JOURNAL OF ALGEBRA 17, 34–40 (1971)

Automorphism Schemes and Forms of Witt Lie Algebras

WILLIAM C. WATERHOUSE

Department of Mathematics, Cornell University, Ithaca, N. Y. 14850

Communicated by Nathan Jacobson

Received June 1, 1969

Let k be a field of characteristic $p > 3$. Let $A = k[X_1, \ldots, X_n]/(X_1{}^p, \ldots, X_n{}^p)$, and let L be the generalized Witt Lie algebra formed by the derivations of A. It was conjectured by Jacobson [7], and proved by Allen and Sweedler [1], that the forms of L (defined below) correspond precisely to the forms of A. In this paper I use a lemma from [1] to prove that the automorphism group schemes of A and L are isomorphic; from this a strengthened form of the Allen-Sweedler result follows by the techniques of faithfully flat descent.

The proof is based on a discussion of automorphism group schemes vis-a-vis formal groups and Hopf algebras. The results here are doubtless known to the *cognoscenti*, but I cannot find them anywhere in writing. Since for example Galois theory for inseparable extensions is being developed from both points of view (compare [9] and [10]), it seems worthwhile to put the facts on record. I have tried to keep the treatment sufficiently elementary and expository that those familiar with either approach may follow the proofs and see how the two methods are connected.

1.1. Let k be a field, V a finite-dimensional vector space over k. For every (commutative) k-algebra R we can consider the group $Gl_V(R)$ of invertible R-linear maps from $V \otimes R$ to itself; this defines a functor Gl_V from k-algebras to groups. Concretely, choose a basis $v_1, \ldots, v_n$ of V; then invertible R-linear maps correspond to n by n matrices with invertible determinant, and thus to algebra homomorphisms of

$$0 = k[X_{11}, \ldots, X_{nn}, 1/\det(X)]$$

into R.

Now in general, if a functor G from k-algebras to groups satisfies $G(R) = \mathrm{Alg}(A, R)$ for some algebra A, we say G is an *affine group scheme* and write $G = \mathrm{Spec}\ A$. (The experts will pardon a slight *abus de langage* here.) Automatically then A acquires the structure of an involutive bialgebra, or Hopf algebra; and conversely a Hopf algebra structure on A induces group structures on all $\mathrm{Alg}(A, R)$ and so defines an affine group scheme [5, Ex. 2, p. 8]. Thus our ring 0 above is naturally a Hopf algebra, and $Gl_V = \mathrm{Spec}\, 0$.

1.2. Let $G = \mathrm{Spec}\, A$ be an affine group scheme. An *operation of G on V* is, for each R, an operation of the group $G(R)$ on $V \otimes R$, functorial in R. This is equivalent [5, Ex. 3, p. 2] to an A-comodule structure on V; that is, a map $\sigma : V \to A \otimes V$ such that $(id_A \otimes \sigma)\, \sigma = (\Delta \otimes id_V)\, \sigma$ and $(e \otimes id_V)\, \sigma = id_V$, where Δ and e are the comultiplication and counit of the Hopf algebra. The group scheme Gl_V is universal for such operations; that is, the operations correspond to homomorphisms $G \to Gl_V$. Explicitly, if $\sigma(v_i) = \sum c_{ji} \otimes v_j$, then the associated Hopf algebra map $A \leftarrow 0$ sends X_{ij} to c_{ij}.

1.3. Let us suppose now that V is furnished with some additional structure, such as a bilinear map $V \times V \to V$. Then we can define a functor **Aut** V by letting **Aut** $V(R) \subseteq Gl_V(R)$ be those maps preserving the induced structure on $V \otimes R$. This condition is easily seen to be equivalent to a set of polynomial equations in the matrix entries, and hence **Aut** V is $\mathrm{Spec}\, 0_1$ for some quotient 0_1 of 0. We say that an operation of a group scheme G on V preserves the given structure if it does so for every R, and clearly such an operation corresponds to a homomorphism $G \to$ **Aut** V.

2.1. We can go through the same constructions replacing the category of k-algebras by that of linearly compact k-algebras. (These are k-algebras B satisfying $B = \varprojlim B/I$ for a filter of ideals I of finite codimension; they are topologized by letting $\{b + I\}$ be a basis of neighborhoods of b.) A functor from such algebras to groups which satisfies

$$F(B) = \text{Contin. Alg. Hom}(S, B)$$

for some linearly compact S is called a *formal group*, written $F = \mathrm{Spf}\, S$. Automatically S acquires the analogue of a Hopf algebra structure (using the completed tensor product: thus Δ maps S to $S \,\widehat{\otimes}\, S$), and any such structure defines a formal group [4, Ex. VII_B]. We say F is *infinitesimal* if S is a local ring. An operation of F on V again corresponds to a map $\sigma : V \to S \otimes V$ satisfying identities like those before. If $\sigma(v_i) = \sum c_{ji} \otimes v_j$, then the condition that a structure be preserved imposes the same equations on (c_{ij}) as in (1.3).

2.2. In place of S we can consider E, the set of continuous linear homomorphisms from S to k. Dualizing the structure on S makes E into a cocommutative Hopf algebra, and every such Hopf algebra gives a formal group. The formal group is infinitesimal iff E is coconnected. An operation of F on V corresponds to an E-module structure on V, and the condition of preserving additional structure becomes precisely the condition in [1, Sec. 2.3].

3.1. Let $G = \operatorname{Spec} A$ be an affine group scheme which is *algebraic*, i.e., such that A is a finitely generated k-algebra. Let N be the kernel of the map $e : A \to k$, and let $\hat{A}_e = \varprojlim A/N^n$. Then $\hat{G} = \operatorname{Spf} \hat{A}_e$ is naturally an infinitesimal formal group, called the *completion of G at the identity.*

3.2. Let $F = \operatorname{Spf} S$ be an infinitesimal formal group, with M the maximal ideal of S. Suppose F operates on V, with $\sigma(v_i) = \sum c_{ji} \otimes v_j$. The second comodule condition says that the image of (c_{ij}) under $e : S \to k$ is the identity matrix; hence (c_{ij}) is nonsingular and defines a map of 0 to S. It follows also that this map takes N (generated by $X_{ij} - \delta_{ij}$) to M (the kernel of $e : S \to k$), and so it extends uniquely to a continuous map of $\hat{0}_e$ into S. The comodule conditions then say precisely that $F \to \operatorname{Spf} \hat{0}_e$ is a homomorphism. Conversely, any such homomorphism corresponds to a map $\psi : \hat{0}_e \to S$ giving an operation of F with $c_{ij} = \psi(X_{ij})$.

3.3. Let us finally give V some additional structure. Then F preserves this structure iff (c_{ij}) satisfies the appropriate polynomial conditions, which happens iff the map $0 \to S$ factors as $0 \to 0_1 \to S$. As before, these correspond to maps $\hat{0}_{1e} \to S$. Thus we have proved:

PROPOSITION 1. *The formal group* (**Aut** V)^ *is universal for structure-preserving actions of infinitesimal formal groups on V.* ∎

If instead of making S local we require only that all its maximal ideals have k as residue field (E "split", in the terminology of [1]), we can construct a correspondingly larger universal group. But the infinitesimal part is all we need.

4. We now prove:

PROPOSITION 2. *Let G and G′ be algebraic affine group schemes, $\varphi : G \to G'$ a homomorphism. Let K be the algebraic closure of k. Assume:*

1) *the map $\varphi(K) : G(K) \to G'(K)$ is an isomorphism, and*
2) *the induced map $\hat{\varphi} : \hat{G} \to \hat{G}'$ is an isomorphism.*

Then φ is an isomorphism.

Proof. Write $\Phi : A' \to A$ for the map of Hopf algebras corresponding to φ. Then Φ is an isomorphism iff the map

$$\Phi \otimes id : A' \otimes K \to A \otimes K$$

is an isomorphism. The same holds for $\hat{\varphi}$, and so we may assume $k = K$.

The functor $H(R) = \mathrm{Ker}[G(R) \to G'(R)]$ is easily seen to be Spec C, where $C = A \otimes_{A'} k$. Since $\mathrm{Alg}(C, k) = H(k)$ has only one element, C is (by the Nullstellensatz) a local ring finite dimensional over k. Hence it is linearly compact, and the map $A \to C$ extends to a map $\hat{A}_e \to C$.

Now by construction $A' \to A \to C$ and the counit map $A' \to A \to k \to C$ coincide; hence also $\hat{A}_e' \to \hat{A}_e \to C$ and $\hat{A}_e' \to \hat{A}_e \to k \to C$ coincide. But by 2) the maps from $\hat{A}_e$ to a linearly compact local algebra are determined by their compositions with $\hat{A}_e' \to \hat{A}_e$. Thus the map $\hat{A}_e \to C$, surjective by construction, must factor through k, whence $C = k$. That is, H is trivial, and φ is a monomorphism. It follows [5, Ex. 2, p. 26] that Φ is surjective.

Let Q now be any maximal ideal of A', corresponding to an element of $G'(k)$. By 1) there is a corresponding element of $G(k)$, and so $Q = \Phi^{-1}(P)$ for some maximal ideal P of A. From Q we get a map "translation by Q":

$$A' \xrightarrow{\Delta} A' \otimes A' \xrightarrow{id \otimes Q} A' \otimes k \simeq A',$$

which by the group scheme axioms is a ring isomorphism. We have a similar isomorphism $A \to A$ induced by P, and since φ is a group map Φ is compatible with these isomorphisms. We know by 2) that Φ induces an isomorphism $\hat{A}_e' \to \hat{A}_e$; it follows that Φ also induces an isomorphism

$$\varprojlim A'/Q^n \xrightarrow{\sim} \varprojlim A/P^n.$$

Let I now be the ideal $\ker(\Phi)$. The isomorphism above shows that I must be contained in Q^n for all n and Q. But this implies $I = 0$. (For example, if $x \in \bigcap Q^n$, then by Krull's theorem [3, p. 65] $(1 - q)x = 0$ for some $q \in Q$, and so the annihilator of x is not contained in any maximal ideal.) ∎

The second half of this proof is rather more natural when phrased in the geometric language of [4] and [5]; the Proposition then extends immediately to non-affine algebraic group schemes.

5.1. Suppose that V is a finite-dimensional space with some additional structure, and V' is another such. Let K be the algebraic closure of k. We say that V' is a *form* of V if $V' \otimes K$ is K-isomorphic to $V \otimes K$. We can illustrate this with an example we will want later:

PROPOSITION 3. *Let k be a field of characteristic $p > 0$. Let A be the k-algebra $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. Then the forms of A are the algebras*

$$A' = k[Y_1, \ldots, Y_n]/(Y_1^p - a_1, \ldots, Y_n^p - a_n),$$

with $a_i \in k$.

Proof. Consider such an A'. In $A' \otimes K$ we can form $x_i = Y_i - (a_i)^{1/p}$; this gives us elements $x_1, \ldots, x_n$ generating $A' \otimes K$ and satisfying $(x_i)^p = 0$, and they define an isomorphism with $A \otimes K$.

Suppose conversely that B is a form of A, and choose a basis $1 = y_0, y_1, y_2, \ldots$ of B. Then y_i^p is in the span of y_0 over K, so it is so over k, and we have $y_i^p = a_i$ for some $a_i \in k$. Again form $x_i = y_i - (a_i)^{1/p}$ in $B \otimes K$; these are nilpotent elements spanning the maximal ideal M of $B \otimes K \simeq A \otimes K$. Since M/M^2 has dimension n, we can find n of the x_i spanning M mod M^2; we may as well assume they are $x_1, \ldots, x_n$. By Nakayama's lemma $x_1, \ldots, x_n$ generate $B \otimes K$. Hence $y_1, \ldots, y_n$ generate $B \otimes K$ and therefore generate B. We thus have

$$k[Y_1, \ldots, Y_n]/(Y_1^p - a_1, \ldots, Y_n^p - a_n)$$

mapping onto B via $Y_i \mapsto y_i$; the map is an isomorphism by dimension-counting.

5.2. Associated with the algebra A is the generalized Witt Lie algebra L, the derivation algebra of A; for any k-algebra R, the R-derivation algebra of $A \otimes R$ is $L \otimes R$. An automorphism θ of A induces an automorphism θ^* of L by $\theta^*(x) = \theta \circ x \circ \theta^{-1}$; this obviously commutes with change of R and so gives us a homomorphism $\mathbf{Aut}\, A \to \mathbf{Aut}\, L$.

THEOREM. *Assume $p > 3$. Then the map* $\mathbf{Aut}\, A \to \mathbf{Aut}\, L$ *is an isomorphism.*

Proof. We can apply Proposition 2. The first hypothesis there was proved (using the assumption $p > 3$) by Jacobson [7, p. 114]. Proposition 1 and (2.2) allow us to translate the second hypothesis into a statement about universal coconnected cocommutative Hopf algebras. A proof of it (independent of the descent theory) can then be found in [1], essentially in Lemmas 3.5.2 and 3.5.4. ∎

5.3. As a corollary to the Theorem we have

COROLLARY 1 (Allen-Sweedler). *Forms of L are in one-to-one correspondence with forms of A. Explicitly, if A' is a form of A, the corresponding form L' is the derivation algebra of A'.*

Proof. The techniques of faithfully flat descent (developed in [6], and simply explained in [2]) classify forms by cohomology of the automorphism scheme; hence there obviously is a one-to-one correspondence. To make it explicit, we recall the construction of the forms. There are two natural maps

$$d_0, d_1 : A \otimes K \to A \otimes K \otimes K,$$

the cocycles θ are certain automorphisms of $A \otimes K \otimes K$, and the form is simply

$$A' = \{a \in A \otimes K \mid d_0 a = \theta d_1 a\}.$$

The same holds for L and θ^*. An obvious computation shows now that L' is exactly the derivations taking A' to itself. ▮

In view of Proposition 3, Corollary 1 is exactly what was conjectured by Jacobson [7, p. 118].

This argument actually yields a stronger corollary. Let k be the field with p elements, R any k-algebra, and S a faithfully flat extension of R. An R-algebra A' is called an *R-form of A split by S* if $A' \otimes_R S \simeq A \otimes_k S$. Then we have

COROLLARY 2. *The R-forms of A split by S are in one-to-one correspondence with the R-forms of L split by S.* ▮

COROLLARY 3. *If k is perfect, L has no nontrivial forms. More generally, each form of L is split by some purely inseparable extension of k with exponent one.*

Proof. It suffices to prove the corresponding statements for A, and there the result is obvious from the proof of Proposition 3. ▮

COROLLARY 4. *Let A' be a form of A, and L' its derivation algebra. Then*

$$\mathbf{Aut}\, A' \xrightarrow{\sim} \mathbf{Aut}\, L'.$$

Proof. The map is defined just as for A. To prove it is an isomorphism we may as in Proposition 2 make a base extension to K; but there the Corollary reduces to the Theorem. ▮

5.4. (Remarks). 1. For $p \geqslant 3$ the Lie algebra $L \otimes K$ is simple [7, p. 109]; hence all forms of L are simple Lie algebras.

2. Since L is a derivation algebra, it has a p-power map making it a restricted Lie algebra. By the previous remark all $L \otimes R$ are centerless for $p \geqslant 3$, and the p-power map on a centerless Lie algebra is unique [8, p. 23].

Hence all automorphisms of $L \otimes R$ preserve the p-power map. It follows that the forms of L *qua* Lie algebra are the same as the forms of L *qua* restricted Lie algebra.

3. Just as faithfully flat descent can replace Galois descent, we see here that it can replace the rather more elaborate Hopf algebra descent developed in [1].

Acknowledgment

The author wishes to thank M. E. Sweedler for bringing this problem to his attention. He also acknowledges support from an NRC-ONR Research Associateship.

References

1. H. P. Allen and M. E. Sweedler, A theory of linear descent based upon Hopf algebraic techniques, *J. Algebra* **12** (1969), 242–294.
2. M. Artin, "Commutative Rings," M.I.T. mimeographed notes, 1966.
3. N. Bourbaki, "Algèbre Commutative," Chap. 3 and 4, Hermann, Paris, 1961.
4. M. Demazure, A. Grothendieck, *et al.* "Schémas en Groupes: Séminaire de Géométrie Algébrique 1963–1964," Inst. Hautes Études Sci., Paris.
5. P. Gabriel, *et al.*, Groupes Algébriques: Séminaire Heidelberg–Strasbourg, 1965–1966.
6. A. Grothendieck, Technique de Descente et Théorèmes d'Existence en Géométrie Algébrique, I, Sém. Bourbaki, No. 190, 1959–1960.
7. N. Jacobson, Classes of restricted Lie algebras of characteristic p, II, *Duke Math. J.* **10** (1943), 107–121.
8. N. Jacobson, Restricted Lie algebras of characteristic p, *Trans. Amer. Math. Soc.* **50** (1941), 15–25.
9. S. Shatz, Galois theory, *in* "Proc. Battelle Conference on Categorical Algebra" (Seattle, Wash., 1968), Springer Lecture Notes, Springer-Verlag, New York/Berlin, to appear.
10. M. E. Sweedler, The Hopf algebra of an algebra applied to field theory, *J. Algebra* **8** (1968), 262–276.