Graduate Texts in Mathematics

William C. Waterhouse

Introduction to Affine Group Schemes

Springer—Verlag
New York Heidelberg Berlin
World Publishing Corporation Beijing China

William C. Waterhouse

Introduction to Affine Group Schemes

Springer-Verlag

New York Heidelberg Berlin

World Publishing Corporation,Beijing,China

William C. Waterhouse
The Pennsylvania State University
Department of Mathematics
215 McAllister Building
University Park, Pennsylvania 16802
USA

AMS Subject Classifications: 14L15, 16A24, 20Gxx

Library of Congress Cataloging in Publication Data

Waterhouse, William C
Introduction to affine group schemes.

(Graduate texts in mathematics ; 66)
Bibliography: p.
Includes indexes.
1. Group schemes (Mathematics) I. Title.
II. Series.
QA564.W37 512'.2 79-12231

Reprinted in China by World Publishing Corporation
For distribution and sale in the People's Republic of China only
只限在中华人民共和国发行

ISBN 0-387-90421-2 Springer-Verlag New York
ISBN 3-540-90421-2 Springer-Verlag Berlin Heidelberg
ISBN 7-5062-0096-1 World Publishing Corporation China

Preface

Ah Love! Could you and I with Him conspire
To grasp this sorry Scheme of things entire!

Khayyam

People investigating algebraic groups have studied the same objects in many different guises. My first goal thus has been to take three different viewpoints and demonstrate how they offer complementary intuitive insight into the subject. In Part I we begin with a functorial idea, discussing some familiar processes for constructing groups. These turn out to be equivalent to the ring-theoretic objects called Hopf algebras, with which we can then construct new examples. Study of their representations shows that they are closely related to groups of matrices, and closed sets in matrix space give us a geometric picture of some of the objects involved.

This interplay of methods continues as we turn to specific results. In Part II, a geometric idea (connectedness) and one from classical matrix theory (Jordan decomposition) blend with the study of separable algebras. In Part III, a notion of differential prompted by the theory of Lie groups is used to prove the absence of nilpotents in certain Hopf algebras. The ring-theoretic work on faithful flatness in Part IV turns out to give the true explanation for the behavior of quotient group functors. Finally, the material is connected with other parts of algebra in Part V, which shows how twisted forms of any algebraic structure are governed by its automorphism group scheme.

I have tried hard to keep the book introductory. There is no prerequisite beyond a training in algebra including tensor products and Galois theory. Some scattered additional results (which most readers may know) are included in an appendix. The theory over base rings is treated only when it is no harder than over fields. Background material is generally kept in the background: affine group schemes appear on the first page and are never far from the center of attention. Topics from algebra or geometry are explained as needed, but no attempt is made to treat them fully. Much supplementary information is relegated to the exercises placed after each chapter, some of which have substantial hints and can be viewed as an extension of the text.

There are also several sections labelled "Vista," each pointing out a large area on which the text there borders. Though non-affine objects are excluded from the text, for example, there is a heuristic discussion of schemes after the introduction of Spec *A* with its topology. There was obviously not enough room for a full classification of semisimple groups, but the results are sketched at one point where the question naturally arises, and at the end of the book is a list of works for further reading. Topics like formal groups and invariant theory, which need (and have) books of their own, are discussed just enough to indicate some connection between them and what the reader will have seen here.

It remains only for me to acknowledge some of my many debts in this area, beginning literally with thanks to the National Science Foundation for support during some of my work. There is of course no claim that the book contains anything substantially new, and most of the material can be found in the work by Demazure and Gabriel. My presentation has also been influenced by other books and articles, and (in Chapter 17) by mimeographed notes of M. Artin. But I personally learned much of this subject from lectures by P. Russell, M. Sweedler, and J. Tate; I have consciously adopted some of their ideas, and doubtless have reproduced many others.

Contents

Part V
Descent Theory

PART I

THE BASIC SUBJECT MATTER

Affine Group Schemes 1

1.1 What We Are Talking About

If R is any ring (commutative with 1), the 2×2 matrices with entries in R and determinant 1 form a group $\mathbf{SL}_2(R)$ under matrix multiplication. This is a familiar process for constructing a group from a ring. Another such process is $\mathbf{GL}_2$, where $\mathbf{GL}_2(R)$ is the group of all 2×2 matrices with invertible determinant. Similarly we can form $\mathbf{SL}_n$ and $\mathbf{GL}_n$. In particular there is $\mathbf{GL}_1$, denoted by the special symbol $\mathbf{G}_m$; this is the *multiplicative group*, with $\mathbf{G}_m(R)$ the set of invertible elements of R. It suggests the still simpler example $\mathbf{G}_a$, the *additive group*: $\mathbf{G}_a(R)$ is just R itself under addition. Orthogonal groups are another common type; we can, for instance, get a group by taking all 2×2 matrices M over R satisfying $MM^t = I$. A little less familiar is $\boldsymbol{\mu}_n$, the nth *roots of unity*: if we set $\boldsymbol{\mu}_n(R) = \{x \in R \mid x^n = 1\}$, we get a group under multiplication. All these are examples of affine group schemes.

Another group naturally occurring is the set of all invertible matrices commuting with a given matrix, say with $\begin{pmatrix} 1 & \sqrt{2} \\ \sqrt{3} & 4 \end{pmatrix}$. But as it stands this is nonsense, because we don't know how to multiply elements of a general ring by $\sqrt{2}$. (We *can* multiply by 4, but that is because $4x$ is just $x + x + x + x$.) To make sense of the condition defining the group, we must specify how elements of R are to be multiplied by the constants involved. That is, we must choose some base ring k of constants—here it might be the reals, or at least $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$—and assign groups only to *k-algebras*, rings R with a specified homomorphism $k \to R$. (If we can take $k = \mathbb{Z}$, this is no restriction.) A few unexpected possibilities are also now allowed. If for instance k is the field with p elements (p prime), then the k-algebras are precisely the rings in which $p = 0$. Define then $\boldsymbol{\alpha}_p(R) = \{x \in R \mid x^p = 0\}$. Since $p = 0$ in R, the binomial theorem gives $(x + y)^p = x^p + y^p$, and so $\boldsymbol{\alpha}_p(R)$ is a group under addition.

We can now ask what kind of process is involved in all these examples. To begin with trivialities, we must have a group $G(R)$ for each k-algebra R. Also, if $\varphi\colon R \to S$ is an algebra homomorphism, it induces in every case a group homomorphism $G(R) \to G(S)$; if for instance $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $\mathbf{SL}_2(R)$, then $\begin{pmatrix} \varphi(a) & \varphi(b) \\ \varphi(c) & \varphi(d) \end{pmatrix}$ is in $\mathbf{SL}_2(S)$, since its determinant is $\varphi(a)\varphi(d) - \varphi(b)\varphi(c) = \varphi(ad - bc) = \varphi(1) = 1$. If we then take some $\psi\colon S \to T$, the map induced by $\psi \circ \varphi$ is the composite $G(R) \to G(S) \to G(T)$. Finally and most trivially, the identity map on R induces the identity map on $G(R)$. These elementary properties are summed up by saying that G is a *functor* from k-algebras to groups.

The crucial additional property of our functors is that the elements in $G(R)$ are given by finding the solutions in R of some family of polynomial equations (with coefficients in k). In most of the examples this is obvious; the elements in $\mathbf{SL}_2(R)$, for instance, are given by quadruples a, b, c, d in R satisfying the equation $ad - bc = 1$. Invertibility can be expressed in this manner because an element uniquely determines its inverse if it has one. That is, the elements x in $\mathbf{G}_m(R)$ correspond precisely to the solutions in R of the equation $xy = 1$.

Affine group schemes are exactly the group functors constructed by solution of equations. But such a definition would be technically awkward, since quite different collections of equations can have essentially the same solutions. For this reason the official definition is postponed to the next section, where we translate the condition into something less familiar but more manageable.

1.2 Representable Functors

Suppose we have some family of polynomial equations over k. We can then form a "most general possible" solution of the equations as follows. Take a polynomial ring over k, with one indeterminate for each variable in the equations. Divide by the ideal generated by the relations which the equations express. Call the quotient algebra A. From the equation for $\mathbf{SL}_2$, for instance, we get $A = k[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{11}X_{22} - X_{12}X_{21} - 1)$. The images of the indeterminates in A are now a solution which satisfies only those conditions which follow formally from the given equations.

Let $F(R)$ be given by the solutions of the equations in R. Any k-algebra homomorphism $\varphi\colon A \to R$ will take our "general" solution to a solution in R corresponding to an element of $F(R)$. Since φ is determined by where it sends the indeterminates, we have an injection of $\mathrm{Hom}_k(A, R)$ into $F(R)$. But since the solution is as general as possible, this is actually bijective. Indeed, given any solution in R, we map the polynomial ring to R sending the indeterminates to the components of the given solution; since it *is* a solution, this homomorphism sends the relations to zero and hence factors through the quotient ring A. Thus for this A we have a natural correspondence between $F(R)$ and $\mathrm{Hom}_k(A, R)$.

Every k-algebra A arises in this way from some family of equations. To see this, take any set of generators $\{x_\alpha\}$ for A, and map the polynomial ring $k[\{X_\alpha\}]$ onto A by sending X_α to x_α. Choose polynomials $\{f_i\}$ generating the kernel. (If we have finitely many generators and k noetherian, only finitely many f_i are needed (A.5).) Clearly then $\{x_\alpha\}$ is the "most general possible" solution of the equations $f_i = 0$. In summary:

Theorem. *Let F be a functor from k-algebras to sets. If the elements in $F(R)$ correspond to solutions in R of some family of equations, there is a k-algebra A and a natural correspondence between $F(R)$ and $\mathrm{Hom}_k(A, R)$. The converse also holds.*

Such F are called *representable*, and one says that *A represents F*. We can now officially define an *affine group scheme* over k as a representable functor from k-algebras to groups.

Among our examples, $\mathbf{G}_m$ is represented by $A = k[X, Y]/(XY - 1)$, which we may sometimes write as $k[X, 1/X]$. The equation for $\boldsymbol{\mu}_n$ has as general solution an element indeterminate except for the condition that its nth power be 1; thus $A = k[X]/(X^n - 1)$. The functor $\mathbf{G}_a(R) = \{x \in R \mid \text{no further conditions}\}$ is represented just by the polynomial ring $k[X]$. As with $\mathbf{G}_m$, we have $\mathbf{GL}_2$ represented by $A = k[X_{11}, \ldots, X_{22}, 1/(X_{11}X_{22} - X_{12}X_{21})]$. To repeat the definition, this means that each $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathbf{GL}_2(R)$ corresponds to a homomorphism $A \to R$ (namely, $X_{11} \mapsto a, \ldots, X_{22} \mapsto d$).

1.3 Natural Maps and Yoneda's Lemma

There are natural maps from some of our groups to others. A good example is det: $\mathbf{GL}_2 \to \mathbf{G}_m$. Here for each R the determinant gives a map from $\mathbf{GL}_2(R)$ to $\mathbf{G}_m(R)$, and it is *natural* in the sense that for any $\varphi\colon R \to S$ the diagram

$$\begin{array}{ccc} \mathbf{GL}_2(R) & \longrightarrow & \mathbf{G}_m(R) \\ \big\downarrow & & \big\downarrow \\ \mathbf{GL}_2(S) & \longrightarrow & \mathbf{G}_m(S) \end{array}$$

commutes (i.e., gives the same result either way around). The naturality is obvious, since there is an explicit formula for det involving just polynomials in the matrix entries. The next result (which is true for representable functors on any category) shows that natural maps can arise only from such formulas.

Theorem (Yoneda's Lemma). *Let E and F be (set-valued) functors represented by k-algebras A and B. The natural maps $E \to F$ correspond to k-algebra homomorphisms $B \to A$.*

PROOF. Let $\varphi\colon B \to A$ be given. An element in $E(R)$ corresponds to a homomorphism $A \to R$, and the composition $B \to A \to R$ then defines an element in $F(R)$. This clearly gives a natural map $E \to F$.

Conversely, let $\Phi\colon E \to F$ be a natural map. Inside $E(A)$ is our "most general possible" solution, corresponding to the identity map $\mathrm{id}_A\colon A \to A$. Applying Φ to it, we get an element of $F(A)$, that is, a homomorphism $\varphi\colon B \to A$. Since any element in any $E(R)$ comes from a homomorphism $A \to R$, and

$$\begin{array}{ccc} E(A) & \longrightarrow & E(R) \\ \downarrow & & \downarrow \\ F(A) & \longrightarrow & F(R) \end{array}$$

commutes, it is easy to see that Φ is precisely the map defined from φ in the first step. □

To elucidate the argument, we work it through for the determinant. In $A = k[X_{11}, \ldots, X_{22}, 1/(X_{11}X_{22} - X_{12}X_{21})]$ we compute det of the "most general possible" solution $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}$, getting $X_{11}X_{22} - X_{12}X_{21}$. This, an invertible element of A, determines a homomorphism from $B = k[X, 1/X]$ to A. Thus $\det\colon \mathbf{GL}_2 \to \mathbf{G}_m$ corresponds to the homomorphism $B \to A$ sending X to $X_{11}X_{22} - X_{12}X_{21}$. All this is basically trivial, and only the reversal of direction needs to be noticed: $E \to F$ gives $A \leftarrow B$.

Suppose now also that $\Phi\colon E \to F$ is a natural correspondence, i.e. is bijective for all R. Then $\Phi^{-1}\colon F \to E$ is defined and natural. It therefore corresponds to a homomorphism $\psi\colon A \to B$. In the theorem composites obviously correspond to composites, so $\varphi \circ \psi\colon A \to B \to A$ corresponds to $\mathrm{id} = \Phi^{-1} \circ \Phi\colon E \to F \to E$. Hence $\varphi \circ \psi$ must be id_A. Similarly $\psi \circ \varphi = \mathrm{id}_B$. Thus ψ is φ^{-1}, and φ is an isomorphism.

Corollary. *The map $E \to F$ is a natural correspondence iff $B \to A$ is an isomorphism.*

This shows that the problem mentioned at the end of (1.1) has been overcome. Unlike specific families of equations, two representing algebras cannot give essentially the same functor unless they themselves are essentially the same.

1.4 Hopf Algebras

Our definition of affine group schemes is of mixed nature: we have an algebra A together with group structure on the corresponding functor. Using the Yoneda lemma we can turn that structure into something involving A.

We will need two small facts about representability. The first is obvious: the functor E assigning just one point to every k-algebra R is represented by k itself. Second, suppose that E and F are represented by A and B; then the product

$$(E \times F)(R) = \{\langle e, f\rangle \mid e \in E(R), f \in F(R)\}$$

is represented by $A \otimes_k B$. Indeed, this merely says that homomorphisms $A \otimes B \to R$ correspond to pairs of homomorphisms A, $B \to R$, which is a familiar property of tensor products. We can even generalize slightly. Suppose we have some G represented by C and natural maps $E \to G$, $F \to G$ corresponding to $C \to A$, $C \to B$. Then the *fiber product*

$$(E \times_G F)(R) = \{\langle e, f\rangle \mid e \text{ and } f \text{ have same image in } G(R)\}$$

is represented by $A \otimes_C B$.

Now, what is a group? It is a set Γ together with maps

$$\begin{aligned} \text{mult}&: \Gamma \times \Gamma \to \Gamma \\ \text{unit}&: \{e\} \to \Gamma \\ \text{inv}&: \Gamma \to \Gamma \end{aligned}$$

such that the following diagrams commute:

$$\begin{array}{ccc} \Gamma \times \Gamma \times \Gamma & \xrightarrow{\text{id} \times \text{mult}} & \Gamma \times \Gamma \\ \downarrow{\scriptstyle \text{mult} \times \text{id}} & & \downarrow{\scriptstyle \text{mult}} \\ \Gamma \times \Gamma & \xrightarrow{\text{mult}} & \Gamma \end{array} \qquad \text{(associativity)},$$

$$\begin{array}{ccc} \{e\} \times \Gamma & \xrightarrow{\text{unit} \times \text{id}} & \Gamma \times \Gamma \\ \wr\! \mid & & \downarrow{\scriptstyle \text{mult}} \\ \Gamma & = & \Gamma \end{array} \qquad \text{(left unit)},$$

and

$$\begin{array}{ccc} \Gamma & \xrightarrow{(\text{inv}, \text{id})} & \Gamma \times \Gamma \\ \downarrow & & \downarrow{\scriptstyle \text{mult}} \\ \{e\} & \xrightarrow{\text{unit}} & \Gamma \end{array} \qquad \text{(left inverse)}.$$