Finite commutative group schemes annihilated by p

Frans Oort

Utrecht University

Workshop on Hopf Algebras,
Hanoi, October-November 2023

Introduction.

Topic of this talk: a classification of finite *commutative* group schemes annihilated by p over a perfect field as announced in 1975 by Hanspeter Kraft. This implies that the set of isomorphisms classes of such group schemes of a fixed rank over an algebraically closed field is *finite*. Dieudonné module theory translates this question into:

Study the category of *modules* $M \in \mathcal{M}$ *of finite length* (of finite dimension over k) over the ring $R = k\{\mathcal{F}, \mathcal{V}\}$.

Here k is an algebraically closed field of characteristic p, and

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

Strategy for the proof

Theorem (Krull-Remak-Schmidt). *Let R be a ring. Consider left-R-modules that are noetherian and artinian* (i.e. satisfying the ascending and descending chain condition). *Such a module can be written as sum of indecomposable modules, and if we have two such decompositions*

$$M \cong \sum_{i \in I} \quad M_i^{(1)} \cong \sum_{j \in J} \quad M_j^{(2)}$$

then there exists a bijection $f : I \to J$ and isomorphism $M_i^{(1)} \cong M_{f(i)}^{(2)}$. (A proof is not very difficult.)

We write $\mathcal{M}$ for the category of modules of finite length (of finite dimension over k) over the ring $R = k\{\mathcal{F}, \mathcal{V}\}$.

Which are the indecomposable objects in $\mathcal{M}$?

An object $0 \neq M$ in an abelian category is *simple* if $0 \subset P \subsetneq M$ implies $0 = P$.
An object $0 \neq M$ in an abelian category is *indecomposable* if $M = P' \oplus P''$ implies either $M = P'$ or $M = P''$.

Example. In the category of finite abelian groups the simple objects are $\mathbb{Z}/p$, where p is a prime number, and the indecomposable objects are $\mathbb{Z}/(p^n)$.

We are going to show properties of Dieudonné modules:

(A) Construct candidates for indecomposable modules in $\mathcal{M}$, bellow introduced as M'_u and M_w.

(D) Then show these are indeed indecomposable,

(E) and prove these are all possible indecomposable modules.

Hanspeter Kraft, 1944 –

Theorem. Every $M \in \mathcal{M}$ decomposes as

$$M = (\oplus_{u \in L} \quad M'_u) \bigoplus (\oplus_{w \in C} \quad M_w).$$

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.

BT$_1$-modules

Remark / Definition. For a module over $k\{\mathcal{F},\mathcal{V}\}$ we have $\mathcal{V}(M) \subset \mathrm{Ker}(\mathcal{F})$ 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; BT$=$ Barsotti-Tate, and we consider BT-modules "truncated at level one".

We will see that indecomposable BT$_1$-modules on the one hand, and indecomposable modules with $\mathcal{V}(M) \subsetneqq \mathrm{Ker}(\mathcal{F})$, "linear modules" will play different roles.

Comment.

The theorem described today was announced in a preprint by Hanspeter Kraft in 1975.
His idea basically is precise and turns out to be correct.
In that preprint proofs seem to be not complete.

For BT_1 group schemes proofs have been given (FO, Ben Moonen).

A complete proof for the general case will appear soon.
Contemplate. Is this an interesting question? In mathematics some problems are more interesting than others. From the classification given in this talk finiteness follows, and we will comment later how this is used in geometry.

A crucial observation: for any abelian variety A the kernel $A[p] = \mathrm{Ker}([p] : A \to A)$ (all "scheme theoretic p-torsion points") is a BT_1 group scheme. Classification of such group schemes provides us with an (important !) invariant for A.

Notation. Consider $0 \neq x \in M$. We write:

- $\mathcal{F}x$ if $x \in \mathrm{Image}(\mathcal{F})$: $\quad \exists y \in M\colon\ y \overset{\mathcal{F}}{\mapsto} x$;
- $\mathcal{V}x$ if $x \notin \mathrm{Ker}(\mathcal{V})$: $\quad 0 \neq \mathcal{V}(x) \overset{\mathcal{V}}{\mapsfrom} x$;
- $\emptyset x$ if $x \notin \mathrm{Image}(\mathcal{F})$ and $\mathcal{V}(x) = 0$;
- $x\mathcal{F}$ if $x \notin \mathrm{Ker}(\mathcal{F})$: $\quad x \overset{\mathcal{F}}{\mapsto} \mathcal{F}(x) \neq 0$;
- $x\mathcal{V}$ if $x \in \mathrm{Image}(\mathcal{V})$: $\quad \exists z \in M\colon\ x \overset{\mathcal{V}}{\mapsfrom} z$;
- $x\emptyset$ if $x \notin \mathrm{Image}(\mathcal{V})$ and $\mathcal{F}(x) = 0$;

note the direction of the arrows:

$$\boxed{\text{$\mathcal{F}$ points to the right, $\mathcal{V}$ points to the left.}}$$

As $\mathcal{F}\mathcal{V} = 0 = \mathcal{V}\mathcal{F}$ we have $\mathrm{Ker}(\mathcal{V}) \subset \mathcal{F}(M)$ and $\mathrm{Ker}(\mathcal{F}) \subset \mathcal{V}(M)$.

Example. We consider $\mathcal{F}x$, i.e. $x \in \mathrm{Image}(\mathcal{F})$;

this means $\exists y \in M$ with $y \overset{\mathcal{F}}{\mapsto} x$, and
it implies $\mathcal{V}(x) = 0$. We determine all possibilities in this case.

There are three possibilities:

- $x = \mathcal{V}(z)$, then $\mathcal{F}(x) = 0$, we write:
  $\boxed{\mathcal{F}x\mathcal{V}, \quad y \overset{\mathcal{F}}{\mapsto} x \overset{\mathcal{V}}{\mapsfrom} z;}$
  if $x \notin \mathrm{Image}(\mathcal{V})$, then either $\mathcal{F}(x) \neq 0$ or $\mathcal{F}(x) = 0$;
- $\mathcal{F}(x) \neq 0$, then $x \notin \mathrm{Image}(\mathcal{V})$, we write:
  $\boxed{\mathcal{F}x\mathcal{F}, \quad y \overset{\mathcal{F}}{\mapsto} x \overset{\mathcal{F}}{\mapsto} \neq 0;}$
- $x \notin \mathrm{Image}(\mathcal{V})$ and $\mathcal{F}(x) = 0$, we write
  $\boxed{\mathcal{F}x\emptyset \quad y \overset{\mathcal{F}}{\mapsto} x \overset{\mathcal{F}}{\mapsto} (= 0), x \overset{\mathcal{V}}{\mapsto} (= 0).}$

I.e. in this case the possibilities are: $\mathcal{F}x?$ with $? \in \{\mathcal{V}, \mathcal{F}, \emptyset\}$.

We list al possibilities:

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

Conclusion: $L_1 x L_2$, with $L_1, L_2 \in \{\mathcal{F}, \mathcal{V}, \emptyset\}$, describes all possibilities for $0 \neq x \in M$ (nine possibilities).

Please understand and remember this. These considerations will be used later in the construction of *directed graphs*.

(A) Construction of M'_u, linear words.

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".

Some properties of M'_u.

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. *For every word u, and $M = M'_u$, we have*

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

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 $z_1 \in \mathrm{Ker}(\mathcal{F})$.

Observe that in the category of modules in $\mathcal{M}$ with $\mathcal{F}$ and $\mathcal{V}$ nilpotent the module $M'_\emptyset = \mathbb{D}(\alpha_p)$ is the unique simple object.

(A) Construction of M_w, circular words.

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

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

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 $M_{\lfloor w \rceil}$.
Notation, sometimes we write M_w instead.

Some properties of M_w.

- The objets $M_{\mathcal{F}} = \mathbb{D}(\mu_p)$ and $M_{\mathcal{V}} = \mathbb{D}(\underline{\mathbb{Z}/p})$ are simple objects in $\mathcal{M}$.
- Every M_w is a BT_1-module.
- If $\mathcal{F}$ and $\mathcal{V}$ both appear in w then M_w is local-local, i.e. $\mathcal{F}$ and $\mathcal{V}$ are nilpotent on M.
- 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 $w' = w^d$.

Plan. Show:

(Du) Every M'_u is indecomposable.

(Dw) For every indecomposable circular word w the module M_w is indecomposable.

- For every indecomposable $M \in \mathcal{M}$ either $\exists u\colon\ M \cong M'_u$, or $\exists w\colon\ M \cong M_w$.

Difficulties.

- Decomposition in indecomposables is far from unique.
- In general there are many homomorphism $M'_u \to M_w$ and $M_w \to M'_u$.
- Perhaps there are direct proofs for (Du) and for (Dw), but these seems complicated.
- Given $M \in \mathcal{M}$ how do you recognize which u and w are needed for the decomposition in indecomposables?

The problems:

- Indecomposability,
- recognize which u and w appear for a given $M \in \mathcal{M}$

seem hard under direct approach. After the break I will discuss a tool, **(B)** *canonical filtrations*, that gives access to these questions.

Please note:

- For a given $M \in \mathcal{M}$ the decomposition isomorphism is in general far from unique.
- There is no canonical maximal BT_1 submodule in M, there is no canonical maximal direct sum of M'_u inside M.
- However, we will see, and this is also clear from the Krull-Remak-Schmidt theorem once we have proved our main result, that for a given M the set of linear words u and the indecomposable circular words w needed is unique. We construct a method to find these sets of words needed for a given M.

Interesting, not discussed in my talk: consider $\mathcal{M}^{\mathrm{BT}} \subset \mathcal{M}$, the category of BT_1-modules. We will see that in this additive category in general the kernel of homomorphism and the cokernel of a homomorphism are not in this category (give examples).

We have seen objects $M_{\mathcal{F}}$ and $M_{\mathcal{V}}$, simple in $\mathcal{M}$ and simple in $\mathcal{M}^{\mathrm{BT}}$.

However $M'_{\emptyset}$ is not in $\mathcal{M}^{\mathrm{BT}}$.
What are the objects simple in $\mathcal{M}^{\mathrm{BT}}$?
A complete classification is known, but it is not easy to describe, and a proof of that classification requires soms work.
If you feel like thinking about this, consider a possible proof for:

$M_{[\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}]}$ is not simple in $\mathcal{M}^{\mathrm{BT}}$,

can you give an inclusion $M_{[w']}$ into this module? But

$M_{[\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{F}\mathcal{V}]}$ is simple in $\mathcal{M}^{\mathrm{BT}}$.

You obtain a feeling for this subtlety.
The notion " simple in $\mathcal{M}^{\mathrm{BT}}$ " will not be used today.

Exercises. Work over $k = \overline{k} \supset \mathbb{F}_p$.
1) Classify all $M \in \mathcal{M}$ with $\mathcal{F}$ and $\mathcal{V}$ nilpotent and $\dim_k(M) = 2$ (you did this already in this workshop, please refresh).

2) Give a bijection $\mathrm{Ext}(M'_\emptyset, M'_\emptyset) = k^2$.
You see this Ext-group is an infinite set. Does this contradict finiteness of isomorphism classes of all M with $M/M'_\emptyset \cong M'_\emptyset$? Explain! and understand.
I will give comments after the break.

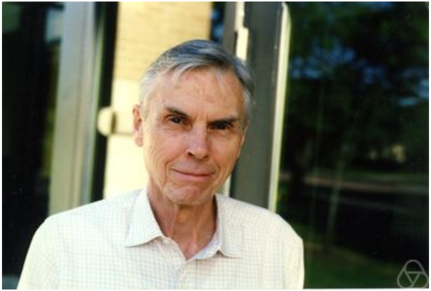
In case you have more time left, you can consider:

3) 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 $\mathcal{M}^{\mathrm{BT}}$.

4) Choose $u = \mathcal{V}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}$; show $P := M'_u$ is indecomposable.
(It seems this gives a hint how to prove indecomposablity directly.)

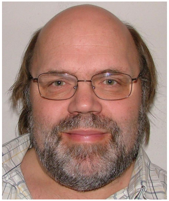
Now we have a BREAK after the first part.

John Tate, 1925 – 2019



John Tate had an impressive influence on developments in arithmetic geometry. For me it was wonderful to be present at a course Tate taught in 1966-1967 at Harvard University, where one of the aims was the classification of group schemes of prime order. Another idea developed by Tate, and also by Barsotti, was the construction of p-divisible groups; their properties are of crucial influence in many considerations of geometry, arithmetic and number theory. I have warm and intense memories to this extraordinary person and great mathematician.

Torsten Ekedahl, 1955 – 2011



In 1985 Torsten Ekedahl discussed an idea with me: For every abelian variety A classify the isomorphism classes $A[p^\infty]$. His idea was the starting point that *the stratum of all abelian varieties with mutually isomorphic p-kernels should be quasi-affine.*

We got stuck in various stages of the this process. One of the obstacles was the result described in this talk. In 2000 finally, details were completed, and Torsten did choose that I should write the publications (2000) under my name only. The result is a stratification, now called the EO-stratification (finite by the results presented today) of $\mathcal{A}_{g,1} \otimes \mathbb{F}_p$; the boundary of every positive dimensional stratum is a union of smaller strata: it looks like a cell decomposition as constructed in manifolds. Many results have been proved using this stratification.

An aside. Minimal p-divisible groups.
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

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

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.

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. And Mumford answered: 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 this topic

The *p*-divisible groups for which $X[p] \cong Y[p]$ implies $X \cong Y$ I 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 characteristic p by isomorphism classes of $A[p^\infty]$. Moreover:

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.

An example.
We show that $M = M_{[\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}]}$ is not simple in $\mathcal{M}^{\mathrm{BT}}$.

Write $z_1\mathcal{F}z_2\mathcal{F}z_3\mathcal{F}z_4\mathcal{F}z_5\mathcal{V}z_6\mathcal{F}z_7\mathcal{V}z_1$.

Note $z_3 \overset{\mathcal{F}}{\mapsto} z_4 \overset{\mathcal{F}}{\mapsto} z_5 \overset{\mathcal{V}}{\mapsfrom} z_6$, and $\mathcal{V}(z_3) = 0 = \mathcal{F}^2(z_6)$.

Choose $P = M_{[\mathcal{F}\mathcal{F}\mathcal{V}]}$ generated by $e \in P$ with $\mathcal{F}^2(e) = \mathcal{V}(e)$.

We define $\varphi : P \hookrightarrow M$ by $\varphi(e) = z_3 + z_6$.
Indeed

$$\varphi(\mathcal{F}^2(e)) = \mathcal{F}^2(z_3 + z_6) = z_5 =$$

$$= z_5 = \mathcal{V}(z_6) = \mathcal{V}(z_3 + z_6) = \varphi(\mathcal{V}(e))).$$

Comments on two of the excercices.
1) All $M \in \mathcal{M}$ with $\mathcal{F}$ and $\mathcal{V}$ nilpotent and $\dim_k(M) = 2$
2) Give a bijection $\mathrm{Ext}(M'_\emptyset, M'_\emptyset) = k^2$.

We know there exist $k{\cdot}e = M'_\emptyset \subset M$. Choose $h \in M$ with $h \notin k{\cdot}e$. The structure of M is defined by $\mathcal{F}(h) = b{\cdot}h$ and $\mathcal{V}(h) = c{\cdot}h$.

Indeed an extension, $P' = k{\cdot}e$,
$M/(k{\cdot}e) \cong P'' = k{\cdot}(f \bmod k{\cdot}e) \cong M'_\emptyset$ is given by any $(b, c) \in k^2$.

The action of $\mathrm{End}(k{\cdot}e) \times \mathrm{End}(P'')$ has four orbits. The set of extensions is *not finite*; the set of isomorphism classes of such M has cardinality 4; orbits:
$(b, c) = (0, 0)$, then $M \cong P' \oplus P''$;
$b = 0, c \neq 0$ then $M \cong M'_\mathcal{V}$;
$b \neq 0, c = 0$ then $M \cong M'_\mathcal{F}$;
$b \neq 0, c \neq 0$ then $M \cong M_{\mathcal{F}\mathcal{V}}$.

We start with: **(B)** *canonical filtrations*

A flag

$$S_* = (0 =\subsetneqq S_1 \subsetneqq \cdots \subsetneqq S_i \subsetneqq S_{i+1} \cdots S_r = M)$$

of Dieudonné submodules is called *saturated* if two conditions are fulfilled: 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

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

(B) Construction of the canonical filtration

For a filtration S_* we use the following operations:

- $(F)(S_*)$: add all $S_i + (\mathcal{F}(S_j) \cap S_{i+1})$ 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:

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

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 $A_t := F^t M$ 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 $(V^{-1}\text{-}F)(S_*)$ 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.

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

Observation. For a direct sum $M = P' \oplus P''$ the canonical filtration of M can be given by constructing the canonical filtrations of P' and P'' separately.

Tool: Directed graphs

Suppose given M and *saturated* flag R_* of Diedonné submodules in M. We define a *directed graph* $\Gamma(R_*)$, remember the possibilities LxL', with $L, L' \in \{\mathcal{F}, \mathcal{V}, \emptyset\}$:

- 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

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

  for any bijective map

  $\mathcal{V} : (R_{i+1}/R_i) \overset{\sim}{\to} (R_{j+1}/R_j)$ an edge is given by $i \mapsfrom j$ with label V.
- Note the direction of the arrows: the last one could also better be baptized, or understood as V^{-1}.

(C) The associated graded

For a given M and a flag R_* of Diedonné submodules in M define

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

As we supposed R_* is saturated, in this case the maps induced by $\mathcal{F}$ and $\mathcal{V}$ on these subquotients give $\mathcal{G}(R_*)$ the structure of a Dieudonné module.

Observation. Suppose $M = P' \oplus P''$ and consider the canonical filtration $Q_*(M)$. Then

$$\mathcal{G}(Q_*(M)) \cong \mathcal{G}(Q_*(P')) \oplus \mathcal{G}(Q_*(P''))$$

A priority, there is no obvious map $M \to \mathcal{G}(M)$ and no obvious $M \leftarrow \mathcal{G}(M)$

Observation. The Dieudonné modules M and $\mathcal{G}(Q_*(M))$ have equal directed graphs

$$\Gamma(Q_*(M)) = \Gamma(\mathcal{G}(Q_*(M)).$$

(D) Indecomposable modules

Proposition. *For every linear word the module M'_u is indecomposable.*
For every indecomposable circular word w the module M_w is indecomposable.

We indicate a proof, leaving out details that can be easily filled in.

Consider $M = M'_u$, and consider the canonical filtration $Q_*(M)$. Observe that $\Gamma(Q_*(M))$ is *connected*: "following the word" u all steps in the filtration are connected by a string of bijections $\mathcal{F}$ and $\mathcal{V}$. If $M = M'_u = P' \oplus P''$ with non-zero summands, then we would have

$$\Gamma(Q_*(M)) = \Gamma(Q_*(P')) \sqcup \Gamma(Q_*(P'')),$$

a contradiction.
Arguments for indecomposability of M_w for an indecomposable w follow the same pattern.

An aside.

In this talk we leave out some technical details, not very important for understanding the general pattern.

Filtrations can be refined. A final filtration is a saturated filtration where all subquotients have dimension one.

Every saturated filtration of M can be refined to a final filtration.

In general there are many final filtrations of M. However the associated graded of two final filtrations are canonically isomorphic. In this way ons shows that, although $(V^{-1}\text{-}F)$ and $(F^{-1}\text{-}V)$ may give different filtrations, refining to final filtrations give "the same" up to a permutation of the steps. Hence, without fear for confusion we can write $\Gamma(M)$, constructions with possible different final filtrations.

The concept $\Gamma(M)$ attached to M is canonical.

Suggestion. If you want to become familiar with canonical filtrations, work out some easy examples, e.g. $Q_*(M_{[\mathcal{F}\mathcal{V}\mathcal{F}\mathcal{V}]})$, $Q_*(M'_{\mathcal{F}\mathcal{F}\mathcal{V}})$, $Q_*(M'_{\mathcal{F}} \oplus M'_{\mathcal{V}} \oplus M_{[\mathcal{F}\mathcal{V}]})$.

Semilinear maps. 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

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

Some excercises.

5) Consider over a field K the matrix

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

5a) Show there does not exist a matrix S with $S^{-1}AS = \mathrm{Diag}(1,1)$.

5b) Suppose $K = k \supset \mathbb{F}_p$ algebraically closed and $q = p^e$. Show for any non-zero $\lambda_1, \lambda_2 \in k$ there exists

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

6) Consider $M := M'_\emptyset \oplus M'_\mathcal{F}$.

(6.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.

(6.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. *Now a BREAK after part two.*

Tool: Semilinear maps

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

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

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

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*

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

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.

Proof of the (Hasse-Witt, Lang-Steinberg)-theorem.
Write $G = \mathrm{GL}_d(k)$.

For any $X \in G$ consider $f_X : \mathrm{G}(k) \to \mathrm{G}(k)$ given by $f_X(U) = U^{-1}XU^{(q)}$

For any $U \in \mathrm{G}(k)$ consider the induced map on tangent spaces

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

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 $X \in G(k)$.

We apply this with $X = A$ and with $X = \mathbf{1}_d$, proving

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

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.

Impressive. The original proof in 1936 by Hasse-Witt is hard, but modern algebraic geometry (including the notion Zariski topology) provides us with an elegant short argument.

(E) Theorem. $\mathcal{G}(M) \cong \left(\bigoplus_{i\in L} M'_{u_i}\right) \bigoplus \left(\bigoplus_{j\in C} M_{\lfloor w_j \rceil}\right).$

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

We consider the canonical filtration $Q_* = Q_*(M)$, and we write $\mathcal{G}(M) = \mathcal{G}(Q_*(M))$.

Consider $\Gamma = \Gamma(Q_*(M))$, the directed graph defined by he saturated flag Q_*. Write

$$\Gamma(Q_*(M)) = \bigsqcup_s \Gamma_s,$$

a disjoint union of connected graphs. Every Γ_s is either a linear graph or a circular graph. Note that $\mathcal{G}(M)$ splits accordingly.

Proposition. **(a)** *For one index s, all subquotients in Γ_s in the filtration $Q_*(M)$ have the same dimension;* write d_s for this dimension.

(b) *Suppose Γ_s is a linear graph;* write u_s for the linear word given by this directed graph. *The corresponding summand of $\mathcal{G}(M)$ is isomorphic with $(M'_{u_s})^{d_s}$.*

(c) *Suppose Γ_s is a circular graph; then the associated circular word u_s is indecomposable and the corresponding summand of $\mathcal{G}(M)$ is isomorphic with $(M_{w_s})^{d_s}$.*

Proof. All steps in the flag $Q_*(M)$ associated with Γ_s are connected by bijective (semilinear) maps, hence they all have the same dimension. This proves (a).

Suppose $Q_j \subsetneqq Q_{j+1}$ is the step in the flag defined by the beginning of the word u_s. Choose a k-basis $\{z_{s,1,1}, \cdots, z_{s,1,d_s}\}$ for the k-vector space Q_{j+1}/Q_j. Following the word u_s and using the semilinear bijections in the saturated $Q_*(M)$ we make bases

$$\{z_{s,r,1}, \cdots, z_{s,r,d_s} \mid 1 \le r \le \mathrm{length}(u_s) + 1\}$$

for all subquotients of steps in $Q_*(M)$ associated with u_s. This proves (b).

Suppose $Q_j \subsetneqq Q_{j+1}$ is the step in the flag by one step defined by the circular word w_s. Suppose $\mathrm{length}(w_s) = h_s$; write $q = p^{h_s}$. Following the word w_s, we have a sequence of semilinear bijective maps, and we obtain a q-semilinear bijetive endomorphism

$$\varphi : Q_{j+1}/Q_j \quad \xrightarrow{\sim} \quad Q_{j+1}/Q_j.$$

By the (Hasse-Witt, Lang-Steinberg)-theorem we can diagonalize this map: we choose a basis for Q_{j+1}/Q_j on which φ is the identity. From here we follow the proof of (b): follow w_s, produce bases in all steps, finally coming back to the starting step with the same basis as we started. This proves (c).

Conclusion. This proves

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

Discussion

Up to here we have described the decomposition in indecomposables of $\mathcal{G}(M)$.
But does this give information about the same for M?
For every $Q_j \subsetneqq Q_{j+1}$ we have a canonical map

$$Q_{j+1} \twoheadrightarrow Q_{j+1}/Q_j \subset \mathcal{G}(M).$$

(E) BB Theorem (the splitting isomorphism). *These canonical maps can be splitted in such a way that these give an isomorphism of Dieudonné modules*

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

A proof is not easy (this fact is stated in the preprint by Kraft, but I cannot find a proof there.) Time permitted, I will show one of the details.

Corollary. *For every indecomposable $M \in \mathcal{M}$*

$$\textit{either } \exists u\colon\ M \cong M'_u, \textit{ or } \exists w\colon\ M \cong M_w.$$

Proof. Choose $\mathcal{G}(M)$. This Diedonné module is a direct sum as indicated above, hence by the isomorphism in the splitting isomophism theorem we obtain a decomposition of M. As M is indecomposable there is only one summand, and this is either of the shape M'_u or of the shape M_w.

Comment. You might complain that this seems a rather complicated proof. However I do not know a short, simple argument to prove this corollary. For example: suppose $\mathcal{G}(M) \cong M_{w_1} \oplus M_{w_2}$; how do you show that M is decomposable (moreover in the same way)? This has been solved, but the proof is somewhat involved.

Perhaps you can work out the general case.

We had the exercise:
4) *Choose* $u = (\mathcal{V}\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{F})$*; show* $P := M'_u$ *is indecomposable.*
Let us try. Write $z_1\mathcal{V}z_2\mathcal{F}z_3\mathcal{F}z_4\mathcal{V}z_5\mathcal{F}z_6$.

$$z_1 \overset{\mathcal{V}}{\mapsfrom} z_2 \overset{\mathcal{F}}{\mapsto} z_3 \overset{\mathcal{F}}{\mapsto} z_4 \overset{\mathcal{V}}{\mapsfrom} z_5 \overset{\mathcal{F}}{\mapsto} z_6.$$

Note z_2 and z_5 are “top elements”; these generate the Dieudonné module M.

If there is an indecomposable summand $P' \subset P$ containing z_2 and z_5 then $P' = P$.

Otherwise there are two indecomposable summands P', and P'' both with non-empty intersection with $kz_2 + kz_5$. Suppose $bz_2 + cz_5 \in P'$ with $b \neq 0$ then $\mathrm{rank}(P') \geq 4$ and $dz_2 + ez_5 \in P''$ with $e \neq 0$ or $d \neq 0$ then $\mathrm{rank}(P'') \geq 3$. The contradiction $4 + 3 > 6 = \mathrm{rank}(P)$ finishes the proof.

It seems this gives a hint how to prove indecomposablity of any M'_u directly.

We give rough sketch of one detail of a proof of the splitting theorem.

Assume Q_* is refined to a final filtration S_* of M and suppose a connected component Γ' of $\Gamma = \Gamma(S_*) = \Gamma(M)$ is connected with a linear word u (and steps in the filtration of dimension one). In this case

$M'_u \cong P' \subset \mathcal{G}(M)$ can be lifted to a direct summand of M, the lifting being compatible with the canonical maps

$$Q_{j+1} \twoheadrightarrow Q_{j+1}/Q_j \subset \mathcal{G}(M).$$

First step. Show that in the canonical filtration, starting with (V^{-1}-F), all $A_t := F^tM$ appear as submodules in Q_*. Hence the same holds for a final refinement.

Second step. We construct a lifting $\mathcal{G}(M) \supset M'_u \hookrightarrow M$.
Define M'_u by $M'_u = \sum_{1 \leq i \leq h+1} \ \ k{\cdot}z_i$. Lift the last z_{h+1} to y_{h+1} in M. Construct $\{y_h, y_{h-1}, \cdots, y_1\}$ inductively by "following the word": where $\mathcal{V}$ appears in the word, take the image, where $\mathcal{F}$ appears use the the first step and lift.
Check: this set of elements $\{y_{h+1}, y_h, \cdots, y_1\} \subset M$ constructs the lifting $P' \subset \mathcal{G}(M)$ we are looking for.

Third step. Use Cartier duality. Check that $(M'_u)^D = M'_{u^D}$; here u^D is the word obtained from u by changing $\mathcal{F} \mapsto \mathcal{V}$ and $\mathcal{V} \mapsto \mathcal{F}$.

Fourth step. Using the second step construct a lifting $\mathcal{G}(M^D) \supset (M'_u)^D \hookrightarrow M^D$ (check all compatibilities). This results in a contraction

$$\left((M'_u)^D \hookrightarrow M^D\right)^D = \left(M'_u \leftarrow M = M^{DD}\right).$$

This proves $M'_u \cong P' \subset \mathcal{G}(M)$ can be lifted to a direct summand of M.

Finale

We have seen:

- A construction of indecomposable modules M'_u and M_w is easy and direct.
- Then construct the canonical filtration and study properties, especially the fact that $Q_*(M)$ is saturated.
- Then prove that the associated graded $\mathcal{G}(M)$ splits into indecomposables (not difficult).
- The non-trivial theorem $M \xleftarrow{\sim} \mathcal{G}(M)$ finishes the proof.

After progressing through all steps indicated we have proved the theorem that any Dieudonné module $M \in \mathcal{M}$ admits a decomposition in indecomposable modules:

$$M \cong \left(\oplus_{i\in L} \quad M'_{u_i}\right) \bigoplus \left(\oplus_{j\in C} \quad M_{\lfloor w_j \rceil}\right).$$

If you want further study, please look at *stratifications and foliations in moduli spaces*, and related questions.
References to be found in the notes.

If you have any further questions, do not hesitate to contact me

f.oort@uu.nl

Thank you for your attention.

I thank the organizers for the invitation to give these talks,
I thank Dr Trung Hieu Ngo for assistance in many ways, and
I thank Dr Dao Van Thinh for sharing with me this talk in guiding you through the exercises.

Wish all of you a nice workshop and a happy future in our beautiful mathematical profession.