

PRINCIPAL HOMOGENEOUS SPACES AND GROUP SCHEME EXTENSIONS

BY

WILLIAM C. WATERHOUSE⁽¹⁾

Abstract. Suppose G is a finite commutative group scheme over a ring R . Using Hopf-algebraic techniques, S. U. Chase has shown that the group of principal homogeneous spaces for G is isomorphic to $\text{Ext}(G', \mathbf{G}_m)$, where G' is the Cartier dual to G and the Ext is in a specially-chosen Grothendieck topology. The present paper proves that the sheaf $\text{Ext}(G', \mathbf{G}_m)$ vanishes, and from this derives a more general form of Chase's theorem. Our Ext will be in the usual (*fpqc*) topology, and we show why this gives the same group. We also give an explicit isomorphism and indicate how it is related to the existence of a normal basis.

0. We begin by summarizing background results and establishing our notation; the facts here stated without proof can be found in [3], [5], [7], and [8]. Let P be a prescheme, G a flat commutative group scheme affine over P . Let X be any prescheme over P . A *principal fiber space* for G over X is a sheaf Y (for the *fpqc* topology) with morphisms $\sigma: G \times_P Y \rightarrow Y$ and $p: Y \rightarrow X$ such that

- (1) G operates on Y (via σ) over X .
- (2) The map $G \times_P Y \rightarrow Y \times_X Y$ defined on \mathcal{Q} -valued points by $(g, y) \mapsto (gy, y)$ is an isomorphism.
- (3) The map p is a sheaf epimorphism.

It is a theorem that every principal fiber space is representable; furthermore, the map $p: Y \rightarrow X$ is affine and faithfully flat. In case $X=P$ we call Y a *principal homogeneous space* for G .

Suppose $P=\text{Spec } R$, $G=\text{Spec } A$, and $X=\text{Spec } T$. Then Y also is affine, say $Y=\text{Spec } S$, and the definition is equivalent to giving maps $\sigma': S \rightarrow A \otimes_R S$ and $p': T \rightarrow S$ such that

- (1') The map σ' is T -linear and makes S an A -comodule.
- (2') The map $(\sigma', 1 \otimes \text{id}): S \otimes_T S \rightarrow A \otimes_R S$ is an isomorphism.
- (3') S is faithfully flat over T .

If $T=R$ we see that these are precisely the "Galois A -objects" of [2].

Suppose Y_1 and Y_2 are principal fiber spaces for G over X . Let G act on $Y_1 \times_X Y_2$ by $g(y_1, y_2) = (gy_1, g^{-1}y_2)$, and let Y be the quotient sheaf. Then Y is another principal fiber space, and this operation turns the set $H^1(X, G)$ of isomorphism classes of such spaces into an abelian group.

Received by the editors May 19, 1969 and, in revised form, February 16, 1970.

AMS 1969 subject classifications. Primary 14S0, 13T0; Secondary 18D0.

Key words and phrases. Commutative group scheme, principal homogeneous space, line bundle, extension group, dual group scheme, Grothendieck topology, normal basis.

⁽¹⁾ The author was supported by an NRC-ONR research associateship.

Copyright © 1971, American Mathematical Society

If a map between principal fiber spaces commutes with the G -actions and the projections to X , it is an isomorphism.

Elements of $H^1(X, \mathbf{G}_m)$, where \mathbf{G}_m is the multiplicative group, are called *line bundles*. To study them, suppose first $X = \text{Spec } T$ is affine. Then $Y = \text{Spec } S$, and σ' is a T -linear map of S into $S[u, u^{-1}]$. Letting $\pi_n(s)$ be the coefficient of u^n in $\sigma'(s)$, we find that the π_n are a set of pairwise orthogonal projections giving a decomposition of S into T -modules S_n ; furthermore $S_0 \simeq T$, the T -module S_1 is invertible, and $S_n \simeq S_1^{\otimes n}$. Every invertible T -module conversely gives a line bundle, and the bundle is trivial iff the module is free. Even for X not affine this reasoning shows $H^1(X, \mathbf{G}_m) = \text{Pic}(X)$. Since an invertible module is locally free, we see also that every line bundle is locally trivial in the Zariski topology, i.e. there is a covering of X by open affines over each of which there is a section.

Let G be as above, and let

$$0 \rightarrow G \rightarrow F \rightarrow H \rightarrow 0$$

be a sequence of commutative group schemes over P . It is called *exact* (in *fpqc*) if it makes F a principal fiber space for G over H . In particular, if we begin with just a sheaf F of commutative groups, we can deduce its representability. The set of isomorphism classes of such extensions is called $\text{Ext}(H, G)$; by the preceding sentence this is the same as $\text{Ext}^1(H, G)$ computed in the abelian category of (*fpqc*) commutative group sheaves. It is thus an abelian group, and the obvious map $\text{Ext}(H, G) \rightarrow H^1(H, G)$ is a homomorphism. The kernel of this map consists of those extensions having a scheme-theoretic section $H \rightarrow F$. These are precisely the extensions corresponding to symmetric (Hochschild) cocycles, so we have an exact sequence

$$0 \rightarrow H_2^2(H, G) \rightarrow \text{Ext}(H, G) \rightarrow H^1(H, G).$$

1. We now state and prove the main theorems. If F_1 and F_2 are commutative group schemes, then for each prescheme Q over P we can form $\text{Ext}_{Q\text{-gp}}(F_{1Q}, F_{2Q})$; this gives a presheaf, and we write $\mathbf{Ext}(F_1, F_2)$ for the associated sheaf. A group scheme G is called *finite* if it is locally represented by algebras which are free modules of finite rank over the base; it is called a *twisted constant group* if there is an (*fpqc*) covering in which it becomes a constant group.

THEOREM 1. *Let G be a commutative group scheme over P which is either finite or a twisted constant group of finite type. Then $\mathbf{Ext}(G, \mathbf{G}_m) = 0$.*

Proof. Let (*) $0 \rightarrow \mathbf{G}_m \rightarrow F \rightarrow G \rightarrow 0$ be an extension over P ; we will prove that it is trivial locally in *fpqc*. Since this will hold then for any Q in place of P , it will follow that the whole \mathbf{Ext} sheaf vanishes. By a first localization we may assume that $P = \text{Spec } R$ is affine, and we want to find a ring B faithfully flat over R such that (*) splits over B .

Suppose first that $G = \text{Spec } T$ is a finite group scheme, so T is a finitely generated projective R -module. Write $F = \text{Spec } S$ as in §0. We begin by considering the sections (if any) of (*) over R ; they correspond naturally to retractions $G_m \leftarrow F$, i.e. sections $R[u, u^{-1}] \rightarrow S$. Such a section is determined by giving an invertible $s \in S$ mapping onto u and such that $\delta s = s \otimes s$ (where $\delta: S \rightarrow S \otimes S$ is the comultiplication corresponding to $F \times F \rightarrow F$). If $\varepsilon: S \rightarrow R$ is the counit, these s can also be characterized as the $s \in S_1$ with $\delta s = s \otimes s$ and $\varepsilon(s) = 1$.

Let $C = \text{Hom}_{R\text{-mod}}(S_1, R)$. It is easy to check that δ takes S_1 to $S_1 \otimes S_1$, and so C has a commutative algebra structure dual to δ and ε . The retractions over R are then precisely the maps

$$\text{Hom}_{R\text{-alg}}(C, R) \subset \text{Hom}_{R\text{-mod}}(C, R) \simeq S_1.$$

But now clearly after base extension the retractions over B are

$$\text{Hom}_{B\text{-alg}}(B \otimes_R C, B) = \text{Hom}_{R\text{-alg}}(C, B).$$

Thus in particular there is a retraction, and hence a section over C ; and C , like S_1 and T , is faithfully flat over R .

Say now G is a twisted constant group; by making a faithfully flat base extension we may assume it is actually a constant group. Since we can split an extension of a direct sum if we can split each part, we may assume that G is either $\mathbb{Z}/n\mathbb{Z}$ or \mathbb{Z} . In the first case the previous argument shows that sections exist. In the second case we note that a homomorphism $\pi: F \rightarrow \mathbb{Z}$ has a section over B as soon as $1 \in \mathbb{Z}(\text{Spec } B)$ equals $\pi(v)$ for some $v \in F(\text{Spec } B)$; for there is always a unique homomorphism $\mathbb{Z} \rightarrow F$ over B taking 1 to a prescribed element in $F(\text{Spec } B)$. Now since in our case $F \rightarrow \mathbb{Z}$ is by hypothesis a sheaf epimorphism, there is a faithfully flat B with $1 \in \pi F(\text{Spec } B)$, and this gives us our section. ■

Recall that commutative group schemes F and F' are called *dual* if there is a bilinear map $F \times F' \rightarrow G_m$ inducing isomorphisms $F' \simeq \mathbf{Hom}(F, G_m)$ and $F \simeq \mathbf{Hom}(F', G_m)$; here of course \mathbf{Hom} is the sheaf assigning $\text{Hom}_{Q\text{-gp}}$ to Q . Every finite commutative F has a finite commutative dual, the Cartier dual. Twisted constant groups of finite type also have duals, called multiplicative finite type groups.

THEOREM 2. *Let G be a commutative group scheme over P which is either finite or multiplicative finite type. Then $H^1(P, G) \simeq \text{Ext}(G', G_m)$.*

Proof. Let Ext^n be the derived functors of Hom in the category of commutative group sheaves. If we define sheaves \mathbf{Ext}^n from them, then [10, p. V-29] the \mathbf{Ext}^n are the derived functors of \mathbf{Hom} . We can define $H^n(P, F)$ as the derived functors of $F \mapsto F(P)$, and $H^1(P, F)$ will be the group previously introduced. By [10, p. V-29] (cf. [6, p. 264]) we have a spectral sequence

$$H^p(P, \mathbf{Ext}^q(E, F)) \Rightarrow \text{Ext}^{p+q}(E, F)$$

yielding in particular an exact sequence

$$0 \rightarrow H^1(P, \mathbf{Hom}(E, F)) \rightarrow \text{Ext}^1(E, F) \rightarrow H^0(P, \mathbf{Ext}^1(E, F)).$$

If we apply this to G' and G_m , then the map

$$H^1(P, \mathbf{Hom}(G', G_m)) \rightarrow \text{Ext}^1(G, G_m)$$

is an isomorphism, since by Theorem 1 the next term in the sequence vanishes. ■

A similar proof of Chase's theorem has been outlined independently by S. Shatz [9].

2. The isomorphism in Theorem 2, derived from a spectral sequence, is not particularly accessible. In this section we describe explicit maps between the two groups.

Suppose first Y is a principal homogeneous space. Let G act on $F_1 = Y \times G' \times G_m$ (the product over P , of course) by

$$g(y, h, \alpha) = (gy, h, \langle g, h \rangle^{-1}\alpha),$$

and let F be the quotient sheaf. We map $F_1 \times F_1 \rightarrow F_1$ by

$$(y, h, \alpha) \cdot (y', h', \alpha') = (y, hh', \langle y^{-1}y', h' \rangle \alpha \alpha');$$

this is compatible with the G -action and so induces a map $F \times F \rightarrow F$. Thereby F becomes a commutative group sheaf over P , the identity being induced by any $(y, 1, 1)$ and the inverse of (y, h, α) being (y, h^{-1}, α^{-1}) . The obvious maps $G_m \rightarrow F$ and $F \rightarrow G'$ make

$$(*) \quad 0 \rightarrow G_m \rightarrow F \rightarrow G' \rightarrow 0$$

exact.

Suppose now conversely that we start with (*); apply $\text{Hom}(G', -)$ to it, getting

$$0 \rightarrow G \rightarrow \text{Hom}(G', F) \rightarrow \text{Hom}(G', G'),$$

and let Y be the inverse image of $\text{id} \in \text{Hom}(G', G')$. In other words, let Y be the sheaf of (group) sections of (*).

THEOREM 2'. *These two constructions are inverse to each other, and induce isomorphisms between $H^1(P, G)$ and $\text{Ext}(G', G_m)$.*

The proof of this is mainly straightforward verification, and we will omit it. The only difficult point is showing that the sheaf of sections satisfies condition (3) for a principal fiber space, and this follows from the argument in Theorem 1.

We can give an alternate description of the first construction, one which avoids even the taking of a quotient. We take $P = \text{Spec } R$, so $G = \text{Spec } A$ and $Y = \text{Spec } S$, the action being given by a map $\sigma': S \rightarrow A \otimes_R S$. If B is an R -algebra, we write B^* for its group of invertible elements, and S_B for the base extension $B \otimes_R S$. We recall that a sheaf is determined by its value on affine schemes; we will restrict to affine schemes and also shorten the functor notation $Y(\text{Spec } B)$ to $Y(B)$.

THEOREM 3. Define a functor by

$$V(B) = \{s \in S_B^* \mid (\exists a \in A_B) \sigma'(s) = a \otimes s\}.$$

Map this to

$$G'(B) = \text{Hom}(G, G_m)(B) = \{a \in A_B^* \mid \delta a = a \otimes a\}$$

by sending s to a^{-1} if $\sigma'(s) = a \otimes s$. Map $G_m(B) = B^*$ into $V(B)$ using the natural map $B \rightarrow S_B$. Then

$$0 \rightarrow G_m \rightarrow V \rightarrow G' \rightarrow 0$$

is isomorphic to the extension (*) associated with Y in Theorem 2'.

Proof. Obviously $V(B \times C) = V(B) \times V(C)$. Let $B \rightarrow C$ be faithfully flat; we claim then

$$0 \rightarrow V(B) \rightarrow V(C) \xrightarrow{\cong} V(C \otimes_B C)$$

is exact. Indeed, we know that

$$0 \rightarrow (B \otimes S)^* \rightarrow (C \otimes S)^* \xrightarrow{\cong} (C \otimes_B C \otimes S)^*$$

is exact. Suppose therefore that we have an $s \in S_B^*$ with $\sigma'(s) = a \otimes s$ in $C \otimes A \otimes S$; we want to know that $a \in B \otimes A$. But

$$a \otimes 1 = s^{-1} \sigma'(s) \in (C \otimes A \otimes R) \cap (B \otimes A \otimes S);$$

since S is faithfully flat, this intersection equals $B \otimes A \otimes R$. We have thus verified that V is a sheaf.

The next step is to construct a functorial map

$$\psi: Y(B) \times G'(B) \times G_m(B)/G(B) \rightarrow V(B);$$

it will then suffice to prove that when $Y(B) \neq \emptyset$ this map is a group isomorphism inducing the stated homomorphisms from G_m and to G' . To simplify notation we will take $B = R$, the general case following by base change.

We suppose then that we have an element $y \in Y(R)$, i.e., a homomorphism $y: S \rightarrow R$. Take elements $\alpha \in R^* = G_m(R)$ and $a \in G'(R) \subset A^*$. Since $(\sigma', 1 \otimes \text{id}): S \otimes S \rightarrow A \otimes S$ is an isomorphism, we can form

$$\psi(y, a, \alpha) = (y, \text{id}) \circ (\sigma', 1 \otimes \text{id})^{-1}(\alpha a \otimes 1);$$

this is an element of S , invertible since αa is. Clearly $\psi(y, 1, \alpha) = \alpha$, so the map from G_m is as described.

Suppose now we take any $g: A \rightarrow R$ in $G(R)$; recall that gy is the map $(g, y) \circ \sigma': S \rightarrow R$. Consider then the commutative diagram in Figure 1. Starting with $\alpha a \otimes 1$ in $A \otimes S$ and going down first gives $\psi(gy, a, \alpha)$; going the other way gives $g(a)\psi(y, a, \alpha) = \psi(y, a, g(a)\alpha)$. Thus ψ is indeed invariant under the action of G .

$$\begin{array}{ccc}
 A \otimes S & \xrightarrow{\delta \otimes \text{id}} & A \otimes A \otimes S \\
 (\sigma', 1 \otimes \text{id}) \uparrow \wr & & \uparrow \wr \quad \text{id} \otimes (\sigma', 1 \otimes \text{id}) \\
 S \otimes S & \xrightarrow{\sigma' \otimes \text{id}} & A \otimes S \otimes S \\
 & & \downarrow (g, y, \text{id}) \\
 & & S
 \end{array}$$

FIGURE 1

Let s be any member of $V(R)$, with $\sigma'(s) = a \otimes s$; here a is invertible since s is. The relation $(\delta \otimes \text{id})\sigma' = (\text{id} \otimes \sigma')\sigma'$ shows that $\delta(a) \otimes s = a \otimes a \otimes s$; since S is faithfully flat, $\delta(a) = a \otimes a$. Thus $a \in G'(R)$. If we look then at the element $y(s)s^{-1} \otimes s$ in $S \otimes S$, we find that it goes to $y(s)a^{-1}$ in $A \otimes S$ and to s under (y, id) . Thus $s = \psi(y, a^{-1}, y(s))$, and all of $V(R)$ is in the image of ψ .

Next we observe that the map $G \times Y \rightarrow G \times Y$ given by

$$(g, z) \mapsto gz \mapsto (y, gz) \mapsto (y(gz)^{-1}, gz)$$

is also given by

$$(g, z) \mapsto (g, y, z) \mapsto (g, yz^{-1}, z) \mapsto (g, g^{-1}, yz^{-1}, z) \mapsto (g^{-1}(yz^{-1}), gz).$$

Hence the corresponding composite maps $A \otimes S \rightarrow A \otimes S$ are equal. Going the first way from $\alpha a \otimes 1$ yields $\sigma'\psi(y, a, \alpha)$; going the other way yields $a^{-1} \otimes \psi(y, a, \alpha)$. Thus ψ does map into $V(R)$, and the map to G' is as described.

It is easy now to show that ψ is injective. For suppose $\psi(y, a, \alpha) = \psi(y', a', \alpha')$. Then $a = a'$, since we can recover a from $\sigma'\psi(y, a, \alpha)$. Using the action of $G(R)$ we may assume $y = y'$. But $\psi(y, a, \alpha) = \alpha\psi(y, a, 1)$, and these are distinct for distinct α .

Finally we verify that ψ is a group homomorphism. Take two elements (y, a, α) and (y', a', α') ; using the G -action we may assume $y = y'$. Their product then is $(y, aa', \alpha\alpha')$. But since the maps used in defining ψ are algebra morphisms, we indeed have $\psi(y, aa', \alpha\alpha') = \psi(y, a, \alpha)\psi(y, a', \alpha')$. ■

REMARK. After eliminating some dualizations in [2], we find that V is precisely the functor constructed there. Working directly with the algebras, however, Chase naturally maps s to a rather than to a^{-1} . Hence the homomorphism he constructs is the negative of ours.

3. Our next goal is to show that the Ext in Theorem 2 can be computed in a coarse Grothendieck topology. For convenience we will continue to regard our sheaves as functors on affine schemes. The basic tool is the following general result:

PROPOSITION 1. *Let \mathcal{S} and \mathcal{T} be two Grothendieck topologies. Suppose that*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is a sequence of commutative group functors which are sheaves in \mathcal{S} , and that the sequence is exact in \mathcal{S} . Then if A and C are sheaves for \mathcal{S} , so is B .

Proof. Let $\{U_i \rightarrow W\}$ be a covering in \mathcal{S} . We first show that

$$B(W) \rightarrow \prod B(U_i)$$

is injective. Indeed, suppose an element b goes to zero. Then its image in $C(W)$ goes to zero in $\prod C(U_i)$ and hence equals zero. By exactness then b comes from an $a \in A(W)$. But all the maps $A(U_i) \rightarrow B(U_i)$ are injective, so a goes to zero in $\prod A(U_i)$ and hence equals zero; thus $b=0$.

Suppose now we have elements $b_i \in B(U_i)$ such that b_i and b_j have the same image b_{ij} in $B(U_i \times U_j)$ —here and throughout the proof, \times stands for the product over W . We must produce an element $b \in B(W)$ yielding all the b_i . This is a diagram-chasing argument, and the reader is encouraged to write out any diagram he feels the urge to chase.

Let $c_i \in C(U_i)$ be the image of b_i . Then c_i and c_j have the same image in $C(U_i \times U_j)$, so there is an element $c \in C(W)$ giving every c_i . By \mathcal{S} -exactness we can find a covering $\{V_\lambda \rightarrow W\}$ in \mathcal{S} such that c is in the image of B there; that is, for each λ , the image of c in $C(V_\lambda)$ comes from some $b_\lambda \in B(V_\lambda)$.

Fix λ , and consider the images of b_λ and b_i in $B(V_\lambda \times U_i)$. They become the same in $C(V_\lambda \times U_i)$, so their difference comes from an $a_{\lambda i} \in A(V_\lambda \times U_i)$. Now b_i and b_j become the same in $B(U_i \times U_j)$; therefore $a_{\lambda i}$ and $a_{\lambda j}$ have the same image in $B(V_\lambda \times U_i \times U_j)$, and hence also in $A(V_\lambda \times U_i \times U_j)$. Since $\{V_\lambda \times U_i \rightarrow V_\lambda\}$ is a covering in \mathcal{S} , and A is a \mathcal{S} -sheaf, there is an $a_\lambda \in A(V_\lambda)$ giving rise to the $a_{\lambda i}$. Replacing b_λ by $b_\lambda + a_\lambda$, we may assume that b_λ and b_i have the same image in $B(V_\lambda \times U_i)$.

We observe now that b_λ and b_μ have the same image (= that of b_i) in $B(V_\lambda \times V_\mu \times U_i)$. Since we already know that

$$B(V_\lambda \times V_\mu) \rightarrow \prod_i B(V_\lambda \times V_\mu \times U_i)$$

is injective, we see that b_λ and b_μ have the same image in $B(V_\lambda \times V_\mu)$. Hence there is an element $b \in B(W)$ giving every b_λ . Since b and b_i have the same image (= that of b_λ) in all $B(V_\lambda \times U_i)$, the b_i must come from b . ■

We now take \mathcal{S} to be the following Grothendieck topology, used in [2]: Let $\text{Spec } C \rightarrow \text{Spec } B$ be a covering if $C = (\prod R_{x_i}) \otimes B$, where $\sum x_i = 1$ and the x_i are not in the Jacobson radical of R . Clearly this is much coarser than the $(fpqc)$ topology. It is fine enough for our purposes, however, because it trivializes enough line bundles.

PROPOSITION 2. *Let Y be a line bundle over $\text{Spec } D$, where D as an R -module is projective of finite type. Then there is an \mathcal{S} -covering in which Y becomes trivial.*

Proof. In view of the remarks in §0, the proposition is equivalent to the following statement: If M is any invertible D -module, there are x_1, \dots, x_n in $R \setminus \text{Rad}(R)$ with $\sum x_i = 1$ and each M_{x_i} free over D_{x_i} . This is straightforward commutative algebra, mostly available in [1, p. 65], and we just sketch the proof.

For each maximal ideal m of R , the ring D_m is semilocal, and hence M_m is free. Then there is an $f \in R \setminus m$ with M_f free over D_f . The collection of all such f generates an ideal lying in no maximal ideal, so there is a relation $1 = \sum r_i f_i$. Dropping the terms which lie in $\text{Rad}(R)$ we get a sum $g = \sum r_i f_i$ with g lying in $1 - \text{Rad}(R)$ and hence invertible. Set $x_i = g^{-1} r_i f_i$. ■

Let H now be a finite commutative group scheme over R . If

$$0 \rightarrow G_m \rightarrow F \rightarrow H \rightarrow 0$$

is exact, i.e. exact in $(fpqc)$, then it is exact in \mathcal{S} ; for Proposition 2 shows that $F \rightarrow H$ is an \mathcal{S} -epimorphism. Conversely, if it is exact in \mathcal{S} , Proposition 1 shows that F is a sheaf in $(fpqc)$; and of course the sequence is still exact there. Thus we have

THEOREM 4. *If H is a finite commutative group scheme over R , then $\text{Ext}(H, G_m)$ is canonically isomorphic to the group $\text{Ext}(H, G_m)$ computed in \mathcal{S} .* ■

It is perhaps worth mentioning that one cannot here replace G_m by an arbitrary group. For example, let R be a field of characteristic $p > 0$, and consider

$$0 \rightarrow \alpha_p \rightarrow \alpha_{p^2} \rightarrow \alpha_p \rightarrow 0,$$

which is exact. Since \mathcal{S} has no coverings, exactness in \mathcal{S} would mean exactness as presheaves, and the final map is not surjective when evaluated on $\text{Spec}(R[u]/u^p)$.

4. Take G again to be a finite commutative group scheme, and assume for simplicity that $P = \text{Spec } R$. Combining Theorem 2 with a remark in §0, we find that there is an exact sequence

$$0 \rightarrow H^2_s(G', G_m) \rightarrow H^1(P, G) \rightarrow \text{Pic}(G').$$

In this section we will give a more explicit description of the map to $\text{Pic}(G')$. Let $G = \text{Spec } A$, so $G' = \text{Spec } A'$ where $A' = \text{Hom}_{R\text{-mod}}(A, R)$.

Set $T = A'$ in the proof of Theorem 1; by Theorem 2' we have $Y = \text{Spec } C$ there. Look first at the G -action induced on the sheaf of retractions. It is given simply by letting elements $a' \in G(B) \subset B \otimes A'$ act on $s \in Y(B) \subset B \otimes S_1$ by multiplication. This means that the action $C \rightarrow A \otimes C$ yields an A' -module structure agreeing with the one naturally induced on

$$C = \text{Hom}_{R\text{-mod}}(S_1, R).$$

Then as an A' -module,

$$\begin{aligned} S_1 &= \text{Hom}_{R\text{-mod}}(C, R) = \text{Hom}_{A'\text{-mod}}(C, A) \\ &= A \otimes_{A'} C^\vee, \end{aligned}$$

where C^\vee is the inverse of C in $\text{Pic}(A')$.

So far, however, we have been looking at the sheaf of retractions. Our actual map takes the sheaf of sections, giving the inverse principal homogeneous space (same C , but different action). Thus going back from C we get the inverse of the above class, and we have

THEOREM 5. *The map $H^1(P, G) \rightarrow \text{Pic}(G')$ sends $\text{Spec } C$ to the class of $C \otimes_{A'} A^\vee$, where A^\vee is the inverse of A as an A' -module. In particular, the kernel of the map consists of those spaces for which C is isomorphic to A as an A' -module. ■*

REMARKS. 1. If we replace C , A , and A' by the corresponding locally free sheaves, we can extend the theorem to nonaffine base preschemes.

2. If $\text{Pic } R=0$, or if G comes by base extension from such a ring, then A is a free A' -module [2, p. 68]; hence in those cases the kernel is those C which are free over A' . This holds in particular if G is a finite constant group. In the case $G = \mathbf{Z}/n\mathbf{Z}$, Theorem 2 and this fact were proved by H. Epp [4].

3. When G is a constant group, A' is the group algebra, and to say C is free is to say that it has a normal basis. At first glance one would be inclined to use this definition in general. But Theorem 5 shows that it may be better to say C has a normal basis if C is isomorphic to A as an A' -module. With this convention we can then conclude that the spaces with a normal basis form a subgroup canonically isomorphic to $H_s^2(G', G_m)$.

REFERENCES

1. S. U. Chase and A. Rosenberg, *Amitsur cohomology and the Brauer group*, Mem. Amer. Math. Soc. No. 52 (1965), 34–79. MR 33 #4119.
2. S. U. Chase and M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Math., no. 97, Springer-Verlag, Berlin, 1969.
3. M. Demazure, A. Grothendieck et al., *Schémas en groupes*. Fasc. 1, Exposés 1 à 4, Séminaire de Géométrie Algébrique, 1963, Inst. Hautes Études Sci., Paris, 1963/64. MR 34 #7517.
4. H. Epp, *Commutative group schemes, Harrison's theorem, and Galois extensions*, Thesis, Northwestern University, 1966, Dissertation Abstracts 27 B (1967). Abstract #3595.
5. P. Gabriel et al., *Groupes algébriques*, Séminaire Heidelberg-Strasbourg, 1965/66.
6. R. Godement, *Topologie algébrique et théorie des faisceaux*, Actualités Sci. Indust., no. 1252, Hermann, Paris, 1958. MR 21 #1583.
7. A. Grothendieck, *Revêtements étales et groupe fondamental*. Fasc. 2, Exposé 8, Séminaire de Géométrie Algébrique, 1960/61, Inst. Hautes Études Sci., Paris, 1963. MR 36 #179b.
8. F. Oort, *Commutative group schemes*, Lecture Notes in Math., no. 15, Springer-Verlag, Berlin, 1966. MR 35 #4229.
9. S. Shatz, *Principal homogeneous spaces for finite group schemes*, Proc. Amer. Math. Soc. 22 (1969), 678–680.
10. J. Verdier, *Cohomologie étale des schémas*, Séminaire de Géométrie Algébrique, 1963, Inst. Hautes Études Sci., Paris, 1963/64.

CORNELL UNIVERSITY,
ITHACA, NEW YORK 14850