Dieudonné theory for Faltings' strict -modules

Gibbons, William

Dieudonné Theory for Faltings' Strict $\mathscr{O}$-modules

William Gibbons

A Thesis presented for the degree of
Doctor of Philosophy

Department of Mathematical Sciences
University of Durham
England

July 2005

Dieudonné Theory for Faltings' Strict $\mathscr{O}$-modules

William Gibbons

Submitted for the degree of Doctor of Philosophy
October 2004

Abstract

The theory of group schemes and their liftings to mixed characteristic valuation rings is well-developed. In [Fal02], a new equi-characteristic analogue of group schemes, known as group schemes with strict $\mathscr{O}$-action, or strict $\mathscr{O}$-modules, was proposed and developed, including Dieudonné theory. In [Abr04], their theory was studied over a complete discrete valuation ring. In this Thesis, a version of Dieudonné theory is developed for the strict $\mathscr{O}$-modules of [Abr04] over a perfect field, using constructions of [Fon77], using very different methods from those deployed in [Fal02].

Declaration

The work in this thesis is based on research carried out at the Department of Mathematical Sciences. No part of this thesis has been submitted elsewhere for any other degree or qualification and it is all my own work unless referenced to the contrary in the text.

Acknowledgements

I thank my supervisor, Victor Abrashkin, for his support and guidance throughout my period of study.

Contents

Chapter 1

Construction of the category of deformed group schemes

1.1 Introduction

In this chapter, we define the basic objects we will work with, which consist of a group scheme G, together with a scheme $G^\flat$ containing G as a closed subscheme via a morphism $i_{\mathcal{G}} : G \to G^\flat$. It will be proved that, for all suitable 'lifts' $G^\flat$ of G, there is a unique lifting of the group morphisms of G to $G^\flat$, such that the triple $(G, G^\flat, i_{\mathcal{G}})$ is a 'group object' (a kind of deformation) $\mathcal{G}$. Having constructed such group objects, we endow them with an '$\mathcal{O}$-action', a homomorphism of rings $\mathcal{O} \to \mathrm{End}(\mathcal{G})$, for some complete discrete valuation rings $\mathcal{O}$.

Objects such as the above triple are essentially Faltings' 'group schemes with strict $\mathcal{O}$-action', as developed in his paper [Fal02]. The form of these objects which we shall use was first introduced in [Abr04].

Our approach differs from Faltings' in that it allows us to define 'minimal' objects, which help us in our attempts to classify categories of objects explicitly. We adopt the definitions of [Abr04].

In this chapter, our exposition is over a perfect field of characteristic p, and over a complete noetherian local ring. Where our statements (and their proofs) are different for fields and rings, we provide different (and separate) statements and proofs, since working over fields often simplifies the situation, and allows us to use more elementary techniques than for rings.

This chapter is the basis for the main results of this thesis, which are contained in chapter 2, and concern Dieudonné Theory in characteristic p. It should be noted that this theory and the results developed in chapter 2 do not depend on any of the results proved here for rings, but merely on the results for fields.

Finally, where we work with finite free (ie, finitely generated and free as R-modules) R-algebras over local rings R, note that this condition is equivalent to requiring our R-algebras to be flat (Lemma A.1); therefore our results can be considered the analogue of results about finite flat R-group schemes, for R local.

1.2 Completions of algebras

In this section, we discuss some basic properties of the algebras we will be working with.

From now on, let R be a complete noetherian local ring. We denote its maximal ideal by $\mathfrak{m}$, and its residue field by k. We assume throughout that k is perfect and of characteristic $p > 0$.

Although our results do not depend on the choice of a particular ring, they are motivated by cases like $R = k$, $R = \mathbb{Z}_p$ or finite ramified extensions of $\mathbb{Z}_p$, $R = \mathbb{Z}_p/(p^n)$, $R = k[[\pi]]$, and $R = k[[\pi]]/(\pi^n)$. We are motivated by analogous results classifying finite flat group schemes over complete discrete valuation rings.

Definition 1.2.1. Let Aug'_R be the category whose objects are augmented R-algebras which are finitely generated as R-modules, with morphisms defined as follows: if $A, B \in \mathrm{Aug}'_R$, with augmentation ideals I_A and I_B respectively, then morphisms $f : A \to B$ are morphisms of R-algebras such that $f(I_A) \subset I_B$. It's easily verified that Aug'_R is a category.

Let Aug_R be the full subcategory of Aug'_R whose objects are free R-modules.

Remark 1.2.2. If $A \in \mathrm{Aug}'_R$, then for any R-algebra S, $A \otimes S \in \mathrm{Aug}'_S$.

Remark 1.2.3. Clearly if $R = k$ is a field, then $\mathrm{Aug}'_R = \mathrm{Aug}_R$.

We define a map from Aug_R to the category of projective limits of augmented R-algebras by

$$A \rightsquigarrow A^{\mathrm{loc}} = \varprojlim_n A/I_A^n$$

for all $A \in \mathrm{Aug}_R$ with augmentation ideal I_A. A morphism $f : A \to B$ in Aug_R, for $B \in \mathrm{Aug}_R$ with augmentation ideal I_B satisfies $f(I_A) \subset I_B$, and therefore $f(I_A^n) \subset I_B^n$ for all $n \in \mathbb{N}$; therefore the composition

$$A \xrightarrow{f} B \to B/I_B^n$$

factors through A/I_A^n for each $n \in \mathbb{N}$, and therefore f induces a family of maps $A/I_A^n \to B/I_B^n$ for each $n \in \mathbb{N}$, and hence a morphism $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$, such that the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\ A^{\mathrm{loc}} \arrow[r, "f^{\mathrm{loc}}"] & B^{\mathrm{loc}} \end{tikzcd}$$

Hence our map $A \rightsquigarrow A^{\mathrm{loc}}$ is a functor.

We now prove that if $R = k$, then any $A \in \mathrm{Aug}_k$ maps to a finite k-algebra A^{loc}; the proof is elementary.

Lemma 1.2.4. *If $A \in \mathrm{Aug}_k$ (with augmentation ideal I_A), then A^{loc} is a quotient of A, hence a k-algebra which is finitely generated as a k-module. Further, A^{loc} is local, with maximal ideal equal to the image of I_A in A^{loc}, which we shall henceforth denote $I_{A^{\mathrm{loc}}}$.*

Proof. Consider the chain of ideals

$$I_A \supset I_A^2 \supset \cdots \supset I_A^n \supset \ldots$$

Each is a k-vector subspace of A. If $I_A^n \neq I_A^{n+1}$, then $\dim_k I_A^n > \dim_k I_A^{n+1}$; hence the chain must stabilize after a finite number of steps: $I_A^n = I_A^{n+1}$ for all $n \geq N$, where N is some fixed positive integer. (In fact, A is an Artin ring).

Therefore $A^{\mathrm{loc}} = \varprojlim_n A/I_A^n = A/I_A^N$, which is finite over k since it is a quotient of A.

To see that A^{loc} is local, with maximal ideal $I_{A^{\mathrm{loc}}}$, note that $I^N_{A^{\mathrm{loc}}} = 0$ for some $N \in \mathbb{N}$; therefore $I_{A^{\mathrm{loc}}}$ is in every prime ideal of A^{loc}. $I_{A^{\mathrm{loc}}}$ is maximal since $A^{\mathrm{loc}}/I_{A^{\mathrm{loc}}} \cong A/I_A \cong k$; therefore $I_{A^{\mathrm{loc}}}$ is the only prime ideal of A^{loc}, and A^{loc} is local. □

We prove an analogous result for $A \in \mathrm{Aug}_R$; however, our methods are somewhat less elementary, and depend on a result from the theory of completions:

Theorem 1.2.5. *Let R be a complete noetherian local ring. If A is a commutative R-algebra that is finite as an R-module, then A has only finitely many maximal ideals $\mathfrak{m}_i$, each localization $A_{\mathfrak{m}_i}$ is a complete local ring over R which is finite as an R-module, and $A = \prod_i A_{\mathfrak{m}_i}$ is the direct product of its localizations.*

Proof. This result is [Eis95, Corollary 7.6], and a complete proof is given there. □

Lemma 1.2.6. *$A^{\mathrm{loc}} \cong \varprojlim_n A/(I_A + \mathfrak{m}A)^n$. Further, A^{loc} is a finite free R-module, and is equal to the localisation of A with respect to $I_A + \mathfrak{m}A$, which is a maximal ideal of A.*

Proof. Because R is complete, $R \cong \varprojlim_n R/\mathfrak{m}^n$ by definition, and since inverse limits commute with finite direct sums, any finite rank free R-module $M = R^{\oplus m}$ satisfies $\varprojlim_n M/\mathfrak{m}M \cong M$. Therefore $A \cong \varprojlim_i A/\mathfrak{m}^i A$, since A is a finite free R-module.

Therefore

$$\begin{aligned}
\varprojlim_n A/I_A^n &\cong \varprojlim_n (\varprojlim_m A/\mathfrak{m}^m A)/I_A^n \\
&\cong \varprojlim_n \varprojlim_m A/(\mathfrak{m}^m A + I_A^n) \\
&\cong \varprojlim_n A/(\mathfrak{m}^n A + I_A^n) \\
&\cong \varprojlim_n A/(\mathfrak{m}A + I_A)^n,
\end{aligned}$$

where the last equality follows by Lemma A.2, because $\mathfrak{m}^n A + I_A^n \subset (\mathfrak{m}A + I_A)^n$ and $(\mathfrak{m}A + I_A)^{2n} \subset \mathfrak{m}^n A + I_A^n$. Hence $A^{\mathrm{loc}} \cong \varprojlim_n A/(I_A + \mathfrak{m}A)^n$.

Clearly $I_A + \mathfrak{m}A$ is a maximal ideal of A; hence the map $A \longrightarrow \varprojlim_n A/(I_A + \mathfrak{m}A)^n$ factors through $A_{I_A+\mathfrak{m}A}$, by a property of completions at maximal ideals. But by Theorem 1.2.5, $A_{I_A+\mathfrak{m}A}$ is complete, so $A_{I_A+\mathfrak{m}A} \cong \varprojlim_n A/(I_A + \mathfrak{m}A)^n$. Further

$\varprojlim_n A/(I_A + \mathfrak{m}A)^n$ is flat over A, as localization is flat. Since A is in turn free over R by definition, $\varprojlim_n A/(I_A + \mathfrak{m}A)^n$ is flat over R. It is also finite over R, as it is a summand of A by Theorem 1.2.5, and therefore free over R by Lemma A.1. □

Therefore, whether we work over R or k, we will be able to assume that $A^{\mathrm{loc}} \cong \varprojlim_n A/I_A^n \cong \varprojlim_n A/(\mathfrak{m}A+I_A)^n \cong A_{\mathfrak{m}A+I_A}$ throughout the rest of this Thesis; these different characterizations will prove useful to us at different times. We will also make use of the fact that A^{loc} is a finite quotient of A from time to time, as established in Theorem 1.2.5.

Remark 1.2.7. Since the functor $A \mapsto A^{\mathrm{loc}}$ maps $A \in \mathrm{Aug}_R$ to some finite flat augmented R-algebra A^{loc}, it is actually a functor from Aug_R to Aug_R.

Finally, we define an invariant of A, for any $A \in \mathrm{Aug}_R$; it is the minimum number of generators of the augmentation ideal of A.

Definition 1.2.8. For any $A \in \mathrm{Aug}'_R$, let $m(A)$ denote the minimum number of elements of A required to generate its augmentation ideal.

Lemma 1.2.9. *Let $A \in \mathrm{Aug}_k$. Then $m(A^{\mathrm{loc}}) = \mathrm{rank}_k\, I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}}$.*

Proof. If

$$k[X_1, \dots, X_n] \to A^{\mathrm{loc}}$$

is any surjection of augmented k-algebras, then it clearly induces a surjection

$$(X_1, \dots, X_n)/(X_1, \dots, X_n)^2 \to I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}}$$

so $m(A^{\mathrm{loc}}) \geq \mathrm{rank}_k\, I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}}$.

Since A^{loc} is a finitely generated local k-algebra, any set of generators $X_1, \dots, X_n$ of $I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}}$ together with 1 lift by Nakayama's Lemma to a set of generators of A^{loc} as a k-algebra. Therefore $m(A^{\mathrm{loc}}) \leq \mathrm{rank}_k\, A^{\mathrm{loc}}/I^2_{A^{\mathrm{loc}}}$, and hence we have equality. □

Corollary 1.2.10. *Let $A \in \mathrm{Aug}_R$. Then $m(I_{A^{\mathrm{loc}}}) = \mathrm{rank}_k\, I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$.*

Proof. By the previous result, $I_{A^{\mathrm{loc}}} \otimes k$ can be generated by $\mathrm{rank}_k\, I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$ generators. Therefore take a set $X_1, \dots, X_n$ of generators of $I_{A^{\mathrm{loc}}} \otimes k$, where $n =$

$\operatorname{rank}_k I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$. Since $I_{A^{\mathrm{loc}}} \otimes k \cong I_{A^{\mathrm{loc}}}/\mathfrak{m}I_{A^{\mathrm{loc}}}$, any lifts of $X_1, \ldots, X_n$ to $I_{A^{\mathrm{loc}}}$ will generate it as an R-module, by Nakayama's Lemma. Therefore $m(A^{\mathrm{loc}}) \leq \operatorname{rank}_k I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$. As in the proof of the previous result, we have $m(A^{\mathrm{loc}}) \geq \operatorname{rank}_k I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$, and hence our equality. □

1.3 Deformations of R-algebras

In this section, we define a category DA_R, of deformations of algebras $A \in \mathrm{Aug}_R$; we first sketch this construction, and then define it rigorously.

To each $A \in \mathrm{Aug}_R$, we associate a triple $(A, A^\flat, i_A)$, where $A^\flat \in \mathrm{Aug}'_R$, and i_A is a surjection $A^\flat \to A^{\mathrm{loc}}$, where i_A satisfies certain properties; such triples will constitute the objects of our category. Morphisms will be pairs $\overline{f} = (f, f^\flat)$, where f and $f^\flat$ are morphisms in Aug_R, satisfying certain compatibility conditions.

Definition 1.3.1. We begin by defining objects in our category. An object $\mathcal{A} \in DA_R$ is a triple $(A, A^\flat, i_A)$, such that $A \in \mathrm{Aug}_R$ (with augmentation ideal I_A) and $A^\flat \in \mathrm{Aug}'_R$ (with augmentation ideal $I_{A^\flat}$) and there is a ring $R[X_1, \ldots, X_m]$ with an ideal $I \subset (X_1, \ldots, X_m)$ such that if

$$A^{\mathrm{loc}} = R[X_1, \ldots, X_m]/I,$$

then

$$A^\flat = R[X_1, \ldots, X_m]/I(X_1, \ldots, X_m).$$

We denote by i_A the natural surjection $A^\flat \to A^{\mathrm{loc}}$ of R-algebras. We denote the image of I_A in A^{loc} under the functor $A \rightsquigarrow A^{\mathrm{loc}}$ by $I_{A^{\mathrm{loc}}}$; in other words,

$$I_{A^{\mathrm{loc}}} = \varprojlim_n I_A/I_A^n.$$

Remark 1.3.2. This definition is slightly different from the one in [Fal02], where there is no A^{loc}; instead, that construction takes a surjection $R[X_1, \ldots, X_m] \twoheadrightarrow A$, and defines $A^\flat = R[X_1, \ldots, X_m]/I(X_1, \ldots, X_m)$, where I is the kernel of the surjection.

Our definition (which follows [Abr04]) has the effect of 'covering' only a local quotient of A. This will allow us to define *minimal* objects DA_R, which behave rather like deformation retracts.

Having defined the objects in DA_R, we now define morphisms.

Definition 1.3.3. A *morphism* $\overline{f} : \mathcal{A} \to \mathcal{B} = (B, B^\flat, i_\mathcal{B})$ where B has augmentation ideal I_B, is a pair of augmented R-algebra morphisms $f : A \to B$ and $f^\flat : A^\flat \to B^\flat$ such the morphism $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$ induced by f (f induces f^{loc} because $f(I_A) \subset I_B$, so f is compatible with the filtration) is compatible with $f^\flat$, in the sense that the squares in the following diagram commute

$$\begin{array}{ccc} A^\flat & \xrightarrow{f^\flat} & B^\flat \\ \downarrow & & \downarrow \\ A^{\mathrm{loc}} & \xrightarrow{f^{\mathrm{loc}}} & B^{\mathrm{loc}} \\ \uparrow & & \uparrow \\ A & \xrightarrow{f} & B. \end{array} \tag{1.3.1}$$

It's easy to see that $f^\flat(I_{A^\flat}) \subset I_{B^\flat}$.

We frequently denote morphisms $\overline{f} : \mathcal{A} \to \mathcal{B}$ in DA_R using the notation $(f, f^\flat)$.

Remark 1.3.4. In order to prove that DA_R is a category, we must prove (see [GM99, Definition 1.1]) that each object $\mathcal{A} \in DA_R$ has an associated identity morphism, that the composition of morphisms is again a morphism, and that composition of morphisms is associative.

If $\mathcal{A} = (A, A^\flat, i_\mathcal{A}) \in DA_R$, we can define $\mathrm{id}_\mathcal{A} = (\mathrm{id}_A, \mathrm{id}^\flat_A)$, which clearly satisfies the condition for it to be a morphism of DA_R.

If $\mathcal{C} = (C, C^\flat, i_\mathcal{C}) \in DA_R$, and we have morphisms $(f, f^\flat) : \mathcal{A} \to \mathcal{B}$ and $(g, g^\flat) : \mathcal{B} \to \mathcal{C}$, then we can take as composition $(g \circ f, g^\flat \circ f^\flat)$; it's easy to verify that this composition satisfies the obvious extension of diagram (1.3.1).

That composition of morphisms is associative follows from the fact that composition of morphisms of R-algebras is.

Therefore, DA_R satisfies the necessary axioms to be a category.

We now define two invariant modules which we can associate to any $\mathcal{A} \in DA_R$; the second, $N_\mathcal{A}$, is actually an ideal of $A^\flat$.

Definition 1.3.5. If $(A, A^\flat, i_\mathcal{A}) \in DA_R$, we define $t^*_\mathcal{A} = I_{A^\flat}/I^2_{A^\flat}$, and $N_\mathcal{A}$ to be the kernel of $i_\mathcal{A} : A^\flat \to A^{\mathrm{loc}}$.

Remark 1.3.6. $N_{\mathcal{A}}$ is clearly equal to the image of the ideal I of Definition 1.3.1 in $A^\flat$. Since $I_{A^\flat}$ is the image of the ideal $(X_1, \ldots, X_n)$ of $R[X_1, \ldots, X_n]$ in this definition, and the ideal defining $A^\flat$ is $I(X_1, \ldots, X_n)$, it follows that $I_{A^\flat} N_{\mathcal{A}} = 0 = N_{\mathcal{A}}^2$ in $A^\flat$.

Lemma 1.3.7. *For all $A \in \mathrm{Aug}_R$ (with augmentation ideal I_A), there is an object $\mathcal{A} \in DA_R$, where $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}}) \in DA_R$, for some $A^\flat$ and $i_{\mathcal{A}}$.*

Proof. Since A^{loc} is finitely generated, there is an augmented polynomial ring $R[X_1, \ldots, X_n]$ and a surjection of augmented R-algebras

$$R[X_1, \ldots, X_n] \to A^{\mathrm{loc}},$$

the kernel of which we will call I. Then we can make the obvious definition $A^\flat = R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)I$, and let $i_{\mathcal{A}}$ be the obvious surjection $A^\flat \to A^{\mathrm{loc}}$. □

Lemma 1.3.8. *Let $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}})$ and $\mathcal{B} = (B, B^\flat, i_{\mathcal{B}})$. Any augmented R-algebra homomorphism $f : A \to B$ extends to a morphism $\mathcal{A} \to \mathcal{B}$ in DA_R.*

Proof. f lifts to a map $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$, since the correspondence $A \to A^{\mathrm{loc}}$ is functorial, so the problem is to prove that this lifts to a map $f^\flat : A^\flat \to B^\flat$.

By the definition of $\mathcal{A}$ and $\mathcal{B}$, there are polynomial rings $R[X_1, \ldots, X_m]$ and $R[Y_1, \ldots, Y_n]$ such that

$$A^{\mathrm{loc}} = R[X_1, \ldots, X_m]/I, A^\flat = R[X_1, \ldots, X_m]/I(X_1, \ldots, X_m),$$

and

$$B^{\mathrm{loc}} = R[Y_1, \ldots, Y_n]/I', B^\flat = R[Y_1, \ldots, Y_n]/I'(Y_1, \ldots, Y_n).$$

Since the polynomial ring $R[X_1, \ldots, X_m]$ satisfies no relations, each X_i can be mapped to an arbitrary term in the ideal $(Y_1, \ldots, Y_n)$ of $R[Y_1, \ldots, Y_n]$. Therefore f^{loc} lifts to a map $\hat{f}$ making the following diagram commute

$$\begin{tikzcd}
R[X_1, \ldots, X_m] \arrow[r, "\hat{f}"] \arrow[d] & R[Y_1, \ldots, Y_n] \arrow[d] \\
A^{\mathrm{loc}} \arrow[r, "f^{\mathrm{loc}}"] & B^{\mathrm{loc}}.
\end{tikzcd}$$

Since $f^{\mathrm{loc}}(I_{A^{\mathrm{loc}}}) \subset I_{B^{\mathrm{loc}}}$, $\hat{f}((X_1, \ldots, X_m)) \subset (Y_1, \ldots, Y_n)$. Since $\hat{f}(I) \subset I'$, it follows that $\hat{f}((X_1, \ldots, X_m)I) \subset (Y_1, \ldots, Y_n)I'$, and therefore $\hat{f}$ induces a map $f^\flat : A^\flat \to B^\flat$ lifting f^{loc}. □

1.4 Minimal deformations

As noted in the previous section, one of the differences between our theory and the theory of [Fal02] is that we 'cover' only the local part of any $A \in \mathrm{Aug}_R$ with a surjection $A^\flat \twoheadrightarrow A$; now we show that our definition allows us to define minimal objects in DA_R.

Definition 1.4.1. We say that $\mathcal{A} \in DA_R$ is *minimal* if the map $A^\flat \otimes k \to A^{\mathrm{loc}} \otimes k$ induces an isomorphism of $t^*_{\mathcal{A}} \otimes k$ to its image, where $t^*_{\mathcal{A}}$ is the module associated to $\mathcal{A}$ defined in Definition 1.3.5. In other words, we require that the induced map $I_{A^\flat}/I^2_{A^\flat} \otimes k \to I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k$ be an isomorphism.

Lemma 1.4.2. *If $\mathcal{A} \in DA_R$ is minimal, then $m(A^\flat) = m(A^{\mathrm{loc}})$.*

Proof. By definition of $\mathcal{A}$, there's a polynomial ring $R[X_1, \ldots, X_n]$ such that

$$A^{\mathrm{loc}} = R[X_1, \ldots, X_n]/I$$
$$A^\flat = R[X_1, \ldots, X_n]/I(X_1, \ldots, X_n),$$

for some ideal $I \subset (X_1, \ldots, X_n)$. Hence $I(X_1, \ldots, X_n) \subset (X_1, \ldots, X_n)^2$, and $\mathrm{rank}_k\, t^*_{\mathcal{A}} \otimes k = \mathrm{rank}\, I_{A^\flat}/I^2_{A^\flat} \otimes k = \mathrm{rank}(X_1, \ldots, X_n) \otimes k/(X_1, \ldots, X_n)^2 \otimes k = n$. Since $\mathcal{A}$ is minimal, $\mathrm{rank}\, t^*_{\mathcal{A}} \otimes k = \mathrm{rank}\, I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} \otimes k = n$, and by Corollary 1.2.10, $m(A^{\mathrm{loc}}) = n$. Since $X_1, \ldots, X_n$ generate $I_{A^\flat}$, it's clear that $m(A^\flat) \le n$, and since $A^\flat \to A^{\mathrm{loc}}$ is a surjection, $m(A^\flat) \ge m(A^{\mathrm{loc}}) = n$; therefore $m(A^\flat) = m(A^{\mathrm{loc}}) = n$. ☐

Lemma 1.4.3. *If $\mathcal{A} \in DA_R$ is given by* $(\mathrm{Spec}\, A, \mathrm{Spec}\, A^\flat, i_{\mathcal{A}})$*, then $A^{\mathrm{loc}} \otimes k$, $I^n_{A^{\mathrm{loc}}} \otimes k = 0$ and $I^m_{A^\flat} \otimes k = 0$ for some $n, m \in \mathbb{N}$.*

Proof. The fact that $I^n_{A^\flat} \otimes k = 0$ for some $n \in \mathbb{N}$ follows by the proof of Lemma 1.2.4, and by Remark 1.3.6.

Since $i_{\mathcal{A}}(I_{A^\flat}) \subset I_{A^{\mathrm{loc}}}$, $i_{\mathcal{A}}(I^n_{A^\flat} \otimes k) = 0$. Therefore $I^n_{A^\flat} \otimes k \subset N_{\mathcal{A}} \otimes k$, and since $I_{A^\flat} N_{\mathcal{A}} = 0$, $I^{n+1}_{A^\flat} \otimes k = 0$, as required. ☐

Now we prove that deformations are compatible with taking the special fibre, in the sense that if $(A, A^\flat, i_{\mathcal{A}}) \in DA_R$, then $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}} \otimes k) \in DA_k$, and if $(A, A^\flat, i_{\mathcal{A}})$ is minimal, then so is $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}} \otimes k)$.

Lemma 1.4.4. *Let $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}}) \in DA_R$. Then $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}} \otimes k) \in DA_k$, and if $(A, A^\flat, i_{\mathcal{A}})$ is minimal, then so is $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}} \otimes k)$. We denote $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}} \otimes k)$ by $\mathcal{A} \otimes k$. Finally, base change $R \to k$ is a functor $DA_R \to DA_k$.*

Proof. By Theorem 1.2.5, we have a decomposition

$$A \cong e_1 A \times \cdots \times e_n A \tag{1.4.1}$$

for some n, where the e_i are orthogonal idempotents of A, and each $e_i A$ is a localisation of A at one of its maximal ideals. Since A^{loc} is the localisation of A at the maximal ideal $\mathfrak{m}A + I_A$, we can define $A^{\text{loc}} = e_1 A$ without loss of generality. Hence $A^{\text{loc}} = A/(e_2, \dots, e_n)$. Hence $A^{\text{loc}} \otimes k = A/(e_2, \dots, e_n) + \mathfrak{m}A$. Since e_1 is invertible in $A^{\text{loc}} = e_1 A$, it is not in $I_A + \mathfrak{m}A$.

On the other hand, tensoring (1.4.1) with k gives

$$A \otimes k \cong e_1 A \otimes k \times \cdots \times e_n A \otimes k.$$

If we localise at $I_A \otimes k$, all e_i map to zero for $i > 1$; since $e_1 \notin I_A + \mathfrak{m}A$ as above, $e_1 \otimes 1$ becomes invertible in $(A \otimes k)_{I_A \otimes k}$, and $e_1 e_i = 0$ for $i > 1$.

Hence localisation $A \otimes k \to (A \otimes k)_{I_A \otimes k}$ factors through $(A \otimes k)/(e_2, \dots, e_n) \otimes k$, which is local with maximal ideal $I_A \otimes k$ since $A/(e_2, \dots, e_n)$ is local with maximal ideal $I_A + \mathfrak{m}A$. Hence $(A \otimes k)^{\text{loc}} \cong A \otimes k/(e_2, \dots, e_n) \otimes k \cong A^{\text{loc}} \otimes k$.

By definition of $\mathcal{A}$, we have

$$\begin{aligned} A^{\text{loc}} &= R[X_1, \dots, X_n]/I \\ A^\flat &= R[X_1, \dots, X_n]/I(X_1, \dots, X_n) \end{aligned}$$

for some polynomial ring $R[X_1, \dots, X_n]$ and ideal I. Tensoring the above with k (and using $(A \otimes k)^{\text{loc}} = A^{\text{loc}} \otimes k$ as we just proved) shows that we can take $(A \otimes k)^\flat = A^\flat \otimes k$. Hence $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}}) \in DA_k$.

If $(A, A^\flat, i_{\mathcal{A}})$ is minimal, the map $I_{A^\flat}/I^2_{A^\flat} \otimes k \to I_{A^{\text{loc}}}/I_{A^{\text{loc}}} \otimes k$ induced by $i_{\mathcal{A}}$ is an isomorphism. Since $A^\flat \otimes k = (A \otimes k)^\flat$ and $A^{\text{loc}} \otimes k = (A \otimes k)^{\text{loc}}$, $(A \otimes k, A^\flat \otimes k, i_{\mathcal{A}}) \in DA_k$ is minimal.

It's obvious that morphisms $(f, f^\flat) \in \text{Hom}_{DA_R}(\mathcal{A}, \mathcal{B})$ reduce to morphisms $(f \otimes \text{id}_k, f^\flat \otimes \text{id}_k) \in \text{Hom}_{DA_k}(\mathcal{A} \otimes k, \mathcal{B} \otimes k)$. $\square$

We now prove that minimal deformations have a property analogous to the theory of deformation retracts from topology; any endomorphism of a minimal deformation $(f, f^\flat) : \mathcal{A} \to \mathcal{A}$ such that f is an isomorphism has the property that $f^\flat$ is also an isomorphism. We prove this result first for the special case $R = k$.

Proposition 1.4.5. *If $\mathcal{A}, \mathcal{B} \in DA_k$ are minimal and $\overline{f} : \mathcal{A} \to \mathcal{B}$ lifts an isomorphism $f : A \to B$, then $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$ and $f^\flat : A^\flat \to B^\flat$ are isomorphisms.*

Proof. If $f : A \to B$ is an isomorphism, then $f(I_A) = I_B$, and so clearly $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$ is an isomorphism.

Since $f^\flat(I_{A^\flat}) \subset I_{B^\flat}$, it follows that $f^\flat(I^n_{A^\flat}) \subset I^n_{B^\flat}$ for all $n \in \mathbb{N}$. Hence there are maps $f^\flat_n : A^\flat/I^n_{A^\flat} \to B^\flat/I^n_{B^\flat}$ induced by taking the composition of $f^\flat$ with $B^\flat \to B^\flat/I^n_{B^\flat}$.

The following commutative diagram implies that the map $t^*_A \to t^*_B$ induced from $f^\flat : A^\flat \to B^\flat$ is an isomorphism

$$\begin{array}{ccc} t^*_A & \longrightarrow & t^*_B \\ \downarrow\cong & & \downarrow\cong \\ I_{A^{\mathrm{loc}}}/I^2_{A^{\mathrm{loc}}} & \xrightarrow[\cong]{} & I_{B^{\mathrm{loc}}}/I^2_{B^{\mathrm{loc}}} \end{array}$$

where the columns are isomorphisms because $\mathcal{A}$ and $\mathcal{B}$ are minimal, and the bottom map is induced by f^{loc}. Hence $f^\flat_2 : k \oplus t^*_A \to k \oplus t^*_B$ is an isomorphism, since it is k-linear.

We now prove by induction that $f^\flat_n$ is a surjection for all $n > 2$. Assume $f^\flat_{n-1}$ is a surjection. Then for all $b \in B^\flat/I^n_{B^\flat}$, there is an $a \in A^\flat/I^n_{A^\flat}$ such that $f^\flat_n(a) = b$ mod $I^{n-1}_{B^\flat}/I^n_{B^\flat}$. Hence it's enough to prove that each $i \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$ is the image of some $a \in A^\flat/I^n_{A^\flat}$, since we will then be able to recover each $b \in B^\flat/I^n_{B^\flat} \otimes k$ by adding or subtracting some $i \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$.

But since $n > 1$, $i = \sum_j b_j b'_j$ for some $b_j, b'_j \in I_{B^\flat}/I^n_{B^\flat}$. By induction there are $a, a' \in I_{A^\flat}/I^n_{A^\flat}$ such that $f^\flat_n(a) = b_j + i'$ and $f^\flat_n(a') = b'_j + i''$ for some $i', i'' \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$. Therefore $f^\flat_n(aa') = (b_j + i')(b'_j + i'') = b_j b'_j \in I_{B^\flat}/I^n_{B^\flat}$. Hence i is in the image of $f^\flat_n(A^\flat/I^n_{A^\flat})$, and therefore $f^\flat_n$ is a surjection, as required.

Since $I^n_{A^\flat} = 0$ for some n by Lemma 1.4.3, it follows that $f^\flat = f^\flat_n$ for some n, and therefore $f^\flat$ is itself a surjection.

By Lemma 1.3.8, there's also a map $g^\flat : B^\flat \to A^\flat$ lifting the inverse isomorphism $g : B \to A$ to f. By the above argument applied to $g^\flat$, it too is surjective. Therefore $g^\flat \circ f^\flat : A^\flat \to A^\flat$ is surjective. Since $A^\flat$ is a finite rank k-algebra, this map is an isomorphism, which implies that $f^\flat$ is injective.

Therefore $f^\flat$ is both injective and surjective, hence an isomorphism.

□

Corollary 1.4.6. *If $\mathcal{A}, \mathcal{B} \in DA_R$ are minimal and $\overline{f} : \mathcal{A} \to \mathcal{B}$ lifts an isomorphism $f : A \to B$, then $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$ and $f^\flat : A^\flat \to B^\flat$ are isomorphisms.*

Proof. f^{loc} is an isomorphism since f is.

By Lemma 1.4.4, $\mathcal{A} \otimes k \in DA_k$, and is minimal.

Letting C be the cokernel of $f^\flat$ as a morphism of R-modules, we have the following exact sequence

$$A^\flat \xrightarrow{f^\flat} B^\flat \to C \to 0$$

of finitely generated R-modules. By Lemma 1.4.4, f induces a morphism $(f \otimes k, f^\flat \otimes k) : \mathcal{A} \otimes k \to \mathcal{B} \otimes k$ of minimal objects on the special fibre, and by the Proposition, $f^\flat \otimes k : A^\flat \otimes k \to B^\flat \otimes k$ is an isomorphism. Since taking the special fibre is right-exact, it follows from the above exact sequence that $C \otimes k = 0$. Since C is finitely generated, Nakayama's Lemma now tells us that $C = 0$, and therefore $f^\flat$ is surjective. Therefore the maps $A^\flat/\mathfrak{m}^n A^\flat \to B^\flat/\mathfrak{m}^n B^\flat$ induced by $f^\flat$ are surjective for each n.

By Lemma 1.3.8, there's also a map $g^\flat : B^\flat \to A^\flat$ lifting the inverse isomorphism $g : B \to A$ to f. By the above argument applied to $g^\flat$, it too is surjective. Therefore $g^\flat \circ f^\flat : A^\flat \to A^\flat$ is surjective.

By [Eis95, Theorem 7.2a], $A^\flat \cong \varprojlim_n A^\flat/\mathfrak{m}^n A^\flat$. Hence if $(g^\flat \circ f^\flat) : A^\flat \to A^\flat$ is not injective, there is some $n \in \mathbb{N}$ such that the induced endomorphism $A^\flat/\mathfrak{m}^n A^\flat \to A^\flat/\mathfrak{m}^n A^\flat$ is not injective.

We now prove that there is a finite length composition series for $A^\flat/\mathfrak{m}^n A^\flat$ as an $R/\mathfrak{m}^n$-module: consider the series

$$A^\flat/\mathfrak{m}^n A^\flat \supset \mathfrak{m}A^\flat/\mathfrak{m}^n A^\flat \supset \cdots \supset \mathfrak{m}^{n-1}A^\flat/\mathfrak{m}^n A^\flat \supset 0.$$

Each quotient of successive terms is of the form $\mathfrak{m}^i A^\flat/\mathfrak{m}^{i+1}A^\flat$, and is therefore an $k = R/\mathfrak{m}$-vector space. Since $A^\flat$ is a finitely generated R-module, each quotient is a finitely generated k-vector space. Therefore, by inserting terms in the above series, it follows that we can exhibit a finite length composition series for $A^\flat/\mathfrak{m}^n A^\flat$.

By above, our induced endomorphism $A^\flat/\mathfrak{m}^n A^\flat \longrightarrow A^\flat/\mathfrak{m}^n A^\flat$ is surjective, and it follows by Lemma A.3 that this map is actually injective.

Therefore $g^\flat \circ f^\flat$ is injective, hence $f^\flat$ is injective. This proves the Corollary. □

Corollary 1.4.7. *If $\mathcal{A} \in DA_R$ is minimal, it is a deformation retract in the sense that for all $\mathcal{B} \in DA_R$, any sequence*

$$\mathcal{A} \to \mathcal{B} \to \mathcal{A}$$

which induces an isomorphism $f : A \longrightarrow A$, also induces an isomorphism $f^\flat : A^\flat \longrightarrow A^\flat$.

Proof. Follows directly from Corollary 1.4.6. □

Corollary 1.4.8. *If $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}}) \in DA_R$ is minimal, then if $\mathcal{A}' = (A, A'^\flat, i_{\mathcal{A}'}) \in DA_R$, $A^\flat$ is both a subalgebra of $A'^\flat$ and a quotient of it, by maps lifting* $\mathrm{id} : A \longrightarrow A$. *In particular, we have the splitting $A'^\flat \cong A^\flat \oplus K$ as an R-module, where $K =$* $\mathrm{Ker}(A'^\flat \longrightarrow A^\flat)$. *Further, $K \cap I^2_{A'^\flat} = \{0\}$.*

Proof. The isomorphism $A \cong A$ lifts to an isomorphism $A^{\mathrm{loc}} \longrightarrow A^{\mathrm{loc}}$ and then to maps $i : A^\flat \longrightarrow A'^\flat$ and $q : A'^\flat \longrightarrow A^\flat$ by Lemma 1.3.8; by Corollary 1.4.6, the composition

$$A^\flat \xrightarrow{i} A'^\flat \xrightarrow{q} A^\flat$$

is an isomorphism, and therefore i is an inclusion, and q is a surjection. The splitting follows from the exact sequence

$$0 \to K \xrightarrow{i'} A'^\flat \xrightarrow{q} A^\flat \to 0$$

since $q \circ i$ is an isomorphism of $A^\flat$, which implies that there is an isomorphism $(i, i') : A^\flat \oplus K \xrightarrow{\cong} A'^\flat$.

Suppose $k \in K \cap I^2_{A'^\flat}$. Then

$$k = \sum_i x_i y_i$$

for some $x_i, y_i \in I_{A'^\flat}$. We can write $x_i = x_i' + k_i$ and $y_i = y_i' + k_i'$ for $x_i', y_i' \in A^\flat$ and $k_i, k_i' \in K$ for each i. Since $KI_{A^\flat} = 0$ by Remark 1.3.6 as $K \subset N_{A'}$ and $K^2 = 0$,

$$k = \sum x_i' y_i'$$

which is clearly in $A^\flat$. Since $A^\flat \cap K = \{0\}$, we're done. □

We now prove a variant of Proposition 1.4.5 which we will need in chapter 2.

Proposition 1.4.9. *If $\mathcal{B} \in DA_k$ is minimal and $\overline{f} : \mathcal{A} \to \mathcal{B}$ lifts a surjection $f : A \to B$, then $f^{\text{loc}} : A^{\text{loc}} \to B^{\text{loc}}$ and $f^\flat : A^\flat \to B^\flat$ are surjections.*

Proof. If $f : A \to B$ is a surjection, then $f^{\text{loc}} \otimes k$ is a surjection by Lemma 1.3.7 as both $A^{\text{loc}} \otimes k$ and $B^{\text{loc}} \otimes k$ are quotients of $A \otimes k$ and $B \otimes k$ by powers of their augmentation ideals; since A and B are finitely generated R-modules, we deduce via Nakayama's Lemma that f^{loc} is a surjection.

Since $f^\flat(I_{A^\flat}) \subset I_{B^\flat}$, it follows that $f^\flat(I^n_{A^\flat}) \subset I^n_{B^\flat}$ for all $n \in \mathbb{N}$. Hence there are maps $f^\flat_n : A^\flat/I^n_{A^\flat} \to B^\flat/I^n_{B^\flat}$ induced by taking the composition of $f^\flat$ with $B^\flat \to B^\flat/I^n_{B^\flat}$.

The following commutative diagram implies that the map $t^*_{\mathcal{A}} \to t^*_{\mathcal{B}}$ induced from $f^\flat : A^\flat \to B^\flat$ is a surjection

$$\begin{array}{ccc} t^*_{\mathcal{A}} & \longrightarrow & t^*_{\mathcal{B}} \\ \downarrow & & \downarrow \cong \\ I_{A^{\text{loc}}}/I^2_{A^{\text{loc}}} & \longrightarrow & I_{B^{\text{loc}}}/I^2_{B^{\text{loc}}} \end{array}$$

where the right vertical map is an isomorphism because $\mathcal{B}$ is minimal, the left column is a surjection, and the bottom map is the surjection induced by f^{loc}. Hence $f^\flat_2 : k \oplus t^*_{\mathcal{A}} \to k \oplus t^*_{\mathcal{B}}$ is a surjection, since it is k-linear.

We now prove by induction that $f^\flat_n$ is a surjection for all $n > 2$. Assume $f^\flat_{n-1}$ is a surjection. Then for all $b \in B^\flat/I^n_{B^\flat}$, there is an $a \in A^\flat/I^n_{A^\flat}$ such that $f^\flat_n(a) = b$ mod $I^{n-1}_{B^\flat}/I^n_{B^\flat}$. Hence it's enough to prove that each $i \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$ is the image of some $a \in A^\flat/I^n_{A^\flat}$, since we will then be able to recover each $b \in B^\flat/I^n_{B^\flat} \otimes k$ by adding or subtracting some $i \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$.

But since $n > 1$, $i = \sum_j b_j b_j'$ for some $b_j, b_j' \in I_{B^\flat}/I^n_{B^\flat}$. By induction there are $a, a' \in I_{A^\flat}/I^n_{A^\flat}$ such that $f^\flat_n(a) = b_j + i'$ and $f^\flat_n(a') = b_j' + i''$ for some $i', i'' \in I^{n-1}_{B^\flat}/I^n_{B^\flat}$.

Therefore $f_n^\flat(aa') = (b_j + i')(b'_j + i'') = b_j b'_j \in I_{B^\flat}^{n-1}/I_{B^\flat}^n$. Hence i is in the image of $f_n^\flat(A^\flat/I_{A^\flat}^n)$, and therefore $f_n^\flat$ is a surjection, as required.

Since $I_{A^\flat}^n = 0$ for some n by Lemma 1.4.3, it follows that $f^\flat = f_n^\flat$ for some n, and therefore $f^\flat$ is itself a surjection. □

We now prove that to every $A \in \mathrm{Aug}_R$, we can associate a minimal object $(A, A^\flat, i_A)$ in DA_R; therefore minimal 'deformations' of any $A \in \mathrm{Aug}_R$ always exist.

Proposition 1.4.10. *If $A \in \mathrm{Aug}_R$, there is an $\mathcal{A} = (A, A^\flat, i_A) \in DA_R$ which is minimal.*

Proof. Let $m = \mathrm{rank}_k\, I_{A^{\mathrm{loc}}}/I_{A^{\mathrm{loc}}}^2 \otimes k$. Pick m generators. Lifting the generators to $I_{A^{\mathrm{loc}}}/I_{A^{\mathrm{loc}}}^2$ gives a set of m generators of $I_{A^{\mathrm{loc}}}/I_{A^{\mathrm{loc}}}^2$ as an R-module by Nakayama's Lemma, which we call $\overline{X}_1, \ldots, \overline{X}_m$.

We can define a map

$$R[X_1, \ldots, X_m] \to A^{\mathrm{loc}} \tag{1.4.2}$$

sending X_i to any lifting of $\overline{X}_i$ to A^{loc}. This map is a surjection modulo $I_{A^{\mathrm{loc}}}^2$ by construction, and therefore a surjection modulo $I_{A^{\mathrm{loc}}}^l$ for all $l \in \mathbb{N}$. Since $A^{\mathrm{loc}} \otimes k = A^{\mathrm{loc}} \otimes k/(I_{A^{\mathrm{loc}}} otimesk)^n$ for some n by Lemma 1.3.7, the induced map $k[X_1, \ldots, X_m] \to A^{\mathrm{loc}} \otimes k$ is a surjection. Since R is local and A^{loc} is a finitely generated R-module the map (1.4.2) is a surjection. We define $A^\flat = R[X_1, \ldots, X_m]/I(X_1, \ldots, X_m)$, where I is the kernel of the surjection. Clearly $t_{\mathcal{A}}^* \otimes k$ has rank at most m as a k-module, and since it surjects to $I_{A^{\mathrm{loc}}}/I_{A^{\mathrm{loc}}}^2 \otimes k$ which is of rank m under the map $A^\flat \to A^{\mathrm{loc}}$. Hence $\mathcal{A}$ is minimal. □

Proposition 1.4.11. *For a given $f : A \to B$ such that $f(I_A) \subset I_B$, the space of all extensions $\overline{f}$ is a principal homogeneous space over the group* $\mathrm{Hom}(t_{\mathcal{A}}, N_{\mathcal{B}})$.

Proof. If two morphisms $f^\flat, f_1^\flat : A^\flat \to B^\flat$ lift the same morphism $f^{\mathrm{loc}} : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$, then taking their difference $d = f^\flat - f_1^\flat$ gives an R-module homomorphism $A^\flat \to B^\flat$, which is non-zero only on at most $I_{A^\flat}$. Since $f^{\mathrm{loc}} \circ i_{\mathcal{A}} = i_{\mathcal{B}} \circ f^\flat = i_{\mathcal{B}} \circ f_1^\flat$, it follows that the R-module map $i_{\mathcal{B}} \circ (f^\flat - f_1^\flat) = i_{\mathcal{B}} \circ d = 0$. So $d(I_{A^\flat}) \subset N_{\mathcal{B}}$. Therefore for all $X_i, X_j \in I_{A^\flat}$, $f_1^\flat(X_i) = f^\flat(X_i) + \alpha$ and $f_1^\flat(X_j) = f^\flat(X_j) + \alpha'$ for some $\alpha, \alpha' \in N_{\mathcal{B}}$, we see that

$$\begin{aligned}
d(X_iX_j) &= f^\flat(X_iX_j) - f_1^\flat(X_iX_j) \\
&= f^\flat(X_i)f^\flat(X_j) - f_1^\flat(X_i)f_1^\flat(X_j) \\
&= f^\flat(X_i)f^\flat(X_j) - (f^\flat(X_i)+\alpha)(f^\flat(X_j)+\alpha') \\
&= f^\flat(X_i)f^\flat(X_j) - f^\flat(X_i)f^\flat(X_j) - \alpha f^\flat(X_j) - \alpha' f^\flat(X_i) - \alpha\alpha' \\
&= -\alpha f^\flat(X_j) - \alpha' f^\flat(X_i) - \alpha\alpha' \\
&= 0,
\end{aligned}$$

since $I_{B^\flat}N_{\mathcal{B}} = N_{\mathcal{B}}^2 = 0$ by Remark 1.3.6.

Therefore $d(I_{A^\flat}^2) = 0$, so d induces a well-defined morphism

$$d : I_{A^\flat}/I_{A^\flat}^2 \to N_{\mathcal{B}},$$

ie $d : t_{\mathcal{A}}^* \to N_{\mathcal{B}}$.

Given a homomorphism $f : A^{\mathrm{loc}} \to B^{\mathrm{loc}}$, we can lift to a homomorphism $f^\flat : A^\flat \to B^\flat$ as in the proof of Lemma 1.3.8. Any $d : t_{\mathcal{A}}^* \to N_{\mathcal{B}}$ gives a map of R-modules $d^\flat : A^\flat \to B^\flat$ such that $d(1) = 0$; consider the R-module map $g^\flat = f^\flat + d^\flat$. The map $A^{\mathrm{loc}} \to B^{\mathrm{loc}}$ induced by $g^\flat$ is f, since $d^\flat(I_{A^\flat}) \subset N_{\mathcal{B}}$ and $d(1) = 0$, and it remains to check that $g^\flat$ is a homomorphism of R-algebras. Let $a, b \in A^\flat$; $a = a' + r, b = b' + r'$ for some polynomials with trivial constant term $a', b' \in I_{A^\flat}$ and $r, r' \in R$.

$$\begin{aligned}
g^\flat(ab) &= f^\flat(ab) + d^\flat(ab) \\
&= f^\flat(a)f^\flat(b) + d^\flat(ab) \\
&= f^\flat(a)f^\flat(b) + d^\flat(a'r' + b'r),
\end{aligned}$$

whereas

$$\begin{aligned}
g^\flat(a)g^\flat(b) &= (f^\flat(a) + d^\flat(a))(f^\flat(b) + d^\flat(b)) \\
&= f^\flat(a)f^\flat(b) + f^\flat(a)d^\flat(b') + d^\flat(a')f^\flat(b) + d^\flat(a')d^\flat(b') \\
&= f^\flat(a)f^\flat(b) + f^\flat(r)d^\flat(b') + d^\flat(a')f^\flat(r') \\
&= f^\flat(a)f^\flat(b) + d^\flat(rb' + r'a')
\end{aligned}$$

by Remark 1.3.6 and R-linearity of $d^\flat$, and so we see that $g^\flat$ is indeed an R-algebra homomorphism. $\square$

Definition 1.4.12. The category DS_R is dual to the category DA_R. Its objects are of the form $\mathcal{G} = (G, G^\flat, i_\mathcal{G})$, where $G^\flat = \operatorname{Spec} A^\flat$, $G = \operatorname{Spec} A$, and there is a closed immersion $i_\mathcal{G} : G^{\mathrm{loc}} \hookrightarrow G^\flat$, for any triple $\mathcal{A} = (A, A^\flat, i_\mathcal{A}) \in DA_R$.

This category has a final object $\mathcal{R} = (\operatorname{Spec} R, \operatorname{Spec} R, \mathrm{id}_\mathcal{R})$, dual to the previously defined initial object $(R, R, \mathrm{id}_\mathcal{R}) \in DA_R$.

We denote the contravariant functor $DA_R \to DS_R$ given by

$$\mathcal{A} \rightsquigarrow (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{A})$$

by $\mathcal{S}$.

Proposition 1.4.13. *To every pair of objects $\mathcal{G}, \mathcal{H} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i_\mathcal{H}) \in DS_R$ (where B has augmentation ideal I_B) there is a direct product, ie*

1. *an object $\mathcal{G} \times \mathcal{H} \in DS_R$, and*

2. *projection morphisms $\overline{p}_1 : \mathcal{G} \times \mathcal{H} \to \mathcal{G}$ and $\overline{p}_2 : \mathcal{G} \times \mathcal{H} \to \mathcal{H}$,*

such that to every $\mathcal{K} \in DS_R$, with morphisms $\overline{f}_1 : \mathcal{K} \to \mathcal{G}$ and $\overline{f}_2 : \mathcal{K} \to \mathcal{H}$, there exists a unique morphism $\overline{g} : \mathcal{K} \to \mathcal{G} \times \mathcal{H}$ making the following diagram commute:

$$\begin{tikzcd} & \mathcal{K} \arrow[dl, "\overline{f}_1"'] \arrow[dr, "\overline{f}_2"] \arrow[dd, dashed, "\overline{g}"] & \\ \mathcal{G} & & \mathcal{H} \\ & \mathcal{G} \times \mathcal{H} \arrow[ul, "\overline{p}_1"] \arrow[ur, "\overline{p}_2"'] & \end{tikzcd} \tag{1.4.3}$$

Proof. Let $C = A \otimes B$, with augmentation ideal $I_A \otimes 1 + 1 \otimes I_B$. Then

$$C^{\mathrm{loc}} = \varprojlim_n (A \otimes B)/(I_A \otimes 1 + 1 \otimes I_B)^n,$$

and we can define $C^\flat$ using the method of the proof of Lemma 1.3.7. This gives us an object $\mathcal{G} \times \mathcal{H} = (\operatorname{Spec} C, \operatorname{Spec} C^\flat, i_{\mathcal{G}\times\mathcal{H}})$. There is a projection map $\mathcal{G} \times \mathcal{H} \to \mathcal{G}$ induced by the inclusion $A \to A \otimes B$ defined by $a \mapsto a \otimes 1$ for $a \in A$ (this lifts to a compatible map $A^\flat \to C^\flat$ by Lemma 1.3.8). Similarly there is a projection map for $\mathcal{H}$. We denote projection onto the first and second factor by $\overline{p}_1$ and $\overline{p}_2$ respectively.

Let $\mathcal{K} = (\operatorname{Spec}\mathscr{O}_K, \operatorname{Spec}\mathscr{O}_K^\flat, i_\mathcal{K}) \in DS_R$, and assume we have pairs of morphisms $\overline{f_1}, \overline{f_2}$ as in the statement of the Proposition. To complete the proof, we need to show that there is a unique morphism $\overline{g} : \mathcal{K} \to \mathcal{G} \times \mathcal{H}$ such that $p_i \circ \overline{g} = \overline{f_i}$ for $i = 1, 2$.

To $f_1 : \operatorname{Spec}\mathscr{O}_K \to G$ and $f_2 : \operatorname{Spec}\mathscr{O}_K \to H$ there's a unique morphism $g : \operatorname{Spec}\mathscr{O}_K \to G \times H$ such that $p_i \circ g = f_i$ for $i = 1, 2$ since $G \times H$ is a direct product in the category of schemes.

Also, again by the universal property of direct products, there is a unique morphism $g' : \operatorname{Spec}\mathscr{O}_K^\flat \to G^\flat \times H^\flat$ extending $f_1^\flat, f_2^\flat : \operatorname{Spec}\mathscr{O}_K^\flat \to G^\flat, H^\flat$. There's a natural closed immersion $(G \times H)^\flat \hookrightarrow G^\flat \times H^\flat$; if we can lift g' to a morphism $g : \operatorname{Spec}\mathscr{O}_K^\flat \to (G \times H)^\flat$, then we'll have proven existence of g. Uniqueness will then follow trivially, since $(G \times H)^\flat \hookrightarrow G^\flat \times H^\flat$ is a closed immersion.

$f_1^\flat$ and $f_2^\flat$ are dual to morphisms of algebras $f_1^{\flat *} : A^\flat \to \mathscr{O}_K^\flat$ and $f_2^{\flat *} : B^\flat \to \mathscr{O}_K^\flat$ such that $f_1^{\flat *}(I_{A^\flat}) \subset I_{K^\flat}$ and $f_2^{\flat *}(I_{B^\flat}) \subset I_{K^\flat}$. Since $f_1^\flat$ and $f_2^\flat$ lift morphisms f_1^{loc} and f_2^{loc}, by definition of morphisms in DS_R, it also follows that $f_1^{\flat *}(N_\mathcal{A}) \subset N_\mathcal{K}$ and $f_2^{\flat *}(N_\mathcal{B}) \subset N_\mathcal{K}$. By definition of direct product of schemes, $g'^* = D^* \circ (f_1^{*\flat} \otimes f_2^{*\flat})$, where $D^* : \mathscr{O}_K^\flat \otimes \mathscr{O}_K^\flat \to \mathscr{O}_K^\flat$ is the algebra map sending $k_1 \otimes k_2$ to $k_1 k_2$, for $k_1, k_2 \in \mathscr{O}_K^\flat$. Therefore $g'^*(I_{A^\flat} \otimes N_\mathcal{B}) \subset D^*(I_{K^\flat} \otimes N_\mathcal{K}) = I_{K^\flat} N_\mathcal{K} = 0$, and similarly $g'^*(N_\mathcal{A} \otimes I_{B^\flat}) \subset D^*(I_{K^\flat} \otimes N_\mathcal{K}) = I_{K^\flat} N_\mathcal{K} = 0$. Therefore the ideal $I_{A^\flat} \otimes N_\mathcal{B} + N_\mathcal{A} \otimes I_{B^\flat}$ is in the kernel of g'^*, so g'^* factors through $(A^\flat \otimes B^\flat)/(I_{A^\flat} \otimes N_\mathcal{B} + N_\mathcal{A} \otimes I_{B^\flat}) \cong (A \otimes B)^\flat$, and hence $g' : \operatorname{Spec}\mathscr{O}_K^\flat \to G^\flat \otimes H^\flat$ factors through $(G \times H)^\flat$, as required.

□

1.5 Deformations of group schemes

We begin with a preliminary Lemma, which is a standard result from commutative algebra:

Lemma 1.5.1. *Let A be an R-algebra. The kernel of the ring morphism $A \otimes_R A \to A$ given by $a \otimes a' \mapsto aa'$ for $a, a' \in A$ is generated as an ideal by $a \otimes 1 - 1 \otimes a$, for all $a \in A$.*

Proof. Clearly $a\otimes 1 - 1\otimes a \mapsto 0$ for all a, so we only have to prove that if $\sum a_i \otimes b_i \mapsto 0$, then $\sum a_i \otimes b_i$ is in the ideal generated by $a\otimes 1 - 1\otimes a$.

$\sum a_i b_i = 0$ in A, since $\sum a_i \otimes b_i \mapsto 0$. But $\sum (a_i \otimes 1 - 1 \otimes a_i)(1\otimes b_j) = \sum a_i \otimes b_i - \sum 1 \otimes a_i b_i = \sum a_i \otimes b_i$, proving the result. $\square$

We now recall some basic properties of R-group schemes, the objects on which our theory of deformations is based.

Definition 1.5.2. Let Gr_R be the category of finite flat commutative affine R-group schemes.

By definition, each $G \in \mathrm{Gr}_R$ is an affine R-scheme admitting morphisms $\varepsilon : \operatorname{Spec} R \to G$, $\Delta : G \otimes G \to G$, and $i : G \to G$ satisfying certain 'group' axioms found in for example, [Tat97].

With these axioms, each group scheme gives rise to a contravariant functor from schemes to groups, given by $S \rightsquigarrow \mathrm{Hom}_R(S, G)$, for each R-scheme S.

Finally, we are ready to introduce the main objects of this thesis: deformations of R-group schemes:

Definition 1.5.3. We define the category DG_R of deformations of R-group schemes to be the category of objects consisting of a $\mathcal{G} \in DS_R$, together with morphisms $\overline{\Delta} : \mathcal{G}\times\mathcal{G} \to \mathcal{G}$, $\overline{\varepsilon} : \mathcal{R} \to \mathcal{G}$ (with ε^* the augmentation morphism) and $\overline{i} : \mathcal{G} \to \mathcal{G}$ (called multiplication, unit, and inverse) such that the following diagrams are commutative:

$$\begin{tikzcd} \mathcal{G}\times\mathcal{G}\times\mathcal{G} \arrow[r, "\overline{\Delta}\times\overline{\mathrm{id}}"] \arrow[d, "\overline{\mathrm{id}}\times\overline{\Delta}"] & \mathcal{G}\times\mathcal{G} \arrow[d, "\overline{\Delta}"] \\ \mathcal{G}\times\mathcal{G} \arrow[r, "\overline{\Delta}"] & \mathcal{G} \end{tikzcd}$$

(associativity)

$$\begin{tikzcd} \mathcal{R}\times\mathcal{G} \arrow[r, "\overline{\varepsilon}\times\overline{\mathrm{id}}"] \arrow[d, "\overline{p}_2"] & \mathcal{G}\times\mathcal{G} \arrow[d, "\overline{\Delta}"] \\ \mathcal{G} \arrow[r, "\cong"] & \mathcal{G} \end{tikzcd}$$

(counit), and

$$\begin{tikzcd} \mathcal{G} \arrow[r, "(\overline{i}\times\overline{\mathrm{id}})\circ\overline{D}"] \arrow[d] & \mathcal{G}\times\mathcal{G} \arrow[d, "\overline{\Delta}"] \\ \mathcal{R} \arrow[r, "\overline{\varepsilon}"] & \mathcal{G} \end{tikzcd}$$

(inverse), where $\overline{D} : \mathcal{G} \to \mathcal{G} \times \mathcal{G}$ is the morphism induced by the algebra map $A^\flat \otimes A^\flat \to A^\flat$ coming from multiplication, as follows: this morphism has kernel containing $I_{A^\flat} \otimes N_{\mathcal{G}} + N_{\mathcal{G}} \otimes I_{A^\flat}$, and since $(A \otimes A)^\flat = (A^\flat \otimes A^\flat)/(I_{A^\flat} \otimes N_{\mathcal{G}} + N_{\mathcal{G}} \otimes I_{A^\flat})$, this morphism factors through $(A \otimes A)^\flat$. By Lemma 1.5.1, the kernel of the resulting homomorphism $(A \otimes A)^\flat \to A^\flat$ is the image in $(A \otimes A)^\flat$ of the ideal of $A^\flat \otimes A^\flat$ generated by $a \otimes 1 - 1 \otimes a$ in $A^\flat \otimes A^\flat$, for all $a \in A^\flat$. The multiplication map $A \otimes A \to A$ induces the same morphism on $A^{\mathrm{loc}} \otimes A^{\mathrm{loc}}$.

Additionally, we require that the following diagram commutes:

$$\begin{tikzcd} \mathcal{G} \times \mathcal{G} \arrow[r, "\overline{T}"] \arrow[d, "\mathrm{id}"] & \mathcal{G} \times \mathcal{G} \arrow[d, "\overline{\Delta}"] \\ \mathcal{G} \times \mathcal{G} \arrow[r, "\overline{\Delta}"] & \mathcal{G} \end{tikzcd}$$

(commutatvity), where $\overline{T} : \mathcal{G} \times \mathcal{G} \to \mathcal{G} \times \mathcal{G}$ is the twisting map induced, on the level of algebras, by the map $(A \otimes A)^\flat \to (A \otimes A)^\flat$ interchanging $X_i \otimes 1$ and $1 \otimes X_i$.

This concludes the definition of objects of DG_R. A *morphism* $\mathcal{G} \to \mathcal{H} \in DG_R$ is a morphism $\overline{f} : \mathcal{G} \to \mathcal{H}$ of $\mathcal{G}$ and $\mathcal{H}$ considered as objects of DS_R, such that it commutes with $\overline{\Delta}, \overline{\varepsilon}, \overline{i}$: $\overline{\Delta}_{\mathcal{H}} \circ (\overline{f} \otimes \overline{f}) = \overline{f} \circ \overline{\Delta}_{\mathcal{G}}$, $\overline{\varepsilon}_{\mathcal{H}} = \overline{f} \circ \overline{\varepsilon}_{\mathcal{G}}$, and $\overline{f} \circ \overline{i}_{\mathcal{G}} = \overline{i}_{\mathcal{H}} \circ \overline{f}$.

Remark 1.5.4. The above axioms imply that $G = \operatorname{Spec} A$ is a commutative affine group scheme with multiplication Δ, unit ε and inverse i. In fact, the above axioms applied to $\operatorname{Spec} A$ give exactly the conditions for a triple of morphisms (Δ, ε, i) to make it a group scheme.

Proposition 1.5.5. *DG_R is an additive category. In particular, DG_R has the following properties (see [ML71, page 190]):*

1. *DG_R has a null (initial and terminal) object.*

2. $\mathrm{Hom}(\mathcal{G}, \mathcal{H})$ *is an abelian group (written additively), and composition of morphisms is bilinear with respect to addition in the group*

3. *To every pair $\mathcal{G}, \mathcal{H} \in DG_R$, we have a biproduct $\mathcal{G} \times \mathcal{H}$, together with projections p_1, p_2 and inclusions i_1, i_2 to and from each of $\mathcal{G}, \mathcal{H}$, such that*

   (a) $p_1 \circ i_1 = \mathrm{id}_{\mathcal{G}}$

(b) $p_2 \circ i_2 = \mathrm{id}_{\mathcal{H}}$

(c) $i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{id}_{\mathcal{G}\times\mathcal{H}}$

where the sum $i_1 \circ p_1 + i_2 \circ p_2$ *is taken in the group* $\mathrm{Hom}(\mathcal{G} \times \mathcal{H}, \mathcal{G} \times \mathcal{H})$.

Proof. Proof of 1):We take $\mathcal{R}$ to be our null object. To every $\mathcal{G} \in DG_R$ there is a unique morphism $\mathcal{G} \to \mathcal{R}$; it's the pair of morphisms making A and $A^\flat$ into R-algebras. There's also a morphism $\overline{\varepsilon} : \mathcal{R} \to \mathcal{G}$, which is unique by compatibility with the unit map: if $\overline{\delta} : \mathcal{R} \to \mathcal{G}$ is another morphism, then we must have $\overline{\delta} \circ \overline{\varepsilon}_{\mathcal{R}} = \overline{\varepsilon}_{\mathcal{G}}$, which uniquely determines $\overline{\delta}$ since $\overline{\varepsilon}_{\mathcal{R}} = \mathrm{id}_{\mathcal{R}}$. This proves that $\mathcal{R}$ is a null object.

Proof of 2): we must first define a group law on $\mathrm{Mor}(\mathcal{G}, \mathcal{H})$. If $\overline{f}, \overline{g} \in \mathrm{Mor}(\mathcal{G}, \mathcal{H})$, we define $\overline{f} * \overline{g} = \overline{\Delta_{\mathcal{H}}} \circ (\overline{f} \otimes \overline{g}) \circ \overline{D}$. It follows from the group axioms satisfied by $\mathcal{H}$ that this makes $\mathrm{Mor}(\mathcal{G}, \mathcal{H})$ into an abelian group, where the identity is the unique map $\mathcal{G} \to \mathcal{R} \to \mathcal{H}$ (unique since $\mathcal{R}$ is a null object by part 1)), and the inverse map is defined by $\overline{f} \mapsto \overline{i}_{\mathcal{H}} \circ \overline{f}$. This group law is commutative since $\mathcal{H}$ is commutative, and it is hereafter denoted by $+$.

In order to show that composition is bilinear with respect to this group law, let $\mathcal{B} \in DG_R$. Then for all morphisms $\overline{g}, \overline{h} \in \mathrm{Hom}(\mathcal{G}, \mathcal{H})$ and $\overline{j}, \overline{k} \in \mathrm{Hom}(\mathcal{H}, \mathcal{B})$, we must show that $(\overline{j} + \overline{k}) \circ (\overline{f} + \overline{g}) = \overline{j} \circ \overline{f} + \overline{j} \circ \overline{g} + \overline{k} \circ \overline{f} + \overline{k} \circ \overline{g}$. This follows because by definition morphisms in DG_R commute with the group operation.

Proof of 3): We take as our biproduct the direct product $\mathcal{G} \times \mathcal{H}$ defined in the category DS_R. We set its group law to be $\overline{\Delta}_{\mathcal{G}\times\mathcal{H}} = \overline{\Delta}_{\mathcal{G}} \times \overline{\Delta}_{\mathcal{H}}$. The unit and inverse maps are defined as follows: $\overline{\varepsilon}_{\mathcal{G}\times\mathcal{H}} = \overline{\varepsilon}_{\mathcal{G}} \times \overline{\varepsilon}_{\mathcal{H}} \circ \overline{D}_{\mathcal{R}}$, and $\overline{i}_{\mathcal{G}\times\mathcal{H}} = \overline{i}_{\mathcal{G}} \times \overline{i}_{\mathcal{H}}$, where $\overline{D}_{\mathcal{R}} : \mathcal{R} \to \mathcal{R} \times \mathcal{R}$ is the map dual to multiplication on the level of algebras: $R \otimes R \to R$. The projection maps we take are those defined for the direct product.

Our inclusion maps $i_1 : \mathcal{G} \to \mathcal{G} \times \mathcal{H}$ and $i_2 : \mathcal{H} \to \mathcal{G} \times \mathcal{H}$ are the maps induced by the algebra map $A \otimes B \to A$ (quotient by $1 \otimes I_B$) and $A \otimes B \to A$ (quotient by $I_A \otimes 1$).

It's clear that the morphisms $p_1 \circ i_1$ and $p_2 \circ i_2$ are the identity on $\mathcal{G}$ and $\mathcal{H}$ respectively, so we only have left to show that $i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{id}_{\mathcal{G}\times\mathcal{H}}$. Translating this condition into group morphisms implies that we must prove $\overline{\Delta}_{\mathcal{G}\times\mathcal{H}} \circ ((i_1 \circ p_1) \times (i_2 \circ p_2)) \circ \overline{D} = \mathrm{id}_{\mathcal{G}\times\mathcal{H}}$.

Since $i_1 \circ p_1 = \mathrm{id}_{\mathcal{G}} \times \varepsilon_{\mathcal{H}}$ and $i_2 \circ p_2 = \varepsilon_{\mathcal{G}} \times \mathrm{id}_{\mathcal{H}}$, it suffices to prove that

$$\overline{\Delta}_{\mathcal{G}\times\mathcal{H}} \circ (\mathrm{id}_{\mathcal{G}} \times \overline{\varepsilon}_{\mathcal{H}}) \times (\overline{\varepsilon}_{\mathcal{G}} \times \mathrm{id}_{\mathcal{H}}) \circ \overline{D} = \mathrm{id}_{\mathcal{G}\times\mathcal{H}}, \tag{1.5.1}$$

where we identify $\varepsilon_{\mathcal{G}}$ with its composition with the unique structure morphism $\mathcal{G} \to \mathcal{R}$, and $\varepsilon_{\mathcal{H}}$ with its composition with the unique structure morphism $\mathcal{H} \to \mathcal{R}$.

By the unit axiom, $\overline{\Delta}_{\mathcal{G}} \circ (\mathrm{id}_{\mathcal{G}} \times \overline{\varepsilon}_{\mathcal{G}}) \circ \overline{D}_{\mathcal{G}} = \mathrm{id}_{\mathcal{G}}$ (and similarly for $\mathcal{H}$). Therefore, comparing with equation (1.5.1), we see that $\overline{\Delta}_{\mathcal{G}\times\mathcal{H}} \circ (i_1 \circ p_1 \times i_2 \circ p_2) \circ \overline{D} = \mathrm{id}_{\mathcal{G}} \times \mathrm{id}_{\mathcal{H}} = \mathrm{id}_{\mathcal{G}\times\mathcal{H}}$.

Therefore part 3) holds, and $\mathcal{G} \times \mathcal{H}$ is the required biproduct. Therefore DG_R is an additive category. □

Lemma 1.5.6. *Given any* $\mathcal{A} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_A) \in DS_R$*, there is a unique* $\overline{\varepsilon}$ *such that* $\operatorname{Ker} \varepsilon^* = I_A$.

Proof. If $\operatorname{Ker} \varepsilon^* = I_A$, then the induced morphism $\varepsilon^{*\mathrm{loc}}$ sends $I_{A^{\mathrm{loc}}}$ to zero. By the compatibility condition for morphisms, $\varepsilon^{*\flat}$ sends $I_{A^\flat}$ to zero, since the projection $A^\flat \to A^{\mathrm{loc}}$ sends $I_{A^\flat}$ to inside $I_{A^{\mathrm{loc}}}$ by definition. Thus $\varepsilon^\flat$, and hence $\overline{\varepsilon}$, is unique. □

Proposition 1.5.7. *Given any* $\mathcal{A} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_A) \in DS_R$*, together with morphisms* (Δ, i, ε) *on* $\operatorname{Spec} A$ *satisfying the axioms for a commutative* R*-group scheme, there's a unique way to extend our morphisms to morphisms* $\overline{\Delta}, \overline{i}, \overline{\varepsilon}$ *in* DS_R *such that* $\mathcal{A}$ *is a group object in* DG_R.

Proof. $\Delta^{*\mathrm{loc}}$ lifts to a morphism $f : A^\flat \to (A \otimes A)^\flat$ by Lemma 1.3.8. In order for the unit axiom to be satisfied, we require that $(\varepsilon^{*\flat} \otimes \mathrm{id}) \circ f = \mathrm{id}_{A^\flat}$, where the isomorphism $R \otimes A^\flat \xrightarrow{\cong} A^\flat$ is implicit on the left hand side.

Let $d_2^\flat = (\varepsilon^{*\flat} \otimes \mathrm{id}) \circ f - \mathrm{id}_{A^\flat}$. Since $(\varepsilon^{*\mathrm{loc}} \otimes \mathrm{id}) \circ \Delta^{*\mathrm{loc}} = \mathrm{id}_{A^{\mathrm{loc}}}$ (as A^{loc} represents a group scheme), and f lifts $\Delta^{*\mathrm{loc}}$, $d_2(I_{A^\flat}) \subset N_{\mathcal{G}}$. Let $f' = f - (p_2 \circ d_2^\flat)$, where $p_2 : A^\flat \to (A \otimes A)^\flat$ is given by $a \mapsto 1 \otimes a$. f' is a morphism of algebras by Proposition 1.4.11. Clearly f' lifts $\Delta^{*\mathrm{loc}}$ and satisfies the left-unit axiom. Further, f' is uniquely determined modulo $I_{A^\flat} \otimes 1$ by the left-unit axiom.

In order to satisfy the right-unit axiom, we take $f'' = f' - (p_1 \circ d_1^\flat)$, for some $d_1^\flat$. This map clearly still satisfies the left-unit axiom, and is now uniquely determined modulo $1 \otimes I_{A^\flat}$.

Hence it is uniquely determined modulo $I_{A^\flat} \otimes I_{A^\flat}$. Since f'' is also uniquely determined modulo $1 \otimes N_G + N_G \otimes 1$ as it lifts $\Delta^{*\mathrm{loc}}$, it is uniquely determined modulo $N_G \otimes 1 + 1 \otimes N_G \cap I_{A^\flat} \otimes I_{A^\flat} = 0$ in $(A \otimes A)^\flat$. Hence there is a unique f'' satisfying the unit axiom and lifting $\Delta^{*\mathrm{loc}}$.

We now prove that our map satisfies the commutativity axiom. f'' is symmetric modulo $N_G \otimes 1 + 1 \otimes N_G$ since it lifts $\Delta^{*\mathrm{loc}}$, and symmetric modulo $I_{A^\flat} \otimes I_{A^\flat}$, by the left and right unit axioms. Since the intersection of these ideals is zero, f'' satisfies the commutativity axiom.

Since A^{loc} is a group scheme, the associativity axiom holds modulo the ideal $1 \otimes 1 \otimes N_G + 1 \otimes N_G \otimes 1 + N_G \otimes 1 \otimes 1$ of $(A \otimes A \otimes A)^\flat$. If we can prove associativity holds modulo $I_{A^\flat} \otimes I_{A^\flat} \otimes I_{A^\flat}$, we'll have proved it holds, since

$$I_{A^\flat} \otimes I_{A^\flat} \otimes I_{A^\flat} \cap (1 \otimes 1 \otimes N_G + 1 \otimes N_G \otimes 1 + N_G \otimes 1 \otimes 1) = \{0\}$$

in $(A \otimes A \otimes A)^\flat$.

The unit axiom tells us that $(\varepsilon^{*\flat} \otimes \mathrm{id}) \circ \Delta^{*\flat} = \mathrm{id}$; substituting this identity into the formulas $(\Delta^{*\flat} \otimes \mathrm{id}) \circ \Delta^{*\flat}$ and $(\mathrm{id} \otimes \Delta^{*\flat}) \circ \Delta^{*\flat}$ gives

$$(\varepsilon^{*\flat} \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\Delta^{*\flat} \otimes \mathrm{id}) \circ \Delta^{*\flat} = (\mathrm{id} \otimes \mathrm{id}) \circ \Delta^{*\flat} = \Delta^{*\flat}$$

and

$$(\varepsilon^{*\flat} \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \Delta^{*\flat}) \circ \Delta^{*\flat} = \Delta^{*\flat} \circ (\varepsilon^{*\flat} \otimes \mathrm{id}) \circ \Delta^{*\flat} = \Delta^{*\flat}.$$

Therefore associativity holds modulo the kernel of $\varepsilon \otimes \mathrm{id} \otimes \mathrm{id}$, which is $I_{A^\flat} \otimes 1 \otimes 1$.

By symmetry, associativity also holds modulo $1 \otimes I_{A^\flat} \otimes 1$ and $1 \otimes 1 \otimes I_{A^\flat}$, and the intersection of these three ideals is $I_{A^\flat} \otimes I_{A^\flat} \otimes I_{A^\flat}$, hence by the above argument, associativity holds.

Therefore letting $\Delta^{*\flat} = f''$, we see that the associativity, commutativity and unit axioms are satisfied. To complete the proof, we need to lift the inverse morphism $i^{*\mathrm{loc}} : A^{\mathrm{loc}} \longrightarrow A^{\mathrm{loc}}$ to a morphism $i^{*\flat} : A^\flat \longrightarrow A^\flat$ satisfying the inverse axiom, ie satisfying the relation

$$D^{*\flat} \circ (i^{*\flat} \otimes \mathrm{id}_{A^\flat}) \circ \Delta^{*\flat} = \varepsilon^{*\flat}. \tag{1.5.2}$$

Let $i' : A^\flat \longrightarrow A^\flat$ be any lifting of i^{loc} (we know we can lift i^{loc} by Lemma 1.3.8).

Let $d : A^\flat \longrightarrow A^\flat$ be the difference $D^{*\flat} \circ (i' \otimes \mathrm{id}_{A^\flat}) \circ \Delta^{*\flat} - \varepsilon^{*\flat}$, as a morphism of R-modules. Since i^{loc} satisfies the inverse axiom for A^{loc}, it follows that $d(I_{A^\flat}) \subset N_{\mathcal{G}}$.

Let $i^{*\flat} = i' - d$, which is a morphism of R-algebras by Proposition 1.4.11. We now show it satisfies relation (1.5.2), ie that it sends any $X \in I_{A^\flat}$ to zero: by consideration of the counit axiom, it follows that

$$\Delta^{*\flat}(X) = X \otimes 1 + 1 \otimes X + \sum_{i,j} Y_i \otimes Z_j$$

for some $Y_i, Z_i \in I_{A^\flat}$.

Applying the left hand side of (1.5.2) to X gives:

$$\begin{aligned} &D^{*\flat} \circ (i^{*\flat} \otimes \mathrm{id}_{A^\flat})(X \otimes 1 + 1 \otimes X + \sum_{i,j} Y_i \otimes Z_j) \\ &= i^{*\flat}(X) + X + \sum_{i,j} i^{*\flat}(Y_i) Z_j = i'(X) - d(X) + X + \sum_{i,j} i'(Y_i) Z_j \end{aligned} \tag{1.5.3}$$

where the last line follows since $d(I_{A^\flat}) \subset N_{\mathcal{G}}$ and $I_{A^\flat} N_{\mathcal{G}} = 0$. Since

$$d(X) = (D^{*\flat} \circ (i' \otimes \mathrm{id}_{A^\flat}) \circ \Delta^{*\flat})(X) - \varepsilon^{*\flat}(X) = i'(X) + X + \sum_{i,j} i'(Y_i) Z_j,$$

it follows that $D^{*\flat} \circ (i^{*\flat} \otimes \mathrm{id}_{A^\flat}) \circ \Delta^{*\flat}(X) = 0$, and therefore the inverse condition (1.5.2) is satisfied.

Therefore, with this choice of lifting $i^{*\flat}$ of $i^{*\mathrm{loc}}$, all the group axioms are satisfied.

Uniqueness of $i^{\flat *}$ follows immediately from the last line of (1.5.3).

□

Corollary 1.5.8. *Let $\mathcal{G}$ and $\mathcal{H}$ be as above. If $f : G \longrightarrow H$ is a morphism of group schemes then any lift of f to a morphism $f^\flat : G^\flat \longrightarrow H^\flat$ has the property that $\Delta^\flat \circ (f^\flat \otimes f^\flat) = f^\flat \circ \Delta^\flat$. (The existence of a lifting of f to $f^\flat$ is guaranteed by Lemma 1.3.8).*

Proof. Suppose otherwise. Then we have two different morphisms $(G \times G)^\flat \longrightarrow H^\flat$: $\Delta^\flat \circ (f^\flat \otimes f^\flat)$, and $f^\flat \circ \Delta^\flat$.

Composing $\overline{\Delta} \circ i_{1,2}$ with $f^\flat$ gives $f^\flat \circ \overline{\Delta} \circ i_{1,2} = f^\flat$ by the unit axiom; $i_{1,2} \circ (f^\flat) = (f^\flat \otimes f^\flat) \circ i_{1,2}$ by the canonical definition of $f^\flat \otimes f^\flat$, and therefore $\overline{\Delta} \circ (f^\flat \otimes f^\flat) \circ i_{1,2} = f^\flat$, and proceeding as in the proof of the previous proposition gives the required result. □

Definition 1.5.9. There's a forgetful functor $DG_R \to \mathrm{Gr}_R$ sending $\mathcal{G} = (G, G^\flat, i_\mathcal{G})$ to G, which we denote by $\mathcal{F}$. This follows since $G \in \mathrm{Gr}_R$ by Remark 1.5.4.

Definition 1.5.10. We define a category DG_R^*. Its objects are the same as those of DG_R, but morphisms are not the same: if $\mathcal{G}, \mathcal{H} \in DG_R$, let S be the subgroup of $\mathrm{Hom}_{DG_R}(\mathcal{G}, \mathcal{H})$ of morphisms $\overline{f}$ such that $\mathcal{F}(\overline{f}) : \mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$ is the unique morphism of group schemes factoring over $\operatorname{Spec} R$. We define $\mathrm{Hom}_{DG_{R^*}}(\mathcal{G}, \mathcal{H}) = \mathrm{Hom}_{DG_R}(\mathcal{G}, \mathcal{H})/S$.

Proposition 1.5.11. *Let $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_R^*$. Then*

1. *there is a minimal object $\mathcal{G}' \in DG_R^*$ such that $\mathcal{F}(\mathcal{G}') \cong \mathcal{F}(\mathcal{G})$, the isomorphism being in Gr_R, and*

2. *any minimal object $\mathcal{G}' \in DG_R^*$ such that $\mathcal{F}(\mathcal{G}') \cong \mathcal{F}(\mathcal{G})$ is isomorphic to $\mathcal{G}$, the isomorphism being in DG_R^*.*

Proof. Let $\mathcal{G}' = (\operatorname{Spec} A, \operatorname{Spec} B^\flat, i_{\mathcal{G}'}) \in DS_R$ be minimal. The comultiplication on A extends to $B^\flat$ by Proposition 1.5.7, making $\mathcal{G}'$ into an object in DG_R. By Corollary 1.5.8, id_A lifts to morphisms $A^\flat \to B^\flat$ and $B^\flat \to A^\flat$ which are compatible with comultiplication, and are therefore in DG_R^*. These morphisms make $\mathcal{G}$ isomorphic to $\mathcal{G}'$.

The existence of such a minimal $\mathcal{G}' \in DS_R$ follows by Lemma 1.4.10; the previous argument shows that the group operation can be lifted to $\operatorname{Spec} B^\flat$, defining an object in DG_R^*. □

Lemma 1.5.12. *There's a functor $\mathcal{F}' : \mathrm{Gr}_R \to DG_R^*$, such that $\mathcal{F}(\mathcal{F}'(G)) = G$ for all $G \in \mathrm{Gr}_R$, and $\mathcal{F}(\mathcal{F}'(f)) = f$ for all morphisms f in Gr_R, where we write $\mathcal{F} : DG_R^* \to \mathrm{Gr}_R$ to denote the functor induced from $\mathcal{F} : DG_R \to \mathrm{Gr}_R$.*

Proof. Let $G \in \mathrm{Gr}_R$ be represented by the R-algebra $A = R[X_1, \ldots, X_n]/I$. By Lemma 1.3.7, since A is flat and hence free over the local ring R, there's a corresponding object $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_R$ for some $A^\flat$. By Proposition 1.5.11, all such $\mathcal{G}$ are isomorphic in DG_R^*, and therefore our object $\mathcal{F}'(G)$ is unique up to isomorphism. Any morphism of group schemes $G \to H$, where H is represented by the R-algebra B and lifts to $\mathcal{H} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i_{\mathcal{H}})$, lifts to a morphism $\mathcal{G} \to \mathcal{H}$ by Corollary 1.5.8. The lifting is unique in $DG^*_{k,\mathcal{O}}$, since any two liftings differ by a morphism $\mathcal{G} \to \mathcal{H}$ lifting the zero morphism $G \to H$, and therefore are identified in $\operatorname{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$. □

Proposition 1.5.13. *The functor induced by $\mathcal{F}$ from DG^*_R to Gr_R is an equivalence of categories.*

Remark 1.5.14. We abuse notation in this proposition by using the same notation for the functors induced from $\mathcal{F}$ and $\mathcal{F}'$ from and to DG^*_R instead of DG_R. That such functors are well-defined is clear.

Remark 1.5.15. We use the criterion of [GM99, §2, Theorem 1.13] (Freyd's Theorem) which states that $\mathcal{F}$ is an equivalence of categories if and only if

1. $\mathcal{F}$ is a fully faithful functor
2. any object $Y \in \mathrm{Gr}_R$ is isomorphic to an object of the form $\mathcal{F}(X)$ for some object $X \in DG^*_R$.

Proof. Consider the map induced by $\mathcal{F}$:

$$\operatorname{Hom}_{DG^*_R}(\mathcal{G}, \mathcal{H}) \to \operatorname{Hom}_{G_R}(\mathcal{F}(\mathcal{G}), \mathcal{F}(\mathcal{H})).$$

This map is injective by construction of DG^*_R, and surjective because any morphism of group schemes lifts to a morphism $\mathcal{G} \to \mathcal{H}$ of deformed schemes by Proposition 1.5.8 (augmentation ideals are mapped inside augmentation ideals by compatibility with the unit morphism). Hence $\mathcal{F}$ is fully faithful.

To see that any $G \in \mathrm{Gr}_R$ is isomorphic to $\mathcal{F}(\mathcal{G})$ for some $\mathcal{G} \in DG^*_R$, note that we can lift G to a $\mathcal{G} = (G, G^\flat, i_{\mathcal{G}}) \in DS_R$ by Lemma 1.3.7. Comultiplication Δ lifts to a (unique) comultiplication on $G^\flat$ by Proposition 1.5.7, and therefore $\mathcal{G} \in DG^*_R$.

Hence $\mathcal{F}$ is an equivalence of categories, by the criterion of Remark 1.5.15. □

Corollary 1.5.16. *If Gr_R is an abelian category for some ring R, then so is DG^*_R.*

1.6 Deformed strict $\mathcal{O}$-modules

Let q be a power of p, such that $\mathbb{F}_q \subset k$, where $\mathbb{F}_q$ is the field with q elements. Let $\mathcal{O} = \mathbb{F}_q[[\pi]]$.

Finally we can introduce the main objects of this thesis; essentially they are objects $\mathcal{G} \in DG_R$, together with a homomorphism of rings

$$\mathcal{O} \longrightarrow \operatorname{End}_{DG_R} \mathcal{G}.$$

where R is an $\mathcal{O}$-algebra.

This is analogous to the usual definition of a module, which is an abelian group G, and a ring R, such that there is a homomorphism of rings $R \longrightarrow \operatorname{End}(G)$.

Formally, if

$$\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG_R,$$

we define an *$\mathcal{O}$-action* of $\mathcal{G}$ to be a homomorphism from $\mathcal{O}$ to $\operatorname{End}_{DG_R}(\mathcal{G})$. This means that $\mathcal{O}$ is compatible with multiplication on G; if this holds, then the $\mathcal{O}$ action on $G^\flat$ will be automatically compatible with $\Delta^\flat$ by Prop 1.5.8. A, A^{loc} and $A^\flat$ are R-algebras, and since R is assumed to be an $\mathcal{O}$-algebra as stated above, we get an action of $o \in \mathcal{O}$ on R, and since $A, A^\flat$ and A^{loc} are R-algebras, we get an action of o on them via the morphisms $R \longrightarrow A, A^{\mathrm{loc}}, A^\flat$, which we denote by $a \longmapsto oa$.

We also get an action of $o \in \mathcal{O}$ on A, A^{loc} and $A^\flat$ coming from the homomorphism from $\mathcal{O}$ to $\operatorname{End}(\mathcal{G})$; we denote this by $a \longmapsto o^*a$, $a^{\mathrm{loc}} \longmapsto o^*a^{\mathrm{loc}}$, and $a^\flat \longmapsto o^*a^\flat$, for $a \in A$, $a^{\mathrm{loc}} \in A^{\mathrm{loc}}$ and $a^\flat \in A^\flat$.

Definition 1.6.1. We say that an $\mathcal{O}$ action on $\mathcal{G}$ is *strict* if the action of $o \in \mathcal{O}$ on $a \in A^\flat$ induces scalar multiplication on $t^*_{\mathcal{G}}$, ie $\overline{o^*a} = o\overline{a}$, where $\overline{a}$ denotes the image of a in $t^*_{\mathcal{G}}$, and if $a \in N_{\mathcal{G}}$, then $o^*a = oa$. We also refer to this as $\mathcal{O}$ acting *by scalars* on $\mathcal{G}$.

We define a category $DG_{R,\mathcal{O}}$ whose objects consist of a $\mathcal{G} \in DG_R$, together with a strict action of $\mathcal{O}$ on $\mathcal{G}$, and whose morphisms are morphisms of the underlying objects in the category DG_R, such that they are compatible with the $\mathcal{O}$-action, ie the following diagram is commutative (where $f : \mathcal{G} \longrightarrow \mathcal{H}$ is any morphism in the sense of DG_R)

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{f} & \mathcal{H} \\ \downarrow{\scriptstyle o^*} & & \downarrow{\scriptstyle o^*} \\ \mathcal{G} & \xrightarrow{f} & \mathcal{H}. \end{array} \tag{1.6.1}$$

Note that this diagram commutes for $f = \overline{\Delta}$ and $\mathcal{H} = \mathcal{G} \times \mathcal{G}$ automatically, since $\mathcal{O}$ acts as endomorphisms of $\mathcal{G}$ by definition.

Similarly to DG^*_R, we define $DG^*_{R,\mathcal{O}}$ to be the category whose objects are identical to those of DG^*_R, but such that for any $\mathcal{G}, \mathcal{H} \in DG^*_{R,\mathcal{O}}$, $\mathrm{Hom}_{DG^*_{R,\mathcal{O}}}(\mathcal{G}, \mathcal{H}) = \mathrm{Hom}_{DG_{R,\mathcal{O}}}(\mathcal{G}, \mathcal{H})/S$, where S is the subgroup of $\mathrm{Hom}_{DG_{R,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$ consisting of those $\overline{f}$ such that $f : G \to H$ factors through $\mathrm{Spec}\, R$, ie is the 'zero' morphism. This definition of morphisms is clearly analogous to that of Definition 1.5.10.

Remark 1.6.2. If $\mathcal{G}, \mathcal{H} \in DG^*_{R,\mathcal{O}}$, then

$$\mathrm{Hom}_{DG^*_{R,\mathcal{O}}}(\mathcal{G}, \mathcal{H}) \subset \mathrm{Hom}_{DG^*_R}(\mathcal{G}, \mathcal{H}),$$

where $\mathcal{G}$ and $\mathcal{H}$ are considered as objects of DG^*_R (without $\mathcal{O}$-action).

Definition 1.6.3. We say that $\mathcal{G} \in DG^*_{R,\mathcal{O}}$ (or $\in DG_{R,\mathcal{O}}$) is étale (resp. connected) if $\mathcal{F}(\mathcal{G})$ is étale (resp. connected). We say that a sequence of strict deformed group schemes

$$0 \to \mathcal{G}' \xrightarrow{\overline{f}} \mathcal{G} \xrightarrow{\overline{f}'} \mathcal{G}'' \to 0$$

is exact (identifying 0 with $\mathcal{R}$) if the corresponding sequence

$$0 \to \mathcal{F}(\mathcal{G}') \xrightarrow{f} \mathcal{F}(\mathcal{G}) \xrightarrow{f'} \mathcal{F}(\mathcal{G}'') \to 0$$

is exact on the level of group schemes, ie if f is a closed immersion and f' is faithfully flat. Note that f need not be flat; for instance, consider the following short exact sequence in Gr_R over a field k of characteristic p:

$$0 \to \alpha_p \hookrightarrow \mathbb{G}_a \xrightarrow{\mathrm{Frob}^p} \mathbb{G}_a \to 0$$

Note that if $\mathcal{G}$ in DG_R (or DG^*_R) is étale, then this immediately implies that $G^{\mathrm{loc}} = \mathrm{Spec}\, A^{\mathrm{loc}}$ is trivial, and therefore any such $\mathcal{G} = (G^{\text{ét}}, G^\flat, i_{\mathcal{G}})$ is isomorphic to a minimal object $(G^{\text{ét}}, \mathrm{Spec}\, R, 0)$ in DG_R (or $DG_{R,\mathcal{O}}$) respectively, by Proposition 1.5.11 (and Corollary 1.8.2) respectively.

Remark 1.6.4. We make some general remarks about base change.

1. Note that the definition of *objects* $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG_{R,\mathcal{O}}$ depends on the structure morphism $\mathcal{G} \mapsto \mathcal{R}$ in a subtler way than the definitions of objects in DG_R and Gr_R do:

   If $\mathcal{G} \in DG^*_{R,\mathcal{O}}$ is not étale, and R' is an $\mathcal{O}$-algebra, then base change $R \longrightarrow R'$ is only a functor if the diagram

$$\begin{tikzcd} R \arrow[rr] & & R' \\ & \mathcal{O} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

   commutes. This diagram must commute in order that $\mathcal{G} \otimes R' \in DG^*_{R,\mathcal{O}}$, because of the induced action on the R'-modules $N_{\mathcal{G}\otimes R'}$ and $t^*_{\mathcal{G}\otimes R'}$; each $o \in \mathcal{O}$ acting via the homomorphism $\mathcal{O} \longrightarrow \operatorname{End} \mathcal{G}$ acts on these R'-modules via the composition $\mathcal{O} \mapsto R \mapsto R'$; if o is to act 'by scalars', this must be equal to the action of o via the map $\mathcal{O} \mapsto R'$.

2. For étale $\mathcal{G} \in DG^*_{R,\mathcal{O}}$, $\mathcal{G} \otimes_R R' \in DG^*_{R',\mathcal{O}}$ for *any* base change morphism $R \longrightarrow R'$, since if $\mathcal{G}$ is étale, $N_{\mathcal{G}}$ and $I_{A^\flat}/I^2_{A^\flat}$ are the zero-module, so the condition that $\mathcal{O}$ act 'by scalars' is vacuous.

3. If $\mathcal{G} \in DG_{R,\mathcal{O}}$, then we can take the special fibre $\mathcal{G} \otimes k$ in DA_R by Lemma 1.4.4; the morphisms $\overline{\Delta}, \overline{\varepsilon}, \overline{i}$ reduce to morphisms of $\mathcal{G} \otimes k$ satisfying the group axioms, and therefore $\mathcal{G} \otimes k \in DG_k$. If we consider k as an $\mathcal{O}$-algebra via the composition $\mathcal{O} \longrightarrow R \longrightarrow k$, then since $N_{\mathcal{G}\otimes k} = N_{\mathcal{G}} \otimes k$ and $t^*_{\mathcal{G}\otimes k} = t^*_{\mathcal{G}} \otimes k$, it follows that $\mathcal{G} \otimes k \in DG^*_{k,\mathcal{O}}$. Therefore the special fibre of a strict $\mathcal{O}$-module is again a strict $\mathcal{O}$-module (in the appropriate category).

1.7 Examples

We're now in a position to define some objects in the categories DG_R and $DG_{R,\mathcal{O}}$.

1. If $R = k$, and k is an $\mathcal{O}$-algebra with π acting as the zero endomorphism of k, we may consider some $\mathcal{G} \in DG^*_{R,\mathcal{O}}$, such that $\mathcal{F}(\mathcal{G}) = \alpha_q$, where $\alpha_q =$

Spec $R[T]/(T^q)$ is the group scheme kernel of qth power Frobenius on $\mathbb{G}_a$.

$$\mathcal{F}'(\alpha_q) = (\operatorname{Spec} k[T]/(T^q), \operatorname{Spec} k[T]/(T^{q+1}), i_{\mathcal{F}'(\alpha_q)}).$$

Here $t^* = (T)/(T^2)$ and $N = (T^q)/(T^{q+1})$. Again we may take $o^*T = oT$ for $o \in \mathcal{O}$ as our strict $\mathcal{O}$-action; this works because $a^q = a$ for $a \in \mathbb{F}_q$ and $\pi^* = \pi = 0$ (so the action of π^* on $N_{\mathcal{G}}$ is also by scalars).

2. Let $\mathcal{LT}[\pi]$ be given by

$$(\operatorname{Spec} R[T]/(T^q - \pi T), \operatorname{Spec} R[T]/((T^q - \pi T)T), i_{\mathcal{LT}[\pi]}),$$

where $i_{\mathcal{LT}[\pi]}$ is dual to the obvious surjection $R[T]/((T^q-\pi T)T) \to R[T]/(T^q-\pi T)$, $\Delta^*(T) = T \otimes 1 + 1 \otimes T$, $\alpha^*T = \alpha T$ for $\alpha \in \mathbb{F}_q$, and $\pi^*T = \pi T - T^q$. Note that the special fibre of $\mathcal{LT}[\pi]$ is isomorphic to α_q as a group scheme, although the isomorphism does *not* extend to an isomorphism in $DG^*_{k,\mathcal{O}}$.

3. If $G = \operatorname{Spec} A$ is any étale R-group scheme, for R some $\mathcal{O}$-algebra, $\mathcal{F}'(G)$ may be made into a strict $\mathcal{O}$-group scheme by taking *any* homomorphism $\mathcal{O} \to \operatorname{End}(\mathcal{F}'(G))$. This is because we may take $A^\flat = A^{\mathrm{loc}} = R$ (if I_A is the augmentation ideal of A, $I_A^2 = I_A$ since G is étale), and then $t^* = N = (0)$, so the condition that $\mathcal{O}$ act 'by scalars' on these modules is vacuous.

1.8 First properties of strict deformations

Note that there are obvious forgetful functors $DG_R \to \mathrm{Gr}_R$ and $\mathcal{F} : DG_{R,\mathcal{O}} \to \mathrm{Gr}_R$ sending $\mathcal{G} = (G, G^\flat, i_G)$ to G.

Proposition 1.8.1. *Let* $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG^*_{R,\mathcal{O}}$. *If*

$$\mathcal{G}' = (\operatorname{Spec} A, 8 \operatorname{Spec} B^\flat, i_{\mathcal{G}})$$

in DG_R is minimal (the existence of such a minimal $\mathcal{G}'$ is guaranteed by Proposition 1.5.7), then the decomposition $A^\flat = B^\flat \oplus K$ of Corollary 1.4.8 is compatible with the $\mathcal{O}$-action, in the sense that $o^*(B^\flat) \subset B^\flat$ and $o^*K \subset K$, for all $o \in \mathcal{O}$.

Proof. $K \subset N_{\mathcal{G}}$, so by definition of strict action, $o^*k = ok$ for all $o \in \mathcal{O}$, hence $o^*K \subset K$ for all $o \in \mathcal{O}$. Suppose $o^*b \notin B^\flat$ for some $b \in I_{B^\flat}$, ie $o^*b = b' + k$ for some $b' \in B^\flat$ and $k \in K$. Reducing modulo $I_{A^\flat}^2$ gives

$$o^*\overline{b} = \overline{b}' + \overline{k}.$$

Since o^* acts on $t_{\mathcal{G}}^* = I_{A^\flat}/I_{A^\flat}^2$ 'by scalars' by definition, it follows that

$$\overline{b}' + \overline{k} = \overline{o}b \mod I_{A^\flat}^2$$

It follows that $\overline{k} = 0 \mod I_{B^\flat}$, and hence $k \in I_{B^\flat} + I_{A^\flat}^2$. But $K \cap I_{A^\flat}^2 = \{0\}$ and $K \cap I_{B^\flat} = \{0\}$ by Corollary 1.4.8. Since $I_{A^\flat}^2, I_{B^\flat} \subset B^\flat$, it follows that $k = 0$, and therefore $o^*B^\flat \subset B^\flat$ as required. □

Corollary 1.8.2. *Any $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG_{R,\mathcal{O}}^*$ is isomorphic to a minimal $\mathcal{G}' \in DG_{R,\mathcal{O}}^*$ (the isomorphism being in $DG_{R,\mathcal{O}}$).*

Proof. By Proposition 1.5.11, there's a minimal $\mathcal{G}' = (\operatorname{Spec} A, \operatorname{Spec} B^\flat, i_{\mathcal{G}}) \in DG_R^*$ which is isomorphic to $\mathcal{G}$ (the isomorphism being in DG_R^*) inducing $A^\flat \cong B^\flat \oplus K$ by Lemma 1.4.8. Since $o^*B^\flat \subset B^\flat$ in $A^\flat$ by the proposition, we can give $B^\flat$ the same $\mathcal{O}$-action it has as a submodule of $A^\flat$, and we get a map $B^\flat \longrightarrow B^\flat \oplus K$ which is $\mathcal{O}$-linear (hence strict). Therefore we get a strict map $\mathcal{G} \longrightarrow \mathcal{G}'$, which is in $DG_{R,\mathcal{O}}^*$. Since $o^*K \subset K$, the projection $B^\flat \oplus K \longrightarrow B^\flat$ is also a $\mathcal{O}$-linear map, giving a map $\mathcal{G}' \longrightarrow \mathcal{G}$. Both of these maps are isomorphisms on the level of $\operatorname{Spec} A$, and therefore they are the identity in $DG_{R,\mathcal{O}}^*$. □

Corollary 1.8.3. *Isomorphisms in $DG_{R,\mathcal{O}}^*$ are two-sided, in the sense that if there is a map $\overline{f} : \mathcal{G} \longrightarrow \mathcal{H}$ inducing an isomorphism $\mathcal{F}(\mathcal{G}) \cong \mathcal{F}(\mathcal{H})$, then there's a map $\overline{g} : \mathcal{H} \longrightarrow \mathcal{G}$ such that $\mathcal{F}(\overline{g}) \circ \mathcal{F}(\overline{f}) = \mathrm{id}_G$ and $\mathcal{F}(\overline{f}) \circ \mathcal{F}(\overline{g}) = \mathrm{id}_H$. Hence $\mathcal{G} \cong \mathcal{H}$ in $DG_{R,\mathcal{O}}^*$.*

Proof. By the preceding corollary, there's a minimal $\mathcal{G}'$ isomorphic to $\mathcal{G}$. Composing with $\overline{f}$, we get an morphism from $\mathcal{G}'$ to $\mathcal{H}$, which is an isomorphism on the level of group schemes and is two-sided by the proof of the previous corollary. Hence we get a morphism $\mathcal{H} \longrightarrow \mathcal{G}' \longrightarrow \mathcal{G}$ which is an isomorphism on the level of group schemes, and composition with its inverse $\mathcal{G} \longrightarrow \mathcal{G}' \longrightarrow \mathcal{G}$ gives the identity map on the level of group schemes on $\mathcal{G}$ and $\mathcal{H}$ respectively. □

Remark 1.8.4. Note that if $\mathcal{G} \in DG_{R,\mathcal{O}}$, it is not necessarily isomorphic to *any* $\mathcal{H} \in DG_{R,\mathcal{O}}$ just because $\mathcal{F}(\mathcal{G}) \cong \mathcal{F}(\mathcal{H})$. For instance, take α_q and $\mathcal{LT}[\pi]$ over k, both of which are minimal. $\mathcal{F}(\alpha_q) \cong \mathcal{F}(\mathcal{LT}[\pi])$, and this isomorphism is even compatible with the strict action on the level of group schemes. But this isomorphism does not extend to an isomorphism from α_q to $\mathcal{LT}[\pi]$ which is $\mathcal{O}$-linear, by consideration of the π^* action.

We now give an explicit construction of the kernel of a flat morphism in $DG^*_{R,\mathcal{O}}$, following [Fal02].

Proposition 1.8.5. *Let* $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}), \mathcal{H} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i_\mathcal{H}) \in DG^*_{R,\mathcal{O}}$*, and let* $\overline{f} : \mathcal{G} \to \mathcal{H}$ *be a morphism between them. Thenif* $\mathcal{F}(f) : \operatorname{Spec} A \to \operatorname{Spec} B$ *is a flat morphism (ie,* A *is flat as a* B*-module),* $\overline{f}$ *has a kernel in* $DG^*_{R,\mathcal{O}}$.

Proof. Let $\mathcal{F}(\mathcal{G}) = G$, and $\mathcal{F}(\mathcal{H}) = H$. Then the flat kernel of $\mathcal{F}(\overline{f})$ is $G \times_H \operatorname{Spec} R$, which will be denoted by K, is represented by the algebra $A/f^*(I_B)$, which is flat. For any $F \in \mathrm{Gr}_R$, the sequence

$$0 \to \operatorname{Hom}_{\mathrm{Gr}_R}(F, K) \to \operatorname{Hom}_{\mathrm{Gr}_R}(F, G) \to \operatorname{Hom}_{\mathrm{Gr}_R}(F, H)$$

is exact, since K is a kernel in Gr_R.

By definition of $\mathcal{G}$, there is a ring $R[X_1, \ldots, X_n]$ with an ideal I such that

$$\begin{aligned} A^{\mathrm{loc}} &\cong R[X_1, \ldots, X_n]/I, \\ A^\flat &\cong R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)I. \end{aligned} \tag{1.8.1}$$

We define an object $\mathcal{K} = (\operatorname{Spec} \mathcal{O}_K, \operatorname{Spec} \mathcal{O}_K^\flat, i_\mathcal{K}) \in DS_R$ by

$$\begin{aligned} \mathcal{O}_K &\cong A/f^*(I_B), \\ \mathcal{O}_K^{\mathrm{loc}} &\cong R[X_1, \ldots, X_n]/(I + f^{*\mathrm{loc}}(I_{B^{\mathrm{loc}}})), \\ \mathcal{O}_K^\flat &\cong R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)(I + f^{*\flat}(I_{B^\flat})). \end{aligned} \tag{1.8.2}$$

There is a unique comultiplication on $\mathcal{O}_K$ making $\operatorname{Spec} \mathcal{O}_K$ an R-subgroup scheme of $\operatorname{Spec} A$ by a property of kernels in Gr_R; the comultiplication lifts uniquely to comultiplication on $\mathcal{O}_K^\flat$ by Proposition 1.5.7, so that $\mathcal{K} \in DG_R$. The map $\mathcal{K} \to \mathcal{G}$ given by $A \mapsto A/f^*(I_B)$ and $A^\flat \mapsto R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)I_A$ is compatible with comultiplication by Proposition 1.5.8; therefore this map is a morphism in DG_R.

We define an action of $\mathcal{O}$ on $\mathcal{O}_K$ and $\mathcal{O}_K^\flat$ as follows: any $x \in \mathcal{O}_K$ is the image of some $a \in A$, where $x = a \mod f^*(I_B)$. Since $o^*(f^*(I_B)) = f^*(o^* I_B) \subset f^*(I_B)$, $o^* a$ is well-defined modulo $f^*(I_B)$, and we set x^* to be equal to the image of $o^* a$ modulo $f^*(I_B)$. Similarly, since $o^* f^*(I_{B^\flat}) \subset f^*(I_{B^\flat})$, we can define an action of $\mathcal{O}$ on $\mathcal{O}_K^\flat$.

Therefore the subscheme $\operatorname{Spec} A/f^*(I_B) \subset \operatorname{Spec} A$ is closed under the action of any $o \in \mathcal{O}$; since o^* is an endomorphism of of $\operatorname{Spec} A$ as a group scheme, it follows that it is also an endomorphism of $\operatorname{Spec} A/f^*(I_B)$ as a subgroup scheme. The fact that the action of o^* on $\operatorname{Spec} \mathcal{O}_K^\flat$ is compatible with comultiplication now follows by Proposition 1.5.8; therefore we have an a homomorphism of rings $\mathcal{O} \to \operatorname{End}_{DG_R} \mathcal{K}$.

Since the maps $A \to \mathcal{O}_K$ and $A^\flat \to \mathcal{O}_K^\flat$ are closed immersions, and the $\mathcal{O}$-action on $\mathcal{O}_K, \mathcal{O}_K^\flat$ is induced from the $\mathcal{O}$-action on $A, A^\flat$, the morphism $\mathcal{K} \to \mathcal{G}$ is $\mathcal{O}$-linear.

If we identify $N_{\mathcal{H}}$ with its image in $\mathcal{O}_K^\flat$, it follows by consideration of equations (1.8.1) and (1.8.2) that $N_{\mathcal{K}} = N_{\mathcal{H}} + f^{\flat *}(I_{B^\flat})$, and $\mathcal{O}$ acts by scalars on this: the action on $N_{\mathcal{H}}$ is by scalars since $\mathcal{H}$ is strict, and the action on $f^{\flat *}(I_{B^\flat})$ is strict since $f^{\flat *}$ is $\mathcal{O}$-linear and the $\mathcal{O}$-action on $I_{B^\flat}$ is by scalars up to terms in $I_{B^\flat}^2$, which are anyway sent by $f^{\flat *}$ to terms projecting to zero in $C^\flat$. It's obvious that the $\mathcal{O}$-action on $t_{\mathcal{K}}^*$ is by scalars since it's a quotient of $t_{\mathcal{G}}^*$, so the action of $\mathcal{O}$ on $\mathcal{K}$ is strict.

Clearly $\mathcal{F}(\mathcal{K}) = K$. Since $\mathcal{F}$ is an equivalence of categories from DG_R^* to Gr_R, the sequence

$$0 \to \operatorname{Hom}_{DG_R^*}(\mathcal{A}, \mathcal{K}) \to \operatorname{Hom}_{DG_R^*}(\mathcal{A}, \mathcal{G}) \to \operatorname{Hom}_{DG_R^*}(\mathcal{A}, \mathcal{H}) \tag{1.8.3}$$

is exact for any $\mathcal{A} \in DG_R^*$. In order to show that $\mathcal{K}$ (with its $\mathcal{O}$ action) is the kernel of $\overline{f}$ in $DG_{R,\mathcal{O}}^*$, we must show that the following sequence is exact:

$$0 \to \operatorname{Hom}_{DG_{R,\mathcal{O}}^*}(\mathcal{A}, \mathcal{K}) \to \operatorname{Hom}_{DG_{R,\mathcal{O}}^*}(\mathcal{A}, \mathcal{G}) \to \operatorname{Hom}_{DG_{R,\mathcal{O}}^*}(\mathcal{A}, \mathcal{H})$$

for each $\mathcal{A} \in DG_{R,\mathcal{O}}^*$. The leftmost arrow is clearly an inclusion, because $K \to G$ is a closed immersion. It suffices to show exactness at the middle term, ie that if $\overline{h} \in \operatorname{Hom}_{DG_{R,\mathcal{O}}^*}(\mathcal{A}, \mathcal{G}) \mapsto 0$, ie $\overline{h} \circ \overline{f} = 0$, then $\overline{h}$ factors through $\mathcal{K}$. But this follows by exactness of (1.8.3), and strictness is automatic. □

Proposition 1.8.6. *If $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG_{R,\mathcal{O}}^*$, then there exists an exact sequence*

$$0 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{G}^{\text{ét}} \to 0 \tag{1.8.4}$$

where $\mathcal{G}^0$ and $\mathcal{G}^{\text{ét}}$ are étale and connected respectively, such that applying $\mathcal{F}$ to the above sequence yields the usual exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0$$

where G^0 is the maximal connected subgroup scheme of G, and $G^{\text{ét}}$ is its maximal étale subquotient, as discussed in [Tat97, §3.7].

Proof. Since R is noetherian, we can apply Theorem 1.2.5, which tells us that A has only finitely many maximal ideals $\mathfrak{m}_i$, and $A = \prod_i A_{\mathfrak{m}_i}$. Therefore $A_{\mathfrak{m}_i} = e_i A$ for some idempotents $e_i \in A$. Since $\varepsilon^*(e_i)$ is idempotent for each e_i, $\varepsilon^*(e_i)$ is 0 or 1 (these being the only idempotents in R). But since $e_i e_j = \delta_{ij}$, $\varepsilon^*(e_i) \neq 0$ for exactly one of these, e_1, say, as ε^* is a non-zero map. Then we take $A^0 = A/(1-e_1)$ to be the algebra of the connected part (as is usual for group schemes). All the other e_i are in I_A, so their image under the map $A \to A^{\text{loc}}$ is zero; therefore, $A^{0\text{loc}} = A^{\text{loc}}$, $A^{0\flat} = A^\flat$, and we can form $\mathcal{G}^0$ in the obvious way. $\mathcal{O}$ gives a well-defined action on A^0 because $o^*(1-e_1) \subset (1-e_1)$ for all $o \in \mathcal{O}$ (o^* must map $1-e_1$ to another idempotent killed by ε^*, and all such idempotents are in the ideal $(1-e_1)$).

The cokernel of the morphism $\mathcal{G}^0 \to \mathcal{G}$ is $\mathcal{G}^{\text{ét}}$, which has algebra $A^{\text{ét}}$ the maximal étale subalgebra of A, and $A^{\text{ét,loc}} = A^{\text{ét},\flat} = R$. □

The following lemma is taken almost verbatim from [Wat79, Theorem 6.8]; we make slight modifications to take account of the fact that we have a strict $\mathcal{O}$-action.

Lemma 1.8.7. *For all $\mathcal{G} \in DG^*_{k,\mathcal{O}}$, $\mathcal{G}$ decomposes as a direct product of $\mathcal{G}^0$ and $\mathcal{G}^{\text{ét}}$ ($\mathcal{G}^0$ and $\mathcal{G}^{\text{ét}}$ are as defined in Proposition 1.8.6):*

$$\mathcal{G} \cong \mathcal{G}^0 \times \mathcal{G}^{\text{ét}}$$

Proof. Let $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}})$. Let N be the nilradical of A. By [Wat79, Theorem 6.2], A/N is separable, and $A/N \otimes A/N$ is reduced. Therefore the map

$$A \xrightarrow{\Delta^*} A \otimes A \to A/N \otimes A/N$$

factors through A/N, and A/N, and defines a closed subgroup scheme on G. By [Wat79, Lemma 6.8], $A/N \cong A^{\text{ét}}$ ($A^{\text{ét}}$ as in the proof of Proposition 1.8.6); therefore

A/N admits an $\mathcal{O}$-action (necessarily strict since it is étale), and the exact sequence (1.8.4) splits, so $\mathcal{G}$ is a semi-direct product of $\mathcal{G}^0$ and $\mathcal{G}^{\text{ét}}$. Since $\mathcal{G}$ is abelian, it follows that $\mathcal{G} \cong \mathcal{G}^0 \times \mathcal{G}^{\text{ét}}$. $\square$

Chapter 2

Dieudonné theory

We work throughout this chapter with k a perfect field of characteristic $p > 0$ containing $\mathbb{F}_q$, where $q = p^r$ for some fixed $r \in \mathbb{N}$, and $\mathscr{O} = \mathbb{F}_q[[\pi]]$. We choose once and for all an inclusion $\mathbb{F}_q \subset k$, such that k is an $\mathscr{O}$-algebra via $\pi \mapsto 0 \in k$ and the map from $\mathbb{F}_q \subset \mathscr{O}$ to k is the above inclusion.

2.1 Summary of the results of this chapter

This chapter consists of finding the correct analogue of classical Dieudonné theory for our situation. We therefore present an introduction to classical Dieudonné theory, and state how our situation is related to the classical one, before describing our main result. A version Dieudonné theory was developed in [Fal02], but using very different methods: the Dieudonné theory developed here is explicitly related to classical Dieudonné theory.

Classical Dieudonné theory over k is based around the ring of Witt vectors $W(k)$ (see [Ser62] for an explicit construction). Essentially this ring consists of infinite sequences

$$(a_0, \dots, a_n, \dots)$$

where $a_i \in k$ for each i, and addition and multiplication of Witt vectors are given by families of polynomials. The simplest example of the Witt vectors is perhaps $W(\mathbb{F}_p)$, which is isomorphic to $\mathbb{Z}_p$.

The most important property of addition of Witt vectors for us is the following:

$$p.(a_0, \ldots, a_n, \ldots) = (0, a_0^p, \ldots, a_n^p, \ldots)$$

where $p.$ denotes addition p times (p being the characteristic of k). This allows us to factorise multiplication by p as a product of the morphisms of rings V (Verschiebung):

$$(a_0, \ldots, a_n, \ldots) \mapsto (0, a_0, \ldots, a_n, \ldots)$$

and F (Frobenius):

$$(a_0, \ldots, a_n, \ldots) \mapsto (a_0^p, \ldots, a_n^p, \ldots).$$

We also have finite quotients of $W(k)$ by V^n for each $n \in \mathbb{N}$, which we denote by $W_n(k)$. For example, $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Using the additive group law (but not the multiplication) on W_n, it's possible to introduce a k-group scheme W_n of finite type representing the Witt vectors of length n, which also admits morphisms V and F. For any k-algebra R, $W_n(R)$ consists of vectors of length n:

$$(a_0, \ldots, a_{n-1})$$

for $a_0, \ldots, a_{n-1} \in R$.

In fact, each finite commutative k-group scheme admits morphisms F and V, such that

$$[p] = F \circ V = V \circ F,$$

where $[p]$ denotes the group operation applied p times.

In [Fon77], Fontaine created an analogue of Witt vectors, called Witt *co*vectors; to each k-algebra R is associated $CW(R)$, the set of infinite series

$$(\ldots, a_{-i}, \ldots, a_{-1}, a_0)$$

where each $a_i \in R$, and there are integers r, s (depending on the infinite series) such that the sth power of the ideal generated by $a_{-r}, a_{-r-1}, \ldots, a_{-n}, \ldots$ is zero. This allows Fontaine to define a group law on such sets, by analogues of the usual formulas for addition of Witt vectors. Analogues of the usual results for Witt vectors hold; for instance,

$$p.(\ldots, a_{-i}, \ldots, a_{-1}, a_0) = (\ldots, a_{-i-1}^p, \ldots, a_{-1}^p)$$

and $[p]$ factors into a product of Frobenius and Verschiebung, as for Witt vectors. The crucial difference between Fontaine's covectors and the usual Witt vectors is that there are non-zero covectors such that V acts as the identity on them (eg $(\dots, a, \dots, a)$ where a is nilpotent), whereas there are clearly no Witt vectors with this property.

With these covectors, Fontaine was able to make an interpretation of the Dieudonné anti-equivalence of categories from the category Gr_k (defined in Definition 1.5.2) to a category of finite-length modules over a certain ring, via the functor

$$G \rightsquigarrow \mathrm{Hom}_k(G, CW).$$

In the course of this chapter, we will discover that for each triple $\mathcal{G}$, given by $(\mathrm{Spec}\, A, \mathrm{Spec}\, A^\flat, i_{\mathcal{G}}) \in DG_{k,\mathcal{O}}$ (and hence also $DG^*_{k,\mathcal{O}}$), its image $G = \mathcal{F}(\mathcal{G}) \in \mathrm{Gr}_k$ (a k-group scheme) has the property that $V = 0$:

Theorem 1 (2.5.1). *Let $\mathcal{G} \in DG_{k,\mathcal{O}}$. Then $V = 0$ on $\mathcal{F}(\mathcal{G})$.*

We will see that we can introduce a functor $\overline{V}_\pi$ (an analogue of V) on $DG^*_{k,\mathcal{O}}$, such that we have the following factorisation,

$$\pi^* = \overline{V}_\pi \circ \overline{F}_\pi = \overline{F}_\pi \circ \overline{V}_\pi,$$

noting that the existence of $\overline{V}_\pi$ was sketched in [Fal02].

We will show that there is an anti-equivalence of categories from $DG^*_{k,\mathcal{O}}$ to the category $(\mathrm{DMod})_k$ of finite length modules over a ring $\mathscr{D}_k$; this is the content of the following Theorem[1]:

Theorem 2 (2.9.8). *Let M be the functor from $DG^*_{k,\mathcal{O}}$ to $(\mathrm{DMod})_k$ given by*

$$\mathcal{G} \rightsquigarrow \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}.$$

Then M is an anti-equivalence of categories.

[1]In the statement of the theorem, the subscript χ_0 denotes the k-submodule of $\mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ on which all $\alpha \in \mathbb{F}_q$ acting via the endomorphism α^* of $\mathcal{F}(\mathcal{G})$ act by scalar multiplication, ie by the map $m \mapsto \alpha m$ for $m \in \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$, where we identify $\alpha \in \mathbb{F}_q$ with its image under the inclusion $\mathbb{F}_q \to k$.

(The subscript M_{χ_0}, for an $\mathscr{O}$-module M, denotes the submodule consisting of those $m \in M$ such that $\alpha^* m = \alpha m$ for all $\alpha \in \mathbb{F}_q^*$).

This is the central result of the chapter, and of this thesis. The rest of this chapter now proceeds as follows:

1. we give an explicit construction of the classical Verschiebung for k-group schemes, which we will make use of subsequently
2. we give precise statements of the results we will use from classical Dieudonné theory
3. we show that, for all objects $\mathcal{G} \in DG^*_{k,\mathscr{O}}$, Verschiebung is trivial on the k-group scheme $\mathcal{F}(\mathcal{G})$ underlying $\mathcal{G}$.
4. we introduce a new functor $\overline{V}_\pi$, which is a functor on $DG^*_{k,\mathscr{O}}$, and acts as a replacement for V
5. finally, we prove our anti-equivalence of categories.

2.2 Classical Verschiebung

We provide the complete construction of the classical Verschiebung V, in the category Gr_k, since we will need to make use of its explicit construction later in this thesis.

In order to do this, we recall some basic constructions from linear algebra

2.2.1 Constructions from multilinear algebra

In this chapter we make use of the nth *symmetric power* of a k-vector space. We provide its construction here, and sketch some basic properties. More details can be found in [FH91, Appendix B.2], although things are slightly different for us, since we work over a field of characteristic $p > 0$.

We denote by S_n the group of bijections of $\{1, \ldots, n\}$.

Definition 2.2.1. Let V be a k-vector space (or equivalently, a k-module). Then for $n \in \mathbb{N}$ the nth *symmetric power* of V, denoted $\mathrm{Sym}^n V$, is the quotient of $V^{\otimes n}$ by the subspace generated by all relations $v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$, for all $\sigma \in S_n$. Let $\pi : V^{\otimes n} \twoheadrightarrow \operatorname{Sym}^n V$ denote the obvious projection. We denote $\pi(v_1 \otimes \cdots \otimes v_n)$ by $v_1 \cdot \ldots \cdot v_n$; we also denote $\pi(v_1^{\otimes n})$ by $v_1^{\cdot n}$.

It will also be useful to define $\operatorname{Sym}^n A$, for A a k-algebra; this means the nth symmetric power of A, *considered as a k-module, not as a k-algebra.*

We recall some basic properties of $\operatorname{Sym}^n V$:

1. if $\{e_i\}$ is a basis of V as a k-vector space (equivalently, as a k-module), then
$$\{e_{i_1} \cdot e_{i_2} \cdot \ldots \cdot e_{i_n} \mid i_1 \leq i_2 \leq \cdots \leq i_n\}$$
is a basis for $\operatorname{Sym}^n V$.

2. In $\operatorname{Sym}^p V$,
$$(v_1 + v_2)^{\cdot p} = v_1^{\cdot p} + v_2^{\cdot p},$$
for all $v_1, v_2 \in V$. This follows since the coefficient of $v_1^{\cdot n} \cdot v_2^{\cdot n-p}$ in the above expression is $\frac{p!}{n!(p-n)!}$ by the binomial theorem, which is equal to zero in k unless $n = p$ or $n = 0$.

We now introduce a k-submodule $\operatorname{TSym}^p V$ of $\operatorname{Sym}^p V$, which is standard when working with comultiplication of group schemes in characteristic p (see [DG70], [Fon77]). We will use it to get an explicit factorisation of $[p]$ (the composition $G \to G^p \to G$ where the first map is the diagonal embedding and the second is multiplication $p-1$ times), thereby allowing us to define a functor V on the category of finite commutative k-group schemes through which $[p]$ factors.

Lemma 2.2.2. *Let* $\operatorname{TSym}^p V$ *denote the subset of* $\operatorname{Sym}^p V$ *consisting of* $v^{\cdot p}$*, for all* $v \in V$*. Then* $\operatorname{TSym}^p V$ *is a k-subspace (equivalently, a k-submodule) of* $\operatorname{Sym}^p V$.

Proof. If $v_1^{\cdot p}, v_2^{\cdot p} \in \operatorname{TSym}^p V$, then $v_1^{\cdot p} + v_2^{\cdot p} = (v_1 + v_2)^{\cdot p}$, as above, so $\operatorname{TSym}^p V$ is closed under addition. If $\lambda \in k$, $\lambda v_1^{\cdot p} = (\lambda^{1/p} v_1)^{\cdot p}$ (pth roots exist in k since it is perfect), so $\operatorname{TSym}^p V$ is closed under multiplication by every $\lambda \in k$. Therefore it is a k-subspace of $\operatorname{Sym}^p V$. □

It is clear from this proof that $\operatorname{TSym}^p V$ has no obvious characteristic zero analogue, since this subset of $\operatorname{Sym}^p V$ is not closed under addition. On the other hand, $\operatorname{TSym}^p V$ easily generalises to k-submodules $\operatorname{TSym}^{p^n} V \subset \operatorname{Sym}^{p^n} V$ for every $n \in \mathbb{N}$.

2.2.2 Construction of V

In this subsection, we show how to define our morphism V on every finite commutative affine group scheme over a perfect field k, such that $[p]$ ($p.\mathrm{id}$) factors as a composition of V and pth power relative Frobenius. An explicit construction of V is given in [DG70], but we provide one here since we need it for subsequent results.

Definition 2.2.3. Let A be the algebra of a finite commutative affine k-group scheme.

Let $A^{(p^n)}$ denote the k-algebra A twisted by nth power Frobenius, ie $k \otimes_k A$, where the map $k \to k$ is the composition of n times the Frobenius $k \to k$ for $n \geq 0$, or $-n$ times the inverse Frobenius, for $n < 0$. (The inverse Frobenius is defined since k is perfect.) We take the algebra morphism $k \to A^{(p^n)}$ to be the map sending $\alpha \in k$ to $\alpha \otimes 1$. Let $F : A^{(p)} \to A$ be the k-linear morphism of algebras given by $\alpha \otimes a \mapsto \alpha a^p$ (clearly this gives rise to a family of maps $F : A^{(p^n)} \to A^{(p^{n-1})}$ for each n). F is clearly functorial on the category of k-algebras, because every morphism commutes with Frobenius, up to a twist $k \to k$.

We denote the k-group scheme represented by $A^{(p^n)}$ (with the structure morphism defined above) by $G^{(p^n)}$.

In this section, we denote by $D^* : A^{\otimes p} \to A$ the map defined by $a_1 \otimes \cdots \otimes a_p \mapsto a_1 \ldots a_p$ (this is dual to the scheme-theoretic diagonal morphism $G \to G^p$). Note that this map factors through the map $\pi : A^{\otimes p} \to \mathrm{Sym}^p A$ of Definition 2.2.1, since A is a commutative algebra. In fact, it is the composition of π with the map $\mathrm{Sym}^p A \to A$ given by $a_1 \cdot a_2 \cdot \cdots \cdot a_p \mapsto a_1 a_2 \ldots a_p$.

Caution 2.2.4. As discussed in Remark 1.6.4, the arbitrary base change of a strict $\mathcal{O}$-group scheme $\mathcal{G} \in DG_{k,\mathcal{O}}$ is *not always strict*, and in particular $\mathcal{G}^{(p)} = (G^{(p)}, G^{\flat(p)}, i_{\mathcal{G}})$ does not have $\mathcal{O}$ acting by scalars for general $\mathcal{O}$ and k. However, in certain special cases, it will be possible to define $\mathcal{G}^{(p^n)}$, for certain n (see below).

Definition 2.2.5. Let A be the algebra of a commutative k-group scheme. We define a morphism $f_n : A \to A^{\otimes n}$ by

$$f_n = (\Delta^* \otimes \mathrm{id}^{\otimes n-2}) \circ (\Delta^* \otimes \mathrm{id}^{\otimes n-3}) \circ \cdots \circ (\Delta^* \otimes \mathrm{id}) \circ \Delta^* : A \to A^{\otimes n}.$$

If $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_k$, then we can define $f_n^\flat$ analogously to f_n:

$$f_n^\flat = (\Delta^{*\flat} \otimes \mathrm{id}^{\otimes n-2}) \circ (\Delta^{*\flat} \otimes \mathrm{id}^{\otimes n-3}) \circ \cdots \circ (\Delta^{*\flat} \otimes \mathrm{id}) \circ \Delta^{*\flat} : A^\flat \to (A^{\otimes n})^\flat.$$

Lemma 2.2.6. *Let A be the algebra of a finite rank commutative k-group scheme. For all $n \geq 2, f_n$ has symmetric image, ie $f_n(a)$ is invariant under the action of the symmetric group S_n on $A^{\otimes n}$ sending $a_1 \otimes \cdots \otimes a_n$ to $a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)}$, for all $\sigma \in S_n$.*

Similarly, if $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_k$, then for all $a \in A^\flat$, $f_n^\flat(a) \in (A^{\otimes p})^\flat$ is invariant under the obvious action of S_n.

Proof. The proof for f_n by induction. For $n = 2$, the result follows by commutativity of Δ^*. So assume the statement is true for $n = r - 1$, and prove it for $n = r$.

By induction, $f_{r-1}(a)$ is invariant under S_{r-1} for all $a \in A$, hence invariant under the transposition $(r-1\ r-2)$. Since $f_r = (\Delta^* \otimes \mathrm{id}^{\otimes r-2}) \circ f_{r-1}$, it follows that $f_r(a)$ is invariant under $(r\ r-1)$ for all $a \in A$.

By the associativity axiom, it follows that the diagram

$$\begin{tikzcd} A \arrow[r, "f_{r-1}"'] \arrow[d, "f_{r-1}"] & A^{\otimes r-1} \arrow[d, "\Delta^* \otimes \mathrm{id}^{\otimes r-2}"] \\ A^{\otimes r-1} \arrow[r, "\mathrm{id} \otimes \Delta^* \otimes \mathrm{id}^{\otimes r-3}"'] & A^{\otimes r} \end{tikzcd}$$

commutes, so $f_r(a)$ is invariant under the permutation $(r\ 1\ \ldots\ r-2\ r-1)$. Since S_r is generated by this permutation and any transposition, the result follows.

The proof for $f_n^\flat$ follows in the same way. $\square$

Lemma 2.2.7. *Let $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_k$. Then $(A^{\otimes n})^\flat \cong (A^\flat)^{\otimes n}/I_n$ for all $n > 2$, where I_n is the ideal*

$$\left(\sum_{1 \leq i \leq n} 1^{\otimes i-1} \otimes I_{A^\flat} \otimes 1^{\otimes n-i} \right) \left(\sum_{1 \leq j \leq n} 1^{\otimes j-1} \otimes N_\mathcal{G} \otimes 1^{\otimes n-j} \right).$$

Further, $I_{(A^{\otimes n})^\flat} \cong \sum_{1 \leq i \leq n} 1^{\otimes i-1} \otimes I_{A^\flat} \otimes 1^{\otimes n-i}$, and $N_{\mathcal{G}^n} \cong \sum_{1 \leq i \leq n} 1^{\otimes i-1} \otimes N_\mathcal{G} \otimes 1^{\otimes n-i}$.

Proof. We prove this by induction. The statement is true for $n = 2$ by the definition of $(A \otimes A)^\flat$ in the proof of Proposition 1.4.13. So assume true for $n = i$, ie $(A^{\otimes i})^\flat \cong (A^\flat)^{\otimes i}/I_i$, with $I_{(A^{\otimes i})^\flat}$ and $N_{\mathcal{G}^i}$ as in the statement of the lemma.

By definition, $(A^{\otimes i+1})^\flat \cong ((A^\flat)^{\otimes i}/I_i) \otimes A^\flat/(I_{(A^{\otimes i})^\flat} \otimes 1 + 1^{\otimes i} \otimes I_{A^\flat})(N_{\mathcal{G}^n} \otimes 1 + 1^{\otimes i} \otimes N_{\mathcal{G}}) \cong (A^\flat)^{\otimes i+1}/I_{i+1}$ as required. The other results follow similarly. □

Lemma 2.2.8. *Let A be the algebra of a finite commutative k-group scheme. Let $e_1, e_2, \dots, e_n$ be any basis for I_A as a k-module. Let $a \in A$. If*

$$f_p(a) = \sum_{i_1,\dots,i_p} \alpha_{i_1,\dots,i_p} e_{i_1} \otimes \cdots \otimes e_{i_p},$$

for some $\alpha_{i_1,\dots,i_p} \in k$, then

$$\pi(f_p(a)) = \sum_i \alpha_{i,\dots,i} e_i^p,$$

where $\pi : A^{\otimes p} \longrightarrow \operatorname{Sym}^p A$ is the map of Definition 2.2.1. Hence the composition $\pi \circ f_p : A \to \operatorname{Sym}^p A$ factors through $\operatorname{TSym}^p A$. Further, $D^*(f_p(a)) = \sum_i \alpha_{i,\dots,i} e_i^p$.

Proof. By Lemma 2.2.6, $f_p(a)$ is invariant under the action of every $\sigma \in S_p$, so $\alpha_{i_1,\dots,i_p} = \alpha_{i_{\sigma(1)},\dots,i_{\sigma(p)}}$. Letting δ_i for $1 \le i \le p$ be the number of times i occurs in $i_1, \dots, i_p$, the coefficient of $e_{i_1} \dots e_{i_p}$ in $D^*(f_p(a))$ is therefore $\frac{p!}{\delta_1! \dots \delta_n!} \alpha_{i_1,\dots,i_p}$. If $i_j \neq i_{j'}$ for some j, j', then this is zero, since $p = 0$ in A, so $\pi(f_p(a)) = \sum_i \alpha_{i,\dots,i} e_i^p$, as required. Hence $\pi \circ f_p : A \to \operatorname{Sym}^p A$ factors through $\operatorname{TSym}^p A \subset \operatorname{Sym}^p A$ by definition of $\operatorname{TSym}^p A$.

The fact that $D^*(f_p(a)) = \sum_i \alpha_{i,\dots,i} e_i^p$ follows since $D^* : A^{\otimes p} \longrightarrow A$ factors through π, as desccribed in Definition 2.2.3.

□

Proposition 2.2.9. *Let A be the algebra of a finite commutative k-group scheme G. Then there is a morphism of k-group schemes $V : G \longrightarrow G^{(1/p)}$ such that $[p]$ factorises as*

$$[p] = F^{(1/p)} \circ V = V^{(p)} \circ F.$$

Proof. Consider the following sequence of k-modules and k-module morphisms:

$$A \xrightarrow{f_p} A^{\otimes p} \xrightarrow{\pi} \operatorname{Sym}^p A$$

where π is the map of Definition 2.2.1. Let $e_1, \dots, e_n$ (linearly independent) generate A as a k-module.

For each $a \in A$, $f_p(a)$ can be expressed uniquely as a sum

$$f_p(a) = \sum_{1 \leq i_1, \ldots, i_p \leq n} \alpha_{i_1, \ldots, i_p} e_{i_1} \otimes \cdots \otimes e_{i_p}$$

for some $\alpha_{i_1, \ldots, i_p} \in k$.

By Lemma 2.2.8,

$$\pi(f_p(a)) = \sum_{1 \leq i \leq n} \alpha_{i, \ldots, i} e_i \cdot \ldots \cdot e_i,$$

and $\pi(f_p(A)) \subset \mathrm{TSym}^p A \subset \mathrm{Sym}^p A$.

We define a morphism $\mathrm{TSym}^p A \longrightarrow A^{(p)}$ of k-modules by $a^{\cdot p} \mapsto 1 \otimes a$, for all $a \in A$. This is a morphism of groups by Lemma 2.2.2, and k-linear since

$$\lambda a^{\cdot p} = (\lambda^{1/p} a)^{\cdot p} \mapsto 1 \otimes \lambda^{1/p} a = \lambda \otimes a$$

for all $a \in A, \lambda \in k$. Let $V : A \longrightarrow A^{(p)}$ be the composition of this morphism with $\pi \circ f_p$, which is a morphism of k-modules; we now show that it is a morphism of k-algebras.

Let $a, a' \in A$ be arbitrary, then

$$f_p(a) = \sum_{i_1, \ldots, i_p} \alpha_{i_1, \ldots, i_p} e_{i_1} \otimes \cdots \otimes e_{i_p}$$

$$f_p(a') = \sum_{i_1, \ldots, i_p} \alpha'_{i_1, \ldots, i_p} e_{i_1} \otimes \cdots \otimes e_{i_p}.$$

By Lemma 2.2.8, $\pi(f_p(a)) = \sum_i \alpha_{i, \ldots, i} e_i^{\cdot p}$, and $\pi(f_p(a')) = \sum_i \alpha'_{i, \ldots, i} e_i^{\cdot p}$, and therefore by definition of V,

$$V(a)V(a') = \left(\sum_i \alpha_{i, \ldots, i} \otimes e_i \right) \left(\sum_i \alpha'_{j, \ldots, j} \otimes e_j \right) = \sum_{i,j} \alpha_{i, \ldots, i} \alpha'_{j, \ldots, j} \otimes e_i e_j. \quad (2.2.1)$$

On the other hand,

$$f_p(aa') = \left(\sum_{1 \leq i_1, \ldots, i_p \leq n} \alpha_{i_1, \ldots, i_p} e_{i_1} \otimes \cdots \otimes e_{i_p} \right) \left(\sum_{1 \leq i'_1, \ldots, i'_p \leq n} \alpha'_{i'_1, \ldots, i'_p} e_{i'_1} \otimes \cdots \otimes e_{i'_p} \right)$$
$$= \sum_{\substack{1 \leq i_1, \ldots, i_p \leq n \\ 1 \leq i'_1, \ldots, i'_p \leq n}} \alpha_{i_1, \ldots, i_p} \alpha_{i'_1, \ldots, i'_p} e_{i_1} e_{i'_1} \otimes \cdots \otimes e_{i_p} e_{i'_p},$$

and therefore

$$\pi(f_p(aa')) = \sum_{\substack{1 \leq i_1, \ldots, i_p \leq n \\ 1 \leq i'_1, \ldots, i'_p \leq n}} \alpha_{i_1, \ldots, i_p} \alpha'_{i'_1, \ldots, i'_p} (e_{i_1} e_{i'_1}) \cdot \ldots \cdot (e_{i_p} e_{i'_p}). \quad (2.2.2)$$

For any choice of $i_1, \ldots, i_p, i'_1, \ldots, i'_p$, the ordered pairs of subscripts of $(e_{i_1} e_{i'_1}), \ldots,$ $(e_{i_p} e_{i'_p})$ occur together in any order in this sum in $p!/(\prod_{i,j} \delta_{i,j}!)$ ways, where $\delta_{i,j}$ is the number of times the ordered pair of subscripts of $(e_i e_j)$ occurs in our list of ordered pairs.

Since $p = 0$ in k, and the coefficients $\alpha_{i_1,\ldots,i_p}$ and $\alpha'_{i'_1,\ldots,i'_p}$ are invariant under permutation of subscripts by Lemma 2.2.6, the terms

$$\alpha_{i_1,\ldots,i_p} \alpha'_{i'_1,\ldots,i'_p} (e_{i_1} e_{i'_1}) \cdot \ldots \cdot (e_{i_p} e_{i'_p})$$

in the sum (2.2.2) cancel unless $i_1 = \cdots = i_p$ and $i'_1 = \cdots = i'_p$ (otherwise $\delta_{i,j} < p$ for all i, j), and

$$\pi(f_p(aa')) = \sum_{\substack{1 \le i \le n \\ 1 \le i' \le n}} \alpha_{i,\ldots,i} \alpha'_{i',\ldots,i'} (e_i e_{i'}) \cdot \ldots \cdot (e_i e_{i'}) = \sum_{i,i'} \alpha_{i,\ldots,i} \alpha'_{i',\ldots,i'} (e_i e_{i'})^{\cdot p}.$$

Therefore

$$V(aa') = \sum_{i,j} \alpha_{i,\ldots,i} \alpha'_{j,\ldots,j} \otimes e_i e_j,$$

and comparing with (2.2.1), we deduce that $V(aa') = V(a)V(a')$, so V is a k-algebra homomorphism as required.

We now show that $F^{(1/p)} \circ V = [p]$: if $\pi(f_p(a)) = \sum \alpha_{i,\ldots,i} e_i \cdot \ldots \cdot e_i$, then $(F \circ V)(a) = F(\alpha_{i,\ldots,i} \otimes e_i) = \alpha_{i,\ldots,i} e_i^p$; on the other hand,

$$\begin{aligned}[p](a) = D^*(f_p(a) = D^* \left(\sum_{i_1,\ldots,i_p} \alpha_{i_1,\ldots,i_p} e_{i_1} \otimes \cdots \otimes e_{i_p} \right) \\ = \sum_i \alpha_{i,\ldots,i} e_i^p,\end{aligned}$$

where the last equality follows by Lemma 2.2.8. Therefore $[p](a) = (F^{(1/p)} \circ V)(a)$, hence $[p] = F^{(1/p)} \circ V$.

F is functorial on the category of k-schemes, since for every pair of k-group schemes G, H and morphism $f : G \to H$, the diagram

$$\begin{array}{ccc} G & \xrightarrow{F_G} & G^{(p)} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^{(p)}} \\ H & \xrightarrow{F_H} & H^{(p)} \end{array}$$

commutes, where F_G and F_H are the Frobenius morphism on G and H respectively. If we let $H = G^{(1/p)}$, and f be the morphism $V : G \to G^{(1/p)}$ defined above, then we get the required result $F^{(1/p)} \circ V = V^{(p)} \circ F$. The fact that V is a morphism of k-group schemes (and not simply a morphism of k-schemes) now follows since $[p]^{(1/p)} \circ V = V \circ F^{(1/p)} \circ V = V \circ [p]$.

□

Remark 2.2.10. It follows that any finite commutative affine k-group scheme G admits a morphism $V : G^{(p)} \to G$. In fact V is functorial in the category of finite commutative affine k-group schemes, although we shall not prove this.

Now we have introduced V, we can define an important subcategory of Gr_k which we shall require later in this chapter.

Definition 2.2.11. Let Gr_k^u be the full subcategory of Gr_k consisting of those k-group schemes on which V is nilpotent.

2.2.3 Examples

1. $V : \mu_p^{(p)} \to \mu_p$ is induced by the map on algebras $k[X]/(X^p - 1) \to k \otimes k[X]/(X^p - 1)$ sending X to $1 \otimes X$. This follows since $\Delta^*(X) = X \otimes X$.

2. $V : \alpha_p^{(p)} \to \alpha_p$ is the unique homomorphism of group schemes factoring over the base, $\operatorname{Spec} k$: if $k[X]/(X^p)$ is its algebra, with comultiplication given by $\Delta^* X = X \otimes 1 + 1 \otimes X$, then $f_p(X) = \sum_{1 \leq i \leq p} 1^{\otimes i-1} \otimes X \otimes 1^{\otimes p-i}$, and hence $\pi(f_p(X)) = 0$, implying that $V(X) = 0$.

3. $V : \mathbb{Z}/p\mathbb{Z}^{(p)} \to \mathbb{Z}/p\mathbb{Z}$ is also the unique homomorphism factoring over $\operatorname{Spec} k$: if its algebra is $k[X]/(X^p - X)$, with comultiplication given by $\Delta^* X = X \otimes 1 + 1 \otimes X$, then the argument given above for α_p applies.

Remark 2.2.12. Of course, twisting the above group schemes by inverse Frobenius on fields ($k \to k$) gives us maps $V : G \to G^{(p^{-1})}$.

For finite group schemes over a field, the operations V and F are dual to one another; for details of this duality, see, for instance, [DG70].

2.3 Results from classical Dieudonné theory

We outline the results from classical Dieudonné Theory which we will need in the course of this chapter.

Classical Dieudonné theory provides an anti-equivalence of categories between the abelian category Gr_k of finite-rank commutative k-group schemes and the category of $\mathbf{D}_k$-modules, where $\mathbf{D}_k$ is the non-commutative ring of Witt vectors $W(k)$ with two endomorphisms F and V adjoined, which satisfy the following relations

$$Fw = w^{(p)}F$$

$$wV = Vw^{(p)}$$

$$FV = VF = p$$

where w denotes $(w_0, w_1, \dots, w_n, \dots) \in W(k)$, and $w^{(p)}$ denotes the Witt vector $(w_0^p, \dots, w_n^p, \dots)$.

We let W_n denote the truncated Witt vectors of length n; this is a finite-type k-group scheme, represented by the algebra $k[X_0, \dots, X_{n-1}]$, with comultiplication given by

$$\Delta^*(X_i) = S_i(X_0 \otimes 1, X_1 \otimes 1, \dots, X_n \otimes 1; 1 \otimes X_0, \dots, 1 \otimes X_n)$$

for all X_i, where the S_i are the polynomials (with coefficients in k) determining addition of Witt vectors, for which formulas are given in [Ser62] and [Fon77].

There is a homomorphism of rings

$$\mathbf{D}_k \to \mathrm{End}_k W_n$$

where F acts as the Frobenius endomorphism of W_n as a k-group scheme, V as the morphism $W_n \to W_n^{(p^{-1})}$ given by $V(X_i \otimes 1) = X_{i-1}$ for $i < n-1$, and $V(X_{n-1} \otimes 1) = 0$ (it can be verified that, with this definition, $F \circ V = V \circ F = [p]$), and such that $w = (w_0, w_1, \dots, w_n, \dots)$ acts on W_n as follows:

Explicitly, the image of $(a, 0, \dots) \in W(k) \subset \mathbf{D}_k$ in $\mathrm{End}_k W_n$ is the endomorphism of W_n given by the algebra map $X_0 \mapsto aX_0, X_1 \mapsto a^pX_1, \dots, X_{n-1} \mapsto a^{p^{n-1}}X_{n-1}$. Since $p.(a_0, a_1, \dots, a_n, \dots) = (0, a_0^p, \dots, a_{n-1}^p, \dots)$, one can reconstruct the endomorphism of W_n which is multiplication by $(a_0, a_1, \dots, a_n, \dots)$ as $(a_0, \dots)+$

$p.(a_1^{1/p}, 0, \dots)+\dots$, from which one can easily derive explicitly the algebra morphism of W_n corresponding to multiplication by an arbitrary Witt vector in $W(k)$.

Analogously to Fontaine's functor (based on covectors), there is a functor M, given by:

$$G \rightsquigarrow \varinjlim_n \mathrm{Hom}_k(G, W_n) \tag{2.3.1}$$

from Gr_k^u to the category of $\mathbf{D}_k$-modules, where $\mathbf{D}_k$ acts on $\mathrm{Hom}_k(G, W_n)$ via its action on W_n for each n. The direct limit is the one induced by the inclusion maps $W_n \to W_{n+1}$ arising from Verschiebung.

This forms the basis for the anti-equivalence of categories of [DG70]:

Theorem 2.3.1. *The functor M is an anti-equivalence of categories from Gr_k^u to the category of finite length $\mathbf{D}_k$-modules on which V is nilpotent.*

Proof. [DG70, Chapter V,§1,Corollary 4.4] □

We also state an analogous version for k-group schemes of finite type, which we shall have reason to use elsewhere in this chapter, since some important k-group schemes such as W_n (the Witt vectors of length n), and $\mathbb{G}_a$ (the additive group scheme) are not finite, but only of finite type over k.

Theorem 2.3.2. *The functor M is an anti-equivalence of categories from the category of unipotent*[2] *k-group schemes of finite type to the category of $\mathbf{D}_k$-modules on which V is nilpotent.*

Proof. [DG70, Chapter V,§1,Theorem 4.3] □

We now state an analogous theorem of Fontaine, which provides an anti-equivalence of categories between Gr_k and the category of finite length $\mathbf{D}_k$-modules. Although this theorem is more general than Theorem 2.3.1 (stated above), we shall have reason to use both theorems in the course of this chapter, because we require some explicit properties of the functor M above.

[2]Here *unipotent* means that the morphism of k-group schemes V defined earlier acts nilpotently on the k-group schemes considered

Theorem 2.3.3. *There is an anti-equivalence of categories between* Gr_k *and the category of* $\mathbf{D}_k$*-modules of finite length, given by*

$$G \rightsquigarrow \mathrm{Hom}(G, \hat{CW}_k)$$

where $\mathrm{Hom}(G, \hat{CW}_k)$ *(henceforth denoted* $\hat{M}(G)$*) is the group of homomorphisms to a group of covectors* $\hat{CW}_k$*. In particular, the action of* $F \in \mathbf{D}_k$ *on* $\hat{M}(G)$ *is dual to Frobenius* $G^{(p)} \to G$*, and the action of* $V \in \mathbf{D}_k$ *is dual to the action of the morphism* $V : G \to G^{(1/p)}$ *defined in Proposition 2.2.9.*

Proof. [Fon77, Chapter III,§1.4,Theorem 1] □

Corollary 2.3.4. *Let* G *be a finite commutative* k*-group scheme. Then there is a splitting*

$$G \cong G^{\text{ét}} \times G^m \times G^l$$

of G *into a product of étale, multiplicative and local-local subschemes, where* F *acts isomorphically on* $G^{\text{ét}}$ *and nilpotently on* G^m *and* G^l*, and* V *acts isomorphically on* G^m *and nilpotently on* $G^{\text{ét}}$ *and* G^l*.*

Proof. Let M be the Dieudonné module associated to G by the anti-equivalence of Theorem 2.3.3. Let M^c be the submodule of M on which F acts nilpotently, which is equal to $\operatorname{Ker} F^n \mid_M = \operatorname{Ker} F^{n+1} \mid_M = \dots$ for some $n \in \mathbb{Z}$. There is an exact sequence

$$0 \to M^c \to M \to M/M^c \to 0.$$

The map $F^n M \to M/\operatorname{Ker} F^n \mid_M$ sending $m \in F^n M \subset M$ to its image in the quotient $M/\operatorname{Ker} F^n \mid_M$ is an isomorphism: it's injective, because if $0 \neq m = F^n m'$, then $m' \notin \operatorname{Ker} F^{n'}$ for any n', so $m \notin \operatorname{Ker} F^n$.

$F^n : M/\operatorname{Ker} F^n \mid_M \to M/\operatorname{Ker} F^n \mid_M$ is an isomorphism since $\operatorname{Ker} F^{2n} \mid_M = \operatorname{Ker} F^n \mid_M$, and therefore for any $\overline{m} \in M/\operatorname{Ker} F^n \mid_M$, we may take $\overline{m}' = F^{-n}(\overline{m})$, which is clearly the image of some $m' \in M$ under the projection $M \to M/\operatorname{Ker} F^n \mid_M$ (F^{-1} is defined as F is an isomorphism of finite rank k-modules). Since the following diagram commutes,

$$\begin{array}{ccc} M & \longrightarrow & \overline{M}/\operatorname{Ker} F^n \mid_M \\ \downarrow{\scriptstyle F^n} & & \downarrow{\scriptstyle F^n} \\ M & \longrightarrow & \overline{M}/\operatorname{Ker} F^n \mid_M \end{array}$$

$m = F^n m'$ maps to $\overline{m}$ under projection $M \to M/\operatorname{Ker} F^n|_M$, and hence our map $F^n M \to M/\operatorname{Ker} F^n|_M$ is surjective. Therefore it is an isomorphism.

Inverting this isomorphism gives us a splitting $M/M^c \to F^n M \subset M$ of this exact sequence, and therefore $M \cong M^c \times M^{\text{ét}}$, where $M^{\text{ét}} = F^n M \cong M/\operatorname{Ker} F^n|_M$. By Theorem 2.3.3 applied to this splitting, we get a splitting $G \cong G^c \times G^{\text{ét}}$. Applying the above argument to G^c with V instead of F gives a further splitting $G^c \cong G^l \times G^m$ of G into local-local and multiplicative parts, where V acts nilpotently on G^l, and as an isomorphism on G^m. □

Proposition 2.3.5. *Let $G \in \mathrm{Gr}_k$ be connected, and satisfy $V = 0$. Then $G \cong \prod_{i=1}^n \alpha_{p^{a_i}}$, for some integers $a_1, \dots, a_n \in \mathbb{N}$.*

Equivalently by Theorem 2.3.1, the Dieudonné module associated to G has generators $m_1, \dots, m_n$, and relations $Vm_1 = \cdots = Vm_n = 0$ and $F^{a_i} m_i = 0$.

Proof. Let $M_0 = M$. M_0/FM_0 is a finitely generated $\mathbf{D}_k$-module (non-trivial since F is nilpotent) with a finite number of generators $\overline{m}_1, \dots, \overline{m}_l$ which can be assumed linearly independent; let $m_1, \dots, m_l$ be any liftings of the generators to M_0. As $\mathbf{D}_k$ is local, we can apply Nakayama's Lemma, which tells us that these liftings generate M_0 as a $\mathbf{D}_k$-module. Let $M_1 = FM + \mathbf{D}_k m_2 + \cdots + \mathbf{D}_k m_l$. Clearly M_0/M_1 has one generator m satisfying $Fm = Vm = 0$, and we have an exact sequence of $\mathbf{D}_k$-modules

$$0 \to M_1 \to M_0 \to km \to 0,$$

and $\dim_k M_1 < \dim_k M_0$. Clearly we can replace M_0 by M_1, and repeat this process to get a sequence of $\mathbf{D}_k$-submodules of M_0:

$$M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

where each quotient $M_i/M_{i+1} \cong km$.

Clearly M_{n-1} has the form described in the Proposition; we now show that if M_i has the form described in the Proposition, then so does M_{i-1}: the result will then follow by induction. We have an exact sequence

$$0 \to M_i \to M_{i-1} \to km \to 0,$$

and M_{i-1} is generated by the generators $m_1, \ldots, m_l$ of M_i, which satisfy relations $Vm_i = 0$ and $F^{a_i}m_i = 0$ for some integers a_i, together with some lift $\hat{m}$ of m which satisfies $V\hat{m} = 0$ and $F\hat{m} \in M_{i-1}$, by exactness.

If $F\hat{m} \in FM_{i-1}$, then $F\hat{m} = Fm'$ for some $m' \in M_{i-1}$, and we can replace $\hat{m}$ by $\hat{m} - m'$ to get $F\hat{m} = 0$, and then the exact sequence splits, and M_i clearly has the form described in the statement of the Proposition.

If $F\hat{m} \notin FM_{i-1}$, then

$$F\hat{m} = \sum_{w,j} F^w \alpha_{w,j} m_j$$

for some constants $\alpha_{w,j} \in k$. We can assume that $\alpha_{w,j} = 0$ for all $j > 0$ by subtracting terms in M_{i-1} from $\hat{m}$, to reduce to an equation

$$F\hat{m} = \sum_{w} \beta_j m_j$$

where $\beta_j = \alpha_{0,j}$. There's some $w \in \mathbb{Z}$ such that the right-hand side is killed by F^w but not by F^{w-1}. Therefore some m_j term is not killed by F^{w-1}; eliminating it from our list of generators gives a Dieudonné module generated by

$$m_1, \ldots, m_{j-1}, m_{j+1}, \ldots, m_l, \hat{m},$$

and satisfying no relations except $Vm_1 = \cdots = Vm_l = V\hat{m} = 0$, $F^{a_i}m_i = 0$ and $F^{a_w+1}\hat{m} = 0$, by a rank argument: $\operatorname{rank} M_i = \operatorname{rank} M_{i-1} + \operatorname{rank} km$ from the exact sequence, and the module just described has rank $\operatorname{rank} M_{i-1} + 1$, hence M_i can satisfy no more relations or else the rank equality would not hold. Hence M_i has the form described in the statement of the Proposition.

Hence, by induction, the result holds. □

Corollary 2.3.6. *The algebra of such a G is $k[X_1, \ldots, X_n]/(X_1^{p^{a_1}}, \ldots, X_n^{p^{a_n}})$, with group morphisms*

$$\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$$
$$i^*(X_i) = -X_i$$
$$\varepsilon^*(X_i) = 0$$

Proof. By definition, the algebra of $\alpha_{p^{a_i}}$ is $k[X_i]/(X_i^{p^{a_i}})$, with $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$, $i^*(X_i) = -X_i$, and $\varepsilon^*(X_i) = 0$. The result now follows from the Proposition. □

Corollary 2.3.7. *If G is presented as in the proof of the previous Corollary, then the only $T \in (X_1, \ldots, X_n)$ such that $\Delta^*T = T \otimes 1 + 1 \otimes T$ are sums of p^ith powers of X_j, ie*

$$T = \sum_{i,j} \alpha_{i,j} X_j^{p^i}$$

for some $\alpha_{i,j} \in k$.

Proof. The Dieudonné module associated to G by equation (2.3.1) is the direct limit $\varinjlim_n \operatorname{Hom}(G, W_n)$, which is equal to $\operatorname{Hom}(G, \mathbb{G}_a)$ since $\operatorname{Ker} V \mid_{W_n} = \mathbb{G}_a$. The Dieudonné module is given by generators $m_1, \ldots, m_n$ satisfying relations $Vm_i = 0$ for all i and $F^{a_i} m_i$ by the Proposition, where each m_i is the homomorphism $G \to \mathbb{G}_a$ sending the parameter of $\mathbb{G}_a$ to X_i.

From $T \in I_A$ such that $\Delta^*T = T \otimes 1 + 1 \otimes T$ we can construct a homomorphism $G \to \mathbb{G}_a$ sending the parameter of $\mathbb{G}_a$ to T; such homomorphisms correspond to elements of the Dieudonné module, each of which can be expressed in the form

$$\sum_{i,j} \alpha_{i,j} F^i m_j$$

and are therefore given by morphisms sending the parameter of $\mathbb{G}_a$ to a sum

$$T = \sum_{i,j} \alpha_{i,j} X_j^{p^i}.$$

□

2.4 Consideration of group schemes admitting an $\mathscr{O}$-action

In this section, we consider what it means for a $\mathcal{G} \in DG_k$ to admit a homomorphism $\mathscr{O} \to \operatorname{End}_{DG_k}(\mathcal{G})$, and if $(G, G^\flat, i_{\mathcal{G}}) \in DG^*_{k,\mathscr{O}}$, then we consider some possible $\mathcal{G}$. This leads naturally into the result of the following section, which is a condition on such G, in terms of classical Verschiebung, V.

Remark 2.4.1. If $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) \in DG_{R,\mathscr{O}}$, then $G = \operatorname{Spec} A$ is killed by p, ie the morphisms $[p] : G \to G$ and $[p]^\flat : G^\flat \to G^\flat$ factor through R. This follows since there is a homomorphism of rings $k[[\pi]] \cong \mathscr{O} \to \operatorname{End}_{DG_R} \mathcal{G}$.

This condition is stronger than simply requiring that $[p] : \mathcal{G} \to \mathcal{G}$ is the zero endomorphism in $DG^*_{R,\mathscr{O}}$, since zero endomorphisms in $DG^*_{R,\mathscr{O}}$ are not required to kill $G^\flat$, but only G. In the following two sections, the full implications of this are discussed.

In the following examples, we simplify matters somewhat by setting $\mathscr{O} = \mathbb{F}_p[[\pi]]$, and asking which group schemes G (of rank p) can occur in a triple $(G, G^\flat, i_\mathcal{G}) \in DG_{k,\mathscr{O}}$. We note that since k is an $\mathscr{O}$-algebra, π^* must act trivially on the algebras of A and $A^\flat$.

Passing to the algebraic closure $\overline{k}$ of k, there are three isomorphism classes of $\mathbf{D}_k$-modules of rank one over k: m_0k, where $F(m_0) = V(m_0) = 0$, m_1k, where $F(m_1) = m_1$ and $V(m_1) = 0$, and m_2k, where $F(m_2) = 0$ and $V(m_2) = m_2$. By the anti-equivalence of Theorem 2.3.3, these correspond to the three isomorphism classes of group schemes of order p over an algebraically closed field k of characteristic $p > 0$; α_p, (the additive k-group scheme of order p) μ_p (the multiplicative k-group scheme of order p), and $\mathbb{Z}/p\mathbb{Z}$ (the étale k-group scheme of order p) respectively. They were all considered in §2.2.3. We now 'lift' them to analogues in DG_k, and try to attach an $\mathscr{O}$-action to each one, such that they become objects in $DG_{k,\mathscr{O}}$.

2.4.1 Lifting α_p

Clearly we can lift α_p to $(\operatorname{Spec} k[T]/(T^p), \operatorname{Spec} k[T]/(T^{p+1}), i_\mathcal{G}) \in DG_k$; we have $\Delta^*(T) = T \otimes 1 + 1 \otimes T$, and via consideration of the counit axiom, $\Delta^{\flat*}(T) = T \otimes 1 + 1 \otimes T$. Therefore $[p] = [p]^\flat = 0$, and in order to get an object in $DG_{k,\mathscr{O}}$, we can set $\alpha^*T = \alpha T$ for all $\alpha \in \mathbb{F}_p$, and π^*T can be chosen in several ways, some of which were considered in chapter 1.

2.4.2 Lifting μ_p

Consider now μ_p. As discussed in §2.2.3, this k-group scheme is represented by $k[X]/(X^p - 1)$, with $\Delta^*(X) = X \otimes X$ and $\varepsilon^*(X) = 1$. We can lift μ_p to an object $(\operatorname{Spec} k[X]/(X^p - 1), \operatorname{Spec} k[X]/(X^p - 1)(X - 1), i) \in DG_k$

Substituting in $T = X - 1$, we see that μ_p is represented by $k[T]/(T^p)$ with

$$f_p(T) = f_p(X-1) = f_p(X) - f_p(1) = (T+1)^{\otimes p} - 1^{\otimes p}.$$

We can lift μ_p to an object $(\operatorname{Spec} k[T]/(T^p), \operatorname{Spec} k[T]/(T^{p+1}), i) \in DG_k$, by Proposition 1.5.7. Since $f_p^\flat$ lifts f_p,

$$f_p^\flat(T) = (T+1)^{\otimes p} - 1^{\otimes p}.$$

Therefore $[p]^\flat(T) = D^{*\flat} \circ f_p^\flat(T) = (T+1)^p - 1^p = T^p \neq 0$, which contradicts our assumption that $[p]^\flat = 0$. Therefore no form of μ_p can occur in any $\mathcal{G} \in DG_{k,\mathscr{O}}$, for $\mathscr{O} = \mathbb{F}_q[[\pi]]$ (even for $p \neq q$), since any such form would not satisfy $[p]^\flat = 0$.

2.4.3 Lifting $(\mathbb{Z}/p\mathbb{Z})$

The étale k-group scheme of order p is $(\mathbb{Z}/p\mathbb{Z})$, and it lifts to $((\mathbb{Z}/p\mathbb{Z}), \operatorname{Spec} k, i_0) \in DG_k$ on which $[p]$ vanishes. To make this object a member of the category $DG_{k,\mathscr{O}}$, it suffices to give an action of π^* which is nilpotent (since the $\mathbb{F}_p$ action is simply comultiplication). Since $\mathbb{F}_p[[\pi]]$ is required to act on our group scheme, π^* must act nilpotently, and the only nilpotent automorphism of $\mathbb{F}_p$ is the map sending every $a \in \mathbb{F}_p$ to zero, so there is a unique constant étale k-group scheme with $\mathbb{F}_p[[\pi]]$-action.

2.5 Comultiplication on $DG^*_{k,\mathscr{O}}$

We now prove the first main theorem of this chapter, which states that V is zero on all objects G in a triple $\mathcal{G} = (G, G^\flat, i_\mathcal{G})$ in $DG_{k,\mathscr{O}}$ (and hence $DG^*_{k,\mathscr{O}}$, since its objects are exactly those of $DG_{k,\mathscr{O}}$). Therefore, in what follows, we can assume that our G (as k-group schemes) lie in a subcategory of Gr_k, which will simplify our subsequent Dieudonné theory and classification.

Theorem 2.5.1. *Let $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG_{k,\mathscr{O}}$. Then $V = 0$ on $\mathcal{F}(\mathcal{G})$.*

Proof. By Remark 2.4.1, $[p]^\flat = 0$ and $[p] = 0$.

We can suppose that k is algebraically closed (ie $\overline{k} = k$), since if $[p]^\flat I_{(A\otimes\overline{k})^\flat} = [p]^\flat I_{A^\flat} \otimes \overline{k} \neq 0$, then $[p]^\flat I_{A^\flat} \neq 0$, as comultiplication is compatible with base change

Applying Corollary 2.3.4, we get a splitting $\operatorname{Spec} A \cong G^{\text{ét}} \times G^l \times G^m$, where V acts as an isomorphism on G^m and nilpotently on G^l and $G^{\text{ét}}$, and F acts as an isomorphism on $G^{\text{ét}}$, and nilpotently on G^l and G^m.

Suppose that $G^{\text{ét}}$ is non-trivial. Then since the functor $\mathcal{F} : DG^*_k \longrightarrow \mathrm{Gr}_k$ is an equivalence of categories, the closed immersion $G^{\text{ét}} \longrightarrow G$ induces a morphism $\mathcal{G}^{\text{ét}} \longrightarrow \mathcal{G}$ in DG^*_k, which is a closed immersion on the level of k-group schemes. $\mathcal{G}^{\text{ét}}$ is a triple $(\operatorname{Spec} A^{\text{ét}}, \operatorname{Spec} A^{\text{ét}^\flat}, i_{\mathcal{G}^{\text{ét}}})$, and the map $A \longrightarrow A^{\text{ét}}$ is a surjection as it is dual to a closed immersion. On $A^{\text{ét}}$, $[p] = F \circ V$, and F is an isomorphism since $A^{\text{ét}}$ is étale. Hence $V = 0$ is implied by $[p] = 0$.

If G^m is non-trivial, then consider its k-subgroup scheme $\operatorname{Ker} F\mid_{G^m}$. It is anti-equivalent by Theorem 2.3.3 to a Dieudonné module M on which V acts as an isomorphism. Since k is algebraically closed, V has an eigenvector $m \in M$ such that $Vm = \lambda m$ for some $\lambda \in k$. Replacing M by $M/\mathbf{D}_k m$ and possibly finding more eigenvectors of V if necessary, we can find a subquotient module M' of M which is of rank one, generated by some $m \in M'$ such that $Vm = m$. By the anti-equivalence, this implies that $\mu_p \subset G^m \subset G$, since M' is dual to μ_p. Since $\mathcal{F} : DG^*_k \longrightarrow \mathrm{Gr}_k$ is an equivalence of categories, there's a morphism $(\mu_p, \mu_p^\flat, i) \subset \mathcal{G}$ which induces an inclusion $\mu_p \longrightarrow G$, where $(\mu_p, \mu_p^\flat, i) \in DG_k$ is the minimal object constructed in §2.4.2, such that if $\mu_p^\flat = \operatorname{Spec} B^\flat$, $[p]^\flat \mid_{I_{B^\flat}} \neq 0$.

By Proposition 1.4.9, there's a surjection $A^\flat \longrightarrow B^\flat$, and therefore $[p]^\flat \mid_{I_{A^\flat}} \neq 0$, which contradicts $[p]^\flat \mid_{I_{A^\flat}} = 0$. Therefore G^m is trivial.

We now consider G^l.

By Theorem 2.3.3, G^l is anti-equivalent to a Dieudonné module $M = M_0$ on which F and V are nilpotent. Suppose that $V\mid_M \neq 0$ (equivalently, $V\mid_{G^l} \neq 0$.

Pick any non-zero $m_0 \in M_0$ such that $Fm_0 = Vm_0 = 0$ (the existence of such an m_0 follows since F and V are nilpotent), and let $M_1 = M_0/\mathbf{D}_k m_0$, so we have an exact sequence

$$0 \longrightarrow \mathbf{D}_k m_0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow 0.$$

. We can replace M_0 by M_1, and continue this procedure to get a series of exact sequences until we arrive at a sequence

$$0 \longrightarrow k m_n \longrightarrow M_n \longrightarrow M_{n+1} \longrightarrow 0$$

such that $V\mid_{M_n}\neq 0$ but $V\mid_{M_{n+1}}=0$.

By Proposition 2.3.5, M_{n+1} is the quotient of the free $\mathbf{D}_k$-module with generators $\overline{n}_1,\ldots,\overline{n}_l$ by the relations $V\overline{n}_1=\cdots=V\overline{n}_l=0$ and $F^{a_i}\overline{n}_i=0$ for some integers a_i. We have an exact sequence

$$0\to ka\to M_n\to M_{n+1}\to 0,$$

where $Fa=Va=0$.

M_n is generated by a (identifying a with its image in M_n) and some pre-images $n_1,\ldots,n_l$ of $\overline{n}_1,\ldots,\overline{n}_l$, such that $F^{a_i}n_i\in ka$, and $Vn_i\in ak$ for all i.

There are now two possibilities, which we consider separately: either $F^{a_i}n_i=0$ for all i, or else $0\neq F^{a_i}n_i\in ka$ for some i. In each case, we prove that $[p]^\flat\neq 0$, which contradicts our above remark that $[p]^\flat=0$ for each $\mathcal{G}\in DG_{k,\mathcal{O}}$. Hence $V=0$ on $\mathcal{F}(\mathcal{G})$.

If $F^{a_i}n_i=0$ for all i, then since $V\mid_{M_n}\neq 0$ and $Va=0$, $0\neq Vn_i\in ka$ for some n_i. Consider the subset of the n_i such that $Vn_i\neq 0$, and pick any n_j (there may be more than one) from this subset such that $a_j\leq a_i$ for any n_i in the subset. Subtracting scalar multiples of n_j from all other n_i in the subset, we may assume that $Vn_j\neq 0$, but $Vn_i=0$ for all other n_i, without changing the relations in F which the n_i satisfy, so M_n is generated by $n_1,\ldots,n_l,a$ with $F^{a_i}n_i=0$ for all i, $Vn_j\neq 0$, $Vn_i=0$ for all $i\neq j$, and $Fa=Va=0$. The quotient of M_n by $\oplus_{i\neq j}\mathbf{D}_kn_i\oplus\mathbf{D}_kFn_j$ is the module generated by a,n_j with the relations $Fa=Va=0$, $Fn_j=0$ and $Vn_j=\lambda a$ for some $\lambda\neq 0$. Since $\lambda\neq 0$, replacing a by λa, we can assume that $Vn_j=a$.

This is the quotient of the Dieudonné module of the Witt vectors of length two (generated by w_0,w_1, and with relations $Vw_0=w_1$ and $Vw_1=0$) by pth power Frobenius. $\operatorname{Ker} F\mid_{W_2}$ is the group scheme $\operatorname{Spec} k[X,Y]/(X^p,Y^p)=\operatorname{Spec} B$, with $VY=0$ and $VX=Y$, and therefore by the construction of V given in Proposition 2.2.9, $\pi(f_p(X))=Y^{\cdot p}$. Therefore, by Lemma 2.2.8,

$$f_p(X)=\sum_{i_1,\ldots,i_p}\alpha_{i_1,\ldots,i_p}Y^{i_1}\otimes\cdots\otimes Y^{i_p}\mod\sum_i(1^{\otimes i}\otimes X\otimes 1^{\otimes p-i-1}),$$

where $\alpha_{1,\ldots,1}=1$, and $\alpha_{i,\ldots,i}=0$ for $i>1$. Letting $B^\flat=k[X,Y]/(X^p,Y^p)(X,Y)$, the triple $\mathcal{B}=(\operatorname{Spec} B,\operatorname{Spec} B^\flat,i)\in DS_k$ is clearly minimal, and comultiplication lifts uniquely to $B^\flat$ by Proposition 1.5.7; therefore

$$f_p^\flat(X) = \sum_{i_1,\dots,i_p} \alpha_{i_1,\dots,i_p} Y^{i_1} \otimes \cdots \otimes Y^{i_p} \mod \sum_i (1^{\otimes i} \otimes X \otimes 1^{\otimes p-i-1})$$

and hence

$$[p]^\flat(X) = D^* \circ f_p^\flat(X) = \sum_i \alpha_{i,\dots,i}(Y^i)^p = Y^p \mod (X),$$

applying the arguments used in the proof of Lemma 2.2.8 to cancel terms $\alpha_{i_1,\dots,i_p}$ where not all subscripts are identical. By Corollary 1.5.8, the inclusion $\operatorname{Spec} B \subset G_n \subset G^l \subset G$ lifts to a morphism $\mathcal{B} \to \mathcal{G}$ in DG_k; by Proposition 1.4.9, the induced algebra morphism $A^\flat \to B^\flat$ is a surjection, hence $[p]^\flat \mid_{I_{A^\flat}} \neq 0$, contradicting $[p]^\flat = 0$.

If, on the other hand, $0 \neq F^{a_i} n_i \in ka$ for some i, then choose n_j from the set of those n_i such that $0 \neq F^{a_i} n_i \in ka$, such that $a_j \geq a_i$ for all i. Subtracting a scalar multiple of $F^{a_j - a_i} n_j$ from each n_i, we can reduce to the case where $F^{a_i} n_i = 0$ for all $i \neq j$.

Since $V \mid_{M_n} \neq 0$, there is at least one n_i such that $0 \neq V n_i \in ka$. Choose $n_{j'}$ from the set of those n_i such that $V n_i \neq 0$, such that $a_{j'} < a_i$ for each i; subtracting a scalar multiple of $n_{j'}$ from each n_i, we can reduce to the case where $V n_i = 0$ for all $i \neq j'$.

We now have two cases: $j = j'$, and $j \neq j'$. If $j = j'$, then we can quotient by $\mathbf{D}_k n_i$ for all $i \neq j$, and we get the Dieudonné module $\mathbf{D}_k n_j$, where $F^{a_j+1} n_j = 0$, and $0 \neq V n_j \in F^{a_j} n_j$. We now consider these two cases separately.

In the first case, using the fact that Frobenius is σ-linear, where $\sigma : k \to k$ is the pth power map, and the fact that k is algebraically closed, we may assume by making the substitution $n = \lambda n_j$ for some $\lambda \in k$ that our Dieudonné module is $\mathbf{D}_k n$, where $F^{a_j+1} n = 0$ and $V n = F^{a_j} n$. Consider the exact sequence of Dieudonné modules

$$0 \to M(W_2) \xrightarrow{f} M(W_2) \to \mathbf{D}_k n \to 0,$$

where $M(W_2)$ is the Dieudonné module associated to the Witt vectors of length two, given by generators x and y, with $Vx = y$, $Vy = 0$, and no other relations, and the map f is the $\mathbf{D}_k$-linear endomorphism of $M(W_2)$ given by $x \mapsto F^{a_j+1} x$ and

$y \mapsto F^{a_j}x$, which has cokernel $\mathbf{D}_k n$. By the Dieudonné anti-equivalence of Theorem 2.3.2, this exact sequence is dual to an exact sequence of k-group schemes

$$0 \to G' \to W_2 \to W_2 \to 0,$$

where the map $W_2 \to W_2$ is dual to the map of algebras $k[X,Y] \to k[X,Y]$ given by $X \mapsto X^{p^{a_j}+1}$ and $Y \mapsto X^{p^{a_j}}$; therefore the algebra of G' is $k[X,Y]/(X^{p^{a_j}+1}, Y - X^{p^{a_j}})$, which is isomorphic to $k[T]/(T^{p^{a_j+1}})$, where $VT = 1 \otimes T^{p^{a_j}}$. Hence $G' \subset G_n$.

By construction of V given in Proposition 2.2.9, $\pi(f_p(T)) = (T^{p^{a_j}})^{\cdot p}$. We can lift $\operatorname{Spec} B$ to a minimal object $(\operatorname{Spec} B, \operatorname{Spec} B^\flat, i) \in DG_k$ as above, where $B^\flat = k[T]/T^{p^{a_j}+2})$.

Since $\pi(f_p(T)) = (T^{p^{a_j}})^{\cdot p}$, we can apply Lemma 2.2.8, which says that $f_p(T)$ has the form

$$f_p(T) = \sum_{i_1,\dots,i_p} \alpha_{i_1,\dots,i_p} T^{i_1} \otimes \cdots \otimes T^{i_p},$$

where $\alpha_{p^{a_j},\dots,p^{a_j}} = 1$, and $\alpha_{i,\dots,i} = 0$ for all $i \neq p^{a_j}$. Therefore

$$f_p^\flat(T) = \sum_{i_1,\dots,i_p} \alpha_{i_1,\dots,i_p} T^{i_1} \otimes \cdots \otimes T^{i_p},$$

and hence $[p]^\flat(T) = D^* \circ f_p^\flat(T) = T^{p^{a_j}+1} \neq 0$. Since $\mathcal{B}$ is minimal, and our inclusion $\operatorname{Spec} B \subset G_n \subset G^l \subset G$ lifts to a morphism $\mathcal{B} \to \mathcal{G}$, we can apply the same arguments as before to deduce that $[p]^\flat \,|_{I_{A^\flat}} \neq 0$, which is a contradiction.

In the second case, we can take the quotient of our Dieudonné module by $\mathbf{D}_k n_i$ for all $i \neq j, j'$ to get the Dieudonné module generated by $n_j, n_{j'}$, where $Vn_j = 0$, $Vn_{j'} = \lambda F^{a_j} n_j$ for some $\lambda \in k$, $F^{a_j+1} n_j = 0$, and $F^{a_{j'}} n_{j'} = 0$. By replacing n_j by $\lambda^{p^{a_j}} n_j$, we can assume that $Vn_{j'} = F^{a_j} n_j$.

Consider the exact sequence of Dieudonné modules

$$0 \to M(W_2 \times W_1) \xrightarrow{f} M(W_2 \times W_1) \to \mathbf{D}_k n_j + \mathbf{D}_k n_{j'} \to 0,$$

where $M(W_2 \times W_1)$ is the Dieudonné module of $W_2 \times W_1$, with generators x, y, z, and relations $Vx = y$ and $Vy = Vz = 0$, and f is the $\mathbf{D}_k$-linear endomorphism of this Dieudonné module given by $x \mapsto F^{a_{j'}}x$, $y \mapsto Fy$, and $z \mapsto y - F^{a_j}z$. By Theorem 2.3.2, this exact sequence is dual to an exact sequence of group schemes

$$0 \to G' \to W_2 \times W_1 \to W_2 \times W_1 \to 0,$$

where G' is a subgroup scheme of G_n by the Dieudonné anti-equivalence, since its Dieudonné module is a quotient of the Dieudonné module of G_n, $W_2 \times W_1$ has algebra $k[X,Y,Z]$, with $VX = 1 \otimes Y$, and $VY = VZ = 0$, and G' has algebra $k[X,Y,Z]/(X^{p^{a_{j'}}}, Y^p, Z^{p^{a_j}})$, with $VX = 1 \otimes Y$ and $VY = VZ = 0$, which is congruent to $B = k[X,Y]/(X^{p^{a_{j'}}}, Y^{p^{a_j+1}})$, with $VX = 1 \otimes Y^p$.

Arguing as for the kernel of Frobenius on W_2 (earlier in this proof), it can be shown that for any minimal $\mathcal{B} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i) \in DG_k$ such that $\mathcal{F}(\mathcal{B}) = \operatorname{Spec} k[X,Y]/(X^{p^{a'_j}}, Y^{p^{a_j+1}})$ and $VX = 1 \otimes Y^p$, $[p]^\flat \mid_{\mathcal{B}} \neq 0$, and that there is a surjection of algebras $A^\flat \to B^\flat$, implying that $[p]^\flat \mid_{I_{A^\flat}} \neq 0$, which is a contradiction.

Therefore we have a contradiction if $V \neq 0$ on G^u, and hence $V = 0$ on G^u.

Therefore, if $V \mid_{G^l} = 0$. Since G^m is trivial, and $V \mid_{G^{\text{ét}}} = 0$ by the above argument, $V = 0$ on $\mathcal{F}(\mathcal{G}) = G^{\text{ét}} \times G^l \times G^m$, and the result is proved. □

2.6 Idempotent operators

In this section, we introduce some operators e_i on the algebras A, A^{loc} and $A^\flat$ associated to an object $\mathcal{G} \in DG_{k,\mathcal{O}}$ which will prove useful later. We also prove a lemma from representation theory, which we will use to construct our Dieudonné anti-equivalence.

Definition 2.6.1. Let $(\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{G}}) = \mathcal{G} \in DG^*_{k,\mathcal{O}}$. Then for each $1 \leq i \leq q-1$, we can define morphisms of k-modules $A \to A$, $A^{\text{loc}} \to A^{\text{loc}}$ and $A^\flat \to A^\flat$

$$e_i = -\sum_{\alpha \in \mathbb{F}_q^*} \alpha^{-i} \alpha^*$$

sending $a \in A$ to $e_i a$, $a^{\text{loc}} \in A^{\text{loc}}$ to $e_i a^{\text{loc}}$ and $a^\flat \in A^\flat$ to $e_i a^\flat$. Note that in this expression, α^* refers to the morphism $\alpha^* : \mathcal{G} \to \mathcal{G}$ of strict $\mathcal{O}$-action on $\mathcal{G}$, and its induced action on A, A^{loc} and $A^\flat$ respectively.

These operators are compatible with the quotient map $q : A^\flat \to A^{\text{loc}}$ in the sense that $q(e_i a^\flat) = e_i q(a^\flat)$ for $a^\flat \in A^\flat$, since the morphisms α^* for $\alpha \in \mathbb{F}_q$ have this property.

Remark 2.6.2. These operators are analogous to the e_i defined in [OT70] for group schemes of order p; we prove that they have very similar properties.

Lemma 2.6.3. *The operator e_i satisfies the following identities:*

1. $\sum_{1\le i\le q-1} e_i = 1$
2. $\alpha^* e_i X = \alpha^i e_i X$ *for any* $X \in A$ *(or* A^{loc}*, or* $A^\flat$*).*
3. $e_i e_j = \delta_{ij} e_i$*, where* δ_{ij} *is the Kronecker delta.*

Proof. 1. The coefficient of α^* in $\sum_{1\le i\le q-1} e_i$ (for $\alpha \in \mathbb{F}_q^*$) is $-\sum_{1\le i\le q-1}\alpha^{-i}$, which is zero unless $\alpha = 1$ (since it is invariant under multiplication by α). The coefficient of 1^* is clearly one, and therefore $\sum_{1\le i\le q-1} e_i = 1$.

2. For $\alpha = 0$, the result is trivial; we now consider the case $\alpha \neq 0$:

$$\begin{aligned}
\beta^* e_i X &= -\sum_{\alpha\in\mathbb{F}_q^*} \alpha^{-i}\beta^*\alpha^* X \\
&= -\sum_{\alpha\in\mathbb{F}_q^*} \alpha^{-i}(\beta\alpha)^* X \\
&= -\sum_{\gamma\in\mathbb{F}_q^*} \gamma^{-i}\beta^i\gamma^* X \text{ (substituting } \gamma = \alpha\beta) \\
&= -\beta^i \sum_{\gamma\in\mathbb{F}_q^*} \gamma^{-i}\gamma^* X \\
&= \beta^i e_i X.
\end{aligned}$$

3.

$$\begin{aligned}
e_i e_i &= \sum_{\alpha\in\mathbb{F}_q^*}\sum_{\beta\in\mathbb{F}_q^*} (\alpha\beta)^{-i}(\alpha\beta)^* \\
&= \sum_{\gamma\in\mathbb{F}_q^*} (q-1)\gamma^{-i}\gamma^* \\
&= -\sum_{\gamma\in\mathbb{F}_q^*} \gamma^{-i}\gamma^* \\
&= e_i,
\end{aligned}$$

since $\alpha\beta = \gamma$ has $q-1$ solutions over $\alpha, \beta \in \mathbb{F}_q^*$. If $i \neq j$, then

$$e_i e_j = \sum_{\alpha\in\mathbb{F}_q^*}\sum_{\beta\in\mathbb{F}_q^*} \alpha^{-i}\beta^{-j}(\alpha\beta)^*.$$

Hence the coefficient of γ^* in $e_i e_j$ is $\sum_{\alpha\in\mathbb{F}_q^*}\alpha^{-i}(\gamma\alpha^{-1})^{-j} = \gamma^{-j}\sum_{\alpha\in\mathbb{F}_q^*}\alpha^{j-i}$, which is clearly invariant under multiplication by β^{j-i} for any $\beta \in \mathbb{F}_q^*$, and therefore zero.

Therefore $e_i e_j = \delta_{ij} e_i$.

$\square$

We need a basic lemma concerning endomorphisms of finite dimensional vector spaces. Let $\chi_d : \mathbb{F}_q \to k$ for $d = 0, \ldots, r-1$ be the homomorphisms of rings given by $\chi_d(\alpha) = \alpha^{p^d}$ for $\alpha \in \mathbb{F}_q$, where we implicitly identify $\alpha \in \mathbb{F}_q$ with its image in k.

Lemma 2.6.4. *Let V be a k-module, and let $\rho : \mathbb{F}_q \to \mathrm{End}_k(V)$ be a homomorphism of rings. Then V decomposes as*

$$V = \bigoplus_{\chi_d} V_{\chi_d},$$

where $V_{\chi_d} \subset V$ is the k-vector subspace of V such that $\rho(\alpha)(v) = \chi_d(\alpha)v$. (It's easy to verify that each V_{χ_d} is a k-vector subspace).

Proof. Let $v \in V$. Define

$$v_i = -\sum_{\alpha \in \mathbb{F}_q^*} \alpha^{-i} \rho(\alpha)(v).$$

Then

$$\begin{aligned} \sum_{1 \le i \le q-1} v_i &= -\sum_{\alpha \in \mathbb{F}_q^*} (\alpha^{-1} + \cdots + \alpha^{1-q}) \rho(\alpha)(v) \\ &= v, \end{aligned} \tag{2.6.1}$$

because (as above) the sum vanishes unless $\alpha = 1$. Further, $\rho(\beta)v_i = \beta^i v_i$, as in the proof of the previous result. If $v_i \neq 0$ for i not a power of p, then $\rho(\alpha + \beta)(v_i) = (\alpha + \beta)^i v_i \neq (\alpha^i + \beta^i)v_i = (\rho(\alpha) + \rho(\beta))(v_i)$, which contradicts the assumption that ρ is a homomorphism of rings. Therefore $v_i \neq 0$ only if i is a power of p. Setting $v_{\chi_i} = v_{p^i}$, (2.6.1) gives

$$v = \sum_{\chi_i} v_{\chi_i}.$$

Any pair $V_{\chi_d}, V_{\chi_{d'}}$, for $d \neq d'$, are orthogonal since any $0 \neq v \in V$ inside both must satisfy $\alpha^* v = \alpha^{p^d} v = \alpha^{p^{d'}} v$ for any $\alpha \in \mathbb{F}_q^*$, which implies that $\alpha^{p^d - p^{d'}} = 1$. Taking α to be a generator of $\mathbb{F}_q^*$, we see that this cannot hold unless $p^d - p^{d'} \equiv 0 \mod q-1$, but by definition $0 \le d, d' < r$, which is a contradiction. This suffices to give the direct sum decomposition, as any V_{χ_d} is clearly a k-submodule of V. $\square$

2.7 Classifying connected schemes

In this section, we provide an explicit classification theorem for all connected $\mathcal{G} \in DG^*_{k,\mathcal{O}}$, where the meaning of *connected* is that defined in the statement of Definition 1.6.3. Since we know that $V\mid_{\mathcal{F}(\mathcal{G})}= 0$, classical results tell us what the structure of the algebras of such $\mathcal{G}$ look like; therefore, it suffices to determine the $\mathcal{O}$-action on $\mathcal{G}$. This theorem is used in the following section, where we define an operation $\overline{V}$ explicitly on such connected $\mathcal{G}$.

In order to prove the theorem, we first need an elementary lemma about congruences.

Lemma 2.7.1. *Let $q = p^r$ for some prime p and $r \in \mathbb{N}$. Then the values of $l \in \mathbb{N} \cup \{0\}$ satisfying the congruence*

$$1 \equiv p^l \mod q-1.$$

are exactly those such that $r \mid l$, ie such that p^l is a power of q.

Proof. Solutions of the congruence correspond to solutions of

$$1 = p^l - w(p^r - 1)$$

for some $l \in \mathbb{N} \cup \{0\}$ and $w \in \mathbb{Z}$. Therefore $l = 0$ or

$$w = \frac{p^l - 1}{p^r - 1}$$

which is integer if and only if $r \mid l$. Therefore $p^l = q^{l/r}$, proving the result. □

Theorem 2.7.2. *Let $\mathcal{G} \in DG^*_{k,\mathcal{O}}$ be connected. Then $\mathcal{G} \cong \mathcal{H} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_{\mathcal{H}})$ with*

$$A \cong k[X_1, \ldots, X_n]/(X_1^{q^{e1}}, \ldots, X_n^{q^{en}}),$$

$I_A = (X_1, \ldots, X_n)$, $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$,

$$A^\flat \cong k[X_1, \ldots, X_n]/(X_1, \ldots, X_n)(X_1^{q^{e1}}, \ldots, X_n^{q^{en}}),$$

$\alpha^* X_i = \alpha X_i$ for $\alpha \in \mathbb{F}_q$, and $\pi^* X_i$ a linear combination of $X_i^{q^m}$; in particular, each polynomial $\pi^* X_i$ factors through qth power Frobenius.

Proof. By Corollary 1.8.2, $\mathcal{G}$ is isomorphic to some minimal $\mathcal{H} \in DG^*_{k,\mathcal{O}}$. By Theorem 2.5.1, $V \mid_{\mathcal{F}(\mathcal{H})}= 0$. Therefore, applying Corollary 2.3.6, we see that $\mathcal{F}(\mathcal{H}) \cong \operatorname{Spec} A$, where

$$A = k[X_1, \dots, X_n]/(X_1^{p^{a_1}}, \dots, X_n^{p^{a_n}})$$

for some integers $a_1, \dots, a_n \in \mathbb{N}$, and $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$ for all i. We may take

$$A^\flat \cong k[X_1, \dots, X_n]/(X_1^{p^{a_1}}, \dots, X_n^{p^{a_n}})(X_1, \dots, X_n);$$

since $(A, A^\flat, i_A) \in DA_R$ is minimal, it's isomorphic to any other minimal object on the level of algebras by Corollary 1.4.6. By the counit axiom, it follows that $\Delta^{*\flat} X_i = X_i \otimes 1 + 1 \otimes X_i$ in $A^\flat$.

The $\mathcal{O}$-action is determined by the action of each $o \in \mathcal{O}$ on each X_i in $A^\flat$; $o^* X_i = oX_i \mod (X_1, \dots, X_n)^2$. We can replace X_1 by $e_1 X_1$; $(e_1 X_1, X_2, \dots, X_n) = (X_1, \dots, X_n) \mod (X_1, \dots, X_n)^2$, since $e_1 X_i = (1 - \sum_{w>1} e_w) X_i = X_i - \sum e_w X_i$, and each $e_w X_i \in (X_1, \dots, X_n)^2$ for $w > 1$ since $\alpha^*(e_w X_i) = \alpha^w e_w X_i$. Therefore $e_1 X_1, \dots, X_n$ generate $A^\flat$ as a k-algebra. Replacing each X_i by $e_i X_i$ in turn, we can assume that each X_i is an eigenvector for the $\mathbb{F}_q^*$-action, in the sense that

$$\alpha^* X_i = \alpha X_i$$

for all $\alpha \in \mathbb{F}_q^*$.

Since π^* induces the zero endomorphism of $(X_1, \dots, X_n)/(X_1, \dots, X_n)^2$ by definition of its strict action, and since it commutes with Δ^*, we can apply Corollary 2.3.7 to see that

$$\pi^{\mathrm{loc}*} X_i = \sum_{j,l>0} a_{j,l} X_j^{p^l}$$

for each i, on A^{loc}, where each $a_{j,l} \in k$. Since $N_{\mathcal{G}}$ is generated as a k-vector space by $X_1^{p^{a_1}}, \dots, X_n^{p^{a_n}}$, and since the action of π^* on A^{loc} determines the action of π^* on $A^\flat$ up to $N_{\mathcal{G}}$, $\pi^{\flat*} X_i$ is also given by

$$\pi^{\flat*} X_i = \sum_{j,l>0} a'_{j,l} X_j^{p^l},$$

in $A^\flat$.

Since $\pi^*\alpha^* = \alpha^*\pi^*$ for α generating $\mathbb{F}_q^*$, it follows that each exponent of X_j must be 1 modulo $q-1$ (since $\alpha^* X_j^{p^n} = \alpha^{p^n} X_j^{p^n}$ and $\alpha^* X_i = \alpha X_i$ on the left hand side). Hence the only possible exponents of X_j are solutions p^l of the congruence

$$1 \equiv p^l \mod p^r - 1.$$

which implies that p^l is a power of q by Lemma 2.7.1. Hence

$$\pi^* X_i = \sum a''_{j,l} X_j^{q^l}$$

for new constants $a''_{j,l}$. In particular, π^* factors through qth power Frobenius, since k is perfect.

Finally, consider the k-module $N_{\mathcal{H}}$ which is the ideal $(X_1^{p^{a_1}}, \ldots, X_n^{p^{a_n}})$ in $A^\flat$. If $\alpha \in \mathbb{F}_q^*$ generates, then $\alpha^*(X_i^{p^{a_i}}) = \alpha^{p^{a_i}} X_i^{p^{a_i}}$; by strictness, this must be equal to $\alpha X_i^{p^{a_i}}$, so $p^{a_i} = 1 \mod q-1$; by Lemma 2.7.1, this implies that p^{a_i} is actually a power of q.

Hence each power of p in our algebra description is actually a power of q, proving the result. □

2.8 Frobenius and Verschiebung

As has already been shown, the classical functor V is trivial on $DG^*_{k,\mathcal{O}}$; in this section we introduce a strict replacement, $\overline{V}_\pi$, in the following sense: classically in the category of k-group schemes (for k of characteristic $p > 0$), there is a factorisation

$$[p] = F \circ V = V \circ F.$$

We show that π^* can be factorised as

$$\pi^* = \overline{V}_\pi \circ \overline{F}_\pi = \overline{F}_\pi \circ \overline{V}_\pi,$$

where $\overline{F}_\pi$ is qth power Frobenius. This factorisation lies at the heart of our Dieudonné theory, and provides the obvious link between our theory and the classical one.

Definition 2.8.1. We can define a functorial morphsim $\overline{F}_\pi$ from DG_k to DG_k: on $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G})$, $F_\pi^\flat = F^r$ (so $F_\pi^\flat$ is qth power Frobenius), and F acts on the k-algebra $A^\flat$. Similarly $F_\pi = F^r$ on A (which makes $\overline{F}_\pi$ a morphism in DG_k). $\overline{F}_\pi$ commutes with multiplication $\overline{\Delta}$ since all morphisms commute with Frobenius, up to a twist $k \longrightarrow k$.. Similarly, $\overline{F}_\pi$ commutes with any morphism $\overline{f} : \mathcal{G} \longrightarrow \mathcal{H}$ for $\mathcal{H} \in DG_k$, so $\overline{F}_\pi$ is functorial.

Lemma 2.8.2. *There is a natural extension of* $\overline{F}_\pi$ *to* $DG^*_{k,\mathcal{O}}$.

Proof. The action of $\mathcal{O}$ on $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG^*_{k,\mathcal{O}}$ is by endomorphisms; clearly endomorphisms commute with any power of Frobenius up to a twist $k \longrightarrow k$, so diagram (1.6.1) commutes; the only remaining thing to check is that on the base change of $\mathcal{G}$ by $\sigma^r : k \longrightarrow k$, $\mathcal{O}$ acts 'by scalars'. On $i \in I_{A^\flat}/I^2_{A^\flat}$, we know that $o \in \mathcal{O}$ acts by $o^* a = oa$; on $k \otimes I_{A^\flat}/I^2_{A^\flat}$ ($I_{A^\flat}$ twisted by σ^r), o acts as multiplication by $\tilde{o} \otimes 1$ (where we define $\tilde{o}$ to be the image of o in k under the morphism $\mathcal{O} \longrightarrow k$), so it sends $1 \otimes a$ to $1 \otimes \sigma^{-r}\tilde{o}a = 1 \otimes \tilde{o}a$ since $\tilde{o} \in \mathbb{F}_q$, on which σ^r (the qth power map) is the identity, which is equal to $o^*(1 \otimes a) = 1 \otimes \tilde{o}a$. Hence the $\mathcal{O}$ action is 'by scalars' on $k \otimes I_{A^\flat}/I^2_{A^\flat}$; similarly it follows that its action on $k \otimes N_\mathcal{G}$ is also 'by scalars'; therefore $\overline{F}_\pi(\mathcal{G}) \in DG^*_{k,\mathcal{O}}$. □

Proposition 2.8.3. *To each* $\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \in DG^*_{k,\mathcal{O}}$, *we can associate a unique morphism* $\overline{V}_\pi : \mathcal{G} \longrightarrow \mathcal{G}^{(q^{-1})}$ *in* $\operatorname{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{G}^{(q^{-1})})$, *such that we have the following factorisation of* π^* :

$$\pi^* = \overline{F}_\pi \circ \overline{V}_\pi = \overline{V}_\pi \circ \overline{F}_\pi.$$

Further, $\overline{V}_\pi$ *is functorial. In other words, the diagram*

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\overline{f}} & \mathcal{H} \\ \downarrow{\scriptstyle \overline{V}_\pi} & & \downarrow{\scriptstyle \overline{V}_\pi} \\ \mathcal{G}^{(q^{-1})} & \xrightarrow{\overline{f}^{(q^{-1})}} & \mathcal{H}^{(q^{-1})} \end{array} \tag{2.8.1}$$

commutes for all objects $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$ *and all morphisms* $\overline{f} : \mathcal{G} \longrightarrow \mathcal{H}$ *in* $DG^*_{k,\mathcal{O}}$.

Proof. It suffices to assume $\mathcal{G}$ is minimal, since every $\mathcal{G} \in DG^*_{k,\mathcal{O}}$ is isomorphic to a minimal $\mathcal{G}$ via a two-sided isomorphism, by Proposition 1.5.11.

By Lemma 1.8.7, $\mathcal{G} \cong \mathcal{G}^0 \times \mathcal{G}^{\text{ét}}$; since Frobenius is invertible on $\mathcal{G}^{\text{ét}}$ and nilpotent on $\mathcal{G}^0$, $\pi^*(A^{\text{loc}}) \subset A^{\text{loc}}$ and $\pi^*(A^{\text{ét}}) \subset A^{\text{ét}}$; similarly for F_π. Therefore it will suffice to define our morphism $\overline{V}_\pi$ on $\mathcal{G}^{\text{ét}}$ and $\mathcal{G}^0$ separately.

On $A^{\text{ét}}$, $F_\pi : k \otimes A \to A$ is surjective; this follows since $A^{\text{ét}}$ is étale, and since k is perfect (so σ^r is surjective on it). Therefore it is bijective, hence invertible as a morphism of Hopf algebras. Let $F_\pi^{-1} : A^{\text{ét}} \to k \otimes A^{\text{ét}}$ denote its inverse. F_π^{-1} commutes with the $\mathcal{O}$-action on $A^{\text{ét}}$ since it's the inverse of F_π, which commutes with the $\mathcal{O}$-action by construction.

Then we define V_π to be the endomorphism of $A^{\text{ét}}$ given by $F_\pi^{-1} \circ \pi^* = \pi^* \circ F_\pi^{-1}$. Clearly this morphism commutes with F_π; it commutes with the $\mathcal{O}$-action on $A^{\text{ét}}$ since F_π^{-1} does, and $V_\pi \circ F_\pi = F_\pi \circ V_\pi = \pi^*$, so V_π (on $A^{\text{ét}}$) has all the required properties.

By the previous Theorem,

$$A^{\text{loc}} \cong k[X_1, \dots, X_n]/(X_1^{q^{e_1}}, \dots, X_n^{q^{e_n}})$$

for some integers e_i, with $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$, and

$$A^\flat \cong k[X_1, \dots, X_n]/(X_1^{q^{e_1}}, \dots, X_n^{q^{e_n}})(X_1, \dots, X_n).$$

Further, $\alpha^* X_i = \alpha X_i$ for $\alpha \in \mathbb{F}_q^*$, and π^* factors through qth power Frobenius. Explicitly $\pi^* : A^\flat \to A^\flat$ is described by

$$\pi^* X_i = \sum_j a_{j,l} X_j^{q^l}$$

for some constants $a_{j,l} \in k$ depending on i, where $l > 0$ for all l. The map $\pi^* : A^{\text{loc}} \to A^{\text{loc}}$ is simply the reduction of this modulo the kernel of the map $i_G : A^\flat \to A^{\text{loc}}$. We can define a morphism $\overline{V}_\pi : \mathcal{G}^{(q)} \to \mathcal{G}$ in $DG^*_{k,\mathcal{O}}$ by

$$V_\pi^\flat(X_i) = \sum_j a_{j,l} \otimes X_j^{q^{l-1}}$$

for each X_i, with the obvious restriction to A^{loc}. It's obvious that $\overline{V}_\pi$ commutes with the action of $\alpha \in \mathbb{F}_q^* \subset \mathcal{O}$, and with Δ^*, and also obvious that $\pi^* = \overline{F}_\pi \circ \overline{V}_\pi$. From this last statement it follows that $\overline{V}_\pi$ commutes with π^*.

Our choice of $V_\pi\ |_{A^{\mathrm{loc}}}$ is unique: by Corollary 2.3.7,

$$V_\pi(X_i) = \sum_{j,l} b_{j,l} \otimes X_j^{p^l},$$

for some coefficients $b_{j,l} \in k$. Since V_π commutes with α^*-action, for any $\alpha \in \mathbb{F}_q$, we know that each power p^l must be congruent to 1 mod $q-1$. Therefore we can apply Lemma 2.7.1 to conclude that

$$V_\pi(X_i) = \sum_{j,l} c_{j,l} \otimes X_j^{q^l},$$

for some coefficients $c_{j,l} \in k$, such that $l < e_j$, and for each i. Any V_π to $V_\pi^\flat$:

$$V_\pi^\flat(X_i) = \sum_{j,l} c_{j,l} \otimes X_j^{q^l} + \sum_j d_j \otimes X_w^{q^{e_j}},$$

must satisfy $F_\pi \circ V_\pi = \pi^*$, and

$$F_\pi^\flat(V_\pi^\flat(X_i)) = \sum_{j,l} c_{j,l} X_j^{q^{l+1}}$$

implies that each $c_{j,l}$ is equal to $a_{j,l}$.

Note that we could have chosen any other lift of V_π^{loc} to $V_\pi^\flat$ as a morphism of algebras $A^\flat \to A^\flat$, provided it commutes with the $\mathcal{O}$-action. However, since the difference of any two such morphisms $V_\pi^\flat, V_\pi'^\flat$ in $\mathrm{Hom}_{DG_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{G}^{(q^{-1})})$ is trivial on A^{loc}, the difference is the trivial morphism in $\mathrm{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{G})$ by construction of morphisms in the category $DG^*_{k,\mathcal{O}}$; therefore $\overline{V}_\pi$ is uniquely defined as a morphism in $DG^*_{k,\mathcal{O}}$.

We have defined a family morphisms $\overline{V}_\pi : \mathcal{G}^{(q^x)} \to \mathcal{G}^{(q^{x-1})}$ for each $x \in \mathbb{Z}$ by twisting $\mathcal{G}$ and $\mathcal{G}^{(q^{-1})}$, and by a slight abuse of notation, we can write

$$\pi^* = \overline{F}_\pi \circ \overline{V}_\pi = \overline{V}_\pi \circ \overline{F}_\pi.$$

Taking the product of V_π on A^{loc} and $A^{\mathrm{\acute{e}t}}$ gives a morphism $A \to A$.

To prove that $\overline{V}_\pi$ is functorial, we need to prove that the diagram (2.8.1) commutes with all morphisms $\overline{f} : \mathcal{G} \to \mathcal{H}$ in $DG^*_{k,\mathcal{O}}$. Let $\mathcal{H} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i_{\mathcal{H}})$, and assume (by Theorem 2.7.2) that $B^{\mathrm{loc}} \cong k[Y_1, \ldots, Y_m]/I_B$, with $\Delta^*(Y_i) = Y_i \otimes 1 + 1 \otimes Y_i$ and $\alpha^* Y_i = \alpha Y_i$ for $\alpha \in \mathbb{F}_q$. It suffices to establish that $V_\pi \circ f = f \circ V_\pi$ on A, since any two morphisms in $DG^*_{k,\mathcal{O}}$ differing only in their image in $H^\flat$ and not in H are identified, by construction of $DG^*_{k,\mathcal{O}}$. On $A^{\text{ét}}$, this follows since it is $F_\pi^{-1} \circ \pi^*$, and both of these morphisms have this property.

The morphism $B \to A^{\text{loc}}$ factors through B^{loc}, as Frobenius is invertible on $B^{\text{ét}}$ and nilpotent on B^{loc}. By Corollary 2.3.7, the morphism is given on the level of coordinates by

$$f(Y_i) = \sum_{j,l} a_{j,l} X_j^{p^l}$$

for some $a_{j,l} \in k$. By compatibility with $\mathcal{O}$, each power p^l must be congruent to 1 mod $q-1$; by Lemma 2.7.1, each power of p is actually a power of q. Hence

$$f^\flat(Y_i) = \sum_{j,l} b_{j,l} X_j^{q^l}$$

for some $b_{j,l} \in k$, since $N_\mathcal{G} = (X_1^{q^{e_1}}, \ldots, X_n^{q^{e_n}})$, and $f^\flat$ is determined by f up to $N_\mathcal{G}$.

It follows that $V_\pi^\flat \circ f^\flat$ and $f^\flat \circ V_\pi^\flat$ differ by linear combinations of q^xth powers of X_i, for various x. Since $\pi^* \circ f = f \circ \pi^*$, it follows that this difference is annihilated by qth power Frobenius; but the only q^xth powers of X_i which are annihilated by $F_\pi^\flat$ are $X_i^{q^{e_i}} \in N_\mathcal{G}$; therefore the difference between $V_\pi^\flat \circ f^\flat$ and $f^\flat \circ V_\pi^\flat$ lies in $N_\mathcal{G}$, and hence f^{loc} and V_π^{loc} commute on the level of B^{loc} and A^{loc}.

Therefore their difference is a morphism $\mathcal{G} \to \mathcal{H}$ which induces the trivial morphism $\operatorname{Spec} B^{\text{loc}} \to \operatorname{Spec} A^{\text{loc}}$; by definition of morphisms in the category $DG^*_{k,\mathcal{O}}$, the difference between $\overline{V}_\pi$ and $\overline{f}$ is zero in $\operatorname{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$, so they commute.

Hence $\overline{V}_\pi$ and $\overline{f}$ commute for all $\overline{f} \in DG^*_{k,\mathcal{O}}$ and $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$; therefore $\overline{V}_\pi$ is functorial in the category $DG^*_{k,\mathcal{O}}$. □

Proposition 2.8.4. *If $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$ are connected, any morphism $f : \mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$ which commutes with V_π and $\mathbb{F}_q \subset \mathcal{O}$-action lifts to a morphism $\overline{f} : \mathcal{G} \to \mathcal{H}$ in $DG^*_{k,\mathcal{O}}$.*

Proof. By Theorem 2.7.2, we can assume

$$\mathcal{G} = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i_\mathcal{G}) \text{ and } \mathcal{H} = (\operatorname{Spec} B, \operatorname{Spec} B^\flat, i_\mathcal{H}),$$

with $A \cong k[X_1, \ldots, X_n]/I_A$, $B \cong k[Y_1, \ldots, Y_m]/I_B$, $A^{\text{loc}} \cong A$, $B^{\text{loc}} \cong B$, $A^\flat \cong k[X_1, \ldots, X_n]/I_A(X_1, \ldots, X_n)$, $B^\flat \cong k[Y_1, \ldots, Y_m]/I_B(Y_1, \ldots, Y_m)$, where

$$I_A = (X_1^{q^{e_1}}, \ldots, X_n^{q^{e_n}})$$

and

$$I_B = (Y_1^{q^{e'_1}}, \ldots, Y_m^{q^{e'_m}})$$

and $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$, and $\Delta^*(Y_i) = Y_i \otimes 1 + 1 \otimes Y_i$. Further, $\alpha^*(X_i) = \alpha X_i$, and $\alpha^* Y_i = \alpha Y_i$, for $\alpha \in \mathbb{F}_q$. f is given by setting $f(Y_i)$ equal to a linear combination of $X_i^{q^l}$ for various i and l, and clearly lifts to a map $f^\flat$ with the same properties. Since $f(V_\pi Y_i) = V_\pi f(Y_i)$, and therefore the difference between $f^\flat(V_\pi^\flat Y_i)$ and $V_\pi^\flat f^\flat(Y_i)$ is in the ideal I_A. Applying F_π (which is V_π and $f^\flat$ linear) to both sides annihilates this difference, from which it follows that $f^\flat$ is π^* compatible, and therefore f lifts to $\overline{f}$ as required. □

Corollary 2.8.5. *If $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$, any morphism $f : \mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$ which commutes with V_π and $\mathbb{F}_q \subset \mathcal{O}$-action lifts to a morphism $\overline{f} : \mathcal{G} \to \mathcal{H}$ in $DG^*_{k,\mathcal{O}}$.*

Proof. By Lemma 1.8.7, we have decompositions $\mathcal{G} \cong \mathcal{G}^{\text{ét}} \times \mathcal{G}^0$ and $\mathcal{H} \cong \mathcal{H}^{\text{ét}} \times \mathcal{H}^0$. Since F is invertible on étale k-group schemes and nilpotent on connected k-group schemes, it suffices to prove that the induced morphisms $\mathcal{F}(\mathcal{G}^{\text{ét}}) \to \mathcal{F}(\mathcal{H}^{\text{ét}})$ and $\mathcal{F}(\mathcal{G}^0) \to \mathcal{F}(\mathcal{H}^0)$ lift to morphisms $\mathcal{G}^{\text{ét}} \to \mathcal{H}^{\text{ét}}$ and $\mathcal{G}^0 \to \mathcal{H}^0$.

By Proposition 1.5.11, it suffices to assume that $\mathcal{G}^{\text{ét}} = (\mathcal{F}(\mathcal{G}^{\text{ét}}), \operatorname{Spec} k, i)$ and $\mathcal{H}^{\text{ét}} = (\mathcal{F}(\mathcal{H}^{\text{ét}}), \operatorname{Spec} k, i)$; in this case, it's clear that any morphism $\mathcal{F}(\mathcal{G}^{\text{ét}}) \to \mathcal{F}(\mathcal{H}^{\text{ét}})$ lifts.

Any morphism $\mathcal{F}(\mathcal{G}^0) \to \mathcal{F}(\mathcal{H}^0)$ lifts by the preceding Proposition; therefore the result follows. □

2.9 The Dieudonné anti-equivalence

In this section we prove the anti-equivalence Theorem 2.9.8, which establishes an anti-equivalence of categories between $DG^*_{k,\mathcal{O}}$ and the category of modules of finite length over a certain ring.

Remark 2.9.1. Since $V = 0$ on $\mathcal{F}(\mathcal{G})$ for all $\mathcal{G} \in DG^*_{k,\mathcal{O}}$ by Theorem 2.5.1, the Dieudonné module associated to $\mathcal{F}(\mathcal{G})$ by (2.3.1) is $M(\mathcal{F}(\mathcal{G})) = \operatorname{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$, as $\mathbb{G}_a = \operatorname{Ker} V : W_n \to W_n$ for all n.

We use this observation throughout this final section.

We now define our Dieudonné ring, which will be the analogue of the usual Dieudonné ring $\mathbf{D}_k$.

Definition 2.9.2. Let $\mathscr{D}_k$ be the non-commutative ring of $k[[\pi]]$ together with operations F_π and V_π satisfying the following relations:

$$\begin{aligned} V_\pi \circ F_\pi &= F_\pi \circ V_\pi = \pi \\ F_\pi \alpha &= \alpha^q V_\pi \text{ for } \alpha \in k \\ V_\pi \alpha^q &= \alpha V_\pi \text{ for } \alpha \in k \end{aligned}$$

Let $(\mathrm{DMod})_k$ be the category of $\mathscr{D}_k$-modules of finite length.

Remark 2.9.3. On $P \in (\mathrm{DMod})_k$ multiplication by $\alpha \in \mathbb{F}_q$ (sending $m \in P$ to αm) is a $k[[\pi]][F_\pi, V_\pi]$-linear morphism (hence a morphism in $(\mathrm{DMod})_k$).

This is analogous to multiplication by $\alpha \in \mathbb{F}_p$ being an endomorphism of classical Dieudonné modules, although multiplication by arbitrary $\alpha \in k$ is not a F-linear endomorphism of classical Dieudonné modules, because $\alpha^p \neq \alpha$ in general.

Let $\mathcal{G} \in DG^*_{k,\mathcal{O}}$. $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ (in the category of group schemes) is a k-module in the sense of classical Dieudonné theory via the action of k on $\mathbb{G}_a$ given by scalar multiplication.

There's also a composition

$$\mathbb{F}_q \subset \mathcal{O} \to \operatorname{End} \mathcal{G}$$

by definition of $\mathcal{G} \in DG^*_{k,\mathcal{O}}$, which restricts to a map $\mathbb{F}_q \to \operatorname{End} \mathcal{F}(\mathcal{G})$; this map induces a homomorphism of rings

$$\mathbb{F}_q \to \operatorname{End}_k \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$$

by composition, which we will denote by $\alpha \mapsto \alpha^* \in \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ for $\alpha \in \mathbb{F}_q$. Therefore we may apply Lemma 2.6.4 to get a decomposition of k-modules

$$\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a) \cong \bigoplus_i \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$$

such that, on $v \in \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$, $\alpha^* v = \chi_i(\alpha) v = \alpha^{p^i} v$, where $\chi_i : \mathbb{F}_q \to k$ is the function defined in §2.6.

Lemma 2.9.4. *Let $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$, and $\overline{f} \in \mathrm{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$. Then the induced morphism of Dieudonné modules $M(\mathcal{F}(\overline{f})) : \mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a) \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ induces a morphism $\mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$.*

Proof. Let $\phi \in \mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_0} \subset \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a) = M(\mathcal{F}(\mathcal{G}))$. We need to prove that $\alpha^*(\phi \circ \mathcal{F}(\overline{f})) = \alpha(\phi \circ \mathcal{F}(\overline{f}))$ for all $\alpha \in \mathbb{F}_q$. But $\alpha^*(\phi \circ \mathcal{F}(\overline{f})) = \phi \circ \mathcal{F}(\overline{f}) \circ \mathcal{F}(\alpha^*)$ by definition, $\phi \circ \mathcal{F}(\overline{f}) \circ \mathcal{F}(\alpha^*) = \phi \circ \mathcal{F}(\alpha^*) \circ \mathcal{F}(\overline{f})$ since $\overline{f} \in \mathrm{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$, and $\alpha\phi \circ \mathcal{F}(\alpha^*) = \phi \circ \mathcal{F}(\alpha^*)$ as $\phi \in \mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_0}$, so the result follows. □

Corollary 2.9.5. *Let $\mathcal{G} = (G, G^\flat, i) \in DG^*_{k,\mathcal{O}}$. Then there is a homomorphism of rings*

$$\mathscr{D}_k \to \mathrm{End}\,\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}.$$

Therefore $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \in (\mathrm{DMod})_k$.

We deduce that the map

$$\mathcal{G} \rightsquigarrow \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$$

is a functor from $DG^*_{k,\mathcal{O}}$ to $(\mathrm{DMod})_k$, *which we will denote by $M'(\mathcal{G})$.*

Proof. By definition of $\mathcal{G}$, there is a homomorphism of rings $\mathcal{O} = \mathbb{F}_q[[\pi]] \to \mathrm{End}\,\mathcal{G}$; by the preceding lemma, this induces a homomorphism of rings

$$\mathcal{O} \to \mathrm{End}\,\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}.$$

It suffices to prove that this homomorphism extends to $\mathscr{D}_k$. Clearly $\overline{F}_\pi$ and $\overline{V}_\pi$ act on $\mathcal{G}$ as endomorphisms. By definition, the action of $\mathbb{F}_q$ on $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$ via its action on $\mathcal{F}(\mathcal{G})$ extends to an action of k on $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$ via its action on $\mathbb{G}_a$; F_π and V_π are σ^r-linear and σ^{-r}-linear respectively, where σ is pth power Frobenius, by definition of F_π and V_π.

Therefore $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \in (\mathrm{DMod})_k$.

By the preceding lemma, any morphism $\overline{f} : \mathcal{G} \to \mathcal{H}$ induces a morphism of k-modules $M'(\mathcal{H}) \to M'(\mathcal{G})$; since any morphism $\mathcal{G} \to \mathcal{H}$ is compatible with $\mathcal{O} = k[[\pi]]$ by definition, and $\overline{V}_\pi$ and $\overline{F}_\pi$ are functors in $DG^*_{k,\mathcal{O}}$, they also commute with $\overline{f}$, and we see by construction of $M'(\overline{f})$ that it is $\mathscr{D}_k$-linear. Hence M' is a functor. □

Lemma 2.9.6. *Let* $\mathcal{G} \in DG^*_{k,\mathcal{O}}$. *Then* $\mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ *is generated as a* $\mathbf{D}_k$*-module by its* k*-submodule* $\mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$. *Further,* $F^i : \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ *is an isomorphism of* k*-modules for all* $i < r$.

Proof. If $\mathcal{F}(\mathcal{G})$ is étale, this is obvious: the restriction of $F^i : \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ is an isomorphism for all i, as F is an isomorphism of étale Dieudonné modules.

If $G = \mathcal{F}(\mathcal{G})$ is connected, $G \cong \mathrm{Spec}\, k[X_1, \ldots, X_n]/(X_1^{q^{a_1}}, \ldots, X_n^{q^{a_n}})$, with comultiplication $\Delta^*(X_i) = X_i \otimes 1 + 1 \otimes X_i$, and $\alpha^*(X_i) = \alpha X_i$ for all i, by Theorem 2.7.2.

$f_j(T) = X_j$ for all j define a series of group scheme homomorphisms such that $\alpha^* f_j^* = \alpha f_j^*$; therefore they're in $\mathrm{Hom}_k(G, \mathbb{G}_a)_{\chi_0}$. By Corollary 2.3.7, any $f \in \mathrm{Hom}_k(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ is simply a linear combination of powers of F acting on each f_j; therefore $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$ generates $\mathrm{Hom}(G, \mathbb{G}_a)$ as a $\mathbf{D}_k$-module. Hence each $F^i : \mathrm{Hom}(G, \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}(G, \mathbb{G}_a)_{\chi_i}$ is surjective.

The fact that $F^i : \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ is injective for $i < r$ and $\mathcal{G}$ connected follows since any $f \in \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$ is given by a homomorphism sending the parameter of $\mathbb{G}_a$ to a sum of p^xth powers of X_i,

$$\sum_{j,l} a_{j,l} X_j^{p^l}$$

for some $a_{j,l} \in k$. Since, by definition, $\mathbb{F}_q$ acts 'by scalars' on any homomorphism in $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}$, each p^j is congruent to $1 \mod q-1$; by Lemma 2.7.1, each power p^j is actually a power of q:

$$\sum_{i,j} b_{j,l} X_i^{q^j}$$

for different coefficients $b_{j,l}$, such that $l < a_j$. Since the ideal defining our algebra is $(X_1^{q^{a_1}}, \ldots, X_n^{q^{a_n}})$, and $(X_j^{q^l})^{p^i} \notin (X_j^{q^{a_j}})$ for $i < r$ where $q = p^r$, F^i does not send any such homomorphism to zero; therefore $F^i : \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ is injective.

Since it is also surjective, it follows that it is an isomorphism for all $i < r$.

Since $\mathcal{G} \cong \mathcal{G}^{\text{ét}} \times \mathcal{G}^0$ by Lemma 1.8.7, the result follows. □

Corollary 2.9.7. *Let $\mathcal{G}, \mathcal{H} \in DG^*_{k,\mathcal{O}}$. Then any $f' \in \mathrm{Hom}_{\mathscr{D}_k}(M'(\mathcal{H}), M'(\mathcal{G}))$ lifts to a unique morphism $f \in \mathrm{Hom}_{\mathbf{D}_k}(M(\mathcal{F}(\mathcal{H})), M(\mathcal{F}(\mathcal{G})))$, in the sense that the following diagram is commutative*

$$\begin{array}{ccc} M'(\mathcal{H}) & \xrightarrow{f'} & M'(\mathcal{G}) \\ \downarrow & & \downarrow \\ M(\mathcal{F}(\mathcal{H})) & \xrightarrow{f} & M(\mathcal{F}(\mathcal{G})) \end{array}$$

where the vertical arrows are the obvious inclusions of k-modules.

Proof. f is clearly unique if it exists at all, since by the lemma, $M(\mathcal{F}(\mathcal{H}))$ is determined as a $\mathbf{D}_k$-module by $M'(\mathcal{H})$; since any f must be $\mathbf{D}_k$-linear, this determines it completely.

We now prove existence of f. $F^i : \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0} \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ is an isomorphism of k-modules by the lemma; therefore it is invertible as a map of k-modules, and we can define $f(x_i) = (F^i \circ f' \circ F^{-i})(x_i)$ for all $x_i \in \mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_i}$ and $i < r$ where $p^r = q$; clearly the morphism defined in this way is F and V-linear, and therefore it is a map of $\mathbf{D}_k$-modules, as required. □

Theorem 2.9.8. *Let M' be the functor given by*

$$\mathcal{G} \rightsquigarrow M'(\mathcal{G}) = \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_0}.$$

Then M' is an anti-equivalence of categories.

Proof. By Freyd's Theorem ([GM99, §2, Theorem 1.13]), it's enough to prove that M' is

1. fully faithful, and

2. surjective.

First, we prove M' is fully faithful. Consider the map

$$M' : \mathrm{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H}) \to \mathrm{Hom}_{\mathscr{D}_k}(M'(\mathcal{H}), M'(\mathcal{G})).$$

Suppose that $\overline{f} : \mathcal{G} \to \mathcal{H}$ maps to zero in $\mathrm{Hom}_{\mathscr{D}_k}(M'(\mathcal{H}), M'(\mathcal{G}))$. By Corollary 2.9.7, this trivial morphism lifts to a unique morphism $M(\mathcal{F}(\mathcal{H})) \to M(\mathcal{F}(\mathcal{G}))$ which must be the trivial one; by construction of M'; applying the classical anti-equivalence of Theorem 2.3.1, this corresponds to the trivial morphism $\mathcal{F}(\overline{f}) : \mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$. Hence by construction of M', $\overline{f}$ induces the trivial morphism $\mathcal{F}(\overline{f}) : \mathcal{G} \to \mathcal{H}$. But such morphisms are themselves trivial by construction of morphisms in our category $DG^*_{k,\mathcal{O}}$; therefore $\overline{f}$ is the trivial morphism. Hence M' is injective on morphisms.

To see that M' is also surjective on morphisms, let $f' \in \mathrm{Hom}_{\mathcal{D}_k}(M'(\mathcal{H}), M'(\mathcal{G}))$. f' lifts to a unique morphism $f : M(\mathcal{F}(\mathcal{H})) \to M(\mathcal{F}(\mathcal{G}))$ by Corollary 2.9.7; by the Dieudonné anti-equivalence, this morphism of $\mathbf{D}_k$-modules comes from a morphism of k-group schemes $\mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$.

By the explicit construction of the morphism f given in Corollary 2.9.7, $f : \mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_i} \to \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ is equal to $F^i \circ f' \circ F^{-i}$.

Similarly, the endomorphisms V_π of $M'(\mathcal{H})$ and $M'(\mathcal{G})$ lift by Corollary 2.9.7 to endomorphisms $F^i \circ V_\pi \circ F^{-i}$ of $\mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ and $\mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_i}$. V_π commutes with f' as f' is $\mathcal{D}_k$-linear, and therefore $(F^i \circ V_\pi \circ F^{-i})$ and $(F^i \circ f' \circ F^{-i})$ commute for each i.

By construction, the endomorphism of $M(\mathcal{F}(\mathcal{G})) = \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)$ induced by the action of V_π on $M'(\mathcal{G})$ is that obtained by composing homomorphisms $\mathcal{F}(\mathcal{G}) \to \mathbb{G}_a$ with $\mathcal{F}(\overline{V}_\pi) : \mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{G})$, and therefore is equal to $M(\mathcal{F}(V_\pi))$, and similarly for $\mathcal{H}$. Therefore the following diagram commutes:

$$\begin{array}{ccc} M(\mathcal{F}(\mathcal{G})) & \xrightarrow[M'(f)]{} & M(\mathcal{F}(\mathcal{H})) \\ \Big\downarrow{\scriptstyle M(V_\pi)} & & \Big\downarrow{\scriptstyle M(V_\pi)} \\ M(\mathcal{F}(\mathcal{G})^{(q^{-1})}) & \xrightarrow[M(f^{(q^{-1})})]{} & M(\mathcal{F}(\mathcal{H})^{(q^{-1})}). \end{array}$$

Since M' is an anti-equivalence of categories by Theorem 2.3.1, it follows that the following diagram also commutes:

$$\begin{array}{ccc} \mathcal{F}(\mathcal{G}) & \xrightarrow[f]{} & \mathcal{F}(\mathcal{H}) \\ \Big\downarrow{\scriptstyle V_\pi} & & \Big\downarrow{\scriptstyle V_\pi} \\ \mathcal{F}(\mathcal{G})^{(q^{-1})} & \xrightarrow[f^{(q^{-1})}]{} & \mathcal{F}(\mathcal{H})^{(q^{-1})}. \end{array}$$

Therefore our morphism $\mathcal{F}(\mathcal{G}) \to \mathcal{F}(\mathcal{H})$ is V_π-linear.

Since $f(\mathrm{Hom}(\mathcal{F}(\mathcal{H}), \mathbb{G}_a)_{\chi_i}) \subset \mathrm{Hom}(\mathcal{F}(\mathcal{G}), \mathbb{G}_a)_{\chi_i}$ by construction of f, f commutes with the induced action of $\mathcal{F}(\alpha^*)$, for all $\alpha \in \mathbb{F}_q$: α^* acts on both k-modules as multiplication by the scalar α^{p^i}, by definition. This action of α^* on $M(\mathcal{F}(\mathcal{G}))$ and $M(\mathcal{F}(\mathcal{H}))$ is the action induced by $\mathcal{F}(\alpha^*)$ on $\mathcal{F}(\mathcal{G})$ and $\mathcal{F}(\mathcal{H})$ respectively, by Corollary 2.9.7; therefore our morphism $\mathcal{F}(\mathcal{G}) \longrightarrow \mathcal{F}(\mathcal{H})$ is also $\mathcal{F}(\alpha^*)$-linear. Since any morphism of k-group schemes is F-linear by definition (and hence F_π-linear), we can apply Corollary 2.8.5, which says that it lifts to a morphism $\overline{f} \in \operatorname{Hom}_{DG^*_{k,\mathcal{O}}}(\mathcal{G}, \mathcal{H})$.

By construction, $M(\mathcal{F}(\overline{f})) = f$, and by definition, $M'(\overline{f})$ is the restriction of f to $M'(\mathcal{F}(\mathcal{H}))$, which is f'; therefore $\overline{f}$ maps to f', and our functor M' is surjective on morphisms, hence fully faithful.

Finally, we have to prove surjectivity of M' on objects: that to every module $W' \in (\mathrm{DMod})_k$, we can construct some $\mathcal{G} \in DG^*_{k,\mathcal{O}}$ such that $M'(\mathcal{G}) = W'$.

The first step is to define a $\mathbf{D}_k$-module P via

$$W = \bigoplus_{0 \leq i < r} W_i,$$

(as k-modules) where $W_i = W'$ for all i, and we define $F : W_i \longrightarrow W_{i+1}$ to be the identity morphism for $i < r - 1$, and $F : W_{r-1} \longrightarrow W_0$ by $F(w) = F_\pi w$ for all $w \in W_{r-1}$.

We define $V = 0$ on all W_i. The action of α^* (for $\alpha \in \mathbb{F}_q$) on W' lifts uniquely to a $\mathbf{D}_k$-linear endomorphism of W by Corollary 2.9.7; similarly V_π on W' lifts to a $\mathbf{D}_k$-linear endomorphism of W.

By Theorem 2.3.1, our $\mathbf{D}_k$-module W is equal to $M(G)$, for some $G \in \mathrm{Gr}_k$, equipped with endomorphisms induced by $\mathbb{F}_q$ and V_π.

We must prove that there is some $\mathcal{G} \in DG^*_{k,\mathcal{O}}$ such that $\mathcal{F}(\mathcal{G}) = G$.

Since we have the decomposition $G \cong G^{\text{ét}} \times G^0$ by Proposition 2.3.5 of G into a product of étale and connected subgroup schemes, it suffices to prove

1. that there is some $\mathcal{G}^{\text{ét}} \in DG^*_{k,\mathcal{O}}$ such that $\mathcal{F}(\mathcal{G}^{\text{ét}}) = G$, and

2. that there is some $\mathcal{G}^0 \in DG^*_{k,\mathcal{O}}$ such that $\mathcal{F}(\mathcal{G}^0) = G^c$.

For $G^{\text{ét}}$, this is obvious: we can take the triple $\mathcal{G}^{\text{ét}} = (G^{\text{ét}}, \operatorname{Spec} k, i) \in DG_k$, together with the endomorphisms induced by $\mathbb{F}_q$ and V_π: $[p] = 0$ on $G^{\text{ét}}$ since $V = 0$ on its Dieudonné module. This gives a homomorphism of rings $\mathcal{O} \longrightarrow \operatorname{End} \mathcal{G}^{\text{ét}}$, and since $t_{\mathcal{G}^{\text{ét}}} = 0$ and $N_{\mathcal{G}^{\text{ét}}} = 0$, this suffices to define an object $\mathcal{G}^{\text{ét}} \in DG^*_{k,\mathcal{O}}$ with the required properties.

For G^0, we can consider its Dieudonné module W. Applying Proposition 2.3.5, it has generators $m_1, \ldots, m_l$, satisfying relations $Vm_i = 0$ and $F^{a_i}m_i = 0$, for some integers a_i. Since it's generated as a $\mathbf{D}_k$-module by its k-submodule W_0, we can assume that $m_i \in W_0$ for all m_i. By construction, $F^r = F_\pi$ on W, and all relations $F^{a_i}m_i = 0$ factor through F^r, since $F^i \mid_{W_0}$ has no kernel for $i < r$, by construction of W. Therefore each a_i divides r.

By Corollary 2.3.6, the algebra of G^0 has a presentation

$$A = k[X_1, \ldots, X_n]/(X_1^{q^{b_i}}, \ldots, X_n^{q^{b_n}}), \tag{2.9.1}$$

with $\Delta^* X_i = X_i \otimes 1 + 1 \otimes X_i$, where $b_i = a_i/r$ for all i.

$\mathbb{F}_q$ acts 'by scalars' on each $m_i \in W_0$; since each m_i can be identified with the homomorphism $G^0 \longrightarrow \mathbb{G}_a$ sending the parameter of $\mathbb{G}_a$ to X_i by the Dieudonné anti-equivalence, the induced action of $\mathbb{F}_q$ on X_i is also by scalar multiplication.

If we let $A^\flat = k[X_1, \ldots, X_n]/(X_1^{q^{b_i}}, \ldots, X_n^{q^{b_n}})(X_1, \ldots, X_n)$, we get a triple $\mathcal{G}^0 = (\operatorname{Spec} A, \operatorname{Spec} A^\flat, i) \in DS_k$, which lifts to a triple in DG_k by Proposition 1.5.7. We can define $\alpha^* X_i = X_i$ for all $\alpha \in \mathbb{F}_q$, and $V_\pi^\flat$ to be any lifting of V_π; if we define $\pi^* = F_\pi \circ V_\pi$, this defines π^* uniquely, since $F_\pi(N_{\mathcal{G}^0}) = 0$. Therefore we have an endomorphism of rings $\mathcal{O} \longrightarrow \operatorname{End}_{DG_k} \mathcal{G}^0$, and since $\mathcal{O}$ clearly acts 'by scalars' on $t_{\mathcal{G}^0}$ and $N_{\mathcal{G}^0}$, we have defined an object $\mathcal{G}^0 \in DG^*_{k,\mathcal{O}}$, which by construction satisfies $M(\mathcal{F}(\mathcal{G})) = W$, and $M'(\mathcal{G}) = W_0$. Hence M' is surjective on objects.

Therefore M is an anti-equivalence of categories. $\square$

Appendix A

Basic and Auxiliary Results

In this section R is a commutative noetherian ring. The following result is adapted from exercises in [Wei94].

Lemma A.1. *Any finitely generated flat R-module, M, is locally free.*

Proof. Let P be a prime ideal of R. It's easy to see that $M_P = M \otimes_R R_P$ is a flat R_P-module. Pick a minimal set $m_1, \ldots, m_n$ of generators of M_P, and define a map of R_P-modules ${R_P}^{\otimes n} \xrightarrow{f} M$ by sending the ith generator of ${R_P}^{\otimes n}$ to m_i. We have an exact sequence

$$0 \to K \to {R_P}^{\otimes n} \xrightarrow{f} M_P \to 0.$$

$K = \operatorname{Ker} f$ is finitely generated since R is noetherian. Tensoring with R_P/P_P gives a long exact sequence

$$\operatorname{Tor}_1^{R_P}(M_P, R_P/P_P) \to K \otimes R_P/P_P \to (R_P/P_P)^{\otimes n} \xrightarrow{\overline{f}} M_P \otimes R_P/P_P \to 0$$

of R_P/P_P-modules. By Nakayama's Lemma, the images of $m_1, \ldots, m_n$ in $M_P \otimes R_P/P_P \cong M_P/P_P$ are a set of minimal generators of M_P/P_P, and since R_P/P_P is a field, $\overline{f}$ is an isomorphism. $\operatorname{Tor}_1^{R_P}(M_P/R_P/P_P) = 0$ since M_P is a flat R_P-module, and therefore $K \otimes R_P/P_P \cong K/P_PK$ is zero. Hence by Nakayama's Lemma, $K = 0$, and therefore ${R_P}^{\otimes n} \cong M_P$, so M_P is free. $\square$

Lemma A.2. *Suppose that $R = \mathfrak{m}_0 \supset \mathfrak{m}_1 \ldots$ and $R = \mathfrak{n}_0 \supset \mathfrak{n}_1 \ldots$ are filtrations of R by ideals, such that*

1. *for each* $\mathfrak{n}_j$ *there is an* $\mathfrak{m}_i$ *such that* $\mathfrak{m}_i \subset \mathfrak{n}_j$, *and*

2. *for each* $\mathfrak{m}_j$ *there is an* $\mathfrak{n}_i$ *such that* $\mathfrak{n}_i \subset \mathfrak{m}_j$,

then there is a natural isomorphism $\hat{R}_{\mathfrak{m}} \cong \hat{R}_{\mathfrak{n}}$.

Proof. This is the content of [Eis95, Lemma 7.14]. □

Lemma A.3. *Let* M *be an* R*-module possessing a finite-length composition series of length* n*:*

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = \{0\},$$

so that each quotient M_i/M_{i+1} *is non-zero and simple. Then any surjection* $f : M \twoheadrightarrow M$ *is an isomorphism.*

Proof. Suppose otherwise. Then let K be the (non-trivial) kernel of our surjection, and consider the series

$$M/K = M_0/(M_0 \cap K) \supset M_1/(M_1 \cap K) \supset \cdots \supset M_n/(M_n \cap K) = \{0\}$$

in which each successive subquotient is simple.

Since $M_n \cap K = \{0\}$, and $M \cap K = K \ncong \{0\}$, there is some i such that $M_i \cap K = \{0\}$, but $M_{i-1} \cap K \ncong \{0\}$. Since $(M_{i-1} \cap K)/(M_i \cap K)$ is non-trivial, and also a submodule of the simple module M_{i-1}/M_i via the inclusion $M_{i-1} \cap K \subset M_{i-1}$, we have an isomorphism $(M_{i-1} \cap K)/M_i \cap K \cong M_{i-1}/M_i$.

Hence $(M_{i-1}/(M_{i-1} \cap K))/(M_i/(M_i \cap K)) \cong \{0\}$. Hence we can get a composition series for M/K of length $m < n$, by removing identical terms from the above sequence.

Since the map $f' : M/K \to M$ induced by f is an isomorphism, our composition series for M/K of length m maps to a composition series for M of length $m < n$ under f'.

But by a standard result [Eis95, Theorem 2.13], every composition series of M is of length n; therefore we have a contradiction.

It follows that $K = \{0\}$, hence f is injective, hence an isomorphism.

□

Bibliography

[Abr04] V. Abrashkin. Galois modules arising from Faltings' strict modules, 2004. 22 pages, http://arXiv.org/pdf/math.NT/0403542math.NT/0403542.

[DG70] M. Demazure and P. Gabriel. *Groupes Algébriques.* Masson & Cie, 1970.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in Graduate Texts in Mathematics. Springer, 1995.

[Fal02] G. Faltings. Group schemes with strict $\mathcal{O}$-action. *Moscow Mathematical Journal*, 2(2):249–279, 2002.

[FH91] W. Fulton and J. Harris. *Representation theory: a first course.* Number 129 in Graduate Texts in Mathematics. Springer, 1991.

[Fon77] J-M. Fontaine. *Groupes p-divisibles sur les corps locaux.* Société mathématique de France, 1977.

[GM99] S. Gelfand and Y. Manin. *Homological Algebra.* Springer, 1999.

[ML71] S. Mac Lane. *Categories for the working mathematician.* Number 5 in Graduate Texts in Mathematics. Springer, 1971.

[OT70] F. Oort and J. Tate. Group schemes of prime order. *Annales Scientifiques de l'École Normale Supérieure*, 4(3):1–21, 1970.

[Ser62] J-P. Serre. *Corps locaux.* Hermann, 1962.

[Tat97] J. Tate. Finite flat group schemes. In G. Cornell, J. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 121–154, University of Boston, 1997. Springer.

[Wat79] W. Waterhouse. *Introduction to Affine Group Schemes.* Number 66 in Graduate Texts in Mathematics. Springer, 1979.

[Wei94] C. Weibel. *An introduction to homological algebra.* Number 38 in Cambridge studies in advanced mathematics. Cambridge University Press, 1994.