The Report Committee for James Hunter Jones

certifies that this is the approved version of the following report:

Two Theorems Related to Group Schemes

APPROVED BY

SUPERVISING COMMITTEE:

Supervisor: ______________________________
Jose Felipe Voloch

____
David Helm

Two Theorems Related to Group Schemes

by

James Hunter Jones, B.A.

REPORT

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF ARTS

THE UNIVERSITY OF TEXAS AT AUSTIN

December 2010

Two Theorems Related to Group Schemes

by

James Hunter Jones, M.A.
The University of Texas at Austin, 2010
SUPERVISOR: Jose Felipe Voloch

After presenting some preliminary information, this paper presents two proofs regarding group schemes. The first relates the category of affine group schemes to the category of commutative Hopf algebras. The second shows that a commutative group scheme of finite order is in fact killed by its order.

Contents

Introduction

In this paper, we endeavor to present two proofs regarding group schemes. The first relates a certain category of algebras to a category of affine group schemes. The second tells us that a group scheme of finite order which is commutative is in fact killed by its order. In order to present these proofs in a cogent manner, we will first clearly define the category of algebras with which the first proof is concerned. Second, we will give some background information about sheaves and schemes necessary for both proofs or at least refer the reader to the appropriate literature to find the information. Finally, in the third section, we present the proof related to the category of algebras, and, in the fourth section, we present Pierre Deligne's proof regarding commutative group schemes as given by Frans Oort and John Tate.

To begin we make note of some assumptions that will hold throughout this paper. All rings are commutative rings with unity. All modules are assumed to be unitary bimodules, though not all constructions necessarily require it. With these out of the way, we define the category of algebras we are concerned with

Hopf Algebras

In order to define a Hopf Algebra we first review certain definitions from commutative algebra, namely those of an algebra, a coalgebra, and a bialgebra.

Definition 1.1. Let S be a ring and let A be an S-module. We say that A is an S-*algebra* if there are S-module homomorphisms $\triangledown : A \otimes_S A \longrightarrow A$ and $\eta : S \longrightarrow A$ such that the following commutative diagrams are satisfied:

$$\begin{array}{ccc} A \otimes_S A \otimes_S A & \xrightarrow{\triangledown\otimes\mathrm{id}} & A \otimes_S A \\ {\scriptstyle \mathrm{id}\otimes\triangledown}\downarrow & & \downarrow{\scriptstyle \triangledown} \\ A \otimes_S A & \xrightarrow[\triangledown]{} & A \end{array} \qquad \begin{array}{ccccc} S \otimes_S A & \xrightarrow{\eta\otimes\mathrm{id}} & A \otimes_S A & \xleftarrow{\mathrm{id}\otimes\eta} & A \otimes_S S \\ {\scriptstyle \cong}\uparrow & & \downarrow{\scriptstyle \triangledown} & & \uparrow{\scriptstyle \cong} \\ A & \xrightarrow[\mathrm{id}]{} & A & \xleftarrow[\mathrm{id}]{} & A \end{array}$$

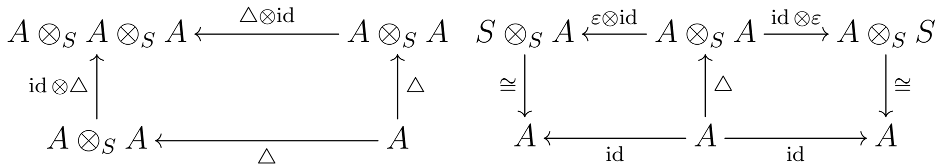
(associativity) (unit)

The map $\triangledown$ is called *multiplication*, and the map η is called the *unit* map.

Sometimes for the sake of clarity we will denote the multiplication and unit maps of the S-algebra A by $\triangledown_A$ and η_A respectively. We say that the multiplication map is *commutative* if, given the S-linear map $\sigma : A \otimes_S A \longrightarrow A \otimes_S A$ defined by $\sigma(a_1 \otimes a_2) = a_2 \otimes a_1$, we have $\triangledown \circ \sigma = \triangledown$. Note that S has a canonical structure as an S-algebra by letting $\triangledown_S : S \otimes_S S \longrightarrow S$ be defined by $\triangledown_S(s_1 \otimes s_2) = s_1 s_2$ and letting $\eta_S = \mathrm{id}_S$. Furthermore, given S-algebras A and B, we can define a new algebra $A \otimes_S B$ by letting the multiplication map be the S-linear map defined by $\triangledown_{A\otimes_S B}((a_1 \otimes b_1) \otimes (a_2 \otimes b_2)) = \triangledown_A(a_1 \otimes a_2) \otimes \triangledown_B(b_1 \otimes b_2)$ and letting the unit map be given by $\eta_{A\otimes_S B} = (\eta_A \otimes \eta_B) \circ \varphi$, where $\varphi : S \longrightarrow S \otimes_S S$ is the canonical isomorphism given by $\varphi(s) = s \otimes 1$. It's a well-known algebraic fact that the construction of an S-algebra given above is the same as giving a ring homomorphism $S \longrightarrow A$. This homomorphism gives the unit map, and the multiplication map, which is by definition commutative, is given in the obvious way by $\triangledown_A(a_1 \otimes a_2) = a_1 a_2$. As such, we will use these two definitions interchangeably. Finally, given S-algebras A and B, we define an

S*-algebra homomorphism* to be an S-module homomorphism $\phi : A \longrightarrow B$ such that $\bigtriangledown_B \circ (\phi \otimes \phi) = \phi \circ \bigtriangledown_A$ and $\phi \circ \eta_A = \eta_B$. Now we move to the definition of a coalgebra, which is a dual concept to that of an algebra.

Definition 1.2. Let S be a ring. Let A be an S-module. We say that A is a *coalgebra* if there are maps $\triangle : A \longrightarrow A \otimes_S A$ and $\varepsilon : A \longrightarrow S$ such that the following diagrams commute:

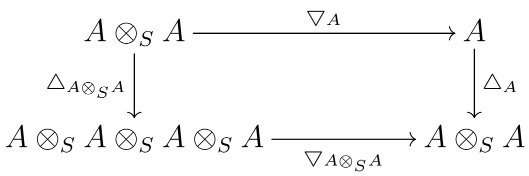


(co-associativity) (co-unit)

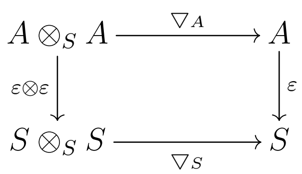
The map $\triangle$ is called *co-multiplication*, and the map ε is called the *co-unit* map.

Again, for the sake of clarity, we will often denote the co-multiplication and co-unit maps of the S-coalgebra A by $\triangle_A$ and ε_A. We say that the co-multiplication is *co-commutative* if $\sigma \circ \triangle = \triangle$, where σ is defined as above. Once again, S has a canonical S-coalgebra structure given by $\triangle_S = \varphi$, where φ is defined as above, and $\varepsilon_S = \mathrm{id}_S$ (note that in fact $\triangle_S$ and $\bigtriangledown_S$ are inverses of each other. This will be used in the future). Now, given coalgebras A and B, we can define the coalgebra $A \otimes_S B$ by letting $\triangle_{A \otimes_S B}$ be the map defined by $\triangle_{A \otimes_S B}(a \otimes b) = f(\triangle_A(a) \otimes \triangle_B(b))$, where $f : A \otimes_S A \otimes_S B \otimes_S B \longrightarrow A \otimes_S B \otimes_S A \otimes_S B$ is defined by $f(a_1 \otimes a_2 \otimes b_1 \otimes b_2) = a_1 \otimes b_1 \otimes a_2 \otimes b_2$, and letting $\varepsilon_{A \otimes_S B} = \bigtriangledown_S \circ (\varepsilon_A \otimes \varepsilon_B)$. Finally, given an S-coalgebra A and B, we define an *S-coalgebra homomorphism* to be an S-module homomorphism $\phi : A \longrightarrow B$ such that $(\phi \otimes \phi) \circ \triangle_A = \triangle_B \circ \phi$ and $\varepsilon_B \circ \phi = \varepsilon_A$. Next we move on to the definition of a bialgebra.

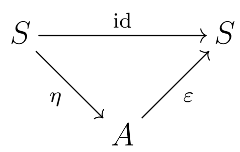
Definition 1.3. Suppose A is both an S-algebra and an S-coalgebra with multiplication, unit, co-multiplication, and co-unit $\bigtriangledown$, η, $\triangle$, and ε respectively. Then we say A is a *bialgebra* if the following diagrams commute:



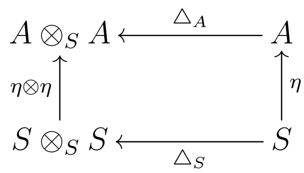
(i)



(ii)



(iii)

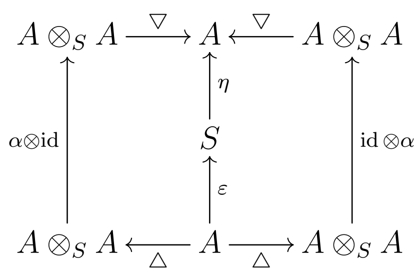


(iv)

Note that, taken together, (i) and (iv) are the same as saying that $\triangle_A$ is an S-algebra homomorphism, (i) and (ii) are the same as saying that $\bigtriangledown_A$ is an S-coalgebra homomorphism, (ii) and (iii) are the same as saying that ε is an S-algebra homomorphism, and (iii) and (iv) are the same as saying that η is an S-coalgebra homomorphism.

We say an S-bialgebra is (co-)commutative if it is (co-)commutative as an S-(co)algebra. Now it's clear that we have a canonical S-bialgebra structure on S by taking exactly the same multiplication, unit, co-multiplication, and co-unit maps we used to define the canonical algebra and coalgebra structures above. Further, an S-bialgebra homomorphism is simply a linear map which is simultaneously an S-algebra and an S-coalgebra homomorphism. Finally, we give the definition of a Hopf algebra.

Definition 1.4. Suppose A is an S-bialgebra with multiplication, unit, co-multiplication, and co-unit given by $\bigtriangledown$, η, $\triangle$, and ε respectively. Then A is a *Hopf S-algebra* if there is an S-linear map $\alpha : A \longrightarrow A$ which satisfies the following diagram:



(antipode)

As indicated, α is called the *antipode* map.

A Hopf S-algebra A is called (co-)commutative if it is (co-)commutative as a bialgebra. S is trivially a Hopf S-algebra by taking the antipode to be the identity map. Finally, given A and B Hopf S-algebras, a *Hopf S-algebra homomorphism* is an S-bialgebra homomorphism $\phi : A \longrightarrow B$ such that $\alpha_B \circ \phi = \phi \circ \alpha_A$. As a matter of notation, we will refer to such a Hopf S-algebra as above by an ordered tuple $(A, \bigtriangledown, \eta, \bigtriangleup, \varepsilon, \alpha)$.

Sheaves and Schemes: Preliminaries

For the remainder of this paper, certain familiarity with concepts from the theory of schemes will be assumed. The information necessary is essentially II.1 - II.5 from [4] and I and VI.1 from [3]. In this section we will recall certain pertinent definitions from these sources for convenience.

Definition 2.1. Given a ringed space, $(X, \mathcal{O}_X)$ and sheaves of $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$ we, rather unsurprisingly, define $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$ to be the group of $\mathcal{O}_X$-module morphisms $\mathcal{F} \longrightarrow \mathcal{G}$. Furthermore, we define the *sheaf Hom*, $\mathscr{H}\!om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$, to be the presheaf (which is also a sheaf) given by

$$U \longmapsto \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{G}|_U).$$

Given $\mathcal{F}$ as above, we define a sheaf of $\mathcal{O}_X$-modules, the *$\mathcal{O}_X$-linear dual of $\mathcal{F}$*, as $\mathcal{F}' = \mathscr{H}\!om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{O}_X)$. Taking $\mathcal{F}$ and $\mathcal{G}$ as above, we define the *tensor product* to be the sheafification of the presheaf $U \longmapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$. Furthermore, we say that an $\mathcal{O}_X$ module $\mathcal{F}$ is *free* if it is isomorphic to $\bigoplus_{i=1}^{n} \mathcal{O}_X$, where the direct sum may be infinite. Similarly, $\mathcal{F}$ is *locally free* if there is a covering of X by open sets $\{U_i\}_{i \in I}$ so that $\mathcal{F}|_{U_i}$ is free over $\mathcal{O}_X|_{U_i}$, or, in other words, $\mathcal{F}|_{U_i} = \bigoplus_{j=1}^{n_i} \mathcal{O}_X|_{U_i}$. In this case, we say that n_i is the *rank* of $\mathcal{F}$ on U_i.

Finally, we say that $\mathcal{F}$ is *locally free of finite rank* $n \in \mathbb{Z}^+$ if $n_i = n$ for all $i \in I$.

Next let $(S, \mathcal{O}_S)$ be a scheme. We define an *$\mathcal{O}_S$-algebra* $\mathcal{A}$ as a sheaf of $\mathcal{O}_S$-modules such that, for each open $U \subseteq S$, $\mathcal{A}(U)$ is an $\mathcal{O}_S(U)$-algebra and such that, given $V \subseteq U$, the restriction homomorphism $\mathcal{A}(U) \longrightarrow \mathcal{A}(V)$ is compatible with the algebra structure via the map $\mathcal{O}_S(U) \longrightarrow \mathcal{O}_S(V)$. Now, for the purposes of this paper we follow [3], pp.40-41, and define a *quasi-coherent sheaf of $\mathcal{O}_S$-algebras* $\mathcal{A}$ as a sheaf of $\mathcal{O}_S$-algebras such that given an affine open $\mathrm{Spec}(R) = U \subset S$ and distinguished open $\mathrm{Spec}(R_f) = U_f \subset U$ the following is satisfied as an equality of $R = \mathcal{O}_S(U)$-algebras:

$$\mathcal{A}(U_f) = \mathcal{A}(U) \otimes_R \mathcal{O}_S(U_f) = \mathcal{A}(U) \otimes_R R_f$$

Remark 2.1. Another way to define such a sheaf is to simply say that it is an $\mathcal{O}_S$-algebra which is quasi-coherent as a sheaf of modules, where quasi-coherent is defined as in [4], p.111, but the current definition is sufficient.

Moreover, given $\mathcal{A}$ a (locally) free $\mathcal{O}_S$-algebra, we can define a map $N : \mathcal{A} \longrightarrow \mathcal{O}_S$ called the *norm*, by defining the map on stalks as the regular algebra norm map (i.e., $N_p : \mathcal{A}_p \longrightarrow (\mathcal{O}_S)_p$ is just the algebra norm map).

We then define, for the purposes of this paper, the *relative spectrum* of such a quasi-coherent sheaf of $\mathcal{O}_S$-algebras $\mathcal{A}$ as follows:

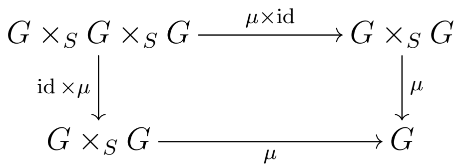
Definition 2.2. Given $\mathcal{A}$ as above, we define $\mathscr{Spec}(\mathcal{A})$ to be the unique S-scheme $\mathscr{Spec}(\mathcal{A}) \xrightarrow{f} S$ such that, given $\mathrm{Spec}(R) = U \subseteq S$, f induces an isomorphism $f^{-1}(U) \cong \mathrm{Spec}(\mathcal{A}(U))$, and such that, given $\mathrm{Spec}(R) = U \subseteq V = \mathrm{Spec}(S)$, the restriction map $\mathcal{A}(V) \longrightarrow \mathcal{A}(U)$ comes from the inclusion $f^{-1}(U) \hookrightarrow f^{-1}(V)$.

Remark 2.2. Of course, this is not really a complete definition as it has not been shown that such a thing exists. However, it does, and it can be constructed in multiple ways. For a construction by gluing see 19.3 and 19.4 of [1] or exercise II.5.17 of [4]. For an alternative construction see p.41 of [3].

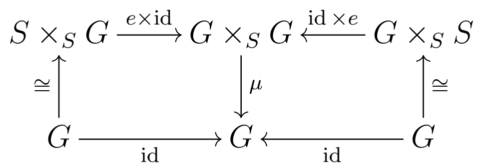
Now, the relative spectrum has many of the same properties as the spectrum of a ring. For example, given $\mathcal{A}$ and $\mathcal{B}$ quasi-coherent sheaves of $\mathcal{O}_S$-algebras, any morphism $\mathscr{Spec}(\mathcal{A}) \longrightarrow \mathscr{Spec}(\mathcal{B})$ comes from a morphism $\mathcal{B} \longrightarrow \mathcal{A}$. Furthermore, we have $\mathscr{Spec}(\mathcal{A}) \times_S \mathscr{Spec}(\mathcal{B}) \cong \mathscr{Spec}(\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{B})$. Finally, it is clear from the definition of a quasi-coherent sheaf of $\mathcal{O}_S$-algebras that $\mathcal{O}_S$ itself is one and that we also have $S \cong \mathscr{Spec}(\mathcal{O}_S)$.

At last, we define the structure that the theorems of this paper are concerned with. For these purposes we define the diagonal map $d : G \longrightarrow G \times_S G$ by $d(g) = g \times g$.

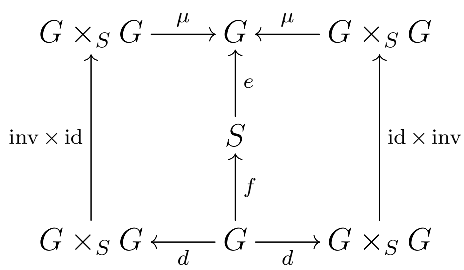
Definition 2.3. Given $G \xrightarrow{f} S$ an S-scheme, we say that G is an *S-group scheme* if we are given S-scheme morphisms $\mu : G \times_S G \longrightarrow G$, $e : S \longrightarrow G$, and $\mathrm{inv} : G \longrightarrow G$ so that the following diagrams commute:



(associativity)



(unit)



(inverse)

The map μ is called the *multiplication* map, e is called the *unit* map, and inv is called the *inverse* map. Furthermore, if $G = \mathrm{Spec}(R)$ and $S = \mathrm{Spec}(T)$ for some rings R and T, we say that G is an *affine group scheme*.

We note and will use liberally that, by Yoneda's Lemma, defining maps as above is the same as giving a factorization of the morphisms functor $\mathrm{Mor}_S(-, G) : \mathbf{Sch}_S^{\mathrm{op}} \longrightarrow \mathbf{Set}$ through the forgetful functor $\mathbf{Grp} \longrightarrow \mathbf{Set}$ (or, in short, giving a group structure on $G(X)$ for any S-scheme X) and vice versa. For a proof of this see pp.2-3 of [2]. Furthermore, we say that the multiplication μ is *commutative* if, given the map $\tau : G \times_S G \longrightarrow G \times_S G$ defined by $\tau(g_1 \times g_2) = g_2 \times g_1$, we have $\mu \circ \tau = \mu$. Equivalently, a group scheme is commutative if $G(X)$ is a commutative group for all S-schemes X.

It's clear that S has a canonical structure as an S-group scheme where μ_S is the isomorphism $\varphi : S \times_S S \longrightarrow S$, and e_S and inv_S are given by the identity map. Further, given S-group schemes G and H, there is a canonical group scheme structure on $G \times_S H$ where $\mu_{G\times_S H} : G \times_S H \times_S G \times_S H \longrightarrow G \times_S H$ is given by $\mu_{G\times_S H}(g_1 \times h_1 \times g_2 \times h_2) = \mu_G(g_1 \times g_2) \times \mu_H(h_1 \times h_2)$, the map $e_{G\times_S H} = (e_G \times e_H) \circ \varphi^{-1}$, and $\text{inv}_{G\times_S H} = \text{inv}_G \times \text{inv}_H$. Given G and H as above, we define an *S-group scheme homomorphism* to be a morphism of S-schemes $\phi : G \longrightarrow H$ such that $\phi \circ \mu_G = \mu_H \circ (\phi \times \phi)$, $\phi \circ e_G = e_H$, and $\phi \circ \text{inv}_G = \text{inv}_H \circ \phi$. Finally, we say that an S-group scheme G has *finite order* r if $G = \mathscr{S}\!pec(\mathcal{A})$ for some quasi-coherent sheaf of $\mathcal{O}_S$-algebras $\mathcal{A}$, and $\mathcal{A}$ is locally free of finite rank r. With these definitions out of the way, we can finally move on to the theorems we are primarily concerned with.

Hopf Algebras and Affine Group Schemes

Theorem 3.1. *The category of affine group schemes over* $\text{Spec}(S)$ *and the category of commutative Hopf S-algebras are antiequivalent via* Spec *and the taking of global sections.*

Proof. Given a commutative Hopf S-algebra $(R, \bigtriangledown, \eta, \bigtriangleup, \varepsilon, \alpha)$, we show that $\text{Spec}(R)$ is a group scheme over $\text{Spec}(S)$. First it's clear that R is a ring by letting $\bigtriangledown$ define the ring multiplication and $\eta(1_S)$ be the unit of the ring. Under this structure it's also clear that the module homomorphisms given are in fact ring homomorphisms and so define scheme morphisms. First, we see that the unit map $\eta : S \longrightarrow R$ gives the structure morphism $f : \text{Spec}(R) \longrightarrow \text{Spec}(S)$.

We take the map $d : G \longrightarrow \operatorname{Spec}(R) \times_{\operatorname{Spec}(S)} \operatorname{Spec}(R) \cong \operatorname{Spec}(R \otimes_S R)$ to be that given by the algebra multiplication $\bigtriangledown : R \otimes_S R \longrightarrow R$, and since this is how the ring multiplication is defined it corresponds to the diagonal morphism (see [4], p.96, Proposition 4.1). Furthermore, the maps $\triangle : R \longrightarrow R \otimes_S R$ and $\varepsilon : R \longrightarrow S$ give the group multiplication and group unit maps $\mu : \operatorname{Spec}(R) \times_{\operatorname{Spec}(S)} \operatorname{Spec}(R) \cong \operatorname{Spec}(R \otimes_S R) \longrightarrow \operatorname{Spec} S$ and $e : \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$. Finally, we get the group inverse map $\operatorname{inv} : \operatorname{Spec}(R) \longrightarrow \operatorname{Spec}(R)$ from the antipode map $\alpha : R \longrightarrow R$. That $\triangle$ satisfies the diagram (co-associativity) implies that μ satisfies the group scheme (associativity) diagram, and that ε satisfies the diagram labeled (co-unit) implies that e satisfies the group scheme (unit) diagram. In addition, the diagrams (i) and (ii) in the Hopf Algebras section under the identifications above amount to saying the map d is a group scheme homomorphism, and (iii) and (iv) amount to saying that μ and e are in fact maps of $\operatorname{Spec}(S)$-schemes. Finally, because α is S-linear, it is a map of $\operatorname{Spec}(S)$-schemes, and that α satisfies the (antipode) diagram implies that inv satisfies the (inverse) diagram. All of the above taken together implies that $\operatorname{Spec}(R)$ is in fact a $\operatorname{Spec}(S)$-group scheme as stated.

On the other hand, given $f : \operatorname{Spec}(R) \longrightarrow \operatorname{Spec}(S)$ a $\operatorname{Spec}(S)$-group scheme, we get the algebra unit map by taking the corresponding group homomorphism $\eta : S \longrightarrow R$, and this turns R into an S-algebra. Note that the diagonal morphism $d : \operatorname{Spec}(R) \longrightarrow \operatorname{Spec}(R) \times_{\operatorname{Spec}(S)} \operatorname{Spec}(R) \cong \operatorname{Spec}(R \otimes_S R)$, which is also clearly an S-group scheme homomorphism, gives the algebra multiplication map $\bigtriangledown : R \otimes_S R \longrightarrow R$ induced by the map η, and this algebra multiplication is commutative since the multiplication in R is. Apart from that, the proof above can be dualized quite easily by taking global sections. For example, to define the co-multiplication $\triangle$ we simply let it be the ring homomorphism corresponding to μ and so on. Continuing in this manner by necessity gives us that R is a commutative Hopf S-algebra, as required. As such, we have that the category of commutative Hopf S-algebras is antiequivalent to the category of affine group schemes over Spec(S). □

Commutative Group Schemes: A Proof by Deligne

At last we come to the final proof of the paper. This is essentially the proof of Deligne presented in [5], pp.2-5 with some elucidation of key points. In general, all schemes are S-schemes unless otherwise stated. Note that many of the claims regarding Hom of sheaves of modules follow essentially because it is true of Hom of modules themselves. With that in mind we begin by stating some preliminary information.

Let $G = \mathscr{Spec}(\mathcal{A})$ be an S-group scheme of finite order r. Define maps $s_{\mathcal{A}} : \mathcal{A} \longrightarrow \mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{A}$ and $t_{\mathcal{A}} : \mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{A} \longrightarrow \mathcal{A}$ via the maps $\mu_G : G \times_S G \longrightarrow G$ and $d : G \longrightarrow G \times_S G$ respectively. That $\mathcal{A}$ is locally free of finite rank r implies that $\mathcal{A}'$ is, in fact, also locally free of finite rank r. Now, there is clearly a homomorphism $\mathcal{A}' \otimes_{\mathcal{O}_S} \mathcal{A}' \longrightarrow (\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{A})'$, and because $\mathcal{A}'$ is locally free of finite rank it is an isomorphism. We can use this isomorphism and the maps $s_{\mathcal{A}}$ and $t_{\mathcal{A}}$ to define maps $t_{\mathcal{A}'} : \mathcal{A}' \otimes_{\mathcal{O}_S} \mathcal{A}' \longrightarrow \mathcal{A}'$ and $s_{\mathcal{A}'} : \mathcal{A}' \longrightarrow \mathcal{A}' \otimes_{\mathcal{O}_S} \mathcal{A}'$ by taking $t_{\mathcal{A}'}$ to be the map defined by $f \longmapsto f \circ s_{\mathcal{A}}$ and $s_{\mathcal{A}'}$ to be the map defined by $f \longmapsto f \circ t_{\mathcal{A}}$. In fact, in much the same way as in the previous section, these two maps make $\mathcal{A}'$ into a co-commutative Hopf $\mathcal{O}_S$-algebra (where a sheaf of Hopf $\mathcal{O}_S$-algebras is defined in the obvious way). Furthermore, G is a commutative group scheme if and only if $\mathcal{A}'$ is a commutative algebra (i.e., $t_{\mathcal{A}'}$ is a commutative algebra multiplication).

If $H \xrightarrow{f} S$ is a group scheme, and $m \in \mathbb{Z}$, we wish to define the map $m_H : H \longrightarrow H$ as the morphism such that, if X is any S-scheme, and $\xi \in H(X)$, then $m_H(\xi) = \xi^m$. If $H = \mathscr{S}\!pec(\mathcal{A})$, then let $[m] : \mathcal{A} \longrightarrow \mathcal{A}$ be the corresponding $\mathcal{O}_S$-algebra map. In that case, the laws of exponents $(\xi^m)^n = \xi^{mn}$ and $\xi^m \xi^n = \xi^{m+n}$ correspond to the clearly true statements $[m] \circ [n] = [mn]$ and $t_{\mathcal{A}} \circ ([m] \otimes [n]) \circ s_{\mathcal{A}} = [m+n]$. Also $[1] = \mathrm{id}_{\mathcal{A}}$ and $[0] = \eta \circ \varepsilon$, where η corresponds to the structure map f, and ε, to the unit map e.

Now, before we begin the proof proper, we need to define a map called the *trace*. To that end, given $G = \mathscr{S}\!pec(\mathcal{A})$ and $T = \mathscr{S}\!pec(\mathcal{B})$ of finite order r and s respectively, we note that we have the following equalities and injection:

$$G(T) = \mathrm{Hom}_{\mathcal{O}_S\text{-alg.}}(\mathcal{A}, \mathcal{B}) = \mathrm{Hom}_{\mathcal{B}\text{-alg.}}(\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{B}, \mathcal{B}) \tag{1}$$

$$\mathrm{Hom}_{\mathcal{B}\text{-alg.}}(\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{B}, \mathcal{B}) \hookrightarrow \mathrm{Hom}_{\mathcal{B}}(\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{B}, \mathcal{B}) \tag{2}$$

$$\mathrm{Hom}_{\mathcal{B}}(\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{B}, \mathcal{B}) = \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{A}, \mathcal{O}_S) \otimes_{\mathcal{O}_S} \mathcal{B} = \Gamma(S, \mathcal{B} \otimes_{\mathcal{O}_S} \mathcal{A}') \tag{3}$$

where the last line follows because we are dealing with $\mathcal{O}_S$-algebras that are locally free of finite rank and because of the natural isomorphism $\mathcal{A}' \otimes_{\mathcal{O}_S} \mathcal{B} \cong \mathcal{B} \otimes_{\mathcal{O}_S} \mathcal{A}'$. Using these, we see that we have an injection, $G(T) \hookrightarrow \Gamma(S, \mathcal{B} \otimes_{\mathcal{O}_S}$

$\mathcal{A}'$), and, in the special case $T = S$, we get $G(S) \hookrightarrow \Gamma(S, \mathcal{A}')$. Now let G and T be as before with $f : T \longrightarrow S$ the structure morphism.

Definition 4.1. We define the *trace map* to be the unique map Tr_f which satisfies the following diagram:

$$\begin{array}{ccc} G(T) & \hookrightarrow & \Gamma(S, \mathcal{B} \otimes_{\mathcal{O}_S} \mathcal{A}') \\ \downarrow{\scriptstyle \mathrm{Tr}_f} & & \downarrow{\scriptstyle N} \\ G(S) & \hookrightarrow & \Gamma(S, \mathcal{A}') \end{array}$$

where the inclusions are as indicated in (1),(2), and (3), and N is the norm map of the $\mathcal{A}'$-algebra $\mathcal{B} \otimes_{\mathcal{O}_S} \mathcal{A}'$, which is locally free of finite rank s over $\mathcal{A}'$. It is clear that Tr_f is a group homomorphism.

Let $u \in G(S)$, let t be an S-automorphism of T, and let $G(f) : G(T) \longrightarrow G(S)$ be the image of f under the functor G. Note that because of the properties of the norm map, the following properties are satisfied by Tr_f:

$$\mathrm{Tr}_f(G(f)(u)) = u^s$$

$$\mathrm{Tr}_f(\beta \circ t) = \mathrm{Tr}_f(\beta) \text{ for all } \beta \in G(T)$$

With Tr_f defined we can state the final theorem and give a proof:

Theorem 4.1. *A commutative S-group scheme of finite order m is killed by m.*

Proof. Suppose that H is a commutative group scheme of order m over some scheme T. Then given any other scheme over T, say S, it is sufficient to show that, for $\xi \in H(S)$, ξ has order dividing m. But, since $H(S) = \mathrm{Mor}_S(S, H \times_T S)$, and being commutative of order m behaves well with respect to base change (this essentially follows from part (2) of [1, Definition 01LX]), we only have to show that, for a commutative group scheme $f : G \longrightarrow S$, $u^m = 1$ for any $u \in G(S)$.

Let $\varphi : G \longrightarrow G \times_S S$ be the canonical isomorphism. Define $t_u : G \longrightarrow G$ by $t_u = \mu \circ (\mathrm{id}_G \times u) \circ \varphi$ (i.e., t_u is the S-automorphism that is translation by u). Now, as defined earlier, we have a map $1_G \in G(G)$. We know that $\mathrm{Tr}_f(1_G \circ t_u) = \mathrm{Tr}_f(1_G)$ and, furthermore, that $1_G \circ t_u = 1_G * G(f)(u)$, where $*$ is the group multiplication. As such, we have $\mathrm{Tr}_f(1_G) = \mathrm{Tr}_f(1_G * G(f)(u)) = \mathrm{Tr}_f(1_G) * \mathrm{Tr}_f(G(f)(u)) = \mathrm{Tr}_f(1_G) * u^m$, and so u^m is the group identity, as required. □

Bibliography

[1] The Stacks Project Authors. *Stacks Project*. http://www.math.columbia.edu/algebraic_geometry/stacks-git.

[2] Robert W. Easton. A note on group schemes. http://www.robertweaston.com/wp-content/uploads/2009/09/Note-on-Group-Schemes-9-20-2009.pdf, 2009.

[3] David Eisenbud and Joe Harris. *The Geometry of Schemes*. Springer-Verlag, 2000.

[4] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[5] Frans Oort and John Tate. Group schemes of prime order. *Annales scientifiques de l'École Normale Supérieure, Sér. 4*, 3(1):1–21, 1970.