Dieudonné modules and \( p \)-divisible groups

Patrick Walls

University of Toronto

April 18, 2013


Our notation for certain categories:

- (Ab) - abelian groups
- (R-Alg) - $R$-algebras
- (R-Mod) - left $R$-modules
- (Mod-R) - right $R$-modules
- (Sch/R) - schemes over Spec $R$
- (GrSch/R) - (commutative) group schemes over Spec $R$

Common group schemes:

\[ \mathbb{G}_a/R : (R\text{-Alg}) \to (\text{Ab}) : A \mapsto (A, +) \]
\[ \mathbb{G}_m/R : (R\text{-Alg}) \to (\text{Ab}) : A \mapsto (A^\times, \times) \]
\[ \mu_{n/R} = \ker(\mathbb{G}_m/R \to \mathbb{G}_m/R : x \mapsto x^n) \]
\[ (\mathbb{Z}/n\mathbb{Z})_R : (R\text{-Alg}) \to (\text{Ab}) : A \mapsto (\mathbb{Z}/n\mathbb{Z})_{\pi_0(\text{Spec } A)} \]
The Witt ring scheme is denoted

\[ \mathcal{W} : \text{(Rings)} \longrightarrow \text{(Rings)} \]

and the Witt scheme of length \( n \) is denoted \( \mathcal{W}_n \).

For example,

\[
\begin{align*}
\mathcal{W}(\mathbb{F}_p) & \cong \mathbb{Z}_p \\
\mathcal{W}(\mathbb{F}_p^n) & \cong \mathbb{Z}_{p^n} \\
\mathcal{W}(\overline{\mathbb{F}}_p) & \cong \widehat{\mathbb{Z}}^\text{un}_{p} \\
\mathcal{W}_n(\mathbb{F}_p) & = \mathbb{Z}/p^n\mathbb{Z}
\end{align*}
\]
Let $k$ be a perfect field of characteristic $p$ with Witt ring $W = \mathbb{W}(k)$.

1. Every group scheme $G$ over $k$ has a Frobenius morphism $F_G$.
2. By Cartier duality, $G$ also has the Vershiebung morphism $V_G$.
3. The category of finite group schemes over $k$ decomposes according to the action of $F_G$ and $V_G$.
4. $G \mapsto M(G) = \lim_n \text{Hom}(G, \mathbb{W}_n)$ is an equivalence between the category of finite group schemes over $k$ killed by some power of $V$ and a full subcategory of Dieudonné modules.
5. The construction extends to an equivalence between the category of finite $p$-torsion group schemes over $k$ and the category of Dieudonné modules of finite length.
6. $p$-divisible groups are limits of finite $p$-torsion group schemes and so the equivalence of the category of $p$-divisible groups onto the category of Dieudonné modules over $k$ is

$$\lim \rightarrow G_i \leftrightarrow \lim \leftarrow \text{M}(G_i)$$
The (Relative) Frobenius $F_X$

The Frobenius map $\sigma : k \to k : x \mapsto x^p$ defines a map on $\text{Spec } k$ and, given any scheme $X$ over $\text{Spec } k$, let $X^{(p)} = X \times_{\text{Spec } k, \sigma} \text{Spec } k$.

The absolute Frobenius map $\sigma_X$ on $X$ is the identity on the topological space $X$ and on the structure sheaf is $\mathcal{O}_X \to \mathcal{O}_X : f \mapsto f^p$.

**Definition**

The **(relative) Frobenius morphism** $F_X : X \to X^{(p)}$ is given by the diagram

![Diagram](image)
The Frobenius morphism commutes with fiber products therefore, if $G$ is a group scheme over $k$, then $G^{(p)}$ has the structure of a group scheme and the Frobenius $F_G : G \longrightarrow G^{(p)}$ is a homomorphism of group schemes over $k$.

For example, if $G = \mathbb{G}_{a/k}$ is the additive group scheme over $k$ then $(\mathbb{G}_{a/k})^{(p)} = \mathbb{G}_{a/k}$ and the Frobenius $F$ acts on $R$-points by

$$F(R) : \mathbb{G}_{a}(R) \longrightarrow \mathbb{G}_{a}(R) : x \mapsto x^p$$

for all $k$-algebras $R$. In fact, we have the following result:

**Proposition**

$\operatorname{End}(\mathbb{G}_{a/k})$ is isomorphic to the noncommutative $k$-algebra $k\{F\}$ generated by $F$ with $F\lambda = \lambda^p F$ for all $\lambda \in k$. 
Exploring the endomorphism ring $k\{F\}$ of $\mathbb{G}_{a/k}$ gives rise to subgroups of $\mathbb{G}_{a/k}$.

Consider $F \in \text{End}(\mathbb{G}_{a/k})$ and $\ker F \subset \mathbb{G}_{a/k}$. This subgroup is denoted $\alpha_{p/k}$ and its $R$-points are given by

$$\alpha_{p/k}(R) = \{x \in R : x^p = 0\}, \text{ for all } k\text{-algebras } R.$$

Since $\alpha_{p/k} = \text{Spec } k[T]/(T^p)$, this is a connected group scheme.
Consider $F - 1 \in \text{End}(\mathbb{G}_{a/k})$ and $H = \ker(F - 1) \subset \mathbb{G}_{a/k}$. The $R$-points of $H$ are

$$H(R) = \{ x \in R : x^p = x \}$$

for all $k$-algebras $R$. This is an étale group scheme since

$$H = \text{Spec} \ k[T] / (T^p - T) = \text{Spec} \ k[T] / \prod_{\lambda \in \mathbb{F}_p} (T - \lambda)$$

$$\cong \bigsqcup_{\mathbb{Z} / p\mathbb{Z}} \text{Spec} \ k$$

$$\cong \left( \mathbb{Z} / p\mathbb{Z} \right)_k.$$
Let $k$ be a perfect field of characteristic $p$ and let $G$ be a finite group scheme over $k$. Then there is a canonical split exact sequence

$$1 \rightarrow G_c \rightarrow G \rightarrow G_e \rightarrow 1$$

where $G_c$ is connected and $G_e$ is étale. In particular, there is an isomorphism

$$G \cong G_c \times G_e$$

For example, the subgroup $H = \ker(F^2 - F) \subset \mathbb{G}_{a/k}$ has the decomposition

$$H \cong \alpha_{p/k} \times \left(\mathbb{Z}/p\mathbb{Z}\right)_k$$

since $F^2 - F = F(F - 1)$. 
**Definition**

Let $G$ be a finite group scheme over $k$. The **Cartier dual of** $G$ is the finite group scheme $G^\vee = \text{Hom}(G, \mathbb{G}_m)$.

In other words, $G^\vee$ is the group scheme defined functorially by

$$G^\vee : (k\text{-Alg}) \rightarrow (\text{Ab}) : R \mapsto \text{Hom}_{(\text{GrSch}/R)}(G_R, \mathbb{G}_m/R)$$

and is represented by the finite $k$-algebra $A^\vee = \text{Hom}_k(A, k)$ where multiplication in the ring $A^\vee$ is defined as the dual of the map $\Delta : A \rightarrow A \otimes_k A$ coming from the group operation $m : G \times G \rightarrow G$.

Furthermore, Cartier duality satisfies

$$(G^\vee)^\vee \cong G \quad \text{and} \quad (G^\vee)^{(p)} \cong (G^{(p)})^\vee.$$
The Verschiebung ("Shift") Morphism $V_G$

**Definition**

Let $G$ be a finite group scheme over $k$. The **Verschiebung morphism** $V_G$ of $G$ is the Cartier dual of the Frobenius $F_{G^\vee}$ on $G^\vee$:

$$ F_{G^\vee} : G^\vee \longrightarrow (G^\vee)^{(p)} = \left( G^{(p)} \right)^\vee \quad \leadsto \quad V_G : G^{(p)} \longrightarrow G $$

**Theorem**

*If $G$ is a finite group scheme over $k$, then*

$$ V_G \circ F_G = p \cdot \text{Id}_G \quad \text{and} \quad F_G \circ V_G = p \cdot \text{Id}_{G^{(p)}}. $$

In fact, for any affine commutative group scheme $G$ over $k$, one can define a morphism $V_G$ satisfying the relations above.
Examples of Cartier Duality

Cartier duality and the Verschiebung operator for the basic finite groups over $k$ are

\[
\begin{array}{c|c|c|c}
G & G^\vee & F_{G^\vee} & V_G \\
\hline
\alpha_p & \alpha_p & F_{\alpha_p} = 0 & V_{\alpha_p} = 0 \\
\mathbb{Z}/p\mathbb{Z} & \mu_p & F_{\mu_p} = 0 & V_{\mathbb{Z}/p\mathbb{Z}} = 0 \\
\mathbb{Z}/\ell\mathbb{Z} & \mu_\ell & F_{\mu_\ell} = \text{isom.} & V_{\mathbb{Z}/\ell\mathbb{Z}} = \text{isom.}
\end{array}
\]

therefore we may distinguish the basic finite group schemes over $k$ by the operators $F$ and $V$

\[
\begin{array}{c|c|c}
G & F_G & V_G \\
\hline
\alpha_p & 0 & 0 \\
\mathbb{Z}/p\mathbb{Z} & \text{isom.} & 0 \\
\mu_p & 0 & \text{isom.} \\
\mathbb{Z}/\ell\mathbb{Z} & \text{isom.} & \text{isom.} \\
\mu_\ell & \text{isom.} & \text{isom.}
\end{array}
\]
The category of finite group schemes over $k$ can be decomposed further by applying the étale-connected dichotomy to Cartier duality . . .

**Definition**

If $G^\vee$ is étale, we say $G$ is **multiplicative**.

If $G^\vee$ is connected, we say $G$ is **unitpotent**.

**Theorem**

- $G$ is étale $\iff F_G$ is an isomorphism
- $G$ is connected $\iff F_G$ is nilpotent
- $G$ is multiplicative $\iff V_G$ is an isomorphism
- $G$ is unipotent $\iff V_G$ is nilpotent
The category of finite group schemes over $k$ decomposes into a product of subcategories

\[(\text{Fem}/k) \times (\text{Feu}/k) \times (\text{Fcm}/k) \times (\text{Fcu}/k)\]

where the four subcategories are

- $(\text{Fem}/k)$ - étale-multiplicative
- $(\text{Feu}/k)$ - étale-unipotent
- $(\text{Fcm}/k)$ - connected-multiplicative
- $(\text{Fcu}/k)$ - connected-unipotent

For example, $\alpha_{p/k} \in (\text{Fcu}/k)$, $(\mathbb{Z}/p\mathbb{Z})_k \in (\text{Feu}/k)$, $\mu_{p/k} \in (\text{Fcm}/k)$ and $(\mathbb{Z}/\ell\mathbb{Z})_k, \mu_{\ell/k} \in (\text{Fem}/k)$ (for $\ell \neq p$).
Let $\mathcal{C}$ be an additive category. For any object $X \in \text{ob}\mathcal{C}$, the set of endomorphisms $\text{Hom}_\mathcal{C}(X, X) = \text{End}(X)$ of $X$ forms a ring $R$ and we get a (covariant) functor

$$h_X : \mathcal{C} \longrightarrow (\text{Mod-}R) : A \mapsto \text{Hom}_\mathcal{C}(X, A)$$

as well as a (contravariant) functor

$$h^*_X : \mathcal{C}^{\text{opp}} \longrightarrow (\text{R-Mod}) : A \mapsto \text{Hom}_\mathcal{C}(A, X).$$

This translates the study of the category $\mathcal{C}$ into $R$-linear algebra!

However, in general, this functor loses a lot of information. The challenge is then to find the right kind of object to capture as much information as possible.
Is there a finite group scheme $G$ over $k$ such that the functor $h^o_G$ defines an equivalence of categories?

No, but we can look at the subcategory of unipotent group schemes and consider the filtration by the subcategories $\mathcal{A}_n$ where $V^n = 0$.

**Theorem**

The category $(\text{UAC}/k)$ of affine unipotent commutative group schemes over $k$ is the limit of subcategories

$$(\text{UAC}/k) = \lim_{\rightarrow} \mathcal{A}_n.$$  

The idea is then to build an equivalence for all finite unipotent group schemes by establishing equivalences for each $\mathcal{A}_n$. 

The Witt scheme $\mathbb{W}_n$ of length $n$ is an affine scheme (of finite type but not finite) such that the Frobenius morphism $F$ and Vershiebung morphisms are in fact endomorphisms

$$F : \mathbb{W}_n \rightarrow \mathbb{W}_n : (a_1, a_2, \ldots, a_n) \mapsto (a_1^p, a_2^p, \ldots, a_n^p),$$

$$V : \mathbb{W}_n \rightarrow \mathbb{W}_n : (a_1, a_2, \ldots, a_n) \mapsto (0, a_1, a_2, \ldots, a_{n-1}).$$

Clearly, $\mathbb{W}_n$ is an object in the category $\mathcal{A}_n$ of affine groups killed by $V^n$, but more importantly . . .

**Theorem**

The Witt group scheme $\mathbb{W}_n$ of length $n$ is an injective cogenerator in $\mathcal{A}_n$. In other words, the functor

$$h^0_{\mathbb{W}_n} : \mathcal{A}_n \rightarrow (\text{End}(\mathbb{W}_n)\text{-Mod}) : G \mapsto \text{Hom}_{\mathcal{A}_n}(G, \mathbb{W}_n)$$

is exact and faithful.
The Endomorphism Ring of $\mathbb{W}_n$

The Frobenius $F$ acts on $\mathbb{W}_n$ by

$$F : \mathbb{W}_n \longrightarrow \mathbb{W}_n : (a_1, a_2, \ldots, a_n) \mapsto (a_1^p, a_2^p, \ldots, a_n^p) ,$$

the Vershiebung operator is the shift

$$V : \mathbb{W}_n \longrightarrow \mathbb{W}_n : (a_1, a_2, \ldots, a_n) \mapsto (0, a_1, a_2, \ldots, a_{n-1})$$

and the Witt ring $W$ of $k$ acts on $\mathbb{W}_n$ by the composition of rings

$$W = W(k) \longrightarrow W(k)/p^nW(k) \cong \mathbb{W}_n(k) \longrightarrow \mathbb{W}_n(R)$$

for all $k$-algebras $R$. This describes the endomorphisms of $\mathbb{W}_n$. 
The Endomorphism Ring of $\mathbb{W}_n$

**Definition**

The Dieudonné ring $\mathcal{D}_k$ is the noncommutative ring over $\mathbb{W}$ generated by $F$ and $V$ subject to the relations

$$F \lambda = \lambda^{(p)} F \quad \text{and} \quad V \lambda^{(p)} = \lambda V \quad \text{for all } \lambda \in \mathbb{W}.$$ 

where $\lambda \mapsto \lambda^{(p)}$ is the Frobenius automorphism of $\mathbb{W}$ (corresponding to $x \mapsto x^p$ on $k$).

The Dieudonné ring packages together the endomorphisms of the Witt schemes $\mathbb{W}_n$ and since we obviously have $V^n$ acting by zero on $\mathbb{W}_n$ we have the following result.

**Proposition**

$$\mathcal{D}_k / \mathcal{D}_k V^n \cong \text{End}(\mathbb{W}_n)$$
An Equivalence for $\mathbb{A}_n$

**Theorem**

The functor

$$h^0_{W_n} : \mathbb{A}_n \rightarrow (\mathcal{D}_k\text{-Mod}) : G \mapsto M(G) = \text{Hom}_{\mathbb{A}_n}(G, W_n)$$

defines an (anti)equivalence between the category of unipotent affine commutative group schemes over $k$ such that $V^n = 0$ and the subcategory of $\mathcal{D}_k$-modules such that $V^n = 0$.

We would like to piece these equivalences together to obtain an equivalence for all unipotent groups. We define

$$\underline{W} : W_1 \xrightarrow{T} W_2 \xrightarrow{T} W_3 \xrightarrow{T} \cdots$$

where $T : W_n \rightarrow W_{n+1} : (a_1, a_2, \ldots, a_n) \mapsto (0, a_1, \ldots, a_{n-1})$. 

Patrick Walls Dieudonné modules and $p$-divisible groups
The Witt ring $\mathcal{W}$ of $k$ acts on $\mathcal{W}_n$ by the composition of rings

$$\mathcal{W} = \mathcal{W}(k) \longrightarrow \mathcal{W}(k)/p^n\mathcal{W}(k) \cong \mathcal{W}_n(k) \longrightarrow \mathcal{W}_n(R)$$

for all $k$-algebras $R$. However, this does not commute with the shift maps defining the limit

$$\mathcal{W} : \mathcal{W}_1 \xrightarrow{T} \mathcal{W}_2 \xrightarrow{T} \mathcal{W}_3 \xrightarrow{T} \cdots$$

We define the twisted action of $\mathcal{W}$ on $\mathcal{W}_n$ by

$$\lambda \ast w = \lambda^{(1-p)}w$$

and this extends to an action of $\mathcal{W}$ on the limit $\mathcal{W}$.

**Proposition**

$$\lim_{\leftarrow n} \mathcal{D}_k/\mathcal{D}_k V^n \cong \text{End}(\mathcal{W})$$
Theorem

The functor

\[ M : (\text{UAC}/k) \longrightarrow (\mathcal{D}_k\text{-Mod}) : G \mapsto M(G) = \lim_{\to} \text{Hom}(G, \mathbb{W}_n) \]

defines an (anti)equivalence between the category of all unipotent affine commutative group schemes over \( k \) and the category of all \( \mathcal{D}_k \)-modules of \( V \)-torsion.

Furthermore, \( G \) is finite if and only if \( M(G) \) has finite \( W \)-length, and

\[
\begin{align*}
G \in (\text{Fcu}/k) & \iff F \text{ is nilpotent on } M(G) \\
G \in (\text{Feu}/k) & \iff F \text{ is bijective on } M(G)
\end{align*}
\]
Extending the Construction to \( (Fcm/k) \)

The construction \( G \mapsto \lim_n \text{Hom}(G, W) \) applies only to unipotent groups but we want to apply it to all \( p \)-torsion groups. To include the category \( (Fcm/k) \) of connected-multiplicative groups, we apply Cartier duality \( G \mapsto G^\vee \) and then apply the functor \( M \). However, this is covariant and we want something contravariant.

For any \( \mathcal{D}_k \)-module \( M \), let \( M^* = \text{Hom}_W(M, W_\infty) \) where

\[
W_\infty = \underbrace{W(k)}_{W_1(k)} \xrightarrow{T} W_2(k) \xrightarrow{T} W_3(k) \xrightarrow{T} \cdots
\]

If \( f \in M^* \), then \((Ff)(m) = f(Vm)^{(p)}\) and \((Vf)(m) = f(Fm)^{(p^{-1})}\).

The functor \( M \mapsto M^* \) is a duality on the category of \( \mathcal{D}_k \)-modules with finite \( W \)-length. For \( G \in (Fcm/k) \), define its Dieudonné module by

\[
M(G) = M(G^\vee)^*.
\]
Equivalence for $p$-Torsion Finite Group Schemes

If $G$ is a finite $p$-torsion group scheme over $k$ then $G = G_u \times G_m$ where $G_u$ is unipotent and $G_m$ is multiplicative and we define

$$M(G) = M(G_u) \oplus M(G_m)^*.$$ 

**Theorem (Dieudonné)**

$$M : (p\text{-fin}/k) \longrightarrow (\mathcal{D}_k\text{-Mod}) : G \mapsto M(G)$$

defines an (anti)equivalence between the category of finite $p$-torsion group schemes over $k$ and the category of all $\mathcal{D}_k$-modules of finite $W$-length. Furthermore,

- $G$ is étale $\iff$ $F$ is bijective on $M(G)$
- $G$ is connected $\iff$ $F$ is nilpotent on $M(G)$
- $G$ is multiplicative $\iff$ $V$ is bijective on $M(G)$
- $G$ is unipotent $\iff$ $V$ is nilpotent on $M(G)$
The Dieudonné modules of the basic finite group schemes over $k$ are

$$M(\alpha_{p/k}) = \mathcal{D}_k / (\mathcal{D}_k F + \mathcal{D}_k V)$$

$$M(\alpha_{p^n/k}) = \mathcal{D}_k / (\mathcal{D}_k F^n + \mathcal{D}_k V) , \quad \alpha_{p^n} = \ker F_{\mathbb{G}_a/k}^n$$

$$M((\mathbb{Z}/p\mathbb{Z})_k) = \mathcal{D}_k / (\mathcal{D}_k (F - 1) + \mathcal{D}_k V)$$

$$M(\mu_{p/k}) = M((\mathbb{Z}/p\mathbb{Z})_k)^* = \mathcal{D}_k / (\mathcal{D}_k F + \mathcal{D}_k (V - 1))$$

$$M(\mathbb{W}_{2,2}) = \mathcal{D}_k / (\mathcal{D}_k F^2 + \mathcal{D}_k V^2)$$
Equivalently, we can describe a Dieudonné module $M$ as a $W$-module equipped with a $\sigma$-linear map $F : M \to M$ and $\sigma^{-1}$-linear map $V : M \to M$ (where $\sigma$ is the Frobenius automorphism of $W$).

For example,

$M(\alpha_{p/k}) = k$ with $F = 0$ and $V = 0$

$M((\mathbb{Z}/p\mathbb{Z})_k) = k$ with $F = \sigma$ and $V = 0$

$M(\mu_{p/k}) = k$ with $F = 0$ and $V = \sigma^{-1}$
A \( p \)-divisible group (or Barsotti-Tate group) over \( k \) of height \( h \) is an inductive system

\[
G = (G_n, i_n) : G_0 \xrightarrow{i_0} G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} \cdots
\]

such that, for each \( n \geq 0 \),

1. \( G_n \) is a finite group scheme over \( k \) of order \( p^{nh} \)
2. the sequence

\[
1 \xrightarrow{} G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}
\]

is exact (in other words, \( G_n \) is isomorphic to \( \ker(G_{n+1} \xrightarrow{p^n} G_{n+1}) \) via the morphism \( i_n \)).
Theorem

The functor

$$\lim_{\to} G_n \leftrightarrow \lim_{\to} M(G_n)$$

defines an (anti)equivalence between the category of p-divisible groups over k and the category of triples $(M, F, V)$ where

1. $M$ is a free $W$-module of finite rank
2. $F : M \to M$ is a $\sigma$-linear map
3. $V : M \to M$ is a $\sigma^{-1}$-linear map
4. $VF = FV = p$

Furthermore,

1. $ht(G) = \text{rank}_W(M(G))$
2. $M(G)/p^nM(G) \cong M(G_n)$
3. $M(G_K) \cong M(G) \otimes_{W(k)} W(K)$ for any perfect extension $K$. 