-1}\text{-}V)(S_*)$.
- Start with $S^{(0)} = (0 \subset M)$. Define

$$S^{(2m+1)} = (V^{-1}\text{-}F)(S^{(2m)}), \quad S^{(2m+2)} = (F^{-1}\text{-}V)(S^{(2m+1)}).$$

- In $S^{(\gg 0)}$ renumber the steps in order to obtain a flag:

  $$Q_* = (0 = \subsetneqq Q_1 \subset Q_i \subsetneqq Q_{i+1} \subset Q_r = M),$$

  the *canonical filtration* of the module M. This is called the V^{-1}-F canonical filtration.

- As we start with $((F))(S_0)$, we see that all $A_t := F^tM$ appear as submodules in Q_*:

  $$0 = A_m := \mathcal{F}^m A \subsetneqq A_{m-1} \subset \cdots A_1 = \mathcal{F}M \subset A_0 := M.$$

- Remark: in general $\mathcal{V}^t A$ do not appear in this filtration and in general $\mathcal{F}^t A$ do not appear in the $(F^{-1} - V)$ canonical flag.

- Remark. For a BT$_1$-module it suffices to choose $(V^{-1}$-$F)(S_*)$ and obtain a saturated filtration; however if at least two different linear words appear this will not give a saturated filtration, and we extend the procedure as is described above.

(4.4) BB Proposition. *For any $M \in \mathcal{M}$ its canonical filtration $Q_* = Q(M)$ is* saturated.

5 Semilinear maps

(5.1) We work over a field $K \supset \mathbb{F}_p$. Let M be a vector space over a field K, and $q = p^e$. We say $\varphi : M \to M$ is a *q-semilinear map*, if it is a homomorphism of additive groups with moreover the property that

$$\varphi(a{\cdot}x) = a^q{\cdot}\varphi(x), \quad a \in K, \quad x \in M.$$

Understanding the theorem below it is useful to grasp the essence of the following exercises.

(5.2) Examples. Consider over any field K the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

(1) *There does not exist an invertible matrix S such that $S^{-1}AS$ is a diagonal matrix.*

Proof. The eigenvalues of A are equal to one. If $S^{-1}AS$ would be a diagonal matrix, this is

$$S^{-1}{\cdot}A{\cdot}S = \mathbf{1}_2; \quad \text{hence} \quad A = S{\cdot}\mathbf{1}_2{\cdot}S^{-1} = \mathbf{1}_2,$$

a contradiction.
(2) *With $K = k \supset \mathbb{F}_p$ algebraically closed, and q-semilinear map defined by A, i.e. $\varphi(1,0) = (1,1)$ and $\varphi(0,1) = (0,1)$, show that for every $\lambda \in k$ there exist $a, b \in k$ such that $\varphi(a,b) = \lambda(a,b)$.*
Proof. Indeed, choose any a with $a^{q-1} = \lambda$ and then b satisfying $b^q - \lambda b + \lambda a = 0$.
Exercise. *For A as above, show for any non-zero λ_1, λ_2 there exists*

$$S \in \mathrm{GL}(2,k) \text{ such that } S^{-1}AS^{(q)} = \mathrm{Diag}(\lambda_1, \lambda_2).$$

Below we will show a result generalizing this exercise; we see that "eigenvalues of q-semilinear map" is not a good concept.

Write $\mathrm{G} = \mathrm{GL}_d$ for the matrix group variety with $G = \mathrm{GL}(d,k) = \mathrm{GL}_d(k)$ the group of square $d \times d$ matrices over k with non-zero determinant.

(5.3) Theorem (Hasse-Witt, Lang-Steinberg). *Let $k = \overline{k} \supset \mathbb{F}_p$ be an algebraically closed field op characteristic p. Let $q = p^e$, and let $d \in \mathbb{Z}_{>0}$, and write $M = k^d$. For any $A \in G := \mathrm{GL}(d,k)$ there exists $T \in G$ such that*

$$T^{-1}AT^{(q)} = \mathbf{1}_d.$$

I.e. any q-semilinear endomorphism on a d-dimensional vector space over k can be written as diagonal matrix $\mathbf{1}_d$ after an appropriate choice of base.

References for the theorem: [11], § 3, Satz 10; [41], Theorem 10.1; [21].

For any X consider the morphism $f_X : \mathrm{G} \to \mathrm{G}$, with $\mathrm{G} = \mathrm{GL}_d$ given by $U \mapsto U^{-1}XU^{(g)}$.

Corollary. (1) *For $A, B \in G$ there exists $S \in G$ such that*

$$B = S^{-1}AS^{(q)}.$$

(2) *For every invertible $X \in G$ the morphism of algebraic varieties*

$$f_X : \mathrm{GL}_d \to \mathrm{GL}_d$$

is surjective on geometric points.
Proof. For given A and given B choose $T^{-1}AT^{(q)} = \mathbf{1}_d$ and $Z^{-1}BZ^{(q)} = \mathbf{1}_d$; write $S = TZ^{-1}$ and conclude $B = S^{-1}AS^{(q)}$. This proves (1).
For $B \in G$ and $X \in G$ we can choose S with $B = S^{-1}XS^{(q)}$, i.e. $f_X(S) = B$. This proves (2).

We give a **proof** of 5.3. For any X and any $U \in \mathrm{G}(k)$ consider the induced map on tangent spaces

$$(df_X)_U : \mathfrak{t}_{G,U} \to \mathfrak{t}_{G,f_X(U)}.$$

Note that the kernel of this tangential map is the same as the kernel of the tangential map at $U \in \mathrm{G}(k)$ defined by $U \mapsto U^{-1}X$; this last one is injective, hence $(df_X)_U$ is injective, hence an isomorphism. This shows that the morphism f_X has finite geometric fibers; as $\mathrm{G} = \mathrm{GL}_d$ is an irreducible variety this shows that $f_X(\mathrm{G}) \subset \mathrm{G}$ contains a Zariski-dense open subset for every X. We apply this with $X = A$ and with $X = \mathbf{1}_d$, proving

$$f_A(\mathrm{G})(k) \cap f_{\mathbf{1}_d}(\mathrm{G})(k) \neq \emptyset.$$

With γ in this intersection we have

$$Y^{-1}AY^{(q)} = \gamma = Z^{-1}\mathbf{1}_d Z^{(q)},$$

hence

$$T^{-1}AT^{(q)} = \mathbf{1}_d \quad \text{for} \quad T = YZ^{-1}.$$

This proves the theorem. □

6 C: Directed graphs

(6.1) Let $R_* = (R_0 \subsetneqq \cdots \subsetneqq R_r = M)$ be a *saturated flag* of $M \in \mathcal{M}$. We define a *directed graph* $\Gamma(R_*)$:
the set vertices is $\{0, \cdots, r-1\}$; this is the same as $\{R_{j+1}/R_j \mid 0 \leq j < r\}$; for any bijective map

$$\mathcal{F} : (R_{i+1}/R_i) \overset{\sim}{\to} (R_{j+1}/R_j) \text{ an edge is given by } i \mapsto j \text{ with label } F;$$

for any bijective map

$$\mathcal{V} : (R_{i+1}/R_i) \overset{\sim}{\to} (R_{j+1}/R_j) \text{ an edge is given by } i \hookleftarrow j \text{ with label } V.$$

Note the direction of the arrows: the last one could also better be baptized, or understood as V^{-1}.

(6.2) Proposition / Notation. *Let*

$$\Gamma_t \subset \Gamma = \Gamma(R_*), \quad 1 \leq t \leq g$$

be the connected components. All subquotients appearing in the same Γ_t *have the same dimension* d_t*. In this way* R_* *determines* $\{(\Gamma_t, d_t) \mid 1 \leq t \leq g\}$*.*

□

In this way R_* determines a set of words v_t with multiplicities d_t for every t with either v_t a linear or a circular word.

(6.3) The word determined by a connected directed graph. Note that any vertex in $\Gamma = \Gamma(R_*)$ has at most two ends of an edge connected to this vertex. Every edge is directed by F or (in the opposite direction) by V. This implies that a connected component $\Gamma_t \subset \Gamma$

either has a beginning, and an end, and the labels F and V give a linear word, which we denote by $u = \mathrm{word}(\Gamma_t)$,

or the graph Γ_t is circular, and the labels F and V give a word, which we denote by $w = \mathrm{word}(\Gamma_t)$.

(6.4) Proposition. *A saturated flag* R_* *determines its associated graded*

$$\mathcal{G}(R_*) := \sum_{1 \leq j < r} R_{j+1}/R_j.$$

The maps induced by $\mathcal{F}$ *and* $\mathcal{V}$ *on these subquotients give* $\mathcal{G}(R_*)$ *the structure of a Dieudonné module. We obtain an isomorphism*

$$\mathcal{G}(R_*) \quad \cong \quad \left(\oplus (M'_u)^{d_u}\right) \bigoplus \left((M_w)^{d_w}\right),$$

sums taken over al words in $\Gamma(R_*)$ *and their multiplicities.*

A *final filtration* $R_* = (R_0 \subsetneqq \cdots \subsetneqq R_r = M)$ is a saturated filtration where moreover all subquotients R_{j+1}/R_j have $\dim_k(R_{j+1}/R_j) = 1$.

(6.5) Proposition. *Any saturated filtration* R_* *can be refined to a final, saturated filtration* R'_* *. These two filtrations define the same sets of words and equal mutiplicities.*

Two saturated filtrations R_* *and* T_* *of* M *give the same sets of words with their multiplicities.*

Conclusion. *For* $M \in \mathcal{M}$ *any saturated filtration gives, up to isomorphism,*

the same decomposition as in (6.4).
Hence without risk for confusion, but up to isomorphism, we can write $\mathcal{G}(M)$.
Proof. Strategy:
(1) we choose an ordered k-basis for $\mathcal{G}(R_*)$ respecting $\sum_{1\leq j<r} \quad R_{j+1}/R_j$;
(2) this defines a final filtration of $\mathcal{G}(R_*)$ and it induces a final filtration R'_*;
(3) the final filtrations R'_* and T'_*, up to a permutation, have isomorphic subquotients.
(1) For a connected $\Gamma_t \subset \Gamma = \Gamma(Q_*)$ we know all submodules appearing in this word have the same dimension d_t.

If word$(\Gamma_t) = u = L_1 \cdots L_h$ is a linear word, consider the subquotient Q_{i+1}/Q_i given by the first position in the word (the beginning). Choose an ordered k-basis for Q_{i+1}/Q_i and using the bijections L_j in the saturated Q_* prolong this basis to all subquotients appearing in Γ_t; use this coherent set of bases in order to refine the filtration, adding steps in these subquotients. In this way we obtain a filtration by Dieudonné modules of $\mathcal{G}(R_*)$ with subquotients of dimension one in the subquotients appearing in Γ_t.

If word$(\Gamma_t) = w = L_1 \cdots L_h$ is a circular word consider the subquotient Q_{i+1}/Q_i given by the first position in this word; the sequence of p-semilinear bijections following the letters of of the word, give a p^h-semilinear bijection $\varphi : Q_{i+1}/Q_i \to Q_{i+1}/Q_i$. By (5.3), note that we work over an algebraically closed field, we can choose a basis on which φ is the identity matrix; use this ordered basis to chose a refinement of all subquotients appearing in Γ_t. We obtain a filtration by Dieudonné modules of $\mathcal{G}(R_*)$ with subquotients of dimension one in the subquotients appearing in Γ_t.

(2) In this way we obtain a final flag $\mathcal{G}(R_*)$ and it induces a final flag R'_* of M refining R_*. The connected graph $\Gamma_t \subset \Gamma(R_*)$ with subquotients of dimension d_t gives d_t connected graphs $\Gamma_{t,s} \subset \Gamma(R_*)$, with $1 \leq s \leq d_t$ and word$(\Gamma_t) =$ word$(\Gamma_{t,s})$. We see that R_* and R'_* give the same decomposition, as in (6.4), of $\mathcal{G}(R_*)$, i.e.

$$\mathcal{G}(R_*) \quad \cong \quad \mathcal{G}(R'_*).$$

(3) Choose refinements to final filtrations R'_* and T'_*. For every R'_{i+1}/R'_i, choose any $x_i \in R'_{i+1}\backslash R'_i$, there is a unique $j = f(i)$ such that $x_i \in T'_{j+1}\backslash T'_j$. The action of $\mathcal{F}$ and of $\mathcal{V}$ coincide on $R'_{i+1} \setminus R'_i$ and $T'_{j+1} \setminus T'_j$ modulo this permutation. This shows

$$\mathcal{G}(R_*) \quad \cong \quad \mathcal{G}(R'_*) \quad \cong \quad \mathcal{G}(T'_*) \quad \cong \quad \mathcal{G}(T_*) \overset{\text{and we write}}{=} \mathcal{G}(M).$$

□ 6.4 + 6.5

Warning/comment. We find a $\mathcal{F}$-stable and $\mathcal{V}$-stable basis of $\Gamma(Q_*)$, resulting in a final filtration on the associated graded Dieudonné module $\mathcal{G}(M)$. However we did not yet prove the existence of a $\mathcal{F}$-stable and $\mathcal{V}$-stable basis on the Dieudonné module M; this is the crucial problem in our proof; that will be done in Section 8.

For later use we observe:

(6.6) Lemma. *Suppose $P', P'' \in \mathcal{M}$. Then*

$$\Gamma(Q_*)(P' \oplus P'') = \Gamma(Q_*)(P') \sqcup \Gamma(Q_*)(P'')$$

and

$$\mathcal{G}(Q_*)(P' \oplus P'')) = \mathcal{G}(Q_*)(P') \oplus \mathcal{G}(Q_*)(P'').$$

Proof. Exercise.

7 D: Indecomposable modules

(7.1) Proposition. *For every linear word the module M'_u is indecomposable.*
For every indecomposable circular word w the module M_w is indecomposable.
Proof. Suppose the length of u is h. Choose a final filtration S_* of M'_u. For every base vector z_j there is unique index i with $z_j \in S_{i+1} \setminus S_i$: if there would be $z_j, z_{j'} \in S_{i+1} \setminus S_i$, with $j < j'$ follow the rest of the word u for both, after $h - j' + 1$ steps the word ends after j' and does not end after j, a contradiction. Hence, any step $S_i \subset M$ contains exactly i of the elements $\{z_1, \cdots, z_{h+1}\}$. This proves that any two of the subquotients of S_* are connected by a path in $\Gamma = \Gamma(S_*)$; this proves that Γ is connected. Note that Γ is independent of the choosen filtration, only depends on M'_u. If we would have $M'_u = P' \oplus P''$ with non-zero summands, than we would have $\Gamma = \Gamma(P') \sqcup \Gamma(P'')$, see (6.6), a non-connected graph. This contradiction shows M'_u is indecomposable.

Suppose $w = [L_1 \cdots L_h]$ is an *indecomposable word*. Because the word w is indecomposable, for any pair $1 \leq j < j' \leq h$ the shift $+(j' - j)$ does not map $\{L_i \mid i \in \mathbb{Z}\}$ to itself. From here repeat the arguments in the previous paragraph, showing M_w is indecomposable. □

Remark. For small words u and w easier proofs exist; for the general situation we use filtrations in order to give a proof for (7.1). Probably a more direct (and also more involved) proof for (7.1) exists.

We still have not shown there are no other indecomposable modules in $\mathcal{M}$.

8 E: A choice of a lifting $M \overset{\sim}{\longleftarrow} \mathcal{G}(M)$, end of the proof.

(8.1) Theorem, BB. *For every $M \in \mathcal{M}$ and any saturated filtration S_* of M that contain all $\mathcal{F}^j M$ as steps we can* choose *an isomorphism of* D-*modules*

$$M \quad \overset{\Phi}{\underset{}{\overset{\sim}{\longleftarrow}}} \quad \mathcal{G}(S_*)$$

such that

for every $S_{i+1} \to S_{i+1}/S_i$ this induces a section $S_{i+1} \quad \overset{\Phi_i}{\longleftarrow} \quad S_{i+1}/S_i$,

and Φ is given by these sections.

Remark. In general Φ is not unique: for a non-zero BT_1-module M with $\mathcal{F}$ and $\mathcal{V}$ nilpotent, there are several different choices for Φ possible.

A proof of (8.1) for BT_1-modules is given in [18]. A new proof of this fact, included in a proof in the general case, will appear in [3].

(8.2) We mention (without proof) steps that together imply Theorem (8.1). Assume S_* is a final (saturated) filtration of M which moreover contains $V^j(M)$ as a step for every $j \geq 0$. Let

$$\Gamma(S_*) = \sqcup_j \ \Gamma_j$$

be the *connected components* of the associated graph. We can show the following facts:

- If $u_j = \mathrm{word}(\Gamma_j)$ is a linear word, the steps in the connected graph Γ_j can be lifted to an inclusion
$$\mathcal{G}(M) \supset M'_{u_j} \hookrightarrow M.$$
- If $w_j = \mathrm{word}(\Gamma_j)$ is a circular word such that Γ_j contains the lowest step $0 = S_0 \subset S_1$ the steps in the connected graph Γ_j can be lifted to an inclusion
$$\mathcal{G}(M) \supset M_{w_j} \hookrightarrow M.$$

- Suppose $\Gamma = \Gamma_1 \sqcup \Gamma_2$ has two connected components; this implies $\mathcal{G}(M) \cong P' \oplus P''$ with $\Gamma(P') = \Gamma_1$ and $\Gamma_2 = \Gamma(P'')$; suppose there is an exact sequence

$$0 \to P' \longrightarrow M \longrightarrow P'' \to 0$$

  such that $P' \hookrightarrow M$ gives $\Gamma(P') = \Gamma_1$ and $M \twoheadrightarrow P''$ gives $\Gamma_=\Gamma(P'')$; then the extension $M/P' = P''$ is split exact.

- Rephrased. In general an extension $M/P' = P''$ is non-split; however if $P' \subset M$ and $M \to P''$

$$\text{give the decomposition } \Gamma(M) = \Gamma(P') \sqcup \Gamma(P'')$$

  then the extension $M/P' = P''$ is split.

- Easy exercise. Assume these facts are proved. Conclude a proof for Theorem (8.1).

This ends a proof of:

(8.3) Theorem. *Any finitely generated module M over the ring $k\{\mathcal{F}, \mathcal{V}\}$ can be written as:*

$$M \quad \overset{\sim}{\longleftarrow} \quad \mathcal{G}(M) \quad \cong \quad \left(\oplus_{i \in L} \quad M'_{u_i}\right) \bigoplus \left(\oplus_{j \in C} \quad M_{\lfloor w_j \rceil}\right),$$

where L is a finite set of linear words and C is a finite a set of indecomposable circular words.

(8.4) Corollary. *Let k be an algebraically closed field of characteristic p. For any $n \in \mathbb{Z}_{>0}$ the set of k-isomorphism classes of finite commutative group schemes of rank p^n annihilated by p is* finite.

9 Some exercises

Convention for the exercises: a prime number p is fixed. We work over a field $k = \overline{k} \supset \mathbb{F}_p$. Write $\mathcal{M}$ for the category of modules over $k\{\mathcal{F}, \mathcal{V}\}$ of finite length, i.e. of finite dimension over k. In this category

$$\text{Image}(\mathcal{V} : M \to M) =: \mathcal{V}M \subset M[\mathcal{F}] := \text{Ker}(\mathcal{F} : M \to M),$$

and

$$\mathcal{F}M \subset M[\mathcal{V}].$$

We use notation M'_u and M_w as explained in the course.
We use BT_1 to indicate a Barsotti-Tate module truncated at level one, i.e. $M \in \mathcal{M}$ with

$$\mathcal{V}M = M[\mathcal{F}]; \quad \text{equivalently} \quad \mathcal{F}M = M[\mathcal{V}];$$

$\mathcal{M}^{\mathrm{BT}}$ is the category of BT_1-modules in $\mathcal{M}$.
We use × for a product of vector spaces, and $\oplus$ for a direct sum of Dieudonné modules.

(1.a) Describe all isomorphism classes of $M \in \mathcal{M}$ of dimension 2 in which $\mathcal{F}$ and $\mathcal{V}$ are nilpotent.
(1.b) Show that $\mathrm{Ext}(M_{\mathcal{F}\mathcal{V}}, M_{\mathcal{F}\mathcal{V}})$ is not finite. Explain that this does not contradict the (finiteness) result obtained in the previous line.

(2.a) Give a morphism $\varphi : Q' \to Q''$ in $\mathcal{M}^{\mathrm{BT}}$ such that $\mathrm{Ker}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are not in $\mathcal{M}^{\mathrm{BT}}$.
E.g. $Q' = M_{\mathcal{F}\mathcal{V}} = Q''$ and $Q' = ke \times k\mathcal{F}e$, and $Q'' = kh \times k\mathcal{F}h$ and $\varphi(e) = \mathcal{F}h$. This gives an exact sequence

$$0 \to M'_{\emptyset} \to Q' = M_{\mathcal{F}\mathcal{V}} \to M_{\mathcal{F}\mathcal{V}} = Q'' \to M'_{\emptyset} \to 0$$

(2.b) Give linear words u_1, and u_2 and a morphism $\varphi : M'_{u_1} \to M'_{u_2}$ such that $\mathrm{Ker}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are in $\mathcal{M}^{\mathrm{BT}}$.

Conclusion. The subcategory $\mathcal{M}^{\mathrm{BT}} \subset \mathcal{M}$ and the subcategory generated by all M'_u are clearly defined; however any $M \in \mathcal{M}$ in general decomposes into summands in these subcategories in many ways. Kernels and cokernels in these subcategories do not exist in general in that subcategory. Extensions in many cases do take us out of these subcategories. In order to prove the theorem announced by Kraft we have to do a lot of work.

(3) Consider $M := M'_{\emptyset} \oplus M'_{\mathcal{F}}$.
(3.a) Apply the process of taking "all $\mathcal{F}$ images, all $\mathcal{V}^{-1}$ images", that is, apply $(V^{-1}\text{-}F)$. Show the filtration $(V^{-1}\text{-}F)(0 \subset M)$ obtained is not saturated.
(3.b) Apply the process of taking "all $\mathcal{V}$ images, all $\mathcal{F}^{-1}$ images", that

is, apply $(F^{-1}\text{-}V)$. Show the filtration $(F^{-1}\text{-}V)(0 \subset M)$ obtained is not saturated.

Remark. For a BT_1 module the operation $(V^{-1}\text{-}F))$ and also the operation $(F^{-1}\text{-}V))$ produces a saturated filtration.The exercise shows that for an arbitrary $M \in \mathcal{M}$ this need not be the case, we really need both processes (applied several times).

Question. Is this true? Check. Let u_1 and u_2 be different linear words; for any set of words $u_1, u_2, \cdots, u_r$ with $r \geq 2$ and $M := \oplus_{1 \leq j \leq r} \ M'_{u_j}$ the filtrations $(V^{-1}\text{-}F)(0 \subset M)$ and $(F^{-1}\text{-}V)(0 \subset M)$ are not saturated.

Question. Is this true? Check. For a linear word u and $M = M'_u$ the filtrations $(V^{-1}\text{-}F)(0 \subset M)$ and $(F^{-1}\text{-}V)(0 \subset M)$ are saturated.

(4) Consider over $K = k \supset \mathbb{F}_p$ algebraically closed and for $q = p^e$ define a q-semilinear map given by the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Show for any non-zero λ_1, λ_2 there exists

$$S \in \mathrm{GL}(2,k) \ \textit{such that} \ S^{-1}AS^{(q)} = \mathrm{Diag}(\lambda_1, \lambda_2).$$

(5) Suppose $M/P' = P''$ is an extension in $\mathcal{M}$ such that $P', P'' \in \mathcal{M}^{\mathrm{BT}}$. Show this implies $M \in \mathcal{M}^{\mathrm{BT}}$.

(6) Find an extension $M/P' = P''$ with the properties:
this extension is non-split,
P' and P'' are indecomposable, and
M is decomposable.

Conclusion. You might be tempted to give a "cheap" proof of the theorem announced by Kraft: apply induction on the number of indecomposable summands, and consider extensions. The exercise shows this methods does not work directly. In our proof we follow this road, with the refinement that using directed graphs, we can recognise which extensions are possible.

We show that an extension $M/P' = P''$ with $\Gamma(M) = \Gamma(P') \sqcup \Gamma(P'')$ and equality induced by $P' \hookrightarrow M$ and $M \twoheadrightarrow P''$ implies that $M \cong P' \oplus P''$.

(7) Show $M'_{\mathcal{VF}}$ cannot be embedded into $M'_{\mathcal{VVFF}}$.

(8 Find all $M_{\mathcal{FV}} \hookrightarrow M'_{\mathcal{VFFV}}$.

(9) Choose $u = \mathcal{VFFVF}$; show $P := M'_u$ is indecomposable.

Remark. It is quite likely that arguments as used in the previous exercise can be used to show any M'_u is indecomposable, and for any indecomposable w, the module M_w is indecomposable.
Problem. Find a direct proof (not using the canonical filtration) for the fact that M'_u is indecomposable for every linear words u and M_w is indecomposable for every indecomposable circular word.

10 Some examples

(10.1) We have assumed in Corollary 1.1 and in Theorem (8.3) that

(1) we work over an *algebraically closed ground field*,

and

(2) that we consider *commutative* group schemes

and

(3) moreover we consider group schemes *annihilated by p*.

We give examples that show these conditions are essential for the classification and finiteness result described in this section. Work over a field $K \supset \mathbb{F}_p$.

(a), (2+3) satisfied. For $K = k(T)$, using notation as in (19.2), see [43]), consider for every $t \in k$ the group scheme $N^{(t)} = G_{T-t,0}$. We know

$$N^{(t)} \cong N^{(s)} \quad \Longleftrightarrow \quad \exists u \in K^* : \quad u^{p-1} \cdot (T-t) = T-s.$$

Assume $p > 2$. We can write $u = A(T)/B(T)$ with coprime $A, B \in k[T]$. Then

$$A^{p-1}(T-t) = B^{p-1}(T-s).$$

Assume $s \neq t$; then we would conclude $T-s$ divides A, and $(T-s)^2$ divides $B^{p-1}(T-s)$, a contradiction.

Conclusion. For $p > 2$ there are *infinitely many isomorphism* classes of group schemes of rank p over $K = k(T)$. Conditions (2) and (3) are satisfied.
Variant. For $K^{(\text{insep})} = \cup_j \;\; k(\sqrt[p^j]{T})$, the inseparable closure of $K = k(T)$ the same conclusion holds.
Variant. For $K^{(\text{sep})}$, the separable closure of $K = k(T)$, there are finitely many isomorphism classes of group schemes of rank p over $K^{(\text{sep})}$.

(b), (1+2) satisfied. **Group schemes not annihilated by p.** Consider over k and $x \in k^*$ the Dieudonné module $M^{(x)}$ with generators e, h, g and $x \in k$ and relations

$$p{\cdot}e = 0, \mathcal{V}(e) = \mathcal{F}^2(e), \quad p{\cdot}g = 0, \mathcal{V}^2(g) = \mathcal{F}(g), \quad \mathcal{V}(h) = e, \quad \mathcal{F}^2(h) = x{\cdot}g.$$

We see:

- e generates $M_{\lfloor \mathcal{V}\mathcal{F}\mathcal{F} \rceil}$, and g generates $M_{\lfloor \mathcal{V}\mathcal{V}\mathcal{F} \rceil}$,
- $M^{(x)}/M^{(x)}[\mathcal{F}^2]$ has $\{e, h\}$ as k-basis,
- $M^{(x)}/M^{(x)}[\mathcal{V}^2]$ has $\{g, h\}$ as k-basis,
- $M^{(x)}/M^{(x)}[p]$ has $\{h\}$ as k-basis, (in particular M is not annihilated by p).

Suppose $x, y \in k$ and consider an isomorphism $\varphi : M^{(x)} \to M^{(y)}$. Then there are $b, c, d \in k^*$ such that

$$\varphi(e) \equiv b{\cdot}e \pmod{M^{(x)}[\mathcal{F}^2]}, \; \varphi(g) \equiv d{\cdot}g \pmod{M^{(x)}[\mathcal{V}^2]}, \; \varphi(h) \equiv c{\cdot}h \pmod{M^{(x)}[p]},$$

and we see $b, c, d, x/y \in \mathbb{F}_{p^3}$. We conclude:
over k algebraically closed of characteristic p there are infinitely many isomorphism classes of finite commutative group schemes of rank p^7 annihilated by p^2.
Conditions (1) and (2) are satisfied. Another example can be given for rank p^5.

(c), (2+3) satisfied; $\mathrm{Ext}(\underline{\mathbb{Z}/p}, \mu_p)$ **over a non-perfect field. Group schemes of order p^2.**
Let $K = k(T)$, and let $N^{(a)}$ be an extension in the exact sequence

$$0 \to \mu_p \longrightarrow N^{(a)} \longrightarrow \underline{\mathbb{Z}/p} \to 0 \quad \text{(a)}.$$

By [17], page 391 we know

$$\mathrm{Ext}^1_K(\underline{\mathbb{Z}/p}, \mu_p) \cong K^*/(K^*)^p.$$

For any $t \in k$, we see

$$((T-t) \bmod (K^*)^p) \in K^*/(K^*)^p$$

is non-trivial (of order p), hence for any $p \geq 2$ the group $K^*/(K^*)^p$ is infinite. Moreover $\mathrm{Aut}(\underline{\mathbb{Z}/p})$ and $\mathrm{Aut}(\mu_p)$ are finite. The sequence (a) is split exact over an algebraic closure of K, hence $N^{(a)}$ is annihilated by p. The set of K-isomorphism classes of group schemes $N^{(a)}$ is infinite over the non-perfect field K, while conditions (2) and (3) are satisfied.

(d), Heisenberg groups. (Sometimes people wonder whether every (abstract) group G with exponent p is commutative; for a group G its exponent is defined as the smallest n such that $x^n = e$ for every $g \in G$; the exponent of G is the least common multiple of all orders of elements in G.)
Easy exercise. A group with exponent $p = 2$ is commutative. Indeed, $(xy)(xy) = e, \quad x^2 = e, \quad y^2 = e$ imply $xy = yx$.
As a corollary we see that *any finite group scheme* (over any base) *annihilated by* $p = 2$ *is commutative.*
However for odd prime numbers the situation is different.

Construction of UT(3,p). Let $p > 2$ be prime number and G be the group generated by x and y with

$$z := x^{-1}y^{-1}xy, \quad xz = zx, \quad yz = zy, \quad x^p = y^p = z^p = e.$$

We see $xy = yxz$, the subgroups $< x, z >$ and $< y, z >$ are normal in G, every element can be written in a unique way as $x^u y^v z^w$, with $0 \leq u, v, w < p$, we have

$$G \quad \cong \quad < x, z > \rtimes < y > \quad \cong \quad < y, z > \rtimes < x >,$$

the order of G equals p^3 and G is *not commutative.*

Claim. The UT(3,p) group G with $p > 2$ is annihilated by p.
Proof. For $p > 2$ we see $1 + 2 + \cdots + (p-1) = p{\cdot}((p-1)/2)$.
Using $xz = zx$ and $yz = zy$ and $xy = yxz$ we see:

$$(x^u y^v z^w)^p = x^{pu} y^{pv} z^{u(1+2+\cdots+(p-1))} z^{pw} = e.$$

□

`https://math.stackexchange.com/questions/3684342/a-p-group-of-exponent-p`
`https://groupprops.subwiki.org/wiki/Unitriangular_matrix_group:UT(3,p)#As_a_semidirect_product`

Hence *for any $p > 2$ there are group schemes annihilated by p that are not commutative*, e.g. the constant group scheme $\underline{UT(3,p)}$.

Inspired by the Heisenberg construction over $K \supset \mathbb{F}_p$ with $p > 2$ we define a non-commutative local group scheme by its Hopf-algebra:

$$E = K[\xi, \eta, \zeta]/(\xi^p, \eta^p, \zeta^p),$$

$$s\xi = \xi \otimes 1 + 1 \otimes \xi, \quad s\eta = \eta \otimes 1 + 1 \otimes \eta, \quad s\zeta = \zeta \otimes 1 + 1 \otimes \zeta + \xi \otimes \eta.$$

This idea can be generalized in the following way.

(e), Heisenberg group schemes, (1+3) satisfied.
Claim. *For any $p > 2$ and $k = \overline{k} \supset \mathbb{F}_p$ there exists a number p^n such there are* infinitely many *isomorphism classes of (non-commutative) finite group schemes over k annihilated by p of rank p^n.* Conditions (1) and (3) are satisfied

Example. Fix $p > 2$ and $k = \overline{k} \supset \mathbb{F}_p$. Choose group schemes X, Y, Z defined by

$$\mathbb{D}(X) = M_{\lfloor \mathcal{F}\mathcal{F}\mathcal{V} \rceil}, \ \ \mathbb{D}(Y) = M_{\lfloor \mathcal{F}\mathcal{V}\mathcal{V} \rceil}, \ \ \mathbb{D}(Z) = M_{\lfloor \mathcal{F}\mathcal{V} \rceil}$$

(group laws written multiplicatively), commutative and annihilated by p. For any $\lambda \in k^*$ we define a group scheme $N^{(\lambda)}$ over k:

- start with $\psi_\lambda = \psi : X \to Z$ given by $\psi(e) = \lambda \cdot \mathcal{F}(h)$ for a generator e of $M_{\lfloor \mathcal{F}\mathcal{F}\mathcal{V} \rceil}$ and a generator h of $M_{\lfloor \mathcal{F}\mathcal{V} \rceil}$;
- define $\varphi : X \to \underline{\mathrm{Aut}}(Y \times Z)$ given by the matrix

$$\varphi_\lambda = \varphi = \begin{pmatrix} id & \psi \\ 0 & id \end{pmatrix};$$

- define

$$N^{(\lambda)} = (Y \times Z) \rtimes_\varphi X.$$

With these definitions the following facts are easily proved.

- The group scheme $N^{(\lambda)}$ is non-commutative and annihilated by p. Indeed, for any k-scheme T and $x \in X(T)$, $y \in Y(T)$, $z \in Z(T)$, we have $xy = yx\psi(x)$, $xz = zx$ and $yz = zy$ and, using $p > 2$, we see
$$(yxz)^p = y^p x^p \psi(x)^{1+\cdots+(p-1)} z^p = 1.$$
- For any $\lambda, \delta \in k^*$,
$$\frac{\lambda}{\delta} \notin \mathbb{F}_{p^6} \quad \Longrightarrow \quad N^{(\lambda)} \ncong N^{(\delta)}.$$

This proves the claim. □

More details about semidirect products can be found in 19.5.

– –

II Is a finite group scheme annihilated by its rank?

11 Introduction. We take a group scheme $G \to S$ of finite presentation and locally free over a base scheme S of constant rank $m = \mathrm{rank}(G/S)$. We ask whether

$$\big([m]_{G/S} : G \to G\big) \quad \overset{?}{=} \quad \Big(G \to S \xrightarrow{e} G\Big).$$

If this is the case, we say G/S is annihilated by its rank.
See [6], Exp. VIII, 7.3.1, see [43], page 5.

In case we write $\mathrm{rank}(G/S)$ we are assuming that $G \to S$ of finite presentation and locally free of this rank. We use the word *order* for the cardinality $\#(H)$ of a finite abstract group, and *rank* as indicated for finite group schemes; if the base ring is local "locally free" for a module is the same as free.

Notation. For a group scheme $G = \mathrm{Spf}(E)$ over a ring R and a positive integer r we write $[r] : G \to G$ and also $[r] : E \to E$ for the morphis/homomorphism given by $x \mapsto x^r$ on all $x \in G(R')$. This amounts to:

$$[r] = \Big(E \xrightarrow{s_r} E^{\otimes r} \overset{\mathrm{mult}}{\longrightarrow} E\Big).$$

We can cover S by affine scheme, and we see the question can be translated into the following. Suppose R is a base ring (commutative with $1 \in R$), let E be an R-Hopf-algebra, of finite presentation, flat of constant rank m. We ask whether

$$[m] : \Big(E \xrightarrow{s_m} E^{\otimes m} \overset{\mathrm{mult}}{\longrightarrow} E\Big) \quad \overset{?}{=} \quad \Big(E \xrightarrow{\varphi} E/I_E = R \to E\Big).$$

In this case we say the Hopf-algebra is annihilated by its rank.

We will see that at present an answer to this question in the general situation is not known. This part of this note is not well-organized, may contain mistakes or misleading arguments.

Convention. Saying that G is a finite group scheme over R we assume G is of finite presentation and locally free of constant rank over a base ring R, unless otherwise mentioned.

Obvious observation / Exercise. Suppose G is a finite flat group scheme over a ring R_1; let $R_1 \hookrightarrow R_2$ be an inclusion of rings, and suppose $G \otimes_{R_1} R_2$ is annihilated by its rank. Then G/R_1 is annihilated by its rank.

We recall some basic facts, used below.

(11.1) *Suppose $K \supset \mathbb{F}_p$ is a* perfect *field, and E is a local K-Hopf-algebra. Then there exist integers $n_1, \cdots, n_d$ and an isomorphism of K-algebras*

$$E \cong_K \; K[\tau_1, \cdots, \tau_d]/(\tau_1^{p^{n_1}}, \cdots, \tau_d^{p^{n_d}}).$$

See [44], 14.4, Theorem.

Example. If $K \supset \mathbb{F}_p$ is a non-perfect field, $a \in K$ with $\sqrt[p]{a} \notin K$,

$$E := K[X,Y]/(X^{p^2}, X^p = aY^p) \quad \text{defines} \quad G := \mathrm{Spf}(E) \subset (\mathbb{G}_a)^2,$$

a subgroup scheme of rank p^3, and E is not of the form described in the previous result.

(11.2) *Suppose G is a group scheme, locally of finite type over a field K. The identity component G^0 is an open and closed subgroup scheme, and for any field extension $K \subset L$ we have $G^0 \otimes_K L = (G \otimes_K L)^0$.*

(11.3) *Suppose G is a finite group scheme over a field K. The identity component G^0 is a normal subgroup scheme, we have an exact sequence*

$$e \to G^0 \longrightarrow G \longrightarrow G^{\mathrm{et}} \to e,$$

and $G \to G^{\mathrm{et}}$ is the largest etale quotient of G.

(11.4) *Suppose G/S is a finite group scheme of finite presentation and locally free over a base scheme S of constant rank $m = \mathrm{rank}(G/S)$. Suppose the integer m is invertible in all local rings of S.Then $G \to S$ is etale.*

(11.5) *Let G be a locally algebraic group scheme over a field K. The center of G is a closed subgroup scheme of G.*
See [40], 39.8 for a definition of the center of a group scheme, and for a proof of this fact.

Example. An abstract finite non-trivial p-group has a non-trivial center. The analogous statements is not true for finite group schemes. The non-split group scheme $G = \alpha_p \rtimes \mu_p$, to be studied below, see (15.1), has rank p^2, is non-commutative, and its center is trivial.

(11.6) *Let G be a finite flat group scheme over a base scheme S and let $G_1 \subset G$ be a normal subgroup scheme flat over S. Then the (categorical) cokernel $G_2 = \mathrm{Coker}(G_1 \to G)$ exists. In case G and G_1 are of constant rank over S, then* $\mathrm{rank}(G) = \mathrm{rank}(G_1) \times \mathrm{rank}(G_2)$.

For further information and for proofs, the reader can consult [24], [6], [43], [42], [37], [36], [32], [35], [44], [22].

12 Known cases

(12.1) Proposition (Edixhoven). *Let A be a finite flat R-Hopf-algebra, with augmentation ideal $I \subset A$. Let p be a prime number. In this case*

$$[p](I) = pI + I^p.$$

For the elegant proof, see [37], Proposition 2.1, [39], Proposition 2.1. From this one concludes:

(12.2) Over a field. Theorem. *Suppose E is a Hopf-algebra over a field $R = K$. In this case E is annihilated by its rank.*
See [37], Corollary 2.2, [39], Corollary 2.2. See [6], VII_A.8.5

We conclude that *any group scheme finite and flat over an integral domain is annihilated by its rank.*

(12.3) Commutative finite group schemes.
Theorem (Deligne, 1970). *Any* commutative *group scheme of finite presentation is annihilated by its rank.*
Comment. In general we can try to transplant a proof in the theory of groups to the theory of group schemes.
Suppose H is a finite *commutative* abstract group; in this case we can prove Lagrange's theorem as follows: for any $y \in H$ with $\#(H) = m$ we have

$$(\prod_{z \in H} z) = \prod_{x \in H} (yx) \overset{*}{=} y^m \times (\prod_{x \in H} x); \quad \text{hence} \quad y^m = e;$$

The equality $\overset{*}{=}$ uses the fact that H is commutative. Deligne had the insight how to formulate this proof "without using elements". For details see [43], Theorem on page 4.

(12.4) Etale group schemes. We observe (a theorem by Larange) that an element in a finite abstract group H has order dividing the order of H. Hence

Theorem. *Any etale group scheme $G \to S$ is annihilated by its rank.*
Indeed, first assume S is connected. We can cover S by affine schemes S_i such that for any $S_i = \mathrm{Spf}(R_i)$ there is an etale cover $\mathrm{Spf}(R'_i) = S'_i \to S_i$ and a finite abstract group H or order equal to $\mathrm{rank}(G/S)$ such that we have $G \otimes R'_i = \underline{H}_{R'_i}$, a constant group scheme, and the Lagrange theorem implies $G \otimes R'_i$, hence G/S is annihilated by its rank.

(12.5) Corollary. *Suppose the integer* $\mathrm{rank}(G/S)$ *is invertible in all local rings of S. Then G/S etale and G/S is annihilated by its rank.*

(12.6) Small artin rings
Theorem (Schoof, 2001), see [37], Theorem 1.1. *Let R be a local artin ring, with maximal ideal $\mathfrak{m} = \mathfrak{m}_R$, and $\mathfrak{m}^p = 0 = p\mathfrak{m}$ and $R/\mathfrak{m} \supset \mathbb{F}_p$. Any finite flat group scheme over R is annihilated by its rank.*

As far as I know these are all known general cases where "annihilated by rank" has been proved.

13 Reduction of the problem

(13.1) Problem. *Let p be a prime number, R a local artin ring, with maximal ideal $\mathfrak{m} = \mathfrak{m}_R$ and algebraically closed residua class field $R/\mathfrak{m} = k \supset \mathbb{F}_p$. Let n be a positive integer. Is every finite flat local R-Hopf-algebra of rank p^n annihilated by its rank?*

Suppose the answer to (13.1) is affirmative. Then it follows that any group scheme $G \to S$ of finite presentation and locally free over a base scheme S of constant rank is annihilated by its rank. We leave this as an exercise to the reader. You can also consult [39], Section 1.

14 Lifting and deformation problems

(14.1) In general deformation problems in algebraic geometry e.g. we already find in a paper by Kodaira and Spencer in 1985; later in the theory of schemes many theoretical results were described by Schlessinger (1986), Grothendieck and many others.

In many cases we can accurately describe a deformation problem in case of a "small surjection" $R \to R'$ of local artin rings; this means a surjective homomorphism φ with $\mathrm{Ker}(\varphi){\cdot}\mathfrak{M}_R = 0$. In case the deformation problem is unobstructed (for example for algebraic curves, for principally polarized abelian varieties) this theory provides us with satisfactory answers.

If a deformation problem is obstructed in a given infinitesimal step, it seems hard in general to obtain final answers to lifting problems. For abelian schemes this was circumvented by Mumford by his theory of "displays", later generalized by Zink in his theory of "windows".

We start with examples for finite group schemes.

(14.2) (1) For $K \supset \mathbb{F}_p$, and a local ring $R \to K$ with $0 \neq p{\cdot}1 \in \mathfrak{m}_R$, and $p{\cdot}1 \notin \mathfrak{m}_R^2$ we see that $\alpha_{p,K}$ cannot be lifted to R. If you would not know the structure of all group schemes of rank p this obstructed situation would seem mysterious.

(2) Let $K \supset \mathbb{F}_p$, and $R' = K[\varepsilon]/(\varepsilon^2)$ and $H' = G_{\varepsilon,\varepsilon}$ in the notation of (19.1). Let $R \to R'$ be a ringhomomorphism with $\mathbb{F}_p \subset R$.In this case H' cannot be lifted to R.

There are many examples of H'/R' and an integral domain R and $R \to R'$ where H' cannot be lifted to R.

(3) Let $G_0 = \alpha_p \rtimes \mu_p$ be a non-split (non-commutative) group scheme over a field K of characteristic p, see (15.1). Let R be a characteristic zero domain with $R \to K$. The group scheme G_0/K cannot be lifted to R (as there does not exist a non-commutative abstract group of order p^2). More difficult, and in fact more interesting:

(4) Let $G_0 = \alpha_p \rtimes \mu_p$ be a non-split (non-commutative) group scheme over a field K of characteristic p, see (15.1) and let R be a local artin ring, $R \to K$

with $0 \neq p{\cdot}1 \in R$. In this case G_0 cannot be lifted to $R \to K$; see [37], Proposition 3.3.

Do there exist group schemes of rank p^2 over a ring R with $0 \neq p{\cdot}1 \in R$? Although the previous examples seems to suggest the answer should be negative, we will give many examples, see 19.6.

We see that there exist a non-commutative finite group scheme that cannot be lifted to characteristic zero. However for commutative group schemes the situation is different:

(14.3) Theorem (Mumford-FO). *A finite* commutative *group scheme N_0 over a field k can be lifted to characteristic zero.* See [29].

Comment. We know in general the lifting situation can be obstructed, e.g. see (14.2.1). In the situation of (14.3) a method was developed bypassing this difficulty: first deform the situation characteristic p to a "better situation", and then lift. This method was successful for commutative group schemes, later it was used for a proof of the "Grothendieck conjecture" and for the (obstructed) situation of lifting an algebraic curve with an automorphism. For a description of this method and for references where this was used see [31].

Suppose we wold know that any G_0 over a local artin ring R' could be lifted to an integral domain $R \to R'$ that would solve the "annihilated by rank" problem. We know however many situations where a lift to an integral domain does not exist.

Do we know any method analogous to this that can be of help for the problem "annihilated by rank"? We do have an extensive theory of obstruction calculus and deformation theory of finite group schemes, however up to now I have not been able to successfully applying this theory tot the problem studied.

(14.4) Obstruction calculus. For a small surjection of artin rings and for finite for group schemes the following references give full solutions to these questions: [12], [13], [14].

15 Group schemes of rank p^2

(15.1) In [43], on pages 6/7 we see a non-commutative group scheme over any characteristic p ring $R \supset \mathbb{F}_p$. An easy way to remember the construction is:

$$\mathcal{T} = \begin{pmatrix} \mu_p & \alpha_p \\ 0 & 1 \end{pmatrix}.$$

This group scheme $\mathcal{T}$ has the following properties:

- rank$(\mathcal{T}) = p^2$ and $\mathcal{T}$ is non-commutative;
- $\mathcal{T} = \mathrm{Spf}(R[\rho, \sigma]/(\rho^p - 1, \sigma^p))$, the comultiplication is given by

  $$s(\rho) = \rho \otimes \rho, \quad s(\sigma) = \rho \otimes \sigma + \sigma \otimes 1,$$

  the augmentation is given by $\rho \mapsto 1$, $\sigma \mapsto 0$,
  and the coinverse is given by $\rho \mapsto 1/\rho$, $\sigma \mapsto -\sigma/\rho$;
- there is an exact sequence

  $$e \to \alpha_p \to \mathcal{T} \to \mu_p \to e,$$

  $$R[\sigma'] \twoheadleftarrow R[\rho, \sigma] \hookleftarrow R[\rho], \quad \sigma' \leftarrow\!\shortmid \sigma,$$

  where the normal subgroup $\alpha_p \subset \mathcal{T}$ is given by $\rho \mapsto 1$
  and there is a subgroup $\mu_p \subset \mathcal{T}$ given by $\sigma = 0$;
- in fact

  $$\mathcal{T} = \alpha_p \rtimes \mu_p, \text{ given by the natural map } \mu_p \hookrightarrow \underline{\mathrm{Aut}}(\alpha_p) \cong \mathbb{G}_m,$$

  and the center of this semi-direct product is the trivial subgroup $e : S \to \mathcal{T}$.
- Note that $\varphi_1 : \mu_p \hookrightarrow \mathbb{G}_m$ and $\varphi_2 : \mu_p \hookrightarrow \mathbb{G}_m$ give

  $$\alpha_p \rtimes_{\varphi_1} \mu_p \cong \alpha_p \rtimes_{\varphi_2} \mu_p.$$

- $\mathcal{T}$ is not annihilated by p, and $\mathcal{T}$ is annihilated by p^2.

(15.2) Proposition. *Any group scheme of rank p^2 over a field K of characteristic p is either commutative or it is non-commutative, and in this case over an algebraic closure of $K \subset k$ isomorphic with $\mathcal{T} \otimes k$.*

Essentially this is contained in [37], proof of Proposition 2.3. Here is a survey of arguments proving (15.2).
It suffices to give the proof in case $K = k$ is algebraically closed. Etale group schemes of rank at most p^2 are constant and commutative.
If G^0 has rank p, then G_0 is commutative and $G = G^0 \times G^{\mathrm{et}}$, hence commutative.
Suppose $G = G^0$, a local group scheme of rank p^2. If $G \neq G[F]$, its Hopf-algebra $E \cong k[X]/(X^{p^2})$ has a maximal ideal generated by one element, and G is commutative.

Remaining case: suppose G is of height one, i.e. $G = G[F]$, and $E \cong k[X,Y]/(X^p, Y^p)$.
Either G is commutative and we are done. Suppose G is not commutative; in [37], page 4 we see that the p-Lie algebra of G/k has a non-zero ideal of dimension one (here we essentially use that this p-Lie algebra has dimension at most two). In this case we conclude there is a normal subgroup scheme $N \subset G$ of rank p. Both N and G/N are commutative and for both there are two possibilities, α_p or μ_p.

A careful analysis of the four resulting cases shows that three of these give a commutative G, and that only the case $N \cong \alpha_p$ and $G/N \cong \mu_p$. A further analysis, case (iv) on [37], page 5, shows that a non-commutative G has the structure of $G \cong \alpha_p \rtimes \mu_p$; as we know all $\mu_p \hookrightarrow \underline{\mathrm{Aut}}(\alpha_p) \cong \mathbb{G}_m$, see the description in (15.1), we are done. □ (15.2)

Remark. See [2] for a discussion of p-Lie algebras. We see there is a simple p-Lie algebra of dimension three, see [2], 4.1.1.

16 Hierarchy and peak group schemes

This section contains new material. However, of any value? We will see in the future.

(16.1) For a finite group scheme G over a field K we consider the pair (G,K). We say (G_1,K_1) and (G_2,K_2) are *geometrically isomorphic*, and we write $(G_1,G_1) \sim (G_2,K_2)$ if there exist a field Ω containing K_1 and containing K_2 and an isomorphism $G_1 \otimes \Omega \cong G_2 \otimes \Omega$; a class under this equivalence relation is denoted by $[G, K]$.

We write $[G_1, K_1] \succ [G_2, K_2]$ (defining a "hierarchy") if "there exists a specialization from G_1 to G_2" , i.e. if there exists an integral scheme S, with a closed point $0 \in S(K)$ and generic point η and a finite flat group scheme $H \to S$ with $(G_1, K_1) \sim (H_\eta, \kappa(\eta))$ and $(G_0, K_0) \sim (H_0, K)$.

Note that the relation "$\succ$" is transitive, see [29], Lemma 2.1.

We say G is a *peak group scheme*, if G is a finite group scheme over a field K and any $(G', K') \succ (G, K)$ implies $(G', K') \sim (G, K)$

(16.2) We recall: *Let $R \twoheadrightarrow R'$ be a surjective homomorphism of local rings. The base change functor gives an equivalence of categories between finite etale algebras over R' and finite etale algebras over R.*
See [9], 18:1 *Une équivalence remarquable de catégories"* in particular Theorem 18.12 on page 109.
We conclude that *any etale finite group scheme (G, K) is a peak group scheme.*

Describe all peak group schemes of rank p^2 over a field $k \supset \mathbb{F}_p$.

17 Moduli

In mathematics, in particular in algebraic geometry it is convenient to classify isomorphism classes of objects considered. In 1857, discussing what we now call Riemann surfaces of genus p, Riemann wrote: *"... und die zu ihr behörende Klasse algebraischer Gleichungen von $3p-3$ stetig veränderlichen Grössen ab, welche die Moduln dieser Klasse genannt werden sollen."* See [34], Section 12.

It took mathematicians some time to formulate precise results (representbable functors, Grothendieck, coarse moduli schemes, Mumford, a long lists of names and statements). One of the obstacles is that the notion of "moduli" is a bit complicated in case objects to be considered have non-trivial automorphisms. There are basically two ways to overcome this. Either use stacks, coarse moduli schemes. Or "rigidify" objects, thus eliminating non-trivial automorphisms. In our case this last method seems the easiest.

(17.1) For a given $m \in \mathbb{Z}_{>0}$ we study triples (R, N, β), were R is a commutative ring with $1 \in R$, and $N = \mathrm{Spf}(E) \to \mathrm{Spf}(R)$ is a (finite) group scheme, with augmentation ideal $I = \mathrm{Ker}(A \to R)$, and

$$\beta : R^{m-1} \xrightarrow{\sim} I$$

is an isomorphism of R-modules. This implies that E is R-free hence R-flat. Note that the interesting case that R is a local ring and E is finitely generated and flat implies that E is R-projective, hence E is R-free, and I is R-free of rank equal to $\mathrm{rank}(E/R) - 1$.

We show that $R \mapsto (R, N, \beta)$ defines a representable functor.

(17.2) Theorem. *There exists such a triple* $(\mathcal{R}^{(m)}, \mathcal{N}^{(m)}, \beta^{(m)})$*, we write* $\mathcal{R} = \mathcal{R}^{(m)}$, $\mathcal{N}^{(m)} = \mathrm{Spf}(\mathcal{A}^{(m)})$, with $\mathcal{A}^{(m)} = \mathcal{A}$,
such that for any triple (R, N, β) *there exists a unique ring homomorphism* $\psi : \mathcal{R}^{(m)} \to R$ *such that*

$$(R, N, \beta) \quad \cong \quad (\mathcal{R}^{(n)}, \mathcal{N}^{(n)}, \beta^{(n)}) \otimes_{\mathcal{R}^{(n)}} R.$$

Proof. The equations for comultiplication, coinverse, and augmentation are given by a finite number of coefficients. Use these as variables T_i; the Hopf-algebra conditions give an ideal $J = J^{(n)} \subset \mathbb{Z}[T_i]$, write $\mathcal{R}^{(n)} = \mathbb{Z}[T_i]/J$, and define the $\mathcal{R}^{(n)}$-Hopf-algebra $\mathcal{A}^{(n)}$ by these relations. For any (R, N, β) the coefficients in its comultiplication, coinverse, and augmentation define $\psi : \mathcal{R}^{(n)} \to R$ and the result follows. □

Remark. For any algebraically closed field k the set of k-isomorphism classes of finite group schemes of rank p equals $\mathrm{GL}(k, p)\backslash\mathrm{RingHom}(\mathcal{R}^{(m)}, k)$. Even in case the quotient $\mathrm{GL}_p/(\mathrm{Spf}(\mathcal{R}^{(m)})$ would exist, in general $\mathcal{N}^{(m)}$ does not descend to this quotient.

(17.3) Example. In case $n = p = 2$ we know $R = \mathrm{Spf}(\mathbb{Z}[A, C]/(AC - p))$, and the structure of $R^{(2)} \subset \mathcal{A}^{(2)}$ is known, see [43], see 19.2.

If $n = p > 2$ the structure of $R^{(p)}$ is more complicated. For Λ_p as in [43], the quotient of $\mathrm{Spf}(\mathcal{R}^{(p)}) \otimes \Lambda_p$ by GL_p and by $\mathbb{Z}/(p-1)$ is isomorphic with $\mathrm{Spf}(\Lambda_p[A, B]/(AB + p))$, which is an integral domain.

It seems not easy to describe $R^{(m)}$ explicitly for every m.

Fix a prime number p and an integer $n > 0$. We see $\mathrm{Spf}(\mathcal{R}^{(p^n)})$ is of finite type over $\mathbb{Z}$, this scheme has finitely many irreducible components. These can can be of three different kinds:

(0) There are irreducible components $T \subset \mathrm{Spf}(\mathcal{R}^{(p^n)})$ such that the generic point of T is in characteristic zero.

(p) It can happen that an irreducible component $T \subset \mathrm{Spf}(\mathcal{R}^{(p^e)})$ is pure in characteristic p.

(0p) For $n > 1$ there exists at least one irreducible component $T \subset \mathrm{Spf}(\mathcal{R}^{(p^n)})$ such that it is not of type (0) and not of type p. This seems an obstacle for progress.

(17.4) Expectation. We expect that in case $m = p^n$ any irreducible component $T \subset \mathrm{Spf}(\mathcal{R}^{(p^n)})$ has a geometric point $P_0 \in T(k)$ such that $\mathcal{N}^{(n)} \times_T P_0 \cong (\alpha_p)^n$.

(17.5) Another approach to be used in 19.8 below. Fix a field $K \supset \mathbb{F}_p$ (we prefer K to be perfect), and a finite group scheme G_0/K. Consider artin local rings R with $R/\mathfrak{m}_R = K$. Consider pairs (G, ψ) of a finite flat group scheme G/R with a given K-isomorphism

$$\psi : G \otimes_R K \xrightarrow{\sim} G_0.$$

This gives a prorepresentable functor $\mathrm{Def}(G_0)$ (the local moduli problem). Properties of the representing object can be studied. This can be studied via a completion of a local ring on $\mathrm{Spf}(\mathcal{R}^{(p^n)})$.

In particular we can choose $G_0 = (\alpha_p)^n$. Choose all (R, G, φ) where R is a local artin ring with residue field $R/\mathfrak{m}R = K$ characteristic p, and a given isomorphism

$$\varphi : (\alpha_p)^n \otimes K \xrightarrow{\sim} G \otimes R.$$

This functor is prorepresentable. We write $\mathcal{A}^{(m)}$ for the ring prorepresenting $\mathrm{Def}((\alpha_p)^n)$. This is a finitely generated $W_\infty(\mathbb{F}_p)$-algebra.

Let $0 = (R, N, \beta)$ with N and β given by $(\alpha_p)^n$. We see that $\mathcal{R}^{(m)}$ is the formal completion

$$\mathcal{A}^{(m)} = (\mathcal{R}^{(m)})^{/0}.$$

If the answer to (17.4) is positive, every component of $\mathrm{Spf}(\mathcal{R}^{(m)})$ can be studied via the universal family over $\mathcal{A}^{(m)}$.

18 (Non)-Ideas?

In this section we collect some ideas that (at present) did not lead to an answer to the question whether every finite group scheme is annihilated by its rank.

(18.1) Torsion subschemes. Let G be a finite flat group scheme over a ring R, and let $q \in \mathbb{Z}_{>0}$. Let $G[q] \hookrightarrow G$, a closed subscheme, be defined by the cartesian diagram

$$\begin{tikzcd} G[q] \arrow[r, hook] \arrow[d] & G \arrow[d, "{[q]}"] \\ S \arrow[r, "e"'] & G. \end{tikzcd}$$

Can this be of any help to study "annihilated by rank"? In general, even over a base field, $G[q] \subset G$ need not be a subgroup scheme (as we see already in the case of abstract groups). Moreover, over an arbitrary base $G[q] \to S$ in general is not flat (examples are easy to give). A far as I know a study of this subscheme is of no help for our problem.

(18.2) Lifting to a domain. Suppose G is a finite group scheme over a ring R_1, let $R_1 \hookrightarrow R_2$ be an inclusion of rings. If $G \otimes_{R_1} R_2$ is annihilated by its rank, then G/R_1 is annihilated by its rank.

If G is a finite group scheme over a ring R_1 and $R_2 \twoheadrightarrow R_1$ is a ringhomomorphism, and if there exists a finite flat group scheme G_2 over R_2 such that $G_1 \cong G_2 \otimes_{R_2} R_1$ and G_2/R_2 is annihilated by its rank, then G/R_1 is annihilated by its rank.

Note that *any finite group scheme G over a domain R is annihilated by its rank.*

Indeed, embedding R into its field of fractions $R \hookrightarrow Q(R) = K$ gives $(G \otimes_R K)/K$, and we know a finite group scheme over a field is annihilated by its rank, hence G/R is annihilated by its rank.

Can we lift any finite group scheme to a domain?

Example. As we see already by the remark on page 6/7 in [43], also see (15.1), there exist commutative group schemes of rank p^2, and these cannot be lifted to a characteristic zero domain. In 19.5 we show that for any prime number p and any $e \in \mathbb{Z}_{\geq 0}$ there exist a ring R in which $0 \neq p^e{\cdot}1 \in R$ and a *non-commuative* group scheme G/R of rank p^2; *for* $e > 0$ *in this situation lifting to an integral domain is not possible.*

Example. Take $R = \mathbb{F}_p[\varepsilon]/(\varepsilon^2)$ and $G = G_{a,b}$ with $a = \varepsilon = b$. *There does not exist a characteristic p domain* R_2 *and a surjective ring homomorphism* $R_2 \twoheadrightarrow R$ *and a lift of this* $G_{a,b}/R$ *to* R_2.

Example. Take $n \geq 2$ and $G_0 = (\alpha_p)^n$. Consider $\mathcal{A}^{(m)} = (\mathcal{R}^{(m)})/0$ as in (17.5). As G_0 can be lifted to every constant groups scheme in charcteristic zerop, we can find two irreducible components $T_1, T_2 \subset \mathrm{Spec}(\mathcal{A}^{(m)})$ say, with generic fibers $\underline{\mathbb{Z}/(p^n)}$ respectively $\underline{(\mathbb{Z}/(p))^n}$. Choose $0 \subset \mathrm{Spf}(R) \subset T_1 \cup T_2 \subset \mathrm{Spec}(\mathcal{A}^{(m)})$ with $\mathrm{Spf}(R) \subsetneqq T_1$ and $\mathrm{Spf}(R) \subsetneqq T_2$. The universal $G/\mathrm{Spf}(R)$ cannot be lifted to a commutative group scheme in characteristic zero.

Conclusion. The method "lifting to a domain" does not answer "annihilated by rank".

(18.3) Finding a subgroup scheme. We will see that there exist finite flat group scheme $G \to S$ of rank p^n for any $n \in \mathbb{Z}_{\geq 2}$. such that there is no subgroup scheme $e \subsetneqq H \subsetneqq G$. See (19.8) This method does not give a proof for the "annihilated by rank" problem.

There is a long list of all kind of ideas and methods I tried, and for the moment, none of these did lead to a conclusion about the "annihilated by rank" problem.

19 Examples

Convention. We will say a ring Γ *has characteristic zero* if it is an integral domain, and the canonical ringhomomorphism $\mathbb{Z} \hookrightarrow \Gamma$ is injective. I.e. For any $n \in \mathbb{Z}_{>0}$ we have $0 \neq n{\cdot}1 \in \Gamma$.

The property "for any $n \in \mathbb{Z}_{>0}$ we have $0 \neq n{\cdot}1 \in \Gamma$" does not imply Γ is an integral domain, we will see examples.

We will say a ring Γ *has characteristic p* if it is an integral domain and $0 = p{\cdot}1 \in \Gamma$.

Suppose N_0 is a finite flat group scheme over a ring R. We say N_0/R

can be lifted to characteristic zero if there exist an integral domain Γ of characteristic zero, a ringhomorphism $\psi : \Gamma \to R$ and a finite flat group scheme N/Γ with $N \otimes_\Gamma R \cong N_0/R$.

We will not discuss: abelian varieties, abelian schemes, matrix algebras.

Over any field of characteristic $p > 0$ there is precisely one local-local group scheme of rank p: α_p. Moreover Cartier duality gives $(\alpha_p)^D = \alpha_p$.
Convention. Schemes of different base schemes should be denoted by different symbols. However we make an exception for examples like α_p, μ_m, where the base scheme in the notation is omitted in case the context makes clear what is intended. However, be careful: $\mathrm{End}(\alpha_p)$ is not well-defined without specifying the base scheme.

Over any algebraically closed field of characteristic $p > 0$ there is precisely one etale group scheme of rank p and it is an etale-local group scheme: $\underline{\mathbb{Z}/p}$; over any perfect field K of characteristic $p > 0$ any etale-local group scheme of rank p is given by a continuous Galois representation $\mathrm{Gal}(K^a/K) \to \mathbb{F}_p^*$.

An analoguous statement for a local-etale group scheme of rank p: for K^a there is precisely one, namely μ_p, and over a perfect K it is given by a continuous Galois representation $\mathrm{Gal}(K^a/K) \to \mathbb{F}_p^*$.

(19.1) TO group schemes. *Group schemes of rank a prime number p* are classified in the paper [43]. In order to obtain a feeling for the topic describe this classification in one special case:

Exercise. *Describe all group schemes over an arbitrary base ring R in the case the augmentation ideal is free of rank one.* See [42], 3.2, [35], 8.6.1.
Hint. The Hopf-algebra is $E = R \oplus I$, write $I = R{\cdot}x$, then $x^2 \in I$ and use the comutiplication and the ring structure in order to describe E explicitly.

We recall results and notations contained in [43].
A first result: a group scheme of prime rank is commutative, and annihilated by it rank, [43], Theorem 1.

For more general base schemes, consult that paper, but let us assume here that the base ring is a noetherian complete local ring R with residue class field $R/\mathfrak{m}_R = \kappa$, a field of characteristic p. Note that in this case $p-1$ is invertible in R, all $(p-1)$-root of unity contained in $\mathbb{F}_p \subset \kappa$ lift uniquely to

R, and any finitely generated, flat R-module is free.

There exists a symmetric polynomial

$$D_p(X,Y) \in \mathbb{Z}[\frac{1}{p-1}, \zeta_{p-1}][X,Y]$$

homogenous of degree p and X and Y do appear in every term;
this polynomial $D_p(X,Y)$ is characterized by $(X+Y+pD_p)^p = X+Y+pD_p$ with $X^p = X$ and $Y^p = Y$.
Examples: $D_2 = -XY$, $D_3 = -(X^2Y + XY^2)/2$.

For

$$a, c \in R \text{ with } ac = p \text{ we define } G_a^c = \mathrm{Spf}(E_a^c) \text{ as follows:}$$

$E_a^c = E = R[x]$, augmentation $x \mapsto 0$, with $x^p = ax$, a comultiplication is given by

$$s(x) = x \otimes 1 + 1 \otimes x + cD_p(x \otimes 1, 1 \otimes x)$$

and a coinverse is given by

$$\iota(x) = -x \quad \text{if} \quad p > 2; \quad \iota(x) = +x \quad \text{if} \quad p = 2$$

.

(19.2) Theorem, see [43], Theorem 2.
(1) *For a noetherian complete local ring R with residue class field $R/\mathfrak{m}_R = \kappa$, a field of characteristic p, and*

$$a, c \in R \textit{ with } ac = p \textit{ and comultiplication } s(-) \textit{ and coinverse } \iota(-)$$

given above the result is a R-Hopf-algebra free of rank p.
(2) *Conversely if G is a flat R-group scheme of rank p there exist a, c, s, ι as above such that $G \cong \mathrm{Spf}(R[x])$.*
Notation. This group scheme will be denoted by $G_a^c = G_{a,R}^c$.
(3) *The group schemes*

$$G_{a_1}^{c_1} \textit{ and } G_{a_2}^{c_2} \textit{ are isomorphic } R\textit{-group schemes}$$

if and only if there exists a unit $u \in R^*$ such that

$$u^{p-1}a_1 = a_2 \quad \textit{and} \quad u^{1-p}c_1 = c_2.$$

(19.3) Let H be a finite abstract group. Over any base scheme S we define $\underline{H}_S$ by the representable group functor $\underline{H}_S(T) = H$ for any connected scheme T and $T \to S$. This is called a *constant finite group scheme.*

Over any base $\mathbb{G}_a$ is given as $\mathbb{A}^1$ with $+$ as group law; for a base scheme $S = \mathrm{Spf}(R)$ its Hopf-algebra is given by $E = R[X]$, the augmentation is given by $X \mapsto 0$, and $s(X) = X \otimes 1 + 1 \otimes X$ and $\iota(X) = -X$.

For a base in characteristic $p > 0$ we have, $\alpha_p = \mathrm{Ker}(F : \mathbb{G}_a \to \mathbb{G}_a)$, and its Hopf-algebra for $p{\cdot}1 = 0 \in R$ is $R[x]$, with $x^p = 0$.

Over any base $\mathbb{G}_{m,S}$ is given as $\mathbb{A}^1 \setminus 0_S$ with $\times$ as group law; over a base ring R its Hopf-algebra is $R[T, 1/T]$, augmentation $T \mapsto 1$, and $s(T) = T \otimes T$); for any integer $m > 1$ over a base ring R we have the finite group scheme $\mu_{m,S} = \mathrm{Ker}([m] : \mathbb{G}_{m,S} \to \mathbb{G}_{m,S})$; over a base ring R its Hopf-algebra is $R[T, 1/T]/(T^m - 1)$ with augmentation $T \mapsto 1$ and $s(T) = T \otimes T$. Over any base scheme we have

$$(\mu_{m,S})^D = \underline{\mathbb{Z}/m}_S \quad \text{and} \quad \left(\underline{\mathbb{Z}/m}_S\right)^D = \mu_{m,S}.$$

Over any base scheme on which m is invertible $\mu_{m,S} \to S$ is etale.

This confirms the solution you probably gave for the exercise above: for $p = 2$ the Hopf-algebra of a group scheme of rank 2 such that I is free of rank one is given by $a, b \in R$ with $ab = 2$, with $E = R[x]$, $x^2 = ax$, and $s(x) = x \otimes 1 + 1 \otimes x - cx \otimes x$, and $\iota(x) = x$.

For the construction of units $w_1 = 1, w_2, \cdots, w_{p-1}$ and w_p we refer to [43], pp. 8-10. Here we need the existence of w_{p-1} and the property $w_p = p{\cdot}w_{p-1}$. These elements satify

$$D_p(X, Y) = \frac{w_{p-1}}{1-p} \sum_{1 \le j \le p-1} \frac{X^j}{w_j} \frac{Y^{p-j}}{w_{p-j}}.$$

One property of these elements is $w_j \equiv j! \pmod{p}$ for $1 \le j \le p-1$. $w_{p-1} \bmod p = -1 \in \mathbb{F}_p$.

The group schemes $G_{a,b}$. Using (over a base ring R, omitted in the notation here) the group scheme G_a^c, with $ac = p$, writing $b = w_{p-1}c$, we define $G_{a,b}$ by

$$G_{a,b} = G_a^c = G_a^{b/w_{p-1}} = G_{a,w_{p-1}c}, \quad aw_{p-1}c = ab = w_{p-1}p.$$

Cartier duality. We have:

$$(G_{a,b})^D = G_{b,a}, \quad (G_a^c)^D = G_{w_{p-1}c}^{a/w_{p-1}}.$$

See [43], page 15.

The group scheme

$\underline{\mathbb{Z}/p}_R = G_1^p = G_{1,w_{p-1}p}$ is given by $\;a = 1,\;\; b = w_p = w_{p-1}{\cdot}p,\;\; c = p,$

and

$\mu_{p,R} = G_{w_p}^{1/w_{p-1}} = G_{w_p,1}$ is given by $\;a = w_p = w_{p-1}{\cdot}p,\;\; b = 1,\;\; c = 1/w_{p-1}.$

See [43], the proposition on page 9.

In particular, if $p{\cdot}1 = 0 \in R$:

$$\underline{\mathbb{Z}/p}_R = G_{1,0} = G_1^0, \quad \text{and} \quad \mu_{p,R} = G_0^{-1} = G_{0,1}.$$

For $a \in k$ and $c \in k^*$, and for R complete local $R/\mathfrak{m}R = k$ and $c \in R^*$ we can scale by $\sqrt[p-1]{w_p}$ and have $G_a^c \cong \mu_{p,k} \cong G_p^1$, respectively $G_a^c \cong \mu_{p,R} \cong G_p^1$.

(19.4) Terminology: eale-reduced. For a commutative ring R we write

$$\sqrt{0} = \{x \in R \mid \exists n \in \mathbb{Z}_{>0} : x^n = 0\}.$$

We say a commutative ring R is reduced if $\sqrt{0} = 0$, i.e. R has no non-zero nilpotent elements.
(1) For a non-perfect field K and a K-algebra E it can happen that E is reduced and $E \otimes_K K^{\text{sep}}$ is non-reduced; here K^{sep} is the smallest perfect field containing K. For example an inseparable extension $K \subsetneq K'$ has this property.
(2) There exists a reduced group scheme G over K such that $G \otimes K^{\text{sep}}$ is non-reduced. For example, choose $a \in K$ with $\sqrt[p]{a} \notin K$. Consider

$$G = \text{Spf}(K[X,Y]/(X^p - aY^p)) \subset \text{Spf}(K[X,Y]) = (\mathbb{G}_{a,K})^2.$$

Show $K[X,Y]/(X^p - aY^p)$ is reduced, but $K[X,Y]/(X^p - aY^p) \otimes K(\sqrt[p]{a})$ is not reduced.

(3) For a scheme T the sheaf of nilpotents $I \subset \mathcal{O}_T$ defines a closed subscheme $T_{\mathrm{red}} := \mathcal{Z}(I) \subset T$.

For a group scheme H over a perfect field L the subscheme $H_{\mathrm{red}} \subset H$ is a L-subgroup scheme.

For a group scheme G over a non-perfect field K, in general, $G_{\mathrm{red}} \subset G$ is not a K-subgroup scheme. For an example se below.
(4) For a group scheme H over a perfect field L the L-subgroup scheme need not be a normal subgroup scheme.
(5) For any field K and a K-algebra E of *finite* K-dimension the following are equivalent:

$$(E/K \quad \text{is etale}) \Leftrightarrow (E \quad \text{is reduced}).$$

See [36], Proposition on page 23.
We see that for a *finite* group schemes over a field the notions "etale" and "reduced" are the same.
(6) **Hidden nilpotents.** Let K ba a non-perfect field with $a \in K$ with $\sqrt[p]{a} \notin K$. The closed subset

$$G := \mathrm{Spf}(E) \quad \subset \mathrm{Spf}(K[X]) = \mathbb{G}_{a,K}, \quad E = K[X]/(X^{p^2} + aX^p))$$

is a finite subgroup scheme. In this case $G_{\mathrm{red}} \subset G$ is not a K-subgroup scheme. We have $E \cong E_1 \times E_2 \times \cdots \times E_p$: the scheme G is a disjoint union of p subschemes, with

$$E_1 \cong K[\tau]/(\tau^p), \quad E_j \cong K(\sqrt[p]{a}), 1 < j \leq p.$$

The ideal $I - (\tau)$ of nilpotents has K-dimension equal to $p - 1$. The ideal of nilpotents of $E \otimes K(\sqrt[p]{a})$ has dimension $p \times (p-1)$ over $K(\sqrt[p]{a})$.
(7) Another example that $G_{\mathrm{red}} \subset G$ is not a K-subgroup scheme and of hidden nilpotents can be found in [4], 3.10: choose an ordinary elliptic curve E_0 over $k \supset \mathbb{F}_p$, take the universal deformation $E/k[[t]]$ in characteristic p and let $G = E[p]$, a finite group scheme of rank p^2 over $K = k[[t]]$. Here G_{red} is nog a subgroup scheme, and we have "hidden nilpotents" as above. Here we see that such examples appear quite naturally.

Reminder. In (15.1) we find a description of a non-commutative group scheme of rank p^2.

(19.5) Semidirect products Let N and H be (abstract) groups, written multiplicatively. Let $\varphi : H \to \mathrm{Aut}(N)$ be a homomorphism of groups. We define the *semidirect product*

$$G = N \rtimes_{\varphi} H$$

as follows: as *sets* we have a bijection $G = N \times H$, and the group law on this product is given by:

$$(x_1, y_1){\cdot}(x_2, y_2) := (x_1{\cdot}\varphi(y_1)(x_2), y_1{\cdot}y_2).$$

We see that conjugation on the normal subgroup $N \subset G$ is given by

$$(1, y){\cdot}(x, 1){\cdot}(1, y^{-1}) = (\varphi(y)(x), 1).$$

Note that $N = \{(x, 1)\} \subset G$ and $H = \{(1, y)\} \subset G$ are subgroups.

For group schemes this can be generalized as follows. Suppose given group schemes N and H over some base scheme S. Define $\underline{\mathrm{Aut}}_S(N)$ as

$$\underline{\mathrm{Aut}}_S(N)(T) = \mathrm{Aut}_T(N_T), \quad \text{for any} \quad T \to S.$$

Example. Show $\underline{\mathrm{Aut}}_K(\alpha_{p,K}) = \mathbb{G}_{m,K}$ for any base field $K \supset \mathbb{F}_p$. For a proof and a generalization see 19.6

(19.6) We compute $\underline{\mathrm{Aut}}(G_a^c)$ over any Λ_p base ring R.
Note that $\mathbb{Z}/p$ operates on a group scheme annihilated by p, hence elements of $(\mathbb{Z}/p)^* \cong \mathbb{Z}/(p-1)$ act as automorphisms; moreover these commute with automorphisms. Suppose the Hopf-algebra of $G_a^c = \mathrm{Spf}(E)$ is free over R; for example this is the case if R is a local ring. The action on $E = R[\tau]/(\tau^p = a\tau)$ splits the augmentation ideal I in eigenspaces, each of them free of rank one, and any automorphism of G_a^c (over any base extension) respects this splitting. This we use to prove the following result.
Theorem.

$$\underline{\mathrm{Aut}}(G_a^c) \cong \mathrm{Spf}(R[\lambda, \frac{1}{\lambda}]/(a(\lambda^{p-1} - 1), c(\lambda^{p-1} - 1)); \quad \text{note that} \quad ac = p{\cdot}1 \in R$$

with comultiplication $\lambda \mapsto \lambda \otimes \lambda$*, coinverse* $\lambda \mapsto 1/\lambda$ *and augmentation* $\lambda \mapsto 1$.
Proof. Over any base ring R' we can view an automorphism of the Hopf-algebra $R'[\tau]/(\tau^p - a\tau)$ as a ringhomorphism given by $\tau \mapsto \lambda{\cdot}\tau$. The condition $\tau^p = a\tau$, after multiplying with $1/\lambda$, gives $a(\lambda^{p-1} - 1) = 0$. This condition applied to the comultiplication gives $c(\lambda^{p-1} - 1) = 0$. Any invertible value of λ satisfying these relations gives an automorphism, and all automorphisms are given in this way. This proves the theorem. □

For example $a = 0 = c$ gives $\underline{\mathrm{Aut}}(\alpha_p) = \mathrm{Spf}(R[\lambda, \frac{1}{\lambda}]) = \mathbb{G}_m$.

Comment. For abstract groups there is no nontrivial homomorphism $\mathbb{Z}/p \hookrightarrow \mathrm{Aut}(\mathbb{Z}/p)$; any $\mathbb{Z}/p \rtimes \mathbb{Z}/p$ is split commutative. However for group schemes an analogous situation is very different. Over k we have a homomorphism $\mu_{p,k} \hookrightarrow \underline{\mathrm{Aut}}(\alpha_{p,k})$. Over several base rings we can have a non-trivial $G_A^C \to \underline{\mathrm{Aut}}(G_a^c)$, and we will see consequences below.

As we will see, $G = \alpha_{p,k} \rtimes \mu_{p,k}$ as above cannot be lifted to a ring R in which $p{\cdot}1 \neq 0$. One could therefore wonder whether there exist non-commutative finite group schemes of rank p^2 over a ring in which $p{\cdot}1 \neq 0$. We will see that for every integer $r \geq 0$ there exists a local artin ring R and a non-commutative group scheme of rank p^2 over R such that $0 \neq p^r{\cdot}1 \in R$, see (19.8).

Acknowledgement. I thank Alexander Petrov who showed me this is not the case, see (5) below for $p = 2$ and $p{\cdot}1 \neq 0 \in R$, and I thank Alexander Petrov and Shizhang Li for further exchange of examples and ideas that lead me to show (5) below.

(19.7) We study (non-commutative) group schemes $G = G_a^c \rtimes_\varphi \ G_A^C$. We write $G_a^c \rtimes G_A^C$ in case φ will be specified later.
Convention for this subsection:
k is an algebraically closed field of characteristic p and
R is a local artin ring with $R/\mathfrak{m}_R \cong k$.
Note that

$$\text{if } a \in R^* \text{ then } G_a^c \cong_R G_1^p \cong_R \underline{\mathbb{Z}/p}_R,$$

and

$$\text{if } c \in R^* \text{ then } G_a^c \cong_R G_{w_p}^{1/w_p} \cong_R G_p^1 \cong_R \mu_{p,R}.$$

We consider a finite flat group scheme G of rank p^2 over k or over R. We mention and show the following properties:

(1) Over R any $\mu_p \rtimes G_A^C$ is commutative and split, and any $\underline{\mathbb{Z}/p} \rtimes G_A^C$ is commutative and split.

(2) A non-commutative group scheme G of rank p^2 over k is $G \cong \alpha_{p,k} \rtimes \mu_{p,k}$ over k, as described in 15.1. In particular, up to k-isomorphism there is only one non-commutative group scheme of rank p^2 over k. See [37], Prop. 2.3.

(3) Suppose G_0/k is $G_0 = \alpha_{p,k} \rtimes \mu_{p,k}$, and suppose G/R is a lift of G_0/k over $R \to k$. (A lift over R is supposed to be flat over R.) Then there exist a, c, φ such that $G \cong G_a^c \rtimes_\varphi \mu_{p,R}$. See [37], theorem on page 13. Comment: compare with 19.8.

(4) In the situation as in (3), if G is non-commutative, then $p{\cdot}1 = 0 \in R$. We give a proof; also see [37], Prop. 3.3.
In other words: $G_0 \cong \alpha_{p,k} \rtimes \mu_{p,k}$ as in (3) *cannot be lifted* to a a ring R in which $p{\cdot}1 \neq 0 \in R$.

(5) For any prime number p, for any integer $r \in \mathbb{Z}_{>0}$ there exists an R with $p^r{\cdot}1 \neq 0 \in R$, and $a, c, C \in \mathfrak{m}_R$ and $A \in R$ and a non-commutative $G_a^c \rtimes G_A^C$ over R.

Proof. (1) For $\mu_p = G_a^c$ over R, the case $c \in R^*$ and for $\underline{\mathbb{Z}/p} = G_a^c$, the case $a \in R*$ we have

$$\underline{\mathrm{Aut}}(G_a^c) \cong \mathrm{Spf}(R[\lambda, \frac{1}{\lambda}]/(a(\lambda^{p-1}-1), c(\lambda^{p-1}-1)) \cong \mathrm{Spf}(R[\lambda]/(\lambda^{p-1}-1),$$

a group scheme of rank $p-1$, and any homomorphism to G_A^C is trivial. This proves $G_a^c \rtimes G_A^C$ is commutative for these cases. This proves (1).

(5) Choose $u, v \in \mathbb{Z}_{>0}$, e.g. $u = 1 = v$. Choose $R = \mathbb{Z}_p[\pi]/[\pi^{u+v} - p, p^r{\cdot}\pi]$; note that $p^r{\cdot}1 \neq 0 \in R$. We take $a = \pi^u$, $c = p^v$, $1 \leq w \leq u + v$, $C = \pi^w$, $A = \pi^{u+v-w}$, and $\xi_1, \cdots, \xi_{p-1} = p^r$; note that $ac = p = AC$, and $C\xi_j = 0$ for every j and $\xi_{j_1}\xi_{j_2} = 0$ for every j_1, j_2. We define

$$\varphi' : R[\lambda, \frac{1}{\lambda}]/(a(\lambda^{p-1}-1), c(\lambda^{p-1}-1)) \to R[\tau]/[\tau^p - A\tau]$$

by $\lambda \mapsto 1 + \sum_{1 \leq j \leq p-1} \ \xi_j \tau^j$. We see that $\varphi'(a(\lambda^{p-1}-1)) = 0 = \varphi'(c(\lambda^{p-1} - 1))$. Hence φ' is a ring homomorphism, defining

$$\varphi : G_A^C \longrightarrow \underline{\mathrm{Aut}}(G_a^c).$$

As $a\xi_j = 0$ every j we see that

$$s(\lambda) = s(1 + \sum_{1 \leq j \leq p-1} \ \xi_j \tau^j)$$

This proves (5).

Survey. We see that

$G \cong \alpha_{p,k} \rtimes \mu_{p,k}$ non-commutive cannot be lifted to a ring R with $p{\cdot}1 \neq 0$, however

$\alpha_{p,k} \times \alpha_{p,k}$ and $\alpha_{p,k} \times \underline{\mathbb{Z}/p}_k$ can be lifted to a ring with $p^r{\cdot}1 \neq 0 \in R$ for any integer $r > 0$.

Comment. Consider $\mathcal{R}^{(p^2)}$ as in 17.2. We see there exists a quotient $\mathcal{R}^{(p^2)} \twoheadrightarrow \Delta$ such that $\mathcal{N}^{(p^2)} \otimes_{\mathcal{R}^{(p^2)}} \Delta$ is non-commutative, and for every integer $r > 0$ we have $p^r{\cdot}1 \neq 0 \in \Delta$, however there is no ring homomorphism from Δ to a characteristic zero *domain*. We will not consider Δ as a characteristic zero ring.

Proofs can be given for statements below.

(19.8) Examples. (1) *For any $r \in \mathbb{Z}_{\geq 0}$ there exists a local artin ring R in which $p{\cdot}1 \neq 0$ and a finite flat non-commutative group scheme G/R of rank p^2 over R such that for any $R \subset R'$, where R' is a local artin ring, there is are non-zero proper subgroup schemes $N_1 \subset G \otimes R'$, and $H \subset G \otimes R'$ both flat of rank p over R' with the property that $(G \otimes_R R') \cong N_1 \rtimes H$.*

(2) *For any $n > 1$ there exists a local artin ring R and a finite flat commutative group scheme G/R of rank p^n over R such that for every $R \subset R'$, where R' is a local artin ring, there is no non-zero proper subgroup scheme $N_1 \subset G \otimes R'$ flat of rank p over R'.*

20 Tate-ℓ-groups, p-divisible groups (Barsotti-Tate groups) and the EO-stratification

In this section we give some background (not essential for understanding my talks).

(20.1) Suppose A is an abelian variety of dimension g over a field K and ℓ is a prime number not equal to the characteristic of K. For every $n \in \mathbb{Z}_{\geq 0}$ the group scheme

$$A[\ell^n] := ([\ell^n] : A \to A)$$

is a finite group scheme of rank ℓ^{2ng} etale over K. It can be described as a Galois module with $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ operating on $(\mathbb{Z}/\ell^n)^{2g}$. The Tate-ℓ-group or the Tate-ℓ-module is defined as

$$T_\ell(A) = \lim_{\leftarrow}(A[\ell^n]), \quad \lim_{\leftarrow} = \text{proj.lim}$$

which is “the same” as $T_\ell(A)(\overline{K}) \cong (\mathbb{Z}_\ell)^{2g}$ with a continuous Galois action. This tool gives an important point of view on the arithmetic of A. Many important theorems in number theory use this approach.

Variant. Suppose S is a base scheme, ℓ is a prime number invertible in all local rings of S and A/S is an abelian scheme. We define $T_\ell(A) = \lim_{\leftarrow}(A[\ell^n])$ and also in this situation this is useful tool

(20.2) How do you use this circle of ideas for a prime number p equal to the characteristic of K? Iacopo Barsotti and John Tate pioneered in the period 1962-1967 by introducing a new concept:

p-divisible groups, also called Barsotti-Tate groups.

The technical advantage is that these can be usefully studied over any base scheme. For an abelian scheme A over a base scheme S define

$$A[p^\infty] = \lim_{\rightarrow}(A[p^n]) = \cup_n \ A[p^n], \quad \lim_{\rightarrow} = \text{ind.lim}.$$

The choices either taking inverse limits, as in $T_\ell(A)$, or inductive limits, as in $A[p^\infty]$ have been made for technical reasons.

Remark. If $p = \ell$ is invertible in all local rings of S, the concepts $T_\ell(A)$ and $A[p^\infty]$ are equivalent notions.

Definition. A p-divisible group of height h over a base scheme S is given as an inductive system $X = (\cdots G_n \subset G_{n+1} \cdots)$, of finite flat group schemes over S, with the property that $(\cup G_n)[p^i] = G_i$. This means that for every m and n there is an exact sequence

$$0 \to G_m \to G_{m+n} \to G_n \to 0.$$

In particular

$$G_{n+1}/G_n = G_1 = \mathrm{Im}([p^n] : G_{n+1} \to G_{n+1}) :$$

you can view X *as a tower of extensions where every consecutive subquotient is isomorphic with* G_1.

We say that $G_n = X[p^n]$ is a Barsotti-Tate group truncated at level n.

(20.3) This opened a whole new approach, carried on by Manin, Grothendieck and many others. Invariants of abelian varieties can be given as:

isomorphism classes of their p-divisible groups,

isogeny classes of their p-divisible groups, and isomorphism classes of their BT_1-modules.

This gives naturally defined *foliations* and *stratifications* of moduli spaces of abelian varieties in characteristic p. For a survey and for references, see [28].

The importance of the Kraft theorem is that

classifying abelian varieties by their BT_1*-modules gives a natural decomposition of the moduli space into a finite union of locally closed subvarieties, called the* EO*-stratification.*

In characteristic p we have no methods like arcs and cell-decompositions, so useful in characteristic zero, *but it turns out that the EO-stratification behaves like a cell-decomposition* (the boundary of every non-complete stratum is a finite union of strata in codimension one, and much more). For a survey, and for references see [28].

(20.4) Minimal p-divisible groups An interesting notion is "minimal p-divisible groups". We have seen that a p-divisible group X is a tower of subquotients all isomorphic with $X[p]$; moreover ons can show that any BT_1 group scheme G over $k = \overline{k}$ is a p-kernel: there exists X with $X[p] \cong G$.

A fascinating story: does $X[p] \cong Y[p]$ imply $X \cong Y$? This was asked by Grothendieck in a letter on January 5, 1970 to David Mumford: see [23], page 745. For many p-divisible groups the answer is "no".

Historical remark. The correspondence between Grothendieck and Mumford only became known and available to me in 2010; I did not know this question by Grothendieck and the answer by Mumford when I worked many years ago on the result to be found in [25]; also see [30], 8.6.

The p-divisible groups for which $X[p] \cong Y[p]$ implies $X \cong Y$ are called "minimal"; a classification is known (the problem being reduced to a combinatorial one). These play a crucial role in understanding the foliation of the moduli space of polarized abelian varieties in characeristic p by isomorphism classes of $A[p^\infty]$. For every X the BT_1 group scheme $X[p] \in \mathcal{M}_k^{\mathrm{BT}}$ is a simple object in $\mathcal{M}_k^{\mathrm{BT}}$ if and only if X is a minimal p-divisible group. For more information, see [25], [28].

21 Some questions

(21.1) Question. Fix p^n. Is the set of $[G,k]$ with $(G) = p^n$ a finite set of isomorphism classes? For the definition of $[G,k]$ see Section 16.

(21.2) Question. Suppose $G = \mathrm{Spf}(E)$ is a finite group scheme over k such that $G[F] = G$; then $E = k[\tau_1, \cdots, \tau_n]/[\tau_1^2, \cdots, \tau_n^2]$. If $n > 1$ does there exist a normal subgroup scheme $0 \subsetneqq N \subsetneqq G$? – The answer is probably negative.

(21.3) For every p and $n > 1$ determine the precise structure of $\mathrm{Spf}(\mathcal{R}^{(p^n)})$.

(21.4) Specific example: $m = p^2$, group schemes of rank p^2. We have seen in Section 15 and in 19.6 that there do exist non-commutative group schemes of rank p^2 over artin rings not in characteristic p Moreover we have a complete classification of group schemes of rank p^2 over an algebraically closed field. We can ask and expect:
Question. Is every irreducible component of $\mathrm{Spf}(\mathcal{R}^{(p^2)} \otimes \mathbb{F}_p)$ reduced, and is the set of these irreducible components in bijetive correspondence with the set of isomorphism classes of $[G,k]$ of rank p^2?
Question. Determine the structure of every irreducible component of $\mathrm{Spf}(\mathcal{R}^{(p^2)}$ not in characteristic p.
We expect: there is one component of $\mathrm{Spf}(\mathcal{R}^{(p^2)} \otimes \mathbb{F}_p)$ with generic point corresponding with a non-commutative group scheme, and this component is not contained in a component in mixed characteristic, and all other irreducible component of $\mathrm{Spf}(\mathcal{R}^{(p^2)} \otimes \mathbb{F}_p)$ are contained in a component in mixed characteristic.
Can we formulate generalizations of these questions to reasonable questions about $\mathrm{Spf}(\mathcal{R}^{(p^n)}$? See below.

We wonder wether every finite group scheme can be "specialized to a product of copies of α_p". Reminder: see (Expectation) (17.4). For a commutative finite group scheme in char zero this is the case. Here is a precise question.

(21.5) Conjecture. Let L_1 be an algebraically closed field of characteristic zero, and $e > 0$. Suppose G is a finite group scheme of rank p^e over L_1. Then (?) there exist an integral domain Δ of characteristic p, a finite flat group scheme $\mathcal{G}$ of rank p^e over Δ, and
(generic fiber) inclusions $\Delta \subset L_2$ and $L_1 \subset L_2$ such that $\mathcal{G} \otimes L_2 \cong G \otimes L_2$

and
(special fiber) a homomorphism $\Delta \to K$ such that $\mathcal{G} \otimes K \cong (\alpha_{p,K})^e$.

(21.6) Let $\mathrm{Spf}(\mathcal{T}^{(p^n)})$ be the "moduli space" in the sense of Section 17 classifying *commutative* group schemes of rank $m = p^n$, with universal object $\mathcal{G}$m-com. Let $\Pi_0(\mathrm{Spf}(\mathcal{T}^{(p^n)}))$ be the set of irreducible components. We expect:

- Every irreducible component T of $\mathrm{Spf}(\mathcal{T}^{(p^n)})$ has its generic point in characteristic zero, i.e. there is a characteristic zero field k such that $\mathrm{Spf}(\mathcal{T}^{(p^n)})(k) \neq \emptyset$.

- Note that for the generic point $\eta \in T$ the geometric fiber $\mathcal{G}_{\overline{\eta}}^{(\text{m-com})}$ is given by a finite commutative p-group N_T. We expect that

  the map from $\Pi_0(\mathrm{Spf}(\mathcal{T}^{(p^n)}))$ to the set of isomorphism classes of finite commutative groups of order $m = p^n$, given by $T \mapsto H_T$ to be bijective

  i.e. if T_1, T_2 are two irreducible components and $N_{T_1} \cong N_{T_2}$ then $T_1 = T_2$.

- Every irreducible component T of $\mathrm{Spf}(\mathcal{T}^{(p^n)})$ admits a point $P_0 \in \mathrm{Spf}(\mathcal{T}^{(p^n)})(K)$ with K algebraically closed of characteristic p and
$$\mathcal{G}_{P_0}^{(\text{m-com})} \quad \cong \quad (\alpha_{p,K})^n .$$

- **Question.** Is every irreducible component T of $\mathrm{Spf}(\mathcal{T}^{(p^n)} \otimes \mathbb{F}_p)$ a reduced scheme?

References

[1] N. Bourbaki – *Eléments de mathématique,* 23. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre 8: Modules et anneaux semi-simples, Actualités Scientifiques et Industrielles, No. 1261, Hermann, Paris, 1958.

[2] Alice Bouillet – *Moduli of Lie p-algebras.* `https://arxiv.org/pdf/2205.00737.pdf`

[3] C.-L. Chai and F. Oort – *Hecke orbits.* To appear.

[4] C.-L. Chai and F. Oort – *Life and work of Alexander Grothendieck.* ICCM Notices **5** (2017), 22–50.

[5] M. Demazure – *Lectures on p-divisible groups.* Lecture Notes in Mathematics, Vol. 302, Springer, Berlin, 1986, Reprint of the 1972 original.

[6] M. Demazure and A. Grothendieck – *Schémas en groupes.* Séminaire de de Géométrie Algébrique du Bois Marie – 1962-64, Vols.I-II-III. Springer-Verlag, 1970, Lecture Notes in Mathematics, **151, 152,153**. `https://webusers.imj-prg.fr/~patrick.polo/SGA3/`

[7] R. Feynman – *'Surely you're joking, Mr. Feynman!' adventures of a curious character.* As told to Ralph Leighton, edited by Edward Hutchings. Unwin, 1985.

[8] E. Goren and M.-H. Nicole – *Lectures on Hilbert modular varieties and modular forms.* CRM Monograph Series, Vol. 14, American Mathematical Society, Providence, RI, 2002.

[9] A. Grothendieck and J. Dieudonné – *Éléments de gomtrie algbrique*: IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie Publications Mathématiques de l'IHÉS, Tome **32** (1967), pp. 5–361.

[10] R. Hartshorne – *Algebraic geometry.* Graduate Texts in Mathematics Vol. **52**, Springer-Verlag 1977.

[11] H. Hasse and E. Witt – *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristiek p.* Monatsh. für Mathematik und Physik **43** (1936), 477–492.

[12] L. Illuse – *Complexe cotangent et déformations. I, II.* Lecture Notes in Math., Vol. **239** Springer-Verlag, Berlin-New York, 1971; Lecture Notes in Math., Vol. **283** Springer-Verlag, Berlin-New York, 1972.

[13] L. Illuse – *Cotangent complex and deformations of torsors and group schemes.* In: Toposes, algebraic geometry and logic. Partial Report on a Conference on Connections between Category Theory and Algebraic Geometry & Intuitionistic Logic, Dalhousie University, Halifax, Nova Scotia, January 16–19, 1971. Edited by F. W. Lawvere. Lecture Notes in Math., Vol. **274**, Springer-Verlag, Berlin-New York, 1972; pp. 159–189.

Illusie, Luc

[14] L. Illuse – *Cotangent complex and deformations of torsors and group schemes.* In: A. Grothendieck and J.L. Verdier, Séminaire de de Géométrie Algébrique SGA4, 1972, Lecture Notes in Math., Vol. **274**, pp. 159-189.

[15] H. Kraft – *Kommutative algebraische p-gruppen.* Mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten. Manuscript, University of Bonn, September 1975; 86 pp.

[16] S. Lang – *Algebra.* Graduate Texts in Mathematics, Vol 211, Springer-Verlag, New York, third ed., 2002.

[17] J.S. Milne – *Arithmetic duality theorems.* Perspectives in Mathematics, Vol. **1**, Academic Press, Inc., Boston, MA, 1986.

[18] B. Moonen – *Group schemes with additional structures and Weyl group cosets.* Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 255–298.

[19] B. Moonen – *A dimension formula for Ekedahl-Oort strata.* Ann. de l'Institut Fourier 54 (2004), 666–698.
`http://www.numdam.org/item/10.5802/aif.2029.pdf`

[20] B. Moonen and T. Wedhorn – *Discrete invariants of varieties in positive characteristic.* IMRN 72 (2004), 3855–3903.

[21] B. Moonen – *Fzips.* To appear.

[22] Draft for a book on abelian varieties.
`https://www.math.ru.nl/~bmoonen/BookAV/BasGrSch.pdf`

[23] D. Mumford – *Selected papers.* Vol. II. On algebraic geometry, including correspondence with Grothendieck. Editors: C.-L. Chai, A. Neeman, T. Shiota. Springer, 2010.

[24] F. Oort – *Commutative group schemes.* Lecture Notes in Mathematics 15, Springer-Verlag 1966.

[25] F. Oort – *Minimal p-divisible groups.* Annals of Math **161** (2005), 1021 – 1036.

[26] F. Oort – *A stratification of a moduli space of abelian varieties.* Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416.

[27] F. Oort – *Simple p-kernels of p-divisible groups.* In: Special volume in honor of Michael Artin: Part I – Edited by Aise Johan De Jong, Eric M. Friedlander, Lance W. Small, John Tate, Angelo Vistoli, James Jian Zhang. Advances in Mathematics **198** (2005), pp. 275 – 310.

[28] F. Oort – *Moduli of abelian varieties in mixed and in positive characteristic.* Handbook of moduli (Eds Gavril Farkas & Ian Morrison), Vol. III, pp. 75–134. Advanced Lectures in Mathematics **25**, International Press, 2013.

[29] F. Oort and D. Mumford– *Deformations and liftings of finite, commutative group schemes.* Invent. Math. **5** (1968), 317–334.

[30] F. Oort – *Did earlier thoughts inspire Grothendieck?* In: Alexandre Grothendieck, A Mathematical Portrait. Edited by Leila Schneps. International Press, 2014; pp. 231–268.

[31] F. Oort – *A method in deformation theory.* In: Papers dedicated to David Mumford, Editors Ching-Li Chai, Amnon Neeman. Pure and Applied Mathematics Quarterly (2021) **17**, 2, p. 703-716

[32] R. Pink – *Finite group schemes.* Lecture course in WS 2004/05, ETH Zürich.
`https://people.math.ethz.ch/~pink/ftp/FGS/CompleteNotes.pdf`

[33] N. Popescu – *Abelian categories with applications to rings and modules.* Academic Press, London-New York, 1973. London Mathematical Society Monographs, No. 3.

[34] B. Riemann – *Theorie der Abel'schen Functionen.* Journ. reine angew. Math. **54** (1857), 101 – 155.

[35] J. Stix – *A course on finite flat group schemes and p-divisible groups.* Heidelberg summer term 2009.
`https://www.uni-frankfurt.de/52288632/Stix_finflat_Grpschemes.pdf`

[36] R. Schoof – *Introduction to finite group schemes,* lecture notes taken by John Voight, October – December 2000.
`https://math.dartmouth.edu/~jvoight/notes/274-Schoof.pdf`

[37] R. Schoof – *Finite flat group schemes over local Artin rings.* Compositio Math. **128** (2001), pp. 1–15.

[38] R. Schoof – *Semistable abelian varieties with good reduction outside 15.* Manuscripta Math. **139** (2012), pp. 49–70.

[39] R. Schoof – *Is a finite locally free group scheme killed by its order?* In: "Open problems in algebraic geometry", Editor F.Oort. Advanced Lectures in Math. 46, International Press, Beijing 2018, 1–7.

[40] *The Stacks project*, an open source textbook and reference work on algebraic geometry.
`https://stacks.math.columbia.edu/`

[41] R. Steinberg – *Endomorphisms of linear algebraic groups.* Memoirs of the American Mathematical Society Volume **1**, 1968. In: R. Steinberg – Collected Papers, Am. Math. Soc., Providence, 1997, pp. 229–285.

[42] J. Tate – *Finite flat group schemes.* In: Cornell, G., Silverman, J.H., Stevens, G. (editors) *Modular forms and Fermat's last theorem.* Springer, 1997; pp. 121–154.

[43] J. Tate and F. Oort – *Group schemes of prime order.* Ann. scient. Ec. Norm. Sup. **3** (1970), pp. 1–21.

[44] W.C. Waterhouse – *Introduction to affine group schemes.* Graduate Texts in Mathematics Vol. **66**, Springer, 1979.

22 Giving a lecture

"Is there a particular example of this general problem?"

Why yes, of course. "Give me one example".

I can't understand anything in general unless I am carrying along in my mind a specific example. When the guy's in the middle of a bunch of equations, I'll say, "Wait a minute! There is an error! That can't be right."

The guy after a while finds the mistake and wonders "How the hell did this guy, who hardly understood at the beginning, find that mistake in the mess of all these equations?"

I have a specific example and I know from instinct and experience the properties of the thing, I know the equation is the wrong way around.

Richard Feynman, [7], pp. 244/245

Suppose you are going to give a lecture about a mathematical topic, or you teach a course for students. Here are some suggestions for rules to be followed (not about the presentation, but about the contents, and the way you explain your material).

- Within the first few minutes of your talk, tell the audience what is the aim of the lecture, a question, a result, or whatever along these lines. – Some talks start with a long series of definitions and lemmas, that usually make no sense to the audience. Start by giving a clear picture of what you are going to do.– Sometimes a list of steps to be taken, or aspects of the topic, helps giving a good structure. In that case after finishing a step you say so, and you announce the next one.

- More generally: at every moment of your talk the audience should receive the information what you are presenting, in which stage of your talk you are.

- Every mathematical talk should contain at least one *proof*. Without some of the people in the audience have no idea whether material presented is easy or difficult. A clear proof indicates what you expect people to understand.

- If possible, give an *example* that is an illustration of what you are doing. Nice trick: if you know you are going to present a hard and difficult proof, first give an easy example, explain well, and you will see that mathematicians recognize later the general pattern of your proof or theorem as a generalization of the example they did understand.

- Try to tell the audience which details of your proofs are easy, which depend on deep abstract facts, and which use complicated arguments like examples, combinatorics and tricks.

- Give the audience possibilities to ask questions; after you answer a question, before proceeding, check whether the person who asked the question did understand your explanation.

- Have a plan in your head: if for some reason you are running out to time (too many questions, or ill-planned schedule), know what you are going to delete, and which important messages you do present in the remaining minutes. – Do not use more time than allowed: an audience loses interest, or people have to go to another urgent meeting, or whatever, if you are still talking after your time slot has ended.

- Take care that you spend the last 5 minutes in giving a survey, give an answer to a question asked in the first minutes, or whatever is necessary to conclude the message you started with. The tail of your talk should abut to the beginning.