Dieudonné modules and p-divisible groups

Patrick Walls

University of Toronto

April 18, 2013

References

M. DEMAZURE. *Lectures on p-divisible groups*. Lecture Notes in Mathematics 302, Springer, 1972.

M. DEMAZURE and P. GABRIEL. *Groupes Algébriques*. North Holland Pub. Co., 1970.

A. GROTHENDIECK. *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Les Presses de l'Université de Montréal, 1974.

Y. MANIN. *The theory of commutative formal groups over fields of finite characteristic*. Russian Math. Sur. 18, 1963.

J. TATE. *p-divisible groups*. Proceedings of a Conference on Local Fields, Springer, 1967.

Notation

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:

$$\mathbb{G}_{a/R} : (R\text{-Alg}) \longrightarrow (\text{Ab}) : A \mapsto (A, +)$$

$$\mathbb{G}_{m/R} : (R\text{-Alg}) \longrightarrow (\text{Ab}) : A \mapsto (A^\times, \times)$$

$$\mu_{n/R} = \ker(\mathbb{G}_{m/R} \longrightarrow \mathbb{G}_{m/R} : x \mapsto x^n)$$

$$\underline{(\mathbb{Z}/n\mathbb{Z})}_R : (R\text{-Alg}) \longrightarrow (\text{Ab}) : A \mapsto (\mathbb{Z}/n\mathbb{Z})^{\pi_0(\text{Spec } A)}$$

Witt Rings

The Witt ring scheme is denoted

$$\mathbb{W} : (\text{Rings}) \longrightarrow (\text{Rings})$$

and the Witt scheme of length n is denoted $\mathbb{W}_n$.

For example,

$$\mathbb{W}(\mathbb{F}_p) \cong \mathbb{Z}_p$$

$$\mathbb{W}(\mathbb{F}_{p^n}) \cong \mathbb{Z}_{p^n}$$

$$\mathbb{W}(\overline{\mathbb{F}}_p) \cong \widehat{\mathbb{Z}_p^{\text{un}}}$$

$$\mathbb{W}_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$$

Outline

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. $G \mapsto M(G) = \varinjlim_n \mathrm{Hom}(G, \mathbb{W}_n)$ 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

$$\varinjlim_i G_i \leftrightarrow \varprojlim_i M(G_i)$$

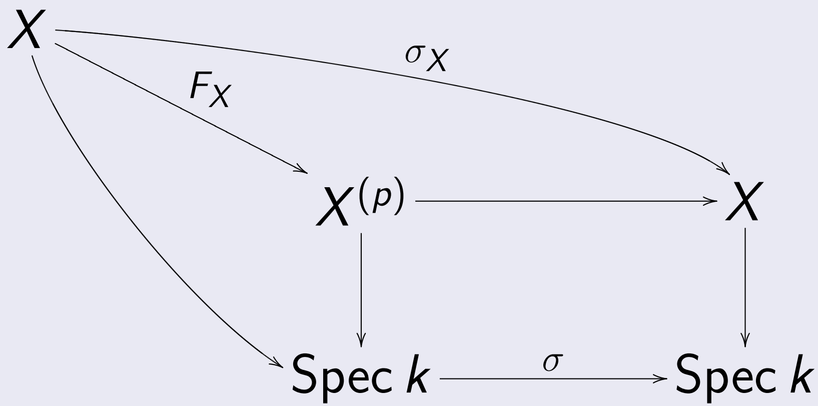
The (Relative) Frobenius F_X

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

The absolute Frobenius map σ_X on X is the identity on the toplogical space X and on the structure sheaf is $\mathscr{O}_X \rightarrow \mathscr{O}_X : f \mapsto f^p$.

Definition

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



The (Relative) Frobenius F_X

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

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 $\lambda \in k$.*

Subgroups of $\mathbb{G}_{a/k}$

Exploring the endomorphism ring $k\{F\}$ of $\mathbb{G}_{a/k}$ gives rise to subgroups of $\mathbb{G}_{a/k}$.

Consider $F \in \mathrm{End}(\mathbb{G}_{a/k})$ 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 $\alpha_{p/k} = \operatorname{Spec} k[T]/(T^p)$, this is a connected group scheme.

Subgroups of $\mathbb{G}_{a/k}$

Consider $F - 1 \in \mathrm{End}(\mathbb{G}_{a/k})$ 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

$$\begin{aligned} H &= \operatorname{Spec} k[T]/(T^p - T) \\ &= \operatorname{Spec} k[T]/\prod_{\lambda \in \mathbb{F}_p} (T - \lambda) \\ &\cong \coprod_{\lambda \in \mathbb{Z}/p\mathbb{Z}} \operatorname{Spec} k \\ &\cong \underline{(\mathbb{Z}/p\mathbb{Z})}_k \ . \end{aligned}$$

Decomposition into étale and connected components

Theorem

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

$$1 \longrightarrow G_c \longrightarrow G \longrightarrow G_e \longrightarrow 1$$

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

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

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

Cartier Duality

Definition

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

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

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

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

Furthermore, Cartier duality satisfies

$$(G^\vee)^\vee \cong G \quad \text{and} \quad (G^\vee)^{(p)} \cong \left(G^{(p)}\right)^\vee .$$

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 $G^\vee$

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

Theorem

If G is a finite group scheme over k, then

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

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

G	$G^\vee$	$F_{G^\vee}$	V_G
α_p	α_p	$F_{\alpha_p} = 0$	$V_{\alpha_p} = 0$
$\mathbb{Z}/p\mathbb{Z}$	μ_p	$F_{\mu_p} = 0$	$V_{\mathbb{Z}/p\mathbb{Z}} = 0$
$\mathbb{Z}/\ell\mathbb{Z}$	μ_ℓ	$F_{\mu_\ell} =$ isom.	$V_{\mathbb{Z}/\ell\mathbb{Z}} =$ isom.

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

G	F_G	V_G
α_p	0	0
$\mathbb{Z}/p\mathbb{Z}$	isom.	0
μ_p	0	isom.
$\mathbb{Z}/\ell\mathbb{Z}$	isom.	isom.
μ_ℓ	isom.	isom.

Decomposing Finite Group Schemes over k

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

$$\begin{aligned}
G \text{ is étale} &\Leftrightarrow F_G \text{ is an isomorphism} \\
G \text{ is connected} &\Leftrightarrow F_G \text{ is nilpotent} \\
G \text{ is multiplicative} &\Leftrightarrow V_G \text{ is an isomorphism} \\
G \text{ is unipotent} &\Leftrightarrow V_G \text{ is nilpotent}
\end{aligned}$$

Decomposing Finite Group Schemes over k

Theorem

The category of finite group schemes over k decomposes into a product of subcategories

$$(\mathrm{Fem}/k) \times (\mathrm{Feu}/k) \times (\mathrm{Fcm}/k) \times (\mathrm{Fcu}/k)$$

where the four subcategories are

(Fem/k) - *étale-multiplicative*
(Feu/k) - *étale-unipotent*
(Fcm/k) - *connected-multiplicative*
(Fcu/k) - *connected-unipotent*

For example, $\alpha_{p/k} \in (\mathrm{Fcu}/k)$, $\underline{(\mathbb{Z}/p\mathbb{Z})}_k \in (\mathrm{Feu}/k)$, $\mu_{p/k} \in (\mathrm{Fcm}/k)$ and $\underline{(\mathbb{Z}/\ell\mathbb{Z})}_k, \mu_{\ell/k} \in (\mathrm{Fem}/k)$ (for $\ell \neq p$).

A General Construction

Let $\mathscr{C}$ be an additive category. For any object $X \in \mathrm{ob}\mathscr{C}$, the set of endomorphisms $\mathrm{Hom}_{\mathscr{C}}(X, X) = \mathrm{End}(X)$ of X forms a ring R and we get a (covariant) functor

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

as well as a (contravariant) functor

$$h_X^o : \mathscr{C}^{\text{opp}} \longrightarrow (R\text{-Mod}) : A \mapsto \mathrm{Hom}_{\mathscr{C}}(A, X) \ .$$

This translates the study of the category $\mathscr{C}$ 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.

In Search of Equivalence: Affine Unipotent Groups

Is there a finite group scheme G over k such that the functor h_G^o defines an equivalence of categories?

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

Theorem

The category (UAC/k) *of affine unipotent commutative group schemes over* k *is the limit of subcategories*

$$(\mathrm{UAC}/k) = \varinjlim_n \mathscr{A}_n \ .$$

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

The Witt Group Scheme $\mathbb{W}_n$ of Length 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

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

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

Clearly, $\mathbb{W}_n$ is an object in the category $\mathscr{A}_n$ 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 $\mathscr{A}_n$. In other words, the functor

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

is exact and faithful.

The Endomorphism Ring of $\mathbb{W}_n$

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

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

the Vershiebung operator is the shift

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

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

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

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

The Endomorphism Ring of $\mathbb{W}_n$

Definition

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

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

where $\lambda \mapsto \lambda^{(p)}$ is the Frobenius automorphism of 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

$$\mathscr{D}_k/\mathscr{D}_k V^n \cong \mathrm{End}(\mathbb{W}_n)$$

An Equivalence for $\mathscr{A}_n$

Theorem

The functor

$$h^0_{\mathbb{W}_n} : \mathscr{A}_n \longrightarrow (\mathscr{D}_k\text{-Mod}) : G \mapsto M(G) = \mathrm{Hom}_{\mathscr{A}_n}(G, \mathbb{W}_n)$$

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

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

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

where $T : \mathbb{W}_n \longrightarrow \mathbb{W}_{n+1} : (a_1, a_2, \ldots, a_n) \mapsto (0, a_1, \ldots, a_{n-1})$.

The Action of W on $\mathbb{W}_n$ Revisited

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

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

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

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

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

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

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

Proposition

$$\varprojlim_n \mathscr{D}_k / \mathscr{D}_k V^n \cong \mathrm{End}(\underrightarrow{\mathbb{W}})$$

An Equivalence for (UAC/k)

Theorem

The functor

$$M : (\mathrm{UAC}/k) \longrightarrow (\mathscr{D}_k\text{-Mod}) : G \mapsto M(G) = \varinjlim_n \mathrm{Hom}(G, \mathbb{W}_n)$$

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

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

$$G \in (\mathrm{Fcu}/k) \ \Leftrightarrow \ F \text{ is nilpotent on } M(G)$$
$$G \in (\mathrm{Feu}/k) \ \Leftrightarrow \ F \text{ is bijective on } M(G)$$

Extending the Construction to (Fcm/k)

The construction $G \mapsto \varinjlim_n \operatorname{Hom}(G, \underrightarrow{\mathbb{W}})$ 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 $\mathscr{D}_k$-module M, let $M^* = \operatorname{Hom}_W(M, W_\infty)$ where

$$W_\infty = \underrightarrow{\mathbb{W}}(k) : \mathbb{W}_1(k) \xrightarrow{T} \mathbb{W}_2(k) \xrightarrow{T} \mathbb{W}_3(k) \xrightarrow{T} \cdots$$

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 $\mathscr{D}_k$-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 multipicative and we define

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

Theorem (Dieudonné)

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

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

$$\begin{array}{rcl} G \text{ is étale} & \Leftrightarrow & F \text{ is bijective on } M(G) \\ G \text{ is connected} & \Leftrightarrow & F \text{ is nilpotent on } M(G) \\ G \text{ is multiplicative} & \Leftrightarrow & V \text{ is bijective on } M(G) \\ G \text{ is unipotent} & \Leftrightarrow & V \text{ is nilpotent on } M(G) \end{array}$$

Examples

The Dieudonné modules of the basic finite group schemes over k are

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

$$M(\alpha_{p^n/k}) = \mathscr{D}_k/(\mathscr{D}_k F^n + \mathscr{D}_k V) \ , \ \alpha_{p^n} = \ker F^n_{\mathbb{G}_{a/k}}$$

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

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

$$M(\mathbb{W}_{2,2}) = \mathscr{D}_k/(\mathscr{D}_k F^2 + \mathscr{D}_k V^2)$$

Examples

Equivalently, we can describe a Dieudonné module M as a W-module equipped with a σ-linear map $F : M \to M$ and σ^{-1}-linear map $V : M \to M$ (where σ is the Frobenius automorphism of W).

For example,

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

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

$$M(\mu_{p/k}) = k \text{ with } F = 0 \text{ and } V = \sigma^{-1}$$

p-Divisible Groups

Definition

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
$$1 \longrightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}$$
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).

Equivalence of Categories

Theorem

The functor

$$\varinjlim_n G_n \mapsto \varprojlim_n M(G_n)$$

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. *$F : M \longrightarrow M$ is a σ-linear map*
3. *$V : M \longrightarrow M$ is a σ^{-1}-linear map*
4. *$VF = FV = p$*

Furthermore,

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