Basic Theory

of

Affine Group Schemes

J.S. Milne

Version 1.00
March 11, 2012

This is a modern exposition of the basic theory of affine group schemes. Although the emphasis is on affine group schemes of finite type over a field, we also discuss more general objects: affine group schemes not of finite type; base rings not fields; affine monoids not groups; group schemes not affine, affine supergroup schemes (very briefly); quantum groups (even more briefly). “Basic” means that we do not investigate the detailed structure of reductive groups using root data except in the final survey chapter (which is not yet written). Prerequisites have been held to a minimum: all the reader really needs is a knowledge of some basic commutative algebra and a little of the language of algebraic geometry.

BibTeX information:

```
@misc{milneAGS,
author={Milne, James S.},
title={Basic Theory of Affine Group Schemes},
year={2012},
note={Available at www.jmilne.org/math/}
}
```

v1.00 March 11, 2012, 275 pages.

Please send comments and corrections to me at the address on my website http://www.jmilne.org/math/.

The photo is of the famous laughing Buddha on The Peak That Flew Here, Hangzhou, Zhejiang, China.

Table of Contents

Preface

> *For one who attempts to unravel the story, the problems are as perplexing as a mass of hemp with a thousand loose ends.*
>
> Dream of the Red Chamber, Tsao Hsueh-Chin.

Algebraic groups are groups defined by polynomials. Those that we shall be concerned with in this book can all be realized as groups of matrices. For example, the group of matrices of determinant 1 is an algebraic group, as is the orthogonal group of a symmetric bilinear form. The classification of algebraic groups and the elucidation of their structure were among the great achievements of twentieth century mathematics (Borel, Chevalley, Tits and others, building on the work of the pioneers on Lie groups). Algebraic groups are used in most branches of mathematics, and since the famous work of Hermann Weyl in the 1920s they have also played a vital role in quantum mechanics and other branches of physics (usually as Lie groups).

The goal of the present work is to provide a modern exposition of the basic theory of algebraic groups. It has been clear for fifty years, that in the definition of an algebraic group, the coordinate ring should be allowed to have nilpotent elements,[1] but the standard expositions[2] do not allow this.[3] What we call an affine algebraic group is usually called an affine group scheme of finite type. In recent years, the tannakian duality[4] between algebraic groups and their categories of representations has come to play a role in the theory of algebraic groups similar to that of Pontryagin duality in the theory of locally compact abelian groups. We incorporate this point of view.

Let k be a field. Our approach to affine group schemes is eclectic.[5] There are three main ways viewing affine group schemes over k:

- ◇ as representable functors from the category of k-algebras to groups;
- ◇ as commutative Hopf algebras over k;
- ◇ as groups in the category of schemes over k.

All three points of view are important: the first is the most elementary and natural; the second leads to natural generalizations, for example, affine group schemes in a tensor category and quantum groups; and the third allows one to apply algebraic geometry and to realize

[1] See, for example, Cartier 1962. Without nilpotents the centre of SL_p in characteristic p is visible only through its Lie algebra. Moreover, the standard isomorphism theorems fail (IX, 4.6), and so the intuition provided by group theory is unavailable. While it is true that in characteristic zero all algebraic groups are reduced, this is a theorem *that can only be stated when nilpotents are allowed.*

[2] The only exceptions I know of are Demazure and Gabriel 1970, Waterhouse 1979, and SGA 3.

[3] Worse, much of the expository literature is based, in spirit if not in fact, on the algebraic geometry of Weil's Foundations (Weil 1962). Thus an algebraic group over k is defined to be an algebraic group over some large algebraically closed field together with a k-structure. This leads to a terminology in conflict with that of modern algebraic geometry, in which, for example, the kernel of a homomorphism of algebraic groups over a field k need not be an algebraic group over k. Moreover, it prevents the theory of split reductive groups being developed intrinsically over the base field.

When Borel first introduced algebraic geometry into the study of algebraic groups in the 1950s, Weil's foundations were they only ones available to him. When he wrote his influential book Borel 1969, he persisted in using Weil's approach to algebraic geometry, and subsequent authors have followed him.

[4] Strictly, this should be called the "duality of Tannaka, Krein, Milman, Hochschild, Grothendieck, Saavedra Rivano, Deligne, et al.," but "tannakian duality" is shorter. In his Récoltes et Semailles, 1985-86, 18.3.2, Grothendieck argues that "Galois-Poincaré" would be more appropriate than "Tannaka" .

[5] Eclectic: Designating, of, or belonging to a class of ancient philosophers who selected from various schools of thought such doctrines as pleased them. (OED).

affine group schemes as examples of groups in the category of all schemes. We emphasize the first point of view, but make use of all three. We also use a fourth: affine group schemes are the Tannaka duals of certain tensor categories.

Terminology

For readers familiar with the old terminology, as used for example in Borel 1969, 1991, we point out some differences with our terminology, which is based on that of modern (post-1960) algebraic geometry.

- ◇ We allow our rings to have nilpotents, i.e., we don't require that our algebraic groups be reduced.
- ◇ For an algebraic group G over k and an extension field K, $G(K)$ denotes the points of G with coordinates in K and G_K denotes the algebraic group over K obtained from G by extension of the base field.
- ◇ We **do not** identify an algebraic group G with its k-points $G(k)$, even when the ground field k is algebraically closed. Thus, a subgroup of an algebraic group G is an algebraic subgroup, not an abstract subgroup of $G(k)$.
- ◇ An algebraic group G over a field k is intrinsically an object over k, and not an object over some algebraically closed field together with a k-structure. Thus, for example, a homomorphism of algebraic groups over k is truly a homomorphism over k, and not over some large algebraically closed field. In particular, the kernel of such a homomorphism is an algebraic subgroup over k. Also, we say that an algebraic group over k is simple, split, etc. when it simple, split, etc. as an algebraic group over k, not over some large algebraically closed field. When we want to say that G is simple over k and remains simple over all fields containing k, we say that G is geometrically (or absolutely) simple.

Beyond its greater simplicity and its consistency with the terminology of modern algebraic geometry, there is another reason for replacing the old terminology with the new: for the study of group schemes over bases other than fields there is no old terminology.

Notations; terminology

We use the standard (Bourbaki) notations: $\mathbb{N} = \{0,1,2,\ldots\}$; $\mathbb{Z}$ = ring of integers; $\mathbb{Q}$ = field of rational numbers; $\mathbb{R}$ = field of real numbers; $\mathbb{C}$ = field of complex numbers; $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ = field with p elements, p a prime number. For integers m and n, $m|n$ means that m divides n, i.e., $n \in m\mathbb{Z}$. Throughout the notes, p is a prime number, i.e., $p = 2,3,5,\ldots$.

Throughout k is the ground ring (always commutative, and often a field), and R always denotes a commutative k-algebra. Unadorned tensor products are over k. Notations from commutative algebra are as in my primer CA (see below). When k is a field, k^{sep} denotes a separable algebraic closure of k and k^{al} an algebraic closure of k. The dual $\mathrm{Hom}_{k\text{-lin}}(V,k)$ of a k-module V is denoted by $V^{\vee}$. The transpose of a matrix M is denoted by M^t.

We use the terms "morphism of functors" and "natural transformation of functors" interchangeably. For functors F and F' from the same category, we say that "a homomorphism $F(X) \to F'(X)$ is natural in X" when we have a family of such maps, indexed by the objects X of the category, forming a natural transformation $F \to F'$. For a natural transformation $\alpha\colon F \to F'$, we often write α_X for the morphism $\alpha(X)\colon F(X) \to F'(X)$. When its action on morphisms is obvious, we usually describe a functor F by giving its action

$X \rightsquigarrow F(X)$ on objects. Categories are required to be locally small (i.e., the morphisms between any two objects form a set), except for the category $\mathsf{A}^{\vee}$ of functors $\mathsf{A} \to \mathsf{Set}$. A diagram $A \to B \rightrightarrows C$ is said to be ***exact*** if the first arrow is the equalizer of the pair of arrows; in particular, this means that $A \to B$ is a monomorphism (cf. EGA I, Chap. 0, 1.4).

Here is a list of categories:

Category	**Objects**	**Page**
Alg_k	commutative k-algebras	
$\mathsf{A}^{\vee}$	functors $\mathsf{A} \to \mathsf{Set}$	
$\mathsf{Comod}(C)$	finite-dimensional comodules over C	p. 118
Grp	(abstract) groups	
$\mathsf{Rep}(G)$	finite-dimensional representations of G	p. 112
$\mathsf{Rep}(\mathfrak{g})$	finite-dimensional representations of $\mathfrak{g}$	
Set	sets	
Vec_k	finite-dimensional vector spaces over k	

Throughout the work, we often abbreviate names. In the following table, we list the shortened name and the page on which we begin using it.

Shortened name	**Full name**	**Page**
algebraic group	affine algebraic group	p. 28
algebraic monoid	affine algebraic monoid	p. 28
bialgebra	commutative bi-algebra	p. 37
Hopf algebra	commutative Hopf algebra	p. 37
group scheme	affine group scheme	p. 75
algebraic group scheme	affine algebraic group scheme	p. 75
group variety	affine group variety	p. 75
subgroup	affine subgroup	p. 109
representation	linear representation	p. 113

When working with schemes of finite type over a field, we typically ignore the nonclosed points. In other words, we work with max specs rather than prime specs, and "point" means "closed point".

We use the following conventions:

$X \subset Y$ X is a subset of Y (not necessarily proper);
$X \overset{\text{def}}{=} Y$ X is defined to be Y, or equals Y by definition;
$X \approx Y$ X is isomorphic to Y;
$X \simeq Y$ X and Y are canonically isomorphic (or there is a given or unique isomorphism);

Passages designed to prevent the reader from falling into a possibly fatal error are signalled by putting the symbol ☠ in the margin.

ASIDES may be skipped; NOTES should be skipped (they are mainly reminders to the author). There is some repetition which will be removed in later versions.

Prerequisites

Although the theory of algebraic groups is part of algebraic geometry, most people who use it are not algebraic geometers, and so I have made a major effort to keep the prerequisites to a minimum. The reader needs to know the algebra usually taught in first-year graduate courses (and in some advanced undergraduate courses), plus the basic commutative algebra to be found in my primer CA. Familiarity with the terminology of algebraic geometry, either varieties or schemes, will be helpful.

References

In addition to the references listed at the end (and in footnotes), I shall refer to the following of my notes (available on my website):

CA A Primer of Commutative Algebra (v2.22, 2011).
GT Group Theory (v3.11, 2011).
FT Fields and Galois Theory (v4.22, 2011).
AG Algebraic Geometry (v5.22, 2012).
CFT Class Field Theory (v4.01, 2011).

The links to CA, GT, FT, and AG in the pdf file will work if the files are placed in the same directory.

Also, I use the following abbreviations:

Bourbaki A Bourbaki, Algèbre.
Bourbaki AC Bourbaki, Algèbre Commutative (I–IV 1985; V–VI 1975; VIII–IX 1983; X 1998).
Bourbaki LIE Bourbaki, Groupes et Algèbres de Lie (I 1972; II–III 1972; IV–VI 1981).
DG Demazure and Gabriel, Groupes Algébriques, Tome I, 1970.
EGA Eléments de Géométrie Algébrique, Grothendieck (avec Dieudonné).
SGA 3 Schémas en Groupes (Séminaire de Géométrie Algébrique, 1962-64, Demazure, Grothendieck, et al.); 2011 edition.
monnnnn http://mathoverflow.net/questions/nnnnn/

Sources

I list some of the works which I have found particularly useful in writing this book, and which may be useful also to the reader: Demazure and Gabriel 1970; Serre 1993; Springer 1998; Waterhouse 1979.

Acknowledgements

The writing of these notes began when I taught a course at CMS, Zhejiang University, Hangzhou in Spring, 2005. I thank the Scientific Committee and Faculty of CMS for the invitation to lecture at CMS, and those attending the lectures, especially Ding Zhiguo, Han Gang, Liu Gongxiang, Sun Shenghao, Xie Zhizhang, Yang Tian, Zhou Yangmei, and Munir Ahmed, for their questions and comments during the course.

I thank the following for providing comments and corrections for earlier versions of these notes: Brian Conrad, Darij Grinberg, Lucio Guerberoff, Florian Herzig, Timo Keller, Chu-Wee Lim, Victor Petrov, David Vogan, Jonathan Wang, Xiandong Wang.

Introductory overview

Loosely speaking, an algebraic group over a field k is a group defined by polynomials. Before giving the precise definition in Chapter I, we look at some examples of algebraic groups.

Consider the group $\mathrm{SL}_n(k)$ of $n \times n$ matrices of determinant 1 with entries in a field k. The determinant of a matrix (a_{ij}) is a polynomial in the entries a_{ij} of the matrix, namely,

$$\det(a_{ij}) = \sum\nolimits_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad (S_n = \text{symmetric group}),$$

and so $\mathrm{SL}_n(k)$ is the subset of $M_n(k) = k^{n^2}$ defined by the polynomial condition $\det(a_{ij}) = 1$. The entries of the product of two matrices are polynomials in the entries of the two matrices, namely,

$$(a_{ij})(b_{ij}) = (c_{ij}) \quad \text{with } c_{ij} = a_{i1}b_{1j} + \cdots + a_{in}b_{nj},$$

and Cramer's rule realizes the entries of the inverse of a matrix with determinant 1 as polynomials in the entries of the matrix,[6] and so $\mathrm{SL}_n(k)$ is an algebraic group (called the ***special linear group***). The group $\mathrm{GL}_n(k)$ of $n \times n$ matrices with nonzero determinant is also an algebraic group (called the ***general linear group***) because its elements can be identified with the n^2+1-tuples $((a_{ij})_{1 \le i,j \le n}, d)$ such that $\det(a_{ij}) \cdot d = 1$. More generally, for a finite-dimensional vector space V, we define $\mathrm{GL}(V)$ (resp. $\mathrm{SL}(V)$) to be the group of automorphisms of V (resp. automorphisms with determinant 1). These are again algebraic groups.

In order to simplify the statements, we assume for the remainder of this section that k is a field of characteristic zero.

The building blocks

We describe the five types of algebraic groups from which all others can be constructed by successive extensions: the finite algebraic groups, the abelian varieties, the semisimple algebraic groups, the tori, and the unipotent groups.

FINITE ALGEBRAIC GROUPS

Every finite group can be realized as an algebraic group, and even as an algebraic subgroup of some $\mathrm{GL}_n(k)$. Let σ be a permutation of $\{1,\ldots,n\}$ and let $I(\sigma)$ be the matrix obtained from the identity matrix by using σ to permute the rows. For any $n \times n$ matrix A, the matrix $I(\sigma)A$ is obtained from A by using σ to permute the rows. In particular, if σ and σ' are two permutations, then $I(\sigma)I(\sigma') = I(\sigma\sigma')$. Thus, the matrices $I(\sigma)$ realize S_n as a subgroup

[6] Alternatively, according to the Cayley-Hamilton theorem, an $n \times n$ matrix A satisfies a polynomial equation

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n = 0$$

with $a_n = (-1)^n \det(A)$, and so

$$A \cdot (A^{n-1} + a_1 A^{n-2} + \cdots + a_{n-1} I) = (-1)^{n+1} \det(A) \cdot I.$$

If $\det(A) \neq 0$, then

$$(-1)^{n+1}(A^{n-1} + a_1 A^{n-2} + \cdots + a_{n-1} I)/\det(A)$$

is an inverse for A.

of GL_n. Since every finite group is a subgroup of some S_n, this shows that every finite group can be realized as a subgroup of GL_n, which is automatically defined by polynomial conditions. Therefore the theory of algebraic groups includes the theory of finite groups. The algebraic groups defined in this way by finite groups are called ***constant finite*** algebraic groups.

More generally, to give an étale finite algebraic group over a field is the same as giving a finite group together with a continuous action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$ — all finite algebraic groups in characteristic zero are of this type.

An algebraic group is ***connected*** if has no nontrivial finite quotient group.

Abelian varieties

Abelian varieties are connected algebraic groups that are projective when considered as algebraic varieties. An abelian variety of dimension 1 is an elliptic curve, which can be described by a homogeneous equation

$$Y^2Z = X^3 + bXZ^2 + cZ^3.$$

Therefore, the theory of algebraic groups includes the theory of abelian varieties. We shall ignore this aspect of the theory. In fact, we shall study only algebraic groups that are ***affine*** when considered as algebraic varieties. These are exactly the algebraic groups that can be realized as a closed subgroup of some GL_n, and, for this reason, are often called ***linear*** algebraic groups.

Semisimple algebraic groups

A connected affine algebraic group G is ***simple*** if it is not commutative and has no normal algebraic subgroups other than 1 and G, and it is ***almost-simple***[7] if its centre Z is finite and G/Z is simple. For example, SL_n is almost-simple for $n > 1$ because its centre

$$Z = \left\{ \begin{pmatrix} \zeta & & 0 \\ & \ddots & \\ 0 & & \zeta \end{pmatrix} \;\middle|\; \zeta^n = 1 \right\}$$

is finite, and the quotient $\mathrm{PSL}_n = \mathrm{SL}_n/Z$ is simple.

An ***isogeny*** of connected algebraic groups is a surjective homomorphism $G \to H$ with finite kernel. Two connected algebraic groups H_1 and H_2 are ***isogenous*** if there exist isogenies

$$H_1 \leftarrow G \to H_2.$$

This is an equivalence relations. When k is algebraically closed, every almost-simple algebraic group is isogenous to exactly one algebraic group on the following list:

A_n $(n \geq 1)$, the special linear group SL_{n+1};
B_n $(n \geq 2)$, the special orthogonal group SO_{2n+1} consisting of all $2n+1 \times 2n+1$ matrices A such that $A^t \cdot A = I$ and $\det(A) = 1$;
C_n $(n \geq 3)$, the symplectic group Sp_{2n} consisting of all invertible $2n \times 2n$ matrices A such that $A^t \cdot J \cdot A = J$ where $J = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$;
D_n $(n \geq 4)$, the special orthogonal group SO_{2n};

[7] Other authors say "quasi-simple" or "simple".

E_6, E_7, E_8, F_4, G_2 the five exceptional groups.

We say that an algebraic group G is an ***almost-direct product*** of its algebraic subgroups $G_1, \ldots, G_r$ if the map

$$(g_1, \ldots, g_r) \mapsto g_1 \cdots g_r \colon G_1 \times \cdots \times G_r \to G$$

is an isogeny. In particular, this means that each G_i is a normal subgroup of G and that the G_i commute with each other. For example,

$$G = \mathrm{SL}_2 \times \mathrm{SL}_2 / N, \quad N = \{(I, I), (-I, -I)\} \tag{1}$$

is the almost-direct product of SL_2 and SL_2, but it is not a direct product of two almost-simple algebraic groups.

A connected algebraic group is ***semisimple*** if it is an almost-direct product of almost-simple subgroups. For example, the group G in (1) is semisimple.

Groups of multiplicative type; algebraic tori

An affine algebraic subgroup T of $\mathrm{GL}(V)$ is said to be of ***multiplicative type*** if, over k^{al}, there exists a basis of V relative to which T is contained in the group $\mathbb{D}_n$ of all diagonal matrices

$$\begin{pmatrix} * & 0 & \cdots & 0 & 0 \\ 0 & * & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & * & 0 \\ 0 & 0 & \cdots & 0 & * \end{pmatrix}.$$

In particular, the elements of an algebraic torus are semisimple endomorphisms of V. A ***torus*** is a connected algebraic group of multiplicative type.

Unipotent groups

An affine algebraic subgroup G of $\mathrm{GL}(V)$ is ***unipotent*** if there exists a basis of V relative to which G is contained in the group $\mathbb{U}_n$ of all $n \times n$ matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * & * \\ 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}. \tag{2}$$

In particular, the elements of a unipotent group are unipotent endomorphisms of V.

Extensions

We now look at some algebraic groups that are nontrivial extensions of groups of the above types.

Solvable groups

An affine algebraic group G is ***solvable*** if there exists a sequence of affine algebraic subgroups

$$G = G_0 \supset \cdots \supset G_i \supset \cdots \supset G_n = 1$$

such that each G_{i+1} is normal in G_i and G_i/G_{i+1} is commutative. For example, the group $\mathbb{U}_n$ is solvable, and the group $\mathbb{T}_n$ of upper triangular $n \times n$ matrices is solvable because it contains $\mathbb{U}_n$ as a normal subgroup with quotient isomorphic to $\mathbb{D}_n$. When k is algebraically closed, a connected subgroup G of $\mathrm{GL}(V)$ is solvable if and only if there exists a basis of V relative to which G is contained in $\mathbb{T}_n$ (Lie-Kolchin theorem XVI, 4.7).

Reductive groups

A connected affine algebraic group is ***reductive*** if it has no connected normal unipotent subgroup other than 1. According to the table below, such groups are the extensions of semisimple groups by tori. For example, GL_n is reductive because it is an extension of the simple group PGL_n by the torus $\mathbb{G}_m$,

$$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1.$$

Here $\mathbb{G}_m = \mathrm{GL}_1$ and the first map identifies it with the group of nonzero scalar matrices in GL_n.

Nonconnected groups

We give some examples of naturally occurring nonconnected algebraic groups.

The orthogonal group. For an integer $n \geq 1$, let O_n denote the group of $n \times n$ matrices A such that $A^t A = I$. Then $\det(A)^2 = \det(A^t)\det(A) = 1$, and so $\det(A) \in \{\pm 1\}$. The matrix $\mathrm{diag}(-1, 1, \ldots)$ lies in O_n and has determinant -1, and so O_n is not connected: it contains $\mathrm{SO}_n \overset{\text{def}}{=} \mathrm{Ker}\left(\mathrm{O}_n \xrightarrow{\det} \{\pm 1\}\right)$ as a normal algebraic subgroup of index 2 with quotient the constant finite group $\{\pm 1\}$.

The monomial matrices. Let M be the ***group of monomial matrices***, i.e., those with exactly one nonzero element in each row and each column. This group contains both the algebraic subgroup $\mathbb{D}_n$ and the algebraic subgroup S_n of permutation matrices. Moreover, for any diagonal matrix $\mathrm{diag}(a_1, \ldots, a_n)$,

$$I(\sigma) \cdot \mathrm{diag}(a_1, \ldots, a_n) \cdot I(\sigma)^{-1} = \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)}). \tag{3}$$

As $M = \mathbb{D}_n \cdot S_n$, this shows that $\mathbb{D}_n$ is normal in M. Clearly $\mathbb{D} \cap S_n = 1$, and so M is the semi-direct product

$$M = \mathbb{D}_n \rtimes_\theta S_n$$

where $\theta \colon S_n \to \mathrm{Aut}(\mathbb{D}_n)$ sends σ to the automorphism in (3).

Summary

Recall that we are assuming that the base field k has characteristic zero. Every algebraic group has a composition series whose quotients are respectively a finite group, an abelian variety, a semisimple group, a torus, and a unipotent group. More precisely:

(a) An algebraic group G contains a unique normal connected algebraic subgroup G° such that G/G° is a finite étale algebraic group (see XIII, 3.7).

(b) A connected algebraic group G contains a largest[8] normal connected affine algebraic subgroup N; the quotient G/N is an abelian variety (Barsotti, Chevalley, Rosenlicht).[9]

(c) A connected affine algebraic group G contains a largest normal connected solvable algebraic subgroup N (see XVII, §1); the quotient G/N semisimple.

(d) A connected solvable affine algebraic group G contains a largest connected normal unipotent subgroup N; the quotient G/N is a torus (see XVII, 1.2; XVI, 5.1).

In the following tables, the group at left has a subnormal series whose quotients are the groups at right.

General algebraic group	
general ●	
│	finite étale
connected ●	
│	abelian variety
connected affine ●	
│	semisimple
solvable ●	
│	torus
unipotent ●	
│	unipotent
$\{1\}$ ●	

Affine algebraic group	
affine ●	
│	finite étale
connected ●	
│	semisimple
solvable ●	
│	torus
unipotent ●	
│	unipotent
$\{1\}$ ●	

Reductive algebraic groups	
reductive ●	
│	semisimple
torus ●	
│	torus
$\{1\}$ ●	

When k is perfect of characteristic $p \neq 0$ and G is smooth, the same statements hold. However, when k is not perfect the situation becomes more complicated. For example, the algebraic subgroup N in (b) need not be smooth even when G is, and its formation need not commute with extension of the base field. Similarly, a connected affine algebraic group G without a normal connected unipotent subgroup may acquire such a subgroup after an extension of the base field — in this case, the group G is said to be pseudo-reductive (not reductive).

Exercises

EXERCISE 0.1 Let $f(X,Y) \in \mathbb{R}[X,Y]$. Show that if $f(x,e^{x}) = 0$ for all $x \in \mathbb{R}$, then f is zero (as an element of $\mathbb{R}[X,Y]$). Hence the subset $\{(x,e^{x}) \mid x \in \mathbb{R}\}$ of $\mathbb{R}^{2}$ is not the zero-set of a family of polynomials.

[8] "largest" = "unique maximal"

[9] The theorem is proved in Barsotti 1955b, Rosenlicht 1956, and Chevalley 1960. Rosenlicht (ibid.) credits Chevalley with an earlier proof. A modern exposition can be found in Conrad 2002.

EXERCISE 0.2 Let T be a commutative subgroup of $\mathrm{GL}(V)$ consisting of diagonalizable endomorphisms. Show that there exists a basis for V relative to which $T \subset \mathbb{D}_n$.

EXERCISE 0.3 Let ϕ be a positive definite bilinear form on a real vector space V, and let $\mathrm{SO}(\phi)$ be the algebraic subgroup of $\mathrm{SL}(V)$ of maps α such that $\phi(\alpha x, \alpha y) = \phi(x, y)$ for all $x, y \in V$. Show that every element of $\mathrm{SO}(\phi)$ is semisimple (but $\mathrm{SO}(\phi)$ is not diagonalizable because it is not commutative).

EXERCISE 0.4 Let k be a field of characteristic zero. Show that every element of $\mathrm{GL}_n(k)$ of finite order is semisimple. (Hence the group of permutation matrices in $\mathrm{GL}_n(k)$ consists of semisimple elements, but it is not diagonalizable because it is not commutative).

CHAPTER I

Definition of an affine group

What is an affine algebraic group? For example, what is SL_n? We know what $\mathrm{SL}_n(R)$ is for any commutative ring R, namely, it is the group of $n \times n$ matrices with entries in R and determinant 1. Moreover, we know that a homomorphism $R \to R'$ of rings defines a homomorphism of groups $\mathrm{SL}_n(R) \to \mathrm{SL}_n(R')$. So what is SL_n without the "(R)"? Obviously, it is a functor from the category of rings to groups. Essentially, this is our definition together with the requirement that the functor be "defined by polynomials".

Throughout this chapter, k is a commutative ring.

1 Motivating discussion

We first explain how a set of polynomials defines a functor. Let S be a subset of $k[X_1,\ldots,X_n]$. For any k-algebra R, the zero-set of S in R^n is

$$S(R) = \{(a_1,\ldots,a_n) \in R^n \mid f(a_1,\ldots,a_n) = 0 \text{ for all } f \in S\}.$$

A homomorphism of k-algebras $R \to R'$ defines a map $S(R) \to S(R')$, and these maps make $R \rightsquigarrow S(R)$ into a functor from the category of k-algebras to the category of sets.

This suggests that we define an affine algebraic group over k to be a functor $\mathsf{Alg}_k \to \mathsf{Grp}$ that is isomorphic (as a functor to sets) to the functor defined by a finite set of polynomials in a finite number of symbols. For example, $R \rightsquigarrow \mathrm{SL}_n(R)$ satisfies this condition because it is isomorphic to the functor defined by the polynomial $\det(X_{ij}) - 1$ where

$$\det(X_{ij}) = \sum\nolimits_{\sigma \in S_n} \mathrm{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in k[X_{11}, X_{12}, \ldots, X_{nn}]. \tag{4}$$

The condition that a functor is defined by polynomials is very restrictive.

Let S be a subset of $k[X_1,\ldots,X_n]$. The ideal $\mathfrak{a}$ generated by S consists of the finite sums

$$\sum g_i f_i, \quad g_i \in k[X_1,\ldots,X_n], \quad f_i \in S.$$

Clearly S and $\mathfrak{a}$ have the same zero-sets for every k-algebra R. Let $A = k[X_1,\ldots,X_n]/\mathfrak{a}$. A homomorphism $A \to R$ is determined by the images a_i of the X_i, and the n-tuples $(a_1,\ldots,a_n)$ that arise from homomorphisms are exactly those in the zero-set of $\mathfrak{a}$. Therefore the functor $R \rightsquigarrow \mathfrak{a}(R)$ sending a k-algebra R to the zero-set of $\mathfrak{a}$ in R^n is canonically isomorphic to the functor

$$R \rightsquigarrow \mathrm{Hom}_{k\text{-alg}}(A, R).$$

Since the k-algebras that can be expressed in the form $k[X_1,\ldots,X_n]/\mathfrak{a}$ are exactly the finitely generated k-algebras, we conclude that the functors $\mathsf{Alg}_k \to \mathsf{Set}$ defined by some set of polynomials in a finite number of symbols are exactly the functors $R \rightsquigarrow \mathrm{Hom}_{k\text{-alg}}(A,R)$ defined by some finitely generated k-algebra A; moreover, the functor can be defined by a *finite* set of polynomials if and only if the k-algebra is *finitely presented.*[1]

This suggests that we define an affine algebraic group over k to be a functor $\mathsf{Alg}_k \to \mathsf{Grp}$ that is isomorphic (as a functor to sets) to the functor $R \rightsquigarrow \mathrm{Hom}_{k\text{-alg}}(A,R)$ defined by a finitely presented k-algebra A. Before making this more precise, we review some category theory.

2 Some category theory

Let A be a category. An object A of A defines a functor

$$h^A\colon \mathsf{A} \to \mathsf{Set} \quad \text{by} \quad \begin{cases} h^A(R) = \mathrm{Hom}(A,R), & R \in \mathrm{ob}(\mathsf{A}), \\ h^A(f)(g) = f \circ g, & f\colon R \to R', \quad g \in h^A(R) = \mathrm{Hom}(A,R). \end{cases}$$

A morphism $\alpha\colon A' \to A$ of objects defines a map $f \mapsto f \circ \alpha\colon h^A(R) \to h^{A'}(R)$ which is natural in R (i.e., it is a natural transformation of functors $h^A \to h^{A'}$). Thus $A \rightsquigarrow h^A$ is a contravariant functor $\mathsf{A} \to \mathsf{A}^\vee$. Symbolically, $h^A = \mathrm{Hom}(A,-)$.

The Yoneda lemma

Let $F\colon \mathsf{A} \to \mathsf{Set}$ be a functor from A to the category of sets, and let A be an object of A. The Yoneda lemma says that to give a natural transformation $h^A \to F$ is the same as giving an element of $F(A)$. Certainly, a natural transformation $T\colon h^A \to F$ defines an element

$$a_T = T_A(\mathrm{id}_A)$$

of $F(A)$. Conversely, an element a of $F(A)$ defines a map

$$h^A(R) \to F(R), \quad f \mapsto F(f)(a),$$

for each R in A. The map is natural in R, and so this family of maps is a natural transformation

$$T_a\colon h^A \to F, \quad (T_a)_R(f) = F(f)(a).$$

2.1 (Yoneda lemma) *The maps $T \mapsto a_T$ and $a \mapsto T_a$ are inverse bijections*

$$\mathrm{Nat}(h^A, F) \simeq F(A) \tag{5}$$

This bijection is natural in both A and F (i.e., it is an isomorphism of bifunctors).

[1] Recall (CA 3.11) that a k-algebra A is finitely presented if it is isomorphic to the quotient of a polynomial algebra $k[X_1,\ldots,X_n]$ by a *finitely generated* ideal. The Hilbert basis theorem (CA 3.6) says that, when k is noetherian, every finitely generated k-algebra is finitely presented.

PROOF. Let T be a natural transformation $h^A \to F$. To say that T is a natural transformation means that a morphism $f: A \to R$ defines a commutative diagram

$$\begin{tikzcd}
h^A(A) \arrow[r, "h^A(f)"] \arrow[d, "T_A"] & h^A(R) \arrow[d, "T_R"] & \mathrm{id}_A \arrow[rr, mapsto] \arrow[d, mapsto] & & f \arrow[d, mapsto] \\
F(A) \arrow[r, "F(f)"] & F(R) & a_T \arrow[r, mapsto] & F(f)(a_T), & T_R(f).
\end{tikzcd}$$

The commutativity of the diagram implies that

$$F(f)(a_T) = T_R(f).$$

Therefore $T_{a_T} = T$. On the other hand, for $a \in F(A)$,

$$(T_a)_A(\mathrm{id}_A) = F(\mathrm{id}_A)(a) = a,$$

and so $a_{T_a} = a$. We have shown that the maps are inverse bijections, and the proof of the naturality is left as an (easy) exercise for the reader. □

2.2 When we take $F = h^B$ in the lemma, we find that

$$\mathrm{Nat}(h^A, h^B) \simeq \mathrm{Hom}(B, A).$$

In other words, the contravariant functor $A \rightsquigarrow h^A: \mathsf{A} \to \mathsf{A}^\vee$ is fully faithful. In particular, a diagram in A commutes if and only if its image under the functor $A \rightsquigarrow h^A$ commutes in $\mathsf{A}^\vee$.

2.3 There is a contravariant version of the Yoneda lemma. For an object A of A, let h_A be the contravariant functor

$$R \rightsquigarrow \mathrm{Hom}(R, A): \mathsf{A} \to \mathsf{Set}.$$

For every contravariant functor $F: \mathsf{A} \to \mathsf{Set}$, the map

$$T \mapsto T_A(\mathrm{id}_A): \mathrm{Nat}(h_A, F) \to F(A)$$

is a bijection, natural in both A and F (apply 2.1 to $\mathsf{A}^{\mathrm{opp}}$). In particular, for any objects A, B of A,

$$\mathrm{Nat}(h_A, h_B) \simeq \mathrm{Hom}(A, B).$$

Representable functors

2.4 A functor $F: \mathsf{A} \to \mathsf{Set}$ is said to be ***representable*** if it is isomorphic to h^A for some object A. A pair (A, a), $a \in F(A)$, is said to ***represent*** F if $T_a: h^A \to F$ is an isomorphism. Note that, if F is representable, say $F \approx h^A$, then the choice of an isomorphism $T: h^A \to F$ determines an element $a_T \in F(A)$ such that (A, a_T) represents F, and so we sometimes say that (A, T) represents F. The Yoneda lemma says that $A \rightsquigarrow h^A$ is a contravariant equivalence from A onto the category of representable functors $A \to \mathsf{Set}$.

2.5 Let F_1 and F_2 be functors $\mathsf{A} \to \mathsf{Set}$. In general, the natural transformations $F_1 \to F_2$ will form a proper class (not a set), but the Yoneda lemma shows that $\mathrm{Hom}(F_1, F_2)$ is a set when F_1 is representable.

Similarly, a contravariant functor is said to be representable if it is isomorphic to h_A for some object A.

Groups and monoids in categories

Throughout this subsection, C is a category with finite products. In particular, there exists a final object $*$ (the empty product) and canonical isomorphisms

$$S\times * \xrightarrow{\simeq} S \xleftarrow{\simeq} *\times S$$

for every object S of C. For example, the category Set has finite products — every one-element set is a final object.

Recall that a monoid is a set G together with an associative binary operation $m\colon G\times G\to G$ and a neutral element e. A homomorphism $(G,m,e)\to(G',m',e')$ of monoids is a map $\varphi\colon G\to G'$ such that $\varphi\circ m = m\circ(\varphi\times\varphi)$ and $\varphi(e)=e'$.

Definition 2.6 A ***monoid in*** C is a triple (G,m,e) consisting of an object G and morphisms $m\colon G\times G\to G$ and $e\colon *\to G$ satisfying the two conditions:

(a) (associativity) the following diagram commutes

$$\begin{tikzcd}
 & G\times G \arrow[dr, "m"] & \\
G\times G\times G \arrow[ur, "\mathrm{id}\times m"] \arrow[dr, "m\times\mathrm{id}"'] & & G \\
 & G\times G \arrow[ur, "m"'] &
\end{tikzcd} \tag{6}$$

(b) (existence of an identity) both of the composites below are the identity map

$$G\simeq *\times G \xrightarrow{e\times\mathrm{id}} G\times G \xrightarrow{m} G$$
$$G\simeq G\times * \xrightarrow{\mathrm{id}\times e} G\times G \xrightarrow{m} G.$$

For example, a monoid in Set is just a monoid in the usual sense.

Recall that a group is a set G together with an associative binary operation $m\colon G\times G\to G$ for which there exist a neutral element and inverses. The neutral element and the inverses are then unique — for example, the neutral element e is the only element such that $e^2=e$. A homomorphism $(G,m)\to(G',m')$ of groups is a map $\varphi\colon G\to G'$ such that $\varphi\circ m = m\circ(\varphi\times\varphi)$; it is automatic that $\varphi(e)=e'$.

Definition 2.7 A ***group in*** C is a pair (G,m) consisting of an object G of C and a morphism $m\colon G\times G\to G$ such that there exist morphisms $e\colon *\to G$ and $\mathrm{inv}\colon G\to G$ for which (G,m,e) is a monoid and the diagram

$$\begin{tikzcd}
G \arrow[r, "(\mathrm{inv},\mathrm{id})"] \arrow[d] & G\times G \arrow[d, "m"] & G \arrow[l, "(\mathrm{id},\mathrm{inv})"'] \arrow[d] \\
* \arrow[r, "e"] & G & *. \arrow[l, "e"']
\end{tikzcd} \tag{7}$$

commutes. Here $(\mathrm{inv},\mathrm{id})$ denotes the morphism whose projections on the factors are inv and id.

When they exist, the morphisms e and inv are unique.

2.8 A morphism $m: G \times G \to G$ defines a natural transformation $h_m: h_{G\times G} \to h_G$. As $h_{G\times G} \simeq h_G \times h_G$, we can regard h_m as a natural transformation $h_G \times h_G \to h_G$. Because the functor $G \rightsquigarrow h_G$ is fully faithful (Yoneda lemma 2.3), we see that (G,m) is a group in C if and only if (h_G, h_m) is a group in the category of contravariant functors $\mathsf{C} \to \mathsf{Set}$.

We make this more explicit.

2.9 For objects G and S in C, let $G(S) = \mathrm{Hom}(S,G) = h_G(S)$. By definition, $*(S)$ is a one-element set. A pair (G,m) is a group in C if and only if, for every S in C, the map $m(S): G(S) \times G(S) \to G(S)$ is a group structure on $G(S)$. Similarly a triple (M,m,e) is a monoid in C if and only if, for every S in C, the map $m(S): M(S) \times M(S) \to M(S)$ makes $M(S)$ into a monoid with neutral element the image of $e(S): *(S) \to M(S)$.

2.10 We shall be particularly interested in this when C is the category of representable functors $\mathsf{A} \to \mathsf{Set}$, where A is a category with finite coproducts. Then C has finite products, and a pair (G,m) is a group in C if and only if, for every R in A, $m(R): G(R) \times G(R) \to G(R)$ is a group structure on $G(R)$ (because $R \rightsquigarrow h^R: \mathsf{A}^{\mathrm{opp}} \to \mathsf{C}$ is essentially surjective). Similarly, a triple (M,m,e) is a monoid in C if and only if, for every R in A, the map $m(R): M(R) \times M(R) \to M(R)$ makes $M(R)$ into a monoid with neutral element the image of $e(R): *(R) \to M(R)$.

3 Affine groups

Recall (CA §8) that the tensor product of two k-algebras A_1 and A_2 is their direct sum (coproduct) in the category Alg_k. Explicitly, if $f_1: A_1 \to R$ and $f_2: A_2 \to R$ are homomorphisms of k-algebras, then there is a unique homomorphism $(f_1, f_2): A_1 \otimes A_2 \to R$ such that $(f_1,f_2)(a_1 \otimes 1) = f_1(a_1)$ and $(f_1,f_2)(1 \otimes a_2) = f_2(a_2)$ for all $a_1 \in A_1$ and $a_2 \in A_2$:

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[dr, "f_1"'] & A_1 \otimes A_2 \arrow[d, dashed, "{(f_1,f_2)}"] & A_2 \arrow[l] \arrow[dl, "f_2"] \\
 & R. &
\end{tikzcd} \tag{8}$$

In other words,

$$h^{A_1 \otimes A_2} \simeq h^{A_1} \times h^{A_2}. \tag{9}$$

It follows that the category of representable functors $\mathsf{Alg}_k \to \mathsf{Set}$ has finite products.

DEFINITION 3.1 An ***affine group*** over k is a representable functor $G: \mathsf{Alg}_k \to \mathsf{Set}$ together with a natural transformation $m: G \times G \to G$ such that, for all k-algebras R,

$$m(R): G(R) \times G(R) \to G(R)$$

is a group structure on $G(R)$. If G is represented by a finitely presented k-algebra, then it is called an ***affine algebraic group***. A ***homomorphism*** $G \to H$ of affine groups over k is a natural transformation preserving the group structures.

Thus, a homomorphism $G \to H$ of affine groups is a family of homomorphisms

$$\alpha(R)\colon G(R) \to H(R)$$

of groups, indexed by the k-algebras R, such that, for every homomorphism $\phi\colon R \to R'$ of k-algebras, the diagram

$$\begin{tikzcd} G(R) \arrow[r, "\alpha(R)"] \arrow[d, "G(\phi)"] & H(R) \arrow[d, "H(\phi)"] \\ G(R') \arrow[r, "\alpha(R')"] & H(R') \end{tikzcd}$$

commutes.

To give an affine group over k amounts to giving a functor $R \rightsquigarrow (G(R), m(R))$ from k-algebras to groups satisfying the following condition: there exists a k-algebra A and "universal" element $a \in G(A)$ such that the maps

$$f \mapsto f(a)\colon \mathrm{Hom}(A,R) \to G(R)$$

are bijections for all R.

Remarks

3.2 The Yoneda lemma shows that if G and H are affine groups over k, then $\mathrm{Hom}(G,H)$ is a set (see 2.5). Therefore, the affine groups over k form a locally small category, with the affine algebraic groups as a full subcategory.

3.3 The pair (A,a) representing G is uniquely determined up to a unique isomorphism by G. Any such A is called the ***coordinate ring*** of A, and is denoted $\mathcal{O}(G)$, and $a \in G(A)$ is called the ***universal element***. We shall see below that there is a even canonical choice for it. It is often convenient to regard the coordinate ring (A,a) of an affine group G as a k-algebra A together with an isomorphism $\alpha\colon h^A \to G$ of functors (cf. 2.4).

3.4 In the language of §2, a pair (G,m) is an affine group over k if and only if (G,m) is a group in the category of representable functors $\mathsf{Alg}_k \to \mathsf{Set}$ (see 2.10).

3.5 Let (G,m) be an affine group over k. Because m is a natural transformation, the map $G(R) \to G(R')$ defined by a homomorphism of k-algebras $R \to R'$ is a group homomorphism. Therefore, (G,m) defines a functor $\mathsf{Alg}_k \to \mathsf{Grp}$. Conversely, a functor $G\colon \mathsf{Alg}_k \to \mathsf{Grp}$ whose underlying set-valued functor is representable defines an affine group.

NOTES It is possible to write down a set of necessary and sufficient conditions in order for a functor $\mathsf{Aff}_k \to \mathsf{Grp}$ to be representable, i.e., to be an affine group. The conditions can be verified for the automorphism functors of some algebraic varieties. See Matsumura and Oort 1967. Sometime I'll add a discussion of when the automorphism functor of an affine algebraic group over a field k is itself an affine algebraic group. See Hochschild and Mostow 1969 in the case that k is algebraically closed of characteristic zero.

Examples

3.6 Let $\mathbb{G}_a$ be the functor sending a k-algebra R to itself considered as an additive group, i.e., $\mathbb{G}_a(R) = (R,+)$. For each element r of a k-algebra R there is a unique k-algebra homomorphism $k[X] \to R$ sending X to r. Therefore $\mathbb{G}_a$ is represented by $(k[X],X)$, and so $\mathbb{G}_a$ is an affine algebraic group with coordinate ring $\mathcal{O}(\mathbb{G}_a) = k[X]$. It is called the ***additive group***.

3.7 Let GL_n be the functor sending a k-algebra R to the group of invertible $n \times n$ matrices with entries in R, and let

$$A = \frac{k[X_{11}, X_{12}, \ldots, X_{nn}, Y]}{(\det(X_{ij}) \cdot Y - 1)} = k[x_{11}, x_{12}, \ldots, x_{nn}, y].$$

The matrix $x = (x_{ij})_{1 \le i,j \le n}$ with entries in A is invertible because the equation $\det(x_{ij}) \cdot y = 1$ implies that $\det(x_{ij}) \in A^{\times}$. For each invertible matrix $C = (c_{ij})_{1 \le i,j \le n}$ with entries in a k-algebra R, there is a unique homomorphism $A \to R$ sending x to C. Therefore GL_n is an affine algebraic group with coordinate ring $\mathcal{O}(\mathrm{GL}_n) = A$.

The canonical coordinate ring of an affine group

Let $\mathbb{A}^1$ be the functor sending a k-algebra R to its underlying set,

$$\mathbb{A}^1 \colon \mathsf{Alg}_k \to \mathsf{Set}, \quad (R, \times, +, 1) \rightsquigarrow R.$$

Let $G \colon \mathsf{Alg}_k \to \mathsf{Grp}$ be a group-valued functor, and let $G_0 = (\text{forget}) \circ G$ be the underlying set-valued functor. Define A to be the set of natural transformations from G_0 to $\mathbb{A}^1$,

$$A = \mathrm{Nat}(G_0, \mathbb{A}^1).$$

Thus an element f of A is a family of maps of sets

$$f_R \colon G_0(R) \to R, \quad R \text{ a } k\text{-algebra},$$

such that, for every homomorphism of k-algebras $\phi \colon R \to R'$, the diagram

$$\begin{tikzcd} G_0(R) \arrow[r, "f_R"] \arrow[d, "G_0(\phi)"] & R \arrow[d, "\phi"] \\ G_0(R') \arrow[r, "f_{R'}"] & R' \end{tikzcd}$$

commutes. For $f, f' \in A$ and $g \in G_0(R)$, define

$$(f \pm f')_R(g) = f_R(g) \pm f'_R(g)$$
$$(ff')_R(g) = f_R(g) f'_R(g).$$

With these operations, A becomes a commutative ring, and even a k-algebra because each $c \in k$ defines a natural transformation

$$c_R \colon G_0(R) \to R, \quad c_R(g) = c \text{ for all } g \in G_0(R).$$

An element $g \in G_0(R)$ defines a homomorphism $f \mapsto f_R(g) \colon A \to R$ of k-algebras. In this way, we get a natural transformation $\alpha \colon G_0 \to h^A$ of set-valued functors.

PROPOSITION 3.8 *The functor G is an affine group if and only if α is an isomorphism (in which case it is an affine algebraic group if and only if A is finitely generated).*

PROOF. If α is an isomorphism, then certainly G_0 is representable (and so G is an affine group). Conversely, suppose that $G_0 = h^B$. Then

$$A \overset{\text{def}}{=} \mathrm{Nat}(G_0, \mathbb{A}^1) = \mathrm{Nat}(h^B, \mathbb{A}^1) \overset{\text{Yoneda}}{\simeq} \mathbb{A}^1(B) = B.$$

Thus $A \simeq B$ as abelian groups, and one checks directly that this is an isomorphism of k-algebras and that $\alpha\colon h^B \to h^A$ is the natural transformation defined by the isomorphism. Therefore α is an isomorphism. This proves the statement (and the parenthetical statement is obvious). □

Thus, for an affine group (G,m), $\mathcal{O}(G) \overset{\text{def}}{=} \mathrm{Hom}(G, \mathbb{A}^1)$ is a (canonical) coordinate ring.

Affine groups and algebras with a comultiplication

A ***comultiplication*** on a k-algebra A is a k-algebra homomorphism $\Delta\colon A \to A \otimes A$. Let Δ be a comultiplication on the k-algebra A. For every k-algebra R, the map,

$$f_1, f_2 \mapsto f_1 \cdot f_2 \overset{\text{def}}{=} (f_1, f_2) \circ \Delta\colon h^A(R) \times h^A(R) \to h^A(R), \qquad (10)$$

is a binary operation on $h^A(R)$, which is natural in R. If this is a group structure for every R, then h^A together with this multiplication is an affine group.

Conversely, let $G\colon \mathsf{Alg}_k \to \mathsf{Set}$ be a representable functor, and let $m\colon G \times G \to G$ be a natural transformation. Let (A,a) represent G, so that $T_a\colon h^A \simeq G$. Then

$$G \times G \simeq h^A \times h^A \overset{(9)}{\simeq} h^{A \otimes A},$$

and m corresponds (by the Yoneda lemma) to a comultiplication $\Delta\colon A \to A \otimes A$. Clearly, (G,m) is an affine group if and only if the map (10) defined by Δ is a group structure for all R.

SUMMARY 3.9 It is essentially the same[2] to give

(a) an affine group (G,m) over k, or

(b) a functor $G\colon \mathsf{Alg}_k \to \mathsf{Grp}$ such that the underlying set-valued functor is representable, or

(c) a k-algebra A together with a comultiplication $\Delta\colon A \to A \otimes A$ such that the map (10) defined by Δ is a group structure on $h^A(R)$ for all R,

We discussed the equivalence of (a) and (b) in (3.5). To pass from (a) to (c), take A to be $\mathrm{Hom}(\mathbb{A}^1, G)$ endowed with the comultiplication $\Delta\colon A \to A \otimes A$ corresponding (by the Yoneda lemma) to m. To pass from (c) to (a), take G to be h^A endowed with the multiplication $m\colon G \times G \to G$ defined by Δ.

[2] More precisely, there are canonical equivalences of categories.

EXAMPLE 3.10 Let M be a group, written multiplicatively. The free k-module with basis M becomes a k-algebra with the multiplication

$$\left(\sum_m a_m m\right)\left(\sum_n b_n n\right) = \sum_{m,n} a_m b_n mn,$$

called the ***group algebra*** of M over k. Assume that M is commutative, so that $k[M]$ is a commutative k-algebra, and let $\Delta\colon k[M] \to k[M] \otimes k[M]$ be the comultiplication with

$$\Delta(m) = m \otimes m \quad (m \in M).$$

Then $h^{k[M]}(R) \simeq \mathrm{Hom}_{\mathrm{group}}(M, R^{\times})$, and Δ defines on $h^{k[M]}(R)$ its natural group structure:

$$(f_1 \cdot f_2)(m) = f_1(m) \cdot f_2(m).$$

Therefore (A, Δ) defines an affine group.

Remarks

3.11 Let $\Delta\colon A \to A \otimes A$ be a homomorphism of k-algebras. In (II, 5.1) we shall see that (A, Δ) satisfies (3.9c) if and only if there exist homomorphisms $\epsilon\colon A \to k$ and $S\colon A \to A$ such that certain diagrams commute. In particular, this will give a finite definition of “affine group” that does not require quantifying over all k-algebras R.

3.12 Let G be an affine algebraic group, and Δ be the comultiplication on its group ring $\mathcal{O}(G)$. Then

$$\mathcal{O}(G) \approx k[X_1, \ldots, X_m]/(f_1, \ldots, f_n)$$

for some m and some polynomials $f_1, \ldots, f_n$. The functor $h^{\mathcal{O}(G)}\colon \mathsf{Alg}_k \to \mathsf{Grp}$ is that defined by the set of polynomials $\{f_1, \ldots, f_n\}$. The tensor product

$$k[X_1, \ldots, X_n] \otimes k[X_1, \ldots, X_n]$$

is a polynomial ring in the $2n$ symbols $X_1 \otimes 1, \ldots, X_n \otimes 1, 1 \otimes X_1, \ldots, 1 \otimes X_n$. Therefore Δ, and hence the multiplication on the groups $h^{\mathcal{O}(G)}(R)$, is also be described by polynomials, namely, by any set of representatives for the polynomials $\Delta(X_1), \ldots, \Delta(X_m)$.

3.13 Let G be an affine group, and let A be its coordinate ring. When we regard A as $\mathrm{Hom}(G, \mathbb{A}^1)$, an element $f \in A$ is a family of maps $f_R\colon G(R) \to R$ (of sets) natural in R. On the other hand, when we regard A as a k-algebra representing G, an element $g \in G(R)$ is a homomorphism of k-algebras $g\colon A \to R$. The two points of views are related by the equation

$$f_R(g) = g(f), \quad f \in A, \quad g \in G(R). \tag{11}$$

Moreover,

$$(\Delta f)_R(g_1, g_2) = f_R(g_1 \cdot g_2). \tag{12}$$

According to the Yoneda lemma, a homomorphism $u\colon G \to H$ defines a homomorphism of k-algebras $u^{\natural}\colon \mathcal{O}(H) \to \mathcal{O}(G)$. Explicitly,

$$(u^{\natural} f)_R(g) = f_R(u_R g), \quad f \in \mathcal{O}(H), \quad g \in G(R). \tag{13}$$

4 Affine monoids

An ***affine monoid*** over k is a representable functor $M\colon \mathsf{Alg}_k \to \mathsf{Set}$ together with natural transformations $m\colon M\times M \to M$ and $e\colon * \to M$ such that, for all k-algebras R, the triple $(M(R), m(R), e(R))$ is a monoid. Equivalently, it is a functor M from Alg_k to the category of monoids such that the underlying set-valued functor is representable. If M is represented by a finitely presented k-algebra, then it is called an affine algebraic monoid.

To give an affine monoid amounts to giving a k-algebra A together with homomorphisms $\Delta\colon A \to A\otimes A$ and $\epsilon\colon A \to k$ such that, for each k-algebra R, Δ makes $h^A(R)$ into a monoid with identity element $A \xrightarrow{\epsilon} k \longrightarrow R$ (cf. 3.9).

EXAMPLE 4.1 For a k-module V, let End_V be the functor

$$R \rightsquigarrow (\mathrm{End}_{R\text{-lin}}(R\otimes_k V), \circ).$$

When V is finitely generated and projective, End_V is represented as a functor to sets by $\mathrm{Sym}(V\otimes_k V^\vee)$, and so it is an algebraic monoid (apply IV, 1.6, below). When V is free, the choice of a basis $e_1,\ldots,e_n$ for V, defines an isomorphism of End_V with the functor

$$R \rightsquigarrow (M_n(R), \times) \quad \text{(multiplicative monoid of } n\times n \text{ matrices)},$$

which is represented by the polynomial ring $k[X_{11}, X_{12}, \ldots, X_{nn}]$.

For a monoid M, the set $M^\times$ of elements in M with inverses is a group (the largest subgroup of M).

PROPOSITION 4.2 *For any affine monoid M over k, the functor $R \rightsquigarrow M(R)^\times$ is an affine group $M^\times$ over k; when M is algebraic, so also is $M^\times$.*

PROOF. For an abstract monoid M, let $M_1 = \{(a,b)\in M\times M \mid ab = 1\}$; then

$$M^\times \simeq \{((a,b),(a',b')) \in M_1\times M_1 \mid a = b'\}.$$

This shows that $M^\times$ can be constructed from M by using only fibred products:

$$\begin{tikzcd} M_1 \arrow[r] \arrow[d] & \{1\} \arrow[d] & M^\times \arrow[r] \arrow[d] & M_1 \arrow[d, "(a{,}b)\mapsto b"] \\ M\times M \arrow[r, "(a{,}b)\mapsto ab"] & M & M_1 \arrow[r, "(a{,}b)\mapsto a"] & M. \end{tikzcd}$$

It follows that, for an affine monoid M, the functor $R \rightsquigarrow M(R)^\times$ can be obtained from M by forming fibre products, which shows that it is representable (see V, §2 below). □

EXAMPLE 4.3 Let B be an associative k-algebra B with identity (not necessarily commutative), and consider the functor sending a k-algebra R to $R\otimes B$ regarded as a multiplicative monoid. When B is free of finite rank n as a k-module, the choice of a basis for B identifies it (as a functor to sets) with $R\mapsto R^n$, which is represented by $k[X_1,\ldots,X_n]$, and so the functor is an affine algebraic monoid. More generally, the functor is an affine algebraic monoid whenever B is finitely generated and projective as a k-module (see IV, 3.2, below). In this case, we let $\mathbb{G}_m^B$ denote the corresponding affine algebraic group

$$R \mapsto (R\otimes B)^\times.$$

If $B = M_n(k)$, then $\mathbb{G}_m^B = \mathrm{GL}_n$.

5 Affine supergroups

The subject of supersymmetry was introduced by the physicists in the 1970s as part of their search for a unified theory of physics consistent with quantum theory and general relativity. Roughly speaking, it is the study of $\mathbb{Z}/2\mathbb{Z}$-graded versions of some of the usual objects of mathematics. We explain briefly how it leads to the notion of an affine "supergroup". Throughout this subsection, k is a field of characteristic zero.

A ***superalgebra*** over a field k is a $\mathbb{Z}/2\mathbb{Z}$-graded associative algebra R over k. In other words, R is an associative k-algebra equipped with a decomposition $R = R_0 \oplus R_1$ (as a k-vector space) such that $k \subset R_0$ and $R_i R_j \subset R_{i+j}$ $(i, j \in \mathbb{Z}/2\mathbb{Z})$. An element a of R is said to be ***even***, and have parity $p(a) = 0$, if it lies in R_0; it is ***odd***, and has parity $p(a) = 1$, if it lies in R_1. The ***homogeneous*** elements of R are those that are either even or odd. A ***homomorphism*** of super k-algebras is a homomorphism of k-algebras preserving the parity of homogeneous elements.

A super k-algebra R is said to be ***commutative*** if $ba = (-1)^{p(a)p(b)}ab$ for all $a, b \in R$. Thus even elements commute with all elements, but for odd elements a, b,

$$ab + ba = 0.$$

The commutative super k-algebra $k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ in the even symbols X_i and the odd symbols Y_i is defined to be the quotient of the k-algebra of noncommuting polynomials in $X_1, \ldots, Y_n$ by the relations

$$X_i X_{i'} = X_{i'} X_i, \quad X_i Y_j = Y_j X_i, \quad Y_j Y_{j'} = -Y_{j'} Y_j, \quad 1 \le i, i' \le m, \quad 1 \le j, j' \le n.$$

When $n = 0$, this is the polynomial ring in the commuting symbols $X_1, \ldots, X_m$, and when $m = 0$, it is the exterior algebra of the vector space with basis $\{Y_1, \ldots, Y_n\}$ provided $2 \neq 0$ in k.

A functor from the category of commutative super k-algebras to groups is an ***affine supergroup*** if it is representable (as a functor to sets) by a commutative super k-algebra. For example, for $m, n \in \mathbb{N}$, let $\mathrm{GL}_{m|n}$ be the functor

$$R \rightsquigarrow \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \middle| \, A \in \mathrm{GL}_m(R_0), \quad B \in M_{m,n}(R_1), \quad C \in M_{n,m}(R_1), \quad D \in \mathrm{GL}_n(R_0) \right\}.$$

It is known that such a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is invertible (Varadarajan 2004, 3.6.1), and so $\mathrm{GL}_{m|n}$ is a functor to groups. It is an affine supergroup because it is represented by the commutative super k-algebra obtained from the commutative super k-algebra

$$k[X_{11}, X_{12}, \ldots, X_{m+n,m+n}, Y, Z]$$

in the even symbols

$$Y, \quad Z, \quad X_{ij} \quad (1 \le i, j \le m, \quad m+1 \le i, j \le m+n)$$

and the odd symbols

$$X_{ij} \quad \text{(remaining pairs } (i, j))$$

by setting

$$Y \cdot (\det(X_{ij})_{1 \le i, j \le m} = 1,$$
$$Z \cdot \det(X_{ij})_{m+1 \le i.j \le m+n} = 1.$$

6 Terminology

From now on "algebraic group" will mean "affine algebraic group" and "algebraic monoid" will mean "affine algebraic monoid".

7 Exercises

EXERCISE I-1 Show that there is no algebraic group G over k such that $G(R)$ has two elements for every k-algebra R.

CHAPTER **II**

Affine Groups and Hopf Algebras

Un principe général: tout calcul relatif aux cogèbres est trivial et incompréhensible.
Serre 1993, p. 39.

In this chapter, we study the extra structure that the coordinate ring of an affine group G acquires from the group structure on G. Throughout k is a commutative ring.

1 Algebras

Recall that an associative algebra over k with identity is a k-module A together with a pair of k-linear maps[1]

$$m\colon A \otimes A \to A \qquad e\colon k \to A$$

satisfying the two conditions:

(a) (associativity) the following diagram commutes

$$\begin{tikzcd} & A \otimes A \arrow[dr, "m"] & \\ A \otimes A \otimes A \arrow[ur, "\mathrm{id} \otimes m"] \arrow[dr, "m \otimes \mathrm{id}"'] & & A \\ & A \otimes A \arrow[ur, "m"'] & \end{tikzcd} \qquad (14)$$

(b) (existence of an identity) both of the composites below are the identity map

$$A \simeq k \otimes A \xrightarrow{e \otimes \mathrm{id}} A \otimes A \xrightarrow{m} A$$
$$A \simeq A \otimes k \xrightarrow{\mathrm{id} \otimes e} A \otimes A \xrightarrow{m} A.$$

On reversing the directions of the arrows, we obtain the notion of a coalgebra.

[1] Warning: I sometimes also use "e" for the neutral element of $G(R)$ (a homomorphism $\mathcal{O}(G) \to R$).

2 Coalgebras

DEFINITION 2.1 A ***co-associative coalgebra*** over k ***with co-identity*** (henceforth, a ***coalgebra*** over k) is a k-module C together with a pair of k-linear maps

$$\Delta: C \to C \otimes C \qquad \epsilon: C \to k$$

satisfying the two conditions:

(a) (co-associativity) the following diagram commutes

$$\begin{tikzcd}
 & C \otimes C \arrow[dr, "\mathrm{id} \otimes \Delta"] & \\
C \arrow[ur, "\Delta"] \arrow[dr, "\Delta"'] & & C \\
 & C \otimes C \arrow[ur, "\Delta \otimes \mathrm{id}"'] &
\end{tikzcd} \tag{15}$$

(b) (co-identity) both of the composites below are the identity map

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\mathrm{id} \otimes \epsilon} C \otimes k \simeq C$$
$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\epsilon \otimes \mathrm{id}} k \otimes C \simeq C.$$

A ***homomorphism of coalgebras*** over k is a k-linear map $f: C \to D$ such that the following diagrams commute

$$\begin{tikzcd}
C \otimes C \arrow[r, "f \otimes f"] & D \otimes D \\
C \arrow[u, "\Delta_C"] \arrow[r, "f"] & D \arrow[u, "\Delta_D"]
\end{tikzcd} \qquad \begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\epsilon_C"] & D \arrow[d, "\epsilon_D"] \\
k \arrow[r, equal] & k
\end{tikzcd} \tag{16}$$

i.e., such that

$$\begin{cases} (f \otimes f) \circ \Delta_C = \Delta_D \circ f \\ \qquad \epsilon_D \circ f = \epsilon_C. \end{cases}$$

2.2 Let (C, Δ, ϵ) be a coalgebra over k. A k-submodule D of C is called a ***sub-coalgebra*** if $\Delta(D) \subset D \otimes D$. Then $(D, \Delta|D, \epsilon|D)$ is a coalgebra (obvious), and the inclusion $D \hookrightarrow C$ is a coalgebra homomorphism.

When A and B are k-algebras, $A \otimes B$ becomes a k-algebra with the multiplication

$$(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'.$$

A similar statement is true for coalgebras.

2.3 Let $(C, \Delta_C, \epsilon_C)$ and $(D, \Delta_D, \epsilon_D)$ be coalgebras over k. Then $C \otimes D$ becomes a coalgebra when $\Delta_{C \otimes D}$ is defined to be the composite

$$C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes D \otimes D \overset{C \otimes t \otimes D}{\simeq} C \otimes D \otimes C \otimes D$$

(t is the ***transposition map*** $c \otimes d \mapsto d \otimes c$) and $\epsilon_{C \otimes D}$ is defined to be the composite

$$C \otimes D \xrightarrow{\epsilon_C \otimes \epsilon_D} k \otimes k \simeq k.$$

In particular, $(C \otimes C, \Delta_{C \otimes C}, \epsilon_{C \otimes C})$ is a coalgebra over k.

3 The duality of algebras and coalgebras

Recall that $V^\vee$ denotes the dual of a k-module V. If V and W are k-modules, then the formula

$$(f \otimes g)(v \otimes w) = f(v) \otimes g(w), \quad f \in V^\vee, g \in W^\vee, v \in V, w \in W,$$

defines a linear map

$$V^\vee \otimes W^\vee \to (V \otimes W)^\vee \tag{17}$$

which is always injective, and is an isomorphism when at least one of V or W is finitely generated and projective (CA 10.8).

Let (C, Δ, ϵ) be a co-associative coalgebra over k with a co-identity. Then $C^\vee$ becomes an associative algebra over k with the multiplication

$$C^\vee \otimes C^\vee \overset{(17)}{\hookrightarrow} (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee$$

and the identity

$$k \simeq k^\vee \xrightarrow{\epsilon^\vee} C^\vee.$$

Let (A, m, e) be an associative algebra over k with an identity such that A is *finitely generated and projective* as a k-module. Then $A^\vee$ becomes a co-associative coalgebra over k with the co-multiplication

$$A^\vee \xrightarrow{m^\vee} (A \otimes A)^\vee \overset{(17)}{\simeq} A^\vee \otimes A^\vee$$

and the co-identity

$$k \simeq k^\vee \xrightarrow{\epsilon^\vee} A^\vee.$$

These statements are proved by applying the functor $^\vee$ to one of the diagrams (14) or (15).

EXAMPLE 3.1 Let X be a set, and let C be the free k-module with basis X. The k-linear maps

$$\begin{aligned} &\Delta: C \to C \otimes C, && \Delta(x) = x \otimes x, && x \in X, \\ &\epsilon: C \to k, && \epsilon(x) = 1, && x \in X, \end{aligned}$$

endow C with the structure of coalgebra over k, because, for an element x of the basis X,

$$\begin{aligned} (\mathrm{id} \otimes \Delta)(\Delta(x)) &= x \otimes (x \otimes x) = (x \otimes x) \otimes x = (\Delta \otimes \mathrm{id})(\Delta(x)), \\ (\epsilon \otimes \mathrm{id})(\Delta(x)) &= 1 \otimes x, \\ (\mathrm{id} \otimes \epsilon)(\Delta(x)) &= x \otimes 1. \end{aligned}$$

The dual algebra $C^\vee$ can be identified with the k-module of maps $X \to k$ endowed with the k-algebra structure

$$\begin{aligned} m(f, g)(x) &= f(x)g(x) \\ e(c)(x) &= cx. \end{aligned}$$

4 Bi-algebras

DEFINITION 4.1 A ***bi-algebra*** over k is a k-module with compatible structures of an associative algebra with identity and of a co-associative coalgebra with co-identity. In detail, a bi-algebra over k is a quintuple (A,m,e,Δ,ϵ) where

(a) (A,m,e) is an associative algebra over k with identity e;
(b) (A,Δ,ϵ) is a co-associative coalgebra over k with co-identity ϵ;
(c) $\Delta\colon A\to A\otimes A$ is a homomorphism of algebras;
(d) $\epsilon\colon A\to k$ is a homomorphism of algebras.

A ***homomorphism*** of bi-algebras $(A,m,\ldots)\to(A',m',\ldots)$ is a k-linear map $A\to A'$ that is both a homomorphism of k-algebras and a homomorphism of k-coalgebras.

The next proposition shows that the notion of a bi-algebra is self dual.

PROPOSITION 4.2 *For a quintuple (A,m,e,Δ,ϵ) satisfying (a) and (b) of (4.1), the following conditions are equivalent:*

(a) *Δ and ϵ are algebra homomorphisms;*
(b) *m and e are coalgebra homomorphisms.*

PROOF Consider the diagrams:

$$\begin{tikzcd}
A\otimes A \arrow[r, "m"] \arrow[d, "\Delta\otimes\Delta"] & A \arrow[r, "\Delta"] & A\otimes A \\
A\otimes A\otimes A\otimes A \arrow[rr, "A\otimes t\otimes A"] & & A\otimes A\otimes A\otimes A \arrow[u, "m\otimes m"']
\end{tikzcd}$$

$$\begin{tikzcd}
A\otimes A & A \arrow[l, "\Delta"'] \\
k\otimes k \arrow[u, "e\otimes e"] & k \arrow[l, "\simeq"'] \arrow[u, "e"]
\end{tikzcd}
\qquad
\begin{tikzcd}
A\otimes A \arrow[r, "m"] \arrow[d, "\epsilon\otimes\epsilon"] & A \arrow[d, "\epsilon"] \\
k\otimes k \arrow[r, "\simeq"] & k
\end{tikzcd}
\qquad
\begin{tikzcd}
 & A \arrow[dr, "\epsilon"] & \\
k \arrow[ur, "e"] \arrow[rr, "\mathrm{id}"] & & k
\end{tikzcd}$$

The first and second diagrams commute if and only if Δ is an algebra homomorphism, and the third and fourth diagrams commute if and only if ϵ is an algebra homomorphism. On the other hand, the first and third diagrams commute if and only if m is a coalgebra homomorphism, and the second and fourth commute if and only if e is a coalgebra homomorphism. Therefore, each of (a) and (b) is equivalent to the commutativity of all four diagrams. □

DEFINITION 4.3 A bi-algebra is said to be ***commutative***, ***finitely generated***, ***finitely presented***, etc., if its underlying algebra is this property.

Note that these notions are not self dual.

DEFINITION 4.4 An ***inversion*** (or ***antipodal map***[2]) for a bi-algebra A is a k-linear map $S\colon A\to A$ such that

[2] Usually shortened to "antipode".

(a) the diagram

$$\begin{tikzcd} A & A \otimes A \arrow[l, "m\circ(S\otimes\mathrm{id})"'] \arrow[r, "m\circ(\mathrm{id}\otimes S)"] & A \\ k \arrow[u, "e"'] & A \arrow[l, "\epsilon"'] \arrow[r, "\epsilon"] \arrow[u, "\Delta"'] & k \arrow[u, "e"'] \end{tikzcd} \tag{18}$$

commutes, i.e.,

$$m \circ (S \otimes \mathrm{id}) \circ \Delta = e \circ \epsilon = m \circ (\mathrm{id} \otimes S) \circ \Delta. \tag{19}$$

and

(b) $S(ab) = S(b)S(a)$ for all $a, b \in A$ and $S(1) = 1$.

When A is commutative, (b) just means that S is a k-algebra homomorphism, and so an inversion of A is a k-algebra homomorphism such that (19) holds.

Aside 4.5 In fact, condition (a) implies condition (b) (Dăscălescu et al. 2001, 4.2.6). Since condition (a) is obviously self-dual, the notion of a Hopf algebra is self-dual. In particular, if $(A, m, e, \Delta, \epsilon)$ is a bi-algebra with inversion S and A is finitely generated and projective as a k-module, then $(A^\vee, \Delta^\vee, \epsilon^\vee, m^\vee, e^\vee)$ is a bi-algebra with inversion $S^\vee$.

Example 4.6 Let X be a monoid, and let $k[X]$ be the free k-module with basis X. The k-linear maps

$$\begin{aligned} m\colon k[X] \otimes k[X] &\to k[X], & m(x \otimes x') &= xx', & x, x' &\in X, \\ e\colon k &\to k[X], & e(c) &= c1_X, & c &\in k, \end{aligned}$$

endow $k[X]$ with the structure of a k-algebra (the ***monoid algebra*** of X over k). When combined with the coalgebra structure in (3.1), this makes $k[X]$ into a bi-algebra over k (i.e., Δ and ϵ are k-algebra homomorphisms). If X is commutative, then $k[X]$ is a commutative bi-algebra. If X is a group, then the map

$$S\colon A \to A, \quad (Sf)(x) = f(x^{-1}), \quad x \in X,$$

is an inversion, because, for x in the basis X,

$$(m \circ (S \otimes \mathrm{id}))(x \otimes x) = 1 = (m \circ (\mathrm{id} \otimes S))(x \otimes x).$$

Proposition 4.7 *Let A and A' be bi-algebras over k. If A and A' admit inversions S and S', then, for any homomorphism $f\colon A \to A'$,*

$$f \circ S = S' \circ f.$$

In particular, a bi-algebra admits at most one inversion.

Proof. For commutative bi-algebras, which is the only case of interest to us, we shall prove this statement in (5.2) below. The general case is proved in Dăscălescu et al. 2001, 4.2.5. □

Definition 4.8 A bi-algebra over k that admits an inversion is called a ***Hopf algebra*** over k. A ***homomorphism*** of Hopf algebras is a homomorphism of bi-algebras.

For example, the group algebra $k[X]$ of a group X is a Hopf algebra (see 4.6).

A sub-bi-algebra B of a Hopf algebra A is a Hopf algebra if and only if it is stable under the (unique) inversion of A, in which case it is called a ***Hopf subalgebra***.

The reader encountering bi-algebras for the first time should do Exercise II-1 below before continuing.

EXAMPLE 4.9 It is possible to define coalgebras, bialgebras, and Hopf algebras in any category with a good notion of a tensor product (see later). For example, let SVec_k be the category of $\mathbb{Z}/2\mathbb{Z}$-graded vector spaces over k (category of super vector spaces). Given two super vector spaces V, W, let $V\hat{\otimes}W$ denote $V\otimes W$ with its natural $\mathbb{Z}/2\mathbb{Z}$-gradation. Let V be a purely odd super vector space (i.e., $V=V_1$). Then the exterior algebra $\bigwedge V$ on V equipped with its natural $\mathbb{Z}/2\mathbb{Z}$-gradation is a superalgebra, i.e., an algebra in SVec_k. The map

$$\Delta\colon V\to\left(\bigwedge V\right)\otimes\left(\bigwedge V\right),\quad v\mapsto v\otimes 1\otimes 1\otimes v,$$

extends to an algebra homomorphism

$$\Delta\colon\bigwedge V\to\left(\bigwedge V\right)\hat{\otimes}\left(\bigwedge V\right).$$

With the obvious co-identity ϵ, $(\bigwedge V,\Delta,\epsilon)$ is a Hopf algebra in SVec_k (see mo84161, MTS).

ASIDE 4.10 To give a k-bi-algebra that is finitely generated and projective as a k-module is the same as giving a pair of k-algebras A and B, both finitely generated and projective as k-modules, together with a nondegenerate k-bilinear pairing

$$\langle\ ,\ \rangle\colon B\times A\to k$$

satisfying compatibility conditions that we leave to the reader to explicate.

5 Affine groups and Hopf algebras

Recall that a commutative bi-algebra over k is a commutative k-algebra A equipped with a coalgebra structure (Δ,ϵ) such that Δ and ϵ are k-algebra homomorphisms.

THEOREM 5.1 *(a) Let A be a k-algebra, and let $\Delta\colon A\to A\otimes A$ and $\epsilon\colon A\to k$ be homomorphisms. Let $M=h^A$, and let $m\colon M\times M\to M$ and $e\colon *\to M$ be the natural transformations defined by Δ and ϵ (here $*$ is the trivial affine monoid represented by k).The triple (M,m,e) is an affine monoid if and only if (A,Δ,ϵ) is a bi-algebra over k.*

(b) Let A be a k-algebra, and let $\Delta\colon A\to A\otimes A$ be a homomorphism. Let $G=h^A$, and let $m\colon G\times G\to G$ be the natural transformation defined by Δ. The pair (G,m) is an affine group if and only if there exists a homomorphism $\epsilon\colon A\to k$ such that (A,Δ,ϵ) is a Hopf algebra.

PROOF. (a) The natural transformations m and e define a monoid structure on $M(R)$ for each k-algebra R if and only if the following diagrams commute:

$$\begin{tikzcd}
M\times M\times M \arrow[r, "\mathrm{id}_M\times m"] \arrow[d, "m\times\mathrm{id}_M"] & M\times M \arrow[d, "m"] & *\times M \arrow[r, "e\times\mathrm{id}_M"] \arrow[dr, "\simeq"'] & M\times M \arrow[d, "m"] & M\times * \arrow[l, "\mathrm{id}_M\times e"'] \arrow[dl, "\simeq"] \\
M\times M \arrow[r, "m"] & M & & M &
\end{tikzcd} \qquad (20)$$

The functor $A \rightsquigarrow h^A$ sends tensor products to products ((9), p. 9), and is fully faithful (I, 19). Therefore these diagrams commute if and only if the diagrams (15) commute.

(b) An affine monoid M is an affine group if and only if there exists a natural transformation $\mathrm{inv}\colon M \to M$ such that

$$\begin{tikzcd} M \arrow[r, "(\mathrm{inv},\mathrm{id})"] \arrow[d] & M \times M \arrow[d, "m"] & M \arrow[l, "(\mathrm{id},\mathrm{inv})"'] \arrow[d] \\ * \arrow[r, "e"] & M & * \arrow[l, "e"'] \end{tikzcd} \tag{21}$$

commutes. Here $(\mathrm{id},\mathrm{inv})$ denotes the morphism whose composites with the projection maps are id and inv. Such a natural transformation corresponds to a k-algebra homomorphism $S\colon A \to A$ such that (18) commutes, i.e., to an inversion for A. □

Thus, as promised in (I, 3.11), we have shown that a pair (A,Δ) is an corresponds to an affine group if and only if there exist homomorphisms ϵ and S making certain diagrams commute.

PROPOSITION 5.2 *Let A and A' be commutative Hopf algebras over k. A k-algebra homomorphism $f\colon A \to A'$ is a homomorphism of Hopf algebras if*

$$(f \otimes f) \circ \Delta = \Delta' \circ f; \tag{22}$$

moreover, then $f \circ S = S' \circ f$ for any inversions S for A and S' for A'.

PROOF. According to (5.1b), $G = (h^A, h^\Delta)$ and $G' = (h^{A'}, h^{\Delta'})$ are affine groups. A k-algebra homomorphism $f\colon A \to A'$ defines a morphism of functors $h^f\colon G \to G'$. If (22) holds, then this morphism sends products to products, and so is a morphism of group-valued functors. Therefore f is a homomorphism of Hopf algebras. As h^f commutes with the operation $g \mapsto g^{-1}$, we have $f \circ S = S' \circ f$. □

COROLLARY 5.3 *For any commutative k-algebra A and homomorphism $\Delta\colon A \to A \otimes A$, there exists at most one pair (ϵ, S) such that $(A, m, e, \Delta, \epsilon)$ is a Hopf algebra and S is an inversion.*

PROOF. Apply (5.2) to the identity map. □

COROLLARY 5.4 *The forgetful functor $(A,\Delta,\epsilon) \rightsquigarrow (A,\Delta)$ is an isomorphism from the category of commutative Hopf algebras over k to the category of pairs (A,Δ) such that (10), p.24, is a group structure on $h^A(R)$ for all k-algebras R.*

PROOF. It follows from (5.1b) and (5.3) that the functor is bijective on objects, and it is obviously bijective on morphisms. □

EXAMPLE 5.5 Let G be the functor sending a k-algebra R to $R \times R \times R$ with the (noncommutative) group structure

$$(x,y,z) \cdot (x',y',z') = (x+x', y+y', z+z'+xy').$$

This is an algebraic group because it is representable by $k[X,Y,Z]$. The map

$$(x,y,z) \mapsto \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

is an injective homomorphism from G into GL_3. As the functor $R \rightsquigarrow R \times R \times R$ also has an obvious commutative group structure (componentwise addition), this shows that the k-algebra $k[X,Y,Z]$ has more than one Hopf algebra structure.

6 Abstract restatement

A commutative bi-algebra is just a monoid in $\mathsf{Alg}_k^{\mathrm{opp}}$ (compare the definitions (I, 2.6, and 2.1).

A commutative Hopf algebra is just a group in $\mathsf{Alg}_k^{\mathrm{opp}}$ (compare the diagrams (7), p.20, and (18), p.33).

By definition, an affine monoid (resp. group) is a monoid (resp. group) in the category of representable functors on Alg_k. Because the functor $A \rightsquigarrow h^A$ is an equivalence from $\mathsf{Alg}_k^{\mathrm{opp}}$ to the category of representable functors on Alg_k (Yoneda lemma I, 2.2), it induces an equivalence from the category of commutative bi-algebras (resp. Hopf algebras) to the category of affine monoids (resp. groups).

7 Commutative affine groups

A monoid or group G commutes if the diagram at left commutes, an algebra A commutes if middle diagram commutes, and a coalgebra or bi-algebra C is ***co-commutative*** if the diagram at right commutes:

$$\begin{tikzcd}
G\times G \arrow[rr, "t"] \arrow[dr, "m"'] & & G\times G \arrow[dl, "m"] & A\otimes A \arrow[rr, "t"] \arrow[dr, "m"'] & & A\otimes A \arrow[dl, "m"] & C\otimes C & & C\otimes C \arrow[ll, "t"'] \\
& G & & & A & & & C \arrow[ul, "\Delta"] \arrow[ur, "\Delta"'] &
\end{tikzcd} \tag{23}$$

In each diagram, t is the transposition map $(x,y) \mapsto (y,x)$ or $x \otimes y \mapsto y \otimes x$.

On comparing the first and third diagrams and applying the Yoneda lemma, we see that an affine monoid or group is commutative if and only if its coordinate ring is co-commutative.

8 Quantum groups

Until the mid-1980s, the only Hopf algebras seriously studied were either commutative or co-commutative. Then Drinfeld and Jimbo independently discovered noncommutative Hopf algebras in the work of physicists, and Drinfeld called them quantum groups. There is, at present, no definition of "quantum group", only examples. Despite the name, a quantum group does not define a functor from the category of noncommutative k-algebras to groups.

One interesting aspect of quantum groups is that, while semisimple algebraic groups can't be deformed (they are determined up to isomorphism by a discrete set of invariants), their Hopf algebras can be. For $q \in k^{\times}$, define A_q to be the free associative (noncommutative) k-algebra on the symbols a, b, c, d modulo the relations

$$\begin{aligned} &ba = qab, \quad bc = cb, \quad ca = qac, \quad dc = qcd, \\ &db = qbd, \quad da = ad + (q - q^{-1})bc, \quad ad = q^{-1}bc = 1. \end{aligned}$$

This becomes a Hopf algebra with Δ defined by

$$\Delta\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ i.e., } \left\{ \begin{array}{lcl} \Delta(a) & = & a \otimes a + b \otimes c \\ \Delta(b) & = & a \otimes b + b \otimes d \\ \Delta(c) & = & c \otimes a + d \otimes c \\ \Delta(d) & = & c \otimes b + d \otimes d \end{array} \right. ,$$

and with suitable maps ϵ and S. When $q = 1$, A_q becomes $\mathcal{O}(\mathrm{SL}_2)$, and so the A_q can be regarded as a one-dimensional family of quantum groups that specializes to SL_2 when $q \to 1$. The algebra A_q is usually referred to as the Hopf algebra of $\mathrm{SL}_q(2)$.

For bi-algebras that are neither commutative nor cocommutative, many statements in this chapter become more difficult to prove, or even false. For example, while it is still true that a bi-algebra admits at most one inversion, the composite of an inversion with itself need not be the identity map (Dăscălescu et al. 2001, 4.27).

9 Terminology

From now on, "bialgebra" will mean "commutative bi-algebra" and "Hopf algebra" will mean "commutative bi-algebra that admits an inversion (antipode)" (necessarily unique). Thus, the notion of a bialgebra is not self dual.[3]

10 Exercises

To avoid possible problems, in the exercises assume k to be a field.

EXERCISE II-1 For a set X, let $R(X)$ be the k-algebra of maps $X \to k$. For a second set Y, let $R(X) \otimes R(Y)$ act on $X \times Y$ by the rule $(f \otimes g)(x, y) = f(x)g(y)$.

(a) Show that the map $R(X) \otimes R(Y) \to R(X \times Y)$ just defined is injective. (Hint: choose a basis f_i for $R(X)$ as a k-vector space, and consider an element $\sum f_i \otimes g_i$.)

(b) Let Γ be a group and define maps

$$\begin{aligned} &\Delta\colon R(\Gamma) \to R(\Gamma \times \Gamma), && (\Delta f)(g, g') = f(gg') \\ &\epsilon\colon R(\Gamma) \to k, && \epsilon f = f(1) \\ &S\colon R(\Gamma) \to R(\Gamma), && (Sf)(g) = f(g^{-1}). \end{aligned}$$

Show that if Δ maps $R(\Gamma)$ into the subring $R(\Gamma) \otimes R(\Gamma)$ of $R(\Gamma \times \Gamma)$, then Δ, ϵ, and S define on $R(\Gamma)$ the structure of a Hopf algebra.

(c) If Γ is finite, show that Δ always maps $R(\Gamma)$ into $R(\Gamma) \otimes R(\Gamma)$.

[3] In the literature, there are different definitions for "Hopf algebra". Bourbaki and his school (Dieudonné, Serre, ...) use "cogèbre" and "bigèbre" for "co-algebra" and "bi-algebra".

EXERCISE II-2 We continue the notations of the last exercise. Let Γ be an arbitrary group. From a homomorphism $\rho\colon\Gamma\to\mathrm{GL}_n(k)$, we obtain a family of functions $g\mapsto\rho(g)_{i,j}$, $1\le i,j\le n$, on G. Let $R'(\Gamma)$ be the k-subspace of $R(\Gamma)$ spanned by the functions arising in this way for varying n. (The elements of $R'(\Gamma)$ are called the ***representative functions*** on Γ.)

(a) Show that $R'(\Gamma)$ is a k-subalgebra of $R(\Gamma)$.

(b) Show that Δ maps $R'(\Gamma)$ into $R'(\Gamma)\otimes R'(\Gamma)$.

(c) Deduce that Δ, ϵ, and S define on $R'(\Gamma)$ the structure of a Hopf algebra.

(Cf. Abe 1980, Chapter 2, §2; Cartier 2007, 3.1.1.)

EXERCISE II-3 Let A be a Hopf algebra. Prove the following statements by interpreting them as statements about affine groups.

(a) $S\circ S=\mathrm{id}_A$.

(b) $\Delta\circ S=t\circ S\otimes S\circ\Delta$ where $t(a\otimes b)=b\otimes a$.

(c) $\epsilon\circ S=\epsilon$.

(d) The map $a\otimes b\mapsto(a\otimes 1)\Delta(b)\colon A\otimes A\to A\otimes A$ is a homomorphism of k-algebras.

Hints: $(a^{-1})^{-1}=e$; $(ab)^{-1}=b^{-1}a^{-1}$; $e^{-1}=e$.

EXERCISE II-4 Verify directly that $\mathcal{O}(\mathbb{G}_a)$ and $\mathcal{O}(\mathrm{GL}_n)$ satisfy the axioms to be a Hopf algebra.

EXERCISE II-5 A subspace V of a k-coalgebra C is a ***coideal*** if $\Delta_C(V)\subset V\otimes C+C\otimes V$ and $\epsilon_C(V)=0$.

(a) Show that the kernel of any homomorphism of coalgebras is a coideal and its image is a sub-coalgebra.

(b) Let V be a coideal in a k-coalgebra C. Show that the quotient vector space C/V has a unique k-coalgebra structure for which $C\to C/V$ is a homomorphism. Show that any homomorphism of k-coalgebras $C\to D$ whose kernel contains V factors uniquely through $C\to C/V$.

(c) Deduce that every homomorphism $f\colon C\to D$ of coalgebras induces an isomorphism of k-coalgebras
$$C/\mathrm{Ker}(f)\to\mathrm{Im}(f).$$

Hint: show that if $f\colon V\to V'$ and $g\colon W\to W'$ are homomorphisms of k-vector spaces, then

$$\mathrm{Ker}(f\otimes g)=\mathrm{Ker}(f)\otimes W+V\otimes\mathrm{Ker}(g).$$

EXERCISE II-6 (cf. Sweedler 1969, 4.3.1). A k-subspace $\mathfrak{a}$ of a k-bialgebra A is a ***bi-ideal*** if it is both an ideal and a co-ideal. When A admits an inversion S, a bi-ideal $\mathfrak{a}$ is a ***Hopf ideal*** if $S(\mathfrak{a})\subset\mathfrak{a}$. In other words, an ideal $\mathfrak{a}\subset A$ is a bi-ideal if

$$\begin{aligned}&\Delta(\mathfrak{a})\subset\mathfrak{a}\otimes A+A\otimes\mathfrak{a}\text{ and}\\&\epsilon(\mathfrak{a})=0,\end{aligned}$$

and it is a Hopf ideal if, in addition,

$$S(\mathfrak{a})\subset\mathfrak{a}.$$

(a) Show that the kernel of any homomorphism of bialgebras (resp. Hopf algebras) is a bi-ideal (resp. Hopf ideal), and that its image is a bialgebra (resp. Hopf algebra).

(b) Let $\mathfrak{a}$ be a bi-ideal in a k-bialgebra A. Show that the quotient vector space $A/\mathfrak{a}$ has a unique k-bialgebra structure for which $A \to A/\mathfrak{a}$ is a homomorphism. Show that any homomorphism of k-bialgebras $A \to B$ whose kernel contains $\mathfrak{a}$ factors uniquely through $A \to A/\mathfrak{a}$. Show that an inversion on A induces an inversion on $A/\mathfrak{a}$ provided that $\mathfrak{a}$ is a Hopf ideal.

(c) Deduce that every homomorphism $f\colon A \to B$ of bialgebras (resp. Hopf algebras) induces an isomorphism of bialgebras (resp. Hopf algebras),

$$A/\operatorname{Ker}(f) \to \operatorname{Im}(f).$$

In this exercise it is not necessary to assume that A is commutative, although it becomes simpler you do, because then it is possible to exploit the relation to affine groups in (5.1).

CHAPTER **III**

Affine Groups and Group Schemes

By definition, affine groups are groups in the category of representable functors $\mathsf{Alg}_k \to \mathsf{Set}$, which, by the Yoneda lemma, is equivalent to the opposite of Alg_k. In this chapter we provide a geometric interpretation of $\mathsf{Alg}_k^{\mathrm{opp}}$ as the category of affine schemes over k. In this way, we realize affine groups as group schemes.

The purpose of this chapter is only to introduce the reader to the language of schemes — we make no serious use of scheme theory in this work. Throughout, k is a ring.

1 The spectrum of a ring

Let A be commutative ring, and let V be the set of prime ideals in A. For an ideal $\mathfrak{a}$ in A, let

$$V(\mathfrak{a}) = \{\mathfrak{p} \in V \mid \mathfrak{p} \supset \mathfrak{a}\}.$$

Clearly,

$$\mathfrak{a} \subset \mathfrak{b} \implies V(\mathfrak{a}) \supset V(\mathfrak{b}).$$

LEMMA 1.1 *There are the following equalities:*

(a) $V(0) = V$; $V(A) = \emptyset$;
(b) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;
(c) *for a family* $(\mathfrak{a}_i)_{i\in I}$ *of ideals,* $V(\sum_{i\in I}\mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$.

PROOF. The first statement is obvious. For (b) note that

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \implies V(\mathfrak{a}\mathfrak{b}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

For the reverse inclusions, observe that if $\mathfrak{p} \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, then there exist an $f \in \mathfrak{a} \smallsetminus \mathfrak{p}$ and a $g \in \mathfrak{b} \smallsetminus \mathfrak{p}$; but then $fg \in \mathfrak{a}\mathfrak{b} \smallsetminus \mathfrak{p}$, and so $\mathfrak{p} \notin V(\mathfrak{a}\mathfrak{b})$. For (c), recall that, by definition, $\sum_{i\in I}\mathfrak{a}_i$ consists of all finite sums of the form $\sum f_i$, $f_i \in \mathfrak{a}_i$. Thus (c) is obvious. □

The lemma shows that the sets $V(\mathfrak{a})$ satisfy the axioms to be the closed sets for a topology on V. This is called the ***Zariski topology***. The set V endowed with the Zariski topology is the ***(prime) spectrum*** $\operatorname{spec}(A)$ of A.

For $f \in A$, the set

$$D(f) = \{\mathfrak{p} \in V \mid f \notin \mathfrak{p}\}$$

is open in V, because it is the complement of $V((f))$. The sets of this form are called the ***principal open subsets*** of V.

For any set S of generators of an ideal $\mathfrak{a}$,

$$V \smallsetminus V(\mathfrak{a}) = \bigcup_{f \in S} D(f)$$

and so the basic open subsets form a base for the topology on V.

By definition, a prime ideal contains a product of elements if and only if it contains one of the elements. Therefore,

$$D(f_1 \cdots f_n) = D(f_1) \cap \cdots \cap D(f_n), \qquad f_1, \ldots, f_n \in A,$$

and so a finite intersection of basic open subsets is again a basic open subset.

Let $\varphi\colon A \to B$ be a homomorphism of commutative rings. For any prime ideal $\mathfrak{p}$ in B, the ideal $\varphi^{-1}(\mathfrak{p})$ is prime because $A/\varphi^{-1}(\mathfrak{p})$ is a subring of the integral domain $B/\mathfrak{p}$. Therefore φ defines a map

$$\operatorname{spec}(\varphi)\colon \operatorname{spec} B \to \operatorname{spec} A, \quad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}),$$

which is continuous because the inverse image of $D(f)$ is $D(\varphi(f))$. In this way, spec becomes a contravariant functor from the category of commutative rings to topological spaces.

A topological space V is said to be ***noetherian*** if every ascending chain of open subsets $U_1 \subset U_2 \subset \cdots$ in V eventually becomes constant; equivalently, if every descending chain of closed subsets eventually becomes constant. A topological space is ***irreducible*** if it is nonempty and not the union of two proper closed subsets. Every noetherian topological space V can be expressed as the union of a finite collection I of irreducible closed subsets,

$$V = \bigcup \{W \mid W \in I\};$$

among such collections I there is only one that is irredundant in the sense that there are no inclusions among its elements (CA 12.10). The elements of this I are called the ***irreducible components*** of V.

Let A be a ring, and let $V = \operatorname{spec}(A)$. For a closed subset W of V, let

$$I(W) = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in W\}.$$

Then $IV(\mathfrak{a}) = \bigcap\{\mathfrak{p} \mid \mathfrak{p} \supset \mathfrak{a}\}$, which is the radical of $\mathfrak{a}$ (CA 2.4). On the other hand, $VI(W) = W$, and so the map $\mathfrak{a} \mapsto V(\mathfrak{a})$ defines a one-to-one correspondence between the radical ideals in A and the closed subsets of V. Therefore, when A is noetherian, descending chains of closed subsets eventually become constant, and $\operatorname{spec}(A)$ is noetherian. Under the one-to-one correspondence between radical ideals and closed subsets, prime ideals correspond to irreducible closed subsets, and maximal ideals to points:

$$\begin{aligned} \text{radical ideals} &\leftrightarrow \text{closed subsets} \\ \text{prime ideals} &\leftrightarrow \text{irreducible closed subsets} \\ \text{maximal ideals} &\leftrightarrow \text{one-point sets.} \end{aligned}$$

The nilradical $\mathfrak{N}$ of A is the smallest radical ideal, and so it corresponds to the whole space $\operatorname{spec}(A)$. Therefore $\operatorname{spec}(A)$ is irreducible if and only if $\mathfrak{N}$ is prime.

2 Schemes

Let A be a commutative ring, and let $V = \operatorname{spec} A$. We wish to define a sheaf of rings $\mathcal{O}_V$ on V such that $\mathcal{O}_V(D(f)) = A_f$ for all basic open subsets $D(f)$. However, this isn't quite possible because we may have $D(f) = D(f')$ with $f \neq f'$, and while A_f and $A_{f'}$ are canonically isomorphic, they are not equal, and so the best we can hope for is that $\mathcal{O}_V(D(f)) \simeq A_f$.

Let $\mathcal{B}$ be the set of principal open subsets. Because $\mathcal{B}$ is closed under the formation of finite intersections, it makes sense to speak of a sheaf on $\mathcal{B}$ — it is a contravariant functor $\mathcal{F}$ on $\mathcal{B}$ satisfying the sheaf condition: for every covering $D = \bigcup_{i\in I} D_i$ of a principal open subset D by principal open subsets D_i, the sequence

$$\mathcal{F}(D) \to \prod\nolimits_{i\in I} \mathcal{F}(D_i) \rightrightarrows \prod\nolimits_{(i,j)\in I\times I} \mathcal{F}(D_i \cap D_j) \tag{24}$$

is exact.[1]

For a principal open subset D of V, we define $\mathcal{O}_V(D)$ to be $S_D^{-1}A$ where S_D is the multiplicative subset $A \smallsetminus \bigcup_{\mathfrak{p}\in D} \mathfrak{p}$ of A. If $D = D(f)$, then S_D is the smallest saturated multiplicative subset of A containing f, and so $\mathcal{O}_V(D) \simeq A_f$ (see CA 6.12). If $D \supset D'$, then $S_D \subset S_{D'}$, and so there is a canonical "restriction" homomorphism $\mathcal{O}_V(D) \to \mathcal{O}_V(D')$. It is not difficult to show that these restriction maps make $D \rightsquigarrow \mathcal{O}_V(D)$ into a functor on $\mathcal{B}$ satisfying the sheaf condition (24).

For an open subset U of V, let $I = \{D \in \mathcal{B} \mid D \subset U\}$, and define $\mathcal{O}_V(U)$ by the exactness of

$$\mathcal{O}_V(U) \to \prod\nolimits_{D\in I} \mathcal{O}_V(D) \rightrightarrows \prod\nolimits_{(D,D')\in I\times I} \mathcal{O}_V(D \cap D'). \tag{25}$$

Clearly, $U \rightsquigarrow \mathcal{O}_V(U)$ is a functor on the open subsets of V, and it is not difficult to check that it is a sheaf. The k-algebra $\mathcal{O}_V(U)$ is unchanged when the set I in (25) is replaced by another subset of $\mathcal{B}$ covering U. In particular, if $U = D(f)$, then

$$\mathcal{O}_V(U) \simeq \mathcal{O}_V(D(f)) \simeq A_f.$$

The stalk of $\mathcal{O}_V$ at a point $\mathfrak{p} \in V$ is

$$\mathcal{O}_{\mathfrak{p}} \overset{\text{def}}{=} \varinjlim_{U\ni\mathfrak{p}} \mathcal{O}_V(U) = \varinjlim_{f\notin\mathfrak{p}} \mathcal{O}_V(D(f)) \simeq \varinjlim_{f\notin\mathfrak{p}} A_f \simeq A_{\mathfrak{p}}$$

(for the last isomorphism, see CA 7.3). In particular, the stalks of $\mathcal{O}_V$ are local rings.

Thus from A we get a locally ringed space $\operatorname{Spec}(A) = (\operatorname{spec}(A), \mathcal{O}_{\operatorname{spec} A})$. We often write V or $(V, \mathcal{O})$ for $(V, \mathcal{O}_V)$, and we call $\mathcal{O}_V(V)$ the ***coordinate ring*** of V. The reader should think of an affine scheme as being a topological space V together with the structure provided by the ring $\mathcal{O}(V)$.

DEFINITION 2.1 An ***affine scheme*** $(V, \mathcal{O}_V)$ is a ringed space isomorphic to $\operatorname{Spec}(A)$ for some commutative ring A. A ***scheme*** is a ringed space that admits an open covering by affine schemes. A ***morphism*** of affine schemes is a morphism of locally ringed spaces, i.e., a morphism of ringed spaces such that the maps of the stalks are local homomorphisms of local rings.

[1] Recall that this means that the first arrow is the equalizer of the pair of arrows. The upper arrow of the pair is defined by the inclusions $D_i \cap D_j \hookrightarrow D_i$ and the lower by $D_i \cap D_j \hookrightarrow D_j$.

A homomorphism $A \to B$ defines a morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ of affine schemes.

PROPOSITION 2.2 *The functor* Spec *is a contravariant equivalence from the category of commutative rings to the category of affine schemes, with quasi-inverse* $(V,\mathcal{O}) \rightsquigarrow \mathcal{O}(V)$.

PROOF. Omitted (but straightforward). □

In other words, Spec is an equivalence from $\mathsf{Alg}_{\mathbb{Z}}^{\text{opp}}$ to the category of affine schemes.

Schemes over k

When "ring" is replaced by "k-algebra" in the above, we arrive at the notion of a k-scheme. To give a k-scheme is the same as giving a scheme V together with a morphism $V \to \operatorname{Spec} k$. For this reason, k-schemes are also called schemes over k.

Let V be a scheme over k. For a k-algebra R, we let

$$V(R) = \operatorname{Hom}(\operatorname{Spec}(R), V).$$

Thus V defines a functor $\mathsf{Alg}_k \to \mathsf{Set}$.

PROPOSITION 2.3 *For a k-scheme V, let $\widetilde{V}$ be the functor $R \rightsquigarrow V(R)\colon \mathsf{Alg}_k \to \mathsf{Set}$. Then $V \rightsquigarrow \widetilde{V}$ is fully faithful.*

PROOF. tba (easy). □

Therefore, to give a k-scheme is essentially the same as giving a functor $\mathsf{Alg}_k \to \mathsf{Set}$ representable by a k-scheme.

Recall that a morphism $u\colon A \to B$ in a category A is a ***monomorphism*** if $f \mapsto u \circ f\colon \operatorname{Hom}(T,B) \to \operatorname{Hom}(T,A)$ is injective for all objects T of A. A morphism $V \to W$ of k-schemes is a monomorphism if and only if $V(R) \to W(R)$ is injective for all k-algebras R.

NOTES The above is only a sketch. A more detailed account can be found, for example, in Mumford 1966, II §1.

3 Affine groups as affine group schemes

Finite products exist in the category of schemes over k. For example,

$$\operatorname{Spec}(A_1 \otimes A_2) = \operatorname{Spec}(A_1) \times \operatorname{Spec}(A_2).$$

A group in the category of schemes over k is called a ***group scheme over*** k. When the underlying scheme is affine, it is called an ***affine group scheme over*** k. Because the affine schemes form a full subcategory of the category of all schemes, to give an affine group scheme over k is the same as giving a group in the category of affine schemes over k.

A group scheme (G,m) over k defines a functor

$$\widetilde{G}\colon \mathsf{Alg}_k \to \mathsf{Set}, \quad R \rightsquigarrow G(R),$$

and a natural transformation

$$\widetilde{m}\colon \widetilde{G}\times\widetilde{G}\to\widetilde{G}.$$

The pair $(\widetilde{G},\widetilde{m})$ is an affine group if and only if G is affine. Conversely, from an affine group (G,m) over k, we get a commutative Hopf algebra $(\mathcal{O}(G),\Delta)$, and hence an affine group scheme $(\mathrm{Spec}(\mathcal{O}(G)),\mathrm{Spec}(\Delta))$. These functors are quasi-inverse, and hence define equivalences of categories.

ASIDE 3.1 Let (G,m) be a group scheme over a scheme S, and consider the commutative diagram

$$\begin{tikzcd}
G \arrow[d] & G\times_S G \arrow[l, "\mathrm{pr}_1"'] \arrow[d, "\mathrm{pr}_2"'] & G\times_S G \arrow[l, "\mathrm{pr}_1\times m"'] \arrow[d, "m"'] \\
S & G \arrow[l] \arrow[r, equal] & G
\end{tikzcd}$$

The first square is cartesian, and so if G is flat, smooth, ... over S, then pr_2 is a flat, smooth, ... morphism. The morphism $\mathrm{pr}_1\times m$ is an isomorphism of schemes because it is a bijection of functors (obviously). Therefore both horizontal maps in the second square are isomorphisms, and so if pr_2 is flat, smooth, ..., then m is flat, smooth, ...

4 Summary

In the table below, the functors in the top row are fully faithful, and define equivalences of the categories in the second and third rows.

$$\begin{tikzcd}
\mathsf{Func}(\mathsf{Alg}_k,\mathsf{Set}) & \mathsf{Alg}_k^{\mathrm{opp}} \arrow[l, "h^A \leftsquigarrow A"'] \arrow[r, "A\rightsquigarrow\mathrm{Spec}(A)"] & \mathsf{Sch}/k \\
\left\{\begin{matrix}\text{Representable}\\ \text{functors}\end{matrix}\right\} \arrow[r, phantom, "\sim"] & \mathsf{Alg}_k^{\mathrm{opp}} \arrow[r, phantom, "\sim"] & \{\text{Affine schemes}\} \\
\{\text{Affine groups}\} \arrow[r, phantom, "\sim"] & \{\text{Groups in } \mathsf{Alg}_k^{\mathrm{opp}}\} \arrow[r, phantom, "\sim"] & \left\{\begin{matrix}\text{Affine group}\\ \text{schemes}\end{matrix}\right\}
\end{tikzcd}$$

Affine group: pair (G,m) with G a representable functor $\mathsf{Alg}_k\to\mathsf{Set}$ and $m\colon G\times G\to G$ a natural transformation satisfying the equivalent conditions:

(a) for all k-algebras R, the map $m(R)\colon G(R)\times G(R)\to G(R)$ is a group structure on the set $G(R)$;

(b) there exist natural transformations $e\colon *\to G$ and $\mathrm{inv}\colon G\to G$ (necessarily unique) satisfying the conditions of I, 2.7.

(c) the pair (G,m) arises from a functor $\mathsf{Alg}_k\to\mathsf{Grp}$.

Group in $\mathsf{Alg}_k^{\mathrm{opp}}$: pair (A,Δ) with A a k-algebra and $\Delta\colon A\to A\otimes A$ a homomorphism satisfying the equivalent conditions:

(a) for all k-algebras R, the map

$$f_1,f_2\mapsto(f_1,f_2)\circ\Delta\colon h^A(R)\times h^A(R)\to h^A(R)$$

is a group structure on the set $h^A(R)$;

(b) (A,Δ) is a commutative Hopf algebra over k, i.e., there exist k-algebra homomorphisms $\epsilon\colon A\to k$ and $S\colon A\to A$ (necessarily unique) satisfying the conditions of II, 2.1, 4.8.

Affine group scheme: pair (G,m) with G an affine scheme over k and $m\colon G\times G\to G$ a morphism satisfying the equivalent conditions:

(a) for all k-algebras R, the map $m(R)\colon G(R)\times G(R)\to G(R)$ is a group structure on the set $G(R)$;

(b) there exist there exist morphisms $e\colon *\to G$ and $\mathrm{inv}\colon G\to G$ (necessarily unique) satisfying the conditions of I, 2.7;

(c) for all k-schemes S, the map $m(S)\colon G(S)\times G(S)\to G(S)$ is a group structure on the set $G(S)$.

CHAPTER **IV**

Examples

Recall (I, 3.5) that to give an affine group amounts to giving a functor $G\colon \mathsf{Alg}_k \to \mathsf{Grp}$ such that the underlying set-valued functor G_0 is representable. An element f of the coordinate ring $\mathcal{O}(G)$ of G is a family of functions $f_R\colon G(R) \to R$ of sets, indexed by the k-algebras, compatible with homomorphisms of k-algebras (I, 3.13). An element $f_1 \otimes f_2$ of $\mathcal{O}(G) \otimes \mathcal{O}(G)$ defines a function $(f_1 \otimes f_2)_R\colon G(R) \times G(R) \to R$ by the rule:

$$(f_1 \otimes f_2)_R(a,b) = (f_1)_R(a) \cdot (f_2)_R(b). \tag{26}$$

For $f \in \mathcal{O}(G)$, $\Delta(f)$ is the unique element of $\mathcal{O}(G) \otimes \mathcal{O}(G)$ such that

$$(\Delta f)_R(a,b) = f_R(ab), \quad \text{for all } R \text{ and all } a,b \in G(R), \tag{27}$$

and ϵf is the element $f(1_G)$ of k,

$$\epsilon f = f(1_G); \tag{28}$$

moreover, Sf is the unique element of $\mathcal{O}(G)$ such that

$$(Sf)_R(a) = f_R(a^{-1}), \quad \text{for all } R \text{ and all } a \in G(R). \tag{29}$$

Throughout this section, k is a ring.

1 Examples of affine groups

1.1 Let $\mathbb{G}_a$ be the functor sending a k-algebra R to itself considered as an additive group, i.e., $\mathbb{G}_a(R) = (R,+)$. Then

$$\mathbb{G}_a(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k[X], R),$$

and so $\mathbb{G}_a$ is an affine algebraic group, called the ***additive group***.

In more detail, $\mathcal{O}(\mathbb{G}_a) = k[X]$ with $f(X) \in k[X]$ acting as $a \mapsto f(a)$ on $\mathbb{G}_a(R) = R$. The ring $k[X] \otimes k[X]$ is a polynomial ring in $X_1 = X \otimes 1$ and $X_2 = 1 \otimes X$,

$$k[X] \otimes k[X] \simeq k[X_1, X_2],$$

and so $\mathbb{G}_a \times \mathbb{G}_a$ has coordinate ring $k[X_1, X_2]$ with $F(X_1, X_2) \in k[X_1, X_2]$ acting as $(a,b) \mapsto F(a,b)$ on $G(R) \times G(R)$. According to (27)

$$(\Delta f)_R(a,b) = f_R(a+b),$$

and so

$$(\Delta f)(X_1,X_2) = f(X_1+X_2), \quad f \in \mathcal{O}(\mathbb{G}_a) = k[X].$$

In other words, Δ is the homomorphism of k-algebras $k[X] \to k[X]\otimes k[X]$ sending X to $X\otimes 1 + 1\otimes X$. Moreover, ϵf is the constant function,

$$\epsilon f = f(0) \quad \text{(constant term of } f\text{)},$$

and $(Sf)_R(a) = f_R(-a)$, so that

$$(Sf)(X) = f(-X).$$

1.2 Let $\mathbb{G}_m$ be the functor $R \rightsquigarrow R^\times$ (multiplicative group). Each $a \in R^\times$ has a unique inverse, and so

$$\mathbb{G}_m(R) \simeq \{(a,b)\in R^2 \mid ab=1\} \simeq \mathrm{Hom}_{k\text{-alg}}(k[X,Y]/(XY-1),R).$$

Therefore $\mathbb{G}_m$ is an affine algebraic group, called the ***multiplicative group***. Let $k(X)$ be the field of fractions of $k[X]$, and let $k[X,X^{-1}]$ be the subalgebra of $k(X)$ of polynomials in X and X^{-1}. The homomorphism

$$k[X,Y] \to k[X,X^{-1}], \quad X \mapsto X, \quad Y \mapsto X^{-1}$$

defines an isomorphism $k[X,Y]/(XY-1) \simeq k[X,X^{-1}]$, and so

$$\mathbb{G}_m(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k[X,X^{-1}],R).$$

Thus $\mathcal{O}(\mathbb{G}_m) = k[X,X^{-1}]$ with $f\in k[X,X^{-1}]$ acting as $a\mapsto f(a,a^{-1})$ on $\mathbb{G}_m(R) = R^\times$. The comultiplication Δ is the homomorphism of k-algebras $k[X,X^{-1}] \to k[X,X^{-1}]\otimes k[X,X^{-1}]$ sending X to $X\otimes X$, ϵ is the homomorphism $k[X,X^{-1}]\to k$ sending $f(X,X^{-1})$ to $f(1,1)$, and S is the homomorphism $k[X,X^{-1}]\to k[X,X^{-1}]$ interchanging X and X^{-1}.

1.3 Let G be the functor such that $G(R)=\{1\}$ for all k-algebras R. Then

$$G(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k,R),$$

and so G is an affine algebraic group, called the ***trivial algebraic group***, often denoted $*$.

More generally, let G be a finite group, and let A be the set of maps $G\to k$ with its natural k-algebra structure. Then A is a product of copies of k indexed by the elements of G. More precisely, let e_σ be the function that is 1 on σ and 0 on the remaining elements of G. The e_σ's form a complete system of orthogonal idempotents for A:

$$e_\sigma^2 = e_\sigma, \quad e_\sigma e_\tau = 0 \text{ for } \sigma\neq\tau, \quad \sum e_\sigma = 1.$$

The maps

$$\Delta(e_\rho) = \sum_{\sigma,\tau \text{ with } \sigma\tau=\rho} e_\sigma\otimes e_\tau, \quad \epsilon(e_\sigma) = \begin{cases} 1 & \text{if } \sigma = 1 \\ 0 & \text{otherwise} \end{cases}, \quad S(e_\sigma) = e_{\sigma^{-1}}.$$

define a bi-algebra structure on A with inversion S (cf. II, 4.6). Let $(G)_k$ be the associated algebraic group, so that

$$(G)_k(R) = \mathrm{Hom}_{k\text{-alg}}(A,R).$$

If R has no idempotents other than 0 or 1, then a k-algebra homomorphism $A \to R$ must send one e_σ to 1 and the remainder to 0. Therefore, $(G)_k(R) \simeq G$, and one checks that the group structure provided by the maps Δ, ϵ, S is the original one. For this reason, $(G)_k$ is called the ***constant algebraic group*** defined by G, even though for k-algebras R with nontrivial idempotents, $(G)_k(R)$ may be bigger than G.

1.4 For an integer $n \geq 1$,

$$\mu_n(R) = \{r \in R \mid r^n = 1\}$$

is a multiplicative group, and $R \rightsquigarrow \mu_n(R)$ is a functor. Moreover,

$$\mu_n(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k[X]/(X^n - 1), R),$$

and so μ_n is an affine algebraic group with $\mathcal{O}(\mu_n) = k[X]/(X^n - 1)$.

1.5 In characteristic $p \neq 0$, the binomial theorem takes the form $(a+b)^p = a^p + b^p$. Therefore, for any k-algebra R over a ring k such that $pk = 0$,

$$\alpha_p(R) = \{r \in R \mid r^p = 0\}$$

is a group under addition, and $R \rightsquigarrow \alpha_p(R)$ is a functor to groups. Moreover,

$$\alpha_p(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k[T]/(T^p), R),$$

and so α_p is an affine algebraic group with $\mathcal{O}(\alpha_p) = k[T]/(T^p)$.

1.6 For any k-module V, the functor of k-algebras[1]

$$D_{\mathfrak{a}}(V)\colon R \rightsquigarrow \mathrm{Hom}_{k\text{-lin}}(V, R) \quad \text{(additive group)} \tag{30}$$

is represented by the symmetric algebra $\mathrm{Sym}(V)$ of V:

$$\mathrm{Hom}_{k\text{-alg}}(\mathrm{Sym}(V), R) \simeq \mathrm{Hom}_{k\text{-lin}}(V, R), \quad R \text{ a } k\text{-algebra},$$

(see CA §8). Therefore $D_{\mathfrak{a}}(V)$ is an affine group over k (and even an affine algebraic group when V is finitely presented).

In contrast, it is known that the functor

$$V_{\mathfrak{a}}\colon R \rightsquigarrow R \otimes V \quad \text{(additive group)}$$

is not representable unless V is finitely generated and projective.[2] Recall that the finitely generated projective k-modules are exactly the direct summands of free k-modules of finite rank (CA §10), and that, for such a module,

$$\mathrm{Hom}_{k\text{-lin}}(V^\vee, R) \simeq R \otimes V$$

(CA 10.8). Therefore, when V is finitely generated and projective, $V_{\mathfrak{a}}$ is an affine algebraic group with coordinate ring $\mathrm{Sym}(V^\vee)$.

When k is not a field, the functor $W_{\mathfrak{a}}$ defined by a submodule W of V need not be a subfunctor of $V_{\mathfrak{a}}$.

When V is finitely generated and projective, the canonical maps ☠

$$\mathrm{End}_{R\text{-lin}}(R \otimes V) \leftarrow R \otimes \mathrm{End}_{k\text{-lin}}(V) \rightarrow R \otimes (V^{\vee} \otimes V),$$

are isomorphisms,[3] and so

$$R \rightsquigarrow \mathrm{End}_{R\text{-lin}}(R \otimes V) \quad \text{(additive group)}$$

is an algebraic group with coordinate ring $\mathrm{Sym}(V \otimes V^{\vee})$.

When V is free and finitely generated, the choice of a basis $e_1, \ldots, e_n$ for V defines isomorphisms $\mathrm{End}_{R\text{-lin}}(R \otimes V) \simeq M_n(R)$ and $\mathrm{Sym}(V \otimes V^{\vee}) \simeq k[X_{11}, X_{12}, \ldots, X_{nn}]$ (polynomial algebra in the n^2 symbols $(X_{ij})_{1 \leq i,j \leq n}$). For $f \in k[X_{11}, X_{12}, \ldots, X_{nn}]$ and $a = (a_{ij}) \in M_n(R)$,

$$f_R(a) = f(a_{11}, a_{12}, \ldots, a_{nn}).$$

1.7 For $n \times n$ matrices M and N with entries in a k-algebra R,

$$\det(MN) = \det(M) \cdot \det(N) \tag{31}$$

and

$$\mathrm{adj}(M) \cdot M = \det(M) \cdot I = M \cdot \mathrm{adj}(M) \qquad \text{(Cramer's rule)} \tag{32}$$

where I denotes the identity matrix and

$$\mathrm{adj}(M) = \left((-1)^{i+j} \det M_{ji}\right) \in M_n(R)$$

with M_{ij} the matrix obtained from M by deleting the ith row and the jth column. These formulas can be proved by the same argument as for R a field, or by applying the principle of permanence of identities (Artin 1991, 12.3). Therefore, there is a functor SL_n sending a k-algebra R to the group of $n \times n$ matrices of determinant 1 with entries in R. Moreover,

$$\mathrm{SL}_n(R) \simeq \mathrm{Hom}_{k\text{-alg}}\left(\frac{k[X_{11}, X_{12}, \ldots, X_{nn}]}{(\det(X_{ij}) - 1)}, R\right),$$

where $\det(X_{ij})$ is the polynomial (4), and so SL_n is an affine algebraic group with $\mathcal{O}(\mathrm{SL}_n) = \frac{k[X_{11}, X_{12}, \ldots, X_{nn}]}{(\det(X_{ij})-1)}$. It is called the ***special linear group***. For $f \in \mathcal{O}(\mathrm{SL}_n)$ and $a = (a_{ij}) \in \mathrm{SL}_n(R)$,

$$f_R(a) = f(a_{11}, \ldots, a_{nn}).$$

[1] Notations suggested by those in DG II, §1, 2.1. In SGA 3, I, 4.6.1, $D_{\mathfrak{a}}(V)$ is denoted $\mathbf{V}(V)$ and $V_{\mathfrak{a}}$ is denoted $\mathbf{W}(V)$.

[2] This is stated without proof in EGA I (1971) 9.4.10: "on peut montrer en effet que le foncteur $T \mapsto \Gamma(T, \mathcal{E}_{(T)})$ ... n'est représentable *que si* $\mathcal{E}$ est localement libre de rang fini". Nitsure (2002, 2004) proves the following statement: let V be a finitely generated module over a noetherian ring k; then $V_{\mathfrak{a}}$ and GL_V are representable (if and) only if V is projective.

[3] When V is free of finite rank, this is obvious, and it follows easily for a direct summand of such a module.

1.8 Similar arguments show that the $n\times n$ matrices with entries in a k-algebra R and with determinant a unit in R form a group $\mathrm{GL}_n(R)$, and that $R \rightsquigarrow \mathrm{GL}_n(R)$ is a functor. Moreover,

$$\mathrm{GL}_n(R) \simeq \mathrm{Hom}_{k\text{-alg}}\left(\frac{k[X_{11},X_{12},\ldots,X_{nn},Y]}{(\det(X_{ij})Y-1)},R\right),$$

and so GL_n is an affine algebraic group with coordinate ring[4] $\frac{k[X_{11},X_{12},\ldots,X_{nn},Y]}{(\det(X_{ij})Y-1)}$. It is called the ***general linear group***.

For $f\in\mathcal{O}(\mathrm{GL}_n)$ and $a=(a_{ij})\in\mathrm{GL}_n(R)$,

$$f_R(a_{ij}) = f(a_{11},\ldots,a_{nn},\det(a_{ij})^{-1}).$$

Alternatively, let A be the k-algebra in $2n^2$ symbols, $X_{11},X_{12},\ldots,X_{nn},Y_{11},\ldots,Y_{nn}$ modulo the ideal generated by the n^2 entries of the matrix $(X_{ij})(Y_{ij})-I$. Then

$$\mathrm{Hom}_{k\text{-alg}}(A,R) = \{(A,B)\mid A,B\in M_n(R),\quad AB=I\}.$$

The map $(A,B)\mapsto A$ projects this bijectively onto $\{A\in M_n(R)\mid A \text{ is invertible}\}$ (because a right inverse of a square matrix is unique if it exists, and is also a left inverse). Therefore $A\simeq\mathcal{O}(\mathrm{GL}_n)$. For $G=\mathrm{GL}_n$,

$$\mathcal{O}(G) = \frac{k[X_{11},X_{12},\ldots,X_{nn},Y]}{(Y\det(X_{ij})-1)} = k[x_{11},\ldots,x_{nn},y]$$

and

$$\left\{\begin{array}{rcl}\Delta x_{ik} &=& \sum_{j=1,\ldots,n} x_{ij}\otimes x_{jk}\\ \Delta y &=& y\otimes y\end{array}\right. \qquad \left\{\begin{array}{rcl}\epsilon(x_{ii}) &=& 1\\ \epsilon(x_{ij}) &=& 0,\ i\neq j\\ \epsilon(y) &=& 1\end{array}\right. \qquad \left\{\begin{array}{rcl}S(x_{ij}) &=& ya_{ji}\\ S(y) &=& \det(x_{ij})\end{array}\right.$$

where a_{ji} is the cofactor of x_{ji} in the matrix (x_{ji}). Symbolically, we can write the formulas for Δ and ϵ as

$$\begin{aligned}\Delta(x) &= (x)\otimes(x)\\ \epsilon(x) &= I\end{aligned}$$

where (x) is the matrix with ijth entry x_{ij}. We check the formula for $\Delta(x_{ik})$:

$$\begin{array}{rlr}(\Delta x_{ik})_R\big((a_{ij}),(b_{ij})\big) & = (x_{ik})_R\big((a_{ij})(b_{ij})\big) & \text{definition (27)}\\ & = \sum_j a_{ij}b_{jk} & \text{as } (x_{kl})_R((c_{ij})) = c_{kl}\\ & = (\sum_{j=1,\ldots,n} x_{ij}\otimes x_{jk})_R\big((a_{ij}),(b_{ij})\big) & \text{as claimed.}\end{array}$$

1.9 Let C be an invertible $n\times n$ matrix with entries in k, and let

$$G(R) = \{T\in\mathrm{GL}_n(R)\mid T^t\cdot C\cdot T = C\}.$$

[4] In other words, $\mathcal{O}(\mathrm{GL}_n)$ is the ring of fractions of $k[X_{11},X_{12},\ldots,X_{nn}]$ for the multiplicative subset generated by $\det(X_{ij})$,

$$\mathcal{O}(\mathrm{GL}_n) = k[X_{11},X_{12},\ldots,X_{nn}]_{\det(X_{ij})}.$$

See CA, 6.2.

If $C = (c_{ij})$, then $G(R)$ consists of the matrices (t_{ij}) (automatically invertible) such that

$$\sum_{j,k} t_{ji} c_{jk} t_{kl} = c_{il}, \quad i,l = 1,\ldots,n,$$

and so

$$G(R) \simeq \mathrm{Hom}_{k\text{-alg}}(A,R)$$

with A equal to the quotient of $k[X_{11}, X_{12}, \ldots, X_{nn}, Y]$ by the ideal generated by the polynomials

$$\sum_{j,k} X_{ji} c_{jk} X_{kl} - c_{il}, \quad i,l = 1,\ldots,n.$$

Therefore G is an affine algebraic group. When $C = I$, it is the ***orthogonal group*** O_n, and when $C = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$, it is the ***symplectic group*** Sp_n.

1.10 There are abstract versions of the last groups. Let V be a finitely generated projective k–module, let ϕ be a nondegenerate symmetric bilinear form $V \times V \to k$, and let ψ be a nondegenerate alternating form $V \times V \to k$. Then there are affine algebraic groups with

$$\begin{aligned}
\mathrm{SL}_V(R) &= \{R\text{-linear automorphisms of } R \otimes_k V \text{ with determinant } 1\}, \\
\mathrm{GL}_V(R) &= \{R\text{-linear automorphisms of } R \otimes_k V\}, \\
\mathrm{O}(\phi)(R) &= \{\alpha \in \mathrm{GL}_V(R) \mid \phi(\alpha v, \alpha w) = \phi(v,w) \text{ for all } v,w \in R \otimes_k V\}, \\
\mathrm{Sp}(\psi)(R) &= \{\alpha \in \mathrm{GL}_V(R) \mid \psi(\alpha v, \alpha w) = \psi(v,w) \text{ for all } v,w \in R \otimes_k V\}.
\end{aligned}$$

When V is free, the choice of a basis for V defines an isomorphism of each of these functors with one of those in (1.7), (1.8), or (1.9), which shows that they are affine algebraic groups in this case. For the general case, use (3.2).

1.11 Let k be a field, and let K be a separable k-algebra of degree 2. This means that there is a unique k-automorphism $a \mapsto \bar{a}$ of K such that $a = \bar{a}$ if and only if $a \in k$, and that either

(a) K is a separable field extension of k of degree 2 and $a \mapsto \bar{a}$ is the nontrivial element of the Galois group, or
(b) $K = k \times k$ and $\overline{(a,b)} = (b,a)$.

For an $n \times n$ matrix $A = (a_{ij})$ with entries in K, define $\bar{A}$ to be $(\overline{a_{ij}})$ and A^* to be the transpose of $\bar{A}$. Then there is an algebraic group G over k such that

$$G(k) = \{A \in M_n(K) \mid A^* A = I\}.$$

More precisely, for a k-algebra R, define $\overline{a \otimes r} = \bar{a} \otimes r$ for $a \otimes r \in K \otimes_k R$, and, with the obvious notation, let

$$G(R) = \{A \in M_n(K \otimes_k R) \mid A^* A = I\}.$$

Note that $A^* A = I$ implies $\overline{\det(A)} \det(A) = 1$. In particular, $\det(A)$ is a unit, and so $G(R)$ is a group.

In case (b),

$$G(R) = \{(A,B) \in M_n(R) \mid AB = I\}$$

and so $(A,B) \mapsto A$ is an isomorphism of G with GL_n.

In case (a), let $e \in K \smallsetminus k$. Then e satisfies a quadratic polynomial with coefficients in k. Assuming $\mathrm{char}(k) \neq 2$, we can "complete the square" and choose e so that $e^2 \in k$ and $\bar{e} = -e$. A matrix with entries in $K \otimes_k R$ can be written in the form $A + eB$ with $A, B \in M_n(R)$. It lies in $G(R)$ if and only if

$$(A^t - eB^t)(A + eB) = I$$

i.e., if and only if

$$\begin{aligned} A^t \cdot A - e^2 B^t \cdot B &= I, \quad \text{and} \\ A^t \cdot B - B^t \cdot A &= 0. \end{aligned}$$

Evidently, G is represented by a quotient of $k[\ldots, X_{ij}, \ldots] \otimes_k k[\ldots, Y_{ij}, \ldots]$.

In the classical case $k = \mathbb{R}$ and $K = \mathbb{C}$. Then $G(\mathbb{R})$ is the set of matrices in $M_n(\mathbb{C})$ of the form $A + iB$, $A, B \in M_n(\mathbb{R})$, such that

$$\begin{aligned} A^t \cdot A + B^t \cdot B &= I, \quad \text{and} \\ A^t \cdot B - B^t \cdot A &= 0. \end{aligned}$$

1.12 There exists an affine algebraic group G, called the ***group of monomial matrices***, such that, when R has no nontrivial idempotents, $G(R)$ is the group of invertible matrices in $M_n(R)$ having exactly one nonzero element in each row and column. For each $\sigma \in S_n$ (symmetric group), let

$$A_\sigma = \mathcal{O}(\mathrm{GL}_n)/(X_{ij} \mid j \neq \sigma(i))$$

and let $\mathcal{O}(G) = \prod_{\sigma \in S_n} A_\sigma$. Then

$$A_\sigma \simeq k[X_{1\sigma(1)}, \ldots, X_{n\sigma(n)}, Y]/(\mathrm{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)} Y - 1),$$

and so

$$G(R) \simeq \bigsqcup\nolimits_\sigma \mathrm{Hom}_{k\text{-alg}}(A_\sigma, R) \simeq \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(G), R).$$

1.13 Let $k = k_1 \times \cdots \times k_n$, and write $1 = e_1 + \cdots + e_n$. Then $\{e_1, \ldots, e_n\}$ is a complete set of orthogonal idempotents in k. For any k-algebra R,

$$R = R_1 \times \cdots \times R_n$$

where R_i is the k-algebra $Re_i \simeq k_i \otimes_k R$. To give an affine group G over k is the same as giving an affine group G_i over each k_i. If $G \leftrightarrow (G_i)_{1 \leq i \leq n}$, then

$$G(R) = \prod\nolimits_i G_i(R_i) \tag{33}$$

for all k-algebras R.

2 Examples of homomorphisms

2.1 The determinant defines a homomorphism of algebraic groups

$$\det\colon \mathrm{GL}_n \to \mathbb{G}_m.$$

2.2 The homomorphisms

$$R \to \mathrm{SL}_2(R), \quad a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

define a homomorphism of algebraic groups $\mathbb{G}_a \to \mathrm{SL}_2$.

2.3 Add example of the (relative) Frobenius map. [Let G be an affine algebraic group over a field k of characteristic $p \neq 0$. The kernel of the relative Frobenius map $F_{G/k}\colon G \to G^{(p)}$ is a finite connected affine group. It has the same Lie algebra as G, and in particular it is noncommutative if the Lie algebra is nonabelian, e.g. for $G = GL_n$, $n \geq 2$. If G is regular (e.g. smooth over k) then $F_{G/k}$ is faithfully flat. See mo84936.]

3 Appendix: A representability criterion

We prove that a functor is representable if it is representable "locally".

THEOREM 3.1 *Let $F\colon \mathsf{Alg}_k \to \mathsf{Set}$ be a functor. If F is representable, then, for every faithfully flat homomorphism $R \to R'$ of k-algebras, the sequence*

$$F(R) \to F(R') \rightrightarrows F(R' \otimes_R R')$$

is exact (i.e., the first arrow maps $F(R)$ bijectively onto the set on which the pair of arrows coincide). Conversely, if there exists a faithfully flat homomorphism $k \to k'$ such that

(a) *$F|\mathsf{Alg}_{k'}$ is representable, and*
(b) *for all k-algebras R, the following sequence is exact*

$$F(R) \to F(R_{k'}) \rightrightarrows F(R_{k'} \otimes R_{k'}),$$

then F is representable.

PROOF. Suppose that F is representable, say $F = h^A$. For every faithfully flat homomorphism of rings $R \to R'$, the sequence

$$R \to R' \rightrightarrows R' \otimes_R R'$$

is exact (CA 9.6). From this it follows that

$$\mathrm{Hom}_{k\text{-alg}}(A, R) \to \mathrm{Hom}_{k\text{-alg}}(A, R') \rightrightarrows \mathrm{Hom}_{k\text{-alg}}(A, R' \otimes_R R')$$

is exact.

Conversely, let $k \to k'$ be a faithfully flat map such that the restriction F' of F to k'-algebras is represented by a k'-algebra A'. Because F' comes from a functor over k, it is equipped with a descent datum, which defines a descent datum on A' (Yoneda lemma), and descent theory shows that A', together with this descent datum, arises from a k-algebra A; in particular, $A' = k' \otimes A$ (Waterhouse 1979, Chapter 17). On comparing the following exact sequences for F and h^A, we see that A represents F:

$$\begin{tikzcd}
F(R) \arrow[r] & F'(R_{k'}) \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\approx"] & F'(R_{k'} \otimes_R R_{k'}) \arrow[d, "\approx"] \\
h^A(R) \arrow[r] & h^{A'}(R_{k'}) \arrow[r, shift left] \arrow[r, shift right] & h^{A'}(R_{k'} \otimes_R R_{k'}).
\end{tikzcd}$$

□

EXAMPLE 3.2 Let $f_1, \ldots, f_r$ be elements of k such that $(f_1, \ldots, f_r) = k$. Then $k \to \prod k_{f_i}$ is faithfully flat because the condition means that no maximal ideal of k contains all f_i. Let F be a functor of k-algebras, and let $F_i = F|\mathsf{Alg}_{k_{f_i}}$. Then F is representable if

(a) each functor F_i is representable, and
(b) for each k-algebra R, the sequence

$$F(R) \to \prod\nolimits_i F(R_{f_i}) \rightrightarrows \prod\nolimits_{i,j} F(R_{f_i} \otimes_R R_{f_j})$$

is exact.

Note that $R_{f_i} \otimes_R R_{f_j} \simeq R_{f_i f_j}$.

ASIDE 3.3 A functor $F\colon \mathsf{Alg}_k \to \mathsf{Set}$ defines a presheaf on $\mathrm{spec}(R)$ for each k-algebra R. We say that F is a sheaf for the Zariski topology if this presheaf is a sheaf for every R. Then (3.2) can be expressed more naturally as: a functor F that is a sheaf for the Zariski topology is representable if it is locally representable for the Zariski topology on $\mathrm{spec}(k)$. A similar statement holds with "Zariski" replaced by "étale".

CHAPTER **V**

Some Basic Constructions

Throughout this chapter, k is a commutative ring.

1 Products of affine groups

Let G_1 and G_2 be affine groups over k. The functor

$$R \rightsquigarrow G_1(R) \times G_2(R)$$

is an affine group $G_1 \times G_2$ over k with coordinate ring

$$\mathcal{O}(G_1 \times G_2) = \mathcal{O}(G_1) \otimes \mathcal{O}(G_2), \tag{34}$$

because, for any k-algebras A, A_2, R,

$$\mathrm{Hom}_{k\text{-alg}}(A_1 \otimes_k A_2, R) \simeq \mathrm{Hom}_{k\text{-alg}}(A_1, R) \times \mathrm{Hom}_{k\text{-alg}}(A_2, R) \tag{35}$$

(see (8), p. 21).

More generally, let $(G_i)_{i \in I}$ be a (possibly infinite) family of affine groups over k indexed by a set I, and let G be the functor

$$R \rightsquigarrow \prod\nolimits_{i \in I} G_i(R).$$

Then G is an affine group with coordinate ring $\bigotimes_{i \in I} \mathcal{O}(G_i)$ (in the infinite case, apply Bourbaki A, III, §5, Prop. 8). Moreover, G together with the projection maps is the product of the G_i in the category of affine groups. If I is finite and each G_i is an algebraic group, then $\prod_{i \in I} G_i$ is an algebraic group.

The trivial group is a final object in the category of affine groups over k, and so all products exist in this category (and all finite products exist in the subcategory of algebraic groups).

2 Fibred products of affine groups

Let G_1, G_2, and H be functors from the category of k-algebras to sets, and let

$$G_1 \to H \leftarrow G_2 \tag{36}$$

be natural transformations. We define the ***fibred product functor*** $G_1 \times_H G_2$ to be the functor

$$R \rightsquigarrow G_1(R) \times_{H(R)} G_2(R).$$

Obviously $G_1 \times_H G_2$ is the fibred product of G_1 and G_2 over H in $\mathsf{Alg}_k^\vee$.

Let B be a k-algebra, and let A_1 and A_2 be B-algebras. For any k-algebra R and choice of a k-algebra homomorphism $B \to R$ (i.e., of a B-algebra structure on R), there is a canonical isomorphism

$$\mathrm{Hom}_{B\text{-alg}}(A_1 \otimes_B A_2, R) \simeq \mathrm{Hom}_{B\text{-alg}}(A_1, R) \times \mathrm{Hom}_{B\text{-alg}}(A_2, R).$$

On taking the union over the different k-algebra homomorphisms $B \to R$, we find that

$$\mathrm{Hom}_{k\text{-alg}}(A_1 \otimes_B A_2, R) \simeq \mathrm{Hom}_{k\text{-alg}}(A_1, R) \times_{\mathrm{Hom}_{k\text{-alg}}(B,R)} \mathrm{Hom}_{k\text{-alg}}(A_2, R). \tag{37}$$

It follows that, if the functors G_1, G_2, and H in (36) are represented by k-algebras A_1, A_2, and B, then the functor $G_1 \times_H G_2$ is represented by the k-algebra $A_1 \otimes_B A_2$.

If the natural transformations $G_1 \to H \leftarrow G_2$ are homomorphisms of affine groups, then $G_1 \times_H G_2$ is a group-valued functor, and the above remark shows that it is an affine group with coordinate ring

$$\mathcal{O}(G_1 \times_H G_2) = \mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2). \tag{38}$$

It is called the ***fibred product*** of G_1 and G_2 over H.

The fibred product of two homomorphisms $\alpha, \beta \colon G \to H$ is the ***equalizer*** of α and β in the category of affine groups over k

$$\mathrm{Eq}(\alpha, \beta) = G \times_{\alpha, H, \beta} G.$$

Let $* \xrightarrow{e} H$ be the unique homomorphism from the trivial group to H. For any homomorphism $\alpha \colon G \to H$, the equalizer of α and e is the ***kernel*** of α in the category of affine groups over k,

$$\mathrm{Ker}(\alpha) = \mathrm{Eq}(\alpha, e) = G \times_H *.$$

Note that

$$\mathcal{O}(\mathrm{Eq}(\alpha, \beta)) = \mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G) \tag{39}$$
$$\mathcal{O}(\mathrm{Ker}(\alpha)) = \mathcal{O}(G) \otimes_{\mathcal{O}(H)} k \tag{40}$$

and that

$$\mathrm{Eq}(\alpha, \beta)(R) = \mathrm{Eq}(\alpha(R), \beta(R))$$
$$\mathrm{Ker}(\alpha)(R) = \mathrm{Ker}(\alpha(R))$$

for all k-algebras R.

3 Limits of affine groups

Recall (MacLane 1971, III 4, p.68) that, for a functor $F \colon I \to \mathsf{C}$ from a small category I to a category C, there is the notion of an inverse limit of F (also called a projective limit, or just limit). This generalizes the notions of a limit over a directed set and of a product.

THEOREM 3.1 *Let F be a functor from a small category I to the category of affine groups over k; then the functor*

$$R \rightsquigarrow \varprojlim F(R) \tag{41}$$

is an affine group, and it is the inverse limit of F in the category of affine groups.

PROOF. Denote the functor (41) by $\underleftarrow{F}$; thus $\underleftarrow{F}(R)$ is the inverse limit of the functor $i \rightsquigarrow F_i(R)$ from I to the category of (abstract) groups. It is easy to see that $\underleftarrow{F} = \varprojlim F$ in the category of functors from k-algebras to groups, and it will follow that $\underleftarrow{F}$ is the inverse limit in the category of affine groups once we show that it is an affine group. But $\underleftarrow{F}$ is equal to the equalizer of two homomorphisms

$$\prod\nolimits_{i \in \mathrm{ob}(I)} F_i \rightrightarrows \prod\nolimits_{u \in \mathrm{arr}(I)} F_{\mathrm{target}(u)} \tag{42}$$

(MacLane 1971, V 2 Theorem 2, p.109). Both products are affine groups, and we saw in (V, §2) that equalizers exist in the category of affine groups. □

In particular, inverse limits of algebraic groups exist as affine groups. Later (VIII, 8.1) we shall see that every affine group arises in this way.

THEOREM 3.2 *Let F be a functor from a finite category I to the category of algebraic groups over k; then the functor*

$$R \rightsquigarrow \varprojlim F_i(R) \tag{43}$$

is an algebraic group, and it is the inverse limit of F in the category of algebraic groups.

PROOF. Both products in (42) are algebraic groups. □

Direct limits, even finite direct limits, are more difficult. For example, the sum of two groups is their free product, but when G_1 and G_2 are algebraic groups, the functor $R \rightsquigarrow G_1(R) * G_2(R)$ will generally be far from being an algebraic group. Moreover, the functor $R \rightsquigarrow \varinjlim_I F_i(R)$ need not be a sheaf. Roughly speaking, when the direct limit of a system of affine groups exists, it can be constructed by forming the naive direct limit in the category of functors, and then forming the associated sheaf (see VII, 11).

4 Extension of the base ring (extension of scalars)

Let k' be a k-algebra. A k'-algebra R can be regarded as a k-algebra through $k \to k' \to R$, and so a functor G of k-algebras "restricts" to a functor

$$G_{k'} \colon R \rightsquigarrow G(R)$$

of k'-algebras. If G is an affine group, then $G_{k'}$ is an affine group with coordinate ring $\mathcal{O}(G_{k'}) = \mathcal{O}(G)_{k'}$ because, for all k'-algebras R,

$$\mathrm{Hom}_{k'\text{-alg}}(k' \otimes \mathcal{O}(G), R) \simeq \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(G), R)$$

(in (8), p. 21, take $A_1 = k'$, $A_2 = \mathcal{O}(G)$, and f_1 equal to the given k'-algebra structure on R). The affine group $G_{k'}$ is said to have been obtained from G by ***extension of the base ring*** or by ***extension of scalars***. If G is an algebraic group, so also is $G_{k'}$. Clearly $G \rightsquigarrow G_{k'}$ is a functor.

EXAMPLE 4.1 Let V be a k-module and let W be a k'-module. A k-linear map $V \to W'$ extends uniquely to a k'-linear map $V_{k'} \to W$:

$$\mathrm{Hom}_{k\text{-lin}}(V, W) \simeq \mathrm{Hom}_{k'\text{-lin}}(V_{k'}, W).$$

On applying this remark with W a k'-algebra R, we see that

$$D_{\mathfrak{a}}(V)_{k'} \simeq D_{\mathfrak{a}}(V_{k'}).$$

Similarly, if V is finitely generated and projective, then

$$(V_{\mathfrak{a}})_{k'} \simeq (V_{k'})_{\mathfrak{a}}.$$

EXAMPLE 4.2 Let G be the unitary group defined by a separable k-algebra K of degree 2 (see IV, 1.11). For any field extension $k \to k'$, $G_{k'}$ is the unitary group defined by the k'-algebra $K \otimes_k k'$, and so, for example, $G_{k^{\mathrm{al}}} \simeq \mathrm{GL}_n$.

5 Restriction of the base ring (Weil restriction of scalars)

Let k' be a k-algebra. For an affine k'-group G, we let $(G)_{k'/k}$ denote the functor

$$R \rightsquigarrow G(k' \otimes_k R) \colon \mathsf{Alg}_k \to \mathsf{Grp}.$$

PROPOSITION 5.1 *Assume that k' is finitely generated and projective as a k-module. For all affine k'-groups G, the functor $(G)_{k'/k}$ is an affine k-group; moreover, for all affine k-groups H and affine k'-groups G, there are canonical isomorphisms*

$$\mathrm{Hom}_k(H, (G)_{k'/k}) \simeq \mathrm{Hom}_{k'}(H_{k'}, G),$$

natural in both H and G.

In other words, $G \rightsquigarrow (G)_{k'/k}$ is a functor from affine k'-groups to affine k-groups which is right adjoint to the functor "extension of the base ring" $k \to k'$.

The affine group $(G)_{k'/k}$ is said to have been obtained from G by ***(Weil) restriction of scalars*** (or by ***restriction of the base ring***), and $(G)_{k'/k}$ is called the ***Weil restriction*** of G. The functor $G \rightsquigarrow (G)_{k'/k}$ is denoted by $\mathrm{Res}_{k'/k}$ or $\Pi_{k'/k}$.

Before proving the proposition, we list some of the properties of $\mathrm{Res}_{k'/k}$ that follow directly from its definition.

Properties of the restriction of scalars functor

Throughout this subsection, k' is finitely generated and projective as a k-module.

5.2 Because it is a right adjoint, $\mathrm{Res}_{k'/k}$ preserves inverse limits MacLane 1971, V, §5). In particular, it takes products to products, fibred products to fibred products, equalizers to equalizers, and kernels to kernels. This can also be checked directly from its definition.

5.3 Let G be an affine group over k'. There is a homomorphism

$$i \colon G \to (\mathrm{Res}_{k'/k}\, G)_{k'}$$

of affine groups over k' such that, for all k'-algebras R, $i(R)$ is the map $G(R) \to G(k' \otimes R)$ defined by $a \mapsto 1 \otimes a \colon R \to k' \otimes R$. The homomorphism i is injective (obviously), and has the following universal property:

every homomorphism $G \to H_{k'}$ from G to the extension of scalars of a k-group H factors uniquely through i.

This simply restates the fact that $\mathrm{Res}_{k'/k}$ is a right adjoint to extension of scalars (MacLane 1971, IV, 1, Theorem 1).

5.4 For any homomorphisms $k \to k' \to k''$ of rings such that k' (resp. k'') is finitely generated and projective over k (resp. k'),

$$\mathrm{Res}_{k'/k} \circ \mathrm{Res}_{k''/k'} \simeq \mathrm{Res}_{k''/k}.$$

Indeed, for any affine group G over k'' and k-algebra R,

$$\begin{aligned}\left(\left(\mathrm{Res}_{k'/k} \circ \mathrm{Res}_{k''/k'}\right)(G)\right)(R) &= \left(\mathrm{Res}_{k'/k}(\mathrm{Res}_{k''/k'} G)\right)(R)\\ &= (\mathrm{Res}_{k''/k'} G))(k' \otimes_k R)\\ &= G(k'' \otimes_{k'} k' \otimes_k R)\\ &\simeq G(k'' \otimes_k R)\\ &= \left(\mathrm{Res}_{k''/k} G\right)(R)\end{aligned}$$

because $k'' \otimes_{k'} k' \otimes_k R \simeq k'' \otimes_k R$. Alternatively, observe that $\mathrm{Res}_{k'/k} \circ \mathrm{Res}_{k''/k'}$ is right adjoint to $H \rightsquigarrow H_{k''}$.

5.5 For any k-algebra K and any affine group G over k',

$$\left(\mathrm{Res}_{k'/k} G\right)_K \simeq \mathrm{Res}_{k' \otimes_k K/K}(G_K); \tag{44}$$

in other words, Weil restriction commutes with extension of scalars. Indeed, for a K-algebra R,

$$\begin{aligned}\left(\mathrm{Res}_{k'/k} G\right)_K(R) &= \left(\mathrm{Res}_{k'/k} G\right)(R)\\ &= G(k' \otimes_k R)\\ &\simeq G(k' \otimes_k K \otimes_K R)\\ &= \mathrm{Res}_{k' \otimes_k K/K}(G_K)(R)\end{aligned}$$

because $k' \otimes_k R \simeq k' \otimes_k K \otimes_K R$.

5.6 Let k' be a product of k-algebras, $k' = k_1 \times \cdots \times k_n$, with each k_i finitely generated and projective as a k-module. Recall (IV, 1.13) that to give an affine group G over k' is the same as giving an affine group G_i over each k_i. In this case,

$$(G)_{k'/k} \simeq (G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}. \tag{45}$$

Indeed, for any k-algebra R,

$$\begin{aligned}(G)_{k'/k}(R) &= G(k' \otimes R)\\ &= G_1(k_1 \otimes R) \times \cdots \times G_n(k_n \otimes R) \quad \text{(by (33), p.53)}\\ &= (G_1)_{k_1/k}(R) \times \cdots \times (G_n)_{k_n/k}(R)\\ &= \left((G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}\right)(R).\end{aligned}$$

5.7 Let k' be a finite separable field extension of a field k, and let K be a field containing all k-conjugates of k', i.e., such that $|\mathrm{Hom}_k(k',K)| = [k':k]$. Then

$$\left(\mathrm{Res}_{k'/k}G\right)_K \simeq \prod\nolimits_{\alpha:k'\to K} \alpha G$$

where αG is the affine group over K obtained by extension of scalars with respect to $\alpha: k' \to K$. Indeed

$$\left(\mathrm{Res}_{k'/k}G\right)_K \overset{(44)}{\simeq} \mathrm{Res}_{k'\otimes K/K}G_K \overset{(45)}{\simeq} \prod\nolimits_{\alpha:k'\to K} G_\alpha$$

because $k' \otimes K \simeq K^{\mathrm{Hom}_k(k',K)}$.

5.8 Let $k' = k[\varepsilon]$ where $\varepsilon^2 = 0$. For any algebraic group G over k', there is an exact sequence

$$0 \to V_{\mathfrak{a}} \to (G)_{k'/k} \to G \to 0$$

where V is the tangent space to G at 1, i.e., $V = \mathrm{Ker}(G(k[\varepsilon]) \to G(k))$. This is proved in XI, 6.3, below.

5.9 We saw in (5.7) that, when k' is a separable field extension of k, $(G)_{k'/k}$ becomes isomorphic to a product of copies of G over some field containing k'. This is far from true when k'/k is an inseparable field extension. For example, let k be a nonperfect field of characteristic 2, so that there exists a nonsquare a in k, and let $k' = k[\sqrt{a}]$. Then

$$k' \otimes_k k' \simeq k'[\varepsilon], \quad \varepsilon = a \otimes 1 - 1 \otimes a, \quad \varepsilon^2 = 0.$$

According to (5.5),

$$\left(\mathrm{Res}_{k'/k}G\right)_{k'} \simeq \mathrm{Res}_{k'[\varepsilon]/k'}G_{k'},$$

which is an extension of $G_{k'}$ by a vector group (5.8).

Proof of Proposition 5.1

We first explain the existence of a right adjoint for functors to sets.

From a functor $F: \mathsf{Alg}_k \to \mathsf{Set}$ we obtain a functor $F_{k'}: \mathsf{Alg}_{k'} \to \mathsf{Set}$ by setting $F_{k'}(R) = F(R)$. On the other hand, from a functor $F': \mathsf{Alg}_{k'} \to \mathsf{Set}$ we obtain a functor $(F')_{k'/k}: \mathsf{Alg}_k \to \mathsf{Set}$ by setting $(F')_{k'/k}(R) = F'(k' \otimes R)$. Let φ be a natural transformation $\varphi: F_{k'} \to F'$. The homomorphisms

$$F(R) \xrightarrow{F(r\mapsto 1\otimes r)} F(k'\otimes R) \xrightarrow{\varphi(k'\otimes R)} F'(k'\otimes R) \overset{\text{def}}{=} (F')_{k'/k}(R)$$

are natural in the k-algebra R, and so their composite is a natural transformation $F \to (F')_{k'/k}$. Thus, we have a morphism

$$\mathrm{Hom}(F_{k'}, F') \to \mathrm{Hom}(F, (F')_{k'/k}). \tag{46}$$

This has an obvious inverse. Given $F \to (F')_{k'/k}$, we need a map $F_{k'} \to F'$. Let R be a k'-algebra, and let R_0 be R regarded as a k-algebra. The given k-algebra map $k' \to R$ and the identity map $R_0 \to R$ define a map $k' \otimes_k R_0 \to R$ (of k'-algebras). Hence we have a map

$$F(R_0) \to F'(k' \otimes_k R_0) \to F'(R),$$

and $F(R_0) = F_{k'}(R)$. Thus (46) is a bijection.

We have shown that the extension of scalars functor $F \rightsquigarrow F_{k'}$ has a right adjoint $F' \rightsquigarrow (F')_{k'/k}$:

$$\operatorname{Hom}(F_{k'}, F') \simeq \operatorname{Hom}(F, (F')_{k'/k}). \tag{47}$$

LEMMA 5.10 *Assume that k' is finitely generated and projective as a k-module. If $F\colon \mathsf{Alg}_{k'} \to \mathsf{Set}$ is represented by a k-algebra (resp. a finitely presented k-algebra), then so also is $(F)_{k'/k}$.*

PROOF. We prove this first in the case that k' is free as a k-module, say,

$$k' = ke_1 \oplus \cdots \oplus ke_d, \quad e_i \in k'.$$

Consider first the case that $F = \mathbb{A}^n$, so that $F(R) = R^n$ for all k'-algebras R. For any k-algebra R,

$$R' \stackrel{\text{def}}{=} k' \otimes R \simeq Re_1 \oplus \cdots \oplus Re_d,$$

and so there is a bijection

$$(a_i)_{1 \le i \le n} \mapsto (b_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le d}} : R'^n \to R^{nd}$$

which sends (a_i) to the family (b_{ij}) defined by the equations

$$a_i = \textstyle\sum_{j=1}^{d} b_{ij} e_j, \quad i = 1, \ldots, n. \tag{48}$$

The bijection is natural in R, and shows that $(F)_{k'/k} \approx \mathbb{A}^{nd}$ (the isomorphism depends only on the choice of the basis $e_1, \ldots, e_d$).

Now suppose that F is the subfunctor of $\mathbb{A}^n$ defined by a polynomial $f(X_1, \ldots, X_n) \in k'[X_1, \ldots, X_n]$. On substituting

$$X_i = \textstyle\sum_{j=1}^{d} Y_{ij} e_j$$

into f, we obtain a polynomial $g(Y_{11}, Y_{12}, \ldots, Y_{nd})$ with the property that

$$f(a_1, \ldots, a_n) = 0 \iff g(b_{11}, b_{12}, \ldots, b_{nd}) = 0$$

when the a's and b's are related by (48). The polynomial g has coefficients in k', but we can write it (uniquely) as a sum

$$g = g_1 e_1 + \cdots + g_d e_d, \quad g_i \in k[Y_{11}, Y_{12}, \ldots, Y_{nd}].$$

Clearly,

$$g(b_{11}, b_{12}, \ldots, b_{nd}) = 0 \iff g_i(b_{11}, b_{12}, \ldots, b_{nd}) = 0 \text{ for } i = 1, \ldots, d,$$

and so $(F)_{k'/k}$ is isomorphic to the subfunctor of $\mathbb{A}^{nd}$ defined by the polynomials $g_1, \ldots, g_d$.

This argument extends in an obvious way to the case that F is the subfunctor of $\mathbb{A}^n$ defined by a finite set of polynomials, and even to the case that it is a subfunctor of an infinite dimensional affine space defined by infinitely many polynomials.

We deduce the general case from the free case by applying IV, Theorem 3.1, in the form of (3.2). According to (CA 10.4), there exist elements $f_1, \ldots, f_r$ of k such that

$(f_1,\ldots,f_r)=k$ and k'_{f_i} is a free k_{f_i}-module for each i. Therefore $\left((F)_{k'/k}\right)_{k_{f_i}}$ is representable for each i. For any faithfully flat homomorphism $R\to R'$ of k-algebras, $R_{k'}\to R'_{k'}$ is a faithfully flat homomorphism of k'-algebras (CA 9.7), and so

$$F(R_{k'})\to F(R'_{k'})\rightrightarrows F(R'_{k'}\otimes_{R_{k'}}R'_{k'})$$

is exact. But this equals

$$(F)_{k'/k}(R)\to(F)_{k'/k}(R')\rightrightarrows(F)_{k'/k}(R'\otimes_R R'),$$

and so $(F)_{k'/k}$ satisfies the condition (b) of IV, 3.2. □

If G is a functor $\mathsf{Alg}_{k'}\to\mathsf{Grp}$, then $(G)_{k'/k}$ is a functor $\mathsf{Alg}_k\to\mathsf{Grp}$. The lemma shows that if G is an affine group or an affine algebraic group, then so also is $(G)_{k'/k}$, and (47) shows that the functor $G'\rightsquigarrow(G')_{k'/k}$ is right adjoint to the functor "extension of scalars".

ASIDE 5.11 Let k' be free as a k-module, with basis $(e_i)_{i\in I}$ (not necessarily finite), and let $F\in\mathsf{Alg}_{k'}^{\vee}$ be the functor represented by $A=k[X_j]_{j\in J}/\mathfrak{a}$. Let $F'=h^{k[X_j]_{j\in J}}$ (affine space with coordinates indexed by J). Then $(F')_{k'/k}$ is represented by $k[Y_{(i,j)}]_{(i,j)\in I\times J}$ (affine space with coordinates indexed by $I\times J$), and so $(F)_{k'/k}$ is represented by a quotient of $k[Y_{(i,j)}]_{(i,j)\in I\times J}$ (see 6.6 below).

6 Transporters

Recall that an ***action*** of a monoid G on a set X is a map

$$(g,x)\mapsto gx\colon G\times X\to X$$

such that

(a) $(g_1g_2)x=g_1(g_2x)$ for all $g_1,g_2\in G$, $x\in X$, and
(b) $ex=x$ for all $x\in X$ (here e is the identity element of G).

Now let G be an affine monoid over k, and let X be a functor from the category of k-algebras to sets, i.e., an object of $\mathsf{Alg}_k^{\vee}$. An ***action*** of G on X is a natural transformation $G\times X\to X$ such that $G(R)\times X(R)\to X(R)$ is an action of the monoid $G(R)$ on the set $X(R)$ for all k-algebras R. Let Z and Y be subfunctors of X. The ***transporter*** $T_G(Y,Z)$ of Y into Z is the functor

$$R\rightsquigarrow\{g\in G(R)\mid gY\subset Z\},$$

where the condition $gY\subset Z$ means that $gY(R')\subset Z(R')$ for all R-algebras R', i.e., that $gY\subset Z$ as functors on the category of R-algebras.

In the remainder of this section, we shall define the notion of a closed subfunctor, and prove the following result.

THEOREM 6.1 *Let $G\times X\to X$ be an action of an affine monoid G on a functor X, and let Z and Y be subfunctors of X such that Z is closed in X. If Y is representable by a k-algebra that is free as a k-module, then $T_G(Y,Z)$ is represented by a quotient of $\mathcal{O}(G)$.*

Closed subfunctors

A subfunctor Z of a functor Y from Alg_k to Set is said to be ***closed*** if, for every k-algebra A and natural transformation $h^A \to Y$, the fibred product $Z \times_Y h^A$ is represented by a quotient of A. The Yoneda lemma identifies a natural transformation $h^A \to Y$ with an element α of $Y(A)$, and, for all k-algebras R,

$$\left(Z \times_Y h^A\right)(R) = \{\varphi\colon A \to R \mid \varphi(\alpha) \in Z(A)\}.$$

Thus, Z is closed in Y if and only if, for every k-algebra A and $\alpha \in Y(A)$, the functor of k-algebras

$$R \rightsquigarrow \{\varphi\colon A \to R \mid \varphi(\alpha) \in Z(A)\}$$

is represented by a quotient of A, i.e., there exists an ideal $\mathfrak{a} \subset A$ such that, for all homomorphism $\varphi\colon A \to R$,

$$Y(\varphi)(\alpha) \in Z(R) \iff \varphi(\mathfrak{a}) = 0.$$

EXAMPLE 6.2 Let Z be a subfunctor of $Y = h^B$ for some k-algebra B. For the identity map $h^B \to Y$, the functor $Z \times_Y h^B = Z$. Therefore, if Z is closed in h^B, then it represented by a quotient of B. Conversely, let $Z \subset h^B$ be the subfunctor represented by a quotient $B/\mathfrak{b}$ of B, so that

$$Z(R) = \{\varphi\colon B \to R \mid \varphi(\mathfrak{b}) = 0\}.$$

For any $\alpha\colon B \to A$, the functor $Z \times_{h^B} h^A$ is

$$R \rightsquigarrow \{\varphi\colon A \to R \mid \varphi \circ \alpha \in Z(R)\},$$

which is represented by $A/\alpha(\mathfrak{b})$. Therefore Z is closed.

EXAMPLE 6.3 Let Y be the functor $\mathbb{A}^n = (R \rightsquigarrow R^n)$. A subfunctor of $\mathbb{A}^n$ is closed if and if it is defined by a finite set of polynomials in $k[X_1,\ldots,X_n]$ in the sense of I, §1. This is the special case $B = k[X_1,\ldots,X_n]$ of Example 6.2.

EXAMPLE 6.4 If Y is the functor of k-algebras defined by a scheme Y' (III, 2), then the closed subfunctors of Y are exactly those defined by closed subschemes of Y'. When Y' is affine, this is a restatement of (6.2), and the general case follows easily.

LEMMA 6.5 *Let B be a k-algebra that is free as a k-module, and let A be a k-algebra. For every ideal $\mathfrak{b}$ in $B \otimes A$, there exists an ideal $\mathfrak{a}$ in A such that, for an ideal $\mathfrak{a}'$ in A,*

$$\mathfrak{a}' \supset \mathfrak{a} \iff B \otimes \mathfrak{a}' \supset \mathfrak{b}.$$

PROOF. Choose a basis $(e_i)_{i \in I}$ for B as k-vector space. Each element b of $B \otimes A$ can be expressed uniquely as $b = \sum_{i \in I} e_i \otimes a_i$, $a_i \in A$, and we let $\mathfrak{a}$ be the ideal in A generated by the coordinates a_i of the elements $b \in \mathfrak{b}$. Clearly $B \otimes \mathfrak{a} \supset \mathfrak{b}$, and so if $\mathfrak{a}' \supset \mathfrak{a}$, then $B \otimes \mathfrak{a}' \supset \mathfrak{b}$. Conversely, if $B \otimes \mathfrak{a}' \supset \mathfrak{b}$ then the coordinates of all elements of $\mathfrak{b}$ lie in $\mathfrak{a}'$, and so $\mathfrak{a}' \supset \mathfrak{a}$. □

For a k-algebra B and functor $X\colon \mathsf{Alg}_B \to \mathsf{Set}$, we let X_* denote the functor $R \rightsquigarrow X(B \otimes R)\colon \mathsf{Alg}_k \to R$ (cf. §5).

LEMMA 6.6 *Let B be a k-algebra that is free as a k-module, and let Z and X be functors $\mathsf{Alg}_B \to \mathsf{Set}$. If Z be a closed subfunctor of X, then Z_* is a closed subfunctor of X_*.*

PROOF. Let A be a k-algebra, and $\alpha \in X_*(A)$. To prove that Z_* is closed in X_* we have to show that there exists an ideal $\mathfrak{a} \subset A$ such that, for every homomorphism $\varphi\colon A \to R$ of k-algebras,

$$X_*(\varphi)(\alpha) \in Z_*(R) \iff \varphi(\mathfrak{a}) = 0,$$

i.e.,

$$X(B \otimes \varphi)(\alpha) \in Z(B \otimes R) \iff \varphi(\mathfrak{a}) = 0.$$

Because Z is closed in X, there exists an ideal $\mathfrak{b}$ in $B \otimes A$ such that, for the homomorphism $B \otimes \varphi\colon B \otimes A \to B \otimes R$,

$$X(B \otimes \varphi)(\alpha) \in Z(B \otimes R) \iff (B \otimes \varphi)(\mathfrak{b}) = 0. \tag{49}$$

According to (6.5), there exists an ideal $\mathfrak{a}$ in A such that

$$\mathfrak{a} \subset \mathfrak{a}' \iff \mathfrak{b} \subset B \otimes \mathfrak{a}' \quad (\mathfrak{a}' \text{ an ideal in } A). \tag{50}$$

On taking $\mathfrak{a}' = \operatorname{Ker}\varphi$, we see that

$$\mathfrak{a} \subset \operatorname{Ker}(\varphi) \iff \mathfrak{b} \subset B \otimes \operatorname{Ker}(\varphi) = \operatorname{Ker}(B \otimes \varphi).$$

Combined with (49), this shows that $\mathfrak{a}$ has the required property. □

LEMMA 6.7 *If Z is a closed subfunctor of X, then, for every natural transformation $T \to X$, $Z \times_X T$ is a closed subfunctor of T.*

PROOF. Let $h^A \to T$ be a natural transformation. Then $Z \times_X T \times_T h^A \simeq Z \times_X h^A$, and so $(Z \times_X T) \times_T h^A$ is represented by a quotient of A. □

LEMMA 6.8 *Let Z and Y be subfunctors of a functor X, and let $G \times X \to X$ be an action of an affine monoid G on X. Assume that $Y = h^B$, and for a k-algebra R, let $y_R \in Y(R \otimes B)$ be the homomorphism $b \mapsto 1 \otimes b\colon B \to R \otimes B$. Then*

$$T_G(Y,Z)(R) = \{g \in G(R) \mid gy_R \in Z(R \otimes B)\}.$$

Hence

$$T_G(Y,Z) = G \times_{X_*} Z_*,$$

where $G \to X_*$ is the natural transformation $g \mapsto gy_R\colon G(R) \to X(R \otimes B)$.

PROOF. Certainly, LHS ⊂ RHS. For the reverse inclusion, let R' be an R-algebra, and let $\alpha \in Y(R') = \operatorname{Hom}(B, R')$. Then y_R maps to α under the map $Y(R \otimes B) \to Y(R')$ defined by $R \to R'$ and $B \xrightarrow{\alpha} R'$, and so

$$gy_R \in Z(R \otimes B) \implies g\alpha \in Z(R').$$

□

Proof of Theorem 6.1

We may suppose that $Y = h^B$. Lemma 6.8 allows us to write

$$T_G(Y,Z) = G \times_{X_*} Z_*.$$

Lemma 6.6 shows that Z_* is a closed subfunctor of X_*, and so it follows from (6.7) that $T_G(Y,Z)$ is a closed subfunctor of G. This means that it is represented by a quotient of $\mathcal{O}(G)$ (see 6.2).

A modest generalization

We say that a k-algebra A is ***locally free*** if there exist exist elements $f_1,\ldots,f_r$ of k such that $(f_1,\ldots,f_r) = k$ and A_{f_i} is a free k_{f_i}-module for each i. For example, a k-algebra is locally free if it is projective and finitely generated as a k-module (CA 10.4, and all k-algebras are (locally) free when k is a field.

THEOREM 6.9 *Let $G \times X \to X$ be an action of an affine monoid G on a functor X, and let Z and Y be subfunctors of X. If Y is representable by a locally free k-algebra and Z is closed in X, then $T_G(Y,Z)$ is a closed subfunctor of G (hence represented by a quotient of $\mathcal{O}(G)$).*

PROOF. Apply IV, 3.2. □

ASIDE 6.10 A little more generally: let G be a monoid in $\mathsf{Alg}_k^\vee$ acting on an X in $\mathsf{Alg}_k^\vee$, and let Y and Z be subfunctors of X. If Y is representable by a locally free k-scheme (i.e., admits a covering by affines U_i such that $\mathcal{O}(U_i)$ is a free k-module) and Z is a closed subfunctor of X, then $T_G(Y,Z)$ is a closed subfunctor of G. See also DG I, §2, 7.7, p. 65, and II, §2, 3.6, p. 165.

7 Galois descent of affine groups

In this section, k is a field. Let Ω be a Galois extension of the field k, and let $\Gamma = \mathrm{Gal}(\Omega/k)$. When Ω is an infinite extension of k, we endow Γ with the Krull topology. By an ***action*** of Γ on an Ω-vector space V we mean a homomorphism $\Gamma \to \mathrm{Aut}_k(V)$ such that each $\sigma \in \Gamma$ acts σ-linearly, i.e., such that

$$\sigma(cv) = \sigma(c)\cdot\sigma(v) \text{ for all } \sigma \in \Gamma,\ c \in \Omega, \text{ and } v \in V.$$

We say that the action is continuous if every element of V is fixed by an open subgroup of Γ, i.e., if

$$V = \bigcup\nolimits_{\Gamma'} V^{\Gamma'} \qquad \text{(union over the open subgroups } \Gamma' \text{ of } \Gamma\text{).}$$

PROPOSITION 7.1 *For any Ω-vector space V equipped with a continuous action of Γ, the map*

$$\textstyle\sum_i c_i \otimes v_i \mapsto \sum_i c_i v_i \colon \Omega \otimes_k V^\Gamma \to V$$

is an isomorphism.

PROOF. See AG, 16.15 (the proof is quite elementary). □

For any vector space V over k, the group Γ acts continuously on $\Omega \otimes V$ according to rule:

$$\sigma(c \otimes v) = \sigma c \otimes v \text{ for all } \sigma \in \Gamma, c \in \Omega, \text{ and } v \in V.$$

PROPOSITION 7.2 *The functor $V \rightsquigarrow \Omega \otimes_k V$ from vector spaces over k to vector spaces over Ω equipped with a continuous action of Γ is an equivalence of categories.*

PROOF. When we choose bases for V and V', then $\mathrm{Hom}_{k\text{-lin}}(V, V')$ and $\mathrm{Hom}_{\Omega\text{-lin}}(\Omega \otimes V, \Omega \otimes V')$ become identified with with certain sets of matrices, and the fully faithfulness of the functor follows from the fact that $\Omega^{\Gamma} = k$. That the functor is essentially surjective follows from (7.1). □

Let G be an affine group over Ω. By a continuous action of Γ on G we mean a continuous action of Γ on $\mathcal{O}(G)$ preserving Δ and the k-algebra structure on A; thus

$$\left.\begin{array}{rcl} \sigma(f \cdot f') & = & \sigma f \cdot \sigma f' \\ \sigma 1 & = & 1 \\ (\sigma \otimes \sigma)(\Delta(f)) & = & \Delta(\sigma f) \end{array}\right\} \text{for all } \sigma \in \Gamma,\ f, f' \in A.$$

PROPOSITION 7.3 *The functor $G \rightsquigarrow G_{\Omega}$ from affine groups over k to affine groups over Ω equipped with a continuous action of Γ is an equivalence of categories.*

PROOF. Proposition 7.2 shows that it is an equivalence of categories on the Hopf algebras.□

EXAMPLE 7.4 Let k' be a finite separable field extension of k, and let Ω be a Galois extension of k containing all conjugates of k'. Let G be the affine group over k' defined by a k-algebra A and a comultiplication Δ (see I, 3.9), and let G_* be the affine group over k' corresponding to the pair

$$(A_*, \Delta_*) = \prod\nolimits_{\tau : k' \to \Omega} (\tau A, \tau \Delta)$$

where τ runs over the k-homomorphisms $k' \to \Omega$. There is an obvious continuous action of $\mathrm{Gal}(\Omega/k)$ on (A_*, Δ_*), and the corresponding affine group over k is $(G)_{k'/k}$. This is essentially the original construction of $(G)_{k'/k}$ in Weil 1960, 1.3.

8 The Greenberg functor

Let A be a local artinian ring with residue field k. For example, A could be the ring $W_m(k)$ of Witt vectors of length m. A general A is a $W_m(k)$-module for some m. For an affine group G over A, consider the functor $\mathcal{G}(G)$:

$$R \rightsquigarrow G(A \otimes_{W_m(k)} W_m(R)) \colon \mathsf{Alg}_k \to \mathsf{Grp}.$$

Then $\mathcal{G}(G)$ is an affine group over k. See Greenberg 1961, 1963.

9 Exercises

EXERCISE 9.1 Let k' be a finite separable extension of a field k. Let $\mathbb{A}^1$ be the functor $\mathsf{Alg}_k \to \mathsf{Set}$ sending R to R, and let U_i, $i \in k$, be the subfunctor of $\mathbb{A}^1$ such that $U_i(R) = \{a \in R \mid a \neq i\}$. Show that $\mathbb{A}^1 = U_0 \cup U_1$ but $\Pi_{k'/k}\mathbb{A}^1 \neq \left(\Pi_{k'/k}U_0\right) \cup \left(\Pi_{k'/k}U_1\right)$ if $k' \neq k$.

EXERCISE 9.2 Let k'/k be a finite field extension. Let $\alpha\colon G_{k'} \to H$ be a homomorphism of algebraic groups over k', and let $\beta\colon G \to \Pi_{k'/k}H$ be the corresponding homomorphism over k. Show that $\operatorname{Ker}(\beta)$ is the unique affine subgroup of G such that $\operatorname{Ker}(\beta)_{k'} = \operatorname{Ker}(\alpha)$.

CHAPTER **VI**

Affine groups over fields

Throughout this chapter, k is a field. When k is a field, the affine scheme attached to an affine algebraic group can be regarded as a variety over k (perhaps with nilpotents in the structure sheaf). This gives us a geometric interpretation of the algebraic group, to which we can apply algebraic geometry.

1 Affine k-algebras

An ***affine*** k***-algebra*** is a finitely generated k-algebra A such that $k^{\mathrm{al}} \otimes_k A$ is reduced. If A is affine, then $K \otimes_k A$ is reduced for all fields K containing k; in particular, A itself is reduced (CA 18.3). When k is perfect, every reduced finitely generated k-algebra is an affine k-algebra (CA 18.1). The tensor product of two affine k-algebras is again an affine k-algebra (CA 18.4).

2 Schemes algebraic over a field

Let k be a field, and let V be an affine k-scheme. When $\mathcal{O}_V(V)$ is a finitely generated k-algebra (resp. an affine k-algebra), V is called an ***affine algebraic scheme*** over k (resp. an ***affine algebraic variety*** over k).

For schemes algebraic over a field it is convenient to ignore the nonclosed points and work only with the closed points. What makes this possible is that, for any homomorphism $\varphi\colon A \to B$ of algebras finitely generated over a field, Zariski's lemma shows that the preimage of a maximal ideal in B is a maximal ideal in A.[1]

For a finitely generated k-algebra A, define $\mathrm{spm}(A)$ to be the set of maximal ideals in A endowed with the topology for which the closed sets are those of the form

$$V(\mathfrak{a}) \overset{\text{def}}{=} \{\mathfrak{m} \text{ maximal} \mid \mathfrak{m} \supset \mathfrak{a}\}, \quad \mathfrak{a} \text{ an ideal in } A.$$

The inclusion map $\mathrm{spm}(A) \hookrightarrow \mathrm{spec}(A)$ identifies $\mathrm{spm}(A)$ with the set of closed points of $\mathrm{spec}(A)$, and the map $S \mapsto S \cap \mathrm{spm}(A)$ is a bijection from the open (resp. closed) subsets of

[1] Recall (CA 11.1) that Zariski's lemma says that if a field K that is finitely generated as an algebra over a subfield k, then it is finitely generated as a vector space over k. Let $\varphi\colon A \to B$ be a homomorphism of finitely generated k-algebras. For any maximal ideal $\mathfrak{m}$ in B, $B/\mathfrak{m}$ is a field, which Zariski's lemma shows to be finite over k. Therefore the image $A/\varphi^{-1}(\mathfrak{m})$ of A in $B/\mathfrak{m}$ is finite over k. As it is an integral domain, this implies that it is a field, and so $\varphi^{-1}(\mathfrak{m})$ is a maximal ideal.

spec(A) onto the open (resp. closed) subsets of spm(A). As noted, Zariski's lemma shows that spm is a contravariant functor from the category of finitely generated k-algebras to topological spaces. On $V = \text{spm}(A)$ there is a sheaf $\mathcal{O}_V$ such that $\mathcal{O}_V(D(f)) \simeq A_f$ for all $f \in A$. It can be defined the same way as for spec(A), or as the restriction to spm(A) of the sheaf on spec(A). When working with affine algebraic schemes (or varieties), implicitly we use max specs. In other words, all points are closed.

When k is algebraically closed, the definition of an affine algebraic variety over k that we arrive at is essentially the same as that in AG, Chapter 3 — see the next example.

EXAMPLE 2.1 Let k be an algebraically closed field, and endow k^n with the topology for which the closed sets are the zero-sets of families of polynomials. Let V be a closed subset of k^n, let $\mathfrak{a}$ be the set of polynomials that are zero on V, and let

$$k[V] = k[X_1,\ldots,X_n]/\mathfrak{a} = k[x_1,\ldots,x_n].$$

A pair of elements $g,h \in k[V]$ with $h \neq 0$ defines a function

$$P \mapsto \tfrac{g(P)}{h(P)} \colon D(h) \to k$$

on the open subset $D(h)$ of V where h is nonzero. A function $f\colon U \to k$ on an open subset U of V is said to be ***regular*** if it is of this form in a neighbourhood of each point of U. Let $\mathcal{O}(U)$ be the set of regular functions on U. Then $U \rightsquigarrow \mathcal{O}(U)$ is a sheaf of k-algebras on V, and $(V,\mathcal{O})$ is an affine algebraic scheme over k with $\mathcal{O}(V) = k[V]$. See AG 3.4 — the map

$$(a_1,\ldots,a_n) \mapsto (x_1 - a_1,\ldots,x_n - a_n)\colon V \to \text{spm}\,(k[V])$$

is a bijection because of the Nullstellensatz. When $V = k^n$, the scheme $(V,\mathcal{O})$ is ***affine n-space*** $\mathbb{A}^n$.

EXAMPLE 2.2 Let k be an algebraically closed field. The affine algebraic scheme

$$\text{Spm}(k[X,Y]/(Y))$$

can be identified with the scheme attached to the closed subset $Y = 0$ of $k \times k$ in (2.1). Now consider

$$\text{Spm}(k[X,Y]/(Y^2)).$$

This has the same underlying topological space as before (namely, the x-axis in $k \times k$), but it should now be thought of as having multiplicity 2, or as being a line thickened in another dimension.

2.3 Let K be a field containing k. An affine algebraic scheme V over k defines an affine algebraic scheme V_K over K with $\mathcal{O}(V_K) = K \otimes_k \mathcal{O}(V)$.

2.4 An affine algebraic scheme V over a field k is said to be ***reduced*** if $\mathcal{O}(V)$ is reduced, and it is said to be ***geometrically reduced*** if $V_{k^{\text{al}}}$ is reduced. Thus V is geometrically reduced if and only if $\mathcal{O}(V)$ is an affine k-algebra, and so a "geometrically reduced affine algebraic scheme" is another name for an "affine algebraic variety". Let $\mathfrak{N}$ be the nilradical of $\mathcal{O}(V)$. Then

$$\begin{aligned} V \text{ is reduced} &\iff \mathfrak{N}=0; \\ V \text{ is irreducible} &\iff \mathfrak{N} \text{ is prime;} \\ V \text{ is reduced and irreducible} &\iff \mathcal{O}(V) \text{ is an integral domain.} \end{aligned}$$

The first statement follows from the definitions, the second statement has already been noted (III, §1), and the third statement follows from the first two.

2.5 Recall (CA 3.12) that the ***height*** $\mathrm{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ in a noetherian ring A is the greatest length d of a chain of distinct prime ideals

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_d,$$

and that the ***Krull dimension*** of A is

$$\sup\{\mathrm{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{spm}(A)\}.$$

2.6 The ***dimension*** of an affine algebraic scheme V is the Krull dimension of $\mathcal{O}(V)$ — this is finite (CA 13.11). When V is irreducible, the nilradical $\mathfrak{N}$ of $\mathcal{O}(V)$ is prime, and so $\mathcal{O}(V)/\mathfrak{N}$ is an integral domain. In this case, the dimension of V is the transcendence degree over k of the field of fractions of $\mathcal{O}(V)/\mathfrak{N}$, and every maximal chain of distinct prime ideals in $\mathcal{O}(V)$ has length $\dim V$ (CA 13.8). Therefore, every maximal chain of distinct irreducible closed subsets of V has length $\dim V$. For example, the dimension of $\mathbb{A}^n$ is the transcendence degree of $k(X_1,\ldots,X_n)$ over k, which is n.

3 Algebraic groups as groups in the category of affine algebraic schemes

Finite products exist in the category of affine algebraic schemes over k. For example, the product of the affine algebraic schemes V and W is $\mathrm{Spec}(\mathcal{O}(V)\otimes\mathcal{O}(W))$, and $* = \mathrm{Spm}(k)$ is a final object. Therefore monoid objects and group objects are defined. A monoid (resp. group) in the category of affine algebraic schemes over k is called an ***affine algebraic monoid scheme*** (resp. ***affine algebraic group scheme***) over k.

As the tensor product of two affine k-algebras is again affine (§1), the category of affine algebraic varieties also has products. A monoid object (resp. group object) in the category of affine algebraic varieties is called an ***affine monoid variety*** (resp. ***affine group variety***).

An affine algebraic scheme V defines a functor

$$R \rightsquigarrow V(R) \overset{\text{def}}{=} \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(V), R), \tag{51}$$

from k-algebras to sets. For example, $\mathbb{A}^n(R) \simeq R^n$ for all k-algebras R. Let V' be the functor defined by V. It follows from (III, 2.2) and the Yoneda lemma that $V \rightsquigarrow V'$ is an equivalence from the category of algebraic schemes over k to the category of functors from k-algebras to sets representable by finitely generated k-algebras. Group structures on V correspond to factorizations of V' through the category of groups. Thus $V \rightsquigarrow V'$ is an equivalence from the category of affine algebraic group schemes over k to the category of functors $\mathsf{Alg}_k \to \mathsf{Grp}$ representable by finitely generated k-algebras, with quasi-inverse $G \rightsquigarrow \mathrm{Spm}(\mathcal{O}(G))$.

The functor $V \rightsquigarrow \mathcal{O}(V)$ is an equivalence from the category of algebraic schemes over k to the category of finitely generated k-algebras (cf. III, 2.2). Group structures on V correspond to Hopf algebra structures on $\mathcal{O}(V)$. Thus $V \rightsquigarrow \mathcal{O}(V)$ is a contravariant equivalence from the category of affine algebraic group schemes over k to the category of finitely generated Hopf algebras over k.

PROPOSITION 3.1 *Let k be a field. The functor $(V,m) \rightsquigarrow (V',m')$ is an equivalence from the category of affine algebraic group schemes over k to the category of affine algebraic groups over k, with quasi-inverse $G \rightsquigarrow \mathrm{Spm}\,\mathcal{O}(G)$.*

There is a similar statement with "group" replaced by "monoid".

For an affine algebraic group G, we let $|G|$, denote the corresponding affine group scheme; thus $|G| = \mathrm{Spm}(\mathcal{O}(G))$. The ***dimension*** of an algebraic group G is defined to be the Krull dimension of $\mathcal{O}(G)$. When $\mathcal{O}(G)$ is an integral domain, this is equal to the transcendence degree of $\mathcal{O}(G)$ over k (CA 13.8).

Is the set $|G|$ a group?

Not usually. The problem is that the functor spm does not send sums to products. For example, when k_1 and k_2 are finite field extensions of k, the set $\mathrm{spm}(k_1 \otimes_k k_2)$ may have several points[2] whereas $\mathrm{spm}(k_1) \times \mathrm{spm}(k_2)$ has only one. For an algebraic group G, there is a canonical map $|G \times G| \to |G| \times |G|$, but the map

$$|G \times G| \to |G|$$

defined by m need not factor through it.

However, $|G|$ *is* a group when k is algebraically closed. Then the Nullstellensatz shows that $|G| \simeq G(k)$, and so $|G|$ inherits a group structure from $G(k)$. To put it another way, for finitely generated algebras A_1 and A_2 over an algebraically closed field k,

$$\mathrm{spm}(A_1 \otimes A_2) \simeq \mathrm{spm}(A_1) \times \mathrm{spm}(A_2) \tag{52}$$

(as sets, not as topological spaces[3]), and so the forgetful functor $(V,\mathcal{O}) \rightsquigarrow V$ sending an affine algebraic scheme over k to its underlying set preserves finite products, and hence also monoid objects and group objects.

[2] For example, if k_1/k is separable, then

$$k_1 = k[a] \simeq k[X]/(f)$$

for a suitable element a and its minimum polynomial f. Let $f = f_1 \cdots f_r$ be the factorization of f into its irreducible factors in k_2 (they are distinct because k_1/k is separable). Now

$$k_1 \otimes_k k_2 \simeq k_2[X]/(f_1 \cdots f_r) \simeq \prod\nolimits_{i=1}^{r} k_2[X]/(f_i)$$

by the Chinese remainder theorem. Therefore $\mathrm{spm}(k_1 \otimes_k k_2)$ has r points.

[3] When regarded as a functor to topological spaces, $(V,\mathcal{O}) \rightsquigarrow V$ does not preserve finite products: the topology on $V \times W$ is not the product topology. For an affine algebraic group G, the map $m\colon |G| \times |G| \to |G|$ is not usually continuous relative to the product topology, and so $|G|$ is not a topological group for the Zariski topology.

Assume k is perfect, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. Then $|G| \simeq \Gamma\backslash G(k^{\mathrm{al}})$ and $G(k) \simeq G(k^{\mathrm{al}})^{\Gamma}$. In other words, $|G|$ can be identified with the set of Γ-orbits in $G(k^{\mathrm{al}})$ and $G(k)$ with the set of Γ-orbits consisting of a single point. While the latter inherits a group structure from $G(k)$, the former need not.

The situation is worse with spec. For example, (52) fails for spec even when k is algebraically closed.

4 Terminology

From now on "group scheme" and "algebraic group scheme" will mean "affine group scheme" and "affine algebraic group scheme"; similarly for "group variety", "monoid variety", "monoid scheme" and "algebraic monoid scheme".

5 Homogeneity

Let G be an algebraic group over a field k. An element a of $G(k)$ defines an element of $G(R)$ for each k-algebra R, which we denote a_R (or just a). Let e denote the identity element of $G(k)$.

PROPOSITION 5.1 *For each $a \in G(k)$, the natural map*

$$L_a\colon G(R) \to G(R), \quad g \mapsto a_R g,$$

is an isomorphism of set-valued functors. Moreover,

$$L_e = \mathrm{id}_G \text{ and } L_a \circ L_b = L_{ab}, \quad \text{all } a,b \in G(k).$$

Here e is the neutral element in $G(k)$.

PROOF. The second statement is obvious, and the first follows from it, because the equalities

$$L_a \circ L_{a^{-1}} = L_e = \mathrm{id}_G$$

show that L_a is an isomorphism. □

The homomorphism $\mathcal{O}(G) \to \mathcal{O}(G)$ defined by L_a is the composite of the homomorphisms

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{a \otimes \mathcal{O}(G)} k \otimes \mathcal{O}(G) \simeq \mathcal{O}(G). \tag{53}$$

For $a \in G(k)$, we let $\mathfrak{m}_a$ denote the kernel of $a\colon \mathcal{O}(G) \to k$; thus

$$\mathfrak{m}_a = \{f \in \mathcal{O}(G) \mid f_k(a) = 0\}$$

(see the notations I, 3.13). Then $\mathcal{O}(G)/\mathfrak{m}_a \simeq k$, and so $\mathfrak{m}_a$ is a maximal ideal in $\mathcal{O}(G)$. Note that $\mathcal{O}(G)_{\mathfrak{m}_a}$ is the ring of fractions obtained from $\mathcal{O}(G)$ by inverting the elements of the multiplicative set $\{f \in \mathcal{O}(G) \mid f_k(a) \neq 0\}$.

PROPOSITION 5.2 *For each $a \in G(k)$, $\mathcal{O}(G)_{\mathfrak{m}_a} \simeq \mathcal{O}(G)_{\mathfrak{m}_e}$.*

PROOF. The isomorphism $\ell_a\colon\mathcal{O}(G)\to\mathcal{O}(G)$ corresponding (by the Yoneda lemma) to L_a is defined by $\ell_a(f)_R(g)=f_R(a_Rg)$, all $g\in G(R)$. Therefore, $\ell_a^{-1}\mathfrak{m}_e=\mathfrak{m}_a$, and so ℓ_a extends to an isomorphism $\mathcal{O}(G)_{\mathfrak{m}_a}\to\mathcal{O}(G)_{\mathfrak{m}_e}$ (because of the universal property of rings of fractions; CA 6.1). □

COROLLARY 5.3 *When k is algebraically closed, the local rings $\mathcal{O}(G)_{\mathfrak{m}}$ at maximal ideals $\mathfrak{m}$ of $\mathcal{O}(G)$ are all isomorphic.*

PROOF. When k is algebraically closed, the Nullstellensatz (CA 11.6) shows that all maximal ideals in $\mathcal{O}(G)$ are of the form $\mathfrak{m}_a$ for some $a\in G(k)$. □

5.4 The corollary fails when k is not algebraically closed. For example, for the algebraic group μ_3 over $\mathbb{Q}$,

$$\mathcal{O}(\mu_3)=\frac{k[X]}{(X^3-1)}\simeq\frac{k[X]}{(X-1)}\times\frac{k[X]}{(X^2+X+1)}\simeq\mathbb{Q}\times\mathbb{Q}[\sqrt{-3}],$$

and so the local rings are $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{-3}]$.

6 Reduced algebraic groups

An algebraic group G is ***reduced*** if $|G|$ is reduced, i.e., if $\mathcal{O}(G)$ has no nilpotents.

PROPOSITION 6.1 *Let G be a reduced algebraic group over a field k. If $G(K)=\{1\}$ for some algebraically closed field K containing k, then G is the trivial algebraic group, i.e., $\mathcal{O}(G)=k$.*

PROOF. Every maximal ideal of $\mathcal{O}(G)$ arises as the kernel of a homomorphism $\mathcal{O}(G)\to K$ (Nullstellensatz, CA 11.5), and so $\mathcal{O}(G)$ has only one maximal ideal $\mathfrak{m}$. As $\mathcal{O}(G)$ is reduced, the intersection of its maximal ideals is zero (CA 11.8), and so $\mathfrak{m}=0$. Therefore $\mathcal{O}(G)$ is a field. It contains k, and the identity element in G is a homomorphism $\mathcal{O}(G)\to k$, and so $\mathcal{O}(G)=k$. □

6.2 The proposition is false for nonreduced groups. For example, $\alpha_p(K)=\{1\}$ for every field K containing k, but α_p is not the trivial group.

For a k-algebra A, we let A_{red} denote the quotient of A by its nilradical. Thus A_{red} is a reduced k-algebra, and the quotient map $A\to A_{\mathrm{red}}$ is universal for homomorphisms from A to reduced k-algebras.

PROPOSITION 6.3 *Let G be an algebraic group over a field k. If the comultiplication map Δ factors through $\mathcal{O}(G)_{\mathrm{red}}$, then there is a unique Hopf algebra structure on $\mathcal{O}(G)_{\mathrm{red}}$ such that $\mathcal{O}(G)\to\mathcal{O}(G)_{\mathrm{red}}$ is a homomorphism of Hopf algebras. Let $G_{\mathrm{red}}\to G$ be the corresponding homomorphism of algebraic groups. Every homomorphism $H\to G$ with H a reduced algebraic group factors uniquely through $G_{\mathrm{red}}\to G$.*

PROOF. Let (Δ, ϵ, S) be the Hopf algebra structure on $\mathcal{O}(G)$, and consider the composites

$$\begin{aligned}
&\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes \mathcal{O}(G) \to \mathcal{O}(G)_{\mathrm{red}} \otimes \mathcal{O}(G)_{\mathrm{red}} \\
&\mathcal{O}(G) \xrightarrow{\epsilon} k \\
&\mathcal{O}(G) \xrightarrow{S} \mathcal{O}(G) \to \mathcal{O}(G)_{\mathrm{red}}.
\end{aligned}$$

The lower two maps obviously factor through $\mathcal{O}(G)_{\mathrm{red}}$, and if the top map $\mathcal{O}(G) \to \mathcal{O}(G)_{\mathrm{red}} \otimes \mathcal{O}(G)_{\mathrm{red}}$ factors through $\mathcal{O}(G)_{\mathrm{red}}$ then the maps define a Hopf algebra structure on $\mathcal{O}(G)_{\mathrm{red}}$, which is the unique Hopf algebra structure for which the quotient map $\mathcal{O}(G) \to \mathcal{O}(G)_{\mathrm{red}}$ is a homomorphism. The rest of the statement is obvious. □

The algebraic group G_{red} is called the reduced algebraic group ***associated with*** or ***attached to*** G.

6.4 If k is perfect, then Δ always factors through $\mathcal{O}(G)_{\mathrm{red}}$ — the k-algebra $\mathcal{O}(G)_{\mathrm{red}}$ is an affine k-algebra (§1), and so $\mathcal{O}(G)_{\mathrm{red}} \otimes \mathcal{O}(G)_{\mathrm{red}}$ is also an affine k-algebra; in particular, it is reduced.

6.5 When k is not perfect, a Hopf algebra structure on A need not pass to the quotient A_{red} For example, let k be a nonperfect field of characteristic p, so that there exists an $a \in k \smallsetminus k^p$, and let G be the algebraic group ☠

$$R \rightsquigarrow G(R) = \{x \in R \mid x^{p^2} = ax^p\}.$$

Then

$$\begin{aligned}
\mathcal{O}(G) &= k[X]/(X^{p^2} - aX^p) \\
\mathcal{O}(G)_{\mathrm{red}} &= k[X]/(X(X^{p(p-1)} - a)).
\end{aligned}$$

Then $\mathcal{O}(G)_{\mathrm{red}} \otimes k^{\mathrm{al}}$ is not reduced but its localization at the ideal (x) is reduced; therefore G_{red} is not an algebraic group. See also Exercise XIII-7 below and SGA 3, VI_A, 1.3.2.

7 Smooth algebraic schemes

We review some definitions and results in commutative algebra.

7.1 Let $\mathfrak{m}$ be a maximal ideal of a noetherian ring A, and let $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$ be the maximal ideal of the local ring $A_{\mathfrak{m}}$; for all natural numbers $r \leq s$, the map

$$a + \mathfrak{m}^s \mapsto a + \mathfrak{n}^s \colon \mathfrak{m}^r/\mathfrak{m}^s \to \mathfrak{n}^r/\mathfrak{n}^s$$

is an isomorphism (CA 6.7).

7.2 Let A be a local noetherian ring with maximal ideal $\mathfrak{m}$ and residue field k. Then $\mathfrak{m}/\mathfrak{m}^2$ is a k-vector space of dimension equal to the minimum number of generators of $\mathfrak{m}$ (Nakayama's lemma, CA 3.9). Moreover, $\mathrm{ht}(\mathfrak{m}) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ (CA 16.5), and when equality holds A is said to be ***regular***. Every regular noetherian local ring is an integral domain (CA 17.3).

7.3 A point $\mathfrak{m}$ of an affine algebraic scheme V is said to be ***regular*** if the local ring $\mathcal{O}(V)_{\mathfrak{m}}$ is regular, and V is said to be ***regular*** if all of its closed points are regular.[4] A regular affine algebraic scheme is reduced. To see this, let f be a nilpotent element of $\mathcal{O}(V)$; as f maps to zero in $\mathcal{O}(V)_{\mathfrak{m}}$, $sf = 0$ for some $s \in \mathcal{O}(V) \setminus \mathfrak{m}$; therefore the annihilator of f is an ideal $\mathcal{O}(V)$ not contained in any maximal ideal, and so it equals $\mathcal{O}(V)$.

7.4 An affine algebraic scheme V over k is said to be ***smooth*** if $V_{k^{\mathrm{al}}}$ is regular. If V is smooth, then V_K is regular for all fields K containing k; in particular, V itself is regular (CA 18.14). If V is smooth, then it follows from (7.3) that $\mathcal{O}(V)$ is an affine k-algebra, and so V is an algebraic variety. Every affine algebraic variety contains a regular point (CA 18.15).

8 Smooth algebraic groups

An algebraic group G is said to be ***smooth*** if $|G|$ is smooth, and it is ***connected*** if $|G|$ is connected (as a topological space).

PROPOSITION 8.1 *Let H be an algebraic subgroup of an algebraic group G. Then* $\dim H \leq \dim G$, *and* $\dim H < \dim G$ *if G is smooth and connected and $H \neq G$.*

PROOF. Because $\mathcal{O}(H)$ is a quotient of $\mathcal{O}(G)$, $\dim(\mathcal{O}(H)) \leq \dim(\mathcal{O}(G))$. If G is smooth and connected, then $\mathcal{O}(G)$ is an integral domain; if $H \neq G$, then $\dim H < \dim G$ by (CA 13.3). □

PROPOSITION 8.2 *An algebraic group G over an algebraically closed field k is smooth if and only if $\mathcal{O}(G)_{\mathfrak{m}_e}$ is regular, where* $\mathfrak{m}_e = \mathrm{Ker}(\epsilon \colon \mathcal{O}(G) \to k)$.

PROOF. If $\mathcal{O}(G)_{\mathfrak{m}}$ is regular for $\mathfrak{m} = \mathfrak{m}_e$, then $\mathcal{O}(G)_{\mathfrak{m}}$ is regular for all $\mathfrak{m}$ by homogeneity (5.2). Hence G is smooth. □

PROPOSITION 8.3 *(a) An algebraic group G is smooth if and only if $|G|$ is geometrically reduced (i.e., an algebraic variety).*

(b) An algebraic group G over a perfect field is smooth if and only if $|G|$ is reduced.

PROOF. (a) If G is smooth, then $|G|$ is an algebraic variety by (7.4). For the converse, we have to show that $G_{k^{\mathrm{al}}}$ is regular. According to (7.4), $G_{k^{\mathrm{al}}}$ has a regular point, and so, by homogeneity (5.2), all of its points are regular.

(b) When k is perfect, a finitely generated k-algebra A is reduced if and only if $k^{\mathrm{al}} \otimes A$ is reduced (see CA 18.1). Thus (b) follows from (a). □

COROLLARY 8.4 *An algebraic group G over an algebraically closed field k is smooth if every nilpotent element of $\mathcal{O}(G)$ is contained in $\mathfrak{m}_e^2$.*

[4] This then implies that local ring at every (not necessarily closed) point is regular (for a noetherian ring A, if $A_{\mathfrak{m}}$ is regular for all maximal ideals, then $A_{\mathfrak{p}}$ is regular for all prime ideals (CA 17.5a).

PROOF. Let $\bar{G}$ be the reduced algebraic group attached to G (see 6.3), and let $\bar{e}$ be the neutral element of $\bar{G}(k)$. By definition, $\mathcal{O}(\bar{G}) = \mathcal{O}(G)/\mathfrak{N}$ where $\mathfrak{N}$ is the nilradical of $\mathcal{O}(G)$. Every prime ideal of $\mathcal{O}(G)$ contains $\mathfrak{N}$, and so the prime ideals of $\mathcal{O}(G)$ and $\mathcal{O}(\bar{G})$ are in natural one-to-one correspondence. Therefore $\mathfrak{m}_e$ and $\mathfrak{m}_{\bar{e}}$ have the same height, and so

$$\dim \mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}} = \dim \mathcal{O}(G)_{\mathfrak{m}_e}$$

(Krull dimensions). The hypothesis on $\mathcal{O}(G)$ implies that

$$\mathfrak{m}_e/\mathfrak{m}_e^2 \to \mathfrak{m}_{\bar{e}}/\mathfrak{m}_{\bar{e}}^2$$

is an isomorphism of k-vector spaces. Because $|\bar{G}|$ is a reduced, $\bar{G}$ is smooth (8.3); in particular, $\mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}}$ is regular, and so

$$\dim_k(\mathfrak{m}_{\bar{e}}/\mathfrak{m}_{\bar{e}}^2) = \dim \mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}}.$$

Therefore

$$\dim_k(\mathfrak{m}_e/\mathfrak{m}_e^2) = \dim \mathcal{O}(G)_{\mathfrak{m}_e},$$

and so $\mathcal{O}(G)_{\mathfrak{m}_e}$ is regular. This implies that G is smooth (8.2). □

☠ 8.5 A reduced algebraic group over a nonperfect field need not be smooth. For example, let k be such a field, so that $\mathrm{char}(k) = p \neq 0$ and there exists an element a of k that is not a pth power. Then the subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $Y^p = aX^p$ is reduced but not smooth. Indeed,

$$\mathcal{O}(G) = k[X,Y]/(Y^p - aX^p),$$

which is an integral domain because $Y^p - aX^p$ is irreducible in $k[X,Y]$, but

$$\mathcal{O}(G_{k^{\mathrm{al}}}) = k^{\mathrm{al}}[X,Y]/(Y^p - aX^p) = k^{\mathrm{al}}[x,y]$$

contains the nilpotent element $y - a^{\frac{1}{p}}x$. The reduced subgroup $(G_{k^{\mathrm{al}}})_{\mathrm{red}}$ of $G_{k^{\mathrm{al}}}$ is the subgroup of $\mathbb{G}_a \times \mathbb{G}_a$ is defined by $Y = a^{\frac{1}{p}}X$, which is not defined over k (as a subgroup of $\mathbb{G}_a \times \mathbb{G}_a$).

Note that G is the kernel of $(x,y) \mapsto y^p - ax^p \colon \mathbb{G}_a \times \mathbb{G}_a \xrightarrow{\alpha} \mathbb{G}_a$. Therefore, although $\mathrm{Ker}(\alpha_{k^{\mathrm{al}}})$ is (of course) defined over k, $\mathrm{Ker}(\alpha_{k^{\mathrm{al}}})_{\mathrm{red}}$ is not.

9 Algebraic groups in characteristic zero are smooth (Cartier's theorem)

We first prove two lemmas.

LEMMA 9.1 *Let V and V' be vector spaces over a field,*[5] *and let W be a subspace of V. For $x \in V$, $y \in V'$,*

$$x \otimes y \in W \otimes V' \iff x \in W \text{ or } y = 0.$$

PROOF. The element $x \otimes y$ lies in $W \otimes V'$ if and only if its image in $V \otimes V'/W \otimes V'$ is zero. But

$$V \otimes V'/W \otimes V' \simeq (V/W) \otimes V',$$

and the image $\bar{x} \otimes y$ of $x \otimes y$ in $(V/W) \otimes V'$ is zero if and only if $\bar{x} = 0$ or $y = 0$. □

[5] It suffices to require V and V' to be modules over a ring with V' faithfully flat.

LEMMA 9.2 *Let (A,Δ,ϵ) be a Hopf algebra over k, and let $I=\mathrm{Ker}(\epsilon)$.*

(a) *As a k-vector space, $A=k\oplus I$.*
(b) *For any $a\in I$,*

$$\Delta(a)=a\otimes 1+1\otimes a \quad \mathrm{mod}\ I\otimes I.$$

PROOF. (a) The maps $k\longrightarrow A\xrightarrow{\epsilon}k$ are k-linear, and compose to the identity. Therefore $A=k\oplus I$ and $a\in A$ decomposes as $a=\epsilon(a)+(a-\epsilon(a))\in k\oplus I$.

(b) Using condition (b) of II, 2.1, we find that, for $a\in I$,

$$(\mathrm{id}\otimes\epsilon)(\Delta(a)-a\otimes 1-1\otimes a)=a-a-0=0$$
$$(\epsilon\otimes\mathrm{id})(\Delta(a)-a\otimes 1-1\otimes a)=a-0-a=0.$$

Hence

$$\begin{aligned}\Delta(a)-a\otimes 1-1\otimes a&\in\mathrm{Ker}(\mathrm{id}\otimes\epsilon)\cap\mathrm{Ker}(\epsilon\otimes\mathrm{id})\\&=A\otimes I\cap I\otimes A\\&=I\otimes I.\end{aligned}$$

□

THEOREM 9.3 (CARTIER 1962) *Every algebraic group over a field of characteristic zero is smooth.*

PROOF. We may replace k with its algebraic closure. Thus, let G be an algebraic group over an algebraically closed field k of characteristic zero, and let $A=\mathcal{O}(G)$. Let $\mathfrak{m}=\mathfrak{m}_e=\mathrm{Ker}(\epsilon)$. Let a be a nilpotent element of A; according to (8.4), it suffices to show that a lies in $\mathfrak{m}^2$.

If a maps to zero in $A_{\mathfrak{m}}$, then it maps to zero in $A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2$, and therefore in $A/\mathfrak{m}^2$ by (7.1), and so $a\in\mathfrak{m}^2$. Thus, we may suppose that there exists an $n\geq 2$ such that $a^n=0$ in $A_{\mathfrak{m}}$ but $a^{n-1}\neq 0$ in $A_{\mathfrak{m}}$. Now $sa^n=0$ in A for some $s\notin\mathfrak{m}$. On replacing a with sa, we find that $a^n=0$ in A but $a^{n-1}\neq 0$ in $A_{\mathfrak{m}}$.

Now $a\in\mathfrak{m}$ (because $A/\mathfrak{m}=k$ has no nilpotents), and so (see 9.2)

$$\Delta(a)=a\otimes 1+1\otimes a+y \quad \text{with} \quad y\in\mathfrak{m}\otimes_k\mathfrak{m}.$$

Because Δ is a homomorphism of k-algebras,

$$0=\Delta(a^n)=(\Delta a)^n=(a\otimes 1+1\otimes a+y)^n. \tag{54}$$

When expanded, the right hand side becomes a sum of terms

$$a^n\otimes 1,\quad n(a^{n-1}\otimes 1)\cdot(1\otimes a+y),\quad (a\otimes 1)^h(1\otimes a)^i y^j\quad (h+i+j=n, i+j\geq 2).$$

As $a^n=0$ and the terms with $i+j\geq 2$ lie in $A\otimes\mathfrak{m}^2$, equation (54) shows that

$$na^{n-1}\otimes a+n(a^{n-1}\otimes 1)y\in A\otimes\mathfrak{m}^2,$$

and so

$$na^{n-1}\otimes a\in a^{n-1}\mathfrak{m}\otimes A+A\otimes\mathfrak{m}^2\quad(\text{inside } A\otimes_k A).$$

In the quotient $A \otimes \left(A/\mathfrak{m}^2\right)$ this becomes

$$na^{n-1} \otimes \bar{a} \in a^{n-1}\mathfrak{m} \otimes A/\mathfrak{m}^2 \quad (\text{inside } A \otimes A/\mathfrak{m}^2). \tag{55}$$

Note that $a^{n-1} \notin a^{n-1}\mathfrak{m}$, because if $a^{n-1} = a^{n-1}m$ with $m \in \mathfrak{m}$, then $(1-m)a^{n-1} = 0$ and, as $1-m$ is a unit in $A_{\mathfrak{m}}$, this would imply $a^{n-1} = 0$ in $A_{\mathfrak{m}}$, which is a contradiction. Moreover n is a unit in A because it is a nonzero element of k. We conclude that $na^{n-1} \notin a^{n-1}\mathfrak{m}$, and so (see 9.1) $\bar{a} = 0$. In other words, $a \in \mathfrak{m}^2$, as required. □

COROLLARY 9.4 *Let G be an algebraic group over a field of characteristic zero. If $G(K) = \{1\}$ for some algebraically closed field K, then G is the trivial algebraic group.*

PROOF. According to the theorem, G is reduced, and so we can apply Proposition 6.1. □

ASIDE 9.5 Let k be an arbitrary commutative ring. A functor $F\colon \mathsf{Alg}_k \to \mathsf{Set}$ is said to be ***formally smooth*** if, for any k-algebra A and nilpotent ideal $\mathfrak{n}$ in A, the map $F(A) \to F(A/\mathfrak{n})$ is surjective. A k-scheme X is ***smooth*** over k if it is locally of finite presentation and the functor $A \rightsquigarrow X(A) \overset{\text{def}}{=} \mathrm{Hom}_k(\operatorname{Spec} A, X)$ is formally smooth. There is the following criterion (SGA1, II):

> a finitely presented morphism is smooth if it is flat and its geometric fibres are nonsingular algebraic varieties.

Therefore, when the ring k contains a field of characteristic zero, Cartier's theorem (9.3) shows that every flat affine group scheme of finite presentation over k is smooth.

ASIDE 9.6 In the language of SGA 3, Theorem 9.3 says that every affine algebraic group scheme over a field of characteristic zero is smooth. More generally, *every* group scheme (not necessarily affine) over a field of characteristic zero is geometrically reduced (extension by Perrin of Cartier's theorem; SGA 3, VI_A, 6.9).

10 Smoothness in characteristic $p \neq 0$

THEOREM 10.1 *An algebraic group G over an algebraically closed field k of characteristic $p \neq 0$ is smooth if $\mathcal{O}(G)$ has the following property:*

$$a \in \mathcal{O}(G), \quad a^p = 0 \implies a = 0. \tag{56}$$

PROOF. Let a be a nilpotent element of $\mathcal{O}(G)$. As in the proof of Theorem 9.3, we may suppose that $a^n = 0$ in $\mathcal{O}(G)$ but $a^{n-1} \neq 0$ in $\mathcal{O}(G)_{\mathfrak{m}_e}$. If $p|n$, then $(a^{\frac{n}{p}})^p = 0$, and so $a^{\frac{n}{p}} = 0$, which is a contradiction. Therefore n is nonzero in k, and the argument in the proof of Theorem 9.3 shows that $a \in \mathfrak{m}_e^2$. □

COROLLARY 10.2 *For all $r \geq 1$, the image of $a \mapsto a^{p^r}\colon \mathcal{O}(G) \to \mathcal{O}(G)$ is a Hopf subalgebra of $\mathcal{O}(G)$, and for all sufficiently large r, it is a reduced Hopf algebra.*

PROOF. Let k be a field of characteristic $p \neq 0$. For a k-algebra R, we let f_R denote the homomorphism $a \mapsto a^p\colon R \to R$. When $R = k$, we omit the subscript. We let ${}_f R$ denote the ring R regarded as a k-algebra by means of the map $k \xrightarrow{f} k \longrightarrow R$. Let G be an algebraic group over k, and let $G^{(p)}$ be the functor $R \rightsquigarrow G({}_fR)$. This is represented by $k \otimes_{f,k} \mathcal{O}(G)$ (tensor product of $\mathcal{O}(G)$ with k relative to the map $f\colon k \to k$),

$$\begin{tikzcd}
 & & R \\
\mathcal{O}(G) \arrow[r] \arrow[urr, dashed] & k \otimes_{f,k} \mathcal{O}(G) \arrow[ur, dashed] & \\
k \arrow[u] \arrow[r, "f"] & k, \arrow[u] \arrow[uur] &
\end{tikzcd}$$

and so it is again an algebraic group. The k-algebra homomorphism $f_R\colon R \to {}_fR$ defines a homomorphism $G(R) \to G^{(p)}(R)$, which is natural in R, and so arises from a homomorphism $F\colon G \to G^{(p)}$ of algebraic groups. This homomorphism corresponds to the homomorphism of Hopf algebras

$$c \otimes a \mapsto ca^p\colon \mathcal{O}(G^{(p)}) \to \mathcal{O}(G).$$

When k is perfect, this has image $\mathcal{O}(G)^p$, which is therefore a Hopf subalgebra of $\mathcal{O}(G)$ (Exercise II-6). On repeating this argument with f and F replaced by f^r and F^r, we find that $\mathcal{O}(G)^{p^r}$ is a Hopf subalgebra of $\mathcal{O}(G)$.

Concerning the second part of the statement, because the nilradical $\mathfrak{N}$ of $\mathcal{O}(G)$ is finitely generated, there exists an exponent n such that $a^n = 0$ for all $a \in \mathfrak{N}$. Let r be such that $p^r \geq n$; then $a^{p^r} = 0$ for all $a \in \mathfrak{N}$. With this r, $\mathcal{O}(G)^{p^r}$ satisfies (56). As it is a Hopf algebra, it is reduced. □

NOTES The first part of (10.2) only requires that k be perfect (probably the same is true of the remaining statements).

11 Appendix: The faithful flatness of Hopf algebras

In this section, we prove the following very important technical result.

THEOREM 11.1 *For any Hopf algebras $A \subset B$ over a field k, B is faithfully flat over A.*

Let k' be a field containing k. The homomorphism $A \to k' \otimes A$ is faithfully flat, and so it suffices to show that $k' \otimes B$ is faithfully flat over $k' \otimes A$ (CA 9.4). This allows us to assume that k is algebraically closed.

The homomorphism $A \to B$ corresponds to a homomorphism $\varphi\colon H \to G$ of affine groups over k with $\mathcal{O}(H) = B$ and $\mathcal{O}(G) = A$:

$$\begin{tikzcd}
\mathcal{O}(H) & \mathcal{O}(G) \arrow[l] \\
H \arrow[r, "\varphi"] & G \\
B & A. \arrow[l]
\end{tikzcd}$$

We regard H and G as algebraic group schemes, i.e., we write H and G for $|H|$ and $|G|$. Because k is algebraically closed, the underlying set of H (resp. G) can be identified with $H(k)$ (resp. $G(k)$), which is a group (see §3)

Case that A is reduced and A and B are finitely generated.

We begin with a remark. Let V be an algebraic scheme over an algebraically closed field. Then V is a finite union $V = V_1 \cup \cdots \cup V_r$ of its irreducible components (III, 1). Assume that V is homogeneous, i.e., for any pair (a,b) of points of V, there exists an isomorphism $V \to V$ sending a to b. As some point of V lies on a single component, all do, and so V is a disjoint union of the V_i. As every V_i is closed, they are also open, and they are the connected components of V. When V_i is reduced, the ring $\mathcal{O}(V_i)$ is an integral domain.

Hence H and G are disjoint unions of their connected components, say $H = \bigsqcup_{i \in I} H_i$ and $G = \bigsqcup_{j \in J} G_j$. Because G is reduced, each ring $\mathcal{O}(G_i)$ is an integral domain, and $\mathcal{O}(G) = \prod_{j \in J} \mathcal{O}(G_j)$. Each connected component H_i of H is mapped by φ into a connected component $G_{j(i)}$ of G. The map $i \mapsto j(i)\colon I \to J$ is surjective, because otherwise $\mathcal{O}(G) \to \mathcal{O}(H)$ would not be injective (if j_0 were not in the image, then an $f \in \mathcal{O}(G)$ such that $f|G_j = 0$ for $j \neq j_0$ would have $f \circ \varphi = 0$).

Let H° (resp. G°) be the connected component of H (resp. G) containing the identity element. Then H° maps into G°. Because $\mathcal{O}(G^\circ)$ is an integral domain, the generic flatness theorem (CA 9.12; CA 16.9) shows that there exists a $c \in H^\circ$ such that $\mathcal{O}(H)_{\mathfrak{m}_c}$ is faithfully flat over $\mathcal{O}(G)_{\mathfrak{m}_{\varphi(c)}}$. Homogeneity, more precisely, the commutative diagrams

$$\begin{tikzcd}
H \arrow[r, "L_b"] \arrow[d] & H \arrow[d] \\
G \arrow[r, "L_{\varphi(b)}"] & G
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\mathcal{O}(H)_{\mathfrak{m}_e} & \mathcal{O}(H)_{\mathfrak{m}_b} \arrow[l, "\simeq"'] \\
\mathcal{O}(G)_{m_e} \arrow[u] & \mathcal{O}(G)_{\mathfrak{m}_{\varphi(b)}} \arrow[l, "\simeq"'] \arrow[u]
\end{tikzcd}$$

(see §5), now implies that $\mathcal{O}(H)_{\mathfrak{m}_b}$ is faithfully flat over $\mathcal{O}(G)_{\mathfrak{m}_{\varphi(b)}}$ for all $b \in H$. Hence $\mathcal{O}(H)$ is flat over $\mathcal{O}(G)$ (CA 9.9), and it remains to show that $\varphi\colon H \to G$ is surjective as a map of sets (CA 9.10c). According to (CA 12.14), $\varphi(H)$ contains a nonempty open subset U of G°. For any $g \in G^\circ$, the sets U^{-1} and Ug^{-1} have nonempty intersection (because G° is irreducible). This means that there exist $u,v \in U$ such that $u^{-1} = vg^{-1}$, and so $g = uv \in U$. Thus $\varphi(H) \supset G^\circ$, and it follows that the translates of G° by points in $\varphi(H)$ cover G (because I maps onto J).

Case that the augmentation ideal of A is nilpotent

We begin with a remark. Let $H \to G$ be a homomorphism of abstract groups with kernel N. Then the map

$$(h,n) \mapsto (hn,h)\colon H \times N \to H \times_G H \tag{57}$$

is a bijection — this just says that two elements of H with the same image in G differ by an element of the kernel. Similarly, for a homomorphism $\varphi\colon H \to G$ of affine groups, there is an isomorphism

$$H \times N \to H \times_G H \tag{58}$$

that becomes the map (57) for each k-algebra R. Because of the correspondence between affine groups and Hopf algebras, this implies that, for any homomorphism $A \to B$ of Hopf algebras, there is a canonical isomorphism of left B-modules

$$B \otimes_A B \to B \otimes_k (B/I_A B) \tag{59}$$

where I_A is the augmentation ideal $\mathrm{Ker}(A \xrightarrow{\epsilon} k)$ of A.

Let $I = I_A$, and assume that I is nilpotent, say $I^n = 0$. Choose a family $(e_j)_{j\in J}$ of elements in B whose image in B/IB is a k-basis and consider the map

$$(a_j)_{j\in J} \mapsto \textstyle\sum_j a_j e_j \colon A^{(J)} \to B \tag{60}$$

where $A^{(J)}$ is a direct sum of copies of A indexed by J. We shall show that (60) is an isomorphism (hence B is even free as an A-module).

Let C be the cokernel of (60). A diagram chase in

$$\begin{tikzcd}
A^{(J)} \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] & 0 \\
(A/I)^{(J)} \arrow[r, "\text{onto}"] & B/IB & &
\end{tikzcd}$$

shows that every element of C is the image of an element of B mapping to zero in B/IB, i.e., lying in IB. Hence $C = IC$, and so $C = IC = I^2C = \cdots = I^nC = 0$. Hence $A^{(J)} \to B$ is surjective.

For the injectivity, consider the diagrams

$$\begin{tikzcd}
 & A^{(J)} \arrow[r, "\text{onto}"] \arrow[d] & B \arrow[d] & k^{(J)} \arrow[r, "\simeq"] \arrow[d] & B/IB \arrow[d] \\
M \arrow[r] & B^{(J)} \arrow[r, "\text{onto}"] & B\otimes_A B & (B/IB)^{(J)} \arrow[r, "\simeq"] & (B/IB)\otimes_k (B/IB)
\end{tikzcd}$$

in which the lower arrows are obtained from the upper arrows by tensoring on the left with B and B/IB respectively, and M is the kernel. If $b \in B^{(J)}$ maps to zero in $B\otimes_A B$, then it maps to zero in $B/IB \otimes_k B/IB$, which implies that it maps to zero in $(B/IB)^{(J)}$. Therefore M is contained in $(IB)^{(J)} = I \cdot B^{(J)}$.

Recall (59) that

$$B\otimes_A B \simeq B\otimes_k B/IB$$

as left B-modules. As B/IB is free as a k-module (k is a field), $B\otimes_k B/IB$ is free as a left B-module, and so $B\otimes_A B$ is free (hence projective) as a left B-module. Therefore $B^{(J)}$ is a direct sum of B-submodules,

$$B^{(J)} = M \oplus N.$$

We know that

$$M \subset I\cdot B^{(J)} = IM \oplus IN,$$

and so $M \subset IM$. Hence $M \subset IM \subset I^2M = \cdots = 0$. We have shown that $B^{(J)} \to B\otimes_A B$ is injective, and this implies that $A^{(J)} \to B$ is injective because $A^{(J)} \subset B^{(J)}$.

Case that A and B are finitely generated

We begin with a remark. For any diagram of abstract groups

$$\begin{tikzcd}
 & H \arrow[d, "\beta"] & \\
M \arrow[r] & G \arrow[r] & G',
\end{tikzcd}$$

with M the kernel of $G \to G'$, the map

$$(m,h) \mapsto (m \cdot \beta(h), h) \colon M \times H \to G \times_{G'} H$$

is an isomorphism. This implies a similar statement for affine groups:

$$M \times H \simeq G \times_{G'} H. \tag{61}$$

After Theorem 9.3, we may suppose that k has characteristic $p \neq 0$. According to (10.2), there exists an n such that $\mathcal{O}(G)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(G)$. Let G' be the algebraic group such that $\mathcal{O}(G') = \mathcal{O}(G)^{p^n}$, and consider the diagrams

$$\begin{tikzcd}
N \arrow[r] \arrow[d] & H \arrow[r] \arrow[d] & G' \arrow[d, equal] \\
M \arrow[r] & G \arrow[r] & G'
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{O}(N) & \mathcal{O}(H) \arrow[l] & \mathcal{O}(G') \arrow[l, "\text{faithfully}", "\text{flat}"'] \\
\mathcal{O}(M) \arrow[u] & \mathcal{O}(G) \arrow[l] \arrow[u, "\text{injective}"'] & \mathcal{O}(G') \arrow[l] \arrow[u, equal]
\end{tikzcd}$$

where N and M are the kernels of the homomorphisms $H \to G'$ and $G \to G'$ respectively. Because $\mathcal{O}(G')$ is reduced, the homomorphism $\mathcal{O}(G') \to \mathcal{O}(H)$ is faithfully flat, and so $\mathcal{O}(G) \to \mathcal{O}(H)$ remains injective after it has been tensored with $\mathcal{O}(H)$:

$$\begin{tikzcd}
\mathcal{O}(G) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) \arrow[r, "\text{injective}"] \arrow[d, "(61)"', "\simeq"] & \mathcal{O}(H) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) \arrow[d, "(59)"', "\simeq"] \\
\mathcal{O}(M) \otimes \mathcal{O}(H) \arrow[r, dashed] & \mathcal{O}(N) \otimes \mathcal{O}(H).
\end{tikzcd}$$

Because $k \to \mathcal{O}(H)$ is faithfully flat (k is a field), the injectivity of the dotted arrow implies that $\mathcal{O}(M) \to \mathcal{O}(N)$ is injective, and hence it is faithfully flat (because the augmentation ideal of $\mathcal{O}(M)$ is nilpotent). Now the dotted arrow's being faithfully flat, implies that the top arrow is faithfully flat, which, because $\mathcal{O}(G') \to \mathcal{O}(H)$ is faithfully flat, implies that $\mathcal{O}(G) \to \mathcal{O}(H)$ is faithfully flat (CA 9.4).

General case

We show in (VIII, 8.3) below that A and B are directed unions of finitely generated Hopf subalgebras A_i and B_i such that $A_i \subset B_i$. As B_i is flat as an A_i-module for all i, B is flat as an A-module (CA 9.13). For the faithful flatness, we use the criterion (CA 9.10b):

$$A \to B \text{ is faithfully flat} \iff \text{for all maximal ideals } \mathfrak{m} \subset A,\ \mathfrak{m}B \neq B.$$

Let $\mathfrak{m}$ be a maximal ideal in A. If $1 \in \mathfrak{m}B$, then $1 = \sum m_j b_j$ for some $m_j \in \mathfrak{m}$ and $b_j \in B$. For some i, A_i will contain all the m_js and B_i will contain all the b_js, and so $1 \in (\mathfrak{m} \cap A_i)B_i$. But $\mathfrak{m} \cap A_i \neq A_i$ (it doesn't contain 1), and so this contradicts the faithful flatness of B_i over A_i. Hence $\mathfrak{m}B \neq B$, and B is faithfully flat over A.

COROLLARY 11.2 *Let $A \subset B$ be Hopf algebras with B an integral domain, and let $K \subset L$ be the fields of fractions of A and B. Then $B \cap K = A$; in particular, $A = B$ if $K = L$.*

PROOF. Because B is faithfully flat over A, $cB \cap A = cA$ for all $c \in A$. If a, c are elements of A such that $a/c \in B$, then $a \in cB \cap A = cA$, and so $a/c \in A$. □

ASIDE 11.3 Some statements have easy geometric proofs for smooth algebraic groups. In extending the proof to all algebraic groups, one often has to make a choice between a nonelementary (sometimes difficult) proof using algebraic geometry, and an elementary but uninformative proof using Hopf algebras. In general, we sketch the easy geometric proof for smooth algebraic groups, and give the elementary Hopf algebra proof in detail.

ASIDE 11.4 In most of the literature, for example, Borel 1991, Humphreys 1975, and Springer 1998, "algebraic group" means "smooth algebraic group" in our sense. Our approach is similar to that in Demazure and Gabriel 1970 and Waterhouse 1979.

The important Theorem 9.3 was announced in a footnote to Cartier 1962; the direct proof presented here follows Oort 1966.

Takeuchi 1972 proves Theorem 11.1 entirely in the context of Hopf algebras, for Hopf algebras that are either commutative or cocommutative, and he states that "it is an open problem whether the restriction of commutativity or cocommutativity can be removed". The proof of the theorem presented here follows Waterhouse 1979, Chapter 14.

ASIDE 11.5 In SGA 3, VI_A, 5.4.1, p.326, it is proved that a homomorphism $u\colon H \to G$ of algebraic groups over a field factors into $H \xrightarrow{p} H/N \xrightarrow{i} G$ with $p^\natural\colon \mathcal{O}(H/N) \to \mathcal{O}(H)$ faithfully flat and i a closed immersion. If $u^\natural\colon \mathcal{O}(G) \to \mathcal{O}(H)$ is injective, then i is an isomorphism, and so $u^\natural$ is faithfully flat (see SGA 3, VI_B, 11.14, p.426). Thus, in SGA 3, Theorem 11.1 is essentially part of the theorem on the existence of quotients by a normal subgroup.

CHAPTER **VII**

Group Theory: Subgroups and Quotient Groups.

In this chapter and in Chapter IX, we extend the basic theory of abstract groups to affine groups. Throughout, k is a ring.

1 A criterion to be an isomorphism

PROPOSITION 1.1 *A homomorphism of affine groups $u\colon H \to G$ is an isomorphism if and only if*

(a) *the map $u(R)\colon H(R) \to G(R)$ is injective for all k-algebras R, and*
(b) *the homomorphism $u^{\natural}\colon \mathcal{O}(G) \to \mathcal{O}(H)$ is faithfully flat.*

When k is a field, (b) can be replaced with:

(b$'$) *the homomorphism $u^{\natural}\colon \mathcal{O}(G) \to \mathcal{O}(H)$ is injective.*

PROOF. The conditions (a) and (b) are obviously necessary. For the sufficiency, note that the maps

$$H \times_G H \rightrightarrows H \xrightarrow{u} G$$

give rise to homomorphisms of Hopf algebras

$$\mathcal{O}(G) \xrightarrow{u^{\natural}} \mathcal{O}(H) \rightrightarrows \mathcal{O}(H) \otimes_{\mathcal{O}(G)} \otimes(H).$$

Condition (a) implies that the two projection maps $H \times_G H \rightrightarrows H$ are equal, and so the homomorphisms

$$\left.\begin{array}{l} x \mapsto x \otimes 1 \\ x \mapsto 1 \otimes x \end{array}\right\} : \mathcal{O}(H) \to \mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H) \tag{62}$$

are equal. But condition (b) implies that the subset of $\mathcal{O}(H)$ on which these homomorphisms is $u^{\natural}(\mathcal{O}(G))$ (see CA 9.6). Therefore $u^{\natural}$ is surjective, and so it is an isomorphism (faithfully flat homomorphisms are injective). When k is a field, condition (b$'$) implies (b) (see VI, 11.1). □

2 Injective homomorphisms

DEFINITION 2.1 Let $u\colon H \to G$ be a homomorphism of affine groups over k.

(a) We say that u is a ***monomorphism*** if $u(R)\colon H(R) \to G(R)$ is injective for all k-algebras R.
(b) We say that u ***injective*** if the map the map $u^{\natural}\colon\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective. An ***embedding*** is an injective homomorphism.

In other words, u is a monomorphism if the map $|u|\colon|H| \to |G|$ of affine k-schemes is a monomorphism, and it is injective (a closed immersion) if $|u|\colon|H| \to |G|$ is a closed immersion.

PROPOSITION 2.2 *If $u\colon H \to G$ is injective, then it is a monomorphism. The converse is true when k is a field.*

PROOF. If $u^{\natural}\colon\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective, then any two homomorphisms $\mathcal{O}(H) \to R$ that become equal when composed with $u^{\natural}$ must already be equal, and so $H(R) \to G(R)$ is injective.

Now suppose that k is a field and that $u(R)$ is injective for all R. The homomorphism $u^{\natural}$ factors into homomorphisms of Hopf algebras

$$\mathcal{O}(G) \twoheadrightarrow u^{\natural}(\mathcal{O}(G)) \hookrightarrow \mathcal{O}(H).$$

Let H' be the affine group whose Hopf algebra is $u^{*}(\mathcal{O}(G))$. Then u factors into

$$H \to H' \to G,$$

and the injectivity of $u(R)$ implies that $H(R) \to H'(R)$ is injective for all k-algebras R. Because $\mathcal{O}(H') \to \mathcal{O}(H)$ is injective, Proposition 1.1 shows that the map $H \to H'$ is an isomorphism, and so $u^{*}(\mathcal{O}(G)) = \mathcal{O}(H)$. □

PROPOSITION 2.3 *Let $u\colon H \to G$ be a homomorphism of affine groups. If u is injective, then $u_{k'}\colon H_{k'} \to G_{k'}$ is injective for every k-algebra k'. Conversely, if $u_{k'}$ is injective for some faithfully flat k-algebra k', then u is injective.*

PROOF. Let k' be a k-algebra. If $A \to B$ is faithfully flat, then $k' \otimes A \to k' \otimes B$ is faithfully flat, and the converse is true if $k \to k'$ is faithfully flat. □

ASIDE 2.4 What we call a monomorphism (resp. an injection) is called a monomorphism (resp. a closed immersion) in SGA 3. For homomorphisms of group schemes (affine or not), it is a subtle problem to determine under what conditions monomorphisms are necessarily closed immersions (see SGA 3 VIII, 7, for a discussion of the problem). Certainly, there are examples of monomorphisms that are not closed immersions.

3 Affine subgroups

DEFINITION 3.1 An ***affine subgroup*** (resp. ***normal affine subgroup)*** of an affine group G is a closed subfunctor H of G such that $H(R)$ is a subgroup (resp. normal subgroup) of $G(R)$ for all R.

In other words, a subfunctor H of an affine group G is an affine subgroup of G if

- ◇ $H(R)$ is a subgroup of $G(R)$ for all k-algebras R, and
- ◇ H is representable by a quotient of $\mathcal{O}(G)$ (cf. V, 6.2).

An affine subgroup H of an affine algebraic group G is an algebraic group, because $\mathcal{O}(H)$ is a quotient of the finitely presented k-algebra $\mathcal{O}(G)$.

PROPOSITION 3.2 *The affine subgroups of an affine group G are in natural one-to-one correspondence with the Hopf ideals on $\mathcal{O}(G)$.*

PROOF. For an affine subgroup H of G,

$$I(H) = \{f \in \mathcal{O}(G) \mid f_R(h) = 1 \text{ for all } h \in H(R) \text{ and all } R\}$$

is a Hopf ideal in G (it is the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$; see Exercise II-6). Conversely, if $\mathfrak{a}$ is a Hopf ideal in G, then the functor

$$R \rightsquigarrow \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \mathfrak{a}\}$$

is an affine subgroup $G(\mathfrak{a})$ of $\mathcal{O}(G)$ (it is represented by $\mathcal{O}(G)/\mathfrak{a}$). The maps $H \mapsto I(H)$ and $\mathfrak{a} \mapsto G(\mathfrak{a})$ are inverse. □

COROLLARY 3.3 *When k is noetherian, the affine subgroups of an algebraic affine group satisfy the descending chain condition (every descending chain of affine subgroups eventually becomes constant).*

PROOF. The ring $\mathcal{O}(G)$ is noetherian (Hilbert basis theorem, CA 3.6), and so the ideals in $\mathcal{O}(G)$ satisfy the ascending chain condition. □

PROPOSITION 3.4 *For any affine subgroup H of an affine algebraic group G, the algebraic scheme $|H|$ is closed in $|G|$.*

PROOF. If $\mathfrak{a}$ is the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$, then $|H|$ is the subspace $V(\mathfrak{a}) \overset{\text{def}}{=} \{\mathfrak{m} \mid \mathfrak{m} \supset \mathfrak{a}\}$ of $|G|$. □

PROPOSITION 3.5 *For any family $(H_j)_{j \in J}$ of affine subgroups of an affine group G, the functor*

$$R \rightsquigarrow \bigcap\nolimits_{j \in J} H_j(R) \quad \text{(intersection inside } G(R)\text{)}$$

is an affine subgroup $\bigcap_{j \in J} H_j$ of G, with coordinate ring $\mathcal{O}(G)/I$ where I is the ideal generated by the ideals $I(H_j)$.

PROOF. We have

$$H_j(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in I(H_j)\}.$$

Therefore,

$$\begin{aligned} H(R) &= \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \bigcup I(H_j)\} \\ &= \mathrm{Hom}(\mathcal{O}(G)/I, R). \end{aligned}$$

□

EXAMPLE 3.6 The intersection of the affine subgroups SL_n and $\mathbb{G}_m$ (scalar matrices) of GL_n is μ_n (matrices $\mathrm{diag}(c,\ldots,c)$ with $c^n = 1$).

DEFINITION 3.7 An affine subgroup H of algebraic group G is said to be ***characteristic*** if, for all k-algebras R and all automorphisms u of G_R, $u(H_R) = H_R$ (cf. DG II, §1, 3.9). When k is a field and the condition holds only when R is a field, we say that H is ***characteristic in the weak sense***.

Both conditions are stronger than requiring that $u(H) = H$ for all automorphisms of G (see XVI, 2.7).

3.8 In the realm of not necessarily affine group schemes over a field, there can exist nonaffine (necessarily nonclosed) subgroup schemes of an affine algebraic group. For example, the constant subgroup scheme $(\mathbb{Z})_k$ of $\mathbb{G}_a$ over $\mathbb{Q}$ is neither closed nor affine. Worse, the (truly) constant subfunctor $R \rightsquigarrow \mathbb{Z} \subset R$ of $\mathbb{G}_a$ is not representable. Over an algebraically closed field k consider the discrete (nonaffine) group scheme with underlying set k; the obvious map $k \to \mathbb{G}_a$ of nonaffine group schemes is a homomorphism, and it is both mono and epi, but it is not an isomorphism.

4 Kernels of homomorphisms

The ***kernel*** of a homomorphism $u: H \to G$ of affine groups is the functor

$$R \rightsquigarrow N(R) \overset{\text{def}}{=} \mathrm{Ker}(u(R): H(R) \to G(R)).$$

Let $\epsilon: \mathcal{O}(G) \to k$ be the identity element of $G(k)$. Then an element $h: \mathcal{O}(H) \to R$ of $H(R)$ lies in $N(R)$ if and only if its composite with $u^\natural: \mathcal{O}(G) \to \mathcal{O}(H)$ factors through ϵ:

$$\begin{tikzcd} \mathcal{O}(H) \arrow[d, "h"] & \mathcal{O}(G) \arrow[l, "u^\natural"'] \arrow[d, "\epsilon"] \\ R & k. \arrow[l, dashed] \end{tikzcd}$$

Let I_G be the kernel of $\epsilon: \mathcal{O}(G) \to k$ (this is called the ***augmentation ideal***), and let $I_G \cdot \mathcal{O}(H)$ denote the ideal generated by its image in $\mathcal{O}(H)$. Then the elements of $N(R)$ correspond to the homomorphisms $\mathcal{O}(H) \to R$ that are zero on $I_G \cdot \mathcal{O}(H)$, i.e.,

$$N(R) = \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(H)/I_G\mathcal{O}(H), R).$$

We have proved:

PROPOSITION 4.1 *For any homomorphism $H \to G$ of affine groups, there is an affine subgroup N of H (called the **kernel** of the homomorphism) such that*

$$N(R) = \mathrm{Ker}(H(R) \to G(R))$$

for all R; its coordinate ring is $\mathcal{O}(H)/I_G\mathcal{O}(H)$.

Alternatively, note that the kernel of u is the fibred product of $H \to G \leftarrow *$, and so it is an algebraic group with coordinate ring

$$\mathcal{O}(H) \otimes_{\mathcal{O}(G)} (\mathcal{O}(G)/I_G) \simeq \mathcal{O}(H)/I_G\mathcal{O}(H)$$

(see V, §2).

EXAMPLE 4.2 Consider the map $g \mapsto g^n : \mathbb{G}_m \to \mathbb{G}_m$. This corresponds to the map on Hopf algebras $Y \mapsto X^n : k[Y, Y^{-1}] \to k[X, X^{-1}]$ because

$$X^n(g) = g^n = Y(g^n)$$

(cf. (13), p.25). The map $\epsilon : k[Y, Y^{-1}] \to k$ sends $f(Y)$ to $f(1)$, and so the augmentation ideal for $\mathbb{G}_m$ is $(Y - 1)$. Thus, the kernel has coordinate ring

$$k[X, X^{-1}]/(X^n - 1) \simeq k[X]/(X^n - 1).$$

In other words, the kernel is the algebraic group μ_n, as we would expect.

EXAMPLE 4.3 Let N be the kernel of the determinant map $\det : \mathrm{GL}_n \to \mathbb{G}_m$. This corresponds to the map on Hopf algebras

$$X \mapsto \det(X_{ij}) : k[X, X^{-1}] \to k[\ldots, X_{ij}, \ldots, \det(X_{ij})^{-1}]$$

because

$$\det(X_{ij})(a_{ij}) = \det(a_{ij}) = X(\det(a_{ij})).$$

As we just noted, the augmentation ideal for $\mathbb{G}_m$ is $(X - 1)$, and so

$$\mathcal{O}(N) = \frac{k[\ldots, X_{ij}, \ldots, \det(X_{ij})^{-1}]}{(\det(X_{ij}) - 1)} \simeq \frac{k[\ldots, X_{ij}, \ldots]}{(\det(X_{ij}) - 1)}.$$

In other words, the kernel of det is the algebraic group SL_n, as we would expect.

PROPOSITION 4.4 *If a homomorphism of affine groups is injective, then its kernel if trivial. The converse is true when k is a field.*

PROOF. The kernel of $u : H \to G$ is trivial if and only if $u(R)$ is injective for all R. Therefore the proposition is a restatement of Proposition 2.2. □

COROLLARY 4.5 *When k is a field of characteristic zero, a homomorphism of affine groups $G \to H$ is injective if and only if $G(k^{\mathrm{al}}) \to H(k^{\mathrm{al}})$ is injective.*

PROOF. When k is a field of characteristic zero, an affine group N is trivial if $N(k^{\mathrm{al}}) = 1$ (VI, 9.4). □

NOTES Need to discuss whether trivial kernel implies injective over rings k. Consider $H \to G$ injective as a map of functors, corresponding to $A \to B$. Can assume $A \to B$ injective, and want to prove that $H(R) = G(R)$. Have $H(R) \subset G(R)$. Given $P \in G(R)$, want $P \in H(R)$. Certainly $P \in H(R \otimes B)$, which implies that $P \in H(R)$ if $R \to R \otimes_A B$ is injective. But why should it? Really seem to need that $A \to B$ is flat. Give examples. Actually, should look at this from the point of view of schemes: a morphism $X \to Y$ with trivial fibres.

☠ 4.6 Proposition 4.5 is false for fields k of characteristic $p \neq 0$. For example, the homomorphism $x \mapsto x^p\colon \mathbb{G}_a \to \mathbb{G}_a$ has kernel α_p, and so it is not injective, but the map $x \mapsto x^p\colon \mathbb{G}_a(R) \to \mathbb{G}_a(R)$ is injective for every reduced k-algebra R.

REMARK 4.7 Let A be an object of some category A. A morphism $u\colon S \to A$ is a ***monomorphism*** if $f \mapsto u \circ f\colon \mathrm{Hom}(T,S) \to \mathrm{Hom}(T,A)$ is injective for all objects T. Two monomorphisms $u\colon S \to A$ and $u'\colon S' \to A$ are said to be ***equivalent*** if each factors through the other. This is an equivalence relation on the monomorphisms with target A, and an equivalence class of monomorphisms is called a ***subobject*** of A.

Let k be a field. A homomorphism of affine groups over k is a injective if and only if it is a monomorphism in the category of affine groups over k. To see this, let $u\colon H \to G$ be a homomorphism of affine groups. If u is injective and the homomorphisms $\beta,\gamma\colon H' \to H$ agree when composed with u, then (1.1a) with $R = \mathcal{O}(H')$ shows that $\beta = \gamma$. Suppose, on the other hand, that u is not injective, so that its kernel N is nontrivial. Then the homomorphisms $n \mapsto 1$, $n \mapsto n\colon N \to N$ are distinct, but they agree when composed with u, and so u is not a monomorphism.

Let G be an affine group. Two monomorphisms $u\colon H \to G$ and $u\colon H' \to G$ are equivalent if and only if $\mathrm{Im}(u_R) = \mathrm{Im}(u'_R)$ for all k-algebras R. It follows that, in each equivalence class of monomorphisms with target G, there is exactly one with H an affine subgroup of G and with u the inclusion map.

ASIDE 4.8 In any category, the equalizer of a pair of morphisms is a monomorphism. A monomorphism that arises in this way is said to be ***regular***. In Grp, every monomorphism is regular (see, for example, van Oosten, Basic Category Theory, Exercise 42, p.21). For example, the centralizer of an element a of a group A (which is not a normal subgroup in general) is the equalizer of the homomorphisms $x \mapsto x$, $x \mapsto axa^{-1}\colon A \to A$. Is it true that every monomorphism in the category of affine (or algebraic) groups is regular?

5 Dense subgroups

Throughout this subsection, k is a field.

Let G be an algebraic group over k. By definition, a point $a \in G(k)$ is a homomorphism $\mathcal{O}(G) \to k$, whose kernel we denote $\mathfrak{m}_a$ (a maximal ideal in $\mathcal{O}(G)$). As we discussed VI, §3, the map $a \mapsto \mathfrak{m}_a\colon G(k) \to |G|$ is injective with image the set of maximal ideals $\mathfrak{m}$ of $\mathcal{O}(G)$ such that $\mathcal{O}(G)/\mathfrak{m} = k$. We endow $G(k)$ with the subspace topology.

PROPOSITION 5.1 *Let G be an algebraic group over a field k, and let Γ be a subgroup of $G(k)$. There exists an affine subgroup H of G such that $H(k) = \Gamma$ if and only if Γ is closed, in which case there exists a unique smallest H with this property. When k is algebraically closed, every smooth affine subgroup of G arises in this way.*

PROOF. If $\Gamma = H(k)$ for an affine subgroup H of G, then $\Gamma = |H| \cap G(k)$, which is closed by (3.4). Conversely, let Γ be a closed subgroup of $G(k)$. Each $f \in \mathcal{O}(G)$ defines a function $\Gamma \to k$, and, for $x, y \in \Gamma$, $(\Delta f)(x,y) = f(x \cdot y)$ (see (12), p. 25). Therefore, when we let $R(\Gamma)$ denote the k-algebra of maps $\Gamma \to k$ and define $\Delta_\Gamma \colon R(\Gamma) \times R(\Gamma) \to R(\Gamma \times \Gamma)$ as in Exercise II-1, we obtain a commutative diagram

$$\begin{tikzcd}
\mathcal{O}(G) \arrow[r, "\Delta_G"] \arrow[d] & \mathcal{O}(G) \otimes \mathcal{O}(G) \arrow[d] \\
R(\Gamma) \arrow[r, "\Delta_\Gamma"] & R(\Gamma \times \Gamma),
\end{tikzcd}$$

which shows that Δ_Γ maps into $R(\Gamma) \otimes R(\Gamma)$, and so $(R(\Gamma), \Delta_\Gamma)$ is a Hopf algebra (ibid.). Because Γ is closed, it is the zero set of the ideal

$$\mathfrak{a} \overset{\text{def}}{=} \operatorname{Ker}(\mathcal{O}(G) \to R(\Gamma)),$$

which is a Hopf ideal because $(\mathcal{O}(G), \Delta_G) \to (R(\Gamma), \Delta_\Gamma)$ is a homomorphism of Hopf algebras (II, 5.2). The affine subgroup H of G with $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a} \subset R(\Gamma)$ has $H(k) = \Gamma$. Clearly, it is the smallest subgroup of G with this property. When k is algebraically closed and H is a smooth subgroup of G, then the group attached to $\Gamma = H(k)$ is H itself. □

REMARK 5.2 For any subgroup Γ of $G(k)$, the closure $\bar{\Gamma}$ of Γ in $G(k) \subset |G|$ is a closed subgroup of $G(k)$.[1] The smallest affine subgroup H of G such that $H(k) = \bar{\Gamma}$ is often called the "Zariski closure" of Γ in G.

REMARK 5.3 When k is not algebraically closed, not every smooth algebraic subgroup of G arises from a closed subgroup of $G(k)$. Consider, for example, the algebraic subgroup $\mu_n \subset \mathbb{G}_m$ over $\mathbb{Q}$. If n is odd, then $\mu_n(\mathbb{Q}) = \{1\}$, and the algebraic group attached to $\{1\}$ is the trivial group.

REMARK 5.4 It is obvious from its definition that $R(\Gamma)$ has no nonzero nilpotents. Therefore the affine subgroup attached to a closed subgroup Γ of $G(k)$ is reduced, and hence smooth if k is perfect. In particular, no nonsmooth subgroup arises in this way.

DEFINITION 5.5 Let G be an algebraic group over a field k, and let k' be a field containing k. We say that a subgroup Γ of $G(k')$ is ***dense*** in G if the only affine subgroup H of G such that $H(k') \supset \Gamma$ is G itself.

5.6 The map $\Gamma \mapsto H$ in (5.1) sets up a one-to-one correspondence between the subgroups Γ of $G(k)$ such that $\Gamma = \bar{\Gamma}$ and the affine subgroups H of G such that $H(k)$ is dense in H. If $H(k)$ is dense in H, then H is reduced, hence smooth when k is perfect (see 5.4). When k is algebraically closed, the affine subgroups H of G such that $H(k)$ is dense in H are exactly the smooth affine subgroups.

[1] It is a general fact that the closure of a subgroup Γ of a topological group is a subgroup. To see this, note that for a fixed $c \in \Gamma$, the maps $x \to cx$ and $x \mapsto x^{-1}$ are continuous, and hence are homeomorphisms because they have inverses of the same form. For $c \in \Gamma$, we have $\Gamma c = \Gamma$, and so $\bar{\Gamma} c = \bar{\Gamma}$. As c is arbitrary, this says that $\bar{\Gamma} \cdot \Gamma = \bar{\Gamma}$. For $d \in \bar{\Gamma}$, $d\Gamma \subset \bar{\Gamma}$, and so $d\bar{\Gamma} \subset \bar{\Gamma}$. We have shown that $\bar{\Gamma} \cdot \bar{\Gamma} \subset \bar{\Gamma}$. Because $x \mapsto x^{-1}$ is a homeomorphism, it maps $\bar{\Gamma}$ onto $(\Gamma^{-1})^{-}$. Therefore $\bar{\Gamma}^{-1} = (\Gamma^{-1})^{-} = \bar{\Gamma}$.

5.7 If $\Gamma \subset G(k')$ is dense in G, then, for any field $k'' \supset k'$, $\Gamma \subset G(k'')$ is dense in G.

5.8 It follows from the proof of (5.1) that $G(k)$ is dense in G if and only if

$$f \in \mathcal{O}(G),\ f(P) = 0 \text{ for all } P \in G(k) \implies f = 0. \tag{63}$$

In other words, $G(k)$ is dense in G if and only if no nonzero element of $\mathcal{O}(G)$ maps to zero under all homomorphisms of k-algebras $\mathcal{O}(G) \to k$:

$$\bigcap_{u:\mathcal{O}(G)\to k} \operatorname{Ker}(u) = 0.$$

5.9 For an affine algebraic variety V over a field k, any $f \in \mathcal{O}(V)$ such that $f(P) = 0$ for all $V(k^{\text{al}})$ is zero (Nullstellensatz; CA 11.5); better, any $f \in \mathcal{O}(V)$ such that $f(P) = 0$ for all $P \in V(k^{\text{sep}})$ is zero (AG 11.15). Therefore, if G is smooth, then $G(k^{\text{sep}})$ (a fortiori, $G(k^{\text{al}})$) is dense in G.

5.10 If $G(k)$ is finite, for example, if the field k is finite, and $\dim G > 0$, then $G(k)$ is never dense in G.

PROPOSITION 5.11 *If k is infinite, then $G(k)$ is dense in G when $G = \mathbb{G}_a$, GL_n, or SL_n.*

PROOF. We use the criterion (5.8). Because k is infinite, no nonzero polynomial in $k[X_1,\ldots,X_n]$ can vanish on all of k^n (FT, proof of 5.18). This implies that no nonzero polynomial f can vanish on a set of the form

$$D(h) \overset{\text{def}}{=} \{a \in k^n \mid h(a) \neq 0\}, \quad h \neq 0,$$

because otherwise hf would vanish on k^n. As

$$\mathrm{GL}_n(k) = \{a \in k^{n^2} \mid \det(a) \neq 0\},$$

this proves the proposition for GL_n.

The proposition is obvious for $\mathbb{G}_a$, and it can be proved for SL_n by realizing $\mathcal{O}(\mathrm{SL}_n)$ as a subalgebra of $\mathcal{O}(\mathrm{GL}_n)$. Specifically, the natural bijection

$$A, r \mapsto A \cdot \operatorname{diag}(r, 1, \ldots, 1) \colon \mathrm{SL}_n(R) \times \mathbb{G}_m(R) \to \mathrm{GL}_n(R)$$

(of set-valued functors) defines an isomorphism of k-algebras

$$\mathcal{O}(\mathrm{GL}_n) \simeq \mathcal{O}(\mathrm{SL}_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

and the algebra on the right contains $\mathcal{O}(\mathrm{SL}_n)$. Hence

$$\bigcap_{u:\mathcal{O}(\mathrm{SL}_n)\to k} \operatorname{Ker}(u) \subset \bigcap_{u:\mathcal{O}(\mathrm{GL}_n)\to k} \operatorname{Ker}(u) = 0.$$

□

PROPOSITION 5.12 *Let G be an algebraic group over a perfect field k, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. Then Γ acts on $G(k^{\mathrm{al}})$, and $H \leftrightarrow H(k^{\mathrm{al}})$ is a one-to-one correspondence between the smooth affine subgroups of G and the closed subgroups of $G(k^{\mathrm{al}})$ stable under Γ.*

PROOF. Combine (5.1) with (V, 7.3). (More directly, both correspond to radical Hopf ideals $\mathfrak{a}$ in the k^{al}-bialgebra $k^{\mathrm{al}} \otimes \mathcal{O}(G)$ stable under the action of Γ; see AG 16.7, 16.8).□

ASIDE 5.13 Let k be an infinite field. We say that a finitely generated k-algebra has "enough maps to k" if $\bigcap_{u:A\to k} \mathrm{Ker}(u) = 0$ (intersection over k-algebra homomorphisms $A \to k$). We saw in the proof of (5.11) that $k[X_1,\ldots,X_n]_h$ has enough maps to k for any $h \neq 0$. Obviously, any subalgebra of an algebra having enough maps to k also has enough maps to k. In particular, any subalgebra of $k[X_1,\ldots,X_n]_h$ has enough maps to k. A connected affine variety V is said to ***unirational*** if $\mathcal{O}(V)$ can be realized as a subalgebra $k[X_1,\ldots,X_n]_h$ in such a way that the extension of the fields of fractions is finite. Geometrically, this means that there is a finite map from an open subvariety of $\mathbb{A}^n$ onto an open subvariety of V. Clearly, if V is unirational, then $\mathcal{O}(V)$ has enough maps to k. Therefore, if a connected algebraic group G is unirational, then $G(k)$ is dense in G. So which algebraic groups are unirational? In SGA 3, XIV 6.11 we find:

> One knows (Rosenlicht) examples of forms of $\mathbb{G}_a$ over a nonperfect field, which have only finitely many rational points, and therefore a fortiori are not unirational. Moreover Chevalley has given an example of a torus over a field of characteristic zero which is not a rational variety. On the other hand, it follows from the Chevalley's theory of semisimple groups that over an algebraically closed field, every smooth connected affine algebraic group is a rational variety.

Borel 1991, 18.2, proves that a smooth connected algebraic group G is unirational if k is perfect or if G is reductive. For a nonunirational nonconnected algebraic group, Rosenlicht gives the example of the group of matrices $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ over $\mathbb{R}$ with $a^2+b^2 = \pm 1$. For a nonunirational connected algebraic group, Rosenlicht gives the example of the subgroup of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $Y^p - Y = tX^p$ over the field $k = k_0(t)$ (t transcendental). On the other hand, if $k[\sqrt{a},\sqrt{b}]$ has degree 4 over k, then the norm torus[2] associated with this extension is a three-dimensional torus that is not a rational variety. Proofs of these statements will be given in a future version of the notes.

ASIDE 5.14 When k is finite, only the finite affine subgroups of G arise as the Zariski closure of a subgroup of $G(k)$ (see 5.10). Nori (1987) has found a more useful way of defining the "closure" of a subgroup Γ of $\mathrm{GL}_n(\mathbb{F}_p)$. Let $X = \{x \in \Gamma \mid x^p = 1\}$, and let Γ^+ be the subgroup of Γ generated by X (it is normal). For each $x \in X$, we get a one-parameter affine subgroup

$$t \mapsto x^t = \exp(t \log x)\colon \mathbb{A}^1 \to \mathrm{GL}_n,$$

where

$$\exp(z) = \sum\nolimits_{i=0}^{p-1} \frac{z^i}{i!} \text{ and } \log(z) = -\sum\nolimits_{i=1}^{p-1} \frac{(1-z)^i}{i}.$$

Let G be the smallest algebraic subgroup of GL_n containing these subgroups for $x \in X$. Nori shows that if p is greater than some constant depending only on n, then $\Gamma^+ = G(\mathbb{F}_p)^+$. If G is semisimple and simply connected, then $G(\mathbb{F}_p)^+ = G(\mathbb{F}_p)$, and so Γ^+ is realized as the group of rational points of the connected algebraic group G. The map $\Gamma \mapsto G$ sets up a one-to-one correspondence between the subgroups Γ of $\mathrm{GL}_n(\mathbb{F}_p)$ such that $\Gamma = \Gamma^+$ and the affine subgroups of $\mathrm{GL}_{n\mathbb{F}_p}$ generated by one-parameter subgroups $t \mapsto \exp(ty)$ defined by elements $y \in M_n(\mathbb{F}_p)$ with $y^p = 0$.

[2] Let $T = (\mathbb{G}_m)_{k[\sqrt{a},\sqrt{b}]/k}$. The norm map defines a homomorphism $T \to \mathbb{G}_m$, and the norm torus is the kernel of this homomorphism.

ASIDE 5.15 (mo56192) Rosenlicht's subgroup $Y^p - Y = tX^p$ of $\mathbb{G}_a \times \mathbb{G}_a$ ($p \neq 2$) and the subgroup $Y^p = tX^p$ of $\mathbb{G}_a \times \mathbb{G}_a$ are examples of algebraic groups G over k such that $G(k)$ is not dense in G (the first is smooth; the second is reduced but not smooth).

A smooth, connected unipotent group is said to be k-split if there is a filtration by k-subgroups for which the successive quotients are isomorphic to $\mathbb{G}_a$. The examples in the above paragraph are non-split unipotent groups. Any smooth connected k-split unipotent group U is even a rational variety (in fact, k-isomorphic as a variety to $\mathbb{A}^n$), and so it is clear that $U(k)$ is Zariski dense in U when is infinite. More generally, let G be a smooth connected affine algebraic group over k and assume that the unipotent radical of $G_{k^{\mathrm{al}}}$ is defined and split over k (both of these conditions can fail). Then as a k-variety, G is just the product of its reductive quotient (G/R_uG) and its unipotent radical (result of Rosenlicht). In particular, is G is unirational, and if k is infinite, then $G(k)$ is dense in G (George McNinch)

A necessary condition when k is imperfect: if $G(k)$ is dense in G, then G_{red} is a smooth algebraic group over k. Proof: the regular locus of G_{red} is open and non-empty, so contains a rational point. This point is then smooth. By translation, G_{red} is smooth at origin, hence smooth everywhere. This implies that it is an algebraic group because it is geometrically reduced (Qing Liu).

ASIDE 5.16 Let k be a commutative ring. Waterhouse 1979, 1.2, p. 5 defines an *affine group scheme* to be a representable functor from k-algebras to groups. He defines an affine group scheme to be *algebraic* if its representing algebra is finitely generated (ibid. 3.3, p. 24) . Now assume that k is a field. He defines an *algebraic matrix group* over k to be a Zariski-closed subgroup of $\mathrm{SL}_n(k)$ for some n (ibid., 4.2, p. 29), and he defines an *affine algebraic group* to be a closed subset of k^n some n with a group law on it for which the multiplication and inverse are polynomial maps (ibid. 4.2, p. 29). Algebraic matrix groups and affine algebraic groups define (essentially the same) affine group schemes.

Waterhouse 1979	This work
affine group scheme	affine group
affine algebraic group scheme	affine algebraic group (or just algebraic group)
algebraic matrix group	affine subgroup G of $\mathrm{GL}_{n,k}$ such that $G(k)$ is dense in G
affine algebraic group	algebraic group G such that $G(k)$ is dense in G.

We shall sometimes use ***algebraic matrix group*** to mean an affine subgroup G of $\mathrm{GL}_{n,k}$ such that $G(k)$ is dense in G.

ASIDE 5.17 Before Borel introduced algebraic geometry into the theory of algebraic groups in a more systematic way, Chevalley defined algebraic groups to be closed subsets of k^n endowed with a group structure defined by polynomial maps. In other words, he studied affine algebraic groups and algebraic matrix groups in the above sense. Hence, effectively he studied reduced algebraic groups G with the property that $G(k)$ is dense in G.

Hochschild adopts a similar approach (Hochschild 1971a, 1981). In our language, he defines an affine algebraic group over a field k to be a pair (G, A) where A is a finitely generated Hopf algebra over k and G is a dense subgroup of the affine group defined by A (ibid. p.21, p.10).

ASIDE 5.18 In the literature one finds statements:

> When k is perfect, any algebraic subgroup of GL_n defined by polynomials with coefficients in k is automatically defined over k (e.g., Borel 1991, Humphreys 1975).

What is meant is the following:

> When k is perfect, any smooth algebraic subgroup G of $\mathrm{GL}_{n,k^{\mathrm{al}}}$ such the subset $G(k^{\mathrm{al}})$ of $\mathrm{GL}_n(k^{\mathrm{al}})$ is defined by polynomials with coefficients in k arises from a smooth algebraic subgroup of $\mathrm{GL}_{n,k}$.

From our perspective, the condition on $G(k^{\mathrm{al}})$ (always) implies that G arises from a reduced algebraic subgroup of $\mathrm{GL}_{n,k}$, which is smooth if k is perfect.

6 Normalizers; centralizers; centres

For a subgroup H of an abstract group G, we let $N_G(H)$ (resp. $C_G(H)$) denote the normalizer (resp. centralizer) of H in G, and we let ZG denote the centre of G.

In this section, we extend these notions to an affine subgroup H of an affine group G. We say that an affine group G is ***locally free*** if $\mathcal{O}(G)$ is a locally free k-algebra (see p. 67). When k is a field, all affine groups are (locally) free.

For $g \in G(R)$, let ${}^{g}H$ be the functor of R-algebras

$$R' \rightsquigarrow g \cdot H(R') \cdot g^{-1} \quad \text{(subset of } G(R')\text{)}.$$

Define N to be the functor of k-algebras

$$R \rightsquigarrow \{g \in G(R) \mid {}^{g}H = H\}.$$

Thus, for any k-algebra R,

$$\begin{aligned} N(R) &= \{g \in G(R) \mid g \cdot H(R') \cdot g^{-1} = H(R') \text{ for all } R\text{-algebras } R'\} \\ &= G(R) \cap \textstyle\bigcap_{R'} N_{G(R')}(H(R')). \end{aligned}$$

PROPOSITION 6.1 *If H is locally free, then the functor N is an affine subgroup of G.*

PROOF. Clearly $N(R)$ is a subgroup of $G(R)$, and so it remains to show that N is representable by a quotient of $\mathcal{O}(G)$. Clearly

$$g \cdot H(R') \cdot g^{-1} = H(R') \iff g \cdot H(R') \cdot g^{-1} \subset H(R') \text{ and } g^{-1} \cdot H(R') \cdot g \subset H(R'),$$

and so, when we let G act on itself by conjugation,

$$N = T_G(H,H) \cap T_G(H,H)^{-1}$$

(notations as in V, §6). Theorem 6.9, of Chapter V, shows that $T_G(H,H)$ is representable, and it follows from (3.5) that N is representable by a quotient of $\mathcal{O}(G)$. □

ASIDE 6.2 In fact $N_G(H) = T_G(H,H)$ if H is finitely presented, because then every injective map $H_R \to H_R$ is bijective (Ax, James, Injective endomorphisms of varieties and schemes. Pacific J. Math. 31 1969 1–7).

The affine subgroup N of G is called the ***normalizer*** $N_G(H)$ of H in G. Clearly a subgroup H of G is normal if and only if $N_G(H) = G$.

It is obvious from its definition that the formation of $N_G(H)$ commutes with extension of scalars: for every k-algebra k',

$$N_G(H)_{k'} \simeq N_{G_{k'}}(H_{k'}).$$

PROPOSITION 6.3 *Assume that k is a field. If H is an affine subgroup of an algebraic group G, and $H(k')$ is dense in H for some field k' containing k, then*

$$N_G(H)(k) = G(k) \cap N_{G(k')}(H(k')).$$

PROOF. Let $g \in G(k) \cap N_{G(k')}(H(k'))$. Because $g \in G(k)$, ${}^{g}H$ is an algebraic subgroup of G, and so ${}^{g}H \cap H$ is an algebraic subgroup of H. Because $g \in N_{G(k')}(H(k'))$,

$$\left({}^{g}H\right)(k') = H(k'),$$

and so $({}^{g}H \cap H)(k') = H(k')$. As $H(k')$ is dense in H, this implies that ${}^{g}H \cap H = H$, and so ${}^{g}H = H$. □

COROLLARY 6.4 *Assume that k is a field. Let H be a smooth affine subgroup of a smooth algebraic group G. If $H(k^{\mathrm{sep}})$ is normal in $G(k^{\mathrm{sep}})$, then H is normal in G.*

PROOF. Because H is smooth, $H(k^{\mathrm{sep}})$ is dense in H, and so (6.3) shows that $N_G(H)(k^{\mathrm{sep}}) = G(k^{\mathrm{sep}})$, and so $N_G(H) = G$. □

☠ 6.5 The corollary is false without the smoothness assumptions, even with k^{al} for k^{sep}. For example, let H be the subgroup of SL_2 in characteristic $p \neq 0$ such that

$$H(R) = \left\{ \left(\begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) \middle| pa = 0 \right\}$$

(so $H \simeq \alpha_p$). Then $H(k^{\mathrm{al}}) = 1$, but H is not normal in SL_2.

PROPOSITION 6.6 *Assume that k is a field. Let H be an affine subgroup of an algebraic group G. Let i_g denote the inner automorphism of G defined by $g \in G(k)$; if $G(k)$ is dense in G and $i_g(H) = H$ for all $g \in G(k)$, then H is normal in G.*

PROOF. Let $N = N_G(H) \subset G$. If $i_g(H) = H$, then $g \in N(k)$. The hypotheses imply that $G(k) \subset N(k)$, and so $N = G$. □

Let H be an affine subgroup of an affine group G, and let N be the normalizer of H. Each $n \in N(R)$ defines a natural transformation i_n

$$h \mapsto nhn^{-1} \colon H(R') \to H(R')$$

of H regarded as a functor from the category of R-algebras to sets, and we define C to be the functor of k-algebras

$$R \rightsquigarrow \{n \in N(R) \mid i_n = \mathrm{id}_H\}.$$

Thus,

$$C(R) = G(R) \cap \bigcap\nolimits_{R'} C_{G(R')}(H(R')).$$

PROPOSITION 6.7 *If H is locally free, then the functor C is an affine subgroup of G.*

PROOF. We have to show that C is representable. Let G act on $G \times G$ by

$$g(g_1, g_2) = (g_1, g g_2 g^{-1}), \quad g, g_1, g_2 \in G(R),$$

and embed H diagonally in $G \times G$,

$$H \to G \times G, \quad h \mapsto (h, h) \text{ for } h \in H(R).$$

Then

$$C = T_{G \times G}(H, H),$$

which is a closed subfunctor of G (V, 6.1). □

The affine subgroup C of G is called the ***centralizer*** $C_G(H)$ of H in G. It is obvious from its definition that the formation of $C_G(H)$ commutes with extension of the base field: for every k-algebra k',

$$C_G(H)_{k'} \simeq C_{G_{k'}}(H_{k'}).$$

PROPOSITION 6.8 *Assume that k is a field. If H is an affine subgroup of an algebraic group G, and $H(k')$ is dense in H for some field $k' \supset k$, then*

$$C_G(H)(k) = G(k) \cap C_{G(k')}(H(k')).$$

PROOF. Let $n \in G(k) \cap C_{G(k')}(H(k'))$. According to (6.3), $n \in N_G(H)(k)$. The maps i_n and id_H coincide on an affine subgroup of H, which contains $H(k')$, and so equals H. Therefore $n \in C_G(H)(k)$. □

COROLLARY 6.9 *Assume that k is a field. Let H be a smooth affine subgroup of a smooth algebraic group G. If $H(k^{\mathrm{sep}})$ is central in $G(k^{\mathrm{sep}})$, then H is central in G.*

PROOF. Because H is smooth, $H(k^{\mathrm{sep}})$ is dense in H, and so (6.8) shows that $C_G(H)(k^{\mathrm{sep}}) = G(k^{\mathrm{sep}})$, and so $C_G(H) = G$. □

The ***centre*** ZG of an affine group G is defined to be $C_G(G)$. If G is locally free, then it is an affine subgroup of G. If k is a field, G is algebraic, and $G(k')$ is dense in G, then

$$ZG(k) = G(k) \cap Z(G(k')).$$

Let $\underline{\mathrm{Aut}}(G)$ be the functor

$$R \rightsquigarrow \mathrm{Aut}(G_R).$$

The action of G on itself by inner automorphisms defines a homomorphism of functors $G \to \underline{\mathrm{Aut}}(G)$, whose kernel is the functor ZG.

6.10 Even when G and H are smooth, $C_G(H)$ need not be smooth. For example, it is ☠ possible for $C_G(H)$ to be nontrivial without $C_G(H)(k')$ being nontrivial for any field k' containing k. To see this, let G be the functor

$$R \rightsquigarrow R \times R^{\times}$$

with the multiplication $(a,u)(b,v) = (a + bu^p, uv)$; here $0 \neq p = \mathrm{char}(k)$. This is an algebraic group because, as a functor to sets, it is isomorphic to $\mathbb{G}_a \times \mathbb{G}_m$. For a pair $(a,u) \in R \times R^{\times}$, $(a,u)(b,v) = (b,v)(a,u)$ for all (b,v) if and only if $u^p = 1$. Therefore, the centre of G is μ_p, and so $ZG(k') = 1$ for all fields k' containing k. Another example is provided by SL_p over a field of characteristic p. The centre of SL_p is μ_p, which is not smooth.

EXAMPLE 6.11 For a k-algebra R, the usual argument shows that the centre of $\mathrm{GL}_n(R)$ is the group of nonzero diagonal matrices. Therefore

$$Z(\mathrm{GL}_n) = \mathbb{G}_m \quad \text{(embedded diagonally).}$$

More abstractly, for any finite-dimensional vector space V,

$$Z(\mathrm{GL}_V) = \mathbb{G}_m \quad (a \in \mathbb{G}_m(R) \text{ acts on } V_R \text{ as } v \mapsto av).$$

EXAMPLE 6.12 Let $G = \mathrm{GL}_n$ over a field k. For an integer N, let H_N be the subfunctor

$$R \rightsquigarrow H_N(R) = \{\mathrm{diag}(a_1,\ldots,a_n) \in \mathrm{GL}_n(R) \mid a_1^N = \cdots = a_n^N = 1\}.$$

of G. Then $H_N \simeq (\mu_N)^n$, and so it is an affine subgroup of G. For N sufficiently large

$$C_G(H_N) = \mathbb{D}_n$$

(group of diagonal matrices) (see (XIV, 6.4)). We consider two cases.

(a) $k = \mathbb{Q}$ and N odd. Then $H_N(k) = \{1\}$, and

$$C_{G(k)}(H_N(k)) = \mathrm{GL}_n(k) \neq \mathbb{D}_n(k) = C_G(H_N)(k).$$

(b) k is algebraic closed of characteristic $p \neq 0$ and N is a power of p. Then $H_N(k) = 1$ and

$$C_{G(k)}(H_N(k)) = \mathrm{GL}_n(k) \neq \mathbb{D}_n(k) = C_G(H_N)(k).$$

An affine subgroup H of an affine group G is said to ***normalize*** (resp. ***centralize***) an affine subgroup N of G if $H(R)$ normalizes (resp. centralizes) $N(R)$ for all k-algebras R; equivalently, if $H \subset N_G(N)$ (resp. $H \subset C_G(N)$).

7 Quotient groups; surjective homomorphisms

What does it mean for a homomorphism of algebraic groups $G \to Q$ to be surjective? One might guess that it means that $G(R) \to Q(R)$ is surjective for all R, but this condition is too stringent. For example, it would say that $x \mapsto x^n\colon \mathbb{G}_m \to \mathbb{G}_m$ is not surjective even though $x \mapsto x^n\colon \mathbb{G}_m(k) \to \mathbb{G}_m(k)$ is surjective whenever k is algebraically closed. In fact, $\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$ is surjective according to the following definition.

DEFINITION 7.1 A homomorphism $G \to Q$ of affine groups is said to be ***surjective*** (and Q is called a ***quotient*** of G) if the homomorphism $\mathcal{O}(Q) \to \mathcal{O}(G)$ is faithfully flat.

A surjective homomorphism is also called a ***quotient map***.

PROPOSITION 7.2 *Let $u\colon H \to G$ be a homomorphism of affine groups. If u is surjective, then so also is $u_{k'}\colon H_{k'} \to G_{k'}$ for every k-algebra k'. Conversely, if $u_{k'}$ is surjective for one faithfully flat k-algebra k', then u is surjective.*

PROOF. Because $k \to k'$ is faithfully flat, the map $\mathcal{O}(G) \to \mathcal{O}(H)$ is faithfully flat if and only if $k' \otimes_k \mathcal{O}(G) \to k' \otimes_k \mathcal{O}(H)$ is faithfully flat (see CA §9). □

PROPOSITION 7.3 *A homomorphism of affine groups that is both injective and surjective is an isomorphism.*

PROOF. A faithfully flat map is injective (CA 9.6). Therefore, the map on coordinate rings is both surjective and injective, and hence is an isomorphism. □

THEOREM 7.4 *Let k be a field. The following conditions on a homomorphism $G \to Q$ are equivalent:*

(a) *$G \to Q$ is surjective, i.e., $\mathcal{O}(Q) \to \mathcal{O}(G)$ is faithfully flat;*
(b) *$\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective;*
(c) *for every k-algebra R and $q \in Q(R)$, there exists a faithfully flat R-algebra R' and a $g \in G(R')$ mapping to the image of q in $Q(R')$:*

$$\begin{tikzcd}
G(R') \arrow[r] \arrow[d] & Q(R') \arrow[d] & & \exists g \arrow[r, mapsto] & * \\
G(R) \arrow[r] & Q(R) & & & q. \arrow[u, mapsto]
\end{tikzcd}$$

PROOF. (a)$\Rightarrow$(c): Let $q \in Q(R)$. Regard q as a homomorphism $\mathcal{O}(Q) \to R$, and form the tensor product $R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R$:

$$\begin{tikzcd}
\mathcal{O}(G) \arrow[d, "g = 1 \otimes q"'] & & \mathcal{O}(Q) \arrow[ll, hook', "\text{faithfully flat}"'] \arrow[d, "q"] \arrow[dll, dashed, "q'"] \\
R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R & & R \arrow[ll, hook']
\end{tikzcd} \tag{64}$$

Then R' is a faithfully flat R-algebra because $\mathcal{O}(G)$ is a faithfully flat $\mathcal{O}(H)$-algebra (apply CA 9.7). The commutativity of the square in (64) means that $g \in G(R')$ maps to the image q' of q in $Q(R')$.

(c)$\Rightarrow$(b): Consider the "universal" element $\mathrm{id}_{\mathcal{O}(Q)} \in Q(\mathcal{O}(Q))$. If $G \to Q$ is surjective, there exists a $g \in G(R')$ with R' faithfully flat over $\mathcal{O}(Q)$ such that g and $\mathrm{id}_{\mathcal{O}(Q)}$ map to the same element of $Q(R')$, i.e., such that the diagram

$$\begin{tikzcd}
\mathcal{O}(G) \arrow[d, "g"] & \mathcal{O}(Q) \arrow[l] \arrow[d, "\mathrm{id}_{\mathcal{O}(Q)}"] \\
R' & \mathcal{O}(Q) \arrow[l, "\text{faithfully flat}"']
\end{tikzcd}$$

commutes. The map $\mathcal{O}(Q) \to R'$, being faithfully flat, is injective (CA 9.6), which implies that $\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective.

(b)$\Rightarrow$(a): According to (VI, 11.1) $\mathcal{O}(Q) \to \mathcal{O}(G)$ is faithfully flat. □

The condition (c) says that every $q \in Q(R)$ lifts to G after a faithfully flat extension. The proof of (a)$\Rightarrow$(c) is valid for k a ring.

COROLLARY 7.5 *Every homomorphism $H \to G$ of affine groups over a field factors into*

$$H \to H' \to G$$

with $H \to H'$ surjective and $H' \to G$ injective.

PROOF. The homomorphism $\mathcal{O}(G) \to \mathcal{O}(H)$ factors into

$$\mathcal{O}(G) \twoheadrightarrow \mathcal{O}(H') \hookrightarrow \mathcal{O}(H).$$ □

The affine group H' in the corollary is called the ***image*** of the homomorphism $H \to G$.

PROPOSITION 7.6 *Assume that k is a field. Let $G \to Q$ be a homomorphism of algebraic groups. If $G \to Q$ is a quotient map, then $G(k^{\mathrm{al}}) \to Q(k^{\mathrm{al}})$ is surjective; the converse is true if Q is smooth.*

PROOF. Let $q \in Q(k^{\mathrm{al}})$. For some finitely generated k^{al}-algebra R, the image of q in $Q(R)$ lifts to an element g of $G(R)$. Zariski's lemma (CA 11.1) shows that there exists a k^{al}-algebra homomorphism $R \to k^{\mathrm{al}}$, and the image of g in $G(k^{\mathrm{al}})$ maps to $q \in Q(k^{\mathrm{al}})$:

$$\begin{tikzcd}
 & G(R) \arrow[r] \arrow[d] & G(k^{\mathrm{al}}) \arrow[d] \\
Q(k^{\mathrm{al}}) \arrow[r] & Q(R) \arrow[r] & Q(k^{\mathrm{al}})
\end{tikzcd}
\qquad
\begin{tikzcd}
 & g \arrow[r, mapsto] \arrow[d, mapsto] & g_{k^{\mathrm{al}}} \arrow[d, mapsto] \\
q \arrow[r, mapsto] & q_R \arrow[r, mapsto] & q
\end{tikzcd}$$

$$\begin{tikzcd}
k^{\mathrm{al}} \arrow[r] \arrow[rr, bend left, "\mathrm{id}"] & R \arrow[r] & k^{\mathrm{al}}
\end{tikzcd}$$

For the converse, we may suppose that k is algebraically closed. Recall (I, 3.13) that an element f of $\mathcal{O}(Q)$ is a family $(f_R)_R$ with f_R a map $Q(R) \to R$. Because Q is smooth, $\mathcal{O}(Q)$ is reduced, and so f is determined by f_k (CA 11.8). As $G(k) \to Q(k)$ is surjective, f is determined by the composite $G(k) \longrightarrow Q(k) \xrightarrow{f_k} k$, and so $\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective. □

More generally, a homomorphism $u\colon G \to H$ of algebraic groups over a field is surjective if, for some field k' containing k, the image of $G(k')$ in $H(k')$ is dense in H (see IX, 3.3 below).

☠ 7.7 The smoothness condition in the second part of the proposition is necessary. Let k be a field of characteristic $p \neq 0$, and consider the homomorphism $1 \to \alpha_p$ where 1 denotes the trivial algebraic group. The map $1(k^{\mathrm{al}}) \to u_p(k^{\mathrm{al}})$ is $\{1\} \to \{1\}$, which is surjective, but $1 \to \alpha_p$ is not a quotient map because the map on coordinate rings is $k[X]/(X^p) \to k$, which is not injective.

THEOREM 7.8 *Let $G \to Q$ be a quotient map with kernel N. Then every homomorphism $G \to Q'$ whose kernel contains N factors uniquely through Q:*

$$\begin{tikzcd}
N \arrow[r] \arrow[rrd, "0"'] & G \arrow[r] \arrow[rd] & Q \arrow[d, dashed] \\
 & & Q'.
\end{tikzcd}$$

PROOF. Note that, if g and g' are elements of $G(R)$ with the same image in $Q(R)$, then $g^{-1}g'$ lies in N and so maps to 1 in $Q'(R)$. Therefore g and g' have the same image in $Q'(R)$. This shows that the composites of the homomorphisms

$$G \times_Q G \rightrightarrows G \to Q'$$

are equal. Therefore, the composites of the homomorphisms

$$\mathcal{O}(G)\otimes_{\mathcal{O}(Q)}\mathcal{O}(G)\leftleftarrows\mathcal{O}(G)\leftarrow\mathcal{O}(Q')$$

are equal. The subring of $\mathcal{O}(G)$ on which the two maps coincide is $\mathcal{O}(Q)$ (CA 9.6), and so the map $\mathcal{O}(Q')\to\mathcal{O}(G)$ factors through uniquely through $\mathcal{O}(Q)\hookrightarrow\mathcal{O}(G)$. Therefore $G\to Q'$ factors uniquely through $G\to Q$. □

COROLLARY 7.9 *If $\theta\colon G\to Q$ and $\theta'\colon G\to Q'$ are quotient maps with the same kernel, then there is a unique homomorphism $u\colon Q\to Q'$ such that $u\circ\theta=\theta'$; moreover, u is an isomorphism.*

PROOF. From the theorem, there are unique homomorphisms $u\colon Q\to Q'$ and $u'\colon Q'\to Q$ such that $u\circ\theta=\theta'$ and $u'\circ\theta'=\theta$. Now $u'\circ u=\mathrm{id}_Q$, because both have the property that $\beta\circ\theta=\theta$. Similarly, $u\circ u'=\mathrm{id}_{Q'}$, and so u and u' are inverse isomorphisms. □

DEFINITION 7.10 A surjective homomorphism $G\to Q$ with kernel N is called the ***quotient of** G **by** N*, and Q is denoted by G/N.

When it exists, the quotient is uniquely determined up to a unique isomorphism by the universal property in (7.8). We shall see later (VIII, 19.4) that quotients by normal subgroups always exist when k is a field.

DEFINITION 7.11 A sequence

$$1\to N\to G\to Q\to 1$$

is ***exact*** if $G\to Q$ is a quotient map with kernel N.

PROPOSITION 7.12 *Assume that k is a field. If*

$$1\to N\to G\to Q\to 1$$

is exact, then

$$\dim G=\dim N+\dim Q.$$

PROOF. For any homomorphism $u\colon G\to Q$ of abstract groups, the map

$$(n,g\mapsto(ng,g))\colon\mathrm{Ker}(u)\times G\to G\times_Q G$$

is a bijection — this just says that two elements of G with the same image in Q differ by an element of the kernel. In particular, for any homomorphism $u\colon G\to Q$ of affine groups and k-algebra R, there is a bijection

$$\mathrm{Ker}(u)(R)\times G(R)\to\big(G\times_Q G\big)(R),$$

which is natural in R. Therefore $N\times G\simeq G\times_Q G$,[3] and so

$$\mathcal{O}(N)\otimes\mathcal{O}(G)\simeq\mathcal{O}(G\times_Q G).$$

[3] This duplicates (58), p. 83.

Recall that the dimension of an algebraic group G has the following description: according to the Noether normalization theorem (CA 5.11), there exists a finite set S of elements in $\mathcal{O}(G)$ such that $k[S]$ is a polynomial ring in the elements of S and $\mathcal{O}(G)$ is finitely generated as a $k[S]$-module; the cardinality of S is $\dim G$. Since $\mathcal{O}(G \times_Q G) = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} \mathcal{O}(G)$, it follows from this description that

$$\dim(G \times_Q G) = 2\dim G - \dim Q.$$

Therefore $2\dim G - \dim Q = \dim N + \dim G$, from which the assertion follows.

[Need to explain this. If $\mathcal{O}(Q) = k[X_1,\ldots,X_m]$ and $\mathcal{O}(G) = k[X_1,\ldots,X_n]$, $n \geq m$, then the tensor product is a polynomial ring in

$$X_{m+1} \otimes 1, \ldots, X_n \otimes 1, 1 \otimes X_{m+1}, \ldots, 1 \otimes X_n,$$

over $k[X_1,\ldots,X_m]$; therefore, it is a polynomial ring in

$$m + (n-m) + (n-m) = 2n - m,$$

symbols over k, as required. In the general case, we can assume that k is algebraically closed and that Q and G are reduced and connected. Let $k(Q)$ be the field of fractions of $\mathcal{O}(Q)$. Then $\dim Q$ is the transcendence degree of $k(Q)$ over Q, and similarly for $\dim G$. Now the statement follows from the fact that $k(G \times_Q G)$ is the field of fractions of $k(G) \otimes_{k(Q)} k(G)$.] □

ASIDE 7.13 Proposition 7.12 can also be proved geometrically. First make a base extension to k^{al}. For a surjective map $\varphi\colon G \to Q$ of irreducible algebraic schemes, the dimension of the fibre over a closed point P of Q is equal $\dim(G) - \dim Q$ for P in a nonempty open subset of Q (cf. AG 10.9b). Now use homogeneity (VI, §5) to see that, when $G \to Q$ is a homomorphism of algebraic group schemes, all the fibres have the same dimension.

ASIDE 7.14 A morphism $u\colon A \to B$ in a category A is said to be an ***epimorphism*** if $\mathrm{Hom}(B,T) \to \mathrm{Hom}(A,T)$ is injective for all objects T.

It is obvious from Theorem 7.4 that a surjective homomorphism of affine groups is an epimorphism. The converse is true for groups (MacLane 1971, Exercise 5 to I 5), but it is false for affine groups. For example, the embedding

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \hookrightarrow \left\{ \begin{pmatrix} * & * \\ * & * \end{pmatrix} \right\} = \mathrm{GL}_2$$

is a nonsurjective epimorphism (any two homomorphisms from GL_2 that agree on B are equal).[4]

[4] This follows from the fact that $\mathrm{GL}_2/B \simeq \mathbb{P}^1$. Let f, f' be two homomorphisms $\mathrm{GL}_2 \to G$. If $f|B = f'|B$, then $g \mapsto f'(g) \cdot f(g)^{-1}$ defines a map $\mathbb{P}^1 \to G$, which has image 1_G because G is affine and $\mathbb{P}^1$ is complete (see AG 7.5).

Alternatively, in characteristic zero, one can show that any homomorphism of $B \cap \mathrm{SL}_2$ has at most one extension to SL_2 because any finite dimensional representation of $\mathfrak{sl}_2$ can be reconstructed from the operators h and y. Specifically, if $hv = mv$ and $y^{m+1}v = 0$, then $xv = 0$; if $hv = mv$ and $u = y^n v$, then $xy^n v$ can be computed as usual using that $[x,y] = h$.

8 Existence of quotients

PROPOSITION 8.1 *Let G be an affine algebraic group over a field k, and let H be an affine subgroup of G. Among the surjective homomorphism $G \to Q$ zero on H, there is a universal one.*

PROOF. For any finite family $(G \xrightarrow{q_i} Q_i)_{i \in I}$ of surjective morphisms such that $H \subset \mathrm{Ker}(q_i)$ all i, let $H_I = \bigcap_{i \in I} \mathrm{Ker}(q_i)$. According to (3.3), there exists a family for which H_I is minimal. For such a family, I claim that the map from G to the image of $(q_i)\colon G \to \prod_{i \in I} Q_i$ is universal. If it isn't, then there exists a homomorphism $q\colon G \to Q$ containing H in its kernel but not H_I. But then $H_{I \cup \{q\}} = H_I \cap \mathrm{Ker}(q)$ is properly contained in H_I.□

Later (VIII, 17.5), we shall show that, when H is normal and k is a field, the kernel of the universal homomorphism $G \to Q$ is exactly H.

9 Semidirect products

DEFINITION 9.1 An affine group G is said to be a ***semidirect product*** of its affine subgroups N and Q, denoted $G = N \rtimes Q$, if N is normal in G and the map $(n,q) \mapsto nq\colon N(R) \times Q(R) \to G(R)$ is a bijection of sets for all k-algebras R.

In other words, G is a semidirect product of its affine subgroups N and Q if $G(R)$ is a semidirect product of its subgroups $N(R)$ and $Q(R)$ for all k-algebras R (cf. GT 3.7).

For example, let $\mathbb{T}_n$ be the algebraic group of upper triangular matrices, so

$$\mathbb{T}_n(R) = \{(a_{ij}) \in \mathrm{GL}_n(R) \mid a_{ij} = 0 \text{ for } i > j\}.$$

Then $\mathbb{T}_n$ is the semidirect product of its (normal) subgroup $\mathbb{U}_n$ and its subgroup $\mathbb{D}_n$.

PROPOSITION 9.2 *Let N and Q be affine subgroups of an affine group G. Then G is the semidirect product of N and Q if and only if there exists a homomorphism $G \to Q$ whose restriction to Q is the identity map and whose kernel is N.*

PROOF. $\Rightarrow$: By assumption, the product map is a bijection of functors $N \times Q \to G$. The composite of the inverse of this map with the projection $N \times Q \to Q$ has the required properties.

$\Leftarrow$: Let $\varphi\colon G \to Q$ be the given homomorphism. For each k-algebra R, $\varphi(R)$ realizes $G(R)$ as a semidirect product $G(R) = N(R) \rtimes Q(R)$ of its subgroups $N(R)$ and $Q(R)$. □

Let G be an affine group and X a functor from the category of k-algebras to sets. Recall V, §6 that an action of G on X is a natural transformation $\theta\colon G \times X \to X$ such that each map $G(R) \times X(R) \to X(R)$ is an action of the group $G(R)$ on the set $X(R)$. Now let N and Q be algebraic groups and suppose that there is given an action of Q on N

$$(q,n) \mapsto \theta_R(q,n)\colon Q(R) \times N(R) \to N(R)$$

such that, for each q, the map $n \mapsto \theta_R(q,n)$ is a group homomorphism. Then the functor

$$R \rightsquigarrow N(R) \rtimes_{\theta_R} Q(R)$$

(cf. GT 3.9) is an affine group because, as a functor to sets, it is $N \times Q$, which is represented by $\mathcal{O}(N) \otimes \mathcal{O}(G)$. We denote it by $N \rtimes_\theta Q$, and call it the ***semidirect product of*** N ***and*** Q ***defined by*** θ.

9.3 When k is a perfect field, G_{red} is an affine subgroup of G (see VI, 6.3), but it need not be normal. For example, over a field k of characteristic 3, let $G = \mu_3 \rtimes (\mathbb{Z}/2\mathbb{Z})_k$ for the (unique) nontrivial action of $(\mathbb{Z}/2\mathbb{Z})_k$ on μ_3; then $G_{\text{red}} = (\mathbb{Z}/2\mathbb{Z})_k$, which is not normal in G (see SGA 3 VI_{A} 0.2).

EXAMPLE 9.4 Let k be a field of characteristic 3. There is a unique nontrivial action of the constant affine group $(\mathbb{Z}/2\mathbb{Z})_k$ on μ_3, and we let $G = \mu_3 \rtimes (\mathbb{Z}/2\mathbb{Z})_k$. The reduced group G_{red} is the subgroup $(\mathbb{Z}/2\mathbb{Z})_k$ of G, which is not normal in G.

EXAMPLE 9.5 Over a field of characteristic p, there is an obvious action of $\mathbb{G}_m$ on α_p, and hence an action of μ_p on α_p. The semi-direct product is a noncommutative finite connected affine group of order p^2.

10 Smooth algebraic groups

PROPOSITION 10.1 *Quotients and extensions of smooth algebraic groups over a field are smooth.*

PROOF. Let Q be the quotient of G by the affine subgroup N. Then $Q_{k^{\text{al}}}$ is the quotient of $G_{k^{\text{al}}}$ by $N_{k^{\text{al}}}$. If G is smooth, $\mathcal{O}(G_{k^{\text{al}}})$ is reduced; as $\mathcal{O}(Q_{k^{\text{al}}}) \subset \mathcal{O}(G_{k^{\text{al}}})$, it also is reduced, and so Q is smooth. For extensions, we (at present) appeal to algebraic geometry: let $W \to V$ be a regular map of algebraic varieties; if V is smooth and the fibres of the map are smooth subvarieties of W with constant dimension, then W is smooth tba... □

10.2 The kernel of a homomorphism of smooth algebraic groups need not be smooth. For example, in characteristic p, the kernels of $x \mapsto x^p \colon \mathbb{G}_m \to \mathbb{G}_m$ and $x \mapsto x^p \colon \mathbb{G}_a \to \mathbb{G}_a$ are not smooth (they are μ_p and α_p respectively).

11 Algebraic groups as sheaves

Some of the above discussion simplifies when regard affine groups as sheaves. Throughout this section, k is a field.

PROPOSITION 11.1 *Let F be a functor from the category of k-algebras to sets. If F is representable, then*

(F1) *for every finite family of k-algebras $(R_i)_{i \in I}$, the canonical map $F(\prod_i R_i) \to \prod_i F(R_i)$ is bijective;*

(F2) *for every faithfully flat homomorphism $R \to R'$ of k-algebras, the sequence*

$$F(R) \to F(R') \rightrightarrows F(R' \otimes_R R')$$

is exact (i.e., the first arrow realizes $F(R)$ as the equalizer of the pair of arrows).

PROOF. (F1). For any k-algebra A, it follows directly from the definition of product that

$$\mathrm{Hom}(A, \prod_{i\in I} R_i) \simeq \prod_{i\in I} \mathrm{Hom}(A, R_i),$$

(F2). If $R \to R'$ is faithfully flat, then it is injective, and so

$$\mathrm{Hom}(A, R) \to \mathrm{Hom}(A, R')$$

is injective for any k-algebra A. According to (CA 9.5), the sequence

$$R \to R' \rightrightarrows R' \otimes_R R'$$

is exact, and it follows that

$$\mathrm{Hom}_{k\text{-alg}}(A, R) \to \mathrm{Hom}_{k\text{-alg}}(A, R') \rightrightarrows \mathrm{Hom}_{k\text{-alg}}(A, R' \otimes_R R')$$

is exact. □

A functor satisfying the conditions (F1) and (F2) is said to be a ***sheaf for the flat topology***[5].

PROPOSITION 11.2 *A functor $F\colon \mathsf{Alg}_k \to \mathsf{Set}$ is a sheaf if and only if it satisfies the following condition:*

(S) *for every k-algebra R and finite family $(R_i)_{i\in I}$ of k-algebras such that $R \to \prod_i R_i$ is faithfully flat, the sequence*

$$F(R) \to \prod_{i\in I} F(R_i) \rightrightarrows \prod_{(i,i')\in I\times I} F(R_i \otimes_k R_{i'})$$

is exact.

PROOF. Easy exercise (cf. Milne 1980, II 1.5). □

We sometimes use (S1) to denote the condition that $F(R) \to \prod_{i\in I} F(R_i)$ is injective and (S2) for the condition that its image is subset on which the pair of maps agree. [Define presheaf and separated sheaf.]

PROPOSITION 11.3 *For any functor $F\colon \mathsf{Alg}_k \to \mathsf{Set}$, there exists a sheaf aF and a natural transformation $F \to aF$ that is universal among natural transformations from F to sheaves.*

PROOF. For $a, b \in F(R)$, set $a \sim b$ if a and b have the same image in $F(R')$ for some faithfully flat R-algebra R'. Then $\sim$ is an equivalence relation on $F(R)$, and the functor $R \rightsquigarrow F(R)/{\sim}$ satisfies (S1). Moreover, any natural transformation from F to a sheaf will factor uniquely through $F \to F/\sim$.

Now let F be a functor satisfying (S1). For any k-algebra R, define

$$F'(R) = \varinjlim \mathrm{Ker}(F(R') \rightrightarrows F(R' \otimes_R R')).$$

where R' runs over the faithfully flat R-algebras. One checks easily that F' is a sheaf, and that any natural transformation from F to a sheaf factors uniquely through $F \to F'$. □

[5] Strictly, for the fpqc (fidèlement plat quasi-compacte) topology.

The sheaf aF is called the ***associated sheaf*** of F.

[The functors Sheaves $\rightsquigarrow$ separated presheaves $\rightsquigarrow$ presheaves have left adjoints. Given a presheaf P, define $\bar{P}(R) = P(R)/\sim$ where $a \sim b$ if there exists a faithfully flat R-algebra R' such that a and b have the same image in $P(R')$. Then $\bar{P}$ is a separated presheaf. Given a separated presheaf P, define $(aP)(R)$ to be the set of equivalence classes of pairs (R', a) where $a \in P(R')$ has the same image under the maps $P(R') \to P(R' \otimes_R R')$ defined by $R \to R' \otimes_R R'$.]

PROPOSITION 11.4 *Let S be a sheaf, and let F be a subfunctor of S. If*

$$S(R) = \bigcup_{R' \text{ a faithfully flat } R\text{-algebra}} \left(S(R) \cap F(R')\right)$$

(intersection inside $S(R')$), then S is the sheaf associated with F.

PROOF. Obviously any natural transformation $F \to F'$ with F' a sheaf extends uniquely to S. □

Let P be the category of functors $\mathsf{Alg}_k \to \mathsf{Set}$, and let S be the full subcategory of P consisting of the sheaves.

PROPOSITION 11.5 *The inclusion functor $i\colon \mathsf{S} \to \mathsf{P}$ preserves inverse limits; the functor $a\colon \mathsf{P} \to \mathsf{S}$ preserves direct limits and finite inverse limits.*

PROOF. By definition $\mathrm{Hom}(a(-),-) \simeq \mathrm{Hom}(-, i(-))$, and so a and i are adjoint functors. This implies (immediately) that i preserves inverse limits and a preserves direct limits. To show that a preserves finite inverse limits, it suffices to show that it preserves finite products and equalizers, which follows from the construction of a. □

PROPOSITION 11.6 *Let $G \to Q$ be a surjective homomorphism of affine groups with kernel N. Then Q represents the sheaf associated with the functor*

$$R \rightsquigarrow G(R)/N(R).$$

PROOF. Let P be the functor $R \rightsquigarrow G(R)/N(R)$. Then P commutes with products, and we shall show:

(a) For any injective homomorphism $R \to R'$ of k-algebras, the map $P(R) \to P(R')$ is injective.

(b) Let
$$P'(R) = \varinjlim_{R'} \mathrm{Ker}(P(R') \rightrightarrows P(R' \otimes_R R'))$$
where the limit is over all faithfully flat R-algebras; then $P' \simeq Q$.

For (a), we have to prove that

$$N(R) = N(R') \cap G(R) \quad \text{(intersection inside } G(R')\text{)}.$$

For some index set I, $N(R)$ is the subset of R^I defined by some polynomial conditions

$$f_j(\ldots, X_i, \ldots) = 0$$

and $N(R')$ is the subset of R'^I defined by the same polynomial conditions. But if an element of R^I satisfies the conditions when regarded as an element of R'^I, then it already satisfies the conditions in R^I (because $R \to R'$ is injective).

For (b), consider the diagram

$$\begin{tikzcd}
K(R') \arrow[r] & P(R') \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & P(R' \otimes_R R') \arrow[d] \\
Q(R) \arrow[r] & Q(R') \arrow[r, shift left] \arrow[r, shift right] & Q(R' \otimes_R R')
\end{tikzcd}$$

where $K(R')$ is the equalizer of the top pair of maps — we know that $Q(R)$ is the equalizer of the bottom pair of maps. For any k-algebra R', the map $P(R') \to Q(R')$ is injective, and so the two vertical arrows induce an injective homomorphism $K(R') \to Q(R)$. When we pass to the limit over R', it follows directly from the definition of "surjective' (see 7.1) that this map becomes surjective. □

NOTES (a) Explain why it is useful to regard the affine groups as sheaves rather than presheaves.

(b) Explain the set-theoretic problems with (11.3) (limit over a proper class), and why we don't really need the result (or, at least, we can avoid the problems). See Waterhouse 1975.

12 Terminology

From now on, "subgroup" of an affine group will mean "affine subgroup". Thus, if G is an affine (or algebraic) group, a subgroup H of G is again an affine (or algebraic) group, whereas a subgroup H of $G(k)$ is an abstract group.

13 Exercises

EXERCISE VII-1 Let A and B be subgroups of the affine group G, and let AB be the sheaf associated with the subfunctor $R \rightsquigarrow A(R)\cdot B(R)$ of G.

(a) Show that AB is representable by $\mathcal{O}(G)/\mathfrak{a}$ where $\mathfrak{a}$ is the kernel of homomorphism $\mathcal{O}(G) \to \mathcal{O}(A) \otimes \mathcal{O}(B)$ defined by the map $a,b \mapsto ab\colon A \times B \to G$ (of set-valued functors).

(b) Show that, for any k-algebra R, an element $G(R)$ lies in $(AB)(R)$ if and only if its image in $G(R')$ lies in $A(R')\cdot B(R')$ for some faithfully flat R-algebra R', i.e.,

$$(AB)(R) = \bigcap\nolimits_{R'} G(R) \cap \left(A(R')\cdot B(R')\right).$$

EXERCISE VII-2 Let A, B, C be subgroups of an affine group G such that A is a normal subgroup of B and B normalizes C. Show:

(a) $C \cap A$ is a normal subgroup of $C \cap B$;
(b) CA is a normal subgroup of CB.

EXERCISE VII-3 (Dedekind's modular laws). Let A, B, C be subgroups of an affine group G such that A is a subgroup of B. Show:

(a) $B \cap AC = A(B \cap C)$;
(b) if $G = AC$, then $B = A(B \cap C)$.

CHAPTER **VIII**

Representations of Affine Groups

One of the main results in this chapter is that all algebraic groups over fields can be realized as subgroups of GL_n for some n. At first sight, this is a surprising result, because it says that all possible multiplications in algebraic groups are just matrix multiplication in disguise.

In this chapter, we often work with algebraic monoids rather than groups since this forces us to distinguish between "left" and "right" correctly. Note that for a *commutative* ring R, the only difference between a left module and a right module is one of notation: it is simply a question of whether we write rm or mr (or better $\overset{r}{m}$). In this chapter, it will sometimes be convenient to regard R-modules as right modules, and write $V \otimes_k R$ instead of $R \otimes_k V$.

Starting with §7, k is a field.

1 Finite groups

We first look at how to realize a finite group G as a matrix group. Let k be a field. A representation of G on a k-vector space V is a homomorphism of groups $G \to \mathrm{Aut}_{k\text{-lin}}(V)$, or, in other words, an action $G \times V \to V$ of G on V in which each $\gamma \in G$ acts k-linearly. Let $X \times G \to X$ be a right action of G on a finite set X. Define V to be the k-vector space of maps $X \to k$, and let G act on V according to the rule:

$$(gf)(x) = f(xg) \quad \text{for } g \in G,\ f \in V,\ x \in X.$$

This defines a representation of G on V, which is faithful if G acts effectively on X. The vector space V has a canonical basis consisting of the maps that send one element of X to 1 and the remainder to 0, and so this gives a homomorphism $G \to \mathrm{GL}_n(k)$ where n is the order of X. For example, for the symmetric group S_n acting on $\{1,2,\ldots,n\}$, this gives the map $\sigma \mapsto I(\sigma)\colon S_n \to \mathrm{GL}_n(k)$ in p.11. When we take $X = G$, the vector space V is the k-algebra $\mathcal{O}(G)$ of maps $G \to k$, and the representation is called the ***regular representation***.

2 Definition of a representation

Let V be a k-module. For a k-algebra R, we let

$$\begin{aligned} V(R) &= V \otimes R, && (R\text{-module}) \\ \mathrm{End}_V(R) &= \mathrm{End}_{R\text{-lin}}(V(R)), && (\text{monoid under composition}) \\ \mathrm{Aut}_V(R) &= \mathrm{Aut}_{R\text{-lin}}(V(R)), && (\text{group under composition}). \end{aligned}$$

Then $R \rightsquigarrow \mathrm{End}_V(R)$ is a functor from the category of k-algebras to monoids and $R \rightsquigarrow \mathrm{Aut}_V(R)$ is a functor from the category of k-algebras to groups. With the terminology of (I, 4.2), $\mathrm{Aut}_V = \mathrm{End}_V^{\times}$. When V is finitely generated and projective, these functors are representable (IV, 1.6), and so End_V is an affine monoid and Aut_V is an affine group in this case.

Let G be an affine monoid or group over k. A ***linear representation*** of G on a k-module V is a natural transformation $r\colon G \to \mathrm{End}_V$ of monoid-valued functors. In other words, it is a family of homomorphisms of monoids

$$r_R\colon G(R) \to \mathrm{End}_{R\text{-lin}}(V(R)), \quad R \text{ a } k\text{-algebra}, \tag{65}$$

such that, for every homomorphism $R \to R'$ of k-algebras, the diagram

$$\begin{tikzcd} G(R) \arrow[r, "r_R"] \arrow[d] & \mathrm{End}_{R\text{-lin}}(V(R)) \arrow[d] \\ G(R') \arrow[r, "r_{R'}"] & \mathrm{End}_{R'\text{-lin}}(V(R')) \end{tikzcd}$$

commutes. When G is an affine group, r takes values in Aut_V and is a natural transformation of group-valued functors. A linear representation is said to be ***finite-dimensional*** if V is finite-dimensional as a k-vector space, and it is ***faithful*** if all the homomorphisms r_R are injective.

When k is a field and W is a subspace of V, then $W(R)$ is a subspace of $V(R)$ for all R, and we say that W is a ***subrepresentation*** if $r_R(g)(W(R)) \subset W(R)$ for all k-algebras R and all $g \in G(R)$.

A ***homomorphism of linear representations*** $(V,r) \to (V',r')$ is a k-linear map $u\colon V \to V'$ such that

$$\begin{tikzcd} V(R) \arrow[r, "u(R)"] \arrow[d, "r_R(g)"] & V'(R) \arrow[d, "r'_R(g)"] \\ V(R) \arrow[r, "u(R)"] & V'(R) \end{tikzcd}$$

commutes for all $g \in G(R)$ and all k-algebras R.

We write V also for the functor $R \rightsquigarrow V(R)$ defined by V. Then a linear representation of G on V can also be defined as an action of G on V,

$$G \times V \to V, \tag{66}$$

such that each $g \in G(R)$ acts R-linearly on $V(R)$.

When $V = k^n$, End_V is the monoid $R \rightsquigarrow (M_n(R), \times)$ and $\mathrm{Aut}_V = \mathrm{GL}_n$. A linear representation of an affine monoid (resp. group) G on V is a homomorphism $G \to (M_n, \times)$ (resp. $G \to \mathrm{GL}_n$).

EXAMPLE 2.1 Let $G=\mathbb{G}_a$ and let k be a field. Let V be a finite-dimensional k-vector space, and let $\rho_0,\ldots,\rho_i,\ldots$ be a sequence of endomorphisms V such that all but a finite number are zero. For $t\in R$, let

$$r_R(t)=\sum\nolimits_{i\geq 0}\rho_i t^i\in \operatorname{End}(V(R)),$$

so $r_R(t)(v\otimes c)=\sum\rho_i(v)\otimes ct^i$. If

$$\begin{cases}\rho_0 & = & \mathrm{id}_V\\ \rho_i\circ\rho_j & = & \binom{i+j}{i}\rho_{i+j} \qquad \text{all } i,j\geq 0,\end{cases} \tag{67}$$

then

$$r_R(t+t')=r_R(t)+r_R(t')\quad \text{for all } t,t'\in R,$$

and so r_R is a representation. We shall see later (6.4) that all finite-dimensional representations of $\mathbb{G}_a$ are of this form. Note that (67) implies that $\rho_i\circ\rho_1=(i+1)\rho_{i+1}$, and so $\rho_1^n=n!\rho_n$. When k has characteristic zero, this implies that ρ_1 is nilpotent and that $\rho_n=\rho_1^n/n!$, and so

$$r_R(t)=\sum(\rho_1 t)^n/n!=\exp(\rho_1 t);$$

hence the finite-dimensional representations of $\mathbb{G}_a$ are just the pairs (V,ρ_1) with ρ_1 a nilpotent endomorphism of V.[1] When k has nonzero characteristic, there are more possibilities. See Abe 1980, p. 185.

EXAMPLE 2.2 Let $G=\mathrm{GL}_n$, and let M_n denote the vector space of all $n\times n$ matrices with entries in k. The actions

$$(P,A)\mapsto PAP^{-1}\colon G(R)\times M_n(R)\to M_n(R)$$

define a linear representation of G on M_n. The orbits of $G(k)$ acting on $M_n(k)$ are the similarity classes, which are represented by the Jordan matrices when k is an algebraically closed field.

EXAMPLE 2.3 There is a unique linear representation r of G on $\mathcal{O}(G)$ (regarded as a k-module) such that

$$(gf)_R(x)=f_R(xg),\quad \text{for all } g\in G(R),\ f\in\mathcal{O}(G),\ x\in G(R). \tag{68}$$

This is called the ***regular representation***. In more detail: the formula (68) defines a map $G(R)\times\mathcal{O}(G)\to R\otimes\mathcal{O}(G)$, which extends by linearity to a map $G(R)\times R\otimes\mathcal{O}(G)\to R\otimes\mathcal{O}(G)$.

3 Terminology

From now on, "representation" will mean "linear representation".

[1] Let k be a ring of characteristic zero (i.e., containing $\mathbb{Q}$). Then the same argument shows that the representations of $\mathbb{G}_a$ on k-modules (not necessarily finitely generated) are the pairs (V,ρ_1) where ρ_1 is a locally nilpotent endomorphism of V (i.e., nilpotent on every finitely generated submodule). Cf. sx108817.

4 Comodules

Let (A,m,e) be a k-algebra, not necessarily commutative. A left A-module is a k-vector space V together with a k-linear map $\mu\colon A\otimes V\to V$ such that the diagrams

$$\begin{tikzcd}
V & A\otimes V \arrow[l, "\mu"'] & V & A\otimes V \arrow[l, "\mu"'] \\
A\otimes V \arrow[u, "\mu"] & A\otimes A\otimes V \arrow[l, "A\otimes\mu"'] \arrow[u, "m\otimes V"] & V \arrow[u, equal] & k\otimes V \arrow[l, "\simeq"'] \arrow[u, "e\otimes V"]
\end{tikzcd} \tag{69}$$

commute. On reversing the directions of the arrows, we obtain the notion of comodule over a coalgebra.

DEFINITION 4.1 Let (C,Δ,ϵ) be a k-coalgebra. A ***right C-comodule***[2] is a k-linear map $\rho\colon V\to V\otimes C$ (called the ***coaction*** of C on V) such that the diagrams

$$\begin{tikzcd}
V \arrow[r, "\rho"] \arrow[d, "\rho"] & V\otimes C \arrow[d, "V\otimes\Delta"] & V \arrow[r, "\rho"] \arrow[d, equal] & V\otimes C \arrow[d, "V\otimes\epsilon"] \\
V\otimes C \arrow[r, "\rho\otimes C"] & V\otimes C\otimes C & V \arrow[r, "\simeq"] & V\otimes k
\end{tikzcd} \tag{70}$$

commute, i.e., such that

$$\begin{cases} (V\otimes\Delta)\circ\rho &=& (\rho\otimes C)\circ\rho \\ (V\otimes\epsilon)\circ\rho &=& V. \end{cases}$$

A ***homomorphism*** $u\colon(V,\rho)\to(V',\rho')$ of C-comodules is a k-linear map $u\colon V\to V'$ such that the diagram

$$\begin{tikzcd}
V \arrow[r, "u"] \arrow[d, "\rho"] & V' \arrow[d, "\rho'"] \\
V\otimes C \arrow[r, "u\otimes C"] & V'\otimes C
\end{tikzcd}$$

commutes. A comodule is said to be ***finite-dimensional*** if it is finite-dimensional as a k-vector space.

EXAMPLE 4.2 (a) The pair (C,Δ) is a right C-comodule (compare (15), p. 30, with (70)). More generally, for any k-module V,

$$V\otimes\Delta\colon V\otimes C\to V\otimes C\otimes C$$

is a right C-comodule (called the ***free comodule on*** V). When V is free, the choice of a basis for V realizes $(V\otimes C, V\otimes\Delta)$ as a direct sum of copies of (C,Δ):

$$\begin{tikzcd}
V\otimes C \arrow[r, "V\otimes\Delta"] \arrow[d, "\approx"] & V\otimes C\otimes C \arrow[d, "\approx"] \\
C^n \arrow[r, "\Delta^n"] & (C\otimes C)^n.
\end{tikzcd}$$

[2] It would be more natural to consider left comodules, except that it is *right* comodules that correspond to *left* representations of monoids. Because we consider right comodules we are more-or-less forced to write $V\otimes R$ where elsewhere we write $R\otimes V$.

(b) Let (V_1,ρ_1) and (V_2,ρ_2) be comodules over coalgebras C_1 and C_2 respectively. The map

$$V_1\otimes V_2 \xrightarrow{\rho_1\otimes\rho_2} V_1\otimes C_1\otimes V_2\otimes C_2 \simeq V_1\otimes V_2\otimes C_1\otimes C_2$$

provides $V_1\otimes V_2$ with the structure of a $C_1\otimes C_2$-comodule.

(c) Let (V,ρ) be a right C-comodule, and let $u\colon C\to C'$ be a homomorphism of coalgebras. The map

$$V \xrightarrow{\rho} V\otimes C \xrightarrow{V\otimes u} V\otimes C'$$

provides V with the structure of a right C'-comodule.

(d) Let V be a k-vector space, and let $\rho\colon V\to V\otimes C$ be a k-linear map. Choose a basis $(e_i)_{i\in I}$ for V, and write

$$\rho(e_j)=\sum_{i\in I} e_i\otimes c_{ij},\quad c_{ij}\in C, \tag{71}$$

(finite sum, so, for each j, almost all c_{ij}'s are zero). Then (V,ρ) is a right comodule if and only if[3]

$$\left.\begin{array}{rcl}\Delta(c_{ij}) & = & \sum_{k\in I} c_{ik}\otimes c_{kj}\\ \epsilon(c_{ij}) & = & \delta_{ij}\end{array}\right\}\quad \text{all } i,j\in I. \tag{72}$$

For a module V over an algebra A, there is a smallest quotient of A, namely, the image of A in $\mathrm{End}_k(V)$, through which the action of A on V factors. In the next remark, we show that for a comodule V over a coalgebra C, there is a smallest subcoalgebra C_V of C through which the co-action of C on V factors.

REMARK 4.3 Assume that k is a field, and let (V,ρ) be a C-comodule.

(a) When we choose a k-basis $(e_i)_{i\in I}$ for V, the equations (72) show that the k-subspace spanned by the c_{ij} is a subcoalgebra of C, which we denote C_V. Clearly, C_V is the smallest subspace of C such that $\rho(V)\subset V\otimes C_V$, and so it is independent of the choice of the basis. When V is finite dimensional over k, so also is C_V.

(b) Recall that for a finite-dimensional k-vector space V,

$$\mathrm{Hom}_{k\text{-lin}}(V,V\otimes C)\simeq \mathrm{Hom}_{k\text{-lin}}(V\otimes V^\vee,C).$$

If $\rho\leftrightarrow\rho'$ under this isomorphism, then

$$\rho(v)=\sum\nolimits_{i\in I} e_i\otimes c_i \implies \rho'(v\otimes f)=\sum\nolimits_{i\in I} f(e_i)c_i.$$

In particular, $\rho'(e_j\otimes e_i^\vee)=c_{ij}$ (notation as in (71)). Therefore C_V is the image of $\rho'\colon V\otimes V^\vee\to C$.

(c) If (V,ρ) is a sub-comodule of (C,Δ), then $V\subset C_V$. To see this, note that the restriction of the co-identity ϵ of C to V is an element ϵ_V of $V^\vee$ and that $\rho'(v\otimes\epsilon_V)=v$

[3] The first equality can be written symbolically as

$$(\Delta(c_{ij}))=(c_{ik})\otimes(c_{kj}).$$

for all $v \in V$ because

$$\begin{aligned}
\rho'(e_j \otimes \epsilon_V) &= \textstyle\sum_{i\in I} \epsilon(e_j)c_{ij} \\
&= (\epsilon \otimes \mathrm{id}_C)\Delta(e_j) \\
&= (\mathrm{id}_C \otimes \epsilon)\Delta(e_j) && \text{(by (15), p. 30)} \\
&= \textstyle\sum_{i\in I} e_j\epsilon(c_{ij}) \\
&= e_j && \text{(by (72)).}
\end{aligned}$$

REMARK 4.4 Assume that k is a field. Recall (II, §3) that the linear dual of a coalgebra (C,Δ,ϵ) is an algebra $(C^\vee,\Delta^\vee,\epsilon^\vee)$ (associative with identity). Let V be a k-vector space, and let $\rho\colon V \to V \otimes C$ be a k-linear map. Define μ to be the composite of

$$C^\vee \otimes V \xrightarrow{C^\vee \otimes \rho} C^\vee \otimes V \otimes C \simeq V \otimes C^\vee \otimes C \xrightarrow{V \otimes \mathrm{ev}} V \otimes k \simeq V$$

where $\mathrm{ev}\colon C^\vee \otimes C \to k$ is the evaluation map. One can check that (V,ρ) is a right C-comodule if and only if (V,μ) is a left $C^\vee$-module. When C and V are finite-dimensional, $\rho \mapsto \mu$ is a bijection

$$\mathrm{Hom}_{k\text{-lin}}(V, V \otimes C) \simeq \mathrm{Hom}_{k\text{-lin}}(C^\vee \otimes V, V),$$

and so there is a one-to-one correspondence between the right C-comodule structures on V and the left $C^\vee$-module structures on V. In the general case, not every $C^\vee$-module structure arises from a C-comodule structure, but it is known which do (Dăscălescu et al. 2001, 2.2; Sweedler 1969, 2.1).

Assume that C is flat over k (i.e., as a k-module), and let (V,ρ) be a C-comodule. If W is a k-submodule V, then $W \otimes C$ is a k-submodule of $V \otimes C$, and we say that W is a ***subcomodule*** of V if $\rho(W) \subset W \otimes C$. Then $(W, \rho|W)$ is a C-comodule.

PROPOSITION 4.5 *Assume that k is a field. Every comodule (V,ρ) is a filtered union of its finite-dimensional sub-comodules.*

PROOF. As a finite sum of (finite-dimensional) sub-comodules is a (finite-dimensional) sub-comodule, it suffices to show that each element v of V is contained in a finite-dimensional sub-comodule. Let $(e_i)_{i\in I}$ be a basis for C as a k-vector space, and let

$$\rho(v) = \textstyle\sum_i v_i \otimes e_i, \quad v_i \in V,$$

(finite sum, i.e., only finitely many v_i are nonzero). Write

$$\Delta(e_i) = \textstyle\sum_{j,k} r_{ijk}(e_j \otimes e_k), \quad r_{ijk} \in k.$$

We shall show that

$$\rho(v_k) = \textstyle\sum_{i,j} r_{ijk}\left(v_i \otimes e_j\right) \tag{73}$$

from which it follows that the k-subspace of V spanned by v and the v_i is a subcomodule containing v. Recall from (70) that

$$(V \otimes \Delta) \circ \rho = (\rho \otimes C) \circ \rho.$$

On applying each side of this equation to v, we find that

$$\sum\nolimits_{i,j,k} r_{ijk}(v_i \otimes e_j \otimes e_k) = \sum\nolimits_k \rho(v_k) \otimes e_k \quad (\text{inside } V \otimes C \otimes C).$$

On comparing the coefficients of $1 \otimes 1 \otimes e_k$ in these two expressions, we obtain (73). □

COROLLARY 4.6 *Assume that k is a field. A coalgebra C is a union of its sub-coalgebras C_V, where V runs over the finite-dimensional sub-comodules of C.*

PROOF. For any finite-dimensional sub-comodule V of C,

$$V \subset C_V \subset C$$

(see 4.3), and so this follows from the proposition. □

ASIDE 4.7 When k is a noetherian ring, every comodule V over a *flat* k-coalgebra C is a filtered union of finitely generated subcomodules (Serre 1993, 1.4). The proof depends on the following lemma:

> Let W be a k-submodule V, and let W° be the set $v \in V$ such that $\rho(v) \in W \otimes C$; then W° is a subcomodule of V.

Now $W^\circ \subset W$ because

$$W^\circ \overset{(70)}{=} ((\mathrm{id}_V \otimes \epsilon) \circ \rho)(W^\circ) \subset (\mathrm{id}_V \otimes \epsilon)(W \otimes C) = W,$$

and it is clear that W° the largest comodule contained in W.

Granted this, let W be a finitely generated k-submodule of V. It suffices to show that W is contained in a finitely generated subcomodule of V. As $\rho(W)$ is a finitely generated over k, there exists a finitely generated k-submodule W_1 of V such that $\rho(W) \subset W_1 \otimes C$. Now W_1° is a subcomodule contained in W_1, hence finitely generated (because k is noetherian), and it obviously contains W.

ASIDE 4.8 Now let k be an arbitrary ring, but assume that C is *projective* as a k-module. Let W be a k-submodule of a C-comodule V, and let $c(W) \subset V$ be the image of the k-module homomorphisms

$$W \otimes C^\vee \xrightarrow{\rho \otimes \mathrm{id}} V \otimes C \otimes C^\vee \xrightarrow{\mathrm{id} \otimes \mathrm{ev}} V.$$

Then $c(W)$ is the smallest subcomodule of V containing W, and it is a finitely generated k-submodule if W is (SGA 3, VI, 11.8). The hypothesis "projective" in this statement can not be replaced by "flat" (ibid. 11.10.1).

5 The category of comodules

Let (C, Δ, ϵ) be a flat coalgebra over k. With the obvious definitions, the standard isomorphism theorems (cf. IX, 1.1, 1.2, 1.3, 1.4 below) hold for comodules over C. For example, if (W, ρ_W) is a sub-comodule of (V, ρ_V), then the quotient vector space V/W has a (unique) comodule structure $\rho_{V/W}$ for which $(V, \rho_V) \to (V/W, \rho_{V/W})$ is a homomorphism. In particular, the sub-comodules are exactly the kernels of homomorphism of comodules. The category of comodules over C is abelian and the forgetful functor to k-vector spaces is exact.

Now assume that k is a field. A bialgebra structure (m,e) on C defines a tensor product structure on the category of comodules over C: when (V_1,ρ_1) and (V_2,ρ_2) are C-comodules, $V_1 \otimes V_2$ has a natural structure of a $C \otimes C$-comodule (see 4.2b), and the homomorphism of coalgebras $m\colon C \otimes C \to C$ turns this into a C-comodule structure (see 4.2c). The tensor product of the empty family of comodules is the ***trivial comodule*** $(k, k \xrightarrow{e} C \simeq k \otimes C)$. The forgetful functor preserves tensor products.

Assume that V is finite dimensional. Under the canonical isomorphisms

$$\mathrm{Hom}_{k\text{-lin}}(V, V \otimes C) \simeq \mathrm{Hom}_{k\text{-lin}}(V \otimes V^{\vee}, C) \simeq \mathrm{Hom}_{k\text{-lin}}(V^{\vee}, C \otimes V^{\vee}), \qquad (74)$$

a right coaction ρ of C on V corresponds to left coaction ρ' of C on $V^{\vee}$. When C is a Hopf algebra, the inversion S can be used to turn ρ' into a right coaction $\rho^{\vee}$, namely, define $\rho^{\vee}$ to be the composite

$$V^{\vee} \xrightarrow{\rho'} A \otimes V^{\vee} \xrightarrow{t} V^{\vee} \otimes A \xrightarrow{V^{\vee} \otimes S} V^{\vee} \otimes A. \qquad (75)$$

The pair $(V^{\vee}, \rho^{\vee})$ is called the ***dual*** or ***contragredient*** of (V,ρ). The forgetful functor preserves duals.

SUMMARY 5.1 Let C be a coalgebra over a field k.

- ◇ The finite-dimensional comodules over C form an abelian category $\mathsf{Comod}(C)$; the forgetful functor to vector spaces is exact.
- ◇ A bialgebra structure on C provides $\mathsf{Comod}(C)$ with a tensor product structure; the forgetful functor preserves tensor products.
- ◇ A Hopf algebra structure on C provides $\mathsf{Comod}(C)$ with a tensor product structure and duals; the forgetful functor preserves duals.

6 Representations and comodules

A ***comodule over a bialgebra*** (A,m,e,Δ,ϵ) is defined to be a comodule over the coalgebra (A,Δ,ϵ).

PROPOSITION 6.1 *Let G be an affine monoid over k, and let V be a k-module. There is a natural one-to-one correspondence between the linear representations of G on V and the $\mathcal{O}(G)$-comodule structures on V.*

We give two independent proofs of the proposition. The first is very simple, but assumes that V is free and makes use of the choice of a basis.

Proof of Proposition 6.1 in the case that V is free

The choice of a basis $(e_i)_{i \in I}$ for V identifies End_V with a matrix algebra, and natural transformations $r\colon G \to \mathrm{End}_V$ with matrices $(r_{ij})_{(i,j) \in I \times I}$ of elements of $\mathcal{O}(G)$:

$$r_R(g) = \left(r_{ijR}(g)\right)_{i,j \in I}, \quad g \in G(R)$$

(recall that $\mathcal{O}(G) = \mathrm{Nat}(G, \mathbb{A}^1)$). Moreover, r is a homomorphism of affine monoids if and only if

$$\left(r_{ij}\right)_R(gg') = \textstyle\sum_{k \in I} \left(r_{ik}\right)_R(g) \cdot \left(r_{kj}\right)_R(g'), \quad \text{all } g, g' \in G(R), \quad i,j \in I, \qquad (76)$$

and $(r_{ij})_R(1) = \delta_{ij}$ $(i,j \in I)$. On the other hand, to give a k-linear map $\rho\colon V \to V \otimes \mathcal{O}(G)$ is the same as giving a matrix $(r_{ij})_{i,j\in I}$ of elements of $\mathcal{O}(G)$,

$$\rho(e_j) = \textstyle\sum_{i\in I} e_i \otimes r_{ij},$$

Moreover, ρ is a co-action if and only if

$$\Delta(r_{ij}) = \textstyle\sum_{k\in I} r_{ik} \otimes r_{kj}, \text{ all } i,j \in I, \tag{77}$$

and $\epsilon(r_{ij}) = \delta_{ij}$ $(i,j \in I)$. (see (72), p. 115). But

$$\Delta(r_{ij})_R(g,g') = \left(r_{ij}\right)_R(g\cdot g')$$

and

$$\left(\textstyle\sum_{k\in I} r_{ik} \otimes r_{kj}\right)_R(g,g') = \textstyle\sum_{k\in I} (r_{ik})_R(g)\cdot\left(r_{kj}\right)_R(g')$$

(see p. 47), and so r is a homomorphism if and only if ρ is a co-action. Therefore

$$r \leftrightarrow (r_{ij}) \leftrightarrow \rho$$

gives a one-to-one correspondence between the linear representations of G on V and the $\mathcal{O}(G)$-comodule structures on V.

SUMMARY 6.2 Let $V = k^n$ with its canonical basis $(e_i)_{i\in I}$; a matrix $(r_{ij})_{i,j\in I}$ of elements of $\mathcal{O}(G)$ satisfying

$$\left.\begin{array}{rcl} \Delta(r_{ij}) & = & \sum_{k\in I} r_{ik} \otimes r_{kj} \\ \epsilon(r_{ij}) & = & \delta_{ij} \end{array}\right\} \quad \text{all } i,j \in I,$$

defines a coaction of $\mathcal{O}(G)$ on V by

$$\rho(e_j) = \textstyle\sum_{i\in I} e_i \otimes r_{ij},$$

and a homomorphism $r\colon G \to \mathrm{GL}_n$ by

$$r(g) = (r_{ij}(g))_{i,j\in I},$$

such that r^* is the homomorphism $\mathcal{O}(\mathrm{GL}_n) \to \mathcal{O}(G)$ sending X_{ij} to r_{ij}.

Proof of Proposition 6.1 in general

We construct a *canonical* correspondence between the representations and the comodule structures. In Proposition 6.8 we show that, when a basis has been chosen, the correspondence becomes that described above.

Let $A = \mathcal{O}(G)$. We prove the following more precise result:

> Let $r\colon G \to \mathrm{End}_V$ be a representation; the "universal" element $a = \mathrm{id}_A$ in $G(A) \simeq \mathrm{Hom}_{k\text{-alg}}(A,A)$ maps to an element of $\mathrm{End}_V(A) \overset{\text{def}}{=} \mathrm{End}_{A\text{-lin}}(V(A))$ whose restriction to $V \subset V(A)$ is a comodule structure $\rho\colon V \to V \otimes A$ on V. Conversely, a comodule structure ρ on V determines a representation r such that, for R a k-algebra and $g \in G(R)$, the restriction of $r_R(g)\colon V(R) \to V(R)$ to $V \subset V(R)$ is
>
> $$V \xrightarrow{\rho} V \otimes A \xrightarrow{V\otimes g} V \otimes R.$$
>
> These operations are inverse.

Let V be a k-module, and let $r\colon G \to \mathrm{End}_V$ be a natural transformation of *set*-valued functors. Let $g \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$, and consider the diagram:

$$\begin{tikzcd}
V \arrow[r, "v\mapsto v\otimes 1"] \arrow[dr, "\rho \overset{\text{def}}{=} r_A(a)|V"'] & V\otimes A \arrow[r, "V\otimes g"] \arrow[d, "r_A(a)"] & V\otimes R \arrow[d, "r_R(g)"] \\
& V\otimes A \arrow[r, "V\otimes g"] & V\otimes R
\end{tikzcd}$$

The k-linear map ρ determines $r_R(g)$ because $r_A(a)$ is the unique A-linear extension of ρ to $V \otimes A$ and $r_R(g)$ is the unique R-linear map making the right hand square commute. Thus the map ρ determines the natural transformation r. Moreover, the diagram can be used to extend any k-linear map $\rho\colon V \to V \otimes A$ to a natural transformation r of set-valued functors, namely, for $g \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$ and define $r_R(g)$ to be the linear map $V(R) \to V(R)$ whose restriction to V is $(V \otimes g) \circ \rho$. Thus,

$$r_R(g)(v \otimes c) = (V \otimes g)(c\rho(v)), \quad \text{for all } g \in G(R),\ v \in V,\ c \in R. \tag{78}$$

In this way, we get a one-to-one correspondence $r \leftrightarrow \rho$ between natural transformations of set-valued functors r and k-linear maps ρ, and it remains to show that r is a representation of G if and only if ρ is a comodule structure on V.

Recall that the identity element $1_{G(k)}$ of $G(k)$ is $A \xrightarrow{\epsilon} k$. To say that $r_k(1_{G(k)}) = \mathrm{id}_{V\otimes k}$ means that the following diagram commutes,

$$\begin{tikzcd}
V \arrow[r, "v\mapsto v\otimes 1"'] \arrow[rr, bend left, "v\mapsto v\otimes 1"] \arrow[dr, "\rho"'] & V\otimes A \arrow[r, "V\otimes\epsilon"'] & V\otimes k \arrow[d, "V\otimes k"] \\
& V\otimes A \arrow[r, "V\otimes\epsilon"'] & V\otimes k
\end{tikzcd}$$

i.e., that the right hand diagram in (70) commutes.

Next consider the condition that $r_R(g) r_R(h) = r_R(gh)$ for $g, h \in G(R)$. By definition (see (10)), gh is the map

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{(g,h)} R,$$

and so $r_R(gh)$ acts on V as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{V\otimes\Delta} V \otimes A \otimes A \xrightarrow{V\otimes(g,h)} V \otimes R. \tag{79}$$

On the other hand, $r_R(g) r_R(h)$ acts as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{V\otimes h} V \otimes R \xrightarrow{\rho\otimes R} V \otimes A \otimes R \xrightarrow{V\otimes(g,\mathrm{id})} V \otimes R,$$

i.e., as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{\rho\otimes A} V \otimes A \otimes A \xrightarrow{V\otimes(g,h)} V \otimes R. \tag{80}$$

The maps (79) and (80) agree for all g, h if and only if the first diagram in (70) commutes.

Complements

EXAMPLE 6.3 Recall (4.2) that, for every k-bialgebra A, the map $\Delta\colon A \to A \otimes A$ is a comodule structure on A. When $A = \mathcal{O}(G)$, this comodule structure on A corresponds to the regular representation of G on $\mathcal{O}(G)$ (2.3).

EXAMPLE 6.4 Assume that k is a field, and let $\rho\colon V \to V \otimes \mathcal{O}(\mathbb{G}_a)$ be a finite-dimensional $\mathcal{O}(\mathbb{G}_a)$-comodule. The k-vector space $\mathcal{O}(\mathbb{G}_a) \simeq k[X]$ has basis $1, X, X^2, \ldots$ and so we can write

$$\rho(v) = \sum\nolimits_{i \geq 0} \rho_i(v) \otimes X^i, \quad v \in V.$$

As ρ is k-linear, so also is each map $v \mapsto \rho_i(v)$, and as the sum is finite, for each v, $\rho_i(v)$ is zero except for a finite number of i. As V is finite-dimensional, this means that only finitely many of the ρ_i are nonzero. It follows that the representations constructed in (2.1) form a complete set.

PROPOSITION 6.5 *Assume that k is a field. Let $r\colon G \to \mathrm{End}_V$ be the representation corresponding to a comodule (V, ρ). A subspace W of V is a subrepresentation if and only if it is a subcomodule.*

PROOF. Routine checking. □

PROPOSITION 6.6 *Assume that k is a field. Every representation of G is a union of its finite-dimensional subrepresentations.*

PROOF. In view of (6.1) and (6.5), this is simply a restatement of Proposition 4.5. □

ASIDE 6.7 Let G be a flat affine group over a ring k (i.e., $\mathcal{O}(G)$ is flat as a k-module), and let (V, r) be a representation of G. Let ρ be the corresponding $\mathcal{O}(G)$-comodule structure on V, and let W be a k-submodule of V. Because $\mathcal{O}(G)$ is flat, $W \otimes \mathcal{O}(G) \subset V \otimes \mathcal{O}(G)$, and $(W, \rho|W)$ is an $\mathcal{O}(G)$-comodule if $\rho(W) \subset W \otimes \mathcal{O}(G)$. When this is so, we call the corresponding representation $(W, r|W)$ of G a subrepresentation of (V, r). Therefore, when G is flat, there is a one-to-one correspondence between subrepresentations of (V, r) and subcomodules of (V, ρ). When k is noetherian and G is flat, every representation of G is a union of its finitely generated subrepresentations (4.7).

PROPOSITION 6.8 *Let $r\colon G \to \mathrm{End}_V$ be the representation corresponding to a comodule (V, ρ). Assume that V is a free k-module, and choose a basis $(e_i)_{i \in I}$ for V. Write*

$$\rho(e_j) = \sum\nolimits_i e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G). \tag{81}$$

Then, for each $g \in G(R)$,

$$r_R(g)(e_j \otimes 1) = \sum\nolimits_{i \in I} e_i \otimes g(a_{ij}) = \sum\nolimits_{i \in I} e_i \otimes a_{ijR}(g) \tag{82}$$

(equality in $V(R)$; recall that a_{ijR} is a map $G(R) \to R$ and that $r_R(g)$ is a map $V(R) \to V(R)$).

PROOF. According to (78),

$$\begin{aligned} r_R(g)(e_j \otimes 1) &= (\mathrm{id}_V \otimes g)(\rho(e_j)) \\ &= (\mathrm{id}_V \otimes g)(\textstyle\sum_i e_i \otimes a_{ij}) \\ &= \textstyle\sum_i e_i \otimes g(a_{ij}) \\ &= \textstyle\sum_i e_i \otimes a_{ijR}(g). \end{aligned}$$

In the last step, we used that $g(f) = f_R(g)$ for $f \in \mathcal{O}(G)$ and $g \in G(R)$ (see I, 3.13). □

COROLLARY 6.9 *Let (G, r) be the representation corresponding to a comodule (V, ρ). Assume that V is a free k-module, with basis $(e_i)_{i \in I}$. Then $\mathcal{O}(\mathrm{End}_V)$ is a polynomial ring in variables X_{ij} $(i, j \in I)$ where X_{ij} acts by sending an endomorphism of V to its (i, j)th matrix entry. The homomorphism $\mathcal{O}(\mathrm{End}_V) \to \mathcal{O}(G)$ defined by r sends X_{ij} to a_{ij} where a_{ij} is given by (81).*

PROOF. Restatement of the proposition. □

COROLLARY 6.10 *Let $r: G \to \mathrm{End}_V$ be the representation corresponding to a comodule (V, ρ). Let H be an affine subgroup of G, and let $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a}$. The following conditions on a vector $v \in V$ are equivalent:*

(a) *for all k-algebras R and all $g \in H(R)$, $r_R(g)(v_R) = v_R$;*
(b) $\rho(v) \equiv v \otimes 1 \mod V \otimes \mathfrak{a}$.

PROOF. We may suppose that $v \neq 0$, and so is part of a basis $(e_i)_{i \in I}$ for V, say $v = e_j$. Let $(a_{ij})_{i,j \in I}$ be as in (81); then (b) holds for e_j if and only if $a_{ij} - \delta_{ij} \in \mathfrak{a}$ for all i. On the other hand, (82) shows that (a) holds for e_j if and only if the same condition holds on (a_{ij}). □

We say that $v \in V$ is ***fixed*** by H if it satisfies the equivalent conditions of the corollary, and we let V^H denote the subspace of fixed vectors in V. If $H(k)$ is dense in H, then $v \in V^H$ if and only if $r(g)v = v$ for all $g \in H(k)$ (because there is a largest subgroup of G fixing v).

LEMMA 6.11 *Let G, r, V, ρ, and H be as in the corollary, and let R be a k-algebra. The following submodules of $V(R)$ are equal:*

(a) $V^H \otimes R$;
(b) $\{v \in V(R) \mid r_{R'}(g)(v_{R'}) = v_{R'}$ *for all R-algebras R' and* $g \in H(R')\}$;
(c) $\{v \in V(R) \mid \rho(v) \equiv v \otimes 1 \mod V \otimes \mathfrak{a} \otimes R\}$.

PROOF. Nothing in this section requires that k be a field (provided one assumes V to be free). Therefore the equality of the sets in (b) and (c) follows by taking $k = R$ in Corollary 6.10. The condition

$$\rho(v) \equiv v \otimes 1 \mod V \otimes \mathfrak{a}$$

is linear in v, and so if W is the solution space over k, then $W \otimes_k R$ is the solution space over R. This proves the equality of the sets in (a) and (c). □

!Need to fix this. In 6.10 we assume that v is part of a basis.!

For the remainder of this chapter, k is a field.

7 The category of representations of G

Let G be an affine monoid over a field k, and let $\mathsf{Rep}(G)$ be the category of representations of G on finite-dimensional k-vector spaces. As this is essentially the same as the category of finite-dimensional $\mathcal{O}(G)$-comodules (see 6.1), it is an abelian category and the forgetful functor to k-vector spaces is exact and faithful.

The ***tensor product*** of two representations (V,r) and (V',r') is defined to be $(V\otimes V,r\otimes r')$ where $(r\otimes r')_R(g)=r_R(g)\otimes r'_R(g)$.

When G is a group, the ***contragredient*** (or ***dual***) of a representation (V,r) is defined to be $(V^\vee,r^\vee)$ where,

$$\left(r_R^\vee(g)(f)\right)(v)=f(r_R(g^{-1})v),\quad g\in G(R),\quad f\in V^\vee(R),\quad v\in V(R)$$

(more succinctly, $(gf)(v)=f(g^{-1}v)$).

PROPOSITION 7.1 *Let (V,r) and (V',r') be representations of G, and let ρ and ρ' be the corresponding comodule structures on V and V'. The comodule structures on $V\otimes V'$ and $V^\vee$ defined by $r\otimes r'$ and $r^\vee$ are those described in §5.*

PROOF. Easy exercise for the reader. □

8 Affine groups are inverse limits of algebraic groups

It is convenient at this point to prove the following theorem.

THEOREM 8.1 *Every affine monoid (resp. group) over a field is an inverse limit of its algebraic quotients.*

In particular, every affine monoid (resp. group) is an inverse limit of algebraic monoids (resp. groups) in which the transition maps are quotient maps.

We prove Theorem 8.1 in the following equivalent form (recall that a k-bialgebra is said to be finitely generated if it is finitely generated as k-algebra, II, 4.3).

THEOREM 8.2 *Every bialgebra (resp. Hopf algebra) over field k is a directed union of its finitely generated sub-bialgebras (resp. Hopf subalgebras) over k.*

PROOF. Let A be a k-bialgebra. By (4.5), every finite subset of A is contained in a finite-dimensional k-subspace V such that $\Delta(V)\subset V\otimes A$. Let (e_i) be a basis for V, and write $\Delta(e_j)=\sum_i e_i\otimes a_{ij}$. Then $\Delta(a_{ij})=\sum_k a_{ik}\otimes a_{kj}$ (see (72), p. 115), and the subspace L of A spanned by the e_i and a_{ij} satisfies $\Delta(L)\subset L\otimes L$. The k-subalgebra A' generated by L satisfies $\Delta(A')\subset A'\otimes A'$, and so it is a finitely generated sub-bialgebra of A. It follows that A is the directed union $A=\bigcup A'$ of its finitely generated sub-bialgebras.

Suppose that A has an inversion S. If $\Delta(a)=\sum b_i\otimes c_i$, then $\Delta(Sa)=\sum Sc_i\otimes Sb_i$ (Exercise II-3b). Therefore, the k-subalgebra A' generated by L and SL satisfies $S(A')\subset A'$, and so it is a finitely generated Hopf subalgebra of A. It follows that A is the directed union of its finitely generated Hopf subalgebras. □

COROLLARY 8.3 *Let B be a Hopf algebra over a field, and let A be a Hopf subalgebra of B. Then A and B are directed unions of finitely generated Hopf subalgebras A_i and B_i such that $A_i\subset B_i$.*

PROOF. Since each finitely generated Hopf subalgebra of A is contained in a finitely generated Hopf subalgebra of B, this follows easily from the theorem. □

COROLLARY 8.4 *Let A be a Hopf algebra over a field k. If A is an integral domain and its field of fractions is finitely generated (as a field) over k, then A is finitely generated.*

PROOF. Any finite subset S of A is contained in a finitely generated Hopf subalgebra A' of A. When S is chosen to generate the field of fractions of A, then A' and A have the same field of fractions, and so they are equal (VI, 11.2). □

COROLLARY 8.5 *A Hopf algebra over a field whose augmentation ideal is finitely generated is itself finitely generated.*

PROOF. Let A be a Hopf algebra. If I_A is finitely generated, then there exists a finitely generated Hopf subalgebra A' of A containing a set of generators for I_A. The inclusion $A' \to A$ corresponds to a quotient map $G \to G'$ whose kernel has Hopf algebra $A \otimes_{A'} A'/I_{A'} \simeq A/I_{A'}A = A/I_A \simeq k$. Proposition VII, 1.1 shows that $G \simeq G'$, and so $A' \simeq A$.□

PROPOSITION 8.6 *Every quotient of an algebraic group over a field is itself an algebraic group.*

PROOF. We have to show that a Hopf subalgebra A of a finitely generated Hopf algebra B is finitely generated. Because B is noetherian, the ideal $I_A B$ is finitely generated, and because B is flat over A, the map $I_A \otimes_A B \to A \otimes_A B \simeq B$ is an isomorphism of $I_A \otimes_A B$ onto $I_A B$. Therefore $I_A \otimes B$ is a finitely generated as a B-module, and as B is faithfully flat over A, this implies that I_A is finitely generated.[4] □

ASIDE 8.7 Proposition 8.6 *does* require proof, because subalgebras of finitely generated k-algebras need not be finitely generated, even when k is a field. For example, the subalgebra $k[X, XY, XY^2, \ldots]$ of $k[X,Y]$ is not even noetherian. There are even subfields K of $k(X_1, \ldots, X_n)$ containing k such that $K \cap k[X_1, \ldots, X_n]$ is not finitely generated as a k-algebra (counterexamples to Hilbert's fourteenth problem; Nagata and others).

ASIDE 8.8 An affine group is said to be ***separable*** if it is an inverse limit of a *countable* collection of algebraic quotients. This is a useful class of affine groups: countable inverse limits are easier to work with than general inverse limits, and most naturally occurring affine groups are separable.

ASIDE 8.9 Theorem 8.1 is also true for nonaffine group schemes: every quasicompact group scheme over a field k is a filtered inverse limit of group schemes of finite type over k (Perrin 1976).

[4] As a B-module, $I_A \otimes_A B$ has a finite set of generators $\{c_1 \otimes b_1, \ldots, c_m \otimes b_m\}$, and the map

$$(a_1, \ldots, a_m) \mapsto \Sigma a_i c_i : A^m \to I_A$$

is surjective because it becomes surjective when tensored with B.

9 Algebraic groups admit finite-dimensional faithful representations

It is obvious that the regular representation (over any ring) is faithful: let $g \in G(R)$ and suppose that $r_A(g) = 1$; then $f_{R'}(x) = f_{R'}(xg)$ for all R-algebras R' and all $x \in G(R')$, which implies that $g = 1$.

We now assume that k is a field, and prove that every sufficiently large finite-dimensional subrepresentation of the regular representation will be faithful.

THEOREM 9.1 *For any algebraic group G, the regular representation of G has faithful finite-dimensional subrepresentations; in particular, the regular representation itself is faithful.*

PROOF. Let $A = \mathcal{O}(G)$, and let V be a finite-dimensional subcomodule of A containing a set of generators for A as a k-algebra. Let $(e_i)_{1 \le i \le n}$ be a basis for V, and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. According to (6.9), the image of $\mathcal{O}(\mathrm{GL}_V) \to A$ contains the a_{ij}. But, because $\epsilon\colon A \to k$ is a co-identity (see (15), p. 30),

$$e_j = (\epsilon \otimes \mathrm{id}_A)\Delta(e_j) = \sum_i \epsilon(e_i) a_{ij},$$

and so the image contains V; it therefore equals A. We have shown that $\mathcal{O}(\mathrm{GL}_V) \to A$ is surjective, which means that $G \to \mathrm{GL}_V$ is injective (VII, 2.1). [Variant: $A_V \supset V$ (see 4.3c), and so $A_V = A$; this implies that the representation on V is faithful.] □

COROLLARY 9.2 *Every affine group admits a faithful family of finite-dimensional representations.*

PROOF. Write G as an inverse limit $G = \varprojlim_{i \in I} G_i$ of algebraic groups, and, for each $i \in I$, choose a faithful finite-dimensional representation (V_i, r_i) of G_i. Each (V_i, r_i) can be regarded as a representation of G, and the family is faithful. □

The theorem says that every algebraic group can be realized as an algebraic subgroup of GL_n for some n. This does *not* mean that we should consider only subgroups of GL_n because realizing an algebraic group in this way involves many choices.

PROPOSITION 9.3 *Let (V, r) be a faithful representation of an algebraic group G. Then V is a union of its finite-dimensional faithful subrepresentations.*

PROOF. Let $(e_i)_{i \in I}$ be a basis for V, and write $\rho(e_j) = \sum_{i \in I} e_i \otimes a_{ij}$, $a_{ij} \in A$. Because (V, r) is faithful, the k-algebra A is generated by the a_{ij} (6.9). Because A is finitely generated as a k-algebra, only finitely many a_{ij}'s are need to generate it, and so there exists a finite subset J of I such that the a_{ij}'s appearing in $\rho(e_j)$ for some $j \in J$ generate A. Every finite-dimensional subrepresentation of (V, r) containing $\{e_j \mid j \in J\}$ is faithful. □

ASIDE 9.4 Does every flat affine group of finite type over a ring admit an injective homomorphism into GL_n for some n? Apparently, this is not known even when k is the ring of dual numbers over a field and G is smooth (mo22078, Brian Conrad). Using (4.7), one sees by the above arguments that a flat affine group scheme G of finite type over a noetherian ring k has a faithful representation on a finitely generated submodule M of the regular representation. If M is flat over k, then it is projective, and hence a direct summand of a free finitely generated k-module L, and so $G \hookrightarrow \mathrm{GL}_{\mathrm{rank}(L)}$. When k is a Dedekind domain and G is flat, the module M is torsion-free, and hence automatically flat. Thus, every flat affine group scheme of finite type over a Dedekind domain admits an embedding into GL_n for some n. As every split reductive group scheme over a ring k arises by base change from a similar group over $\mathbb{Z}$ (Chevalley), such group schemes admit embeddings into GL_n. Since every reductive group splits over a finite étale extension of the base ring (SGA 3), an argument using restriction of scalars proves the statement for every reductive group (mo22078).

10 The regular representation contains all

Let (V, r_V) be a representation of G. For $v \in V(R)$ and $u \in V^\vee(R)$, let $\langle u, v\rangle = u(v) \in R$. For a fixed $v \in V$ and $u \in V^\vee$, the maps

$$x \mapsto \langle u, r_V(x)v\rangle \colon G(R) \to R$$

are natural in R, and so define an element of $\mathcal{O}(G)$, i.e., there exists a $\phi_u(v) \in \mathcal{O}(G)$ such that

$$\phi_u(v)_R(x) = \langle u, r_V(x)v\rangle \text{ (in } R\text{) for all } x \in G(R).$$

Let $A = \mathcal{O}(G)$, and let r_A be the regular representation of G on A.

PROPOSITION 10.1 *The map ϕ_u is a homomorphism of representations $(V, r_V) \to (A, r_A)$.*

PROOF. We have to show that

$$(\phi_u)_R \circ r_V(g) = r_A(g) \circ (\phi_u)_R$$

for all k-algebras R and all $g \in G(R)$. For any $v \in V(R)$ and $x \in G(R)$,

$$\begin{aligned}
(\mathrm{LHS}(v))(x) &= \phi_u(r_V(g)v)_R(x) \\
&= \langle u, r_V(x) r_V(g) v\rangle && \text{(definition of } \phi_u\text{)} \\
&= \langle u, r_V(xg)v\rangle && (r_V \text{ is a homomorphism}) \\
&= \phi_u(v)_R(xg) && \text{(definition of } \phi_u\text{)} \\
&= (r_A(g)\phi_u(v))_R(x) && \text{((68), p. 113)} \\
&= (\mathrm{RHS}(v))(x),
\end{aligned}$$

as required. □

PROPOSITION 10.2 *If $u_1, \ldots, u_n$ span $V^\vee$, then the k-linear map*

$$v \mapsto (\phi_{u_1}(v), \ldots, \phi_{u_n}(v)) \colon V \to A^n \tag{83}$$

is injective.

PROOF. Note that $\phi_u(v)(1) = \langle u, v\rangle$, and so the composite

$$V(R) \to A^n(R) \to R^n$$

of (83) with the map "evaluate at 1" is

$$v \mapsto (\langle u_1, v\rangle, \ldots, \langle u_n, v\rangle),$$

which is injective by our choice of the u_i's. □

Thus, V embeds into a finite sum of copies of the regular representation. We give a second proof of this.

PROPOSITION 10.3 *Assume that G is a flat affine group over a ring k, and let (V,ρ) be a representation of G. Let V_0 denote V regarded as a k-module, and let $V_0 \otimes \mathcal{O}(G)$ be the free comodule on V_0 (see 4.2). Then*

$$\rho\colon V \to V_0 \otimes \mathcal{O}(G)$$

is an injective homomorphism of representations.

PROOF. The coaction on $V_0 \otimes \mathcal{O}(G)$ is

$$V_0 \otimes \Delta\colon V_0 \otimes \mathcal{O}(G) \to V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G).$$

The commutative diagram (see (70), p. 114)

$$\begin{tikzcd}
V \arrow[r, "\rho"] \arrow[d, "\rho"] & V_0 \otimes \mathcal{O}(G) \arrow[d, "V_0 \otimes \Delta"] \\
V \otimes \mathcal{O}(G) \arrow[r, "\rho \otimes \mathcal{O}(G)"] & V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)
\end{tikzcd}$$

says exactly that the map $\rho\colon V \to V_0 \otimes \mathcal{O}(G)$ is a homomorphism of comodules. It is injective because its composite with $\mathrm{id}_V \otimes \epsilon$ is injective (VIII, 4.1). □

11 Every faithful representation generates $\mathsf{Rep}(G)$

Let (C,Δ,ϵ) be a coalgebra over k, and let (V,ρ) be a comodule over C. Recall (4.3) that C_V denotes the smallest subspace of C such that $\rho(V) \subset V \otimes C_V$. The space C_V is a sub-coalgebra of C, and, for any basis $(e_i)_{i\in I}$ of V, it is spanned by the elements c_{ij} determined by the equation

$$\rho(e_j) = \sum\nolimits_{i\in I} e_i \otimes c_{ij}.$$

Note that

$$C_{\oplus V_i} = \sum\nolimits_i C_{V_i} \quad \text{(sum of subspaces of } C\text{)}.$$

Any C_V-comodule (W,ρ_W) can be regarded as a C-comodule with the coaction

$$W \xrightarrow{\rho_W} W \otimes C_V \subset W \otimes C.$$

LEMMA 11.1 *Let (V,ρ) be a finite-dimensional C-comodule. Every finite-dimensional C_V-comodule (considered as a C-comodule) is isomorphic to a quotient of a sub-comodule of V^n for some n.*

PROOF. We may replace C with C_V, and so assume that C is finite dimensional. Let $A = C^\vee$. Because of the correspondence between right C-comodule structures and left A-module structures (4.4), it suffices to prove the following statement:

> let A be a finite k-algebra and let V be a finite-dimensional faithful left A-module; then every finite-dimensional A-module W is isomorphic to a quotient of a submodule of V^n for some n.

Every module W is isomorphic to a quotient of the free module A^m for some m, and so it suffices to prove that A itself is isomorphic to a submodule of V^n for some n. But if $e_1,\ldots,e_n$ span V as a k-vector space, then $a \mapsto (ae_1,\ldots,ae_n)\colon A \to V^n$ is injective because V is faithful. □

Now assume that A is a bialgebra over k. Then the tensor product of two A-comodules has a natural A-comodule structure (§5).

LEMMA 11.2 *Let A be a bialgebra over k, and let V and V' be finite-dimensional A-comodules. Then $A_{V\otimes V'} = A_V \cdot A_{V'}$.*

PROOF. Choose k-bases $(e_i)_{i\in I}$ and $(e_i')_{i\in I'}$ for V and V', and write

$$\rho_V(e_j) = \sum_{i\in I} e_i \otimes a_{ij}, \quad \rho_{V'}(e_j') = \sum_{i\in I'} e_i' \otimes a_{ij}'.$$

Then $(e_i \otimes e_{i'})_{(i,i')\in I\otimes I'}$ is a basis for $V \otimes_k V'$, and

$$\rho_{V\otimes V'}(e_j \otimes e_{j'}) = \textstyle\sum_{i,i'} (e_i \otimes e_{i'}) \otimes (a_{ij} \cdot a_{i'j'}')$$

(see §5). As

$$\begin{aligned} A_V &= \langle a_{ij} \mid i,j \in I\rangle \\ A_{V'} &= \langle a_{ij} \mid i,j \in I'\rangle \\ A_{V\otimes V'} &= \langle a_{ij} \cdot a_{i'j'}' \mid i,j \in I, \quad i',j' \in I'\rangle, \end{aligned}$$

the statement is clear. (Alternatively, note that $A_V \otimes A_{V'}$ is the sub-coalgebra attached to the $A\otimes A$-comodule $V \otimes V'$, and that $A_{V\otimes V'}$ is the image of this by the multiplication map $m\colon A\otimes A \to A$.) □

Now assume that A is a Hopf algebra over k. Then the dual of an A-comodule has a natural A-comodule structure (§5).

LEMMA 11.3 *Let A be a Hopf algebra over k, and let $S\colon A \to A$ be its inversion. For any finite-dimensional A-comodule (V,ρ), $A_{V^\vee} = SA_V$.*

PROOF. Under the isomorphisms (74), the right co-action $\rho\colon V \to V\otimes A$ corresponds to a left co-action $\rho'\colon V^\vee \to A\otimes V^\vee$, and A_V is also the smallest subspace of A such that $\rho'(V^\vee) \subset A_V \otimes V^\vee$. It follows from the definition of $\rho^\vee$ (see (75)) that SA_V is the smallest subspace of A such that $\rho^\vee(V^\vee) \subset V^\vee \otimes A$. □

LEMMA 11.4 *Let V be a finite-dimensional comodule over a k-bialgebra A. Then*

$$A(V) \overset{\text{def}}{=} \textstyle\sum_{n\geq 0} A_{V^{\otimes n}} \subset A$$

is the smallest sub-bialgebra of A containing A_V and 1.

PROOF. It follows from Lemma 11.2 that

$$A_{V^{\otimes n}} = A_V \cdots A_V \quad (n \text{ factors}),$$

and so it is clear that $A(V)$ is the subalgebra of A generated by A_V and 1. □

Note that $A = \bigcup_V A(V)$ because $A = \bigcup_V A_V$ (see 4.6).

LEMMA 11.5 *Let V be a finite-dimensional comodule over a Hopf k-algebra A. Then $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing A_V and 1 and stable under S (in other words, it is the smallest Hopf subalgebra of A containing A_V and 1).*

PROOF. From Lemma 11.4, $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing $A_{V \oplus V^\vee}$ and 1. But

$$A_{V \oplus V^\vee} = A_V + A_{V^\vee} \overset{11.3}{=} A_V + SA_V,$$

and so it is the smallest sub-bialgebra of A containing A_V, SA_V, and 1. □

Let G be an algebraic group over k, and let $A = \mathcal{O}(G)$.

LEMMA 11.6 *Let (V, r) be a finite-dimensional representation of G, and let (V, ρ) be the corresponding A-comodule. The representation r is faithful if and only if $A(V \oplus V^\vee) = A$.*

PROOF. Choose a basis $(e_i)_{i \in I}$ for V, and write $\rho(e_j) = \sum e_i \otimes a_{ij}$. Then $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing the a_{ij} and 1 and stable under S (by 11.5). On the other hand, the image of $\mathcal{O}(\mathrm{GL}_V) \to \mathcal{O}(G) = A$ is the k-subalgebra generated by the a_{ij} (6.9). As this image is a sub-bialgebra stable under S, we see that $\mathcal{O}(\mathrm{GL}_V) \to \mathcal{O}(G)$ is surjective (so r is faithful) if and only if $A(V \oplus V^\vee) = A$. □

THEOREM 11.7 *Let $G \to \mathrm{GL}_V$ be a representation of G. If V is faithful, then every finite-dimensional representation of G is isomorphic to a quotient of a sub-representation of a direct sum of representations $\bigotimes^n (V \oplus V^\vee)$.*

PROOF. Let W be the direct sum of the representations $\bigotimes^n (V \oplus V^\vee)$. By definition, $A(V \oplus V^\vee) = A_W$. According to Lemma 11.1, every finite-dimensional A_W-comodule is isomorphic to a quotient of a sub-comodule of W. When V is faithful, $A_W = A$. □

COROLLARY 11.8 *Every simple G-module is a Jordan-Hölder quotient of $\bigotimes^n (V \oplus V^\vee)$ for some n.*

PROOF. Immediate consequence of the theorem. □

We close this section with some remarks.

11.9 When M is an affine monoid with coordinate ring $\mathcal{O}(M) = A$, we let M_V denote the quotient affine monoid of M with coordinate ring $A(V)$. Similarly, when G is an affine group, we let G_V denote the quotient affine group of G with coordinate ring $A(V \oplus V^\vee)$. Both M_V and G_V act faithfully on V. Moreover,

$$M = \varprojlim M_V, \quad G = \varprojlim G_V$$

because $A = \bigcup A(V)$.

11.10 Let (V,ρ) be a finite-dimensional comodule over a Hopf k-algebra A. Choose a basis $(e_i)_{i\in I}$ for V and define the matrix (a_{ij}) by $\rho(e_j)=\sum_{i\in I} e_i\otimes a_{ij}$. Let $\delta_V=\det(a_{ij})$. Then δ_V is an invertible element of A, contained in $A(V)$, and

$$A(V\oplus V^{\vee})=A(V)\left[\frac{1}{\delta_V}\right].$$

11.11 The quotient M_V of M is the smallest affine submonoid of End_V containing the image of r, and the quotient G_V of G is the smallest affine subgroup of GL_V containing the image of r.

11.12 Let $\det(V)=\bigwedge^{\dim V} V$. Then every simple G-module is a Jordan-Hölder quotient of $\bigotimes^n V\otimes\bigotimes^m \det(V)^{\vee}$ for some m,n.

11.13 It sometimes happens that $\mathcal{O}(G_V)$ is a quotient of $\mathcal{O}(\mathrm{End}_V)$ (and not just of $\mathcal{O}(\mathrm{GL}_V)$), i.e., that $A(V)=A(V\oplus V^{\vee})$. This is the case, for example, if G_V is contained in SL_V. In this case, Theorem 11.7 and its corollary simplify: the tensor powers of $V\oplus V^{\vee}$ can be replaced by those of V.

ASIDE 11.14 Our exposition of Theorem 11.7 follows Serre 1993.

12 Stabilizers of subspaces

PROPOSITION 12.1 *Let $G\to\mathrm{GL}_V$ be a representation of G, and let W be a subspace of V. The functor*

$$R\rightsquigarrow\{g\in G(R)\mid gW_R=W_R\}$$

*is a subgroup of G (denoted G_W, and called the **stabilizer** of W in G).*

PROOF. Let $(e_i)_{i\in J}$ be a basis for W, and extend it to a basis $(e_i)_{J\sqcup I}$ for V. Write

$$\rho(e_j)=\textstyle\sum_{i\in J\sqcup I} e_i\otimes a_{ij},\quad a_{ij}\in\mathcal{O}(G).$$

Let $g\in G(R)=\mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(G),R)$. Then (see 6.8)

$$ge_j=\textstyle\sum_{i\in J\sqcup I} e_i\otimes g(a_{ij}).$$

Thus, $g(W\otimes R)\subset W\otimes R$ if and only if $g(a_{ij})=0$ for $j\in J$, $i\in I$. As $g(a_{ij})=(a_{ij})_R(g)$ (see I, 3.13), this shows that the functor is represented by the quotient of $\mathcal{O}(G)$ by the ideal generated by $\{a_{ij}\mid j\in J, i\in I\}$. □

ASIDE 12.2 Let k be a ring (not necessarily a field). Let $G\times V\to V$ be a linear action of an affine k-group G on a k-module V, and let W be a submodule of V. By definition, the functor

$$G_W=T_G(W,W).$$

If W is projective and finitely generated, then $\mathrm{Sym}(W)$ is a locally free k-module, and so G_W is represented by a quotient of $\mathcal{O}(G)$ (see V, 6.9).

We say that an affine subgroup H of G ***stabilizes*** W if $H\subset G_W$, i.e., if $hW_R=W_R$ for all k-algebras R and $h\in H(R)$.

COROLLARY 12.3 *Let H be an algebraic subgroup of G such that $H(k)$ is dense in H. If $hW = W$ for all $h \in H(k)$, then H stabilizes W.*

PROOF. As $hW = W$ for all $h \in H(k)$, we have $(H \cap G_W)(k) = H(k)$, and so $H \cap G_W = H$. □

PROPOSITION 12.4 *Let G act on V and V', and let W and W' be nonzero subspaces of V and V'. Then the stabilizer of $W \otimes W'$ in $V \otimes V'$ is $G_W \cap G_{W'}$.*

PROOF. Clearly $G_W \cap G_{W'} \subset G_{W \otimes W'}$. Conversely, if g is an element of $G(R)$ not in $G_W(R)$, then there exists a nonzero $w \in W$ such that $gw \notin W_R$. For any nonzero element w' of W', the element $g(w \otimes w') = gw \otimes gw'$ of $V_R \otimes V'_R$ is not in $W_R \otimes W'_R$,[5] and so $g \notin G_{W \otimes W'}(R)$. □

PROPOSITION 12.5 *Let $G \to \mathrm{GL}_V$ be a representation of G, and let $v \in V$. The functor*

$$R \rightsquigarrow G_v(R) \overset{\text{def}}{=} \{g \in G(R) \mid g(v \otimes 1) = v \otimes 1 \text{ (in } V_R\text{)}\}$$

is a subgroup of G (denoted G_v, and called the ***isotropy*** *or* ***stability group*** *of v in G).*

PROOF. If $v = 0$, then $G_v = G$ and there is nothing to prove. Otherwise, choose a basis $(e_i)_{i \in I}$ for V with $e_{i_0} = v$ for some $i_0 \in I$. Write

$$\rho(e_j) = \textstyle\sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

An element $g \in G(R)$ fixes $v \otimes 1$ if and only if

$$g(a_{ii_0}) = \begin{cases} 1 & \text{if} \quad i = i_0 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore G_v is represented by the quotient of $\mathcal{O}(G)$ by the ideal generated by $\{a_{ii_0} - \delta_{ii_0} \mid i \in I\}$. □

DEFINITION 12.6 For a representation $r\colon G \to \mathrm{GL}_V$ of G,

$$V^G = \{v \in V \mid gv = v \text{ (in } V_R\text{) for all } k\text{-algebras } R \text{ and } g \in G(R)\}.$$

It is the largest subspace of V on which the action of G is trivial. If ρ denotes the corresponding coaction, then

$$V^G = \{v \in V \mid \rho(v) = v \otimes 1\}.$$

[5] Let e and e' be nonzero elements of V and V'; if $e \otimes e' \in W_R \otimes W'_R$ for some k-algebra R, then $e \in W$ and $e' \in W'$. To see this, write $V = W \oplus W_1$, so that

$$V \otimes V' = W \otimes V' \oplus W_1 \otimes V'.$$

Let $e = e_0 + e_1$ with $e_0 \in W$ and $e_1 \in W_1$. If $e_1 \neq 0$, then $e_1 \otimes e' \neq 0$ in $W_1 \otimes V' \subset (W_1 \otimes V')_R$, and so $e \otimes e' \notin (W \otimes V')_R$.

13 Chevalley's theorem

THEOREM 13.1 (CHEVALLEY) *Every subgroup of an algebraic group G is the stabilizer of a one-dimensional subspace in a finite-dimensional representation of G.*

PROOF. Let H be a subgroup of G, and let $\mathfrak{a}$ be the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$. According to (4.5), there exists a finite-dimensional k-subspace V of $\mathcal{O}(G)$ containing a generating set of $\mathfrak{a}$ as an ideal and such that

$$\Delta(V) \subset V \otimes \mathcal{O}(G).$$

Let $W = \mathfrak{a} \cap V$ in V. Let $(e_i)_{i \in J}$ be a basis for W, and extend it to a basis $(e_i)_{J \sqcup I}$ for V. Let

$$\Delta e_j = \textstyle\sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

As in the proof of 12.1, G_W is represented by the quotient of $\mathcal{O}(G)$ by the ideal $\mathfrak{a}'$ generated by $\{a_{ij} \mid j \in J, i \in I\}$. Because $\mathcal{O}(G) \to \mathcal{O}(H)$ is a homomorphism of coalgebras[6]

$$\begin{aligned}&\Delta(\mathfrak{a}) \subset \mathrm{Ker}(\mathcal{O}(G) \otimes \mathcal{O}(G) \to \mathcal{O}(H) \otimes \mathcal{O}(H)) = \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G),\\ &\epsilon(\mathfrak{a}) = 0.\end{aligned}$$

The first of these applied to e_j, $j \in J$, shows that $\mathfrak{a}' \subset \mathfrak{a}$, and the second shows that

$$e_j = (\epsilon, \mathrm{id})\Delta(e_j) = \textstyle\sum_{i \in I} \epsilon(e_i) a_{ij}.$$

As the e_j, $j \in J$, generate $\mathfrak{a}$ (as an ideal), so do the a_{ij}, $j \in J$, and so $\mathfrak{a}' = \mathfrak{a}$. Thus $H = G_W$. The next (elementary) lemma shows that W can be taken to be one-dimensional. □

LEMMA 13.2 *Let W be a finite-dimensional subspace of a vector space V, and let $D = D = \bigwedge^{\dim W} W \subset \bigwedge^{\dim W} V$. Let u be an automorphism of V_R for some k-algebra R. Then $uW_R = W_R$ if and only if $uD_R = D_R$.*

PROOF. Let $(e_j)_{j \in J}$ be a basis for W, and extend it to a basis $(e_i)_{J \sqcup I}$ of V. Let $w = \bigwedge_{j \in J} e_j$. For any k-algebra R,

$$W_R = \{v \in V_R \mid v \wedge w = 0 \text{ (in } \textstyle\bigwedge^{d+1} V_R)\}.$$

To see this, let $v \in V_R$ and write $v = \sum_{i \in J \sqcup I} a_i e_i$, $a_i \in R$. Then

$$v \wedge w = \textstyle\sum_{i \in I} a_i e_1 \wedge \cdots \wedge e_d \wedge e_i.$$

As the elements $e_1 \wedge \cdots \wedge e_d \wedge e_i$, $i \in I$, are linearly independent in $\bigwedge^{d+1} V$, we see that

$$v \wedge w = 0 \iff a_i = 0 \text{ for all } i \in I.$$

Let $u \in \mathrm{GL}(V_R)$. If $uW_R = W_R$, then obviously $(\bigwedge^d u)(D_R) = D_R$. Conversely, suppose that $(\bigwedge^d u)(D_R) = D_R$, so that $(\bigwedge^d u)w = cw$ for some $c \in R^\times$. When $v \in W_R$, $v \wedge w = 0$, and so

$$0 = (\textstyle\bigwedge^{d+1} u)(v \wedge w) = uv \wedge (\bigwedge^d u)w = c\,((uv) \wedge w),$$

which implies that $uv \in W_R$. □

[6] We use the following elementary fact: for any subspace W of a vector space V, the kernel of $V \otimes V \to V/W \otimes V/W$ is $V \otimes W + W \otimes V$. To prove this, write $V = W \oplus W'$.

COROLLARY 13.3 *A subgroup H of an algebraic group G is the subgroup of G fixing a vector in some finite-dimensional representation of G in each of the following two cases:*

(a) *all the representations of H are semisimple;*
(b) *a nonzero multiple of each character of H defined over k extends to a similar character of G.*

PROOF. According to Chevalley's theorem, H is the stabilizer of a line D in a finite-dimensional representation V of G. Let $D^\vee$ be the dual of D with H acting contragrediently. If we can find a representation V' of G containing $D^\vee$ as an H-stable subspace, then H will be the subgroup of G fixing any nonzero vector in $D \otimes D^\vee \subset V \otimes V'$.[7]

Certainly $D^\vee$ occurs as a quotient of $V^\vee$, and so, in case (a), it also occurs as a direct summand of $V^\vee$ (regarded as an H-module). In this case, we can take $V' = V^\vee$.

The action of H on D defines a character of H, which in case (b) extends to a character of G. In this case, we can take $V' = D^\vee$. □

14 Sub-coalgebras and subcategories

Let C be a coalgebra over k. As before, $\mathsf{Comod}(C)$ denotes the category of finite-dimensional right C-comodules. Let D be a sub-coalgebra of C. Any D-comodule (V,ρ) becomes a C-comodule with the coaction

$$V \xrightarrow{\rho} V \otimes D \subset V \otimes C.$$

In this way, we get an exact fully faithful functor $\mathsf{Comod}(D) \to \mathsf{Comod}(C)$. We let $D^\vee$ denote the full subcategory of $\mathsf{Comod}(C)$ whose objects are isomorphic to a comodule in the image of this functor.

DEFINITION 14.1 A full subcategory of an abelian category is ***replete*** if it is closed under the formation of finite direct sums, subobjects, and quotient objects.

In particular, every object isomorphic to an object in a replete subcategory also lies in the subcategory. A replete subcategory is an abelian category, and the inclusion functor is exact.

THEOREM 14.2 *The map $D \mapsto D^\vee$ is a bijection from the set of sub-coalgebras of C onto the set of replete subcategories of $\mathsf{Comod}(C)$.*

PROOF. It is obvious that $D^\vee$ is replete. Let S be a replete subcategory of $\mathsf{Comod}(C)$, and let

$$C(\mathsf{S}) = \sum\nolimits_{V \in \mathsf{S}} C_V \quad \text{(sub-coalgebra of } C\text{)}.$$

To prove the theorem, we have to show that:

◇ $C(D^\vee) = D$ for all sub-coalgebras D of C, and

[7] Let v be a nonzero vector in D. Then

$$H \subset G_{v \otimes v^\vee} \subset G_{D \otimes D^\vee} = G_D \cap G_{D^\vee} = G_D = H.$$

◇ $C(\mathsf{S})^\vee = \mathsf{S}$ for all replete subcategories S of $\mathsf{Comod}(C)$. □

The first statement follows from Corollary 4.6, and the second follows from Lemma 11.1.

PROPOSITION 14.3 *Let A be a bialgebra over k.*

(a) *A sub-coalgebra D of A is a sub-bialgebra of A if and only if $D^\vee$ is stable under tensor products and contains the trivial comodule.*

(b) *Assume A has an inversion S. A sub-bialgebra D is stable under S if and only if $D^\vee$ is stable under the contragredient functor.*

PROOF. (a) If D is a sub-bialgebra of A, then certainly $D^\vee$ is stable under tensor products and contains the trivial comodule (see §5). For the converse, recall that $D = \bigcup D_V$ and that $D_V \cdot D_{V'} = D_{V \otimes V'}$ (see 11.2), and so D is closed under products. Because $D^\vee$ contains $V_0 = k$, D contains $D_{V_0} = k$.

(b) Use the formula $A_{V^\vee} = SA_V$ (11.3). □

15 Quotient groups and subcategories

For an affine group G over k, $\mathsf{Rep}(G)$ denotes the category of finite-dimensional G-modules. Let $G \to Q$ be a quotient of G. A representation $r\colon Q \to \mathrm{GL}_V$ defines a representation $G \to Q \xrightarrow{r} \mathrm{GL}_V$ of G. We get in this way an exact fully faithful functor $\mathsf{Rep}(Q) \to \mathsf{Rep}(G)$. The essential image of the functor consists of the representations of G containing $\mathrm{Ker}(G \to Q)$ in their kernel. We let $Q^\vee$ denote this subcategory of $\mathsf{Rep}(G)$.

THEOREM 15.1 *The map $Q \mapsto Q^\vee$ is a bijection from the set of isomorphism classes of quotients of G to the set of replete subcategories of $\mathsf{Rep}(G)$ closed under the formation of tensor products (including the empty tensor product) and under passage to the contragredient.*

PROOF. Obvious from (14.2), (14.3), and the dictionary between Hopf algebras and their comodules and affine groups and their representations. □

16 Characters and eigenspaces

A ***character*** of an affine group G is a homomorphism $G \to \mathbb{G}_m$. As $\mathcal{O}(\mathbb{G}_m) = k[X, X^{-1}]$ and $\Delta(X) = X \otimes X$, we see that to give a character χ of G is the same as giving an invertible element $a = a(\chi)$ of $\mathcal{O}(G)$ such that $\Delta(a) = a \otimes a$; such an element is said to be ***group-like***. A one-dimensional representation L of G defines a character of G (because $\mathrm{GL}_L \simeq \mathbb{G}_m$).

A character $\chi\colon G \to \mathbb{G}_m$ defines a representation of G on any finite-dimensional space V: let $g \in G(R)$ act on V_R as multiplication by $\chi(g) \in R^\times$. For example, χ defines a representation of G on $V = k^n$ by

$$g \mapsto \begin{pmatrix} \chi(g) & & 0 \\ & \ddots & \\ 0 & & \chi(g) \end{pmatrix}, \quad g \in G(R).$$

Let $r\colon G \to \mathrm{GL}_V$ be a representation of G. We say that G acts on V ***through a character*** χ if

$$r(g)v = \chi(g)v \text{ all } g \in G(R),\, v \in V_R.$$

More precisely, this means that the image of r is contained in the centre $\mathbb{G}_m$ of GL_V and is the composite of

$$T \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V\,. \tag{84}$$

More generally, we say that G acts on a subspace W of V ***through a character*** χ if W is stable under G and G acts on W through χ. Note that this means, in particular, that the elements of W are common eigenvectors for the $g \in G(k)$: if $w \in W$, then for every $g \in G(k)$, $r(g)w$ is a scalar multiple of w. If G acts on subspaces W and W' through a character χ, then it acts on $W + W'$ through χ. Therefore, there is a largest subspace V_χ of V on which G acts through χ, called the ***eigenspace for*** G ***with character*** χ.

LEMMA 16.1 *Let (V,r) be a representation of G, and let (V,ρ) be the corresponding comodule. For any character χ of G,*

$$V_\chi = \{v \in V \mid \rho(v) = v \otimes a(\chi)\}.$$

PROOF. Let W be a subspace of V. Then G acts on W through χ if and only if $\rho|W$ factors as

$$W \xrightarrow{w \mapsto w\otimes X} W \otimes \mathcal{O}(\mathbb{G}_m) \xrightarrow{w\otimes X \mapsto w \otimes a(\chi)} W \otimes \mathcal{O}(G).$$

□

THEOREM 16.2 *Let $r\colon G \to \mathrm{GL}(V)$ be a representation of an algebraic group on a vector space V. If V is a sum of eigenspaces, $V = \sum_{\chi\in\Xi} V_\chi$, then it is a direct sum of the eigenspaces*

$$V = \bigoplus\nolimits_{\chi\in\Xi} V_\chi.$$

PROOF. We first prove this when G is smooth. We may replace k with a larger field, and so assume that k is algebraically closed. If the sum is not direct, there exists a finite subset $\{\chi_1,\ldots,\chi_m\}$, $m \geq 2$, of Ξ and a relation

$$v_1 + \cdots + v_m = 0,\; v_i \in V_{\chi_i},\; v_i \neq 0. \tag{85}$$

On applying $g \in G(k)$ to (85), we get a relation

$$\chi_1(g)v_1 + \cdots + \chi_{m-1}(g)v_{m-1} + \chi_m(g)v_m = 0. \tag{86}$$

As $\chi_m \neq \chi_{m-1}$ and G is smooth, there exists a $g \in G(k)$ such that $\chi_m(g) \neq \chi_{m-1}(g)$. Multiply (86) by $\chi_m(g)^{-1}$ and subtract it from (85). This will give us a new relation of the same form but with fewer terms. Continuing in this fashion, we arrive at a contradiction.

For the proof of the general case, we shall make use of the elementary lemma XIV, 1.2, which says that any set of units a in $\mathcal{O}(G)$ satisfying $\Delta(a) = a \otimes a$ is linearly independent. From the relation (85), we get a relation

$$0 = \sum\nolimits_{i\in J} \rho(v_i) = \sum\nolimits_{i\in J} v_i \otimes a(\chi_i)$$

which contradicts the linear independence of the $a(\chi_i)$. □

In Chapter XV we shall show that when G is a split torus, V is always a sum of the eigenspaces V_χ. In general, this will be far from true. For example, SL_n has no nontrivial characters.

17 Every normal affine subgroup is a kernel

LEMMA 17.1 *Let v and w be nonzero vectors in vector spaces V and W respectively, and let u and β be endomorphisms of V_R and W_R for some k-algebra R. If $v \otimes w$ is fixed by $u \otimes \beta$, then there exists a $c \in R^\times$ such that $u(v) = cv$ and $\beta(w) = c^{-1}w$.*

PROOF. Write

$$V = \langle v\rangle \oplus V', \quad W = \langle w\rangle \oplus W'.$$

Then

$$V \otimes W = \langle v \otimes w\rangle \;\oplus\; \langle v\rangle \otimes W' \;\oplus\; V' \otimes \langle w\rangle \;\oplus\; V' \otimes W',$$

where $\langle v \otimes w\rangle = \langle v\rangle \otimes \langle w\rangle \neq 0$. Write

$$uv = av + v', \quad \beta w = bw + w', \quad a,b \in R, \quad v' \in V'_R, \quad w' \in W'_R.$$

Then

$$(u \otimes \beta)(v \otimes w) = ab(v \otimes w) + av \otimes w' + v' \otimes bw + v' \otimes w'.$$

If $(u \otimes \beta)(v \otimes w) = v \otimes w$, then $ab = 1$ and

$$a\left(v \otimes w'\right) = 0 = b\left(v' \otimes w\right).$$

As $a,b \in R^\times$ and $v \neq 0 \neq w$, this implies that $w' = 0 = v'$, as required. □

LEMMA 17.2 *For any normal subgroup N of an affine group G and representation (V,r) of G, the subspace V^N is stable under G.*

PROOF. Let $w \in (V^N)_R$ and let $g \in G(R)$ for some k-algebra R. For any R-algebra R' and $n \in N(R')$

$$r(n)(r(g)w) = r(ng)w = r(gn')w = r(g)r(n')w = r(g)w,$$

because $n' = g^{-1}ng \in N(R')$. Therefore, $r(g)w \in (V^N)_R$, as required. □

LEMMA 17.3 *Let G be an affine group over k, and let (V,r) be a representation of G. If V is a sum of simple subrepresentations, say $V = \sum_{i \in I} S_i$ (the sum need not be direct), then for any subrepresentation W of V, there is a subset J of I such that*

$$V = W \oplus \bigoplus\nolimits_{i \in J} S_i.$$

In particular, V is semisimple.

PROOF. Let J be maximal among the subsets of I such the sum $S_J \overset{\text{def}}{=} \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). For this, it suffices to show that each S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals S_i or 0. In the first case, $S_i \subset W + S_J$, and in the second $S_J \cap S_i = 0$ and $W \cap (S_J + S_i) = 0$, contradicting the definition of I. □

LEMMA 17.4 *Suppose that k is algebraically closed. Every normal subgroup of an algebraic group G over k occurs as the kernel of representation of G.*

PROOF. Let N be a normal subgroup of G. According to Chevalley's theorem 13.1, N is the stabilizer of a line L in a representation V of G. Let N act on L through the character χ. After possibly replacing (V, L) with a second pair, we shall find a G-module U and a line L' in U such that N acts on L' through χ and L' is a direct summand of U as an N-module. Then $U^{\vee}$ contains a line $L^{\vee}$ on which N acts through the character χ^{-1}, and $L \otimes L^{\vee} \subset (V \otimes U^{\vee})^{N}$. If an element u of $G(R)$ acts trivially on $(V \otimes U^{\vee})^{N}_{R}$, then it acts trivially on $(L \otimes L^{\vee})_{R}$, and so it stabilizes L_R in V_R (by 17.1); hence $u \in N(R)$. Therefore N is the kernel of the representation of G on $(V \otimes U^{\vee})^{N}$.

It remains to construct U. Suppose first that G is smooth. In this case, we take U to be the smallest G-stable subspace of V containing L. The subspace $\sum_{g \in G(k)} gL$ of V is stable under $G(k)$, hence under G (12.3), and so equals U. According to Lemma 17.3, U decomposes into a direct sum $U = \bigoplus_{i \in I} L_i$ of lines L_i stable under N, one of which can be taken to be L.

If G is not smooth, then the characteristic of k is $p \neq 0$, and there exists an n such that $\mathcal{O}(G)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(G)$ (see VI, 10.2). In this case, we replace V by $V^{\otimes p^n}$ and L by $L^{\otimes p^n}$ — Proposition 12.4 shows that N is still the stabilizer of L. Let G' be the quotient of G such that $\mathcal{O}(G') = \mathcal{O}(G)^{p^n}$. Choose a basis $(e_i)_{i \in I}$ for V containing a nonzero element e of L. Write

$$\rho(e) = e \otimes a + \sum\nolimits_{e_i \neq e} e_i \oplus a_i, \quad a_{i1} \in \mathfrak{a} = \mathrm{Ker}(\mathcal{O}(G) \to \mathcal{O}(N)). \tag{87}$$

In replacing L with $L^{\otimes p^r}$, we replaced the original a with a^{p^n}, which now lies in $\mathcal{O}(G')$. Let $L' = \langle a \rangle \subset \mathcal{O}(G')$, and consider the representation

$$G \to G' \to \mathrm{GL}_{\mathcal{O}(G')}$$

of G on $\mathcal{O}(G')$. The character χ of N corresponds to the element $\bar{a}$ of $\mathcal{O}(N)$, where $\bar{a}$ is the image of b in $\mathcal{O}(N) = \mathcal{O}(G)/\mathfrak{a}$ (see (87)). As

$$\Delta(a) \equiv a \otimes a \mod \mathcal{O}(G) \otimes \mathcal{O}(G)/\mathfrak{a},$$

N acts on the line L' through the same character χ. Because G' is smooth, we can take U to be the smallest G'-stable subspace of $\mathcal{O}(G')$ containing L', as in the paragraph above. □

THEOREM 17.5 *Let N be a normal subgroup of an algebraic group G. The universal surjective homomorphism $G \to Q$ containing N its kernel (see VII, 8.1) has kernel exactly N.*

PROOF. Lemma 17.4 show that, over some finite extension k' of k, there exists a homomorphism $G_{k'} \to H$ with kernel $N_{k'}$. The kernel of $G \to \Pi_{k'/k} H$ is N. From the universal property of $G \to Q$, we see that $\mathrm{Ker}(G \to Q) \subset N$, and hence the two are equal. □

COROLLARY 17.6 *For any distinct normal subgroups $N \subset N'$ of an affine group G, there exists a representation of G on which N acts trivially but N' acts nontrivially.*

PROOF. Let $Q = G/N$ be the quotient of G by N, and let $Q \to \mathrm{GL}_V$ be a faithful representation of Q. The composite $G \to Q \to \mathrm{GL}_V$ is the required representation. □

18 Variant of the proof of the key Lemma 17.4

LEMMA 18.1 *Let (V,r) be a finite-dimensional faithful representation of an algebraic group G, and let N be the kernel of the representation of G on $V^{\vee}\otimes V$. Then*

$$N(R)=\{u\in G(R)\mid \text{there exists a } c\in R \text{ such that } ux=cv \text{ for all } v\in V\}.$$

In other words, for any subgroup G of GL_V, the subgroup of G acting trivially on $V^{\vee}\otimes V$ is the subgroup acting on V by scalars.

PROOF. Let $(e_i)_{1\leq i\leq n}$ be a basis for V, and let $e_{ij}=e_i^{\vee}\otimes e_j$. Let u be endomorphism of V_R for some k-algebra R. A direct calculation shows that $u(e_{ij})=e_{ij}$ for all i,j if and only if there exists a $c\in R$ such that $ue_i=ce_i$ for all i. □

LEMMA 18.2 *Let G be an algebraic group, and let H be a subgroup of G. The following are equivalent:*

(a) *H is normal in G;*
(b) *for each representation V of G and k-character χ of H, the subspace V^{χ} of V on which H acts through χ is stable under G;*
(c) *every H-isotypic component of a representation of G is stable under G.*

PROOF. See André 1992, Lemma 1. (We sketch the proof of (a) $\implies$ (b). For any $g\in G(k)$, $gV^{\chi}=V^{g\chi}$, but the action of G on the set of k-characters of H is trivial, because G is connected and the set is discrete. When G is smooth, this is shown in the proof of (XVI, 4.7).) □

We now prove that every normal subgroup N of a connected algebraic group G occurs as the kernel of a representation of G (without assumption on the field k). Let L be a line in a representation V of G such that $G_L=N$. Then N acts on L through a character χ. Let W be the smallest G-stable subspace of V containing L. Then $W\subset V^{\chi}$ by (18.2), and so N is contained in the kernel H of $G\to\mathrm{GL}_{W^{\vee}\otimes W}$. According to (18.1), H acts on W through a k-character. In particular, it stabilizes L, and so $H\subset N$.

19 Applications of Corollary 17.6

LEMMA 19.1 *Let N_1 and N_2 be normal subgroups of an affine group G. If $\mathsf{Rep}(G)^{N_1}=\mathsf{Rep}(G)^{N_2}$ then $N_1=N_2$.*

PROOF. If $N_1\neq N_2$, then Corollary 17.6 shows that there exists a representation (V,r) of G and a $v\in V$ fixed by N_1 but not by N_1N_2. Then V^{N_1} is an object of $\mathsf{Rep}(G)^{N_1}$ but not of $\mathsf{Rep}(G)^{N_2}$, which contradicts the hypothesis. □

THEOREM 19.2 *Let N be a normal subgroup of an affine group G, and let Q be a quotient of G. Then $N=\mathrm{Ker}(G\to Q)$ if and only if $\mathsf{Rep}(G)^{N}=Q^{\vee}$.*

PROOF. $\Rightarrow$: According to Theorem 7.8, Chapter VII, a representation $r\colon G \to \mathrm{GL}_V$ factors through Q (and so lies in $Q^\vee$) if and only if r maps N to 1 (and so (V,r) lies in $\mathsf{Rep}(G)^N$).

$\Leftarrow$: Let N' be the kernel of $G \to Q$. Then $\mathsf{Rep}(G)^{N'} = Q^\vee$, and so $\mathsf{Rep}(G)^N = \mathsf{Rep}(G)^{N'}$. This implies that $N = N'$. □

COROLLARY 19.3 *The map $N \mapsto \mathsf{Rep}(G)^N$ is a bijection from the set of normal subgroups of G to the set of replete subcategories of $\mathsf{Rep}(G)$ closed under tensor products and passage to the contragredient.*

PROOF. Let S be a replete subcategory of $\mathsf{Rep}(G)$ closed under tensor products and passage to the contragredient. The $\mathsf{S} = Q^\vee$ for some quotient Q of G, well-defined up to isomorphism, and the kernel N of $G \to Q$ is a normal subgroup of G. The maps $\mathsf{S} \mapsto N$ and $N \mapsto \mathsf{Rep}(G)^N$ are inverse. □

THEOREM 19.4 *For any normal subgroup N of an affine group G, there exists a quotient map with kernel N.*

PROOF. The subcategory $\mathsf{Rep}(G)^N$ of $\mathsf{Rep}(G)$ is replete and closed under tensor products and passage to the contragredient. Therefore $\mathsf{Rep}(G)^N = Q^\vee$ for some quotient Q of G, and the Theorem 19.2 implies that N is the kernel of $G \to Q$. □

NOTES Add a discussion of the correspondence between normal subgroups of an affine group G and the normal Hopf ideals in $\mathcal{O}(G)$ (Abe 1980, p. 179), and also of the correspondence between normal Hopf ideals and Hopf subalgebras (ibid. 4.4.7, p. 207, in the case that k is algebraically closed and the Hopf algebras are assumed to be reduced).

NOTES Add a discussion of the general theorem on the existence of quotients of group schemes over artinian rings (SGA 3, VI_A).

CHAPTER IX

Group Theory: the Isomorphism Theorems

In this chapter, we show that the (Noether) isomorphism theorems in abstract group theory hold also for affine groups. Throughout, k is a field.

1 Review of abstract group theory

For a group G (in the usual sense), we have the notions of subgroup, a normal subgroup, an embedding (injective homomorphism), and of a quotient map (surjective homomorphism). Moreover, there are the following basic results, which are often referred to collectively as the isomorphisms theorems.[1]

1.1 (Existence of quotients). The kernel of a quotient map $G \to Q$ is a normal subgroup of G, and every normal subgroup N of G arises as the kernel of a quotient map $G \to G/N$.

1.2 (Homomorphism theorem). The image of a homomorphism $u\colon G \to G'$ is a subgroup uG of G', and u defines an isomorphism from $G/\mathrm{Ker}(u)$ onto uG; in particular, every homomorphism is the composite of a quotient map and an embedding.

1.3 (Isomorphism theorem). Let H and N be subgroups of G such that H normalizes N; then HN is a subgroup of G, N is a normal subgroup of HN, $H \cap N$ is a normal subgroup of H, and the map

$$h(H \cap N) \mapsto hN\colon H/H \cap N \to HN/N$$

is an isomorphism.

1.4 (Correspondence theorem). Let N be a normal subgroup of G. The map $H \mapsto H/N$ defines a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N. A subgroup H of G containing N is normal if and only if H/N is normal in G/N, in which case the map

$$G/H \to (G/N)/(H/N)$$

defined by the quotient map $G \to G/N$ is an isomorphism.

[1] Statements (1.2), (1.3), and (1.4) are sometimes called the first, second, and third isomorphism theorems, but the numbering varies. In Noether 1927, the first isomorphism theorem is (1.4) and the second is (1.3).

In this chapter, we shall see that, appropriately interpreted, all these notions and statements extend to affine groups (in particular, to algebraic groups).

2 The existence of quotients

THEOREM 2.1 *The kernel of a quotient map $G \to Q$ of affine groups over k is a normal affine subgroup of G, and every normal affine subgroup N of G arises as the kernel of a quotient map $G \to G/N$.*

PROOF. See Theorem 17.5, Chapter VIII. □

EXAMPLE 2.2 Let PGL_n be the quotient of GL_n by its centre, and let PSL_n be the quotient of SL_n by its centre:

$$\mathrm{PGL}_n = \mathrm{GL}_n/\mathbb{G}_m, \quad \mathrm{PSL}_n = \mathrm{SL}_n/\mu_n.$$

The homomorphism $\mathrm{SL}_n \to \mathrm{GL}_n \to \mathrm{PGL}_n$ contains μ_n in its kernel, and so defines a homomorphism

$$\mathrm{PSL}_n \to \mathrm{PGL}_n. \tag{88}$$

Is this an isomorphism? Note that

$$\mathrm{SL}_n(k)/\mu_n(k) \to \mathrm{GL}_n(k)/\mathbb{G}_m(k) \tag{89}$$

is injective, but not in general surjective: not every invertible $n \times n$ matrix can be written as the product of a matrix with determinant 1 and a scalar matrix (such a matrix has determinant in $k^{\times n}$). Nevertheless, I claim that (88) is an isomorphism of algebraic groups. In characteristic zero, this follows from the fact that (89) is an isomorphism when $k = k^{\mathrm{al}}$ (apply VII, 4.5 and 7.6). In the general case, we have to check the conditions (VII, 2.1a and 7.1).

Let $q \neq 1 \in \mathrm{PSL}_n(R)$. For some faithfully flat R-algebra R', there exists a $g \in \mathrm{SL}_n(R')$ mapping to q in $\mathrm{PSL}_n(R')$. The image of g in $\mathrm{GL}_n(R')$ is not in $\mathbb{G}_m(R')$ (because $q \neq 1$); therefore, the image of g in $\mathrm{PGL}_n(R')$ is $\neq 1$, which implies that the image of q in $\mathrm{PGL}(R)$ is $\neq 1$:

$$\begin{tikzcd}
\mathrm{PSL}_n(R') \arrow[r] & \mathrm{PGL}_n(R') \\
\mathrm{PSL}_n(R) \arrow[r] \arrow[u] & \mathrm{PGL}_n(R). \arrow[u, "\text{injective}"']
\end{tikzcd}$$

We have checked condition (VII, 2.1a).

Let $q \in \mathrm{PGL}_n(R)$. For some faithfully flat R-algebra R', there exists a $g \in \mathrm{GL}_n(R')$ mapping to q. If $a \overset{\text{def}}{=} \det(g)$ is an nth power, say $a = t^n$, then $g = g_0 t$ with $\det(g_0) = 1$, and the image of g in $\mathrm{GL}_n(R')/\mathbb{G}_m(R')$ is in the image of $\mathrm{SL}_n(R')/\mu_n(R')$. Hence, the image of q in $\mathrm{PGL}_n(R')$ is in the image of $\mathrm{PSL}_n(R')$. If a is not an nth power in R', we replace R' by the faithfully flat (even free) algebra $R'[T]/(T^n - a)$ in which it does become an nth power. We have checked condition (VII, 7.1).

3 The homomorphism theorem

A homomorphism $u\colon G \to G'$ of affine groups defines a homomorphism $u^\natural\colon \mathcal{O}(G') \to \mathcal{O}(G)$ of Hopf algebras, whose kernel $\mathfrak{a}$ is a Hopf ideal in $\mathcal{O}(G')$.[2] Thus

$$\mathfrak{a} = \{f \in \mathcal{O}(G') \mid f_R(u_R(P)) = 0 \text{ for all } k\text{-algebras } R \text{ and all } P \in G(R)\}.$$

The subgroup H of G' corresponding to $\mathfrak{a}$ (see VII, 3.2) is called the ***image*** of u (and often denoted uG). Thus

$$H(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for } f \in \mathfrak{a}\}.$$

THEOREM 3.1 *(Homomorphism theorem) For any homomorphism $u\colon G \to G'$ of affine groups, the kernel N of u is a normal subgroup of G, the image uG of u is a subgroup of G', and u factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{tikzcd}
G \arrow[r, "u"] \arrow[d, "\text{surjective}"'] & G' \\
G/N \arrow[r, "\text{isomorphism}"] & uG. \arrow[u, "\text{injective}"']
\end{tikzcd}$$

If G is an algebraic group, then so also are G/N and uG.

PROOF. The factorization

$$\mathcal{O}(G) \leftarrow \mathcal{O}(G')/\mathfrak{a} \leftarrow \mathcal{O}(G')$$

of $u^\natural$ defines a factorization

$$G \to uG \to G'$$

of u into a surjection followed by an injection. As $G \to G/N$ and $G \to uG$ are both quotient maps with kernel N, there is a unique isomorphism $G/N \to uG$ such that the composite

$$G \to G/N \to uG$$

is $G \xrightarrow{u} uG$ (apply VII, 7.9).

The final statement follows from (VIII, 8.6). □

COROLLARY 3.2 *For any k-algebra R,*

$$(uG)(R) = \bigcup\nolimits_{R'} G(R) \cap \operatorname{Im} u(R')$$

where R' runs over the faithfully flat R-algebras. Therefore uG represents the sheaf associated with

$$R \rightsquigarrow \operatorname{Im}(u(R)).$$

Moreover, uG is the intersection of the subgroups H of G' with the property that $\operatorname{Im} u(R) \subset H(R)$ for all k-algebras R.

[2] In fact, we don't need to use that $\mathfrak{a}$ is a Hopf ideal, just that it is an ideal.

PROOF. The map $G \to uG$ is a quotient map, and so the first statement follows from (VII, 11.6). If H is a subgroup of G' such that $H(R) \supset \operatorname{Im} u(R)$ for all k-algebras R, then, for any fixed k-algebra R,

$$H(R) \supset \bigcup\nolimits_{R'} G(R) \cap \operatorname{Im} u(R') = (uG)(R),$$

and so $H \supset uG$. □

COROLLARY 3.3 *A homomorphism $u\colon G \to G'$ of algebraic groups is surjective if, for some field K containing k, the image of $G(K)$ in $G'(K)$ is dense in G'.*

PROOF. As $u(G(K)) \subset (uG)(K) \subset G'(K)$, the condition implies that $uG = G$. □

Let $u\colon G \to G'$ be a homomorphism of algebraic groups. Then $G(k^{\mathrm{al}}) \to (uG)(k^{\mathrm{al}})$ is surjective (see VII, 7.6), and so

$$\begin{aligned}(uG)(k) &= G'(k) \cap (uG)(k^{\mathrm{al}})\\ &= G'(k) \cap \operatorname{Im}(G(k^{\mathrm{al}}) \xrightarrow{u(k^{\mathrm{al}})} G'(k^{\mathrm{al}})).\end{aligned}$$

4 The isomorphism theorem

Let H and N be algebraic subgroups of G such that H normalizes N. The natural action of $H(R)$ on $N(R)$ defines an action θ of H on N by group homomorphisms, and multiplication defines a homomorphism

$$N \rtimes_\theta H \to G.$$

We define $NH = HN$ to be the image of this homomorphism. The following statements are obvious from §3.

4.1 For any k-algebra R, $(HN)(R)$ consists of the elements of $G(R)$ that lie in $H(R')N(R')$ for some finitely generated faithfully flat R-algebra R'. Therefore HN represents the sheaf associated with the functor

$$R \rightsquigarrow H(R) \cdot N(R) \subset G(R).$$

Moreover, HN is the intersection of the subgroups G' of G such that, for all k-algebras R, $G'(R)$ contains both $H(R)$ and $N(R)$.

4.2 We have

$$(HN)(k^{\mathrm{al}}) = H(k^{\mathrm{al}}) \cdot N(k^{\mathrm{al}}),$$

and so

$$(HN)(k) = G(k) \cap (H(k^{\mathrm{al}}) \cdot N(k^{\mathrm{al}})).$$

☠ 4.3 It is not true that $(HN)(R) = H(R)N(R)$ for all k-algebras R. For example, consider the algebraic subgroups SL_n and $\mathbb{G}_m$ (nonzero scalar matrices) of GL_n. Then $\mathrm{GL}_n = \mathrm{SL}_n \cdot \mathbb{G}_m$, but a matrix $A \in \mathrm{GL}_n(R)$ whose determinant is not an nth power is not the product of a scalar matrix with a matrix of determinant 1.

THEOREM 4.4 *(Isomorphism theorem) Let H and N be algebraic subgroups of the algebraic group G such that H normalizes N. The natural map*

$$H/H\cap N\to HN/N \tag{90}$$

is an isomorphism.

PROOF. We have an isomorphism of group-valued functors

$$H(R)/(H\cap N)(R)\to H(R)N(R)/N(R)\subset(HN)(R)/N(R).$$

The statement now follows from (VII, 11.6), or by passing to the associated sheaves. □

EXAMPLE 4.5 Let $G=\mathrm{GL}_n$, $H=\mathrm{SL}_n$, and $N=\mathbb{G}_m$ (scalar matrices in G). Then $N\cap H=\mu_n$ (obviously), $HN=\mathrm{GL}_n$ (by the arguments in 2.2), and (90) becomes the isomorphism

$$\mathrm{SL}_n/\mu_n\to\mathrm{GL}_n/\mathbb{G}_m.$$

EXAMPLE 4.6 The isomorphism theorem fails in the category of smooth algebraic groups. Consider, for example, the subgroups $H=\mathbb{G}_m$ (diagonal) and $N=\mathrm{SL}_p$ of GL_p over a field of characteristic p. In the category of smooth algebraic groups, $N\cap H=1$, and the map $H/H\cap N\to HN/N$ is the homomorphism $\mathrm{SL}_p\to\mathrm{PGL}_p$, which is an inseparable isogeny of degree p — it is injective and surjective in the category of smooth algebraic groups, but it is not an isomorphism.

5 The correspondence theorem

THEOREM 5.1 *(Correspondence theorem). Let N be a normal algebraic subgroup of G. The map $H\mapsto H/N$ defines a one-to-one correspondence between the set of algebraic subgroups of G containing N and the set of algebraic subgroups of G/N. An algebraic subgroup H of G containing N is normal if and only if H/N is normal in G/N, in which case the map*

$$G/H\to(G/N)/(H/N) \tag{91}$$

defined by the quotient map $G\to G/N$ is an isomorphism.

PROOF. The first statement follows from the fact that the analogous statement holds for Hopf algebras (cf. Exercise II-6). For the second statement, note that the map

$$G(R)/H(R)\to(G(R)/N(R))/(H(R)/N(R))$$

defined by the quotient map $G(R)\to G(R)/N(R)$ is an isomorphism. This isomorphism is natural in R, and when we pass to the associated sheaves, we obtain the isomorphism (91). □

ASIDE 5.2 Let $q\colon G\to G/N$ be the quotient map. For any subgroup H of G, qH is a subgroup of G/N, which corresponds to HN. Deduce that if H' is normal in H, then $H'N$ is normal in HN.

NOTES Need to discuss how much of the isomorphism theorems hold for smooth groups. Should move the smoothness part of (XVII, 1.1) here.

6 The Schreier refinement theorem

LEMMA 6.1 (BUTTERFLY LEMMA) *Let $H_1 \supset N_1$ and $H_2 \supset N_2$ be algebraic subgroups of an algebraic group G with N_1 and N_2 normal in H_1 and H_2. Then $N_1(H_1 \cap N_2)$ and $N_2(N_1 \cap H_2)$ are normal algebraic subgroups of the algebraic groups $N_1(H_1 \cap H_2)$ and $N_2(H_2 \cap H_1)$ respectively, and there is a canonical isomorphism of algebraic groups*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}$$

PROOF. The algebraic group $H_1 \cap N_2$ is normal in $H_1 \cap H_2$ and so $N_1(H_1 \cap H_2)$ is normal in $N_1(H_1 \cap N_2)$ (see Exercise VII-2). Similarly, $N_2(H_2 \cap N_1)$ is normal in $N_2(H_2 \cap H_1)$.

The subgroup $H_1 \cap H_2$ of G normalizes $N_1(H_1 \cap N_2)$, and so the isomorphism Theorem 4.4 shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \simeq \frac{(H_1 \cap H_2) \cdot N_1(H_1 \cap N_2)}{N_1(H_1 \cap N_2)}. \tag{92}$$

As $H_1 \cap N_2 \subset H_1 \cap H_2$, we have that $H_1 \cap H_2 = (H_1 \cap H_2)(H_1 \cap N_2)$, and so

$$N_1 \cdot (H_1 \cap H_2) = N_1 \cdot (H_1 \cap H_2) \cdot (H_1 \cap N_2).$$

The first of Dedekind's modular laws (Exercise VII-3a) with $A = H_1 \cap N_2$, $B = H_1 \cap H_2$, and $C = N_1$ becomes

$$\begin{aligned}(H_1 \cap H_2) \cap N_1 (H_1 \cap N_2) &= (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) \\ &= (H_1 \cap N_2)(N_1 \cap H_2).\end{aligned}$$

Therefore (92) is an isomorphism

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}.$$

A symmetric argument shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)},$$

and so

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)}.$$

□

A ***subnormal series*** in an affine group G is a finite sequence of subgroups, beginning with G and ending with 1, such that each subgroup is normal in the preceding subgroup.

PROPOSITION 6.2 *Let H be a subgroup of an affine group G. If*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

is a subnormal series for G, then

$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_s = \{1\}$$

is a subnormal series for H, and

$$H \cap G_i / H \cap G_{i+1} \hookrightarrow G_i / G_{i+1}.$$

PROOF. Obvious. □

Two subnormal sequences

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$
$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\}$$

are said to be ***equivalent*** if $s = t$ and there is a permutation π of $\{1,2,\ldots,s\}$ such that $G_i/G_{i+1} \approx H_{\pi(i)}/H_{\pi(i)+1}$.

THEOREM 6.3 *Any two subnormal series in an algebraic group have equivalent refinements.*

PROOF. Let $G_{ij} = G_{i+1}(H_j \cap G_i)$ and let $H_{ji} = H_{j+1}(G_i \cap H_j)$. According to the butterfly lemma

$$G_{ij}/G_{i,j+1} \simeq H_{ji}/H_{j,i+1},$$

and so the refinement (G_{ij}) of (G_i) is equivalent to the refinement (H_{ji}) of (H_i). □

A subnormal series is a ***composition series*** if no quotient group G_i has a proper nontrivial normal subgroup.

THEOREM 6.4 *For any two composition series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$
$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\},$$

$s = t$ and there is a permutation π of $\{1,2,\ldots,s\}$ such that G_i/G_{i+1} is isomorphic to $H_{\pi(i)}/H_{\pi(i)+1}$ for each i.

PROOF. Use that, for each i, only one of the quotients $G_{i+1}(H_j \cap G_i)/G_{i+1}(H_{j+1} \cap G_i)$ is nontrivial □

An algebraic group is ***strongly connected*** if it has no finite quotient. An algebraic group G with $\dim G > 0$ is ***almost-simple*** if for every proper normal subgroup N we have $\dim N < \dim G$. An almost-simple group is strongly connected.

THEOREM 6.5 *Let G be a strongly connected algebraic group. There exists a subnormal sequence*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

such that each G_i is strongly connected and G_i/G_{i+1} is almost-simple. If

$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\}$$

is a second such sequence, then $s = t$ and there is a permutation π of $\{1,2,\ldots,s\}$ such that G_i/G_{i+1} is isogenous to $H_{\pi(i)}/H_{\pi(i)+1}$ for each i.

7 The category of commutative algebraic groups

THEOREM 7.1 *The commutative algebraic groups over a field form an abelian category.*

PROOF. The Hom sets are commutative groups, and the composition of morphisms is bilinear. Moreover, the product $G_1 \times G_2$ of two commutative algebraic groups is both a product and a sum of G_1 and G_2. Thus the category of commutative algebraic groups over a field is additive. Every morphism in the category has both a kernel and cokernel (VII, 4.1; VIII, 17.5), and the canonical morphism from the coimage of the morphism to its image is an isomorphism (homomorphism theorem, 3.1). Therefore the category is abelian. □

COROLLARY 7.2 *The finitely generated commutative co-commutative Hopf algebras over a field form an abelian category.*

ASIDE 7.3 Theorem 7.1 is generally credited to Grothendieck but, as we have seen, it is a fairly direct consequence of allowing the coordinate rings to have nilpotent elements. See SGA 3, VI_A, 5.4; DG III §3, 7.4, p. 355.

Corollary 7.2 is proved purely in the context of Hopf algebras in Sweedler 1969, Chapter XVI, for finite-dimensional commutative co-commutative Hopf algebras, and in Takeuchi 1972, 4.16, for finitely generated commutative co-commutative Hopf algebras.

In the latest version of SGA 3, it is shown (VI_A, 5.4.2) that the category of commutative algebraic group schemes (not necessarily affine) over a field is abelian. It is then shown that the category of *affine* commutative algebraic group schemes is thick in the full category, and so it also is abelian (ibid. 5.4.3). Moreover, the category of all commutative affine groups (not necessarily algebraic) over a field is abelian.

ASIDE 7.4 Let G be an algebraic group scheme over a field k. If G is affine, then every *algebraic* subgroup scheme is affine, and every quotient of G by a normal algebraic subscheme is affine. Moreover, every extension of an affine algebraic group scheme by an affine algebraic group scheme is again an affine algebraic group scheme (SGA 3, VI_B, 9.2(viii)).

8 Exercises

EXERCISE IX-1 Let H and N be subgroups of the algebraic group G such that H normalizes N. Show that the kernel of $\mathcal{O}(G) \to \mathcal{O}(HN)$ is equal to the kernel of the composite

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes_k \mathcal{O}(G) \to \mathcal{O}(H) \otimes_k \mathcal{O}(N).$$

ASIDE 8.1 As noted earlier, in much of the expository literature (e.g., Borel 1991, Humphreys 1975, Springer 1998), "algebraic group" means "smooth algebraic group". With this terminology, many of the results in this chapter become false.[3][4] Fortunately, because of Theorem 9.3, Chapter VI, this is only a problem in nonzero characteristic. The importance of allowing nilpotents was

[3] For example, in the category of smooth groups, the homomorphism $H/H \cap N \to HN/N$ is a purely inseparable isogeny of degree q where q is the multiplicity of $H \cap N$ in the intersection product $H \bullet N$.

[4] The situation is even worse, because these books use a terminology based on Weil's Foundations, which sometimes makes it difficult to understand their statements. For example, in Humphreys 1975, p. 218, one finds the following statement: "for a homomorphism $\varphi: G \to G'$ of k-groups, the kernel of φ need not be defined over k." By this, he means the following: form the kernel N of $\varphi_{k^{\mathrm{al}}}: G_{k^{\mathrm{al}}} \to G'_{k^{\mathrm{al}}}$ (in our sense); then N_{red} need not arise from a smooth algebraic group over k. Of course, with our (or any reasonable) definitions, the kernel of a homomorphism of algebraic groups over k is certainly an algebraic group over k.

pointed out by Cartier (1962) more than forty years ago, but, except for Demazure and Gabriel 1970 and Waterhouse 1979, this point-of-view has not been adopted in the expository literature. Contrast our statement and treatment of the isomorphism theorems and the Schreier refinement theorem with those in Barsotti 1955a and Rosenlicht 1956.

CHAPTER **X**

Categories of Representations (Tannaka Duality)

A character of a topological group is a continuous homomorphism from the group to the circle group $\{z \in \mathbb{C} \mid z\bar{z} = 1\}$. A finite commutative group G can be recovered from its group $G^\vee$ of characters because the canonical homomorphism $G \to G^{\vee\vee}$ is an isomorphism.

More generally, a locally compact commutative topological group G can be recovered from its character group because, again, the canonical homomorphism $G \to G^{\vee\vee}$ is an isomorphism (Pontryagin duality). Moreover, the dual of a compact commutative group is a discrete commutative group, and so, the study of compact commutative topological groups is equivalent to that of discrete commutative groups.

Clearly, "commutative" is required in the above statements, because every character is trivial on the derived group. However, Tannaka showed that it is possible to recover a compact noncommutative group from the category of its unitary representations.

In this chapter, we prove the analogue of this for algebraic groups. Initially, k is allowed to be a commutative ring.

1 Recovering a group from its representations

Let G be an affine monoid with coordinate ring A. Recall that for the regular representation $r_A\colon G \to \mathrm{End}_A$, an element g of $G(R)$ acts on $f \in A$ according to the rule:

$$(gf)_R(x) = f_R(x \cdot g) \text{ all } x \in G(R). \tag{93}$$

LEMMA 1.1 *Let G be an affine monoid over a ring k, and let $A = \mathcal{O}(G)$ be its coordinate ring. Let u be a k-algebra endomorphism of A. If the diagram*

$$\begin{tikzcd} A \arrow[r, "\Delta"] \arrow[d, "u"] & A \otimes A \arrow[d, "1\otimes u"] \\ A \arrow[r, "\Delta"] & A \otimes A \end{tikzcd}$$

commutes, then there exists a $g \in G(k)$ such that $u = r_A(g)$.

PROOF. According to the Yoneda lemma, there exists a natural transformation $\phi\colon G \to G$ of set-valued functors such that

$$(uf)_R(x) = f_R(\phi_R x) \text{ all } f \in A,\, x \in G(R). \tag{94}$$

The commutativity of the diagram says that, for $f \in A$,

$$(\Delta \circ u)(f) = ((1 \otimes u) \circ \Delta)(f).$$

On evaluating this at $(x,y) \in G(R) \times G(R)$, we find that[1]

$$f_R(\phi_R(x \cdot y)) = f_R(x \cdot \phi_R y).$$

As this holds for all $f \in A$,

$$\phi_R(x \cdot y) = x \cdot \phi_R(y), \quad \text{all } x,y \in G(R).$$

On setting $y = e$ in the last equation, we find that $\phi_R(x) = x \cdot g$ with $g = \phi_R(e)$. Therefore, for $f \in A$ and $x \in G(R)$,

$$(uf)_R(x) \overset{(94)}{=} f_R(x \cdot g) \overset{(93)}{=} (gf)_R(x) \overset{\text{def}}{=} (r_A(g)f)_R(x).$$

Hence $u = r_A(g)$. □

THEOREM 1.2 *Let G be a flat affine monoid (or group) over a noetherian ring k, and let R be a k-algebra. Suppose that, for each representation (V, r_V) of G on a finitely generated k-module V, we are given an R-linear map $\lambda_V\colon V_R \to V_R$. If the family (λ_V) satisfies the conditions,*

(a) *for all representations V, W,*

$$\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W,$$

(b) *$\lambda_{\mathbb{1}}$ is the identity map (here $\mathbb{1} = k$ with the trivial action)*

[1] Here are the details. We shall need the formulas (p. 47)

$$(\Delta f)_R(x,y) = f_R(x \cdot y) \text{ for } f \in A$$
$$(f_1 \otimes f_2)_R(x,y) = (f_1)_R(x) \cdot (f_2)_R(y) \text{ for } f_1, f_2 \in A$$

For $x, y \in G(R)$,

$$(\text{LHS})_R(x,y) = ((\Delta \circ u)(f))_R(x,y) = (\Delta(uf))_R(x,y) = (uf)_R(x \cdot y) = f_R(\phi_R(x \cdot y)).$$

Let $\Delta f = \sum f_i \otimes g_i$; then

$$\begin{aligned}(\text{RHS})_R(x,y) = \left((1 \otimes u) \circ (\textstyle\sum_i f_i \otimes g_i)\right)_R(x,y) &= \left(\textstyle\sum_i f_i \otimes ug_i\right)_R(x,y)\\ &= \textstyle\sum_i f_{iR}(x) \cdot (ug_i)_R(y)\\ &= \textstyle\sum_i f_{iR}(x) \cdot g_{iR}(\phi_R y)\\ &= \left(\textstyle\sum_i f_i \otimes g_i\right)_R(x, \phi_R y)\\ &= (\Delta f)_R(x, \phi_R y)\\ &= f_R(x \cdot \phi_R y).\end{aligned}$$

(c) *for all G-equivariant maps $u\colon V\to W$,*

$$\lambda_W\circ u_R = u_R\circ\lambda_V,$$

then there exists a unique $g\in G(R)$ such that $\lambda_V = r_V(g)$ for all V.

PROOF. Under our hypotheses, every representation V of G is a union of its finitely generated representations, $V=\bigcup_{i\in I}V_i$ (see VIII, 6.7). It follows from (c) that

$$\lambda_{V_i}|V_i\cap V_j = \lambda_{V_i\cap V_j} = \lambda_{V_j}|V_i\cap V_j$$

for all $i,j\in I$.Therefore, there is a unique R-linear endomorphism λ_V of V_R such that $\lambda_V|W=\lambda_W$ for every finitely generated subrepresentation $W\subset V$. The conditions (a,b,c) will continue to hold for the enlarged family.

Let $A=\mathcal{O}(G)_R$, and let $\lambda_A\colon A\to A$ be the R-linear map corresponding to the regular representation r of G on A. The map $m\colon A\otimes A\to A$ is equivariant[2] for the representations $r\otimes r$ and r, which means that λ_A is a k-algebra homomorphism. Similarly, the map $\Delta\colon A\to A\otimes A$ is equivariant for the representations r on A and $1\otimes r$ on $A\otimes A$, and so the diagram in (1.1) commutes with u replaced by λ_A. Now Lemma 1.1, applied to the affine monoid G_R over R, shows that there exists a $g\in G(R)$ such $\lambda_A=r(g)$.

Let (V,r_V) be a finitely generated representation of G, and let V_0 denote the underlying k-module. There is an injective homomorphism of representations

$$\rho\colon V\to V_0\otimes\mathcal{O}(G)$$

(VIII, 10.3). By definition λ and $r(g)$ agree on $\mathcal{O}(G)$, and they agree on V_0 by condition (b). Therefore they agree on $V_0\otimes\mathcal{O}(G)$ by (a), and so they agree on V by (c).

This proves the existence of g. It is unique because the regular representation is faithful (VIII, §9). □

Remarks

1.3 Each $g\in G(R)$ of course defines a family as in the theorem. Thus, from the category $\mathsf{Rep}(G)$ of representations of G on finitely generated k-modules we can recover $G(R)$ for all R, and hence the group G itself. For this reason, Theorem 1.2 is often called the *reconstruction theorem.*

1.4 Let (λ_V) be a family satisfying the conditions (a,b,c) of Theorem 1.4. When G is an affine group (rather than just a monoid), each λ_V is an isomorphism, and the family satisfies the condition $\lambda_{V^\vee}=(\lambda_V)^\vee$ (because this is true of the family $(r_V(g))$).

1.5 Let ω_R be the forgetful functor $\mathsf{Rep}_R(G)\to\mathsf{Mod}_R$, and let $\mathrm{End}^{\otimes}(\omega_R)$ be the set of natural transformations $\lambda\colon\omega_R\to\omega_R$ commuting with tensor products — the last condition means that λ satisfies conditions (a) and (b) of the theorem. The theorem says that the

[2] Here are the details. For $x\in G(R)$,

$$(r(g)\circ m)(f\otimes f')(x) = (r(g)(ff'))(x) = (ff')(xg) = f(xg)\cdot f'(xg)$$
$$(m\circ r(g)\otimes r(g))(f\otimes f')(x) = ((r(g)f)\cdot(r(g)f')(x) = f(xg)\cdot f'(xg).$$

canonical map $G(R) \to \mathrm{End}^{\otimes}(\omega_R)$ is an isomorphism. Now let $\underline{\mathrm{End}}^{\otimes}(\omega)$ denote the functor $R \rightsquigarrow \mathrm{End}^{\otimes}(\omega_R)$; then $G \simeq \underline{\mathrm{End}}^{\otimes}(\omega)$. When G is an affine group, this can be written $G \simeq \underline{\mathrm{Aut}}^{\otimes}(\omega)$.

1.6 When k is a Dedekind domain, it suffices to consider representations on finitely generated projective k-modules in the theorem (because every finitely generated submodule of $\mathcal{O}(G)$ is projective). In fact, the theorem holds for finitely generated free k-modules.

1.7 Assume that k is a Dedekind domain and that G is a flat affine group over k. A homomorphism $u: V \to W$ of finitely generated projective k-modules corresponds to a tensor $u' \in V^{\vee} \otimes W$, and u is G-equivariant if and only if u' is fixed by G. Let H be a flat affine subgroup of G. It follows from the theorem that, for each k-algebra R, $H(R)$ is the subgroup of $G(R)$ of elements fixing all tensors in all representations of G fixed by H.

1.8 Suppose that k is an algebraically closed field, and that G is reduced, so that $\mathcal{O}(G)$ can be identified with a ring of k-valued functions on $G(k)$. It is possible to give an explicit description description of $\mathcal{O}(G)$ in terms of the representations of G. For each representation (V, r_V) of G (over k) and $u \in V^{\vee}$, we have a function ϕ_u on $G(k)$,

$$\phi_u(g) = \langle u, r_V(g)\rangle \in k.$$

Then $\phi_u \in \mathcal{O}(G)$, and every element of $\mathcal{O}(G)$ arises in this way (cf. Springer 1998, p.39, and Exercise II-2).

1.9 Suppose that k is a field. In (1.7), instead of all representations of G, it suffices to choose a faithful representation V and take all quotients of subrepresentations of a direct sum of representations of the form $\otimes^n(V \oplus V^{\vee})$ (by VIII, 11.7).

1.10 In general, we can't omit "quotients of" from (1.9).[3] However, we can omit it if some nonzero multiple of every homomorphism $H \to \mathbb{G}_m$ extends to a homomorphism $G \to \mathbb{G}_m$ (VIII, 13.3).

2 Application to Jordan decompositions

In this section, we require k to be a field.

The Jordan decomposition of a linear map

In this subsection, we review some linear algebra.

Recall that an endomorphism α of a vector space V is ***diagonalizable*** if V has a basis of eigenvectors for α, and that it is ***semisimple*** if it becomes diagonalizable after an extension of the base field k. For example, the linear map $x \mapsto Ax: k^n \to k^n$ defined by an $n \times n$ matrix A is diagonalizable if and only if there exists an invertible matrix P with entries in k

[3] Consider for example, the subgroup $B = \left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\right\}$ of GL_2 acting on $V = k \times k$ and suppose that a vector $v \in (V \oplus V^{\vee})^{\otimes n}$ is fixed by B. Then $g \mapsto gv$ is a regular map $\mathrm{GL}_2/B \to (V \oplus V^{\vee})^{\otimes n}$ of algebraic varieties (not affine). But $\mathrm{GL}_2/B \simeq \mathbb{P}^1$, and so any such map is trivial. Therefore, v is fixed by GL_2, and so $B' = B$. Cf VII, 7.14.

such that PAP^{-1} is diagonal, and it is semisimple if and only if there exists such a matrix P with entries in some field containing k.

From linear algebra, we know that α is semisimple if and only if its minimum polynomial $m_\alpha(T)$ has distinct roots; in other words, if and only if the subring $k[\alpha] \simeq k[T]/(m_\alpha(T))$ of $\mathrm{End}_k(V)$ generated by α is étale.

Recall that an endomorphism α of a vector space V is ***nilpotent*** if $\alpha^m = 0$ for some $m > 0$, and that it is ***unipotent*** if $\mathrm{id}_V - \alpha$ is nilpotent. Clearly, if α is nilpotent, then its minimum polynomial divides T^m for some m, and so the eigenvalues of α are all zero, even in k^{al}. From linear algebra, we know that the converse is also true, and so α is unipotent if and only if its eigenvalues in k^{al} all equal 1.

Let α be an endomorphism of a finite-dimensional vector space V over k. We say that α ***has all of its eigenvalues*** in k if the characteristic polynomial $P_\alpha(T)$ of α splits in $k[X]$:

$$P_\alpha(T) = (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}, \quad a_i \in k.$$

For each eigenvalue a of α in k, the ***primary space***[4] is defined to be:

$$V^a = \{v \in V \mid (\alpha - a)^N v = 0, \quad N \text{ sufficiently divisible}^{5}\}.$$

PROPOSITION 2.1 *If α has all of its eigenvalues in k, then V is a direct sum of its primary spaces:*

$$V = \bigoplus\nolimits_i V^{a_i}.$$

PROOF. Let $P(T)$ be a polynomial in $k[T]$ such that $P(\alpha) = 0$, and suppose that $P(T) = Q(T)R(T)$ with Q and R relatively prime. Then there exist polynomials $a(T)$ and $b(T)$ such that

$$a(T)Q(T) + b(T)R(T) = 1.$$

For any $v \in V$,

$$a(\alpha)Q(\alpha)v + b(\alpha)R(\alpha)v = v, \tag{95}$$

which implies immediately that $\mathrm{Ker}(Q(\alpha)) \cap \mathrm{Ker}(R(\alpha)) = 0$. Moreover, because $Q(\alpha)R(\alpha) = 0$, (95) expresses v as the sum of an element of $\mathrm{Ker}(R(\alpha))$ and an element of $\mathrm{Ker}(Q(\alpha))$. Thus, V is the direct sum of $\mathrm{Ker}(Q(\alpha))$ and $\mathrm{Ker}(P(\alpha))$.

On applying this remark repeatedly, we find that

$$V = \mathrm{Ker}(T - a_1)^{n_1} \oplus \mathrm{Ker}((T - a_2)^{n_2} \cdots (T - a_r)^{n_r}) = \cdots = \bigoplus\nolimits_i \mathrm{Ker}(T - a_i)^{n_i},$$

as claimed. □

THEOREM 2.2 *Let V be a finite-dimensional vector space over a perfect field. For any automorphism α of V, there exist unique automorphisms α_s and α_u of V such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, *and*

[4] This is Bourbaki's terminology (LIE VII, §1); "generalized eigenspace" is also used.

[4] By this I mean that there exists an N_0 such that the statement holds for all positive integers divisible by N_0, i.e., that N is sufficiently large for the partial ordering

$$M \leq N \iff M \text{ divides } N.$$

(b) α_s *is semisimple and* α_u *is unipotent.*

Moreover, each of α_s *and* α_u *is a polynomial in* α.

PROOF. Assume first that α has all of its eigenvalues in k, so that V is a direct sum of the primary spaces of α, say, $V = \bigoplus_{1 \leq i \leq m} V^{a_i}$ where the a_i are the distinct roots of P_α. Define α_s to be the automorphism of V that acts as a_i on V^{a_i} for each i. Then α_s is a semisimple automorphism of V, and $\alpha_u \overset{\text{def}}{=} \alpha \circ \alpha_s^{-1}$ commutes with α_s (because it does on each V^{a_i}) and is unipotent (because its eigenvalues are 1). Thus α_s and α_u satisfy (a) and (b).

Because the polynomials $(T - a_i)^{n_i}$ are relatively prime, the Chinese remainder theorem shows that there exists a $Q(T) \in k[T]$ such that

$$Q(T) \equiv a_i \bmod (T - a_i)^{n_i}, \qquad i = 1, \ldots, m.$$

Then $Q(\alpha)$ acts as a_i on V^{a_i} for each i, and so $\alpha_s = Q(\alpha)$, which is a polynomial in α. Similarly, $\alpha_s^{-1} \in k[\alpha]$, and so $\alpha_u \overset{\text{def}}{=} \alpha \circ \alpha_s^{-1} \in k[\alpha]$.

It remains to prove the uniqueness of α_s and α_u. Let $\alpha = \beta_s \circ \beta_\alpha$ be a second decomposition satisfying (a) and (b). Then β_s and β_α commute with α, and therefore also with α_s and α_u (because they are polynomials in α). It follows that $\beta_s^{-1}\alpha_s$ is semisimple and that $\alpha_u \beta_\alpha^{-1}$ is unipotent. Since they are equal, both must equal 1. This completes the proof in this case.

In the general case, because k is perfect, there exists a finite Galois extension k' of k such that α has all of its eigenvalues in k'. Choose a basis for V, and use it to attach matrices to endomorphisms of V and $k' \otimes_k V$. Let A be the matrix of α. The first part of the proof allows us to write $A = A_s A_\alpha = A_\alpha A_s$ with A_s a semisimple matrix and A_α a unipotent matrix with entries in k'; moreover, this decomposition is unique.

Let $\sigma \in \mathrm{Gal}(k'/k)$, and for a matrix $B = (b_{ij})$, define σB to be (σb_{ij}). Because A has entries in k, $\sigma A = A$. Now

$$A = (\sigma A_s)(\sigma A_\alpha)$$

is again a decomposition of A into commuting semisimple and unipotent matrices. By the uniqueness of the decomposition, $\sigma A_s = A_s$ and $\sigma A_\alpha = A_\alpha$. Since this is true for all $\sigma \in \mathrm{Gal}(K/k)$, the matrices A_s and A_α have entries in k. Now $\alpha = \alpha_s \circ \alpha_u$, where α_s and α_u are the endomorphisms with matrices A_s and A_α, is a decomposition of α satisfying (a) and (b).

Finally, the first part of the proof shows that there exist $a_i \in k'$ such that

$$A_s = a_0 + a_1 A + \cdots + a_{n-1} A^{n-1} \qquad (n = \dim V).$$

The a_i are unique, and so, on applying σ, we find that they lie in k. Therefore,

$$\alpha_s = a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \in k[\alpha].$$

Similarly, $\alpha_u \in k[\alpha]$. □

The automorphisms α_s and α_u are called the ***semisimple*** and ***unipotent parts*** of α, and

$$\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$$

is the ***(multiplicative) Jordan decomposition*** of α.

PROPOSITION 2.3 *Let α and β be automorphisms of vector spaces V and W over a perfect field, and let $\varphi\colon V \to W$ be a linear map. If $\varphi\circ\alpha = \beta\circ\varphi$, then $\varphi\circ\alpha_s = \beta_s\circ\varphi$ and $\varphi\circ\alpha_u = \beta_\alpha\circ\varphi$.*

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k. Recall that α_s acts on each primary space V^a, $a\in k$, as multiplication by a. As φ obviously maps V^a into W^a, it follows that $\varphi\circ\alpha_s = \beta_s\circ\varphi$. Similarly, $\varphi\circ\alpha_s^{-1} = \beta_s^{-1}\circ\varphi$, and so $\varphi\circ\alpha_u = \beta_\alpha\circ\varphi$. □

COROLLARY 2.4 *Every subspace W of V stable under α is stable under α_s and α_u, and $\alpha|W = \alpha_s|W\circ\alpha_u|W$ is the Jordan decomposition of $\alpha|W$.*

PROOF. It follows from the proposition that W is stable under α_s and α_u, and it is obvious that the decomposition $\alpha|W = \alpha_s|W\circ\alpha_u|W$ has the properties to be the Jordan decomposition. □

PROPOSITION 2.5 *For any automorphisms α and β of vector spaces V and W over a perfect field,*

$$(\alpha\otimes\beta)_s = \alpha_s\otimes\beta_s$$
$$(\alpha\otimes\beta)_\alpha = \alpha_u\otimes\beta_\alpha.$$

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k. For any $a,b\in k$, $V^a\otimes_k W^b \subset (V\otimes_k W)^{ab}$, and so $\alpha_s\otimes\beta_s$ and $(\alpha\otimes\beta)_s$ both act on $V_a\otimes_k W_b$ as multiplication by ab. This shows that $(\alpha\otimes\beta)_s = \alpha_s\otimes\beta_s$. Similarly, $(\alpha_s^{-1}\otimes\beta_s^{-1}) = (\alpha\otimes\beta)_s^{-1}$, and so $(\alpha\otimes\beta)_\alpha = \alpha_u\otimes\beta_\alpha$. □

2.6 Let k be a nonperfect field of characteristic 2, so that there exists an $a\in k$ that is not a square in k, and let $M = \left(\begin{smallmatrix}0&1\\a&0\end{smallmatrix}\right)$. In the algebraic closure of k, M has the Jordan decomposition

$$M = \begin{pmatrix}\sqrt{a} & 0\\ 0 & \sqrt{a}\end{pmatrix}\begin{pmatrix}0 & 1/\sqrt{a}\\ \sqrt{a} & 0\end{pmatrix}.$$

These matrices do not have coefficients in k, and so, if M had a Jordan decomposition in $M_2(k)$, it would have two distinct Jordan decompositions in $M_2(k^{\mathrm{al}})$, contradicting the uniqueness.

Infinite-dimensional vector spaces

Let V be a vector space, possibly infinite dimensional, over a perfect field k. An endomorphism α of V is ***locally finite*** if V is a union of finite-dimensional subspaces stable under α. A locally finite endomorphism is ***semisimple*** (resp. ***locally nilpotent***, ***locally unipotent***) if its restriction to each stable finite-dimensional subspace is semisimple (resp. nilpotent, unipotent).

Let α be a locally finite automorphism of V. By assumption, every $v\in V$ is contained in a finite-dimensional subspace W stable under α, and we define $\alpha_s(v) = (\alpha|W)_s(v)$. According to (2.2), this is independent of the choice of W, and so in this way we get a semisimple automorphism of V. Similarly, we can define α_u. Thus:

THEOREM 2.7 *For any locally finite automorphism α of V, there exist unique automorphisms α_s and α_u such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, *and*
(b) α_s *is semisimple and* α_u *is locally unipotent.*

For any finite-dimensional subspace W of V stable under α,

$$\alpha|W = (\alpha_s|W) \circ (\alpha_u|W) = (\alpha_u|W) \circ (\alpha_s|W)$$

is the Jordan decomposition of $\alpha|W$.

Jordan decompositions in algebraic groups

Finally, we are able to prove the following important theorem.

THEOREM 2.8 *Let G be an algebraic group over a perfect field k. For any $g \in G(k)$ there exist unique elements $g_s, g_u \in G(k)$ such that, for all representations (V, r_V) of G, $r_V(g_s) = r_V(g)_s$ and $r_V(g_u) = r_V(g)_u$. Furthermore,*

$$g = g_s g_u = g_u g_s. \tag{96}$$

PROOF. In view of (2.3) and (2.5), the first assertion follows immediately from (1.2) applied to the families $(r_V(g)_s)_V$ and $(r_V(g)_u)_V$. Now choose a faithful representation r_V. Because

$$r_V(g) = r_V(g_s) r_V(g_u) = r_V(g_u) r_V(g_s),$$

(96) follows. □

The elements g_s and g_u are called the ***semisimple*** and ***unipotent parts*** of g, and $g = g_s g_u$ is the ***Jordan decomposition*** of g.

2.9 To check that a decomposition $g = g_s g_u$ is the Jordan decomposition, it suffices to check that $r(g) = r(g_s) r(g_u)$ is the Jordan decomposition of $r(g)$ for a single faithful representation of G.

2.10 Homomorphisms of groups preserve Jordan decompositions. To see this, let $u\colon G \to G'$ be a homomorphism and let $g = g_s g_u$ be a Jordan decomposition in $G(k)$. For any representation $\varphi\colon G' \to \mathrm{GL}_V$, $\varphi \circ u$ is a representation of G, and so $(\varphi \circ u)(g) = ((\varphi \circ u)(g_s)) \cdot ((\varphi \circ u)(g_u))$ is the Jordan decomposition in $\mathrm{GL}(V)$. If we choose φ to be faithful, this implies that $u(g) = u(g_s) \cdot u(g_u)$ is the Jordan decomposition of $u(g)$.

NOTES Our proof of the existence of Jordan decompositions (Theorem 2.8) is the standard one, except that we have made Lemma 1.1 explicit. As Borel has noted (1991, p. 88; 2001, VIII 4.2, p. 169), the result essentially goes back to Kolchin 1948, 4.7.

3 Characterizations of categories of representations

Pontryagin duality has two parts. First it shows that a locally compact abelian group G can be recovered from its dual $G^{\vee}$. This it does by showing that the canonical map $G \to G^{\vee\vee}$ is an isomorphism. Secondly, it characterizes the abelian groups that arise as dual groups. For example, it shows that the duals of discrete abelian groups are exactly the compact abelian groups, and that the duals of locally compact abelian groups are exactly the locally compact abelian groups.

In Theorem 1.2 we showed how to recover an algebraic group G from its "dual" $\mathsf{Rep}(G)$ (reconstruction theorem). In this section, we characterize the categories that arise as the category of representations of an algebraic or affine group (*description* or *recognition theorem*).

Throughout this section, k is a field.

Categories of comodules

An additive category C is said to be k***-linear*** if the Hom sets are k-vector spaces and composition is k-bilinear. Functors of k-linear categories are required to be k-linear, i.e., the maps $\mathrm{Hom}(a,b) \to \mathrm{Hom}(Fa, Fb)$ defined by F are required to be k-linear.

For example, if C is k-coalgebra, then $\mathsf{Comod}(C)$ is a k-linear category. In fact, $\mathsf{Comod}(C)$ is a k-linear abelian category (VIII, §5), and the forgetful functor $\omega\colon \mathsf{Comod}(C) \to \mathsf{Vec}_k$ is exact, faithful, and k-linear. The next theorem provides a converse to this statement.

THEOREM 3.1 *Let C be an essentially small*[6] *k-linear abelian category, and let $\omega\colon \mathsf{C} \to \mathsf{Vec}_k$ be an exact faithful k-linear functor. Then there exists a coalgebra C such that C is equivalent to the category of C-comodules of finite dimension.*

The proof will occupy the rest of this section.

Because ω is faithful, $\omega(\mathrm{id}_X) = \omega(0)$ if and only if $\mathrm{id}_X = 0$, and so $\omega(X)$ is the zero object if and only if X is the zero object. It follows that, if $\omega(u)$ is a monomorphism (resp. an epimorphism, resp. an isomorphism), then so also is u. For objects X, Y of C, $\mathrm{Hom}(X,Y)$ is a subspace of $\mathrm{Hom}(\omega X, \omega Y)$, and hence has finite dimension over k.

For monomorphisms $X \xrightarrow{x} Y$ and $X' \xrightarrow{x'} Y$ with the same target, we write $x \le x'$ if there exists a morphism $X \to X'$ (necessarily unique) giving a commutative triangle. The lattice of subobjects of Y is obtained from the collection of monomorphisms by identifying two monomorphisms x and x' if $x \le x'$ and $x' \le x$. The functor ω maps the lattice of subobjects of Y injectively[7] to the lattice of subspaces of ωY. Hence X has finite length.

Similarly ω maps the lattice of quotient objects of Y injectively to the lattice of quotient spaces of ωY.

For X in C, we let $\langle X\rangle$ denote the full subcategory of C whose objects are the quotients of subobjects of direct sums of copies of X. For example, if C is the category of finite-dimensional comodules over a coalgebra C, then $\langle X\rangle$ is the category of finite-dimensional comodules over C_X (see VIII, 11.1).

[6] A category is essentially small if it is locally small and it admits a set of representatives for its isomorphism classes of objects.

[7] If $\omega(X) = \omega(X')$, then the kernel of

$$\binom{x}{x'}\colon X \times X' \to Y$$

projects isomorphically onto each of X and X' (because it does after ω has been applied).

Let X be an object of C, and let S be a subset of $\omega(X)$. The intersection of the subobjects Y of X such that $\omega(Y) \supset S$ is the smallest subobject with this property — we call it the subobject of X ***generated*** by S.

An object Y is ***monogenic*** if it is generated by a single element, i.e., there exists a $y \in \omega(Y)$ such that

$$Y' \subset Y,\ y \in \omega(Y') \implies Y' = Y.$$

Proof in the case that C *is generated by a single object*

In the next three lemmas, we assume that $\mathsf{C} = \langle X \rangle$ for some X.

LEMMA 3.2 *For every monogenic object Y of* C,

$$\dim_k \omega(Y) \leq (\dim_k \omega(X))^2.$$

PROOF. By hypothesis, there are maps $Y \xleftarrow{\text{onto}} Y_1 \hookrightarrow X^m$. Let y_1 be an element of $\omega(Y_1)$ whose image y in $\omega(Y)$ generates Y, and let Z be the subobject of Y_1 generated by y_1. The image of Z in Y contains y and so equals Y. Hence it suffices to prove the lemma for Z, i.e., we may suppose that $Y \subset X^m$ for some m. We shall deduce that $Y \hookrightarrow X^{m'}$ for some $m' \leq \dim_k \omega(X)$, from which the lemma follows.

Suppose that $m > \dim_k \omega(X)$. The generator y of Y lies in $\omega(Y) \subset \omega(X^m) = \omega(X)^m$. Let $y = (y_1, \ldots, y_m)$ in $\omega(X)^m$. Since $m > \dim_k \omega(X)$, there exist $a_i \in k$, not all zero, such that $\sum a_i y_i = 0$. The a_i define a surjective morphism $X^m \to X$ whose kernel N is isomorphic to X^{m-1}.[8] As $y \in \omega(N)$, we have $Y \subset N$, and so Y embeds into X^{m-1}. Continue in this fashion until $Y \subset X^{m'}$ with $m' \leq \dim_k \omega(X)$. □

As $\dim_k \omega(Y)$ can take only finitely many values when Y is monogenic, there exists a monogenic P for which $\dim_k \omega(P)$ has its largest possible value. Let $p \in \omega(P)$ generate P.

LEMMA 3.3 (a) *The pair (P, p) represents the functor ω.*

(b) *The object P is a projective generator for* C, *i.e., the functor* $\operatorname{Hom}(P, -)$ *is exact and faithful.*

PROOF. (a) Let X be an object of C, and let $x \in \omega(X)$; we have to prove that there exists a unique morphism $f\colon P \to X$ such that $\omega(f)$ sends p to x. The uniqueness follows from the fact p generates P (the equalizer E of two f's is a subobject of P such that $\omega(E)$ contains p). To prove the existence, let Q be the smallest subobject of $P \times X$ such that $\omega(Q)$ contains (p, x). The morphism $Q \to P$ defined by the projection map is surjective because P is generated by p. Therefore,

$$\dim_k \omega(Q) \geq \dim_k \omega(P),$$

but because $\dim_k(\omega(P))$ is maximal, equality must hold, and so $Q \to P$ is an isomorphism. The composite of its inverse with the second projection $Q \to X$ is a morphism $P \to X$ sending p to x.

[8] Extend $(a_1, \ldots, a_m)$ to an invertible matrix $\begin{pmatrix} a_1, \ldots, a_m \\ A \end{pmatrix}$; then $A\colon X^m \to X^{m-1}$ defines an isomorphism of N onto X^{m-1}, because $\omega(A)$ is an isomorphism $\omega(N) \to \omega(X)^{m-1}$.

(b) The object P is projective because ω is exact, and it is a generator because ω is faithful. □

Let $A = \mathrm{End}(P)$ — it is a k-algebra of finite dimension as a k-vector space (not necessarily commutative) — and let h^P be the functor $X \rightsquigarrow \mathrm{Hom}(P,X)$.

LEMMA 3.4 *The functor h^P is an equivalence from C to the category of right A-modules of finite dimension over k. Its composite with the forgetful functor is canonically isomorphic to ω.*

PROOF. Because P is a projective generator, h^P is exact and faithful. It remains to prove that it is essentially surjective and full.

Let M be a right A-module of finite dimension over k, and choose a finite presentation for M,

$$A^m \xrightarrow{u} A^n \to M \to 0$$

where u is an $m \times n$ matrix with coefficients in A. This matrix defines a morphism $P^m \to P^n$ whose cokernel X has the property that $h^P(X) \simeq M$. Therefore h^P is essentially surjective.

We have just shown that every object X in C occurs in an exact sequence

$$P^m \xrightarrow{u} P^n \to X \to 0.$$

Let Y be a second object of C. Then

$$\mathrm{Hom}(P^m,Y) \simeq h^P(Y)^m \simeq \mathrm{Hom}(A^m,h^P(Y)) \simeq \mathrm{Hom}(h^P(P^m),h^P(Y)),$$

and the composite of these maps is that defined by h^P. From the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(X,Y) \arrow[r] \arrow[d] & \mathrm{Hom}(P^n,Y) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom}(P^m,Y) \arrow[d, "\simeq"] \\
0 \arrow[r] & \mathrm{Hom}(h^P(X),h^P(Y)) \arrow[r] & \mathrm{Hom}(A^n,h^P(Y)) \arrow[r] & \mathrm{Hom}(A^m,h^P(Y))
\end{tikzcd}$$

we see that $\mathrm{Hom}(X,Y) \to \mathrm{Hom}(h^P(X),h^P(Y))$ is an isomorphism, and so h^P is full.

For the second statement,

$$\omega(X) \simeq \mathrm{Hom}(P,X) \simeq \mathrm{Hom}(h^P(P),h^P(X)) = \mathrm{Hom}(A,h^P(X)) \simeq h^P(X).$$ □

As A is a finite k-algebra, its linear dual $C = A^\vee$ is a k-coalgebra, and to give a right A-module structure on a k-vector space is the same as giving a left C-comodule structure (see VIII, 4.4). Together with (3.4), this completes the proof in the case that $\mathsf{C} = \langle X \rangle$. Note that

$$A \overset{\text{def}}{=} \mathrm{End}(P) \simeq \mathrm{End}(h^P) \simeq \mathrm{End}(\omega),$$

and so

$$C \simeq \mathrm{End}(\omega)^\vee,$$

i.e., the coalgebra C is the k-linear dual of the algebra $\mathrm{End}(\omega)$.

EXAMPLE 3.5 Let A be a finite k-algebra (not necessarily commutative). Because A is finite, its dual $A^{\vee}$ is a coalgebra (II, §3), and we saw in (VIII, 4.4) that left A-module structures on k-vector space correspond to right $A^{\vee}$-comodule structures. If we take C to be $\mathsf{Mod}(A)$, ω to the forgetful functor, and X to be A regarded as a left A-module, then

$$\mathrm{End}(\omega|\langle X\rangle)^{\vee} \simeq A^{\vee},$$

and the equivalence of categories $\mathsf{C} \to \mathsf{Comod}(A^{\vee})$ in (3.6) simply sends an A-module V to V with its canonical $A^{\vee}$-comodule structure. This is explained in detail in (3.9) and (3.10).

Proof in the general case

We now consider the general case. For an object X of C, let $A_X = \mathrm{End}(\omega|\langle X\rangle)$, and let $C_X = A_X^{\vee}$. For each Y in $\langle X\rangle$, A_X acts on $\omega(Y)$ on the left, and so $\omega(Y)$ is a right C_X-comodule; moreover, $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories

$$\langle X\rangle \to \mathsf{Comod}(C_X).$$

Define a partial ordering on the set of isomorphism classes of objects in C by the rule:

$$[X] \leq [Y] \text{ if } \langle X\rangle \subset \langle Y\rangle.$$

Note that $[X], [Y] \leq [X \oplus Y]$, so that we get a directed set, and that if $[X] \leq [Y]$, then restriction defines a homomorphism $A_Y \to A_X$. When we pass to the limit over the isomorphism classes, we obtain the following more precise form of the theorem.

THEOREM 3.6 *Let C be an essentially small k-linear abelian category and let $\omega\colon \mathsf{C} \to \mathsf{Vec}_k$ be a k-linear exact faithful functor. Let $C(\omega)$ be the k-coalgebra $\varinjlim_{[X]} \mathrm{End}(\omega|\langle X\rangle)^{\vee}$. For each object Y in C, the vector space $\omega(Y)$ has a natural structure of a right $C(\omega)$-comodule, and the functor $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories $\mathsf{C} \to \mathsf{Comod}(C(\omega))$.*

ASIDE 3.7 Let C be a k-linear abelian category with a tensor product structure (cf. 3.13). A ***coalgebra in*** C is an object C of C together with morphisms $\Delta\colon C \to C \otimes C$ and $\epsilon\colon C \to k$ such that the diagrams (15), p.30, commute. Similarly, it is possible to define the notion of a ***C-comodule in*** C. Assume that there exists an exact faithful k-linear functor to Vec_k preserving tensor products, and that C admits duals and a generator X. Then there exists a coalgebra C *in* C together with a coaction of C on each object of C such that, for every exact faithful k-linear functor ω to Vec_k preserving tensor products, $\omega(C) \simeq \mathrm{End}(\omega)^{\vee}$ (as coalgebras) and ω preserves the comodule structures. Moreover, the tensor product makes C into a bialgebra in C, which is a Hopf algebra. In fact, we can take $C = (X^{\vee} \otimes X)^{\vee}$.

ASIDE 3.8 For the proof of Theorem 3.6, we have followed Serre 1993, 2.5. For a slightly different proof, see Deligne and Milne 1982, §2, or Saavedra Rivano 1972. It is also possible to deduce it from Grothendieck's theorem on the pro-representability of right exact functors.

Categories of comodules over a bialgebra

Let C be a coalgebra over k. We saw in (VIII, §5), that a bialgebra structure on C defines a tensor product structure on $\mathsf{Comod}(C)$, and that an inversion on C defines duals. In this section we prove the converse: a tensor product structure on $\mathsf{Comod}(C)$ defines a bialgebra structure on C, and the existence of duals implies the existence of an inversion.

3.9 Let A be a finite k-algebra (not necessarily commutative), and let R be a commutative k-algebra. Consider the functors

$$\mathsf{Mod}(A) \xrightarrow[\text{forget}]{\omega} \mathsf{Vec}(k) \xrightarrow[V \rightsquigarrow R\otimes_k V]{\phi_R} \mathsf{Mod}(R).$$

For $M \in \mathrm{ob}(\mathsf{Mod}(A))$, let $M_0 = \omega(M)$. An element λ of $\mathrm{End}(\phi_R \circ \omega)$ is a family of R-linear maps

$$\lambda_M : R \otimes_k M_0 \to R \otimes_k M_0,$$

functorial in M. An element of $R \otimes_k A$ defines such a family, and so we have a map

$$u : R \otimes_k A \to \mathrm{End}(\phi_R \circ \omega),$$

which we shall show to be an isomorphism by defining an inverse β. Let $\beta(\lambda) = \lambda_A(1 \otimes 1)$. Clearly $\beta \circ u = \mathrm{id}$, and so we only have to show $u \circ \beta = \mathrm{id}$. The A-module $A \otimes_k M_0$ is a direct sum of copies of A, and the additivity of λ implies that $\lambda_{A \otimes M_0} = \lambda_A \otimes \mathrm{id}_{M_0}$. The map $a \otimes m \mapsto am : A \otimes_k M_0 \to M$ is A-linear, and hence

$$\begin{tikzcd}
R \otimes_k A \otimes_k M_0 \arrow[r] \arrow[d, "\lambda_A \otimes \mathrm{id}_{M_0}"] & R \otimes_k M \arrow[d, "\lambda_M"] \\
R \otimes_k A \otimes_k M_0 \arrow[r] & R \otimes_k M
\end{tikzcd}$$

commutes. Therefore

$$\lambda_M(1 \otimes m) = \lambda_A(1) \otimes m = (u \circ \beta(\lambda))_M(1 \otimes m) \text{ for } 1 \otimes m \in R \otimes M,$$

i.e., $u \circ \beta = \mathrm{id}$.

3.10 Let C be a k-coalgebra, and let ω be the forgetful functor on $\mathsf{Comod}(C)$. When C is finite over k, to give an object of $\mathsf{Comod}(C)$ is essentially the same as giving a finitely generated module over the k-algebra $A = C^\vee$ (VIII, 4.4), and so (3.9) shows that

$$C \simeq \mathrm{End}(\omega)^\vee.$$

In the general case,

$$C \simeq \varinjlim_{[X]} C_X \simeq \varinjlim_{[X]} \mathrm{End}(\omega_C | \langle X \rangle)^\vee. \tag{97}$$

Let $u : C \to C'$ be a homomorphism of k-coalgebras. A coaction $V \to V \otimes C$ of C on V defines a coaction $V \to V \otimes C'$ of C' on V by composition with $\mathrm{id}_V \otimes u$. Thus, u defines a functor $F : \mathsf{Comod}(C) \to \mathsf{Comod}(C')$ such that

$$\omega_{C'} \circ F = \omega_C. \tag{98}$$

Lemma 3.11 *Every functor $F : \mathsf{Comod}(C) \to \mathsf{Comod}(C')$ satisfying (98) arises, as above, from a unique homomorphism of k-coalgebras $C \to C'$.*

PROOF. The functor F defines a homomorphism

$$\varinjlim_{[X]} \mathrm{End}(\omega_{C'}|\langle FX\rangle) \to \varinjlim_{[X]} \mathrm{End}(\omega_C|\langle X\rangle),$$

and $\varinjlim_{[X]} \mathrm{End}(\omega_{C'}|\langle FX\rangle)$ is a quotient of $\varinjlim_{[Y]} \mathrm{End}(\omega_{C'}|\langle Y\rangle)$. On passing to the duals, we get a homomorphism

$$\varinjlim \mathrm{End}(\omega_C|\langle X\rangle)^{\vee} \to \varinjlim \mathrm{End}(\omega_{C'}|\langle Y\rangle)^{\vee}$$

and hence a homomorphism $C \to C'$. This has the required property. □

Let C be a coalgebra over k. Recall (II, 2.3) that $C \otimes C$ is again a coalgebra over k. A coalgebra homomorphism $m: C \otimes C \to C$ defines a functor

$$\phi^m: \mathsf{Comod}(C) \times \mathsf{Comod}(C) \to \mathsf{Comod}(C)$$

sending (V, W) to $V \otimes W$ with the coaction

$$V \otimes W \xrightarrow{\rho_V \otimes \rho_W} V \otimes C \otimes W \otimes C \simeq V \otimes W \otimes C \otimes C \xrightarrow{V \otimes W \otimes m} V \otimes W \otimes C$$

(cf. VIII, 4.2b, §5).

PROPOSITION 3.12 *The map $m \mapsto \phi^m$ defines a one-to-one correspondence between the set of k-coalgebra homomorphisms $m: C \otimes C \to C$ and the set of k-bilinear functors*

$$\phi: \mathsf{Comod}(C) \times \mathsf{Comod}(C) \to \mathsf{Comod}(C)$$

such that $\phi(V, W) = V \otimes W$ as k-vector spaces.

(a) *The homomorphism m is associative (i.e., the diagram in (14), p.29, commutes) if and only if the canonical isomorphisms of vector spaces*

$$u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w: U \otimes (V \otimes W) \to (U \otimes V) \otimes W$$

are isomorphisms of C-comodules for all C-comodules U, V, W.

(b) *The homomorphism m is commutative (i.e., $m(a,b) = m(b,a)$ for all $a, b \in C$) if and only if the canonical isomorphisms of vector spaces*

$$v \otimes w \mapsto w \otimes v: V \otimes W \to W \otimes V$$

are isomorphisms of C-comodules for all C-comodules W, V.

(c) *There is an identity map $e: k \to C$ (i.e., a k-linear map such that the right hand diagram in (14) p.29, commutes) if and only if there exists a C-comodule U with underlying vector space k such that the canonical isomorphisms of vector spaces*

$$U \otimes V \simeq V \simeq V \otimes U$$

are isomorphisms of C-comodules for all C-comodules V.

PROOF. The pair $(\mathsf{Comod}(C)\times\mathsf{Comod}(C),\omega\otimes\omega)$, with $(\omega\otimes\omega)(X,Y)=\omega(X)\otimes\omega(Y)$ (as a k-vector space), satisfies the conditions of (3.6), and $\varinjlim \mathrm{End}(\omega\otimes\omega|\langle(X,Y)\rangle)^\vee = C\otimes C$. Thus

$$(\mathsf{Comod}(C)\times\mathsf{Comod}(C),\omega_C\otimes\omega_C)\simeq(\mathsf{Comod}(C\otimes C),\omega_{C\otimes C}),$$

and so the first statement of the proposition follows from (3.11). The remaining statements involve only routine checking. □

Let $\omega\colon\mathsf{A}\to\mathsf{B}$ be a faithful functor. We say that a morphism $\omega X\to\omega Y$ ***lives in*** A if it lies in $\mathrm{Hom}(X,Y)\subset\mathrm{Hom}(\omega X,\omega Y)$.

For k-vector spaces U,V,W, there are canonical isomorphisms

$$\begin{aligned}\phi_{U,V,W}&\colon U\otimes(V\otimes W)\to(U\otimes V)\otimes W, && u\otimes(v\otimes w)\mapsto(u\otimes v)\otimes w\\ \phi_{U,V}&\colon U\otimes V\to V\otimes U, && u\otimes v\mapsto v\otimes u.\end{aligned}$$

THEOREM 3.13 *Let* C *be an essentially small* k*-linear abelian category, and let* $\otimes\colon\mathsf{C}\times\mathsf{C}\to\mathsf{C}$ *be a* k*-bilinear functor. Let* $\omega\colon\mathsf{C}\to\mathsf{Vec}_k$ *be a* k*-linear exact faithful functor such that*

(a) $\omega(X\otimes Y)=\omega(X)\otimes\omega(Y)$ *for all* X,Y;
(b) *the isomorphisms* $\phi_{\omega X,\omega Y,\omega Z}$ *and* $\phi_{\omega X,\omega Y}$ *live in* C *for all* X,Y,Z;
(c) *there exists an (identity) object* $\mathbb{1}$ *in* C *such that* $\omega(\mathbb{1})=k$ *and the canonical isomorphisms*

$$\omega(\mathbb{1})\otimes\omega(X)\simeq\omega(X)\simeq\omega(X)\otimes\omega(\mathbb{1})$$

live in C.

Let $C(\omega)=\varinjlim\mathrm{End}(\omega|\langle X\rangle)^\vee$, *so that* ω *defines an equivalence of categories* $\mathsf{C}\to\mathsf{Comod}(C(\omega))$ *(Theorem 3.6). Then* $C(\omega)$ *has a unique structure* (m,e) *of a commutative* k*-bialgebra such that* $\otimes=\phi^m$ *and* $\omega(\mathbb{1})=(k\xrightarrow{e}C(\omega)\simeq k\otimes C(\omega))$.

PROOF. To give a bialgebra structure on a coalgebra (A,Δ,ϵ), one has to give coalgebra homomorphisms (m,e) such that m is commutative and associative and e is an identity map (II, 4.2; II, §9). Thus, the statement is an immediate consequence of Proposition 3.12. □

Categories of representations of affine groups

THEOREM 3.14 *Let* C *be an essentially small* k*-linear abelian category, let* $\otimes\colon\mathsf{C}\times\mathsf{C}\to\mathsf{C}$ *be a* k*-bilinear functor. Let* ω *be an exact faithful* k*-linear functor* $\mathsf{C}\to\mathsf{Vec}_k$ *satisfying the conditions (a), (b), and (c) of (3.13). For each* k*-algebra* R, *let* $G(R)$ *be the set of families*

$$(\lambda_V)_{V\in\mathrm{ob}(\mathsf{C})},\quad \lambda_V\in\mathrm{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

- ◇ $\lambda_{V\otimes W}=\lambda_V\otimes\lambda_W$ *for all* $V,W\in\mathrm{ob}(\mathsf{C})$,
- ◇ $\lambda_{\mathbb{1}}=\mathrm{id}_{\omega(\mathbb{1})}$ *for every identity object of* $\mathbb{1}$ *of* C, *and*
- ◇ $\lambda_W\circ\omega(u)_R=\omega(u)_R\circ\lambda_V$ *for all arrows* u *in* C.

Then G *is an affine monoid over* k, *and* ω *defines an equivalence of tensor categories,*

$$\mathsf{C}\to\mathsf{Rep}(G).$$

When ω *satisfies the following condition,* G *is an affine group:*

(d) *for any object X such that $\omega(X)$ has dimension* 1, *there exists an object X^{-1} in* C *such that $X \otimes X^{-1} \approx \mathbb{1}$.*

PROOF. Theorem 3.13 allows us to assume that $\mathsf{C} = \mathsf{Comod}(C)$ for C a k-bialgebra, and that $\otimes$ and ω are the natural tensor product structure and forgetful functor. Let G be the affine monoid corresponding to C. Using (3.9) we find that, for any k-algebra R,

$$\underline{\mathrm{End}}(\omega)(R) \overset{\text{def}}{=} \mathrm{End}(\phi_R \circ \omega) = \varprojlim \mathrm{Hom}_{k\text{-lin}}(C_X, R) = \mathrm{Hom}_{k\text{-lin}}(C, R).$$

An element $\lambda \in \mathrm{Hom}_{k\text{-lin}}(C_X, R)$ corresponds to an element of $\underline{\mathrm{End}}(\omega)(R)$ commuting with the tensor structure if and only if λ is a k-algebra homomorphism; thus

$$\underline{\mathrm{End}}^{\otimes}(\omega)(R) = \mathrm{Hom}_{k\text{-alg}}(C, R) = G(R).$$

We have shown that $\underline{\mathrm{End}}^{\otimes}(\omega)$ is representable by the affine monoid $G = \mathrm{Spec}\, C$ and that ω defines an equivalence of tensor categories

$$\mathsf{C} \to \mathsf{Comod}(C) \to \mathsf{Rep}_k(G).$$

On applying (d) to the highest exterior power of an object of C, we find that $\underline{\mathrm{End}}^{\otimes}(\omega) = \underline{\mathrm{Aut}}^{\otimes}(\omega)$, which completes the proof. □

REMARK 3.15 Let (C, ω) be $(\mathsf{Rep}_k(G)$,forget). On following through the proof of (3.14) in this case one recovers Theorem 1.2: $\underline{\mathrm{End}}^{\otimes}(\omega^G)$ is represented by G.

EXAMPLE 3.16 Let G be a connected complex Lie group, and let C be the category of analytic representations of G on finite-dimensional complex vector spaces. With the obvious functors $\otimes\colon \mathsf{C} \times \mathsf{C} \to \mathsf{C}$ and $\omega\colon \mathsf{C} \to \mathsf{Vec}_{\mathbb{C}}$, this satisfies the hypotheses of Theorem 3.13, and so is the category of representations of an affine group $A(G)$. Almost by definition, there exists a homomorphism $P\colon G \to A(G)(\mathbb{C})$ such that, for every analytic representation (V, ρ) of G, there exists a unique representation $(V, \widehat{\rho})$ of $A(G)$ such that $\widehat{\rho} = \rho \circ P$. The group $A(G)$ is sometimes called the Hochschild-Mostow group (for a brief exposition of the work of Hochschild and Mostow, see Magid, Andy, Notices AMS, Sept. 2011, p.1089; should add more on the history of these things).

NOTES Add discussion of how much of this section extends to base rings k. (Cf. mo3131.) See Schäppi 2011, arXiv:1112.5213 and the references therein.

4 Homomorphisms and functors

Throughout this section, k is a field. A homomorphism $f\colon G' \to G$ of affine groups over k defines an exact faithful functor

$$(V, r) \rightsquigarrow (V, r \circ f)\colon \mathsf{Rep}(G) \to \mathsf{Rep}(G'),$$

which we denote ω^f. For example, if G' is the trivial group, then ω^f is the forgetful functor ω_G.

PROPOSITION 4.1 *A homomorphism $f\colon G \to Q$ of affine groups is surjective if and only if ω^f is fully faithful and every subobject of an object in the essential image*[9] *of ω^f is also in the essential image.*

PROOF. If f is a quotient map, then ω^f identifies $\mathsf{Rep}(Q)$ with the full subcategory of $\mathsf{Rep}(G)$ of representations $r\colon G \to \mathrm{GL}_V$ factoring through Q. It is therefore obvious that ω^f has the stated properties. Conversely, the hypotheses imply that ω^f defines an equivalence of $\mathsf{Rep}(Q)$ with a full subcategory of $\mathsf{Rep}(G)$, and that its restriction to $\langle X\rangle \to \langle \omega^f(X)\rangle$ is an equivalence for each object X of $\mathsf{Rep}(Q)$; in particular,

$$\mathrm{End}(\omega_Q|\langle X\rangle)^\vee \simeq \mathrm{End}(\omega_G|\langle\omega^f(X)\rangle)^\vee.$$

Now

$$\begin{aligned}\mathcal{O}(Q) = \varinjlim_{[X]} \mathrm{End}(\omega_Q|\langle X\rangle)^\vee &\simeq \varinjlim_{[X]} \mathrm{End}(\omega_G|\langle\omega^f(X)\rangle)^\vee \\ &\subset \varinjlim_{[Y]} \mathrm{End}(\omega_G|\langle Y\rangle)^\vee = \mathcal{O}(G),\end{aligned}$$

where X (resp. Y) runs over a set of representatives for the isomorphism classes of objects in $\mathsf{Rep}(Q)$ (resp. $\mathsf{Rep}(G)$). Because $\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective, it is faithfully flat (VI, 11.1), and so $G \to Q$ is a quotient map. □

REMARK 4.2 When $\mathsf{Rep}(G)$ is semisimple, the second hypothesis in the proposition is superfluous: $f\colon G \to Q$ is a quotient map if and only if ω^f is fully faithful. (Let X be in the essential image, and let Y be a subobject of X; because $\mathsf{Rep}(G)$ is semisimple, there exists an endomorphism u of X such that $uX = Y$; because ω^f is fully faithful, u lives in $\mathsf{Rep}(Q)$.)

PROPOSITION 4.3 *A homomorphism $f\colon H \to G$ of affine groups is injective if and only if every object of $\mathsf{Rep}(H)$ is a subquotient of an object in the essential image of ω^f.*

PROOF. Let C be the strictly full subcategory of $\mathsf{Rep}(H)$ whose objects are subquotients of objects in the essential image of ω^f. The functors

$$\mathsf{Rep}(G) \to \mathsf{C} \to \mathsf{Rep}(H)$$

correspond to homomorphisms of k-bialgebras

$$\mathcal{O}(G) \to C \to \mathcal{O}(H).$$

An argument as in the proof of Proposition 4.1 shows that $C \to \mathcal{O}(H)$ is injective. Moreover,

$$\mathrm{End}(\omega_H|\langle\omega^f(X)\rangle) \to \mathrm{End}(\omega_G|\langle X\rangle)$$

is injective for every object X of $\mathsf{Rep}(G)$, and so $\mathcal{O}(G) \to C$ is surjective:

$$\mathcal{O}(G) \twoheadrightarrow C \hookrightarrow \mathcal{O}(H).$$

If f is injective, then $\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective and it follows that $C \xrightarrow{\simeq} \mathcal{O}(H)$, and so $\mathsf{C} = \mathsf{Rep}(H)$. Conversely, if $\mathsf{C} = \mathsf{Rep}(H)$, then $C = \mathcal{O}(H)$ and $\mathcal{O}(H) \to \mathcal{O}(G)$ is surjective. □

[9] Recall that the essential image of a functor consists of the objects isomorphic to an object in the actual image.

Let $f\colon H \to G$ be an injective homomorphism of affine algebraic groups. Let (V,r) be a faithful representation of G. Then $\omega^f(V,r) = (V, r \circ f)$ is a faithful representation of H, and so every finite-dimensional representation of H is isomorphic to a quotient of a subrepresentation of a direct sum of representations $\left(\omega^f(V,r) \oplus \omega^f(V,r)^\vee\right)^{\otimes m}$ (VIII, 11.7). This gives another proof of the sufficiency.

CHAPTER XI

The Lie Algebra of an Affine Group

The Lie algebra of an affine group is a linear approximation to the group. It holds a surprisingly large amount of information about the group, especially in characteristic zero, and especially for semisimple algebraic groups.

Throughout this chapter, k is a field (for the present).

1 Definition of a Lie algebra

DEFINITION 1.1 A ***Lie algebra***[1] over a field k is a vector space $\mathfrak{g}$ over k together with a k-bilinear map

$$[\ ,\ ]\colon \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$$

(called the ***bracket***) such that

(a) $[x,x]=0$ for all $x\in\mathfrak{g}$,
(b) $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ for all $x,y,z\in\mathfrak{g}$.

A ***homomorphism of Lie algebras*** is a k-linear map $u\colon\mathfrak{g}\to\mathfrak{g}'$ such that

$$u([x,y])=[u(x),u(y)]\quad\text{for all } x,y\in\mathfrak{g}.$$

A ***Lie subalgebra*** of a Lie algebra $\mathfrak{g}$ is a k-subspace $\mathfrak{s}$ such that $[x,y]\in\mathfrak{s}$ whenever $x,y\in\mathfrak{s}$ (i.e., such that $[\mathfrak{s},\mathfrak{s}]\subset\mathfrak{s}$).

Condition (b) is called the ***Jacobi identity***. Note that (a) applied to $[x+y,x+y]$ shows that the Lie bracket is skew-symmetric,

$$[x,y]=-[y,x],\text{ for all } x,y\in\mathfrak{g},\tag{99}$$

and that (99) allows the Jacobi identity to be rewritten as

$$[x,[y,z]]=[[x,y],z]+[y,[x,z]]\tag{100}$$

[1] Bourbaki LIE, Historical Notes to Chapter I to III writes:

> The term “Lie algebra” was introduced by H. Weyl in 1934; in his work of 1925, he had used the expression “infinitesimal group”. Earlier mathematicians had spoken simply of the “infinitesimal transformations $X_1f,\dots,X_rf$” of the group, which Lie and Engel frequently abbreviated by saying “the group $X_1f,\dots,X_rf$”.

or

$$[[x,y],z] = [x,[y,z]] - [y,[x,z]] \tag{101}$$

An injective homomorphism is sometimes called an ***embedding***, and a surjective homomorphism is sometimes called a ***quotient map***.

We shall be mainly concerned with finite-dimensional Lie algebras.

EXAMPLE 1.2 For any associative k-algebra A, the bracket $[a,b] = ab - ba$ is k-bilinear. It makes A into a Lie algebra because $[a,a]$ is obviously 0 and the Jacobi identity can be proved by a direct calculation. In fact, on expanding out the left side of the Jacobi identity for a,b,c one obtains a sum of 12 terms, 6 with plus signs and 6 with minus signs; by symmetry, each permutation of a,b,c must occur exactly once with a plus sign and exactly once with a minus sign. When A is the endomorphism ring $\mathrm{End}_{k\text{-lin}}(V)$ of a k-vector space V, this Lie algebra is denoted $\mathfrak{gl}_V$, and when $A = M_n(k)$, it is denoted $\mathfrak{gl}_n$. Let e_{ij} be the matrix with 1 in the ijth position and 0 elsewhere. These matrices form a basis for $\mathfrak{gl}_n$, and

$$[e_{ij}, e_{i'j'}] = \delta_{ji'} e_{ij'} - \delta_{ij'} e_{i'j} \quad (\delta_{ij} = \text{ Kronecker delta}).$$

EXAMPLE 1.3 Let A be a k-algebra (not necessarily associative). A ***derivation*** of A is a k-linear map $D\colon A \to A$ such that

$$D(ab) = D(a)b + a\,D(b) \text{ for all } a,b \in A.$$

The composite of two derivations need not be a derivation, but their bracket

$$[D,E] \overset{\text{def}}{=} D \circ E - E \circ D$$

is, and so the set of k-derivations $A \to A$ is a Lie subalgebra $\mathrm{Der}_k(A)$ of $\mathfrak{gl}_A$.

EXAMPLE 1.4 For $x \in \mathfrak{g}$, let $\mathrm{ad}_{\mathfrak{g}} x$ (or $\mathrm{ad}\, x$) denote the map $y \mapsto [x,y]\colon \mathfrak{g} \to \mathfrak{g}$. Then $\mathrm{ad}_{\mathfrak{g}} x$ is a k-derivation because (100) can be rewritten as

$$\mathrm{ad}(x)[y,z] = [\mathrm{ad}(x)y, z] + [y, \mathrm{ad}(x)z].$$

In fact, $\mathrm{ad}_{\mathfrak{g}}$ is a homomorphism of Lie algebras $\mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ because (101) can be rewritten as

$$\mathrm{ad}([x,y])z = \mathrm{ad}(x)(\mathrm{ad}(y)z) - \mathrm{ad}(y)(\mathrm{ad}(x)z).$$

The kernel of $\mathrm{ad}_{\mathfrak{g}}\colon \mathfrak{g} \to \mathrm{Der}_k(\mathfrak{g})$ is the ***centre*** of $\mathfrak{g}$,

$$z(\mathfrak{g}) \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid [x,\mathfrak{g}] = 0\}.$$

The derivations of $\mathfrak{g}$ of the form $\mathrm{ad}\, x$ are said to be ***inner*** (by analogy with the automorphisms of a group of the form $\mathrm{inn}\, g$).

2 The isomorphism theorems

An ***ideal*** in a Lie algebra $\mathfrak{g}$ is a subspace $\mathfrak{a}$ such that $[x,a] \in \mathfrak{a}$ for all $x \in \mathfrak{g}$ and $a \in \mathfrak{a}$ (i.e., such that $[\mathfrak{g},\mathfrak{a}] \subset \mathfrak{a}$). When $\mathfrak{a}$ is an ideal, the quotient vector space $\mathfrak{g}/\mathfrak{a}$ becomes a Lie algebra with the bracket

$$[x+\mathfrak{a}, y+\mathfrak{a}] = [x,y] + \mathfrak{a}.$$

The following statements are straightforward consequences of the similar statements for vector spaces.

2.1 (Existence of quotients). The kernel of a homomorphism $\mathfrak{g} \to \mathfrak{q}$ of Lie algebras is an ideal, and every ideal $\mathfrak{a}$ is the kernel of a quotient map $\mathfrak{g} \to \mathfrak{g}/\mathfrak{a}$.

2.2 (Homomorphism theorem). The image of a homomorphism $u\colon \mathfrak{g} \to \mathfrak{g}'$ of Lie algebras is a Lie subalgebra $u\mathfrak{g}$ of $\mathfrak{g}'$, and u defines an isomorphism of $\mathfrak{g}/\operatorname{Ker}(u)$ onto $u\mathfrak{g}$; in particular, every homomorphism of Lie algebras is the composite of a surjective homomorphism with an injective homomorphism.

2.3 (Isomorphism theorem). Let $\mathfrak{h}$ and $\mathfrak{a}$ be Lie subalgebras of $\mathfrak{g}$ such that $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$; then $\mathfrak{h} + \mathfrak{a}$ is a Lie subalgebra of $\mathfrak{g}$, $\mathfrak{h} \cap \mathfrak{a}$ is an ideal in $\mathfrak{h}$, and the map

$$x + \mathfrak{h} \cap \mathfrak{a} \mapsto x + \mathfrak{a}\colon \mathfrak{h}/\mathfrak{h} \cap \mathfrak{a} \to (\mathfrak{h} + \mathfrak{a})/\mathfrak{a}$$

is an isomorphism.

2.4 (Correspondence theorem). Let $\mathfrak{a}$ be an ideal in a Lie algebra $\mathfrak{g}$. The map $\mathfrak{h} \mapsto \mathfrak{h}/\mathfrak{a}$ is a one-to-one correspondence between the set of Lie subalgebras of $\mathfrak{g}$ containing $\mathfrak{a}$ and the set of Lie subalgebras of $\mathfrak{g}/\mathfrak{a}$. A Lie subalgebra $\mathfrak{h}$ containing $\mathfrak{a}$ is an ideal if and only if $\mathfrak{h}/\mathfrak{a}$ is an ideal in $\mathfrak{g}/\mathfrak{a}$, in which case the map

$$\mathfrak{g}/\mathfrak{h} \to (\mathfrak{g}/\mathfrak{a})/(\mathfrak{h}/\mathfrak{a})$$

is an isomorphism

3 The Lie algebra of an affine group

Let G be an affine group over a field k, and let $k[\varepsilon]$ be the ring of ***dual numbers***:

$$k[\varepsilon] \overset{\text{def}}{=} k[X]/(X^2).$$

Thus $k[\varepsilon] = k \oplus k\varepsilon$ as a k-vector space and $\varepsilon^2 = 0$. There is a homomorphism

$$\pi\colon k[\varepsilon] \longrightarrow k, \quad \pi(a + \varepsilon b) = a.$$

DEFINITION 3.1 For an affine group G over k,

$$\operatorname{Lie}(G) = \operatorname{Ker}(G(k[\varepsilon]) \xrightarrow{\pi} G(k)).$$

Following a standard convention, we often write $\mathfrak{g}$ for $\operatorname{Lie}(G)$, $\mathfrak{h}$ for $\operatorname{Lie}(H)$, and so on.

EXAMPLE 3.2 Let $G = \mathrm{GL}_n$, and let I_n be the identity $n \times n$ matrix. An $n \times n$ matrix A gives an element $I_n + \varepsilon A$ of $M_n(k[\varepsilon])$, and

$$(I_n + \varepsilon A)(I_n - \varepsilon A) = I_n;$$

therefore $I_n + \varepsilon A \in \operatorname{Lie}(\mathrm{GL}_n)$. Clearly every element of $\operatorname{Lie}(\mathrm{GL}_n)$ is of this form, and so the map

$$A \mapsto E(A) \overset{\text{def}}{=} I_n + \varepsilon A\colon M_n(k) \to \operatorname{Lie}(\mathrm{GL}_n)$$

is a bijection. Note that

$$\begin{aligned} E(A)E(B) &= (I_n + \varepsilon A)(I_n + \varepsilon B) \\ &= I_n + \varepsilon(A + B) \\ &= E(A + B). \end{aligned}$$

In the language of algebraic geometry, $\mathrm{Lie}(G)$ is the tangent space to $|G|$ at 1_G (see CA §18).

PROPOSITION 3.3 *Let I_G be the augmentation ideal in $\mathcal{O}(G)$, i.e., $I_G = \mathrm{Ker}(\epsilon\colon \mathcal{O}(G) \to k)$. Then*

$$\mathrm{Lie}(G) \simeq \mathrm{Hom}_{k\text{-}lin}(I_G/I_G^2, k). \tag{102}$$

PROOF. By definition, an element x of $\mathrm{Lie}(G)$ gives a commutative diagram

$$\begin{tikzcd} \mathcal{O}(G) \arrow[r, "x"] \arrow[d, "\epsilon"] & k[\varepsilon] \arrow[d, "\pi"] \\ k \arrow[r, equal] & k, \end{tikzcd}$$

and hence a homomorphism $I_G \to \mathrm{Ker}(\pi) \simeq k$ on the kernels. That this induces an isomorphism (102) is proved in CA 18.9. □

From (102), we see that $\mathrm{Lie}(G)$ has the structure of k-vector space, and that Lie is a functor from the category of algebraic groups over k to k-vector spaces.

THEOREM 3.4 *There is a unique way of making $G \rightsquigarrow \mathrm{Lie}(G)$ into a functor to Lie algebras such that $\mathrm{Lie}(\mathrm{GL}_n) = \mathfrak{gl}_n$ (as Lie algebras).*

Without the condition on $\mathrm{Lie}(\mathrm{GL}_n)$, we could, for example, take the bracket to be zero. It is clear from the definition of the Lie algebra of an affine group that an injective family of homomorphisms of affine groups defines an injective family of homomorphisms of Lie algebras. Since every affine group admits a faithful family of finite-dimensional representations, the uniqueness assertion is clear. The existence assertion will be proved later in this chapter.

REMARK 3.5 If $a \neq 0$, then $a + b\varepsilon = a(1 + \frac{b}{a}\varepsilon)$ has inverse $a^{-1}(1 - \frac{b}{a}\varepsilon)$ in $k[\varepsilon]$, and so

$$k[\varepsilon]^{\times} = \{a + b\varepsilon \mid a \neq 0\}.$$

An element of $\mathrm{Lie}(G)$ is a k-algebra homomorphism $u\colon \mathcal{O}(G) \to k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0$ is ϵ. Therefore, elements of $\mathcal{O}(G)$ not in the kernel $\mathfrak{m}$ of ϵ map to units in $k[\varepsilon]$, and so u factors uniquely through the local ring $\mathcal{O}(G)_{\mathfrak{m}}$. This shows that $\mathrm{Lie}(G)$ depends only on $\mathcal{O}(G)_{\mathfrak{m}}$. In particular, $\mathrm{Lie}(G^{\circ}) \simeq \mathrm{Lie}(G)$.

REMARK 3.6 There is a more direct way of defining the action of k on $\mathrm{Lie}(G)$: an element $c \in k$ defines a homomorphism of k-algebras

$$u_c\colon k[\varepsilon] \to k[\varepsilon], \quad u_c(a + \varepsilon b) = a + c\varepsilon b$$

such that $\pi \circ u_c = \pi$, and hence a commutative diagram

$$\begin{tikzcd} G(k[\varepsilon]) \arrow[r, "G(u_c)"] \arrow[d, "G(\pi)"] & G(k[\varepsilon]) \arrow[d, "G(\pi)"] \\ G(k) \arrow[r, "\mathrm{id}"] & G(k), \end{tikzcd}$$

which induces a homomorphism of groups $\mathrm{Lie}(G) \to \mathrm{Lie}(G)$. For example, when $G = \mathrm{GL}_n$,

$$G(u_c)E(A) = G(u_c)(I_n + \varepsilon A) = I_n + c\varepsilon A = E(cA).$$

This defines a k-vector space structure on $\mathrm{Lie}\, G$, which agrees that given by (102).

NOTES The definition (3.1) is valid for any functor $G\colon \mathsf{Alg}_k \to \mathsf{Grp}$. See DG II, §4, 1, p. 200.

4 Examples

4.1 By definition

$$\mathrm{Lie}(\mathrm{SL}_n) = \{I + A\varepsilon \in M_n(k[\varepsilon]) \mid \det(I + A\varepsilon) = 1\}.$$

When we expand $\det(I + \varepsilon A)$ as a sum of $n!$ products, the only nonzero term is

$$\textstyle\prod_{i=1}^{n}(1 + \varepsilon a_{ii}) = 1 + \varepsilon \sum_{i=1}^{n} a_{ii},$$

because every other term includes at least two off-diagonal entries. Hence

$$\det(I + \varepsilon A) = 1 + \varepsilon\, \mathrm{trace}(A)$$

and so

$$\begin{aligned}\mathfrak{sl}_n \overset{\text{def}}{=} \mathrm{Lie}(\mathrm{SL}_n) &= \{I + \varepsilon A \mid \mathrm{trace}(A) = 0\} \\ &\simeq \{A \in M_n(k) \mid \mathrm{trace}(A) = 0\}.\end{aligned}$$

For $n \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$,

$$\mathrm{trace}(AB) = \textstyle\sum_{1 \le i,j \le n} a_{ij} b_{ji} = \mathrm{trace}(BA). \tag{103}$$

Therefore $[A, B] = AB - BA$ has trace zero, and $\mathfrak{sl}_n$ is a Lie subalgebra of $\mathfrak{gl}_n$.

4.2 Recall that $\mathbb{T}_n$ (resp. $\mathbb{U}_n$, resp. $\mathbb{D}_n$) is the group of upper triangular (resp. upper triangular with 1s on the diagonal, resp. diagonal) invertible matrices. As

$$\mathrm{Lie}(\mathbb{T}_n) = \left\{ \begin{pmatrix} 1+\varepsilon c_{11} & \varepsilon c_{12} & \cdots & \varepsilon c_{1\,n-1} & \varepsilon c_{1\,n} \\ 0 & 1+\varepsilon c_{22} & \cdots & \varepsilon c_{2\,n-1} & \varepsilon c_{2\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1+\varepsilon c_{n-1\,n-1} & \varepsilon c_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 1+\varepsilon c_{n\,n} \end{pmatrix} \right\},$$

we see that

$$\mathfrak{b}_n \overset{\text{def}}{=} \mathrm{Lie}(\mathbb{T}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i > j\} \quad \text{(upper triangular matrices)}.$$

Similarly,

$$\begin{aligned}\mathfrak{n}_n &\overset{\text{def}}{=} \mathrm{Lie}(\mathbb{U}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \ge j\} \quad \text{(strictly upper triangular matrices)} \\ \mathfrak{d}_n &\overset{\text{def}}{=} \mathrm{Lie}(\mathbb{D}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \ne j\} \quad \text{(diagonal matrices)}.\end{aligned}$$

These are Lie subalgebras of $\mathfrak{gl}_n$.

4.3 Assume that the characteristic $\neq 2$, and let O_n be orthogonal group:

$$\mathrm{O}_n = \{A \in \mathrm{GL}_n \mid A^t \cdot A = I\} \quad (A^t = \text{transpose of } A).$$

For $I + \varepsilon A \in M_n(k[\varepsilon])$,

$$(I + \varepsilon A)^t \cdot (I + \varepsilon A) = (I + \varepsilon A^t) \cdot (I + \varepsilon A) = I + \varepsilon A^t + \varepsilon A,$$

and so

$$\begin{aligned} \mathrm{Lie}(\mathrm{O}_n) &= \{I + \varepsilon A \in M_n(k[\varepsilon]) \mid A^t + A = 0\} \\ &\simeq \{A \in M_n(k) \mid A \text{ is skew symmetric}\}. \end{aligned}$$

Similarly, $\mathrm{Lie}(\mathrm{SO}_n)$ consists of the skew symmetric matrices with trace zero, but obviously the second condition is redundant, and so

$$\mathrm{Lie}(\mathrm{SO}_n) = \mathrm{Lie}(\mathrm{O}_n).$$

This also follows from the fact that $\mathrm{SO}_n = \mathrm{O}_n^\circ$ (see 3.5).

4.4 Let G be a finite étale algebraic group: this means that $\mathcal{O}(G)$ is a separable k-algebra, and that every quotient of $\mathcal{O}(G)$ is separable (XII, 2.1, 2.4). The only separable subalgebra of $k[\varepsilon]$ is k, and so $G(k[\varepsilon]) = G(k)$ and $\mathrm{Lie}(G) = 0$. This also follows from the fact that

$$\mathrm{Lie}(G) = \mathrm{Lie}\left(G^\circ\right) = \mathrm{Lie}(1) = 0$$

(see 3.5).

4.5 Let k have characteristic $p \neq 0$, and let $G = \alpha_p$, so that $\alpha_p(R) = \{r \in R \mid r^p = 0\}$ (see IV, 1.5). Then $\alpha_p(k) = \{0\}$ and $\alpha_p(k[\varepsilon]) = \{a\varepsilon \mid a \in k\}$. Therefore,

$$\mathrm{Lie}(\alpha_p) = \{a\varepsilon \mid a \in k\} \simeq k.$$

Similarly,

$$\mathrm{Lie}(\mu_p) = \{1 + a\varepsilon \mid a \in k\} \simeq k.$$

As the bracket on a one-dimensional Lie algebra must be trivial, this shows that α_p and μ_p have the same Lie algebra.

4.6 Let V be a vector space over k. Every element of $V(\varepsilon) \overset{\text{def}}{=} k[\varepsilon] \otimes_k V$ can be written uniquely in the form $x + \varepsilon y$ with $x, y \in V$, i.e., $V(\varepsilon) = V \oplus \varepsilon V$. The $k[\varepsilon]$-linear maps $V(\varepsilon) \to V(\varepsilon)$ are the maps $u + \varepsilon\beta$, $u, \beta \in \mathrm{End}_{k\text{-lin}}(V)$, where

$$(u + \varepsilon\beta)(x + \varepsilon y) = u(x) + \varepsilon(u(y) + \beta(x)). \tag{104}$$

To see this, note that $\mathrm{End}_{k\text{-lin}}(V(\varepsilon)) \simeq M_2(\mathrm{End}_{k\text{-lin}}(V))$, and that ε acts as $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in M_2(\mathrm{End}_k(V))$. Thus

$$\begin{aligned} \mathrm{End}_{k[\varepsilon]\text{-lin}}(V(\varepsilon)) &= \left\{ \begin{pmatrix} u & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathrm{End}_k(V)) \,\middle|\, \begin{pmatrix} u & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & \beta \\ \gamma & \delta \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} u & 0 \\ \beta & u \end{pmatrix} \in M_2(\mathrm{End}_k(V)) \right\}. \end{aligned}$$

It follows that

$$\mathrm{GL}_V(k[\varepsilon]) = \{u + \varepsilon\beta \mid u \text{ invertible}\}$$

and that

$$\mathrm{Lie}(\mathrm{GL}_V) = \{\mathrm{id}_V + \varepsilon u \mid u \in \mathrm{End}(V)\} \simeq \mathrm{End}(V) = \mathfrak{gl}_V.$$

4.7 Let V be a finite-dimensional k-vector space, and let $D_{\mathfrak{a}}(V)$ denote the algebraic group $R \rightsquigarrow \mathrm{Hom}_{k\text{-lin}}(V,R)$ (see IV, 1.6). Then

$$\mathrm{Lie}(D_{\mathfrak{a}}(V)) \simeq \mathrm{Hom}_{k\text{-lin}}(V,k) = V^{\vee}$$

(as a k-vector space). Similarly,

$$\mathrm{Lie}(V_{\mathfrak{a}}) \simeq V.$$

4.8 Let $\phi\colon V \times V \to k$ be a k-bilinear form, and let G be the subgroup of GL_V of u preserving the form, i.e., such that

$$G(R) = \{u \in \mathrm{GL}_V(R) \mid \phi(ux,ux') = \phi(x,x') \quad \text{for all } x,x' \in V(R)\}.$$

Then $\mathrm{Lie}(G)$ consists of the endomorphisms $\mathrm{id} + \varepsilon u$ of $V(\varepsilon)$ such that

$$\phi((\mathrm{id}+\varepsilon u)(x+\varepsilon y),(\mathrm{id}+\varepsilon u)(x'+\varepsilon y')) = \phi(x+\varepsilon y, x'+\varepsilon y'), \quad \text{all } x,y,x',y' \in V.$$

The left hand side equals

$$\phi(x+\varepsilon y+\varepsilon\cdot ux, x'+\varepsilon y'+\varepsilon\cdot ux') = \phi(x+\varepsilon y, x'+\varepsilon y') + \varepsilon(\phi(ux,x')+\phi(x,ux')),$$

and so

$$\mathrm{Lie}(G) \simeq \{u \in \mathrm{End}_{k\text{-lin}}(V) \mid \phi(ux,x')+\phi(x,ux') = 0 \text{ all } x,x' \in V\}.$$

4.9 Let G be the unitary group defined by a quadratic extension K of k (IV, 1.11). The Lie algebra of G consists of the $A \in M_n(K)$ such that

$$(I+\varepsilon A)^*(I+\varepsilon A) = I$$

i.e., such that

$$A^* + A = 0.$$

Note that this is *not* a K-vector space, reflecting the fact that G is an algebraic group over k, not K.

4.10 Let M be a commutative group, written multiplicatively. The functor

$$R \rightsquigarrow \mathrm{Hom}(M, R^{\times}) \quad \text{(homomorphisms of abstract groups)}$$

is an affine group over k (see XIV, §3). On applying the functor $\mathrm{Hom}(M,-)$ to the split-exact sequence of commutative groups

$$0 \longrightarrow k \xrightarrow{a\mapsto 1+a\varepsilon} k[\varepsilon]^{\times} \xrightarrow{\varepsilon\mapsto 0} k^{\times} \longrightarrow 0,$$

we find that

$$\mathrm{Lie}(G) \simeq \mathrm{Hom}(M,k) \simeq \mathrm{Hom}(M,\mathbb{Z}) \otimes_{\mathbb{Z}} k.$$

A split torus T is an affine group of the form $D(M)$ with M finitely generated. For such a group,

$$X(T) \overset{\text{def}}{=} \mathrm{Hom}(T,\mathbb{G}_m) \simeq M,$$

and so

$$\begin{aligned} \mathrm{Lie}(T) &\simeq \mathrm{Hom}(X(T),\mathbb{Z}) \otimes_{\mathbb{Z}} k \\ \mathrm{Hom}_{k\text{-lin}}(\mathrm{Lie}(T),k) &\simeq k \otimes_{\mathbb{Z}} X(T). \end{aligned}$$

5 Description of $\mathrm{Lie}(G)$ in terms of derivations

DEFINITION 5.1 Let A be a k-algebra and M an A-module. A k-linear map $D\colon A \to M$ is a ***k*-derivation** of A into M if

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad \text{(Leibniz rule)}.$$

For example, $D(1) = D(1 \times 1) = D(1) + D(1)$ and so $D(1) = 0$. By k-linearity, this implies that

$$D(c) = 0 \text{ for all } c \in k. \tag{105}$$

Conversely, every additive map $A \to M$ satisfying the Leibniz rule and zero on k is a k-derivation.

Let $u\colon A \to k[\varepsilon]$ be a k-linear map, and write

$$u(f) = u_0(f) + \varepsilon u_1(f).$$

Then

$$u(fg) = u(f)u(g)$$

if and only if

$$\begin{aligned} &u_0(fg) = u_0(f)u_0(g) \text{ and} \\ &u_1(fg) = u_0(f)u_1(g) + u_0(g)u_1(f). \end{aligned}$$

The first condition says that u_0 is a homomorphism $A \to k$ and, when we use u_0 to make k into an A-module, the second condition says that u_1 is a k-derivation $A \to k$.

Recall that $\mathcal{O}(G)$ has a co-algebra structure (Δ,ϵ). By definition, the elements of $\mathrm{Lie}(G)$ are the k-algebra homomorphisms $\mathcal{O}(G) \to k[\varepsilon]$ such that the composite

$$\mathcal{O}(G) \xrightarrow{u} k[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} k$$

is ϵ, i.e., such that $u_0 = \epsilon$. Thus, we have proved the following statement.

PROPOSITION 5.2 *There is a natural one-to-one correspondence between the elements of* $\mathrm{Lie}(G)$ *and the* k*-derivations* $\mathcal{O}(G) \to k$ *(where* $\mathcal{O}(G)$ *acts on* k *through* ϵ*), i.e.,*

$$\mathrm{Lie}(G) \simeq \mathrm{Der}_{k,\epsilon}(\mathcal{O}(G),k). \tag{106}$$

The correspondence is $\epsilon + \varepsilon D \leftrightarrow D$, and the Leibniz condition is

$$D(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f) \tag{107}$$

6 Extension of the base field

PROPOSITION 6.1 *For any field K containing k,* $\mathrm{Lie}(G_K) \simeq K \otimes_k \mathrm{Lie}(G)$.

PROOF. We use the description of the Lie algebra in terms of derivations (106). Let e_i be a basis for $\mathcal{O}(G)$ as a k-vector space, and let

$$e_i e_j = \sum a_{ijk} e_k, \quad a_{ijk} \in k.$$

In order to show that a k-linear map $D\colon A \to k$ is a k-derivation, it suffices to check the Leibniz condition on the elements of the basis. Therefore, D is a k-derivation if and only if the scalars $c_i = D(e_i)$ satisfy

$$\sum\nolimits_k a_{ijk} c_k = \epsilon(e_i) c_j + \epsilon(e_j) c_i$$

for all i, j. This is a homogeneous system of linear equations in the c_i, and so a basis for the solutions in k is also a basis for the solutions in K (see the next lemma).

(Alternatively, use that

$$\mathrm{Lie}(G) \simeq \mathrm{Hom}_{k\text{-lin}}(I_G/I_G^2, k)$$

and that $I_{G_K} \simeq K \otimes_k I_G$.) □

LEMMA 6.2 *Let S be the space of solutions in k of a system of homogeneous linear equations with coefficients in k. Then the space of solutions in any k-algebra R of the system of equations is $R \otimes_k S$.*

PROOF. The space S is the kernel of a linear map

$$0 \to S \to V \xrightarrow{u} W.$$

Tensoring this sequence with R gives a sequence

$$0 \to R \otimes_k S \to R \otimes_k V \xrightarrow{\mathrm{id}_R \otimes u} R \otimes_k W,$$

which is exact because R is flat. Alternatively, for a finite system, we can put the matrix of the system of equations in row echelon form (over k), from which the statement is obvious. □

REMARK 6.3 Let G be an affine group over k. For a k-algebra R, define

$$\mathfrak{g}(R) = \mathrm{Ker}(G(R[\varepsilon]) \to G(R))$$

where $R[\varepsilon] = k[\varepsilon] \otimes_k R \simeq R[X]/(X^2)$. Then, as in (5.2), $\mathfrak{g}(R)$ can be identified with the space of k-derivations $A \to R$ (with R regarded as an A-module through ϵ), and the same proof shows that

$$\mathfrak{g}(R) \simeq R \otimes_k \mathfrak{g}(k) \tag{108}$$

where $\mathfrak{g}(k) = \mathrm{Lie}(G)$. In other words, the functor $R \rightsquigarrow \mathfrak{g}(R)$ is canonically isomorphic to $\mathfrak{g}_{\mathfrak{a}}$.

7 The adjoint map $\mathrm{Ad}\colon G \to \mathrm{Aut}(\mathfrak{g})$

For any k-algebra R, we have homomorphisms

$$R \xrightarrow{i} R[\varepsilon] \xrightarrow{\pi} R, \quad i(a) = a + \varepsilon 0, \quad \pi(a + \varepsilon b) = a, \quad \pi \circ i = \mathrm{id}_R .$$

For an affine group G over k, they give homomorphisms

$$G(R) \xrightarrow{i} G(R[\varepsilon]) \xrightarrow{\pi} G(R), \quad \pi \circ i = \mathrm{id}_{G(R)}$$

where we have written i and π for $G(i)$ and $G(\pi)$. Let $\mathfrak{g}(R) = \mathrm{Ker}(G(R[\varepsilon]) \xrightarrow{\pi} G(R))$, so that

$$\mathfrak{g}(R) \simeq R \otimes_k \mathfrak{g}(k)$$

(see 6.3). We define

$$\mathrm{Ad}\colon G(R) \to \mathrm{Aut}(\mathfrak{g}(R))$$

by

$$\mathrm{Ad}(g)x = i(g) \cdot x \cdot i(g)^{-1}, \quad g \in G(R), \quad x \in \mathfrak{g}(R) \subset G(R[\varepsilon]).$$

The following formulas hold:

$$\begin{aligned} \mathrm{Ad}(g)(x + x') &= \mathrm{Ad}(g)x + \mathrm{Ad}(g)x', \quad g \in G(R), \quad x, x' \in \mathfrak{g}(R) \\ \mathrm{Ad}(g)(cx) &= c(\mathrm{Ad}(g)x), \quad g \in G(R), \quad c \in R, \quad x \in \mathfrak{g}(R). \end{aligned}$$

The first is clear from the definition of Ad, and the second follows from the description of the action of c in (3.6). Therefore Ad maps into $\mathrm{Aut}_{R\text{-lin}}(\mathfrak{g}(R))$. All the constructions are clearly natural in R, and so we get a natural transformation

$$\mathrm{Ad}\colon G \to \underline{\mathrm{Aut}}(\mathfrak{g}_{\mathfrak{a}})$$

of group-valued functors on Alg_k.

Let $f\colon G \to H$ be a homomorphism of affine groups over k. Because f is a functor, the diagrams

$$\begin{tikzcd} G(R[\varepsilon]) \arrow[r, "\pi"] \arrow[d, "f(R[\varepsilon])"] & G(R) \arrow[d, "f(R)"] \\ H(R[\varepsilon]) \arrow[r, "\pi"] & H(R) \end{tikzcd} \qquad \begin{tikzcd} G(R[\varepsilon]) \arrow[d, "f(R[\varepsilon])"] & G(R) \arrow[l, "i"'] \arrow[d, "f(R)"] \\ H(R[\varepsilon]) & H(R) \arrow[l, "i"'] \end{tikzcd}$$

commute. Thus f defines a homomorphism of functors

$$\mathrm{Lie}(f)\colon \mathfrak{g}_{\mathfrak{a}} \to \mathfrak{h}_{\mathfrak{a}},$$

and the diagrams

$$\begin{tikzcd} G(R) \arrow[d, "f"] & \times & \mathfrak{g}(R) \arrow[r] \arrow[d, "\mathrm{Lie}(f)"] & \mathfrak{g}(R) \\ H(R) & \times & \mathfrak{h}(R) \arrow[r] & \mathfrak{g}(R) \arrow[u, "\mathrm{Lie}(f)"] \end{tikzcd}$$

commute for all R, i.e.,

$$\mathrm{Lie}(f)(\mathrm{Ad}_G(g) \cdot x) = \mathrm{Ad}_H(f(g)) \cdot x, \quad g \in G(R), \quad x \in \mathfrak{g}(R). \tag{109}$$

8 First definition of the bracket

The idea of the construction is the following. In order to define the bracket $[\,,\,]\colon \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$, it suffices to define the map $\mathrm{ad}\colon\mathfrak{g}\to\mathfrak{gl}_{\mathfrak{g}}$, $\mathrm{ad}(x)(y)=[x,y]$. For this, it suffices to define a homomorphism of affine groups $\mathrm{ad}\colon G\to\mathrm{GL}_{\mathfrak{g}}$, or, in other words, an action of G on $\mathfrak{g}$. But G acts on itself by inner automorphisms, and hence on its Lie algebra.

In more detail, in the last section, we defined a homomorphism of affine groups

$$\mathrm{Ad}\colon G\to\mathrm{GL}_{\mathfrak{g}}.$$

Specifically,

$$\mathrm{Ad}(g)x=i(g)\cdot x\cdot i(g)^{-1},\quad g\in G(R),\quad x\in\mathfrak{g}(R)\subset G(R[\varepsilon]).$$

On applying the functor Lie to the homomorphism Ad, we obtain a homomorphism of k-vector spaces

$$\mathrm{ad}\colon\mathrm{Lie}\,G\to\mathrm{Lie}\,\mathrm{GL}_{\mathfrak{g}}\overset{(4.6)}{\simeq}\mathrm{End}_{k\text{-lin}}(\mathfrak{g}).$$

DEFINITION 8.1 For $a,x\in\mathrm{Lie}(G)$,

$$[a,x]=\mathrm{ad}(a)(x).$$

LEMMA 8.2 *For $G=\mathrm{GL}_n$, the construction gives $[A,X]=AX-XA$.*

PROOF. An element $I+\varepsilon A\in\mathrm{Lie}(\mathrm{GL}_n)$ acts on $M_n(k[\varepsilon])$ as

$$X+\varepsilon Y\mapsto(I+\varepsilon A)(X+\varepsilon Y)(I-\varepsilon A)=X+\varepsilon Y+\varepsilon(AX-XA).$$

On comparing this with (4.6), we see that $\mathrm{ad}(A)$ acts as $\mathrm{id}+\varepsilon u$ where $u(X)=AX-XA$. □

LEMMA 8.3 *The construction is functorial in G, i.e., the map $\mathrm{Lie}\,G\to\mathrm{Lie}\,H$ defined by a homomorphism of affine groups $G\to H$ is compatible with the two brackets.*

PROOF. This follows from (109). □

Because the bracket $[A,X]=AX-XA$ on $\mathfrak{gl}_n$ satisfies the conditions in (VIII, 1.1) and every algebraic G can be embedded in GL_n (VIII, 9.1), the bracket on $\mathrm{Lie}(G)$ makes it into a Lie algebra. This completes the first proof of Theorem 3.4.

9 Second definition of the bracket

Let $A=\mathcal{O}(G)$, and consider the space $\mathrm{Der}_k(A,A)$ of k-derivations of A into A (with A regarded as an A-module in the obvious way). The bracket

$$[D,D']\overset{\text{def}}{=}D\circ D'-D'\circ D$$

of two derivations is again a derivation. In this way $\mathrm{Der}_k(A,A)$ becomes a Lie algebra.

Let G be an affine group. A derivation $D\colon\mathcal{O}(G)\to\mathcal{O}(G)$ is ***left invariant*** if

$$\Delta\circ D=(\mathrm{id}\otimes D)\circ\Delta. \tag{110}$$

If D and D' are left invariant, then

$$\begin{aligned}\Delta\circ[D,D'] &= \Delta\circ(D\circ D'-D'\circ D)\\ &= (\mathrm{id}\otimes(D\circ D')-\mathrm{id}\otimes(D'\circ D))\\ &= (\mathrm{id}\otimes[D,D'])\circ\Delta\end{aligned}$$

and so $[D,D']$ is left invariant.

PROPOSITION 9.1 *The map* $D\mapsto\epsilon\circ D\colon\mathrm{Der}_k(\mathcal{O}(G),\mathcal{O}(G))\to\mathrm{Der}_k(\mathcal{O}(G),k)$ *defines an isomorphism from the subspace of left invariant derivations onto* $\mathrm{Der}_k(\mathcal{O}(G),k)$.

PROOF. If D is a left invariant derivation $\mathcal{O}(G)\to\mathcal{O}(G)$, then

$$D=(\mathrm{id}\otimes\epsilon)\circ\Delta\circ D\overset{(110)}{=}(\mathrm{id}\otimes\epsilon)\circ(\mathrm{id}\otimes D)\circ\Delta=(\mathrm{id}\otimes(\epsilon\circ D))\circ\Delta,$$

and so D is determined by $\epsilon\circ D$. Conversely, if $d\colon\mathcal{O}(G)\to k$ is a derivation, then $D=(\mathrm{id}\otimes d)\circ\Delta$ is a left invariant derivation $\mathcal{O}(G)\to\mathcal{O}(G)$. □

Thus, $\mathrm{Lie}(G)$ is isomorphic (as a k-vector space) to the space of left invariant derivations $\mathcal{O}(G)\to\mathcal{O}(G)$, which is a Lie subalgebra of $\mathrm{Der}_k(\mathcal{O}(G),\mathcal{O}(G))$. In this way, $\mathrm{Lie}(G)$ acquires a Lie algebra structure, which is clearly natural in G.

It remains to check that, when $G=\mathrm{GL}_n$, this gives the bracket $[A,B]=AB-BA$ (left as an exercise for the present).

10 The functor Lie preserves fibred products

PROPOSITION 10.1 *For any homomorphisms* $G\to H\leftarrow G'$ *of affine groups,*

$$\mathrm{Lie}(G\times_H G')\simeq\mathrm{Lie}(G)\times_{\mathrm{Lie}(H)}\mathrm{Lie}(G'). \tag{111}$$

PROOF. By definition (V, §2),

$$\big(G\times_H G'\big)(R)=G(R)\times_{H(R)}G'(R),\qquad R\text{ a }k\text{-algebra.}$$

Therefore,

$$\begin{aligned}\mathrm{Lie}(G\times_H G') &= \mathrm{Ker}\big(G(k[\varepsilon])\times_{H(k[\varepsilon])}G'(k[\varepsilon])\to G(k)\times_{H(k)}G'(k)\big)\\ &= \{(g,g')\in G(k[\varepsilon])\times G'(k[\varepsilon])\mid g,g'\text{ have the same image in }H(k[\varepsilon]),\,G(k),\text{ and }G'(k)\}\\ &= \mathrm{Ker}(G(k[\varepsilon])\to G(k))\times_{H(k[\epsilon])}\mathrm{Ker}\big(G'(k[\varepsilon])\to G'(k)\big)\\ &= \mathrm{Lie}(G)\times_{\mathrm{Lie}(H)}\mathrm{Lie}(G').\end{aligned}$$

□

EXAMPLE 10.2 Let k be a field of characteristic $p\neq 0$. There are fibred product diagrams:

$$\begin{tikzcd}
\mu_p \arrow[r] \arrow[dd] & \mathbb{G}_m \arrow[dd, "y\mapsto(y^p,y)"] & & & k \arrow[r, "\mathrm{id}"] \arrow[dd, "\mathrm{id}"] & k \arrow[dd, "c\mapsto(0,c)"] \\
& & {} \arrow[r, rightsquigarrow, "\mathrm{Lie}"] & {} & & \\
\mathbb{G}_m \arrow[r, "x\mapsto(1,x)"'] & \mathbb{G}_m\times\mathbb{G}_m & & & k \arrow[r, "c\mapsto(0,c)"'] & k\times k.
\end{tikzcd}$$

EXAMPLE 10.3 Recall (VII, 4.1) that the kernel of a homomorphism $u\colon G \to H$ of affine groups can be obtained as a fibred product:

$$\begin{tikzcd}
\mathrm{Ker}(u) \arrow[r] \arrow[d] & \{1_H\} \arrow[d] \\
G \arrow[r, "u"] & H
\end{tikzcd}$$

Therefore (111) shows that

$$\mathrm{Lie}(\mathrm{Ker}(u)) = \mathrm{Ker}(\mathrm{Lie}(u)).$$

In other words, an exact sequence of affine groups $1 \to N \to G \to H$ gives rise to an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}\, N \to \mathrm{Lie}\, G \to \mathrm{Lie}\, H.$$

For example, the exact sequence (cf. 10.2)

$$1 \to \mu_p \xrightarrow{x \mapsto (x,x)} \mathbb{G}_m \times \mathbb{G}_m \xrightarrow{(x,y)\mapsto(y^p, x/y)} \mathbb{G}_m \times \mathbb{G}_m$$

gives rise to an exact sequence

$$0 \to k \xrightarrow{x \mapsto (x,x)} k \oplus k \xrightarrow{(x,y)\mapsto(0,x-y)} k \oplus k.$$

EXAMPLE 10.4 Let H and H' be affine subgroups of an affine group G. The affine subgroup $H \cap H'$ with $(H \cap H')(R) = H(R) \cap H'(R)$ (inside $G(R)$) is the fibred product of the inclusion maps, and so

$$\mathrm{Lie}(H \cap H') = \mathrm{Lie}(H) \cap \mathrm{Lie}(H') \quad (\text{inside } \mathrm{Lie}(G)).$$

More generally,

$$\mathrm{Lie}\left(\bigcap\nolimits_{i \in I} H_i\right) = \bigcap\nolimits_{i \in I} \mathrm{Lie}\, H_i \quad (\text{inside } \mathrm{Lie}(G)) \tag{112}$$

for any family of affine subgroups H_i of G.

For example, the homomorphisms in (10.2) realize $\mathbb{G}_m$ in two ways as subgroups of $\mathbb{G}_m \times \mathbb{G}_m$, which intersect in μ_p, and so

$$\mathrm{Lie}(\mu_p) = \mathrm{Lie}(\mathbb{G}_m) \cap \mathrm{Lie}(\mathbb{G}_m) \quad (\text{inside } \mathrm{Lie}(\mathbb{G}_m \times \mathbb{G}_m)).$$

10.5 The examples 10.2–10.4 show that the functor Lie does *not* preserve fibred products, left exact sequences, or intersections in the category of *smooth* affine groups. ☠

10.6 The sequence ☠

$$1 \to \mu_p \xrightarrow{x \mapsto (x,x)} \mathbb{G}_m \times \mathbb{G}_m \xrightarrow{(x,y)\mapsto(y^p, x/y)} \mathbb{G}_m \times \mathbb{G}_m \to 1$$

is exact in the category of affine groups over k, but

$$0 \to k \xrightarrow{x \mapsto (x,x)} k \oplus k \xrightarrow{(x,y)\mapsto(0,x-y)} k \oplus k \to 0$$

is not exact, and so the functor Lie is *not* right exact.

11 Commutative Lie algebras

A Lie algebra $\mathfrak{g}$ is said to be ***commutative*** (or ***abelian***) if $[x,y]=0$ for all $x,y\in\mathfrak{g}$. Thus, to give an commutative Lie algebra amounts to giving a finite-dimensional vector space.

If G is commutative, then $\mathrm{Lie}(G)$ is commutative. This can be seen directly from the first definition of the bracket because the inner automorphisms are trivial if G is commutative. Alternatively, observe that if G is a commutative subgroup of GL_n, then $\mathrm{Lie}(G)$ is a commutative subalgebra of $\mathrm{Lie}(\mathrm{GL}_n)$. More generally, for a connected algebraic affine group G,

$$\mathrm{Lie}(ZG)\subset\mathfrak{z}(\mathfrak{g}),$$

with equality if k has characteristic zero (tba).

Recall that an endomorphism u of a vector space V is said to be diagonalizable if V has a basis of eigenvectors, and that it is semisimple if it becomes diagonalizable after an extension of the base field k. Note that a nilpotent semisimple endomorphism is zero. If u is semisimple, then its restriction to any subspace W such that $uW\subset W$ is also semisimple.

PROPOSITION 11.1 *A Lie algebra is commutative if all of its elements are semisimple.*

PROOF. We may suppose that k is algebraically closed. Let x be an element of such a Lie algebra.. We have to show that $\mathrm{ad}(x)=0$. If not, $\mathrm{ad}(x)$ will have a nonzero eigenvalue, say, $\mathrm{ad}(x)(y)=cy$, $c\neq 0$, $y\neq 0$. Then $\mathrm{ad}(y)(x)=-\mathrm{ad}(x)(y)=-cy\neq 0$, but $\mathrm{ad}(y)^2(x)=-c[y,y]=0$. Thus, the restriction of $\mathrm{ad}(y)$ to the subspace spanned by x and y is nonzero, nilpotent, and semisimple, which is a contradiction. □

12 Normal subgroups and ideals

A normal algebraic subgroup N of an affine group G is the kernel of a quotient map $G\to Q$ (see VIII, 17.5); therefore, $\mathrm{Lie}(N)$ is the kernel of a homomorphism of Lie algebras $\mathrm{Lie}\,G\to\mathrm{Lie}\,Q$ (see 10.3), and so is an ideal in $\mathrm{Lie}\,G$. Of course, this can also be proved directly.

13 Algebraic Lie algebras

A Lie algebra is said to be ***algebraic*** if it is the Lie algebra of an affine algebraic group. A sum of algebraic Lie algebras is algebraic. Let $\mathfrak{g}=\mathrm{Lie}(G)$, and let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$. The intersection of the algebraic Lie subalgebras of $\mathfrak{g}$ containing $\mathfrak{h}$ is again algebraic (see 10.4) — it is called the ***algebraic envelope*** or ***hull*** of $\mathfrak{h}$.

Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{gl}_V$. A necessary condition for $\mathfrak{h}$ to be algebraic is that the semisimple and nilpotent components of each element of $\mathfrak{h}$ (as an endomorphism of $\mathfrak{gl}_V$) lie in $\mathfrak{h}$. However, this condition is not sufficient, even in characteristic zero.

Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{gl}_V$ over a field k of characteristic zero. We explain how to determine the algebraic hull of $\mathfrak{h}$. For any $X\in\mathfrak{h}$, let $\mathfrak{g}(X)$ be the algebraic hull of the Lie algebra spanned by X. Then the algebraic hull of $\mathfrak{h}$ is the Lie subalgebra of $\mathfrak{gl}_V$ generated by the $\mathfrak{g}(X)$, $X\in\mathfrak{h}$. In particular, $\mathfrak{h}$ is algebraic if and only if each X is contained in an algebraic Lie subalgebra of $\mathfrak{h}$. Write X as the sum $S+N$ of its semisimple and nilpotent components. Then $\mathfrak{g}(N)$ is spanned by N, and so it remains to determine $\mathfrak{g}(X)$ when X is semisimple. For some finite extension L of k, there exists a basis of $L\otimes V$ for which the matrix of X is $\operatorname{diag}(u_1,\ldots,u_n)$. Let W be the subspace $M_n(L)$ consisting of the matrices $\operatorname{diag}(a_1,\ldots,a_n)$ such that

$$\sum\nolimits_i c_i u_i = 0,\, c_i \in L \implies \sum\nolimits_i c_i a_i = 0,$$

i.e., such that the a_i satisfy every linear relation over L that the u_i do. Then the map

$$\mathfrak{gl}_V \to L \otimes \mathfrak{gl}_V \simeq M_n(L)$$

induces maps

$$\mathfrak{g}(X) \to L \otimes \mathfrak{g}(X) \simeq W,$$

which determine $L \otimes \mathfrak{g}(X)$. See Chevalley 1951 (also Fieker and de Graaf 2007 where it is explained how to implement this as an algorithm).

13.1 The following rules define a five-dimensional solvable Lie algebra $\mathfrak{g} = \bigoplus_{1\le i\le 5} kx_i$:

$$[x_1,x_2] = x_5, [x_1,x_3] = x_3, [x_2,x_4] = x_4\,, [x_1,x_4] = [x_2,x_3] = [x_3,x_4] = [x_5,\mathfrak{g}] = 0$$

(Bourbaki LIE, I, §5, Exercise 6). For every injective homomorphism $\mathfrak{g} \hookrightarrow \mathfrak{gl}_V$, there exists an element of $\mathfrak{g}$ whose semisimple and nilpotent components (as an endomorphism of V) do not lie in $\mathfrak{g}$ (ibid., VII, §5, Exercise 1). It follows that the image of $\mathfrak{g}$ in $\mathfrak{gl}_V$ is not the Lie algebra of an algebraic subgroup of GL_V (ibid., VII, §5, 1, Example).

13.2 The functor $G \rightsquigarrow \operatorname{Lie}(G)$ is not full. For example

$$\operatorname{End}(\mathbb{G}_m) = \mathbb{Z} \subsetneq k = \operatorname{End}(\operatorname{Lie}(\mathbb{G}_m)).$$

For another example, let k be an algebraically closed field of characteristic zero, and let $G = \mathbb{G}_a \rtimes \mathbb{G}_m$ with the product $(a,u)(b,v) = (a+ub, uv)$. Then

$$\operatorname{Lie}(G) = \operatorname{Lie}(\mathbb{G}_a) \times \operatorname{Lie}(\mathbb{G}_m) = ky + kx$$

with $[x,y] = y$. The Lie algebra morphism $\operatorname{Lie}(G) \to \operatorname{Lie}(\mathbb{G}_a)$ such that $x \mapsto y$, $y \mapsto 0$ is surjective, but it is not the differential of a homomorphism of algebraic groups because there is no nonzero homomorphism $\mathbb{G}_m \to \mathbb{G}_a$.

NOTES Need to prove the statements in this section (not difficult). They are important for the structure of semisimple algebraic groups and their representations.

14 The exponential notation

Let S be an R-algebra, and let a be an element of S such that $a^2 = 0$. There is a unique R-algebra homomorphism $R[\varepsilon] \to S$ sending ε to a. Following DG, II §4, 3.7, p.209, we denote the image of $x \in \operatorname{Lie}(G)(R)$ under the composite

$$\operatorname{Lie}(G)(R) \hookrightarrow G(R[\varepsilon]) \to G(S)$$

by e^{ax}. For example, $x = e^{\varepsilon x}$ in $G(R[\varepsilon])$. For $x, y \in \operatorname{Lie}(G)(R)$,

$$e^{a(x+y)} = e^{ax}e^{ay} \quad (\text{in } G(S)).$$

The action of $a \in R$ on $x \in \mathrm{Lie}(G)(R)$ is described by

$$e^{(\varepsilon a)x} = e^{\varepsilon(ax)} \quad (\text{in } G(R[\varepsilon])).$$

If $f\colon G \to H$ is a homomorphism of algebraic groups and $x \in \mathrm{Lie}(G)(R)$, then

$$f(e^{ax}) = e^{a(\mathrm{Lie}(f)(x))}.$$

The adjoint map Ad is described by

$$ge^{\varepsilon x}g^{-1} = e^{\varepsilon(\mathrm{Ad}(g)x)} \quad (\text{in } G(R[\varepsilon]),$$

$(g \in G(R),\ x \in \mathrm{Lie}(G)(R))$. Moreover,

$$\mathrm{Ad}(e^{\varepsilon x}) = \mathrm{id} + \varepsilon\,\mathrm{ad}(x) \quad (\text{in } \mathrm{Aut}_{R\text{-lin}}(\mathrm{Lie}(G)(R)).$$

Let $x, y \in \mathrm{Lie}(G)(R)$ and let $a, b \in S$ be of square 0. Then

$$e^{ax}e^{by}e^{-ax}e^{-by} = e^{ab[x,y]} \quad (\text{in } G(S))$$

(ibid. 4.4).

15 Arbitrary base rings

Now let k be a commutative ring, and let $k[\varepsilon] = k[X]/(X^2)$. For any smooth affine group G over k, define $\mathfrak{g} = \mathrm{Lie}(G)$ to be

$$\mathrm{Lie}(G) = \mathrm{Ker}(G(k[\varepsilon]) \xrightarrow{\varepsilon \mapsto 0} G(k)).$$

This is a finitely generated projective k-module, and for any k-algebra R,

$$\mathrm{Lie}(G_R) = R \otimes \mathfrak{g}.$$

Therefore, the functor $R \rightsquigarrow \mathrm{Lie}(G_R)$ is equal to $\mathfrak{g}_{\mathfrak{a}}$. The action of G on itself by inner automorphisms defines an action of G on $\mathfrak{g}$, and, in fact, a homomorphism

$$\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$$

of affine groups over k. On applying the functor Lie to this, we get the adjoint map

$$\mathrm{ad}\colon \mathfrak{g} \to \mathrm{Hom}_{k\text{-lin}}(\mathfrak{g}, \mathfrak{g}).$$

Now we can define a bracket operation on $\mathfrak{g}$ by

$$[x, y] = \mathrm{ad}(x)y.$$

Equipped with this bracket, $\mathfrak{g}$ is a Lie algebra over k. Most of the material in this section extends to smooth affine groups over rings.

NOTES Should rewrite the chapter for k a ring.

NOTES (mo84255) If you are interested in PBW for Lie algebras over rings, here is a nice (and well written) paper: P.J. Higgins, Baer Invariants and the Birkhoff-Witt theorem, J. of Alg. 11, 469-482, (1969). (Grinberg)

There is a joke definition of a Lie algebra, due to my adviser John Moore, that is relevant. His definition of a Lie algebra over a commutative ring R is that it is a module L with a bracket operation such that there exists an associative R-algebra A and a monomorphism $L \to A$ of R-modules that takes the bracket operation to the commutator in A. The point is to try to build in the PBW and dodge the question of which identities characterize Lie algebras. It is equivalent to the usual definition when R is a field, as one sees by proving PBW using only the standard identities, but not so over a general commutative ring.

Even over a field (char $\neq 2$ for simplicity) there is an interesting contrast with the definition of a Jordan algebra. There the analogue of the commutator is $1/2(ab+ba)$. One writes down the identities this satisfies and defines a Jordan algebra to be a vector space that satisfies the identities. But Jordan algebras do not generally embed in associative algebras (those that do are called special). (Peter May)

16 More on the relation between algebraic groups and their Lie algebras

In Chapter VI, we defined the dimension of an affine algebraic group G to be the dimension of the associated algebraic scheme $|G|$.

16.1 We list some alternative descriptions of $\dim G$.

(a) According to the Noether normalization theorem (CA 5.11), there exists a finite set S of elements in $\mathcal{O}(G)$ such that $k[S]$ is a polynomial ring in the elements of S and $\mathcal{O}(G)$ is finitely generated as a $k[S]$-module. The cardinality of S is $\dim G$.

(b) Let G° be the identity component of G (see XIII, 3.1). The algebraic variety $|G^\circ|$ is irreducible, and so $\mathcal{O}(G^\circ)/\mathfrak{N}$ is an integral domain (XIII, 3.2). The transcendence degree of its field of fractions is $\dim G$.

(c) Let $\mathfrak{m}$ be a maximal ideal of $\mathcal{O}(G)$. The height of $\mathfrak{m}$ is $\dim G$.

PROPOSITION 16.2 *For an affine algebraic group G, $\dim \operatorname{Lie} G \geq \dim G$, with equality if and only if G is smooth.*

PROOF. Because $\operatorname{Lie}(G_{k^{\mathrm{al}}}) \simeq \operatorname{Lie}(G) \otimes_k k^{\mathrm{al}}$ (see 6.1), we may suppose $k = k^{\mathrm{al}}$. According to (3.3),

$$\operatorname{Lie}(G) \simeq \operatorname{Hom}_{k\text{-lin}}(\mathfrak{m}/\mathfrak{m}^2, k)$$

where $\mathfrak{m} = \operatorname{Ker}(\mathcal{O}(G) \xrightarrow{\epsilon} k)$. Therefore, $\dim \operatorname{Lie}(G) \geq \dim G$, with equality if and only if the local ring $\mathcal{O}(G)_{\mathfrak{m}}$ is regular (VI, 7.3), but $\mathcal{O}(G)_{\mathfrak{m}}$ is regular if and only if G is smooth (VI, 8.2). □

EXAMPLE 16.3 We have

$$\begin{aligned}
\dim \operatorname{Lie} \mathbb{G}_a &= 1 = \dim \mathbb{G}_a \\
\dim \operatorname{Lie} \alpha_p &= 1 > 0 = \dim \alpha_p \\
\dim \operatorname{Lie} \mathrm{SL}_n &= n^2 - 1 = \dim \mathrm{SL}_n .
\end{aligned}$$

PROPOSITION 16.4 *If*

$$1 \to N \to G \to Q \to 1$$

is exact, then

$$\dim G = \dim N + \dim Q.$$

PROOF. See VII, 7.12. □

Applications

PROPOSITION 16.5 *Let H be a smooth affine algebraic subgroup of a connected affine algebraic group G. If $\operatorname{Lie} H = \operatorname{Lie} G$, then G is smooth and $H = G$.*

PROOF. We have

$$\dim H \overset{(16.2)}{=} \dim \operatorname{Lie} H = \dim \operatorname{Lie} G \overset{(16.2)}{\geq} \dim G.$$

Because H is a subgroup of G, $\dim H \leq \dim G$ (see VI, 8.1). Therefore

$$\dim H = \dim \operatorname{Lie}(G) = \dim G,$$

and so G is smooth (16.2) and $H = G$ (see VI, 8.1). □

COROLLARY 16.6 *Assume* $\operatorname{char}(k) = 0$ *and that G is connected. A homomorphism $H \to G$ is a surjective if* $\operatorname{Lie} H \to \operatorname{Lie} G$ *is surjective.*

PROOF. We know (VIII, 17.5) that $H \to G$ factors into

$$H \to \bar{H} \to G$$

with $H \to \bar{H}$ surjective and $\bar{H} \to G$ injective. Correspondingly, we get a diagram of Lie algebras

$$\operatorname{Lie} H \to \operatorname{Lie} \bar{H} \to \operatorname{Lie} G.$$

Because $\bar{H} \to G$ is injective, $\operatorname{Lie} \bar{H} \to \operatorname{Lie} G$ is injective (10.3). If $\operatorname{Lie} H \to \operatorname{Lie} G$ is surjective, then $\operatorname{Lie} \bar{H} \to \operatorname{Lie} G$ is an isomorphism. As we are in characteristic zero, $\bar{H}$ is smooth (VI, 9.3), and so (16.5) shows that $\bar{H} = G$. □

COROLLARY 16.7 *Assume* $\operatorname{char}(k) = 0$. *If*

$$1 \to N \to G \to Q \to 1$$

is exact, then

$$0 \to \operatorname{Lie}(N) \to \operatorname{Lie}(G) \to \operatorname{Lie}(Q) \to 0$$

is exact.

PROOF. The sequence $0 \to \operatorname{Lie}(N) \to \operatorname{Lie}(G) \to \operatorname{Lie}(Q)$ is exact (by 10.3), and the equality

$$\dim G \overset{(16.4)}{=} \dim N + \dim Q$$

implies a similar statement for the Lie algebras (by 16.2, as the groups are smooth). This implies (by linear algebra) that $\operatorname{Lie}(G) \to \operatorname{Lie}(Q)$ is surjective. □

COROLLARY 16.8 *The Lie algebra of G is zero if and only if G is étale; in particular, a connected affine algebraic group with zero Lie algebra is trivial.*

PROOF. We have seen that the Lie algebra of an étale group is zero (4.4). Conversely, if $\mathrm{Lie}\, G = 0$ then G has dimension 0, and so $\mathcal{O}(G)$ is a finite k-algebra; moreover, $I_G/I_G^2 = 0$, which implies that $\mathcal{O}(G)$ is étale. □

COROLLARY 16.9 *In characteristic zero, a homomorphism $G \to H$ of connected affine algebraic groups is an isogeny if and only if $\mathrm{Lie}(G) \to \mathrm{Lie}(H)$ is an isomorphism.*

PROOF. Apply (16.6), (16.7), and 16.8). □

16.10 The smoothness and connectedness assumptions are necessary in (16.5) because ☠

$$\mathrm{Lie}(\alpha_p) = \mathrm{Lie}(\mathbb{G}_a) \text{ but } \alpha_p \neq \mathbb{G}_a \text{ and}$$
$$\mathrm{Lie}(\mathrm{SO}_n) = \mathrm{Lie}(\mathrm{O}_n) \text{ but } \mathrm{SO}_n \neq \mathrm{O}_n.$$

The same examples show that the characteristic and connectedness assumptions are necessary in (16.6). The characteristic assumption is necessary in (16.7) because

$$0 \to \alpha_p \to \mathbb{G}_a \xrightarrow{x \mapsto x^p} \mathbb{G}_a \to 0$$

is exact, but the sequence

$$0 \to \mathrm{Lie}\, \alpha_p \to \mathrm{Lie}\, \mathbb{G}_a \to \mathrm{Lie}\, \mathbb{G}_a \to 0$$

is

$$0 \to k \xrightarrow{\simeq} k \xrightarrow{0} k \to 0,$$

which is not exact.

THEOREM 16.11 *Assume that $\mathrm{char}(k) = 0$ and that G is connected. The map $H \mapsto \mathrm{Lie}\, H$ from connected affine algebraic subgroups of G to Lie subalgebras of $\mathrm{Lie}\, G$ is injective and inclusion preserving.*

PROOF. Let H and H' be connected algebraic subgroups of G. Then (see 10.4)

$$\mathrm{Lie}(H \cap H') = \mathrm{Lie}(H) \cap \mathrm{Lie}\, H').$$

If $\mathrm{Lie}(H) = \mathrm{Lie}(H')$, then

$$\mathrm{Lie}(H) = \mathrm{Lie}(H \cap H') = \mathrm{Lie}(H'),$$

and so (16.5) shows that

$$H = H \cap H' = H'.$$

□

EXAMPLE 16.12 Let k be a field of characteristic zero, and consider GL_n as an algebraic group over k. According to VIII, 9.1, every algebraic group over k can be realized as a subgroup of GL_n for some n, and, according to (16.11), the algebraic subgroups of GL_n are in one-to-one correspondence with the algebraic Lie subalgebras of $\mathfrak{gl}_n$. This suggests two questions: find an algorithm to decide whether a Lie subalgebra of $\mathfrak{gl}_n$ is algebraic (i.e., arises from an algebraic subgroup)[2]; given an algebraic Lie subalgebra of $\mathfrak{gl}_n$, find an algorithm to construct the group. For a recent discussion of these questions, see, de Graaf, Willem, A. Constructing algebraic groups from their Lie algebras. J. Symbolic Comput. 44 (2009), no. 9, 1223–1233.[3]

PROPOSITION 16.13 *Assume* $\mathrm{char}(k) = 0$. *Let* u, v *be homomorphisms of affine algebraic groups* $G \to H$. *If* $\mathrm{Lie}(u) = \mathrm{Lie}(v)$ *and* G *is connected, then* $u = v$.

PROOF. Let Δ denote the diagonal in $G \times G$ — it is an algebraic subgroup of $G \times G$ isomorphic to G. The homomorphisms u and β agree on the algebraic group

$$G' \overset{\text{def}}{=} \Delta \cap G \times_H G.$$

The hypothesis implies $\mathrm{Lie}(G') = \mathrm{Lie}(\Delta)$, and so $G' = \Delta$. □

Thus, when $\mathrm{char}(k) = 0$, the functor $G \rightsquigarrow \mathrm{Lie}(G)$ from connected algebraic groups to Lie algebras is faithful and exact. It is not fully faithful, because

$$\mathrm{End}(\mathbb{G}_m) = \mathbb{Z} \neq k = \mathrm{End}(\mathrm{Lie}(\mathbb{G}_m)).$$

Moreover, it is trivial on étale algebraic groups.

16.14 Even in characteristic zero, infinitely many nonisomorphic connected algebraic groups can have the same Lie algebra. For example, let $\mathfrak{g}$ be the two-dimensional Lie algebra $\langle x, y \mid [x, y] = y \rangle$, and, for each nonzero $n \in \mathbb{N}$, let G_n be the semidirect product $\mathbb{G}_a \rtimes \mathbb{G}_m$ defined by the action $(t, a) \mapsto t^n a$ of $\mathbb{G}_m$ on $\mathbb{G}_a$. Then $\mathrm{Lie}(G_n) = \mathfrak{g}$ for all n, but no two groups G_n are isomorphic.

However, there is the following theorem: let k be an algebraically closed field; for every algebraic Lie algebra $\mathfrak{g}$ over k, there exists a connected affine algebraic group $G^{\mathfrak{g}}$ with unipotent centre such that $\mathrm{Lie}(G^{\mathfrak{g}}) = \mathfrak{g}$; if $\mathfrak{g}'$ is a second algebraic Lie algebra over k, then every isomorphism $\mathfrak{g} \to \mathfrak{g}'$ is the differential of an isomorphism $G^{\mathfrak{g}} \to G^{\mathfrak{g}'}$. In particular, $G^{\mathfrak{g}}$ is uniquely determined up to isomorphism, and $\mathrm{Aut}(G^{\mathfrak{g}}) = \mathrm{Aut}(\mathfrak{g})$ (Hochschild 1971b). Exercise: prove this by identifying which subcategory of $\mathsf{Rep}(\mathfrak{g})$ is equal to $\mathsf{Rep}(G^{\mathfrak{g}})$.

Representations

A ***representation*** of a Lie algebra $\mathfrak{g}$ on a k-vector space V is a homomorphism $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$. Thus ρ sends $x \in \mathfrak{g}$ to a k-linear endomorphism $\rho(x)$ of V, and

$$\rho([x, y]) = \rho(x)\rho(y) - \rho(y)\rho(x).$$

[2] See §13.

[3] de Graaf (ibid.) and his MR reviewer write: “A connected algebraic group in characteristic 0 is uniquely determined by its Lie algebra.” This is obviously false — for example, SL_2 and its quotient by $\{\pm I\}$ have the same Lie algebra. What they mean (but didn’t say) is that a connected algebraic subgroup of GL_n in characteristic zero is uniquely determined by its Lie algebra as a subalgebra of $\mathfrak{gl}_n$.

We often call V a $\mathfrak{g}$-***module*** and write xv for $\rho(x)(v)$. With this notation

$$[x,y]v = x(yv) - y(xv). \tag{113}$$

A representation ρ is said to be ***faithful*** if it is injective. The representation $x \mapsto \operatorname{ad} x\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$ is called the ***adjoint representation*** of $\mathfrak{g}$ (see 1.4).

Let W be a subspace of V. The ***stabilizer*** of W in $\mathfrak{g}$ is

$$\mathfrak{g}_W \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xW \subset W\}.$$

It is clear from (113) that $\mathfrak{g}_W$ is a Lie subalgebra of $\mathfrak{g}$.

Let $v \in V$. The ***isotropy algebra*** of v in $\mathfrak{g}$ is

$$\mathfrak{g}_v \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xv = 0\}.$$

It is a Lie subalgebra of $\mathfrak{g}$. The Lie algebra $\mathfrak{g}$ is said to ***fix*** v if $\mathfrak{g} = \mathfrak{g}_v$, i.e., if $\mathfrak{g}v = 0$.

Let $r\colon G \to \mathrm{GL}_V$ be a representation of G on a k-vector space V. Then $\operatorname{Lie}(r)$ is a representation of $\operatorname{Lie}(G)$ on V. Recall (VIII, 12.1) that, for any subspace W of V, the functor

$$R \rightsquigarrow G_W(R) \overset{\text{def}}{=} \{g \in G(R) \mid g(W \otimes R) = W \otimes R\}$$

is an affine subgroup of G, called the stabilizer of W in G .

PROPOSITION 16.15 *For any representation $G \to \mathrm{GL}_V$ and subspace $W \subset V$,*

$$\operatorname{Lie} G_W = (\operatorname{Lie} G)_W.$$

PROOF. By definition, $\operatorname{Lie} G_W$ consists of the elements $\mathrm{id} + \varepsilon u$ of $G(k[\varepsilon])$, $u \in \operatorname{End}(V)$, such that

$$(\mathrm{id} + \varepsilon u)(W + \varepsilon W) \subset W + \varepsilon W,$$

(cf. 4.6), i.e., such that $u(W) \subset W$. □

COROLLARY 16.16 *If W is stable under G, then it is stable under $\operatorname{Lie}(G)$, and the converse is true when $\operatorname{char}(k) = 0$ and G is connected.*

PROOF. To say that W is stable under G means that $G = G_W$, but if $G = G_W$, then $\operatorname{Lie} G = \operatorname{Lie} G_W = (\operatorname{Lie} G)_W$, which means that W is stable under $\operatorname{Lie} G$. Conversely, to say that W is stable under $\operatorname{Lie} G$, means that $\operatorname{Lie} G = (\operatorname{Lie} G)_W$. But if $\operatorname{Lie} G = (\operatorname{Lie} G)_W$, then $\operatorname{Lie} G = \operatorname{Lie} G_W$, which implies that $G_W = G$ when $\operatorname{char}(k) = 0$ and G is connected (16.5). □

Chapter XII

Finite Affine Groups

In this chapter, we allow k to be a commutative ring. As usual, unadorned tensor products are over k.

1 Definitions

DEFINITION 1.1 An affine group G over k is ***finite*** (resp. ***flat***, resp. ***finite locally free***) if $\mathcal{O}(G)$ is finitely generated (resp. flat, resp. finitely generated and projective) as a k-module.

In particular, a finite affine group is algebraic.

According to (CA 10.4) an affine group G over k is finite and locally free if and only if $\mathcal{O}(G)$ satisfies the following equivalent conditions:

◇ $\mathcal{O}(G)$ is finitely generated and projective as a k-module;

◇ $\mathcal{O}(G)$ is finitely presented as a k-module and $\mathcal{O}(G)_{\mathfrak{m}}$ is a free $k_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ of k;

◇ there exists a finite family $(f_i)_{i\in I}$ of elements of k generating the ideal k and such that, for all $i \in I$, the k_{f_i}-module $\mathcal{O}(G)_{f_i}$ is free of finite rank;

◇ $\mathcal{O}(G)$ is finitely presented and flat as a k-module;

◇ (k an integral domain) $\mathcal{O}(G)$ is finitely presented and $\dim_{k(\mathfrak{p})}(M \otimes_k k(\mathfrak{p}))$ is the same for all prime ideals $\mathfrak{p}$ of k (here $k(\mathfrak{p})$ is the field of fractions of $k/\mathfrak{p}$).

In general, if G is finite and locally free, the function

$$\mathfrak{p} \mapsto \dim_{k(\mathfrak{m})} M \otimes k(\mathfrak{m})\colon \mathrm{spm}(k) \to \mathbb{N}$$

is locally constant (because of the third condition above). It is called the ***order*** of G over k. When k is noetherian, "finite flat" is equivalent to "finite locally free" (because "finitely generated" is equivalent to "finitely presented").

When k is a field, flatness is automatic, and an affine group G over k is finite if and only if $\dim_k \mathcal{O}(G)$ is finite (and $\dim_k \mathcal{O}(G)$ is then the order of G over k).

DEFINITION 1.2 An affine group G over a field is ***profinite*** if its algebraic quotients are finite.

Thus, an affine group over a field is profinite if and only if it is an inverse limit of finite affine groups (VIII, 8.1). A profinite affine group is algebraic if and only if it is finite.

DEFINITION 1.3 A homomorphism of affine groups over a field is an isogeny if its kernel and cokernel are both profinite.

As the kernel and cokernel of a homomorphism of algebraic groups over a field are algebraic, such a homomorphism is an isogeny if and only if its kernel and cokernel are finite.

PROPOSITION 1.4 *An algebraic group G over a field is finite if and only if there exists a finite-dimensional representation (V,r) such that every finite-dimensional representation of G is isomorphic to a subrepresentation of V^n for some $n \geq 0$.*

PROOF. If G is finite, then the regular representation X of G is finite-dimensional, and (VIII, 10.3) says that it has the required property. Conversely if, with the notations of (X, §3), $\mathsf{Rep}_k(G) = \langle X \rangle$, then $G = \operatorname{Spec} B$ where B is the linear dual of the finite k-algebra $A_X = \operatorname{End}(\omega)$. □

Recall (p.147) that an algebraic group over a field is strongly connected if it has no nontrivial finite quotient.

COROLLARY 1.5 *An algebraic group G over a field is strongly connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\mathsf{Rep}(G)$ of subquotients of V^n, $n \geq 0$, is not stable under $\otimes$.*

PROOF. An algebraic group G is strongly connected if and only if there is no non-trivial epimorphism $G \to G'$ with G' finite. According to (VIII, 15.1), this is equivalent to $\mathsf{Rep}_k(G)$ having no non-trivial subcategory of the type described in (1.4). □

PROPOSITION 1.6 *An algebraic group G over a field k is finite if and only if $G(k^{\mathrm{al}})$ is finite.*

PROOF. Let $A = \mathcal{O}(G)$. If A is finite, then $G(k^{\mathrm{al}}) = \operatorname{Hom}_{k\text{-algebra}}(A, k^{\mathrm{al}})$ is obviously finite. Conversely, if $\operatorname{Hom}_{k\text{-algebra}}(A, k^{\mathrm{al}})$ is finite, then A has only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, the nilradical $\mathfrak{N}$ of A equals $\bigcap_i \mathfrak{m}_i$, and $A/\mathfrak{N} \simeq \prod A/\mathfrak{m}_i$ (Chinese remainder theorem). Each quotient $A/\mathfrak{m}_i$ is finite-dimensional over k by Zariski's lemma (CA 11.1), and so $A/\mathfrak{N}$ is finite-dimensional as a k-vector space. Because the ideal $\mathfrak{N}$ is finitely generated, $\mathfrak{N}^s = 0$ for some integer s, and each quotient space $\mathfrak{N}^i/\mathfrak{N}^{i+1}$ is finite-dimensional. Therefore A is a finite k-algebra. □

ASIDE 1.7 Let G be a finite flat affine group over an integral domain k. If k is a Dedekind domain, then $\mathcal{O}(G)_{\mathrm{red}}$ is flat over k, but probably not in general otherwise (mo61570). Moreover, $\mathcal{O}(G) \otimes \mathcal{O}(G)$ need not be reduced, so the Hopf algebra structure on $\mathcal{O}(G)$ need not pass to the quotient.

NOTES In SGA 3 a finite group scheme over a scheme S is defined to be a group scheme $f\colon G \to S$ such that f is a finite map. When S is affine, say, $S = \operatorname{Spec}(k)$, this agrees with our definition. Similarly our definition of "finite locally free" agrees with SGA 3 (cf. DG I, §5, 1.1, p.127). Our definition of "isogeny" agrees with that in DG V, §3, 1.6, p. 577.

2 Étale affine groups

Unless we say otherwise, k is a field in this section.

Étale algebras over a field

DEFINITION 2.1 An algebra A over a field k is ***diagonalizable*** if it is isomorphic to the product algebra k^n for some n, and it is ***étale*** if $L \otimes A$ is diagonalizable for some field L containing k.[1]

Let k be a field, and let A be a finite k-algebra. For any finite set S of maximal ideals in A, the Chinese remainder theorem (CA 2.12) shows that the map $A \to \prod_{\mathfrak{m}\in S} A/\mathfrak{m}$ is surjective with kernel $\bigcap_{\mathfrak{m}\in S}\mathfrak{m}$. In particular, $|S| \leq [A{:}k]$, and so A has only finitely many maximal ideals. If S is the set of all maximal ideals in A, then $\bigcap_{\mathfrak{m}\in S}\mathfrak{m}$ is the nilradical $\mathfrak{N}$ of A (CA 11.8), and so $A/\mathfrak{N}$ is a finite product of fields.

PROPOSITION 2.2 *The following conditions on a finite k-algebra A are equivalent:*

(a) *A is étale;*
(b) *$L \otimes A$ is reduced for all fields L containing k;*
(c) *A is a product of separable field extensions of k.*

PROOF. (a)⇒(b). Let L be a field containing k. By hypothesis, there exists a field L' containing k such that $L' \otimes A$ is diagonalizable. Let L'' be a field containing (copies of) both L and L' (e.g., take L'' to be a quotient of $L \otimes L'$ by a maximal ideal). Then $L'' \otimes A = L'' \otimes_{L'} L' \otimes A$ is diagonalizable, and the map $L \otimes A \to L'' \otimes A$ defined by the inclusion $L \to L''$ is injective, and so $L \otimes A$ is reduced.

(b)⇒(c). The map $a \mapsto a \otimes 1\colon A \to L \otimes A$ is injective, and so if $L \otimes A$ is reduced, then so also is A. The discussion above shows that it is a finite product of fields. Let k' be one of the factors of A. If k' is not separable over k, then k has characteristic $p \neq 0$ and there exists an element u of k' whose minimum polynomial is of the form $f(X^p)$ with $f \in k[X]$ (see FT 3.6, et seq.). Let L be a field containing k such that all the coefficients of f are pth powers in L. Then

$$L \otimes k[u] \simeq L \otimes (k[X]/(f(X^p)) \simeq L[X]/(f(X^p)),$$

which is not reduced because $f(X^p)$ is a pth power in $L[X]$. Hence $L \otimes A$ is not reduced.

(c)⇒(a). We may suppose that A itself is a separable field extension of k. From the primitive element theorem (FT 5.1), we know that $A = k[u]$ for some u. Because $k[u]$ is separable over k, the minimum polynomial $f(X)$ of u is separable, which means that

$$f(X) = \prod (X - u_i), \quad u_i \neq u_j \text{ for } i \neq j,$$

in a splitting field L for f. Now

$$L \otimes A \simeq L \otimes k[X]/(f) \simeq L[X]/(f),$$

and, according to the Chinese remainder theorem (CA 2.12),

$$L[X]/(f) \simeq \prod\nolimits_i L[X]/(X - u_i) \simeq L \times \cdots \times L.$$

□

[1] This is Bourbaki's terminology, Bourbaki A, V §6.

COROLLARY 2.3 *Let k^{sep} be a separable closure of k. A k-algebra A is étale if and only if $k^{\text{sep}} \otimes A$ is diagonalizable.*

PROOF. The proof that (c) implies (a) in (2.2) shows that $L \otimes A$ is diagonalizable if certain separable polynomials split in L. By definition, all separable polynomials split in k^{sep}. □

PROPOSITION 2.4 *Finite products, tensor products, and quotients of diagonalizable (resp. étale) k-algebras are diagonalizable (resp. étale).*

PROOF. This is obvious for diagonalizable algebras, and it follows for étale algebras. □

COROLLARY 2.5 *The composite of any finite set of étale subalgebras of a k-algebra is étale.*

PROOF. Let A_i be étale subalgebras of B. Then $A_1 \cdots A_n$ is the image of the map

$$a_1 \otimes \cdots \otimes a_n \mapsto a_1 \cdots a_n \colon A_1 \otimes \cdots \otimes A_n \to B,$$

and so is a quotient of $A_1 \otimes \cdots \otimes A_n$. □

PROPOSITION 2.6 *If A is étale over k, then $k' \otimes A$ is étale over k' for every field k' containing k.*

PROOF. Let L be such that $L \otimes A \approx L^m$, and let L' be a field containing (copies of) both L and k'. Then

$$L' \otimes_{k'} \left(k' \otimes A\right) \simeq L' \otimes A \simeq L' \otimes_L L \otimes A \approx L' \otimes_L L^m \simeq \left(L'\right)^m. \qquad \square$$

Classification of the étale algebras over a field

Let k^{sep} be a separable closure of k. If k is perfect, for example, of characteristic zero, then k^{sep} is an algebraic closure of k. Let Γ be the group of k-automorphisms of k^{sep}. For any subfield K of k^{sep}, finite and Galois over k, an easy Zorn's lemma argument[2] shows that

$$\sigma \mapsto \sigma|K \colon \Gamma \to \text{Gal}(K/k)$$

is surjective. Let X be a finite set with an action of Γ,

$$\Gamma \times X \to X.$$

We say that the action is continuous if it is continuous for the discrete topology on X and the Krull topology on Γ. Because X is finite, this is equivalent to saying that it factors through $\Gamma \to \text{Gal}(K/k)$ for some subfield K of k^{sep} finite and Galois over k.

For an étale k-algebra A, let

$$F(A) = \text{Hom}_{k\text{-alg}}(A, k^{\text{sep}}).$$

[2] Let $\sigma_0 \in \text{Gal}(K/k)$. Apply Zorn's lemma to the set of all pairs (E,u) where E is a subfield of k^{sep} containing k and u is homomorphism $E \to k^{\text{sep}}$ whose restriction to K is σ_0.

Then Γ acts on $F(A)$ through its action on k^{sep}:

$$(\gamma f)(a) = \gamma(f(a)), \quad \gamma \in \Gamma,\ f \in F(A),\ a \in A.$$

The images of all homomorphisms $A \to k^{\mathrm{sep}}$ lie in some finite Galois extension of k, and so the action of Γ on $F(A)$ is continuous.

THEOREM 2.7 *The map $A \rightsquigarrow F(A)$ defines a contravariant equivalence from the category étale of k-algebras to the category of finite sets with a continuous action of Γ.*

PROOF. This is a restatement of the fundamental theorem of Galois theory (FT §3), and is left as an exercise to the reader (the indolent may see Waterhouse 1979, 6.3). □

2.8 We sketch the proof of the theorem. Let $\bar{k} = k^{\mathrm{sep}}$. For any étale k-algebra A, there is a canonical isomorphism

$$a \otimes c \mapsto (\sigma a \cdot c)_{\sigma \in F(A)} \colon \bar{k} \otimes A \to \bar{k}^{F(A)}, \tag{114}$$

where

$$\bar{k}^{F(A)} \overset{\mathrm{def}}{=} \mathrm{Hom}(F(A), \bar{k}) = \prod\nolimits_{\sigma \in F(A)} k_\sigma, \quad k_\sigma = \bar{k}.$$

In other words, $\bar{k}^{F(A)}$ is a product of copies of $\bar{k}$ indexed by the elements of $F(A)$. When we let Γ act on $\bar{k} \otimes A$ through its action of $\bar{k}$ and on $\bar{k}^{F(A)}$ through its actions on both $\bar{k}$ and $F(A)$,

$$(\gamma f)(\sigma) = \gamma(f(\gamma^{-1}\sigma)), \quad \gamma \in \Gamma, \quad f \colon F(A) \to \bar{k}, \quad \sigma \in F(A),$$

then the (114) becomes equivariant. Now:

(a) for any étale k-algebra A,
$$A = (\bar{k} \otimes A)^\Gamma;$$

(b) for any finite set S with a continuous action of Γ, $(\bar{k}^S)^\Gamma$ is an étale k-subalgebra of $\bar{k}^S$, and
$$F((\bar{k}^S)^\Gamma) \simeq S.$$

Therefore, $A \rightsquigarrow F(A)$ is an equivalence of categories with quasi-inverse $S \mapsto (\bar{k}^S)^\Gamma$.

2.9 Suppose that A is generated by a single element, say, $A = k[u] \simeq k[X]/(f(X))$. Then A is étale if and only if $f(X)$ has distinct roots in k^{al}. Assume this, and choose $f(X)$ to be monic. A k-algebra homomorphism $A \to k^{\mathrm{sep}}$ is determined by the image of u, which can be any root of f in k^{sep}. Therefore, $F(A)$ can be identified with the set of roots of f in k^{sep}. Suppose $F(A)$ decomposes into r orbits under the action of Γ, and let $f_1, \ldots, f_r$ be the monic polynomials whose roots are the orbits. Then each f_i is fixed by Γ, and so has coefficients in k (FT 7.8). It follows that $f = f_1 \cdots f_r$ is the decomposition of f into its irreducible factors over k, and that

$$A \simeq \prod\nolimits_{1 \le i \le r} k[X]/(f_i(X))$$

is the decomposition of A into a product of fields.

Étale affine groups over a field

Let k be a field. An affine group G over k is ***étale*** if $\mathcal{O}(G)$ is an étale k-algebra; in particular, an étale affine group is finite (hence algebraic).[3]

2.10 Recall (VI, 8.3) that an algebraic group G over k is smooth if and only if $k^{\mathrm{al}} \otimes \mathcal{O}(G)$ is reduced. Therefore, a finite affine group G over k is étale if and only if it is smooth. If k has characteristic zero, then every finite affine group is étale (VI, 9.3). If k is perfect of characteristic $p \neq 0$, then $\mathcal{O}(G)^{p^r}$ is a reduced Hopf algebra for some r (VI, 10.2); as the kernel of the map $x \mapsto x^{p^r}\colon \mathcal{O}(G) \to \mathcal{O}(G)^{p^r}$ has dimension a power of p, we see that a finite affine group of order n is étale if p does not divide n.

Let $\mathcal{A}$ be the category of étale k-algebras. The functor $G \rightsquigarrow \mathcal{O}(G)$ is an equivalence from the category of étale affine groups over k to the category of group objects in the category $\mathcal{A}^{\mathrm{opp}}$ (see II, §6). As $G(k^{\mathrm{sep}}) = \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(G), k^{\mathrm{sep}})$, Theorem 2.7 shows that $G \rightsquigarrow G(k^{\mathrm{sep}})$ is an equivalence from the category of étale affine groups over k to the category of groups in the category of finite continuous Γ-sets. Clearly, a group in the category of finite sets with a continuous action of Γ is nothing but a finite group together with a continuous action of Γ by group homomorphisms.

THEOREM 2.11 *The functor $G \rightsquigarrow G(k^{\mathrm{sep}})$ is an equivalence from the category of étale algebraic groups over k to the category of finite groups endowed with a continuous action of Γ.*

Let K be a subfield of k^{sep} containing k, and let Γ' be the subgroup of Γ consisting of the σ fixing the elements of K. Then K is the subfield of k^{sep} of elements fixed by Γ' (see FT 7.10), and it follows that $G(K)$ is the subgroup $G(k^{\mathrm{sep}})$ of elements fixed by Γ'.

Examples

For an étale algebraic group G, the order of G is the order of the (abstract) group $G(k^{\mathrm{al}})$.

Since $\mathrm{Aut}(X) = 1$ when X is a group of order 1 or 2, there is exactly one étale algebraic group of order 1 and one of order 2 over any field k (up to isomorphism).

Let X be a group of order 3. Such a group is cyclic and $\mathrm{Aut}(X) = \mathbb{Z}/2\mathbb{Z}$. Therefore the étale algebraic groups of order 3 over k correspond to homomorphisms $\Gamma \to \mathbb{Z}/2\mathbb{Z}$ factoring through $\mathrm{Gal}(K/k)$ for some finite Galois extension K of k. A separable quadratic extension K of k defines such a homomorphism, namely,

$$\sigma \mapsto \sigma|K\colon \Gamma \to \mathrm{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$$

and all nontrivial such homomorphisms arise in this way (see FT §7). Thus, up to isomorphism, there is exactly one étale algebraic group G^K of order 3 over k for each separable quadratic extension K of k, plus the constant group G_0. For G_0, $G_0(k)$ has order 3. For G^K, $G^K(k)$ has order 1 but $G^K(K)$ has order 3. There are infinitely many distinct quadratic extensions of $\mathbb{Q}$, for example, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, ..., $\mathbb{Q}[\sqrt{p}]$, ... Since $\mu_3(\mathbb{Q}) = 1$ but $\mu_3(\mathbb{Q}[\sqrt[3]{1}]) = 3$, μ_3 must be the group corresponding to $\mathbb{Q}[\sqrt[3]{1}]$.

[3] Algebraic geometers will recognize that an affine group G is étale if and only if the morphism of schemes $|G| \to \mathrm{Spec}\, k$ is étale.

Finite étale affine groups over ring

We sketch the theory over an arbitrary commutative ring k.

DEFINITION 2.12 A k-algebra A is ***étale*** if it is flat of finite presentation as a k-module and $k(\mathfrak{p})\otimes A$ is étale over the field $k(\mathfrak{p})$ for all prime ideals $\mathfrak{p}$ in k (here $k(\mathfrak{p})$ is the field of fractions of $k/\mathfrak{p}$).

Assume that $\operatorname{Spec} k$ is connected, and choose a homomorphism x from k into a separably closed field Ω. For a finite étale k-algebra A, let $F(A)$ denote the set $\operatorname{Hom}_{k\text{-alg}}(A,\Omega)$. Then $A \rightsquigarrow F(A)$ is a functor. The automorphism group Γ of F is a profinite group, which is called the ***fundamental group*** $\pi_1(\operatorname{Spec} k, x)$ of $\operatorname{Spec} k$. It acts on each set $F(A)$, and the functor F is a contravariant equivalence from the category of finite étale k-algebras to the category of finite sets with a continuous action of Γ (see my Lectures on Etale Cohomology, §3, or Murre 1967).

An affine group G over k is ***étale*** if $\mathcal{O}(G)$ is an étale k-algebra. As in the case that k is a field, the functor

$$G \rightsquigarrow G(\Omega)$$

is an equivalence from the category of étale affine groups over k to the category of finite groups endowed with a continuous action of Γ.

NOTES EGA IV 17.3.1 defines a morphism of schemes to be étale if it is locally of finite presentation and formally étale. For a morphism of affine schemes, this agrees with our definition (cf. ibid. 17.3.2 (ii)).

3 Finite flat affine p-groups

Recall that the augmentation ideal I_G of an affine group G is the kernel of $\epsilon\colon\mathcal{O}(G)\to k$.

PROPOSITION 3.1 *Let G be a finite affine group over a field k of characteristic $p\neq 0$, and suppose that $x^p=0$ for all $x\in I_G$. For every basis $x_1,\ldots,x_r$ of I_G/I_G^2, the monomials*

$$x_1^{m_1}\cdots x_r^{m_r},\quad 0\leq m_i<p$$

form a basis for $\mathcal{O}(G)$ as a k-vector space (and so $[\mathcal{O}(G)\colon k]=p^r$).

PROOF. Omitted for the moment (see Waterhouse 1979, 11.4). □

The proposition says that $\mathcal{O}(G)\simeq k[X_1,\ldots,X_r]/(X_1^p,\ldots,X_r^p)$. This generalizes.

THEOREM 3.2 *Let G be a finite group scheme over a perfect field k of characteristic $p\neq 0$ such that $|G|$ is connected. For any basis $x_1,\ldots,x_r$ of I_G/I_G^2, there exist integers $e_1,\ldots,e_r\geq 1$ such that*

$$\mathcal{O}(G)\simeq k[X_1,\ldots,X_r]/(X_1^{p^{e_1}},\ldots,X_r^{p^{e_r}}).$$

PROOF. Omitted for the moment (see Waterhouse 1979, 14.4). □

Let k be nonperfect, and let $a\in k\smallsetminus k^p$. The subgroup G of $\mathbb{G}_a\times\mathbb{G}_a$ defined by the equations $x^{p^2}=0$, $y^p=ax^p$ is finite and connected, but $\mathcal{O}(G)$ is not a truncated polynomial algebra, i.e., (3.2) fails for G (Waterhouse 1979, p. 113).

Classification of finite commutative affine groups over a perfect field (Dieudonné modules)

Let k be a perfect field of characteristic p. Finite affine groups over k of order prime to p are étale (2.10), and so are classified in terms of the Galois group of k (2.11). In this subsection, we explain the classification of commutative finite affine groups over k of order a power of p (which we call finite affine ***p*-groups**).

Let W be the ring of Witt vectors with entries in k. Thus W is a complete discrete valuation ring with maximal ideal generated by $p = p1_W$ and residue field k. For example, if $k = \mathbb{F}_p$, then $W = \mathbb{Z}_p$. The Frobenius automorphism σ of W is the unique automorphism such that $\sigma a \equiv a^p \pmod{p}$.

THEOREM 3.3 *There exists a contravariant equivalence $G \rightsquigarrow M(G)$ from the category of commutative finite affine p-groups to the category of triples (M, F, V) in which M is a W-module of finite length and F and V are endomorphisms of M satisfying the following conditions ($c \in W$, $m \in M$):*

$$\begin{aligned} F(c \cdot m) &= \sigma c \cdot Fm \\ V(\sigma c \cdot m) &= c \cdot Vm \\ FV = p \cdot \mathrm{id}_M &= VF. \end{aligned}$$

The order of G is $p^{\text{length}(M(G))}$. For any perfect field k' containing k, there is functorial isomorphism

$$M(G_{k'}) \simeq W(k') \otimes_{W(k)} M(G).$$

PROOF. The proof is quite long, and will not be included. See Demazure 1972, Chap. III, or Pink 2005. □

For example:

$$\begin{aligned} M(\mathbb{Z}/p\mathbb{Z}) &= W/pW, \quad F = \sigma, \quad V = 0; \\ M(\mu_p) &= W/pW, \quad F = 0, \quad V = p\sigma^{-1}; \\ M(\alpha_p) &= W/pW, \quad F = 0, \quad V = 0. \end{aligned}$$

Let $D = W_\sigma[F, V]$ be the W-algebra of noncommutative polynomials in F and V over W, subject to the relations:

◇ $F \cdot c = \sigma c \cdot F$, all $c \in W$;
◇ $\sigma c \cdot V = V \cdot c$, all $c \in W$;
◇ $FV = p = VF$.

To give a triple (M, F, V) as in the theorem is the same as giving a D-module of finite length over W. The module $M(G)$ attached to a commutative finite affine p-group G is called the ***Dieudonné module*** of G.

The theorem is very important since it reduces the study of commutative affine p-groups over perfect fields to semi-linear algebra. There are important generalizations of the theorem to Dedekind domains, and other rings.

4 Cartier duality

In this section, we allow k to be a ring.

The Cartier dual as a Hopf algebra

If (A,m,e,Δ,ϵ) is a bi-algebra over k and A is finitely generated and projective as a k-module, then $(A^\vee,\Delta^\vee,\epsilon^\vee,m^\vee,e^\vee)$ is also a k-bialgebra (see II, §3 and II, Proposition 4.2). If moreover (A,m,e,Δ,ϵ) is commutative (resp. co-commutative), then $(A^\vee,\Delta^\vee,\epsilon^\vee,m^\vee,e^\vee)$ is co-commutative (resp. commutative).

The coordinate ring $\mathcal{O}(G)$ of a commutative finite locally free affine monoid is a commutative co-commutative bi-algebra, and so its dual $\mathcal{O}(G)^\vee$ is also the coordinate ring of a commutative finite locally free algebraic monoid $G^\vee$, called the ***Cartier dual*** of G:

$$\mathcal{O}(G)=(A,m,e,\Delta,\epsilon)\leftrightarrow(A^\vee,\Delta^\vee,\epsilon^\vee,m^\vee,e^\vee)=\mathcal{O}(G^\vee).$$

LEMMA 4.1 *If $\mathcal{O}(G)$ is a Hopf algebra, then so also is $\mathcal{O}(G^\vee)$ (and so $G^\vee$ is an affine group).*

PROOF. More precisely, we show that if S is an inversion for $\mathcal{O}(G)$, then $S^\vee$ is an inversion for $\mathcal{O}(G)$. Condition (a) of the Definition II, 4.4 is obviously self-dual. For (b) we have to show that $S^\vee$ is an algebra homomorphism. For this we have to check that $\Delta^\vee\circ(S^\vee\otimes S^\vee)=S^\vee\circ\Delta^\vee$, or, equivalently, that $\Delta\circ S=(S\otimes S)\circ\Delta$. In other words, we have to check that the diagram at left below commutes. This corresponds (under a category equivalence) to the diagram at right, which commutes precisely because G is commutative (the inverse of a product is the product of the inverses):

$$\begin{tikzcd}
\mathcal{O}(G) \arrow[r, "\Delta"] \arrow[d, "S"] & \mathcal{O}(G)\otimes\mathcal{O}(G) \arrow[d, "S\otimes S"] \\
\mathcal{O}(G) \arrow[r, "\Delta"] & \mathcal{O}(G)\otimes\mathcal{O}(G)
\end{tikzcd}
\qquad
\begin{tikzcd}
G & G\times G \arrow[l, "m"'] \\
G \arrow[u, "\mathrm{inv}"'] & G\times G. \arrow[l, "m"'] \arrow[u, "\mathrm{inv}\times\mathrm{inv}"']
\end{tikzcd}$$

(Alternatively, we could appeal to the unproven (II, 4.5), which says that condition (b) is superfluous. We had to use the commutativity of G in the above proof of condition (b) because we checked it in the form $S^\vee(ab)=S^\vee(a)S^\vee(b)$.) □

The functor $G\rightsquigarrow G^\vee$ is a contravariant equivalence from the category of commutative finite locally free affine groups to itself, and $(G^\vee)^\vee\simeq G$.

The Cartier dual as a functor

In this subsection, we describe the functor defined by the Cartier dual $G^\vee$ of a commutative finite locally free affine group G.

For k-algebra R, let $\underline{\mathrm{Hom}}(G,\mathbb{G}_m)(R)$ be the set of homomorphisms of $u\colon G_R\to\mathbb{G}_{mR}$ of affine groups over R. This becomes a group under the multiplication

$$(u_1\cdot u_2)(g)=u_1(g)\cdot u_2(g),\quad g\in G(R'),\quad R'\text{ an }R\text{-algebra.}$$

In this way,

$$R\rightsquigarrow\underline{\mathrm{Hom}}(G,\mathbb{G}_m)(R)$$

becomes a functor $\mathsf{Alg}_k\to\mathsf{Grp}$.

THEOREM 4.2 *There is a canonical isomorphism*

$$G^{\vee} \simeq \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$$

of functors $\mathsf{Alg}_k \to \mathsf{Grp}$.

PROOF. Let R be a k-algebra. We have

$$G(R) = \mathrm{Hom}_{R\text{-alg}}(\mathcal{O}(G), R) \hookrightarrow \mathrm{Hom}_{R\text{-lin}}(\mathcal{O}(G), R) = \mathcal{O}(G^{\vee})_R. \qquad (115)$$

The multiplication in $\mathcal{O}(G)$ corresponds to comultiplication in $\mathcal{O}(G^{\vee})$, from which it follows that the image of (115) consists of the group-like elements in $\mathcal{O}(G^{\vee})_R$. On the other hand, we know that $\mathrm{Hom}(G^{\vee}_R, \mathbb{G}_m)$ also consists of the group-like elements in $\mathcal{O}(G^{\vee})_R$ (VIII, §16). Thus,

$$G(R) \simeq \underline{\mathrm{Hom}}(G^{\vee}, \mathbb{G}_m)(R).$$

This isomorphism is natural in R, and so we have shown that $G \simeq \underline{\mathrm{Hom}}(G^{\vee}, \mathbb{G}_m)$. To obtain the required isomorphism, replace G with $G^{\vee}$ and use that $(G^{\vee})^{\vee} \simeq G$. □

NOTES For more on Cartier duality, see Pink 2005, §24, and the notes on Cartier duality on Ching-Li Chai's website

EXAMPLE 4.3 Let $G = \alpha_p$, so that $\mathcal{O}(G) = k[X]/(X^p) = k[x]$. Let $1, y, y_2, \ldots, y_{p-1}$ be the basis of $\mathcal{O}(G^{\vee}) = \mathcal{O}(G)^{\vee}$ dual to $1, x, \ldots, x^{p-1}$. Then $y^i = i!y_i$; in particular, $y^p = 0$. In fact, $G^{\vee} \simeq \alpha_p$, and the pairing is

$$a, b \mapsto \exp(ab)\colon \alpha_p(R) \times \alpha_p(R) \to R^{\times}$$

where

$$\exp(ab) = 1 + \frac{ab}{1!} + \frac{(ab)^2}{2!} + \cdots + \frac{(ab)^{p-1}}{(p-1)!}.$$

The category of finite locally free affine groups over a ring

Let $FL(k)$ denote the category of finite locally free affine groups over a ring k. When k is a field, then $FL(k)$ has most of the good properties of the category of groups; in particular, the category of commutative finite affine groups over a field is abelian. See Chapter IX.

When k is not a field, the situation is much more complicated. For example, let $k = \mathbb{Z}$ and consider the homomorphism $u\colon (\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}} \to (\mu_2)_{\mathbb{Z}}$ corresponding to the map of rings

$$T \mapsto (1, -1)\colon \mathbb{Z}[T]/(T^2 - 1) \to \mathbb{Z} \times \mathbb{Z}.$$

This is both a monomorphism and an epimorphism in $FL(k)$, but it is not an isomorphism. The kernel of u in the category of finite affine groups over k has trivial fibre over all primes ideals of $\mathbb{Z}$ except (2), where it has fibre is μ_2. The kernel of u in $FL(k)$ is zero, but the kernel of the base change of u to $\mathbb{F}_2$ is $\mathbb{Z}/2\mathbb{Z}$.

The main positive result is the following theorem of Grothendieck.

THEOREM 4.4 *Let G be a finite locally free affine group over k, and let $G \times X \to X$ be an action of G on a functor X in $\mathsf{Alg}_k^\vee$. Assume that X is representable and that the natural transformation*

$$(g,x) \mapsto (g,gx)\colon G \times X \to X \times X$$

is closed (see V, §6). Then there exists a representable functor $G\backslash X$ and a morphism $u\colon X \to G\backslash X$ such that

(a) *u is constant on the orbits of G, and every natural transformation $X \to Y$ of representable functors with this property factors uniquely through u;*
(b) *X is finite and locally free over $G\backslash X$;*
(c) *for every k-algebra R, $G(R)\backslash X(R) \to (X\backslash G)(R)$ is injective (in other words, the map from the naive quotient to the genuine quotient is injective);*
(d) *if G and X are represented by A and B respectively, then $G\backslash X$ is represented by the equalizer of the map $b \mapsto 1 \otimes b\colon B \to A \otimes B$ with the map defined by u.*

PROOF. See Tate 1997, 3.4, for a discussion of the theorem. See also Mumford, Abelian Varieties, III, §12. (The proof will be included in the next version — it is about 6 pages.) □

As a corollary, one sees that quotients of affine groups by normal finite locally free affine groups exist as affine groups, and have the expected properties.

For a homomorphism of finite locally free affine groups whose kernel is locally free, everything works as expected: the kernel, cokernel, image, and co-image exist, and the map from the co-image to the image is an isomorphism.

In general, the category of finite locally free commutative affine groups over a ring k is exact but not abelian (see mo7688, especially the answer of Laurent Fargues).

ASIDE 4.5 The theory of finite locally free affine groups is extensive. See Tate 1997 for a short introduction.

5 Exercises

In the exercises, k is a field.

EXERCISE XII-1 Show that A is étale if and only if there are no nonzero k-derivations $D\colon A \to k$. [Regard A as a left A-module by left multiplication. Let A be a k-algebra and M an A-module. A k ***-derivation*** is a k-linear map $D\colon A \to M$ such that

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad \text{(Leibniz rule).]}$$

EXERCISE XII-2 How many finite algebraic groups of orders $1,2,3,4$ are there over $\mathbb{R}$ (up to isomorphism)?

EXERCISE XII-3 Let G be the constant algebraic group over k defined by a finite commutative group Γ. Let n be the exponent of Γ, and assume that k contains n distinct nth roots of 1 (so, in particular, n is not divisible by the characteristic of k). Show that the Cartier dual of G is the constant algebraic group defined by the dual group $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$.

EXERCISE XII-4 If k has characteristic $p \neq 0$, show that $\alpha_p^\vee \simeq \alpha_p$ and $(\mathbb{Z}/p\mathbb{Z})_k^\vee \simeq \mu_p$ (hence $\mu_p^\vee \simeq (\mathbb{Z}/p\mathbb{Z})_k$) (here $(\mathbb{Z}/p\mathbb{Z})_k$, μ_p, and α_p are the groups in (IV, 1.3), (IV, 1.4), and (IV, 1.5)).

CHAPTER **XIII**

The Connected Components of an Algebraic Group

Recall that a topological space X is connected if it is not the union of two disjoint nonempty open subsets. This amounts to saying that, apart from X itself and the empty set, there is no subset of X that is both open and closed. For each point x of X, the union of the connected subsets of X containing x is again connected, and so it is the largest connected subset containing x — it is called the connected component of x. The set of the connected components of the points of X is a partition of X by closed subsets. Write $\pi_0(X)$ for the set of connected components of X.

In a topological group G, the connected component of the neutral element is a closed normal connected subgroup G° of G, called the neutral (or identity) component of G. Therefore, the quotient $\pi_0(G) = G/G^\circ$ is a separated topological group. For example, $\mathrm{GL}_2(\mathbb{R})$ has two connected components, namely, the identity component consisting of the matrices with determinant > 0 and another connected component consisting of the matrices with determinant < 0.

In this chapter, we discuss the identity component G° of an algebraic affine group and the (étale) quotient group $\pi_0(G)$ of its connected components. Throughout, k is a field.

1 Idempotents and connected components

Throughout this section, A is a commutative ring. An element e of A is ***idempotent*** if $e^2 = e$. For example, 0 and 1 are both idempotents — they are called the ***trivial idempotents***. Idempotents $e_1,\ldots,e_n$ are ***orthogonal*** if $e_ie_j = 0$ for $i \neq j$. A sum of orthogonal idempotents is again idempotent. A finite set $\{e_1,\ldots,e_n\}$ of orthogonal idempotents is ***complete*** if $e_1 + \cdots + e_n = 1$. Every finite set of orthogonal idempotents $\{e_1,\ldots,e_n\}$ can be completed by adding the idempotent $e = 1-(e_1+\cdots+e_n)$.

If $A = A_1 \times \cdots \times A_n$ (direct product of rings), then the elements

$$e_1 = (1,0,\ldots), e_2 = (0,1,0,\ldots), \ \ldots, e_n = (0,\ldots,0,1)$$

form a complete set of orthogonal idempotents. Conversely, if $\{e_1,\ldots,e_n\}$ is a complete set of orthogonal idempotents in A, then Ae_i becomes a ring with the addition and multiplication induced by that of A (but with the identity element e_i), and $A \simeq Ae_1 \times \cdots \times Ae_n$.

LEMMA 1.1 *The space* spec A *is disconnected if and only if* A *contains a nontrivial idempotent.*

PROOF. Let e be a nontrivial nilpotent, and let $f = 1-e$. For a prime ideal $\mathfrak{p}$, the map $A \to A/\mathfrak{p}$ must send exactly one of e or f to a nonzero element. This shows that spec A is a disjoint union of the sets[1] $D(e)$ and $D(f)$, each of which is open. If $D(e) = \operatorname{spec} A$, then e would be a unit (CA 2.2), and hence can be cancelled from $ee = e$ to give $e = 1$. Therefore $D(e) \neq \operatorname{spec} A$, and similarly, $D(f) \neq \operatorname{spec} A$.

Conversely, suppose that spec A is disconnected, say, the disjoint union of two nonempty closed subsets $V(\mathfrak{a})$ and $V(\mathfrak{b})$. Because the union is disjoint, no prime ideal contains both $\mathfrak{a}$ and $\mathfrak{b}$, and so $\mathfrak{a}+\mathfrak{b} = A$. Thus $a+b = 1$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. As $ab \in \mathfrak{a} \cap \mathfrak{b}$, all prime ideals contain ab, which is therefore nilpotent (CA 2.5), say $(ab)^m = 0$. Any prime ideal containing a^m contains a; similarly, any prime ideal containing b^m contains b; thus no prime ideal contains both a^m and b^m, which shows that $(a^m, b^m) = A$. Therefore, $1 = ra^m + sb^m$ for some $r,s \in A$. Now

$$\begin{aligned}(ra^m)(sb^m) &= rs(ab)^m = 0,\\ (ra^m)^2 &= (ra^m)(1-sb^m) = ra^m,\\ (sb^m)^2 &= sb^m\\ ra^m + sb^m &= 1,\end{aligned}$$

and so $\{ra^m, sb^m\}$ is a complete set of orthogonal idempotents. Clearly $V(\mathfrak{a}) \subset V(ra^m)$ and $V(\mathfrak{b}) \subset V(sb^m)$. As $V(ra^m) \cap V(sb^m) = \emptyset$, we see that $V(\mathfrak{a}) = V(ra^m)$ and $V(\mathfrak{b}) = V(sb^m)$, and so each of ra^m and sb^m is a nontrivial idempotent. □

PROPOSITION 1.2 *Let* $\{e_1, \ldots, e_n\}$ *be a complete set of orthogonal idempotents in* A. *Then*

$$\operatorname{spec} A = D(e_1) \sqcup \ldots \sqcup D(e_n)$$

is a decomposition of spec A *into a disjoint union of open subsets. Moreover, every such decomposition arises in this way.*

PROOF. Let $\mathfrak{p}$ be a prime ideal in A. Because $A/\mathfrak{p}$ is an integral domain, exactly one of the e_i's maps to 1 in $A/\mathfrak{p}$ and the remainder map to zero. This proves that spec A is the disjoint union of the sets $D(e_i)$.

Now consider a decomposition

$$\operatorname{spec} A = U_1 \sqcup \ldots \sqcup U_n$$

each U_i open. We use induction on n to show that it arises from a complete set of orthogonal idempotents. When $n = 1$, there is nothing to prove, and when $n \geq 2$, we write

$$\operatorname{spec} A = U_1 \sqcup (U_2 \sqcup \ldots \sqcup U_n).$$

The proof of the lemma shows that there exist orthogonal idempotents e_1, $e_1' \in A$ such that $e_1 + e_1' = 1$ and

$$\begin{aligned}U_1 &= D(e_1)\\ U_2 \sqcup \ldots \sqcup U_n &= D(e_1') = \operatorname{spec} Ae_1'.\end{aligned}$$

[1] The set $D(e)$ consists of the prime ideals of A *not* containing e, and $V(\mathfrak{a})$ consists of all prime ideals containing $\mathfrak{a}$.

By induction, there exist orthogonal idempotents $e_2, \ldots, e_n$ in Ae'_1 such that $e_2 + \cdots + e_n = e'_1$ and $U_i = D(e_i)$ for $i = 2, \ldots, n$. Now $\{e_1, \ldots, e_n\}$ is a complete set of orthogonal idempotents in A such that $U_i = D(e_i)$ for all i. □

1.3 Recall that a ring A is said to be Jacobson if every prime ideal is an intersection of maximal ideals, and that every finitely generated algebra over a field is Jacobson (see CA 12.3 et seq.). In a Jacobson ring, the nilradical is an intersection of maximal ideals. When A is Jacobson, "prime ideal" can be replaced by "maximal ideal" and "spec" with "spm" in the above discussion. In particular, for a Jacobson ring A, there are natural one-to-one correspondences between

- ◇ the decompositions of $\operatorname{spm}(A)$ into a finite disjoint union of open subspaces,
- ◇ the decompositions of A into a finite direct products of rings, and
- ◇ the complete sets of orthogonal idempotents in A.

Now consider a ring $A = k[X_1, \ldots, X_n]/\mathfrak{a}$. When k is an algebraically closed field,

$$\operatorname{spm} A \simeq \text{the zero set of } \mathfrak{a} \text{ in } k^n$$

as topological spaces (Nullstellensatz, CA 11.6), and so $\operatorname{spm} A$ is connected if and only if the zero set of $\mathfrak{a}$ in k^n is connected.

LEMMA 1.4 *Let A be a finitely generated algebra over a separably closed field k. The number of connected components of* $\operatorname{spm} A$ *is equal to the largest degree of an étale k-subalgebra of A (and both are finite).*

PROOF. Because $\operatorname{spm} A$ is noetherian, it is a finite disjoint union of its connected components, each of which is open (CA 12.12). Let E be an étale k-subalgebra of A. Because k is separably closed, E is a product of copies of k. A decomposition of E corresponds to a complete set $(e_i)_{1 \leq i \leq m}$ of orthogonal idempotents in E, and $m = [E{:}k]$. Conversely, a complete set $(e_i)_{1 \leq i \leq m}$ of orthogonal idempotents in A defines an étale k-subalgebra of A of degree m, namely, $\sum k e_i$. Thus the statement follows from (1.3). □

LEMMA 1.5 *Let A be a finitely generated k-algebra. Assume that k is algebraically closed, and let K be an algebraically closed field containing k. If* $\operatorname{spm} A$ *is connected, so also is* $\operatorname{spm} A_K$.

PROOF. Write $A = k[X_1, \ldots, X_n]/\mathfrak{a}$, so that $A_K = K[X_1, \ldots, X_n]/\mathfrak{b}$ where $\mathfrak{b}$ is the ideal generated by $\mathfrak{a}$. By assumption, the zero set $V(\mathfrak{a})$ of $\mathfrak{a}$ in k^n is connected, and it lies in the zero set $V(\mathfrak{b})$ of $\mathfrak{b}$ in K^n. As the closure of a connected set is connected, it suffices to show that $V(\mathfrak{b})$ is the Zariski closure of $V(\mathfrak{a})$. For this it suffices to show that if an element f of $K[X_1, \ldots, X_n]$ is zero on $V(\mathfrak{a})$, then it is zero on $V(\mathfrak{b})$. Choose a basis $(a_i)_{i \in I}$ for K over k, and write

$$f = \sum\nolimits_i a_i f_i \quad (f_i \in k[X_1, \ldots, X_n], \text{ finite sum}).$$

As f is zero on $V(\mathfrak{a})$, so also is each f_i. By the Strong Nullstellensatz (CA 11.7), some power of f_i lies in $\mathfrak{a} \subset \mathfrak{b}$. Hence each f_i is zero on $V(\mathfrak{b})$, and so f is zero on $V(\mathfrak{b})$. □

LEMMA 1.6 *Let A and B be finitely generated algebras over an algebraically closed field k. If* $\operatorname{spm} A$ *and* $\operatorname{spm} B$ *are connected, then so also is* $\operatorname{spm} A \otimes B$.

PROOF. Because of the Nullstellensatz, we can identify $\operatorname{spm} A \otimes B$ with $\operatorname{spm} A \times \operatorname{spm} B$ (as a set). For $\mathfrak{m}_1 \in \operatorname{spm} A$, the k-algebra homomorphisms

$$B \simeq (A/\mathfrak{m}_1) \otimes B \twoheadleftarrow A \otimes B$$

give continuous maps

$$\mathfrak{n} \mapsto (\mathfrak{m}_1, \mathfrak{n}) \colon \operatorname{spm}(B) \simeq \operatorname{spm}(A/\mathfrak{m}_1 \otimes B) \overset{\text{closed}}{\hookrightarrow} \operatorname{spm}(A \otimes B) \simeq \operatorname{spm}(A) \times \operatorname{spm}(B).$$

Similarly, for $\mathfrak{n}_2 \in \operatorname{spm} B$, we have continuous maps

$$\mathfrak{m} \mapsto (\mathfrak{m}, \mathfrak{n}_2) \colon \operatorname{spm}(A) \simeq \operatorname{spm}(A \otimes B/\mathfrak{n}_2) \overset{\text{closed}}{\hookrightarrow} \operatorname{spm}(A \otimes B) \simeq \operatorname{spm}(A) \times \operatorname{spm}(B).$$

The images of $\operatorname{spm} A$ and $\operatorname{spm} B$ in $\operatorname{spm}(A) \times \operatorname{spm}(B)$ intersect in $(\mathfrak{m}_1, \mathfrak{n}_2)$ and are connected, which shows that $(\mathfrak{m}_1, \mathfrak{n}_1)$ and $(\mathfrak{m}_2, \mathfrak{n}_2)$ lie in the same connected component of $\operatorname{spm} A \times \operatorname{spm} B$ for all $\mathfrak{n}_1 \in \operatorname{spm}(B)$ and $\mathfrak{m}_2 \in \operatorname{spm}(A)$. □

ASIDE 1.7 On $\mathbb{C}^n$ there are two topologies: the Zariski topology, whose closed sets are the zero sets of collections of polynomials, and the complex topology. Clearly Zariski-closed sets are closed for the complex topology, and so the complex topology is the finer than the Zariski topology. It follows that a subset of $\mathbb{C}^n$ that is connected in the complex topology is connected in the Zariski topology. The converse is false. For example, if we remove the real axis from $\mathbb{C}$, the resulting space is not connected for the complex topology but it is connected for the topology induced by the Zariski topology (a nonempty Zariski-open subset of $\mathbb{C}$ can omit only finitely many points). Thus the next result is a surprise:

> If $V \subset \mathbb{C}^n$ is closed and irreducible for the Zariski topology, then it is connected for the complex topology.

For the proof, see Shafarevich 1994, VII 2.

2 Étale subalgebras

Let A be a finitely generated k-algebra. An étale k-subalgebra of A will give an étale k^{al}-subalgebra of the same degree of $A_{k^{\mathrm{al}}}$ (XII, 2.6), and so its degree is bounded by the number of connected components of $\operatorname{spm} A_{k^{\mathrm{al}}}$ (1.4). The composite of two étale subalgebras of A is étale (XII, 2.5), and so there is a largest étale k-subalgebra $\pi_0(A)$ of A, containing all other étale subalgebras.

Let K be a field containing k. Then $K \otimes \pi_0(A)$ is an étale K-subalgebra of $K \otimes A$ (see XII, 2.6). We shall need to know that it is the largest étale subalgebra.

PROPOSITION 2.1 *Let A be a finitely generated k-algebra, and let K be a field containing k. Then*

$$K \otimes \pi_0(A) = \pi_0(K \otimes A).$$

PROOF. We first prove the statement with $K = k^{\mathrm{sep}}$. It follows from (XII, 2.8) that the map

$$B \mapsto k^{\mathrm{sep}} \otimes B$$

is a bijection from the set of étale k-subalgebras of A to the set of étale k^{sep}-algebras of $k^{\mathrm{sep}} \otimes A$ stable under the action of $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$; its inverse is $B \mapsto B^{\Gamma}$. Because it is the (unique) largest étale k^{sep}-algebra in $k^{\mathrm{sep}} \otimes A$, $\pi_0(k^{\mathrm{sep}} \otimes A)$ is stable under the action of Γ. The étale k-subalgebras $\pi_0(A)$ and $\pi_0(k^{\mathrm{sep}} \otimes A)^{\Gamma}$ correspond to the étale k^{sep}-subalgebras $k^{\mathrm{sep}} \otimes \pi_0(A)$ and $\pi_0(k^{\mathrm{sep}} \otimes A)$ respectively. As $k^{\mathrm{sep}} \otimes \pi_0(A) \subset \pi_0(k^{\mathrm{sep}} \otimes A)$, we have $\pi_0(A) \subset \pi_0(k^{\mathrm{sep}} \otimes A)^{\Gamma}$; hence $\pi_0(A) = \pi_0(k^{\mathrm{sep}} \otimes A)^{\Gamma}$ (maximality of $\pi_0(A)$), and so $k^{\mathrm{sep}} \otimes \pi_0(A) = \pi_0(k^{\mathrm{sep}} \otimes A)$.

We next prove the statement when $k = k^{\mathrm{sep}}$ and $K = k^{\mathrm{al}}$. If $K \neq k$, then k has characteristic $p \neq 0$ and K is purely inseparable over it. Let $e_1, \ldots, e_m$ be a basis of idempotents for $\pi_0(A \otimes K)$. Write $e_j = \sum a_i \otimes c_i$ with $a_i \in A$ and $c_i \in K$. For some r, all the elements $c_i^{p^r}$ lie in k, and then $e_j^{p^r} = \sum a_i^{p^r} \otimes c_i^{p^r} \in A$. But $e_j = e_j^{p^r}$, and so $\pi_0(A \otimes K)$ has a basis in A.

We now prove the statement when k and K are both algebraically closed. We may suppose that A is not a product of k-algebras, and so has no nontrivial idempotents. We have to show that then $A \otimes K$ also has no nontrivial idempotents, but this follows from 1.5.

Finally, we prove for a general K. Let K^{al} be an algebraic closure of K, and let k^{al} be the algebraic closure of k in K^{al}. If $K \otimes \pi_0(A)$ is not the largest étale subalgebra of $K \otimes A$, then $K^{\mathrm{al}} \otimes \pi_0(A) = K^{\mathrm{al}} \otimes_K K \otimes \pi_0(A)$ is not the largest étale subalgebra of $K^{\mathrm{al}} \otimes A$, but this contradicts the above statements. □

COROLLARY 2.2 *Let A be a finitely generated k-algebra. The degree $[\pi_0(A){:}k]$ of $\pi_0(A)$ is equal to the number of connected components of* $\mathrm{spm}(k^{\mathrm{al}} \otimes A)$.

PROOF. We have

$$[\pi_0(A){:}k] = [k^{\mathrm{al}} \otimes \pi_0(A){:}k^{\mathrm{al}}] = [\pi_0(k^{\mathrm{al}} \otimes A){:}k^{\mathrm{al}}],$$

and so this follows from 1.4. □

Let A and A' be finitely generated k-algebras. Then $\pi_0(A) \otimes \pi_0(A')$ is an étale subalgebra of $A \otimes A'$ (see XII, 2.4). We shall need to know that it is the largest étale subalgebra.

PROPOSITION 2.3 *Let A and A' be finitely generated k-algebras. Then*

$$\pi_0(A \otimes A') = \pi_0(A) \otimes \pi_0(A').$$

PROOF. As $\pi_0(A) \otimes \pi_0(A') \subset \pi_0(A \otimes A')$, we may suppose that k is algebraically closed (2.1), and we may replace each of A and A' with a direct factor and so suppose that $\pi_0(A) = 1 = \pi_0(A')$. We then have to show that $\pi_0(A \otimes A') = 1$, but this follows from 1.6. □

ASIDE 2.4 Let V be an algebraic variety over a field k, and let $\pi_0(V_{k^{\mathrm{sep}}})$ be the set of connected components of V over k^{sep}. Then $\pi_0(V_{k^{\mathrm{sep}}})$ is a finite set with an action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$, and so defines an étale k-algebra B (XII, 2.7). Let $\pi_0(V) = \mathrm{spm}\, B$. Then $\pi_0(V)$ is an algebraic variety, (finite and) étale over k, and there is a canonical morphism $V \to \pi_0(V)$ of algebraic varieties whose fibres are connected.[2] For a projective variety, this is the Stein factorization of the morphism $V \to \mathrm{Spm}\, k$ (cf. Hartshorne 1977, III, 11.5). For an affine variety $V = \mathrm{spm}\, A$, $\pi_0(V) = \mathrm{spm}(\pi_0(A))$.

[2] More precisely, let $\mathfrak{m}$ be a point of $\mathrm{spm}(\pi_0(V))$, and let $k(\mathfrak{m})$ be the residue field at $\mathfrak{m}$ (finite extension of k). Then the fibre over $\mathfrak{m}$ is a geometrically connected algebraic variety over $k(\mathfrak{m})$.

3 Algebraic groups

In this section, G is an affine algebraic group with coordinate ring $A = \mathcal{O}(G)$. The map $\Delta\colon A \to A \otimes A$ is a k-algebra homomorphism, and so sends $\pi_0(A)$ into $\pi_0(A \otimes A) \overset{2.3}{=} \pi_0(A) \otimes \pi_0(A)$. Similarly, $S\colon A \to A$ sends $\pi_0(A)$ into $\pi_0(A)$, and we can define ϵ on $\pi_0(A)$ to be the restriction of ϵ on A. Therefore $\pi_0(A)$ is a Hopf subalgebra of A.

DEFINITION 3.1 Let G be an algebraic group over a field k.

(a) The ***group of connected components*** $\pi_0(G)$ of G is the quotient algebraic group corresponding to the Hopf subalgebra $\pi_0(\mathcal{O}(G))$ of $\mathcal{O}(G)$.
(b) The ***identity component*** G° of G is the kernel of the homomorphism $G \to \pi_0(G)$.

PROPOSITION 3.2 *The following four conditions on an algebraic group G are equivalent:*

(a) *the étale affine group $\pi_0(G)$ is trivial;*
(b) *the topological space* $\mathrm{spm}(\mathcal{O}(G))$ *is connected;*
(c) *the topological space* $\mathrm{spm}(\mathcal{O}(G))$ *is irreducible;*
(d) *the ring* $\mathcal{O}(G)/\mathfrak{N}$ *is an integral domain.*

PROOF. (b)⇒(a). Condition (b) implies that $\pi_0(\mathcal{O}(G))$ has no nontrivial idempotents (see 1.3), and so is a field. The existence of the k-algebra homomorphism $\epsilon\colon\mathcal{O}(G) \to k$ then implies that $\pi_0(\mathcal{O}(G)) = k$.

(c)⇒(b). Trivial.

(d)⇔(c). In general, $\mathrm{spm}\, A$ is irreducible if and only if the nilradical of A is prime (see III, §1).

(a)⇒(d). If $\pi_0(G)$ is trivial, so also is $\pi_0(G_{k^{\mathrm{al}}})$ (Lemma 2.1). Write $\mathrm{spm}\,\mathcal{O}(G_{k^{\mathrm{al}}})$ as a union of its irreducible components. By definition, no irreducible component is contained in the union of the remainder. Therefore, there exists a point that lies on exactly one irreducible component. By homogeneity (VI, 5.1), all points have this property, and so the irreducible components are disjoint. As $\mathrm{spm}\,\mathcal{O}(G_{k^{\mathrm{al}}})$ is connected, there must be only one, and so $G_{k^{\mathrm{al}}}$ is irreducible. Let $\mathfrak{N}'$ be the nilradical of $\mathcal{O}(G_{k^{\mathrm{al}}})$ — we have shown that $\mathcal{O}(G_{k^{\mathrm{al}}})/\mathfrak{N}'$ is an integral domain. The canonical map $\mathcal{O}(G) \to k^{\mathrm{al}} \otimes \mathcal{O}(G) \simeq \mathcal{O}(G_{k^{\mathrm{al}}})$ is injective, and remains injective after we have passed to the quotients by the respective nilradicals, and so $\mathcal{O}(G)/\mathfrak{N}$ is an integral domain. □

DEFINITION 3.3 An affine algebraic group is ***connected*** if it satisfies the equivalent conditions of the proposition.

Thus an algebraic group G is connected if and only if it has no nontrivial étale quotient.

PROPOSITION 3.4 *The fibres of the map $|G| \to |\pi_0(G)|$ are the connected components of the topological space $|G|$.*

PROOF. The connected components of $|G|$ and the points of $|\pi_0(G)|$ are both indexed by the elements of a maximal complete set of orthogonal idempotents. □

PROPOSITION 3.5 *Every homomorphism from G to an étale algebraic group factors uniquely through $G \to \pi_0(G)$.*

PROOF. Let $G \to H$ be a homomorphism from G to an étale algebraic group H. The image of $\mathcal{O}(H)$ in $\mathcal{O}(G)$ is étale (see XII, 2.4), and so is contained in $\pi_0(\mathcal{O}(G)) \overset{\text{def}}{=} \mathcal{O}(\pi_0 G)$. □

PROPOSITION 3.6 *The subgroup G° of G is connected, and every homomorphism from a connected algebraic group to G factors through $G^\circ \to G$.*

PROOF. The homomorphism of k-algebras $\epsilon\colon \mathcal{O}(\pi_0 G) \to k$ decomposes $\mathcal{O}(\pi_0 G)$ into a direct product

$$\mathcal{O}(\pi_0 G) = k \times B.$$

Let $e = (1,0)$. Then the augmentation ideal of $\mathcal{O}(\pi_0 G)$ is $(1-e)$, and

$$\mathcal{O}(G) = e\mathcal{O}(G) \times (1-e)\mathcal{O}(G)$$

with $e\mathcal{O}(G) \simeq \mathcal{O}(G)/(1-e)\mathcal{O}(G) = \mathcal{O}(G^\circ)$ (see VII, 4.1). Clearly, $k = \pi_0(e\mathcal{O}(G)) \simeq \pi_0(\mathcal{O}(G^\circ))$. Therefore $\pi_0 G^\circ = 1$, which implies that G° is connected.

If H is connected, then the composite $H \to G \to \pi_0(G)$ has trivial image. □

PROPOSITION 3.7 *The subgroup G° is the unique connected normal affine subgroup of G such that G/G° is étale.*

PROOF. The subgroup G° is normal with étale quotient by definition, and we have shown it to be connected. Suppose that H is a second normal algebraic subgroup of G. If G/H is étale, then (by (a)) the homomorphism $G \to G/H$ factors through $\pi_0(G)$, and so we get a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & G^\circ \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & \pi_0 G \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & G/H \arrow[r] & 1
\end{tikzcd}$$

with exact rows. The similar diagram with each $*$ replaced with $*(R)$ gives, for each k-algebra R, an exact sequence

$$1 \to G^\circ(R) \to H(R) \to (\pi_0 G)(R). \tag{116}$$

Since this functorial in R, it gives a sequence of algebraic groups

$$1 \to G^\circ \to H \to \pi_0 G.$$

The exactness of (116) shows that G° is the kernel of $H \to \pi_0 G$. This map factors through $\pi_0 H$, and so if $\pi_0 H = 1$, its kernel is H: therefore $G^\circ \simeq H$. □

Proposition 3.7 says that, for any algebraic group G, there is a unique exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

such that G° is connected and $\pi_0(G)$ is étale. This is sometimes called the ***connected-étale exact sequence***.

The next proposition says that the functors $G \rightsquigarrow \pi_0 G$ and $G \rightsquigarrow G^\circ$ commute with extension of the base field.

PROPOSITION 3.8 *For any field extension $k' \supset k$,*

$$\pi_0(G_{k'}) \simeq \pi_0(G)_{k'}$$
$$(G_{k'})^{\circ} \simeq (G^{\circ})_{k'}.$$

In particular, G is connected if and only if $G_{k'}$ is connected.

PROOF. As $\mathcal{O}(G_{k'}) \simeq \mathcal{O}(G) \otimes_k k'$, this follows from (2.1). □

PROPOSITION 3.9 *For any algebraic groups G and G',*

$$\pi_0(G \times G') \simeq \pi_0(G) \times \pi_0(G')$$
$$(G \times G')^{\circ} \simeq G^{\circ} \times G'^{\circ}.$$

In particular, $G \times G'$ is connected if and only if both G and G' are connected.

PROOF. The coordinate ring $\mathcal{O}(G \times G') \simeq \mathcal{O}(G) \otimes \mathcal{O}(G')$, and so the first isomorphism follows from (2.3). □

REMARK 3.10 Let G be an algebraic group over k. For any field k' containing k, Proposition 3.8 shows that G is connected if and only if $G_{k'}$ is connected. In particular, if an algebraic group G over a field is connected, then so also is $G_{k^{\mathrm{al}}}$. In other words, a connected algebraic group is geometrically connected. This is false for algebraic varieties: for example,

$$X^2 + Y^2 = 0$$

is connected over $\mathbb{R}$ (even irreducible), but becomes a disjoint union of the two lines

$$X + \pm iY = 0$$

over $\mathbb{C}$ — the ring $\mathbb{R}[X,Y]/(X^2+Y^2)$ is an integral domain, but

$$\mathbb{C}[X,Y]/(X^2+Y^2) \simeq \mathbb{C}[X,Y]/(X+iY) \times \mathbb{C}[X,Y]/(X-iY).$$

The reason for the difference is the existence of the homomorphism $\epsilon\colon \mathcal{O}(G) \to k$ (the neutral element of $G(k)$). An integral affine algebraic variety V over a field k is geometrically connected if and only if k is algebraically closed in $\mathcal{O}(V)$, which is certainly the case if there exists a k-algebra homomorphism $\mathcal{O}(V) \to k$ (AG 11.5).

PROPOSITION 3.11 *Let*

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of algebraic groups. If N and Q are connected, so also is G; conversely, if G is connected, so also is Q.

PROOF. Assume N and Q are connected. Then N is contained in the kernel of $G \to \pi_0(G)$, so this map factors through $G \to Q$ (see VII, 7.8); therefore it factors through $\pi_0(Q) = 1$. Conversely, since G maps onto $\pi_0(Q)$, it must be trivial if G is connected. □

Examples

3.12 Let G be finite. When k has characteristic zero, G is étale, and so $G = \pi_0(G)$ and $G^\circ = 1$. Otherwise, there is an exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1.$$

When k is perfect, the homomorphism $G \to \pi_0(G)$ has a section, and so G is a semidirect product

$$G = G^\circ \rtimes \pi_0(G).$$

To see this, note that the homomorphism $G_{\mathrm{red}} \to \pi_0(G)$ is an isomorphism because both groups are étale and it is an isomorphism on k^{al}-points:

$$G_{\mathrm{red}}(k^{\mathrm{al}}) = G(k^{\mathrm{al}}) \xrightarrow{\approx} \pi_0(G)(k^{\mathrm{al}}).$$

The groups $\mathbb{G}_a$, GL_n, $\mathbb{T}_n$ (upper triangular), $\mathbb{U}_n$ (strictly upper triangular), $\mathbb{D}_n$ are connected because in each case $\mathcal{O}(G)$ is an integral domain. For example,

$$k[\mathbb{T}_n] = k[\mathrm{GL}_n]/(X_{ij} \mid i > j),$$

which is isomorphic to the polynomial ring in the symbols X_{ij}, $1 \leq i \leq j \leq n$, with the product $X_{11} \cdots X_{nn}$ inverted.

3.13 For the group G of monomial matrices (IV, 1.12), $\pi_0(\mathcal{O}(G))$ is a product of copies of k indexed by the elements of S_n. Thus, $\pi_0 G = S_n$ (regarded as a constant algebraic group, and $G^\circ = \mathbb{D}_n$.

3.14 The group SL_n is connected. As we noted in the proof of (VII, 5.11), the natural isomorphism of set-valued functors

$$A, r \mapsto A \cdot \mathrm{diag}(r, 1, \ldots, 1) \colon \mathrm{SL}_n(R) \times \mathbb{G}_m(R) \to \mathrm{GL}_n(R)$$

defines an isomorphism of k-algebras

$$\mathcal{O}(\mathrm{GL}_n) \simeq \mathcal{O}(\mathrm{SL}_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

and the algebra on the right contains $\mathcal{O}(\mathrm{SL}_n)$. In particular, $\mathcal{O}(\mathrm{SL}_n)$ is a subring of $\mathcal{O}(\mathrm{GL}_n)$, and so it is an integral domain.

3.15 Assume $\mathrm{char}(k) \neq 2$. For any nondegenerate quadratic space (V, q), the algebraic group $\mathrm{SO}(q)$ is connected. It suffices to prove this after replacing k with k^{al}, and so we may suppose that q is the standard quadratic form $X_1^2 + \cdots + X_n^2$, in which case we write $\mathrm{SO}(q) = \mathrm{SO}_n$. The latter is shown to be connected in Exercise XIII-4 below.

The determinant defines a quotient map $O(q) \to \{\pm 1\}$ with kernel $\mathrm{SO}(q)$. Therefore $O(q)^\circ = \mathrm{SO}(q)$ and $\pi_0(O(q)) = \{\pm 1\}$ (constant algebraic group).

3.16 The symplectic group Sp_{2n} is connected (for some hints on how to prove this, see Springer 1998, 2.2.9).

ASIDE 3.17 According to (1.7) and (3.2), an algebraic group G over $\mathbb{C}$ is connected if and only if $G(\mathbb{C})$ is connected for the complex topology. Thus, we could for example deduce that GL_n over $\mathbb{C}$ is a connected algebraic group from knowing that $\mathrm{GL}_n(\mathbb{C})$ is connected for the complex topology. However, it is easier to deduce that $\mathrm{GL}_n(\mathbb{C})$ is connected from knowing that GL_n is connected (of course, this requires the serious theorem stated in (1.7)).

3.18 An algebraic group G over $\mathbb{R}$ may be connected without $G(\mathbb{R})$ being connected for the real topology, and conversely. For example, GL_2 is connected as an algebraic group, but $\mathrm{GL}_2(\mathbb{R})$ is not connected for the real topology, and μ_3 is not connected as an algebraic group, but $\mu_3(\mathbb{R}) = \{1\}$ is certainly connected for the real topology.

3.19 In characteristic zero, an algebraic group is connected if and only if it is strongly connected (XII, 2.10).

4 Affine groups

Let G be an affine group, and write it as the inverse limit $G = \varprojlim_{i\in I} G_i$ of its family $(G_i)_{i\in I}$ of algebraic quotients (see VIII, 8.1). Define

$$G^\circ = \varprojlim_{i\in I} G_i^\circ,$$
$$\pi_0 G = \varprojlim_{i\in I} \pi_0 G_i.$$

ASIDE 4.1 For a smooth group scheme G of finite presentation over a scheme S, there is a unique open subgroup scheme G° of G such that $(G^\circ)_s = (G_s)^\circ$ for all $s \in S$. See SGA 3, VI_B, 3.10, p.355. However, even when G is affine over S, G° need not be affine over S.

NOTES Discuss connectedness over a base ring (or scheme). The useful condition is not that G be connected as a scheme, but that its fibres be connected.

5 Exercises

EXERCISE XIII-1 Show that if $1 \to N \to G \to Q \to 1$ is exact, so also is $\pi_0(N) \to \pi_0(G) \to \pi_0(Q) \to 1$. Give an example to show that $\pi_0(N) \to \pi_0(G)$ need not be injective.

EXERCISE XIII-2 What is the map $\mathcal{O}(\mathrm{SL}_n) \to \mathcal{O}(\mathrm{GL}_n)$ defined in example 3.14?

EXERCISE XIII-3 Prove directly that $\pi_0(\mathcal{O}(\mathrm{O}_n)) = k \times k$.

EXERCISE XIII-4 (Springer 1998, 2.2.2). Assume k has characteristic $\neq 2$. For any k-algebra R, let $V(R)$ be the set of skew-symmetric matrices, i.e., the matrices A such that $A^t = -A$.

(a) Show that the functor $R \mapsto V(R)$ is represented by a finitely generated k-algebra A, and that A is an integral domain.

(b) Show that $A \mapsto (I_n + A)^{-1}(I_n - A)$ defines a bijection from a nonempty open subset of $\mathrm{SO}_n(k^{\mathrm{al}})$ onto an open subset of $V(k^{\mathrm{al}})$.

(c) Deduce that SO_n is connected.

EXERCISE XIII-5 Let A be a product of copies of k indexed by the elements of a finite set S. Show that the k-bialgebra structures on A are in natural one-to-one correspondence with the group structures on S.

EXERCISE XIII-6 Let G be a finite affine group. Show that the following conditions are equivalent:

(a) the k-algebra $\mathcal{O}(G_{\mathrm{red}})$ is étale;
(b) $\mathcal{O}(G_{\mathrm{red}}) \otimes \mathcal{O}(G_{\mathrm{red}})$ is reduced;
(c) G_{red} is a subgroup of G;
(d) G is isomorphic to the semi-direct product of G° and $\pi_0 G$.

EXERCISE XIII-7 Let k be a nonperfect field of characteristic 2, so that there exists an $a \in k$ that is not a square. Show that the functor $R \rightsquigarrow G(R) \overset{\mathrm{def}}{=} \{x \in R \mid x^4 = ax^2\}$ becomes a finite commutative algebraic group under addition. Show that $G(k)$ has only one element but $\pi_0(G)$ has two. Deduce that G is not isomorphic to the semi-direct product of G° and $\pi_0(G)$. (Hence XIII-6 shows that $\mathcal{O}(G)/\mathfrak{N}$ is not a Hopf algebra.)

EXERCISE XIII-8 Let k be a field of characteristic p. Show that the extensions

$$0 \to \mu_p \to G \to \mathbb{Z}/p\mathbb{Z} \to 0$$

with G a finite commutative algebraic group are classified by the elements of $k^{\times}/k^{\times p}$ (the split extension $G = \mu_p \times \mathbb{Z}/p\mathbb{Z}$ corresponds to the trivial element in $k^{\times}/k^{\times p}$). Show that G_{red} is not a subgroup of G unless the extension splits.

6 Where we are

As discussed in the first section, every affine algebraic group has a composition series with the quotients listed at right:

$$\begin{tikzcd}
\text{affine} & G \arrow[d, dash, "\text{finite étale}"] \\
\text{connected} & G^{\circ} \arrow[d, dash, "\text{semisimple}"] \\
\text{solvable} & \bullet \arrow[d, dash, "\text{torus}"] \\
\text{unipotent} & \bullet \arrow[d, dash, "\text{unipotent}"] \\
 & \{1\}
\end{tikzcd}$$

We have constructed the top segment of this picture. Next we look at tori and unipotent groups. Then we study the most interesting groups, the semisimple ones, and finally, we put everything together.

CHAPTER **XIV**

Groups of Multiplicative Type; Tori

In this chapter we study the affine groups that become diagonalizable over an extension field. Through k is a field.

We state for reference:

$$\begin{array}{lllll} \mathbb{G}_m(R) = R^\times & \mathcal{O}(\mathbb{G}_m) = k[X, X^{-1}] & \Delta(X) = X \otimes X & \epsilon(X) = 1 & S(X) = X^{-1} \\ \mu_n(R) = \{\zeta \in R \mid \zeta^n = 1\} & \mathcal{O}(\mu_n) = \frac{k[X]}{(X^n - 1)} = k[x] & \Delta(x) = x \otimes x & \epsilon(x) = 1 & S(x) = x^{n-1} \end{array}$$

For an algebraic group G over a field k,

$$\begin{aligned} X(G) &= \mathrm{Hom}(G, \mathbb{G}_m) \quad \text{(meaning homomorphisms over } k\text{)} \\ X^*(G) &= \mathrm{Hom}(G_{k^{\mathrm{sep}}}, \mathbb{G}_{m k^{\mathrm{sep}}}). \end{aligned}$$

[Need to prove somewhere: a smooth connected algebraic group is a torus if and only if all the elements of $G(k^{\mathrm{al}})$ are semisimple.]

1 Group-like elements

DEFINITION 1.1 Let $A = (A, \Delta, \epsilon)$ be a k-coalgebra. An element a of A is ***group-like*** if $\Delta(a) = a \otimes a$ and $\epsilon(a) = 1$.

LEMMA 1.2 *The group-like elements in A are linearly independent.*

PROOF. If not, it will be possible to express one group-like element e as a linear combination of other group-like elements $e_i \neq e$:

$$e = \textstyle\sum_i c_i e_i, \quad c_i \in k. \tag{117}$$

We may even suppose that the e_i occurring in the sum are linearly independent. Now

$$\begin{aligned} \Delta(e) &= e \otimes e = \textstyle\sum_{i,j} c_i c_j e_i \otimes e_j \\ \Delta(e) &= \textstyle\sum_i c_i \Delta(e_i) = \textstyle\sum_i c_i e_i \otimes e_i. \end{aligned}$$

The $e_i \otimes e_j$ are also linearly independent, and so this implies that

$$\begin{cases} c_i c_i = c_i & \text{all } i \\ c_i c_j = 0 & \text{if } i \neq j. \end{cases}$$

We also know that

$$\begin{aligned}\epsilon(e) &= 1\\ \epsilon(e) &= \sum c_i\epsilon(e_i) = \sum c_i.\end{aligned}$$

On combining these statements, we see that the c_i form a complete set of orthogonal idempotents in the field k, and so one of them equals 1 and the remainder are zero, which contradicts our assumption that e is not equal to any of the e_i. □

Let A be a k-bialgebra. If a and b are group-like elements in A, then

$$\begin{aligned}\Delta(ab) &= \Delta(a)\Delta(b) = (a\otimes a)(b\otimes b) = ab\otimes ab\\ \epsilon(ab) &= \epsilon(a)\epsilon(b) = 1\end{aligned}$$

because Δ and ϵ are k-algebra homomorphisms. Therefore the group-like elements form a submonoid of $(A,\times)$.

Let A be a Hopf algebra, and let $a\in A$. If a is group-like, then

$$1 = (e\circ\epsilon)(a) \overset{\text{II, (19)}}{=} (\text{mult}\circ(S\otimes\text{id}_A)\circ\Delta)(a) = S(a)a,$$

and so a is a unit in A with $a^{-1} = S(a)$. Conversely, if a is a unit in A such that $\Delta(a) = a\otimes a$, then

$$a \overset{\text{II}}{=} ((\epsilon,\text{id}_A)\circ\Delta)(a) = \epsilon(a)a,$$

and so $\epsilon(a) = 1$. Thus the group-like elements of A are exactly the units such that $\Delta(a) = a\otimes a$.

ASIDE 1.3 We have just seen that the group-like elements in a Hopf algebra over a field are invertible. Conversely, if the group-like elements in a commutative or cocommutative bialgebra are invertible, then the bialgebra admits an inversion, but this is false for a general bialgebra. See mo86197.

2 The characters of an affine group

Recall that a character of an affine group G is a homomorphism $\chi\colon G\to\mathbb{G}_m$. To give a character χ of G is the same as giving a homomorphism of k-algebras $\mathcal{O}(\mathbb{G}_m)\to\mathcal{O}(G)$ respecting the comultiplications, and this is the same as giving a unit $a(\chi)$ of $\mathcal{O}(G)$ (the image of X) such that $\Delta(a(\chi)) = a(\chi)\otimes a(\chi)$. Therefore, $\chi\leftrightarrow a(\chi)$ is a one-to-one correspondence between the characters of G and the group-like elements of $\mathcal{O}(G)$.

For characters χ,χ', define

$$\chi+\chi'\colon G(R)\to R^\times$$

by

$$(\chi+\chi')(g) = \chi(g)\cdot\chi'(g).$$

Then $\chi+\chi'$ is again a character, and the set of characters is an commutative group, denoted $X(G)$. The correspondence $\chi\leftrightarrow a(\chi)$ between characters and group-like elements has the property that

$$a(\chi+\chi') = a(\chi)\cdot a(\chi').$$

ASIDE 2.1 Recall (I, 3.13) that an element f of $\mathcal{O}(G)$ can be regarded as a natural transformation $f\colon G \to \mathbb{A}^1$. Suppose that

$$\begin{cases} f(1_G) = 1, & \text{for } 1_G \text{ the identity element in } G(R)\text{, and} \\ f(xy) = f(x)f(y), & \text{for } x, y \in G(R),\ R \text{ a } k\text{-algebra.} \end{cases} \tag{118}$$

Then $f(R)$ takes values in $R^\times \subset \mathbb{A}^1(R)$ and is a homomorphism $G(R) \to R^\times$. In other words, f is a character of G. One can see directly from the definitions that the condition (118) holds if and only if f is group-like.

3 The affine group $D(M)$

Let M be a commutative group (written multiplicatively), and let $k[M]$ be the k-vector space with basis M. Thus, the elements of $k[M]$ are finite sums

$$\textstyle\sum_i a_i m_i, \quad a_i \in k, \quad m_i \in M.$$

When we endow $k[M]$ with the multiplication extending that on M,

$$\left(\textstyle\sum_i a_i m_i\right)\left(\textstyle\sum_j b_j n_j\right) = \textstyle\sum_{i,j} a_i b_j m_i n_j,$$

then $k[M]$ becomes a k-algebra, called the ***group algebra*** of M. It becomes a Hopf algebra when we set

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1} \qquad (m \in M)$$

because, for m an element of the basis M,

$$\begin{aligned} (\mathrm{id} \otimes \Delta)(\Delta(m)) = m \otimes (m \otimes m) = (m \otimes m) \otimes m = (\Delta \otimes \mathrm{id})(\Delta(m)), \\ (\epsilon \otimes \mathrm{id})(\Delta(m)) = 1 \otimes m, \qquad (\mathrm{id} \otimes \epsilon)(\Delta(m)) = m \otimes 1, \\ (\mathrm{mult} \circ (S \otimes \mathrm{id}))(m \otimes m) = 1 = (\mathrm{mult} \circ (\mathrm{id} \otimes S))(m \otimes m) \end{aligned}$$

(see also II, 4.6). Note that $k[M]$ is generated as a k-algebra by any set of generators for M, and so it is finitely generated if M is finitely generated.

EXAMPLE 3.1 Let M be a cyclic group, generated by e.

(a) Case e has infinite order. Then the elements of $k[M]$ are the finite sums $\sum_{i \in \mathbb{Z}} a_i e^i$ with the obvious addition and multiplication, and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, $S(e) = e^{-1}$. Therefore, $k[M] \simeq k[\mathbb{G}_m]$.

(b) Case e is of order n. Then the elements of $k[M]$ are sums $a_0 + a_1 e + \cdots + a_{n-1} e^{n-1}$ with the obvious addition and multiplication (using $e^n = 1$), and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, and $S(e) = e^{n-1}$. Therefore, $k[M] \simeq k[\mu_n]$.

EXAMPLE 3.2 Recall that if W and V are vector spaces with bases $(e_i)_{i \in I}$ and $(f_j)_{j \in J}$, then $W \otimes_k V$ is a vector space with basis $(e_i \otimes f_j)_{(i,j) \in I \times J}$. Therefore, if M_1 and M_2 are commutative groups, then

$$(m_1, m_2) \leftrightarrow m_1 \otimes m_2 \colon k[M_1 \times M_2] \leftrightarrow k[M_1] \otimes k[M_2]$$

is an isomorphism of k-vector spaces, and one checks easily that it respects the Hopf k-algebra structures.

PROPOSITION 3.3 *For any commutative group M, the functor $D(M)$*

$$R \rightsquigarrow \operatorname{Hom}(M, R^{\times}) \quad \textit{(homomorphisms of groups)}$$

is an affine group, with coordinate ring $k[M]$. When M is finitely generated, the choice of a basis for M determines an isomorphism of $D(M)$ with a finite product of copies of $\mathbb{G}_m$ and various μ_n's.

PROOF. To give a k-linear map $k[M] \to R$ is the same as giving a map $M \to R$. The map $k[M] \to R$ is a k-algebra homomorphism if and only if $M \to R$ is a homomorphism from M into $R^{\times}$. This shows that $D(M)$ is represented by $k[M]$, and it is therefore an affine group.

A decomposition of commutative groups

$$M \approx \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

defines a decomposition of k-bialgebras

$$k[M] \approx k[\mathbb{G}_m] \otimes \cdots \otimes k[\mathbb{G}_m] \otimes k[\mu_{n_1}] \otimes \cdots \otimes k[\mu_{n_r}]$$

(3.1,3.2). Since every finitely generated commutative group M has such a decomposition, this proves the second statement. □

LEMMA 3.4 *The group-like elements of $k[M]$ are exactly the elements of M.*

PROOF. Let $e \in k[M]$ be group-like. Then

$$e = \sum c_i e_i \text{ for some } c_i \in k,\ e_i \in M.$$

The argument in the proof of Lemma 1.2 shows that the c_i form a complete set of orthogonal idempotents in k, and so one of them equals 1 and the remainder are zero. Therefore $e = e_i$ for some i. □

Thus

$$X(D(M)) \simeq M.$$

The character of $D(M)$ corresponding to $m \in M$ is

$$D(M)(R) \overset{\text{def}}{=} \operatorname{Hom}(M, R^{\times}) \xrightarrow{f \mapsto f(m)} R^{\times} \overset{\text{def}}{=} \mathbb{G}_m(R).$$

SUMMARY 3.5 Let p be the characteristic exponent[1] of k. Then:

$D(M)$ is algebraic	$\iff$	M is finitely generated
$D(M)$ is connected	$\iff$	M has only p-torsion
$D(M)$ is algebraic and smooth	$\iff$	M is finitely generated and has no p-torsion
$D(M)$ is algebraic, smooth, and connected	$\iff$	M is free and finitely generated.

[1] The characteristic exponent of a field k is p if k has characteristic $p \neq 0$, and it is 1 if k has characteristic zero.

We noted above that $D(M)$ is algebraic if M is finitely generated. If M is not finitely generated, then $D(M)$ is an infinite product of nontrivial groups, and so can't be algebraic. The affine group $D(\mathbb{Z}) = \mathbb{G}_m$ is connected and smooth. Let $n = n' \times p^m$ where n' is prime to p. Then $D(\mathbb{Z}/n\mathbb{Z}) = \mu_{n'} \times \mu_{p^m}$; the finite affine group $\mu_{n'}$ is étale (hence smooth), and it is nonconnected if $n' \neq 1$; the finite affine group μ_{p^m} is connected, and it is nonsmooth if $p^m \neq 1$.

Note that

$$\begin{aligned} D(M)^\circ &= D(M/\{\text{prime-to-}p \text{ torsion}\} \\ D(M)_{\text{red}} &= D(M/\{p\text{-torsion}\} \\ D(M)^\circ_{\text{red}} &= D(M/\{\text{torsion}\}. \end{aligned}$$

ASIDE 3.6 When M is an *additive* commutative group, it is more natural to define $k[M]$ to be the vector space with basis the set of symbols $\{e^m \mid m \in M\}$. The multiplication is then $e^m \cdot e^n = e^{m+n}$ and the comultiplication is $\Delta(e^m) = e^m \otimes e^m$.

4 Diagonalizable groups

DEFINITION 4.1 An affine group G is ***diagonalizable*** if the group-like elements in $\mathcal{O}(G)$ span it as a k-vector space.

THEOREM 4.2 *An affine group G is diagonalizable if and only if it is isomorphic to $D(M)$ for some commutative group M.*

PROOF. The group-like elements of $k[M]$ span it by definition. Conversely, suppose the group-like elements M span $\mathcal{O}(G)$. Lemma 1.2 shows that they form a basis for $\mathcal{O}(G)$ (as a k-vector space), and so the inclusion $M \hookrightarrow \mathcal{O}(G)$ extends to an isomorphism $k[M] \to \mathcal{O}(G)$ of vector spaces. That this isomorphism is compatible with the bialgebra structures (m, e, Δ, ϵ) can be checked on the basis elements $m \in M$, where it is obvious. □

ASIDE 4.3 When we interpret the characters of G as elements of $\mathcal{O}(G)$ satisfying (118), we can say that G is diagonalizable if and only if $\mathcal{O}(G)$ is spanned by characters.

THEOREM 4.4 *(a) The functor $M \rightsquigarrow D(M)$ is a contravariant equivalence from the category of commutative groups to the category of diagonalizable affine groups (with quasi-inverse $G \rightsquigarrow X(G)$).*
(b) If

$$1 \to M' \to M \to M'' \to 1$$

is an exact sequence of commutative groups, then

$$1 \to D(M'') \to D(M) \to D(M') \to 1$$

is an exact sequence of affine groups.
(c) Subgroups and quotient groups of diagonalizable affine groups are diagonalizable.

PROOF. (a) Certainly, we have a contravariant functor

$$D\colon \{\text{commutative groups}\} \rightsquigarrow \{\text{diagonalizable groups}\}.$$

We first show that D is fully faithful, i.e., that

$$\operatorname{Hom}(M,M') \to \operatorname{Hom}(D(M'),D(M)) \tag{119}$$

is an isomorphism for all M,M'. It sends direct limits to inverse limits and direct sums to products, and so it suffices to prove that (119) is an isomorphism when M and M' are cyclic. If, for example, M and M' are both infinite cyclic groups, then

$$\operatorname{Hom}(M,M') = \operatorname{Hom}(\mathbb{Z},\mathbb{Z}) \simeq \mathbb{Z},$$
$$\operatorname{Hom}(D(M'),D(M)) = \operatorname{Hom}(\mathbb{G}_m,\mathbb{G}_m) = \{X^i \mid i \in \mathbb{Z}\} \simeq \mathbb{Z},$$

and (119) is an isomorphism. The remaining cases are similarly easy.

Theorem 4.2 shows that the functor is essentially surjective, and so it is an equivalence.

(b) The map $k[M'] \to k[M]$ is injective, and so $D(M) \to D(M')$ is a quotient map (by definition). Its kernel is represented by $k[M]/I_{k[M']}$, where $I_{k[M']}$ is the augmentation ideal of $k[M']$ (see VII, 4.1). But $I_{k[M']}$ is the ideal generated the elements $m-1$ for $m \in M'$, and so $k[M]/I_{k[M']}$ is the quotient ring obtained by putting $m=1$ for all $m \in M'$. Therefore $M \to M''$ defines an isomorphism $k[M]/I_{k[M']} \to k[M'']$.

(c) If H is a subgroup of G, then $\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective, and so if the group-like elements of $\mathcal{O}(G)$ span it, the same is true of $\mathcal{O}(H)$.

Let $D(M) \to Q$ be a quotient map, and let H be its kernel. Then $H = D(M'')$ for some quotient M'' of M. Let M' be the kernel of $M \to M''$. Then $D(M) \to D(M')$ and $D(M) \to Q$ are quotient maps with the same kernel, and so are isomorphic (VII, 7.9). □

ASIDE 4.5 Our definition of a diagonalizable group agrees with that in SGA 3, VIII 1.1: a group scheme is diagonalizable if it is isomorphic to a scheme of the form $D(M)$ for some commutative group M.

Diagonalizable representations

DEFINITION 4.6 A representation of an affine group is ***diagonalizable*** if it is a sum of one-dimensional representations.

According to VIII, 17.3, a diagonalizable representation is a *direct* sum of one-dimensional representations.

Recall that $\mathbb{D}_n$ is the group of invertible diagonal $n \times n$ matrices; thus

$$\mathbb{D}_n \simeq \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n \text{ copies}} \simeq D(\mathbb{Z}^n).$$

A finite-dimensional representation (V,r) of an affine group G is diagonalizable if and only if there exists a basis for V such that $r(G) \subset \mathbb{D}_n$. In more down-to-earth terms, the representation defined by an inclusion $G \subset \mathrm{GL}_n$ is diagonalizable if and only if there exists an invertible matrix P in $M_n(k)$ such that, for all k-algebras R and all $g \in G(R)$,

$$PgP^{-1} \in \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}.$$

A character $\chi\colon G \to \mathbb{G}_m$ defines a representation of G on any finite-dimensional space V: let $g \in G(R)$ act on V_R as multiplication by $\chi(g) \in R^\times$. For example, χ defines a representation of G on k^n by

$$g \mapsto \begin{pmatrix} \chi(g) & & 0 \\ & \ddots & \\ 0 & & \chi(g) \end{pmatrix}.$$

Let (V,r) be a representation of G. We say that G ***acts on*** V ***through*** χ if

$$r(g)v = \chi(g)v \text{ all } g \in G(R),\ v \in V_R.$$

This means that the image of r is contained in the centre $\mathbb{G}_m$ of GL_V and that r is the composite of

$$G \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V.$$

Let $\rho\colon V \to V \otimes \mathcal{O}(G)$ be the coaction defined by r. Then G acts on V through the character χ if and only if

$$\rho(v) = v \otimes a(\chi), \quad \text{all } v \in V.$$

When V is 1-dimensional, $\mathrm{GL}_V = \mathbb{G}_m$, and so G always acts on V through some character.

Let (V,r) be a representation of G. If G acts on subspaces W and W' through the character χ, then it acts on $W + W'$ through the character χ. Therefore, for each $\chi \in X(G)$, there is a largest subspace V_χ (possibly zero) such that G acts on V_χ through χ. We have (VIII, 16.1)

$$V_\chi = \{v \in V \mid \rho(v) = v \otimes a(\chi)\}.$$

THEOREM 4.7 *The following conditions on an affine group G are equivalent:*

(a) *G is diagonalizable;*
(b) *every finite-dimensional representation of G is diagonalizable;*
(c) *every representation of G is diagonalizable;*
(d) *for every representation (V,r) of G,*

$$V = \bigoplus\nolimits_{\chi \in X(T)} V_\chi.$$

PROOF. (a)⇒(c): Let $\rho\colon V \to V \otimes \mathcal{O}(G)$ be the comodule corresponding to a representation of G (see VIII, 6.1). We have to show that V is a sum of one-dimensional representations or, equivalently, that V is spanned by vectors u such that $\rho(u) \in \langle u \rangle \otimes \mathcal{O}(G)$.

Let $v \in V$. As the group-like elements form a basis $(e_i)_{i \in I}$ for $\mathcal{O}(G)$, we can write

$$\rho(v) = \sum\nolimits_{i \in I} u_i \otimes e_i, \quad u_i \in V.$$

On applying the identities (p. 114)

$$\begin{cases} (\mathrm{id}_V \otimes \Delta) \circ \rho &= (\rho \otimes \mathrm{id}_A) \circ \rho \\ (\mathrm{id}_V \otimes \epsilon) \circ \rho &= \mathrm{id}_V. \end{cases}$$

to v, we find that

$$\sum\nolimits_i u_i \otimes e_i \otimes e_i = \sum\nolimits_i \rho(u_i) \otimes e_i$$
$$v = \sum u_i.$$

The first equality shows that

$$\rho(u_i) = u_i \otimes e_i \in \langle u_i \rangle \otimes_k A,$$

and the second shows that the set of u_i's arising in this way span V.

(c)⇒(a): In particular, the regular representation of G is diagonalizable, and so $\mathcal{O}(G)$ is spanned by its eigenvectors. Let $f \in \mathcal{O}(G)$ be an eigenvector for the regular representation, and let χ be the corresponding character. Then

$$f(hg) = f(h)\chi(g) \quad \text{for } h,g \in G(R),\ R \text{ a } k\text{-algebra.}$$

In particular, $f(g) = f(e)\chi(g)$, and so f is a multiple of χ. Hence $\mathcal{O}(G)$ is spanned by its characters.

(b)⇒(c): As every representation is a sum of finite-dimensional subrepresentations (VIII, 9.3), (b) implies that every representation is a sum of one-dimensional subrepresentations.

(c)⇒(b): Trivial.

(c)⇒(d): Certainly, (c) implies that $V = \sum_{\chi \in X(G)} V_\chi$, and Theorem 16.2, Chapter VIII, implies that the sum is direct.

(d)⇒(c): Clearly each space V_χ is a sum of one-dimensional representations. □

NOTES Part of this section duplicates VIII, §16.

NOTES An affine group G is diagonalizable if and only if $\mathsf{Rep}(G)$ is semisimple and every simple object has dimension 1 (equivalently, the tensor product of two simple objects in simple). Explain that to give a representation of $D(M)$ on V is the same as giving a gradation on V (for a base ring, see CGP A.8.8.). Explain that the categories of representations of diagonalizable affine groups are exactly the neutral tannakian categories graded by some commutative group M, and the Tannaka dual is $D(M)$. See also the last chapter.

Split tori

4.8 A ***split torus*** is an algebraic group isomorphic to a finite product of copies of $\mathbb{G}_m$. Equivalently, it is a connected diagonalizable algebraic group. Under the equivalence of categories $M \rightsquigarrow D(M)$ (see 4.4a), the split tori correspond to free commutative groups M of finite rank. A quotient of a split torus is again a split torus (because it corresponds to a subgroup of a free commutative group of finite rank), but a subgroup of a split torus need not be a split torus. For example, μ_n is a subgroup of $\mathbb{G}_m$ (the map $\mu_n \to \mathbb{G}_m$ corresponds to $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$).

EXAMPLE 4.9 Let T be the split torus $\mathbb{G}_m \times \mathbb{G}_m$. Then $X(T) \simeq \mathbb{Z} \oplus \mathbb{Z}$, and the character corresponding to $(m_1, m_2) \in \mathbb{Z} \oplus \mathbb{Z}$ is

$$(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2} \colon T(R) \to \mathbb{G}_m(R).$$

A representation V of T decomposes into a direct sum of subspaces $V_{(m_1,m_2)}$, $(m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}$, such that $(t_1, t_2) \in T(k)$ acts on $V_{(m_1,m_2)}$ as $t_1^{m_1} t_2^{m_2}$. In this way, the category $\mathsf{Rep}(T)$ acquires a gradation by the group $\mathbb{Z} \times \mathbb{Z}$.

5 Groups of multiplicative type

DEFINITION 5.1 An affine group G is of ***multiplicative type*** if $G_{k^{\mathrm{sep}}}$ is diagonalizable.

Let M be an commutative group, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. A ***continuous action*** of Γ on M is a homomorphism $\Gamma \to \mathrm{Aut}(M)$ such that every element of M is fixed by an open subgroup of Γ, i.e.,

$$M = \bigcup\nolimits_{K} M^{\mathrm{Gal}(k^{\mathrm{sep}}/K)}$$

where K runs through the finite Galois extensions of k contained in k^{sep}.

For an affine group G, we define

$$X^{*}(G) = \mathrm{Hom}(G_{k^{\mathrm{sep}}}, \mathbb{G}_m).$$

LEMMA 5.2 *The canonical action of Γ on $X^{*}(G)$ is continuous.*

PROOF. When G is algebraic, $X^{*}(G)$ is finitely generated, and each of its generators is defined over a finite separable extension of k; therefore the action factors through $\mathrm{Gal}(K/k)$ for some finite Galois extension K of k. In the general case, every homomorphism $G_{k^{\mathrm{sep}}} \to \mathbb{G}_m$ factors through an algebraic quotient of G, and so $X^{*}(G) = \bigcup X^{*}(Q)$ with Q algebraic. □

THEOREM 5.3 *The functor X^{*} is a contravariant equivalence from the category of affine groups of multiplicative type over k to the category of commutative groups with a continuous action of Γ. Under the equivalence, short exact sequences correspond to short exact sequences.*

PROOF. To give a continuous semilinear action of Γ on $k^{\mathrm{sep}}[M]$ is the same as giving a continuous action of Γ on M (because M is the set of group-like elements in $k^{\mathrm{sep}}[M]$ and M is a k^{sep}-basis for $k^{\mathrm{sep}}[M]$), and so this follows from Theorem 4.4 and Proposition 7.3, Chapter V. □

Let G be a group of multiplicative type over k. For any $K \subset k^{\mathrm{sep}}$,

$$G(K) = \mathrm{Hom}(X^{*}(G), k^{\mathrm{sep}\times})^{\Gamma_K}$$

where Γ_K is the subgroup of Γ of elements fixing K, and the notation means the $G(K)$ equals the group of homomorphisms $X^{*}(G) \to k^{\mathrm{sep}\times}$ commuting with the actions of Γ_K.

EXAMPLE 5.4 Take $k = \mathbb{R}$, so that Γ is cyclic of order 2, and let $X^{*}(G) = \mathbb{Z}$. Then $\mathrm{Aut}(\mathbb{Z}) = \mathbb{Z}^{\times} = \{\pm 1\}$, and so there are two possible actions of Γ on $X^{*}(G)$.

(a) Trivial action. Then $G(\mathbb{R}) = \mathbb{R}^{\times}$, and $G \simeq \mathbb{G}_m$.

(b) The generator ι of Γ acts on $\mathbb{Z}$ as $m \mapsto -m$. Then $G(\mathbb{R}) = \mathrm{Hom}(\mathbb{Z}, \mathbb{C}^{\times})^{\Gamma}$ consists of the elements of $\mathbb{C}^{\times}$ fixed under the following action of ι,

$$\iota z = \overline{z}^{-1}.$$

Thus $G(\mathbb{R}) = \{z \in \mathbb{C}^{\times} \mid z\overline{z} = 1\}$, which is compact.

EXAMPLE 5.5 Let K be a finite separable extension of k, and let T be the functor $R \rightsquigarrow (R \otimes_k K)^\times$. Then T is the group of multiplicative type corresponding to the Γ-module $\mathbb{Z}^{\mathrm{Hom}_k(K,k^{\mathrm{sep}})}$ (families of elements of $\mathbb{Z}$ indexed by the k-homomorphisms $K \to k^{\mathrm{sep}}$).

ASIDE 5.6 SGA 3, IX 1.1, defines a group scheme to be of multiplicative type if it is locally diagonalizable group for the flat (fpqc) topology. Over a field k, this amounts to requiring the group scheme to become diagonalizable over some field extension of k. Because of Theorem 5.11 below, this is equivalent to our definition.

Tori

DEFINITION 5.7 A ***torus*** is an algebraic group T such that $T_{k^{\mathrm{sep}}}$ is a split torus.

In other words, the tori are the algebraic groups T of multiplicative type such that $X^*(T)$ is torsion free.

PROPOSITION 5.8 *For a torus T, there exist (unique) subtori $T_1, \ldots, T_r$ such that*

- $T = T_1 \cdots T_r$,
- $T_i \cap T_j$ *is finite for all* $i \neq j$, *and*
- $X^*(T_i)_{\mathbb{Q}}$ *is a simple* Γ*-module for all* i.

PROOF. Let $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Because $X^*(T)$ is finitely generated, Γ acts on it through a finite quotient. Therefore Maschke's theorem (GT 7.4) shows that $X^*(T)_{\mathbb{Q}}$ is a direct sum of simple Γ-modules, say,

$$X^*(T)_{\mathbb{Q}} = V_1 \oplus \cdots \oplus V_r.$$

Let M_i be the image of $X^*(T)$ in V_i. Then there is an exact sequence

$$0 \to X^*(T) \to M_1 \times \cdots \times M_r \to F \to 0$$

of continuous Γ-modules with F finite. On applying the functor D, we get an exact sequence of algebraic groups of multiplicative type

$$0 \to D(F) \to D(M_1) \times \cdots \times D(M_r) \to T \to 0.$$

Take $T_i = D(M_i)$. □

A torus is ***anisotropic*** if $X(T) = 0$, i.e., $X^*(T)^\Gamma = 0$.

COROLLARY 5.9 *Every torus has a largest split subtorus T_s and a largest anisotropic subtorus T_a. The intersection $T_s \cap T_a$ is finite and $T_s \cdot T_a = T$.*

PROOF. In fact T_s is the product of the T_i in the proposition such that Γ act trivially on $X^*(T_i)$ and T_a is the product of the remainder. □

Representations of a group of multiplicative type

When G is a diagonalizable affine group, $\mathsf{Rep}(G)$ is a semisimple abelian category whose simple objects are in canonical one-to-one correspondence with the characters of G. When G is of multiplicative type, the description of $\mathsf{Rep}(G)$ is only a little more complicated.

Let k^{sep} be a separable closure of k, and let $\varGamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

THEOREM 5.10 *Let G be an affine group of multiplicative type. Then $\mathsf{Rep}(G)$ is a semisimple abelian category whose simple objects are in canonical one-to-one correspondence with the orbits of $\varGamma$ acting on $X^*(G)$.*

PROOF. It suffices to prove this in the case that G is algebraic, and so we may suppose that G is split by a finite Galois extension $\varOmega$ of k with Galois group $\bar{\varGamma}$. Let $\bar{\varGamma}$ act on $\mathcal{O}(G_{\varOmega}) \simeq \varOmega \otimes \mathcal{O}(G)$ through its action on $\varOmega$. By a semilinear action of $\bar{\varGamma}$ on a representation (V, r) of $G_{\varOmega}$, we mean a semilinear action of $\bar{\varGamma}$ on V such that $\gamma\rho = \rho$ where ρ is the coaction of $\mathcal{O}(G)$ on V. It follows from Proposition 7.2, Chapter V, that the functor $V \rightsquigarrow V_{\varOmega}$ from $\mathsf{Rep}_k(G)$ to the category of objects of $\mathsf{Rep}_{\varOmega}(G_{\varOmega})$ equipped with a semilinear action of $\bar{\varGamma}$ is an equivalence of categories.

Let V be a finite-dimensional representation of $G_{\varOmega}$ equipped with a semilinear action of $\bar{\varGamma}$. Then

$$V = \bigoplus\nolimits_{\chi \in X(G_{\varOmega})} V_{\chi}.$$

An element γ of $\varGamma$ acts on V by mapping V_{χ} isomorphically onto $V_{\gamma\chi}$. Therefore, as a representation of $G_{\varOmega}$ equipped with a semilinear action of $\bar{\varGamma}$, V decomposes into a direct sum of simple objects corresponding to the orbits of $\bar{\varGamma}$ acting on $X(G_{\varOmega})$. As these are also the orbits of $\varGamma$ acting on $X^*(G_{k^{\mathrm{sep}}}) \simeq X(G_{\varOmega})$, the statement follows. □

Criteria for an affine group to be of multiplicative type

Recall that if C is a finite-dimensional cocommutative coalgebra over k, then its linear dual $C^{\vee}$ is a commutative algebra over k (II, §3). We say that C is ***coétale*** if $C^{\vee}$ is étale. More generally, we say that a cocommutative coalgebra over k is ***coétale*** if every finite-dimensional subcoalgebra is coétale (cf. VIII, 4.6).

THEOREM 5.11 *The following conditions on an affine group G over k are equivalent:*

(a) *G is of multiplicative type (i.e., G becomes diagonalizable over k^{sep});*
(b) *G becomes diagonalizable over some field $K \supset k$;*
(c) *G is commutative and $\mathrm{Hom}(G, \mathbb{G}_a) = 0$;*
(d) *G is commutative and $\mathcal{O}(G)$ is coétale.*

PROOF. (a)⇒(b): Trivial.

(b)⇒(c): Clearly

$$\mathrm{Hom}(G, \mathbb{G}_a) \simeq \{f \in \mathcal{O}(G) \mid \varDelta(f) = f \otimes 1 + 1 \otimes f\}.$$

The condition on f is linear, and so, for any field $K \supset k$,

$$\mathrm{Hom}(G_K, \mathbb{G}_{aK}) \simeq \mathrm{Hom}(G, \mathbb{G}_a) \otimes K.$$

Thus, we may suppose that G is diagonalizable. If $u\colon G \to \mathbb{G}_a$ is a nontrivial homomorphism, then

$$g \mapsto \begin{pmatrix} 1 & u(g) \\ 0 & 1 \end{pmatrix}$$

is a nonsemisimple representation of G, which contradicts (4.7).

(c)⇒(d): We may assume that k is algebraically closed. Let C be finite-dimensional subcoalgebra of $\mathcal{O}(G)$, i.e., a finite-dimensional k-subspace such that $\Delta(C) \subset C \otimes C$. Let $A = C^\vee$. Then A is a finite product of local Artin rings with residue field k (CA 15.7). If one of these local rings is not a field, then there exists a surjective homomorphism of k-algebras

$$A \to k[\varepsilon], \quad \varepsilon^2 = 0.$$

This can be written $x \mapsto \langle x, a\rangle + \langle x, b\rangle \varepsilon$ for some $a, b \in C$ with $b \neq 0$. For $x, y \in A$,

$$\langle xy, a\rangle + \langle xy, b\rangle \varepsilon = \langle xy, \Delta a\rangle + \langle x \otimes y, \Delta b\rangle \varepsilon$$

and

$$\begin{aligned}(\langle x,a\rangle + \langle x,b\rangle\varepsilon)(\langle y,a\rangle + \langle y,b\rangle\varepsilon &= \langle x,a\rangle\langle y,a\rangle + (\langle x,a\rangle\langle y,b\rangle + \langle x,b\rangle\langle y,a\rangle)\varepsilon \\ &= \langle x\otimes y, a\rangle + \langle x \otimes y, a\otimes b + b \otimes b\rangle\varepsilon.\end{aligned}$$

It follows that

$$\begin{aligned}\Delta a &= a \otimes a \\ \Delta b &= a \otimes b + b \otimes a.\end{aligned}$$

On the other hand, the structure map $k \to A$ is $(\epsilon|C)^\vee$, and so $\epsilon(a) = 1$. Therefore a is a group-like element of $\mathcal{O}(G)$, and so it is a unit (see §1). Now

$$\begin{aligned}\Delta(ba^{-1}) = \Delta b \cdot \Delta a^{-1} &= (a \otimes b + b \otimes a)(a^{-1} \otimes a^{-1}) \\ &= 1 \otimes ba^{-1} + ba^{-1} \otimes 1,\end{aligned}$$

and so $\mathrm{Hom}(G, \mathbb{G}_a) \neq 0$, which contradicts (c). Therefore A is a product of fields.

(d)⇒(a): We may suppose that k is separably closed. Let C be a finite-dimensional subcoalgebra of $\mathcal{O}(G)$, and let $A = C^\vee$. By assumption, A is a product of copies of k. Let $a_1, \ldots, a_n$ be elements of C such that

$$x \mapsto (\langle x, a_1\rangle, \ldots, \langle x, a_n\rangle)\colon A \to k^n$$

is an isomorphism. Then $\{a_1, \ldots, a_n\}$ spans C and the argument in the above step shows that each a_i is a group-like element of C. As $\mathcal{O}(G)$ is a union of its finite-dimensional subcoalgebras (VIII, 4.6), this shows that $\mathcal{O}(G)$ is spanned by its group-like elements. □

COROLLARY 5.12 *An affine group G is of multiplicative type if and only if $G_{k^{\mathrm{al}}}$ is diagonalizable.*

PROOF. Certainly, $G_{k^{\mathrm{al}}}$ is diagonalizable if G is of multiplicative type, and the converse follows the theorem. □

COROLLARY 5.13 *A smooth commutative group G is of multiplicative type if and only if $G(k^{\mathrm{al}})$ consists of semisimple elements.*

PROOF. We may replace k with k^{al}. Let (V,r) be a faithful finite-dimensional representation (V,r) of G. If G is of multiplicative type, there exists a basis for V such that $r(G) \subset \mathbb{D}_n$; from this it follows that the elements of $G(k^{\mathrm{al}})$ are semisimple. Conversely, if the elements of $G(k^{\mathrm{al}})$ are semisimple, hence diagonalizable, we know from linear algebra that there exists a basis for V such that $(rG)(k^{\mathrm{al}}) \subset \mathbb{D}_n(k^{\mathrm{al}})$. Therefore $r(G) \subset \mathbb{D}_n$. □

ASIDE 5.14 The condition "commutative" is unnecessary. If $G(k^{\mathrm{al}})$ consists of semisimple elements, then the same is true of Lie(G), which is therefore commutative (XI, 11.1). It follows that G is commutative if k has characteristic zero. In nonzero characteristic, the proofs in the literature are more elaborate (Kohls 2011, 3.1).

COROLLARY 5.15 *A commutative affine group G is of multiplicative type if and only if* $\mathsf{Rep}(G)$ *is semisimple.*

PROOF. We saw in 5.10 that $\mathsf{Rep}(G)$ is semisimple if G is of multiplicative type. Conversely, if $\mathsf{Rep}(G)$ is semisimple, then $\mathrm{Hom}(G,\mathbb{G}_a) = 0$, and so G is of multiplicative type. □

ASIDE 5.16 In nonzero characteristic, the groups of multiplicative type are the *only* algebraic groups whose representations are all semisimple.[2] In characteristic zero, the reductive groups also have semisimple representations (see XVII, 5.4).

6 Rigidity

Later (see the proof of XVII, Theorem 5.1) we shall need the following result.

THEOREM 6.1 *Every action of a connected affine group G on an algebraic group H of multiplicative type is trivial.*

Clearly, it suffices to prove the theorem for an algebraically closed base field k.

PROOF OF THE THEOREM WHEN H IS FINITE.

When $H = \mu_n$, an action of G on H is a natural transformation

$$G \to \underline{\mathrm{Aut}}(\mu_n) \subset \underline{\mathrm{Hom}}(\mu_n,\mu_n) \simeq \underline{\mathrm{Hom}}(\mu_n,\mathbb{G}_m) \simeq \mathbb{Z}/n\mathbb{Z}$$

(see XII, §4), which is trivial, because G is connected. A similar argument proves the theorem when H is finite (hence a finite product of groups of the form μ_n).

[2] More precisely, for an algebraic group over a field k of characteristic $p \neq 0$, $\mathsf{Rep}(G)$ is semisimple if and only if G° is of multiplicative type and G/G° has order prime to p (Nagata's theorem, DG IV §3 3.6, p. 509; Kohls 2011).

PROOF OF THE THEOREM IN THE CASE THAT G IS SMOOTH.

We shall use that $G(k)$ is dense in G. We may suppose that H is a torus T. The kernel of $x \mapsto x^m\colon T \to T$ is a product of copies of μ_m, and so G acts trivially on it. Because of the category equivalence $T \rightsquigarrow X(T)$, it suffices to show that $g \in G(k)$ acts trivially on the $X(T)$, and because g acts trivially on the kernel of $m\colon T \to T$ it acts trivially on $X(T)/mX(T)$. We can now apply the following elementary lemma.

LEMMA 6.2 *Let M be a finitely generated commutative group, and let $u\colon M \to M$ be a homomorphism such that*

$$\begin{tikzcd} M \arrow[r, "u"] \arrow[d] & M \arrow[d] \\ M/mM \arrow[r, "\mathrm{id}"] & M/mM \end{tikzcd}$$

commutes for all m. Then $u = \mathrm{id}$.

PROOF. We may suppose that M is torsion-free. Choose a basis e_i for M, and write $u(e_j) = \sum_i a_{ij} e_i$, $a_{ij} \in \mathbb{Z}$. The hypothesis is that, for every integer m,

$$(a_{ij}) \equiv I_n \mod m,$$

i.e., that $m|a_{ij}$ for $i \neq j$ and $m|a_{ii} - 1$. Clearly, this implies that $(a_{ij}) = I_n$. □

PROOF OF THE THEOREM IN THE GENERAL CASE.

This doesn't use the smooth case.

LEMMA 6.3 *Let V be a k-vector space, and let M be a finitely generated commutative group. Then the family of homomorphisms*

$$V \otimes k[M] \to V \otimes k[M/nM], \quad n \geq 2,$$

is injective.

PROOF. An element f of $V \otimes k[M]$ can be written uniquely in the form

$$f = \textstyle\sum_{m \in M} f_m \otimes m, \quad f_m \in V.$$

Assume $f \neq 0$, and let $I = \{m \in M \mid f_m \neq 0\}$. As I is finite, for some n, the elements of I will remain distinct in M/nM, and for this n, the image of f in $V \otimes_k k[M/nM]$ is nonzero. □

As k is algebraically closed, the group H is diagonalizable. We saw above, that G acts trivially on H_n for all n. Let $H = D(M)$ with M a finitely generated commutative group. Then $\mathcal{O}(H) = k[M]$ and $\mathcal{O}(H_n) = k[M/nM]$. Let

$$\rho\colon k[M] \to \mathcal{O}(G) \otimes k[M]$$

give the action. We have to show that $\rho(x) = 1 \otimes x$ for each $x \in k[M]$, but this follows from the fact that G acts trivially on H_n for all $n \geq 2$, and the family of maps

$$\mathcal{O}(G) \otimes_k k[M] \to \mathcal{O}(G) \otimes_k k[M/nM], \quad n \geq 2,$$

is injective.

Density of the torsion points

PROPOSITION 6.4 *Let T be an algebraic group of multiplicative type, and let T_n be the kernel of $n\colon T \to T$. Let $u\colon T \to T$ be a homomorphism whose restriction to T_n is the identity map for all n. Then u is the identity map.*

PROOF. It suffices to show that $X^*(u)\colon X^*(T) \to X^*(T)$ is the identity map, but the hypothesis says that $X^*(u)$ induces the identity map on the quotient $X^*(T)/nX^*(T) = X^*(T_n)$ for all n, and so this follows from Lemma 6.2. □

7 Smoothness

LEMMA 7.1 *Let H and G be algebraic groups over a ring R, and let R_0 denote the quotient of R by an ideal I of square zero. If H is of multiplicative type, then every homomorphism $u_0\colon H_{R_0} \to G_{R_0}$ lifts to a homomorphism $u\colon H \to G$; if u' is a second lift, then $u' = \mathrm{inn}(g) \circ u$ for some $g \in \mathrm{Ker}(G(R) \to G(R_0))$.*

PROOF. The proof uses Hochschild cohomology $H^n(G,V)$, which is defined for any representation (V,r) of an algebraic group G. The lemma is a consequence of the following statements:

> Let G and H be algebraic groups over R, let $R_0 = R/I$ with $I^2 = 0$, and let $* \rightsquigarrow *_0$ denote base change $R \to R_0$.
>
> ◇ The obstruction to lifting a homomorphism $u_0\colon H_0 \to G_0$ to R is a class in $H^2(H_0, \mathrm{Lie}(G_0) \otimes I)$; if the class is zero, then the set of lifts modulo the action of $\mathrm{Ker}(G(R) \to G(R_0))$ by conjugation is a principal homogeneous space for the group $H^1(H_0, \mathrm{Lie}(G_0) \otimes I)$.
>
> ◇ If G is diagonalizable, then $H^n(G,V) = 0$ for $n > 0$ (DG, II, §3, 4.2, p195). □

PROPOSITION 7.2 *Let G be an algebraic group over a field k, acting on itself by conjugation, and let H and H' be subgroups of G. If G is smooth and H is of multiplicative type, then the transporter $T_G(H,H')$ is smooth.*

PROOF. We use the following criterion:

> An algebraic scheme X over a field k is smooth if and only if, for all k-algebras R and ideals I in R such that $I^2 = 0$, the map $X(R) \to X(R/I)$ is surjective (DG I, §4, 4.6, p.111).

We may replace k with its algebraic closure. Let $g_0 \in T_G(H,H')(R_0)$. Because G is smooth, g_0 lifts to an element $g \in G(R)$. On the other hand, because H is of multiplicative type, the homomorphism

$$\mathrm{inn}(g_0)\colon H_0 \to H'_0$$

lifts to a homomorphism $u\colon H \to H'$ (see 7.1). The homomorphisms

$$\begin{aligned} \mathrm{inn}(g)\colon H &\to G \\ u\colon H &\to H' \hookrightarrow G \end{aligned}$$

both lift $\mathrm{inn}(g_0)\colon H_0 \to G_0$, and so $u = \mathrm{inn}(g'g)$ for some $g' \in G(R)$ (see 7.1). Now $g'g$ is an element of $T_G(H,H')(R)$ lifting g_0. □

COROLLARY 7.3 *Let H be a subgroup of an algebraic group G. If G is smooth and H is of multiplicative type, then $N_G(H)$ and $C_G(H)$ are both smooth.*

PROOF. In fact,

$$\begin{aligned} N_G(H) &= T_G(H,H) \\ C_G(H) &= T_{G\times G}(H,H) \end{aligned}$$

(cf. the proofs of VII, 6.1, 6.7). □

8 Group schemes

Add a brief summary of SGA 3, VIII, IX, X.

9 Exercises

EXERCISE XIV-1 Show that the functor

$$C \rightsquigarrow \{\text{group-like elements in } C \otimes k^{\mathrm{sep}}\}$$

is an equivalence from the category of coétale finite cocommutative k-coalgebras to the category of finite sets with a continuous action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. (Hint: use XII, 2.7.)

EXERCISE XIV-2 Show that $\underline{\mathrm{Aut}}(\mu_m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (constant group defined by the group of invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$). Hint: To recognize the elements of $\underline{\mathrm{Aut}}(\mu_m)(R)$ as complete systems of orthogonal idempotents, see the proof of (1.2).

EXERCISE XIV-3 Let k'/k be a cyclic Galois extension of degree n with Galois group Γ generated by σ, and let $G = (\mathbb{G}_m)_{k'/k}$.

(a) Show that $X^*(G) \simeq \mathbb{Z}[\Gamma]$ (group algebra $\mathbb{Z} + \mathbb{Z}\sigma + \cdots + \mathbb{Z}\sigma^{n-1}$ of Γ).

(b) Show that

$$\mathrm{End}_\Gamma(X^*(G)) = \left\{ \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_n \\ \vdots & \vdots & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \middle| \, a_i \in \mathbb{Z} \right\}.$$

CHAPTER XV

Unipotent Affine Groups

Recall that an endomorphism of a finite-dimensional vector space V is unipotent if its characteristic polynomial is $(T-1)^{\dim V}$. For such an endomorphism, there exists a basis of V relative to which its matrix lies in

$$\mathbb{U}_n(k) \overset{\text{def}}{=} \left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}.$$

Let G be an algebraic group over a perfect field k. We say that $g \in G(k)$ is unipotent if $r(g)$ is unipotent for all finite-dimensional representations (V,r) of G. It suffices to check that $r(g)$ is unipotent for some faithful representation (V,r), or that $g = g_u$ (see X, 2.8).

By definition, a smooth algebraic group G over a field k is unipotent if the elements of $G(k^{\mathrm{al}})$ are all unipotent. However, not all unipotent groups are smooth, and so we adopt a different definition equivalent to requiring that the group be isomorphic to a subgroup of $\mathbb{U}_n$.

Throughout this chapter, k is a field. We remind the reader that "algebraic group" means "affine algebraic group".

1 Preliminaries from linear algebra

LEMMA 1.1 *Let $G \to \mathrm{GL}(W)$ be a simple linear representation of an abstract group G on a finite-dimensional vector space W over an algebraically closed field k. Let G act on $\mathrm{End}(W)$ by the rule:*

$$(gf)(w) = g(f(w)), \quad g \in G, \quad f \in \mathrm{End}(W), \quad w \in W.$$

Then every nonzero G-subspace X of $\mathrm{End}(W)$ contains an element $f_0\colon W \to W$ such that $f_0(W)$ has dimension one.

PROOF. We may suppose that X is simple. Then the k-algebra of G-endomorphisms of X is a division algebra, and hence equals k (Schur's lemma, GT 7.24, 7.29). For any $w \in W$, the map φ_w,

$$f \mapsto f(w)\colon X \to W$$

is a G-homomorphism. As $X \neq 0$, there exists an $f \in X$ and a $w_0 \in W$ such that $f(w_0) \neq 0$. Then $\varphi_{w_0} \neq 0$, and so it is an isomorphism (because X and W are simple). Let $f_0 \in X$ be such that $\varphi_{w_0}(f_0) = w_0$.

Let $w \in W$. Then $\varphi_{w_0}^{-1} \circ \varphi_w$ is a G-endomorphism of X, and so $\varphi_w = c(w)\varphi_{w_0}$ for some $c(w) \in k$. On evaluating this at f_0, we find that $f_0(w) = c(w)w_0$, and so $f_0(W) \subset \langle w_0 \rangle$.□

PROPOSITION 1.2 *Let V be a finite-dimensional vector space, and let G be a subgroup of* $\mathrm{GL}(V)$ *consisting of unipotent endomorphisms. Then there exists a basis of V for which G is contained in $\mathbb{U}_n$.*

PROOF. It suffices to show that $V^G \neq 0$, because then we can apply induction on the dimension of V to obtain a basis of V with the required property[1].

Choose a basis $(e_i)_{1 \leq i \leq n}$ for V. The condition that a vector $v = \sum a_i e_i$ be fixed by all $g \in G$ is linear in the a_i, and so has a solution in k^n if and only if it has a solution in $(k^{\mathrm{al}})^n$.[2] Therefore we may suppose that k is algebraically closed.

Let W be a nonzero subspace of V of minimal dimension among those stable under G. Clearly W is simple. For each $g \in G$, $\mathrm{Tr}_W(g) = \dim W$, and so

$$\mathrm{Tr}_W(g(g'-1)) = \mathrm{Tr}_W(gg') - \mathrm{Tr}_W(g) = 0.$$

Let $U = \{f \in \mathrm{End}(W) \mid \mathrm{Tr}_W(gf) = 0 \text{ for all } g \in G\}$. If G acts nontrivially on W, then U is nonzero because $(g'-1)|W \in U$ for all $g' \in G$. The lemma then shows that U contains an element f_0 such that $f_0(W)$ has dimension one. Such an f_0 has $\mathrm{Tr}_W\, f_0 \neq 0$, which contradicts the fact that $f_0 \in U$. We conclude that G acts trivially on W. □

2 Unipotent affine groups

DEFINITION 2.1 An affine group G is ***unipotent*** if every nonzero representation of G has a nonzero fixed vector (i.e., a nonzero $v \in V$ such that $\rho(v) = v \otimes 1$ when V is regarded as a $\mathcal{O}(G)$-comodule).

Equivalently, G is unipotent if every simple object in $\mathsf{Rep}(G)$ is trivial. We shall see that the unipotent algebraic groups are exactly the algebraic groups isomorphic to affine subgroups of $\mathbb{U}_n$ for some n. For example, $\mathbb{G}_a$ and its subgroups are unipotent.

[1] We use induction on the dimension of V. Let $e_1, \ldots, e_m$ be a basis for V^G. The induction hypothesis applied to G acting on V/V^G shows that there exists a basis $\bar{e}_{m+1}, \ldots, \bar{e}_n$ for V/V^G such that

$$u(\bar{e}_{m+i}) = c_{1,i}\bar{e}_{m+1} + \cdots + c_{i-1,i}e_{m+i-1} + \bar{e}_{m+i} \text{ for all } i \leq n-m.$$

Let $\bar{e}_{m+i} = e_{m+i} + V^G$ with $e_{m+i} \in V$. Then $e_1, \ldots, e_n$ is a basis for V relative to which $G \subset \mathbb{U}_n(k)$.

[2] For any representation (V, r) of an abstract group G, the subspace V^G of V is the intersection of the kernels of the linear maps

$$v \mapsto gv - v \colon V \to V, \quad g \in G.$$

It follows that $(V \otimes \bar{k})^{G_{\bar{k}}} \simeq V^G \otimes \bar{k}$, and so

$$(V \otimes \bar{k})^{G_{\bar{k}}} \neq 0 \implies V^G \neq 0.$$

PROPOSITION 2.2 *An algebraic group G is unipotent if and only if, for every finite-dimensional representation (V,r) of G, there exists a basis of V for which the image of G is contained in $\mathbb{U}_n$.*

PROOF. $\Rightarrow$: This can be proved by induction on the dimension of V (see footnote 1).

$\Leftarrow$: If $e_1,\ldots,e_n$ is such a basis, then $\langle e_1\rangle$ is fixed by G. □

DEFINITION 2.3 A Hopf algebra A is said to be ***coconnected*** if there exists a filtration $C_0\subset C_1\subset C_2\subset\cdots$ of A by subspaces C_i such that[3]

$$C_0=k,\ \bigcup\nolimits_{r\geq 0}C_r=A,\text{ and }\Delta(C_r)\subset\sum\nolimits_{0\leq i\leq r}C_i\otimes C_{r-i}. \tag{120}$$

THEOREM 2.4 *The following conditions on an algebraic group G are equivalent:*

(a) *G is unipotent;*
(b) *G is isomorphic to an algebraic subgroup of $\mathbb{U}_n$ for some n;*
(c) *the Hopf algebra $\mathcal{O}(G)$ is coconnected.*

PROOF. (a)$\Rightarrow$(b). Apply Proposition 2.2 to a faithful finite-dimensional representation of G (which exists by VIII, 9.1).

(b)$\Rightarrow$(c). Every quotient of a coconnected Hopf algebra is coconnected because the image of a filtration satisfying (120) will still satisfy (120), and so it suffices to show that $\mathcal{O}(\mathbb{U}_n)$ is coconnected. Recall that $\mathcal{O}(\mathbb{U}_n)\simeq k[X_{ij}\mid i<j]$, and that

$$\Delta(X_{ij})=X_{ij}\otimes 1+1\otimes X_{ij}+\sum_{i<r<j}X_{ir}\otimes X_{rj}.$$

Assign a weight of $j-i$ to X_{ij}, so that a monomial $\prod X_{ij}^{n_{ij}}$ will have weight $\sum n_{ij}(j-i)$, and let C_r be the subspace spanned by the monomials of weight $\leq r$. Clearly, $C_0=k$, $\bigcup_{r\geq 0}C_r=A$, and $C_iC_j\subset C_{i+j}$. It suffices to check the third condition in (120) on the monomials. For the X_{ij} it is obvious. We proceed by induction on weight of a monomial. If the condition holds for monomials P, Q of weights r,s, then $\Delta(PQ)=\Delta(P)\Delta(Q)$ lies in

$$\begin{aligned}\left(\sum C_i\otimes C_{r-i}\right)\left(\sum C_j\otimes C_{r-j}\right)&\subset\sum\left(C_iC_j\otimes C_{r-i}C_{s-j}\right)\\&\subset\sum C_{i+j}\otimes C_{r+s-i-j}.\end{aligned}$$

(c)$\Rightarrow$(a). Now assume that $\mathcal{O}(G)$ is a coconnected Hopf algebra, and let $\rho\colon V\to V\otimes\mathcal{O}(G)$ be a comodule. Then V is a union of the subspaces

$$V_r=\{v\in V\mid\rho(v)\in V\otimes C_r\}.$$

If V_0 contains a nonzero vector v, then $\rho(v)=v'\otimes 1$ for some vector v'; on applying ϵ, we find that $v=v'$, and so v is fixed. We complete the proof by showing that

$$V_r=0\implies V_{r+1}=0.$$

[3] This definition is probably as mysterious to the reader as it is to the author. Basically, it is the condition you arrive at when looking at Hopf algebras with only one group-like element (so the corresponding affine group has only one character). See Sweedler, Moss Eisenberg. Hopf algebras with one grouplike element. Trans. Amer. Math. Soc. 127 1967 515–526.

By definition, $\rho(V_{r+1}) \subset V \otimes C_{r+1}$, and so

$$(\mathrm{id} \otimes \Delta)\rho(V_{r+1}) \subset V \otimes \sum\nolimits_i C_i \otimes C_{r-i}.$$

Hence V_{r+i} maps to zero in $V \otimes A/C_r \otimes A/C_r$. We now use that $(\mathrm{id} \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}) \circ \rho$. The map $V \to V \otimes A/C_r$ defined by ρ is injective because $V_r = 0$, and on applying $\rho \otimes \mathrm{id}$ we find that $V \to (V \otimes A/C_r) \otimes A/C_r$ is injective. Hence $V_{r+1} = 0$. □

NOTES The exposition of 2.4 follows Waterhouse 1979, 8.3.

COROLLARY 2.5 *Subgroups, quotients, and extensions of unipotent groups are unipotent.*

PROOF. If G is isomorphic to a subgroup of $\mathbb{U}_n$, then so also is a subgroup of G.

A representation of a quotient of G can be regarded as a representation of G, and so has a nonzero fixed vector if it is nontrivial and G is unipotent.

Suppose that G contains a normal subgroup N such that both N and G/N are unipotent. For any representation (V,r) of G, the subspace V^N is stable under G (see VIII, 17.2), and so it defines a representation of G/N. If $V \neq 0$, then $V^N \neq 0$, and so $V^G = (V^N)^{G/N} \neq 0$. □

COROLLARY 2.6 *Let G be an algebraic group. If G is unipotent, then all elements of $G(k)$ are unipotent, and the converse is true when $G(k)$ is dense in G.*

PROOF. Let G be unipotent, and let (V,r) be a finite-dimensional representation of V. For some basis of V, the $r(G) \subset \mathbb{U}_n$ and so $r(G(k)) \subset \mathbb{U}_n(k)$; in particular, the elements of $r(G(k))$ are unipotent. For the converse, choose a faithful representation $G \to \mathrm{GL}_V$ of G and let $n = \dim V$. According to Proposition 1.2, there exists a basis of V for which $G(k) \subset \mathbb{U}_n(k)$. Because $G(k)$ is dense in G, this implies that $G \subset \mathbb{U}_n$. □

2.7 For an algebraic group G, even over an algebraically closed field k, it is possible for all elements of $G(k)$ to be unipotent without G being unipotent. For example, in characteristic p, the algebraic group μ_p has $\mu_p(k^{\mathrm{al}}) = 1$, but it is not unipotent.

COROLLARY 2.8 *Let k' be a field containing k. An algebraic group G over k is unipotent if and only if $G_{k'}$ is unipotent.*

PROOF. If G is unipotent, then $\mathcal{O}(G)$ is coconnected. But then $k' \otimes \mathcal{O}(G)$ is obviously coconnected, and so $G_{k'}$ unipotent. Conversely, suppose that $G_{k'}$ is unipotent. For any representation (V,r) of G, the subspace V^G of V is the kernel of the linear map

$$v \mapsto \rho(v) - v \otimes 1 \colon V \to V \otimes \mathcal{O}(G).$$

It follows that

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k',$$

and so

$$(V \otimes k')^{G_{k'}} \neq 0 \implies V^G \neq 0.$$

□

COROLLARY 2.9 *Let G be an algebraic group over k. If G is unipotent, then $\pi_0(G)$ has order a power of the characteristic exponent of k; in particular, G is connected if k has characteristic zero.*

PROOF. We may assume that k is algebraically closed. A representation of $\pi_0(G)$ can be regarded as a representation of G. Therefore, every representation of the finite group $\pi_0(G)$ is unipotent. This implies that $\pi_0(G)$ has order a power of the characteristic exponent of k (Maschke's theorem, GT 7.4). □

For example, if k has characteristic $p \neq 0$, then $(\mathbb{Z}/p\mathbb{Z})_k$ is unipotent[4] (but not connected).

EXAMPLE 2.10 Let k be a nonperfect field of characteristic $p \neq 0$, and let $a \in k \smallsetminus k^p$. The affine subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^p = X - aX^p$$

becomes isomorphic to $\mathbb{G}_a$ over $k[a^{\frac{1}{p}}]$, but it is not isomorphic to $\mathbb{G}_a$ over k. To see this, let C be the complete regular curve whose function field $k(C)$ is the field of fractions of $\mathcal{O}(G)$. The inclusion $\mathcal{O}(G) \hookrightarrow k(C)$ realizes G as an open subset of C, and one checks that the complement consists of a single point whose residue field is $k[a^{\frac{1}{p}}]$. For $G = \mathbb{G}_a$, the same construction realizes G as an open subset of $\mathbb{P}^1$ whose complement consists of a single point with residue field k.

COROLLARY 2.11 *A smooth algebraic group G is unipotent if $G(k^{\mathrm{al}})$ consists of unipotent elements.*

PROOF. If $G(k^{\mathrm{al}})$ consists of unipotent elements, then $G_{k^{\mathrm{al}}}$ is unipotent (2.6), and so G is unipotent (2.8). □

2.12 A unipotent group need not be smooth. For example, in characteristic p, the subgroup of $\mathbb{U}_2$ consisting of matrices $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$ with $a^p = 0$ is not smooth (it is isomorphic to α_p). ☠

COROLLARY 2.13 *An algebraic group is unipotent if and only if it admits a subnormal series whose quotients are isomorphic to affine subgroups of $\mathbb{G}_a$.*

PROOF. The group $\mathbb{U}_n$ has a subnormal series whose quotients are isomorphic to $\mathbb{G}_a$ — for example, the following subnormal series

$$\mathbb{U}_4 = \left\{\begin{pmatrix}1 & * & * & *\\ 0 & 1 & * & *\\ 0 & 0 & 1 & *\\ 0 & 0 & 0 & 1\end{pmatrix}\right\} \supset \left\{\begin{pmatrix}1 & 0 & * & *\\ 0 & 1 & 0 & *\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}\right\} \supset \left\{\begin{pmatrix}1 & 0 & 0 & *\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}\right\} \supset 1$$

has quotients $\mathbb{G}_a \times \mathbb{G}_a \times \mathbb{G}_a$, $\mathbb{G}_a \times \mathbb{G}_a$, $\mathbb{G}_a$. Therefore any affine subgroup of $\mathbb{U}_n$ has a subnormal series whose quotients are isomorphic to affine subgroups of $\mathbb{G}_a$ (see IX, 6.2). For the converse, note that $\mathbb{G}_a$ is unipotent, and so we can apply (2.5). □

[4] To give a representation of $(\mathbb{Z}/p\mathbb{Z})_k$ on a k-vector space V is the same as giving an endomorphism u of V of order p. The characteristic polynomial of such an u is $X^p - 1 = (X-1)^p$.

COROLLARY 2.14 *Every homomorphism from a unipotent algebraic group to an algebraic group of multiplicative type is trivial.*

PROOF. A nontrivial homomorphism $U \to H$ over k gives rise to a nontrivial homomorphism over k^{al}. Over an algebraically closed field, every algebraic group H of multiplicative type is a subgroup of $\mathbb{G}_m^n$ for some n (because every finitely generated commutative group is a quotient of $\mathbb{Z}^n$ for some n), and so it suffices to show that $\mathrm{Hom}(U,\mathbb{G}_m) = 0$ when U is unipotent. But a homomorphism $U \to \mathbb{G}_m$ is a one-dimensional representation of G, which is trivial by definition. □

COROLLARY 2.15 *The intersection of a unipotent affine subgroup of an algebraic group with an affine subgroup of multiplicative type is trivial (i.e., maps to* 1*)*

PROOF. The intersection is unipotent (2.5), and so the inclusion of the intersection into the group of multiplicative type is trivial. □

For example, $\mathbb{U}_n \cap \mathbb{D}_n = 1$ (which, of course, is obvious).

PROPOSITION 2.16 *An algebraic group G is unipotent if and only if every nontrivial affine subgroup of it admits a nonzero homomorphism to $\mathbb{G}_a$.*

PROOF. It follows from (2.13) that every nontrivial unipotent algebraic group admits a nontrivial homomorphism to $\mathbb{G}_a$. But every affine subgroup of a unipotent algebraic group is unipotent (2.5).

For the converse, let G_1 be the kernel of a nontrivial homomorphism $G \to \mathbb{G}_a$. If $G_1 \neq 1$, let G_2 be the kernel of a nontrivial homomorphism $G_1 \to \mathbb{G}_a$. Continuing in this fashion, we obtain a subnormal series whose quotients are affine subgroups of $\mathbb{G}_a$ (the series terminates in 1 because the topological space $|G|$ is noetherian and only finitely many G_i can have the same underlying topological space). Now apply (2.13). □

COROLLARY 2.17 *Every homomorphism from a group of multiplicative type to a unipotent algebraic group is trivial.*

PROOF. Let $u\colon T \to U$ be such a homomorphism. If $uT \neq 1$, then it admits a nontrivial homomorphism to $\mathbb{G}_a$, but this contradicts the fact that uT is of multiplicative type (XIV, 5.11). □

EXAMPLE 2.18 Let k be a nonperfect field characteristic p. For every finite sequence $a_0,\ldots,a_m$ of elements of k with $a_0 \neq 0$ and $n \geq 1$, the affine subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^{p^n} = a_0 X + a_1 X^P + \cdots + a_m X^{p^m}$$

is a form[5] of $\mathbb{G}_a$, and every form of $\mathbb{G}_a$ arises in this way (Russell 1970, 2.1; or apply 4.1). Note that G is the fibred product

$$\begin{tikzcd} G \arrow[r] \arrow[d] & \mathbb{G}_a \arrow[d, "a_0F+\cdots+a_mF^{p^m}"] \\ \mathbb{G}_a \arrow[r, "F^n"] & \mathbb{G}_a. \end{tikzcd}$$

In particular, G is an extension of $\mathbb{G}_a$ by a finite subgroup of $\mathbb{G}_a$ (so it does satisfy 2.13). There is a criterion for when two forms are isomorphic (ibid. 2.3). In particular, any form becomes isomorphic to $\mathbb{G}_a$ over a purely inseparable extension of k.

DEFINITION 2.19 A unipotent algebraic group is said to be ***split*** if it admits a subnormal series whose quotients are isomorphic to $\mathbb{G}_a$ (and not just subgroups of $\mathbb{G}_a$).[6]

Such a group is automatically smooth (VII, 10.1) and connected (XIII, 3.11).

PROPOSITION 2.20 *Every smooth connected unipotent algebraic group over a perfect field is split.*

PROOF. tba (cf. Borel 1991, 15.5(ii)). □

In particular, every smooth connected unipotent algebraic group splits over a purely inseparable extension.

Although the definition of "unipotent" applies to all affine groups, we have stated most of the above results for algebraic groups. The next statement shows how to extend them to affine groups.

PROPOSITION 2.21 *(a) An inverse limit of unipotent affine groups is unipotent.*

(b) An affine group is unipotent if and only if all of its algebraic quotients are unipotent.

PROOF. Obvious from the definitions. □

3 Unipotent affine groups in characteristic zero

Let $H(X,Y)=\sum_{n>0}H^n(X,Y)$ denote the Hausdorff series. Recall (IV, 1.6) that, for a finite-dimensional vector space V, $V_{\mathfrak{a}}$ denotes the algebraic group $R \rightsquigarrow R\otimes_k V$.

PROPOSITION 3.1 *Let G be a unipotent algebraic group. Then*

$$\exp(x)\cdot\exp(y)=\exp(\mathfrak{h}(x,y)) \tag{121}$$

for all $x,y\in\mathfrak{g}_R$ and k-algebras R.

[5] I.e., becomes isomorphic to $\mathbb{G}_a$ over an extension of k.

[6] Cf. SGA3, XVII, 5.10: Let k be a field and G an algebraic k-group. Following the terminology introduced by Rosenlicht (*Questions of rationality for solvable algebraic groups over nonperfect fields.* Ann. Mat. Pura Appl. (4) 61 1963 97–120), we say that G is "k-résoluble" if G has a composition series whose successive quotients are isomorphic to $\mathbb{G}_a$ ...

PROOF. We may identify G with a subgroup of GL_V for some finite-dimensional vector space V. Then $\mathfrak{g} \subset \mathfrak{gl}_V$, and, because G is unipotent, $\mathfrak{g}$ is nilpotent. Now (121) holds in G because it holds in GL_V. □

THEOREM 3.2 *Assume* $\mathrm{char}(k) = 0$.

(a) For any finite-dimensional nilpotent Lie algebra over k, the maps

$$(x,y) \mapsto \textstyle\sum_{n>0} H^n(x,y) \colon \mathfrak{g}(R) \times \mathfrak{g}(R) \to \mathfrak{g}(R)$$

(R a k-algebra) make $\mathfrak{g}_{\mathfrak{a}}$ into a unipotent algebraic group over k.

(b) The functor $\mathfrak{g} \rightsquigarrow \mathfrak{g}_{\mathfrak{a}}$ is an equivalence from the category of finite-dimensional nilpotent Lie algebras over k to the category of unipotent algebraic groups, with quasi-inverse $G \rightsquigarrow \mathrm{Lie}(G)$.

PROOF. Omitted for the moment (see ALA, II §4; DG IV §2 4.5, p. 499; Hochschild 1971a, Chapter 10). □

COROLLARY 3.3 *Every Lie subalgebra of $\mathfrak{gl}_V$ formed of nilpotent endomorphisms is algebraic.*

See the discussion XI, §13.

REMARK 3.4 In the equivalence of categories in (b), commutative Lie algebras (i.e., finite-dimensional vector spaces) correspond to commutative unipotent algebraic groups. In other words, $U \rightsquigarrow \mathrm{Lie}(U)$ is an equivalence from the category of commutative unipotent algebraic groups over a field of characteristic zero to the category of finite-dimensional vector spaces, with quasi-inverse $V \rightsquigarrow V_{\mathfrak{a}}$.

Miscellaneous results on unipotent groups (moved from Lie algebras)

LEMMA 3.5 *Let U be a unipotent subgroup of an algebraic group G. Then G/U is isomorphic to a subscheme of an affine scheme.*

PROOF. Let (V,r) be a representation of G such that U is the stabilizer of a line L in V. As U is unipotent, it acts trivially on L, and so $L^U = L$. For any nonzero $x \in L$, the map $g \mapsto gx$ is an injective regular map $G/U \to V_{\mathfrak{a}}$. Cf. DG, IV, 2 2.8, p. 489. □

LEMMA 3.6 *For any connected algebraic group G, the quotient* $\mathrm{Ker}(\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}})/ZG$ *is unipotent .*

PROOF. We may suppose that k is algebraically closed. Let $\mathcal{O}_e = \mathcal{O}(G)_e$ (the local ring at the identity element), and let $\mathfrak{m}_e$ be its maximal ideal. Then G acts on k-vector space $\mathcal{O}_e/\mathfrak{m}_e^{r+1}$ by k-algebra homomorphisms. By definition, Ker(Ad) acts trivially on $\mathfrak{m}_e/\mathfrak{m}_e^2$, and so it acts trivially on each of the quotients $\mathfrak{m}_e^i/\mathfrak{m}_e^{i+1}$. Let C_r be the centralizer of $\mathcal{O}(G)_e/\mathfrak{m}^{r+1}$ in G. Clearly $\mathrm{Ker}(\mathrm{Ad})/C_r$ is unipotent, and $C_r = ZG$ for r sufficiently large. Cf. DG IV 2 2.12, p. 490. □

PROPOSITION 3.7 *Let G be a smooth connected algebraic group over an algebraically closed field k. If G contains no subgroup isomorphic to $\mathbb{G}_m$, then it is unipotent.*

PROOF. Let (V,r) be a faithful representation of G, and let F be the variety of maximal flags in V. Then G acts on V, and according to AG 10.6, there exists a closed orbit, say $Gd \simeq G/U$. Then U is solvable, and so, by the Lie-Kolchin theorem XVI, 4.7, $U_{\mathrm{red}}^{\circ} \subset \mathbb{T}_n$ for some choice of basis. By hypothesis, $U_{\mathrm{red}}^{\circ} \cap \mathbb{D}_n = 0$, and so U_{red}° is unipotent. Now $G/U_{\mathrm{red}}^{\circ}$ is affine and connected, and so its image in F is a point. Hence $G = U_{\mathrm{red}}^{\circ}$. Cf. DG, IV, 2, 3.11, p. 496. □

COROLLARY 3.8 *Let G be a smooth connected algebraic group. The following conditions are equivalent:*

(a) *G is unipotent;*
(b) *The centre of G is unipotent and* $\mathrm{Lie}(G)$ *is nilpotent;*
(c) *For every representation (V,r) of G,* $\mathrm{Lie}\, r$ *maps the elements of* $\mathrm{Lie}(G)$ *to nilpotent endomorphisms of V;*
(d) *Condition (c) holds for one faithful representation (V,r).*

PROOF. (a)⇒(c). There exists a basis for V such that G maps into $\mathbb{U}_n$ (see 2.2).

(c)⇒(d). Trivial.

(a)⇒(b). Every subgroup of a unipotent group is unipotent (2.5), and G has a filtration whose quotients are isomorphic to subgroups of $\mathbb{G}_a$ (2.13).

(d)⇒(a). We may assume that k is algebraically closed (2.8). If G contains a subgroup H isomorphic to $\mathbb{G}_m$, then $V = \bigoplus_{n\in\mathbb{Z}} V_n$ where $h \in H(k)$ acts on V_n as h^n. Then $x \in \mathrm{Lie}(H)$ acts on V_n as nx, which contradicts the hypothesis.

(b)⇒(a). If the centre of G is unipotent, then the kernel of the adjoint representation is an extension of unipotent groups, and so it is unipotent (2.5). Suppose that G contains a subgroup H isomorphic to $\mathbb{G}_m$. Then H acts faithfully on $\mathfrak{g}$, and its elements act semisimply, contradicting the nilpotence of $\mathfrak{g}$.

Cf. DG, IV, 2 3.12, p. 496. □

4 Group schemes

Add a brief summary of SGA 3 XVII and Tits 1967 etc..

ASIDE 4.1 The unipotent algebraic groups over a field of characteristic $p \neq 0$ are more complicated than in characteristic zero. However, those isomorphic to a subgroup of $\mathbb{G}_a^n$ for some n are classified by the finite-dimensional $k[F]$-modules (polynomial ring with $Fa = a^p F$). See DG IV §3, 6.6 et seq., p. 521.

ASIDE 4.2 We compare the different definitions of unipotent in the literature.

(a) In SGA 3, XVII 1.3, an algebraic group scheme G over a field k is defined to be unipotent if there exists an algebraically closed field $\bar{k}$ containing k such that $G_{\bar{k}}$ admits a composition series whose quotients are isomorphic to algebraic subgroups of $\mathbb{G}_a$. It is proved ibid. 2.1 that such a group is affine, and so 2.8 and 2.13 show that this definition is equivalent to our definition.

(b) In DG IV, §2, 2.1, p. 485, a group scheme G over a field is defined to be unipotent if it is affine and every nontrivial affine subgroup H admits a nontrivial homomorphism $H \to \mathbb{G}_a$. Statement 2.16 shows that this is equivalent to our definition. (They remark that an algebraic group scheme satisfying the second condition is automatically affine. However, the constant group scheme $(\mathbb{Z})_k$ satisfies the second condition but is not affine.)

(c) In Conrad et al. 2010, A.1.3, p. 393, a group scheme U over a field is defined to be unipotent if it is affine of finite type and $U_{k^{\mathrm{al}}}$ admits a finite composition series over k^{al} with successive quotients isomorphic to a k^{al}-subgroup of $\mathbb{G}_a$. This is equivalent to our definition, except that we don't require the group scheme to be algebraic.

(d) In Springer 1998, p. 36, a linear algebraic group is defined to be unipotent if all its elements are unipotent. Implicitly, the group G is assumed to be a smooth affine algebraic group over an algebraically closed field, and the condition is that all the elements of $G(k)$ are unipotent. For such groups, this is equivalent to our definition because of (2.6) (but note that not all unipotent algebraic groups are smooth).

ASIDE 4.3 Unipotent groups are extensively studied in Tits 1967. For summaries of his results, see Oesterlé 1984, Chap. V, and Conrad et al. 2010 IV Appendix B. (A unipotent group is said to be ***wound*** if every map of varieties $\mathbb{A}^1 \to G$ is constant. Every smooth unipotent algebraic group G has a unique largest split affine subgroup G_s, called the ***split part*** of G. It is normal in G, and the quotient G/G_s is wound. The formation of G_s commutes with separable extensions.)

CHAPTER XVI

Solvable Affine Groups

Let G be an abstract group. Recall that the commutator of $x, y \in G$ is

$$[x,y] = xyx^{-1}y^{-1} = (xy)(yx)^{-1}.$$

Thus, $[x,y] = 1$ if and only if $xy = yx$, and G is commutative if and only if every commutator equals 1. The ***(first) derived group*** G' (or $\mathcal{D}G$) of G is the subgroup generated by commutators. Every automorphism of G maps commutators to commutators, and so G' is a characteristic subgroup of G (in particular, it is normal). In fact, it is the smallest normal subgroup such that G/G' is commutative.

The map (not a group homomorphism)

$$(x_1, y_1, \ldots, x_n, y_n) \mapsto [x_1, y_1] \cdots [x_n, y_n] \colon G^{2n} \to G$$

has image the set of elements of G that can be written as a product of at most n commutators, and so $\mathcal{D}G$ is the union of the images of these maps. Note that the map $G^{2n-2} \to G$ factors through $G^{2n} \to G$,

$$(x_1, y_1, \ldots, x_{n-1}, y_{n-1}) \mapsto (x_1, y_1, \ldots, x_{n-1}, y_{n-1}, 1, 1) \mapsto [x_1, y_1] \cdots [x_{n-1}, y_{n-1}].$$

A group G is said to be ***solvable*** if the ***derived series***

$$G \supset \mathcal{D}G \supset \mathcal{D}^2 G \supset \cdots$$

terminates with 1. For example, if $n \geq 5$, then S_n (symmetric group on n letters) is not solvable because its derived series $S_n \supset A_n$ terminates with A_n.

In this chapter we extend this theory to algebraic groups. Throughout, k is a field.

1 Trigonalizable affine groups

DEFINITION 1.1 An affine group G is ***trigonalizable***[1] if every nonzero representation of G has a one-dimensional subrepresentation. In terms of the associated comodule (V, ρ), this means that there exists a nonzero $v \in V$ such that $\rho(v) = v \otimes a$, some $a \in \mathcal{O}(G)$.

Equivalently, G is trigonalizable if every simple object in $\mathsf{Rep}(G)$ is one-dimensional.

[1] I follow Borel 1991, p. 203, and DG IV §2 3.1. Other names: triangulable (Waterhouse 1979, p. 72); triagonalizable.

PROPOSITION 1.2 *An algebraic group G is trigonalizable if and only if, for every finite-dimensional representation (V,r) of G, there exists a basis of V such that the image of G is contained in $\mathbb{T}_n$.*

PROOF. $\Rightarrow$: This can be proved by induction on the dimension of V.

$\Leftarrow$: If $e_1,\ldots,e_n$ is such a basis, then $\langle e_1\rangle$ is stable by G. □

The next theorem says that trigonalizable algebraic groups are exactly the algebraic groups isomorphic to affine subgroups of $\mathbb{T}_n$ for some n; diagonalizable and unipotent groups are both trigonalizable, and every trigonalizable group is an extension of one by the other.

THEOREM 1.3 *The following conditions on an algebraic group G are equivalent:*

(a) *G is trigonalizable;*
(b) *G is isomorphic to an affine subgroup of $\mathbb{T}_n$ for some n;*
(c) *there exists a normal unipotent affine subgroup U of G such that G/U is diagonalizable.*

PROOF. (a)$\Rightarrow$(b). Apply Proposition 1.2 to a faithful finite-dimensional representation of G (which exists by VIII, 9.1).

(b)$\Rightarrow$(c). Embed G into $\mathbb{T}_n$, and let $U=\mathbb{U}_n\cap G$. Then U is normal because $\mathbb{U}_n$ is normal in $\mathbb{T}_n$, and it is unipotent by XV, 2.4.

(c)$\Rightarrow$(a). Let U be as in (c), and let (V,r) be a nonzero representation of G. Because U is normal in G, the subspace V^U of V is stable under G (VIII, 17.2), and so G/U acts on V^U. Because U is unipotent, $V^U\neq 0$, and because G/U is diagonalizable, it is a sum of one-dimensional subrepresentations. □

COROLLARY 1.4 *Subgroups and quotients of trigonalizable algebraic groups are trigonalizable.*

PROOF. If G is isomorphic to a subgroup of $\mathbb{T}_n$, then so also is every affine subgroup of G. If every nontrivial representation of G has a stable line, then the same is true of every quotient of G (because a representation of the quotient can be regarded as a representation of G). □

COROLLARY 1.5 *If an algebraic group G over k is trigonalizable, then so also is $G_{k'}$ for every extension field k'.*

PROOF. If $G\subset\mathbb{T}_n$, then the same is true of $G_{k'}$. □

PROPOSITION 1.6 *(a) An inverse limit of trigonalizable affine groups is trigonalizable.*

(b) An affine group is trigonalizable if and only if all of its algebraic quotients are trigonalizable.

PROOF. Obvious from the definitions. □

THEOREM 1.7 *Let G be a trigonalizable algebraic group, and let U be a normal unipotent subgroup such that G/U is diagonalizable. Then the exact sequence*

$$1 \to U \to G \to G/U \to 1$$

splits in each of the following cases: k is algebraically closed; k has characteristic zero; k is perfect and G/U is connected; U is split.

PROOF. See DG IV §2 3.5, p. 494; SGA 3, XVII, 5.1.1. (We won't use this.) □

ASIDE 1.8 In DG IV §3 3.1, a group scheme G over a field is defined to be trigonalizable if it is affine and has a normal unipotent subgroup U such that G/U is diagonalizable. Because of Theorem 1.3, this is equivalent to our definition.

2 Commutative algebraic groups

Smooth commutative algebraic groups are geometrically trigonalizable

Let u be an endomorphism of a finite-dimensional vector space V over k. If all the eigenvalues of u lie in k, then there exists a basis for V relative to which the matrix of u lies in

$$\mathbb{T}_n(k) = \left\{ \begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\}$$

We extend this elementary statement to sets of commuting endomorphisms.

LEMMA 2.1 *Let V be a finite-dimensional vector space over an algebraically closed field k, and let S be a set of commuting endomorphisms of V. There exists a basis of V for which S is contained in the group of upper triangular matrices, i.e., a basis $e_1, \dots, e_n$ such that*

$$u(\langle e_1, \dots, e_i \rangle) \subset \langle e_1, \dots, e_i \rangle \text{ for all } i. \tag{122}$$

In more down-to-earth terms, let S be a set of commuting $n \times n$ matrices; then there exists an invertible matrix P such that PAP^{-1} is upper triangular for all $A \in S$.

PROOF. We prove this by induction on the dimension of V. If every $u \in S$ is a scalar multiple of the identity map, then there is nothing to prove. Otherwise, there exists an $u \in S$ and an eigenvalue a for u such that the eigenspace $V_a \neq V$. Because every element of S commutes with u, V_a is stable under the action of the elements of S: for $\beta \in S$ and $x \in V_a$,

$$u(\beta x) = \beta(ux) = \beta(ax) = a(\beta x).$$

The induction hypothesis applied to S acting on V_a and V/V_a shows that there exist bases $e_1, \dots, e_m$ for V_a and $\bar{e}_{m+1}, \dots, \bar{e}_n$ for V/V_a such that

$$\begin{aligned} u(\langle e_1, \dots, e_i \rangle) &\subset \langle e_1, \dots, e_i \rangle \quad \text{for all } i \leq m \\ u(\langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle) &\subset \langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle \text{ for all } i \leq n-m. \end{aligned}$$

Let $\bar{e}_{m+i} = e_{m+i} + V_a$ with $e_{m+i} \in V$. Then $e_1, \dots, e_n$ is a basis for V satisfying (122). □

PROPOSITION 2.2 *Let V be a finite-dimensional vector space over an algebraically closed field k, and let G be a smooth commutative affine subgroup of GL_V. Then there exists a basis of V for which G is contained in $\mathbb{T}_n$.*

PROOF. According to the lemma, there exists a basis of V for which $G(k) \subset \mathbb{T}_n(k)$. Now $G \cap \mathbb{T}_n$ is a subgroup of G such that $(G \cap \mathbb{T}_n)(k) = G(k)$. As $G(k)$ is dense in G (see VII, 5.9), this implies that $G \cap \mathbb{T}_n = G$, and so $G \subset \mathbb{T}_n$. □

Decomposition of a smooth commutative algebraic group

DEFINITION 2.3 Let G be an algebraic group over a perfect field k. An element g of $G(k)$ is ***semisimple*** (resp. ***unipotent***) if $g = g_s$ (resp. $g = g_u$) with the notations of X, 2.8.

Thus, g is semisimple (resp. unipotent) if $r(g)$ is semisimple (resp. unipotent) for one faithful representation (V, r) of G, in which case $r(g)$ is semisimple (resp. unipotent) for all representations r of G (X, 2.9).

Theorem 2.8, Chapter X, shows that

$$G(k) = G(k)_s \times G(k)_u \text{ (cartesian product of sets)} \tag{123}$$

where $G(k)_s$ (resp. $G(k)_u$) is the set of semisimple (resp. unipotent) elements in $G(k)$. However, this will not in general be a decomposition of groups, because Jordan decompositions do not respect products, for example, $(gh)_u \neq g_u h_u$ in general. However, if G is commutative, then

$$G \times G \xrightarrow{\text{multiplication}} G$$

is a homomorphism of groups, and so it does respect the Jordan decompositions (X, 2.10). Thus, in this case (123) realizes $G(k)$ as a product of subgroups. We can do better.

PROPOSITION 2.4 *Every smooth commutative algebraic group G over a perfect field is a direct product of two affine subgroups*

$$G \simeq G_u \times G_s$$

such that $G_u(k^{\mathrm{al}}) = G(k^{\mathrm{al}})_u$ and $G_s(k^{\mathrm{al}}) = G(k^{\mathrm{al}})_s$. The decomposition is unique: in fact, G_u is the largest unipotent affine subgroup of G and G_s is the largest affine subgroup of G of multiplicative type.

PROOF. Because of the uniqueness, if the decomposition exists over k^{al}, it will be stable under the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$, and so will arise from a decomposition over k. Hence we may assume that $k = k^{\mathrm{al}}$. First note that the subgroups $\mathbb{D}_n$ and $\mathbb{U}_n$ of $\mathbb{T}_n$ have trivial intersection, because

$$\mathbb{D}_n(R) \cap \mathbb{U}_n(R) = \{I_n\} \quad \text{(inside } \mathbb{T}_n(R))$$

for all R (alternatively, apply XIV, 2.15).

On applying (2.2) to a faithful representation of G, we obtain an embedding $G \hookrightarrow \mathbb{T}_n$ for some n. Let $G_s = G \cap \mathbb{D}_n$ and $G_u = G \cap \mathbb{U}_n$. Because G is commutative,

$$G_s \times G_u \to G \tag{124}$$

is a homomorphism with kernel $G_s \cap G_u$. Because $\mathbb{D}_n \cap \mathbb{U}_n = 1$ as algebraic groups, $G_s \cap G_u = 1$, and so (124) is injective; because $G_s(k)G_u(k) = G(k)$ and G is smooth, (124) is surjective (VII, 7.6); therefore it is an isomorphism.

That G_u is unipotent follows from XV, 2.11; that G_s is of multiplicative type follows from XIV, 5.13. For any other unipotent affine subgroup U of G, the map $U \to G/G_u \simeq G_s$ is trivial (XV, 2.14), and so $U \subset G_u$; similarly any other affine subgroup of multiplicative type is contained in G_s. □

REMARK 2.5 Let G be a smooth algebraic group over an algebraically closed field k (not necessarily commutative). In general, $G(k)_s$ will not be closed for the Zariski topology. However, $G(k)_u$ is closed. To see this, embed G in GL_n for some n. A matrix A is unipotent if and only if its characteristic polynomial is $(T-1)^n$. But the coefficients of the characteristic polynomial of A are polynomials in the entries of A, and so this is a polynomial condition.

Decomposition of a commutative algebraic group

THEOREM 2.6 *Let G be a commutative algebraic group over a field k.*

(a) *There exists a largest affine subgroup G_s of G of multiplicative type; this is a characteristic subgroup (in the weak sense) of G, and the quotient G/G_s is unipotent.*

(b) *If k is perfect, there exists a largest unipotent affine subgroup G_u of G, and $G = G_s \times G_u$. This decomposition is unique.*

PROOF. (a) Let G_s be the intersection of the affine subgroups H of G such that G/H is unipotent. Then $G/G_s \to \prod G/H$ is injective, and so G/G_s is unipotent (XV, 2.5). A nontrivial homomorphism $G_s \to \mathbb{G}_a$ would have a kernel H such that G/H is unipotent (XV, 2.5); but $G_s \not\subset H$, so this would contradict the definition of G_s. Therefore G_s is of multiplicative type (XIV, 5.11). If H is a second affine subgroup of G of multiplicative type, then the map $H \to G/G_s$ is trivial (XV, 2.17), and so $H \subset G_s$. Therefore G_s is the largest affine subgroup of G of multiplicative type. From this description, it is clear that $uG_s = G_s$ for every automorphism u of G.

(b) Assume k is perfect. Then it suffices to show that $G = T \times U$ with T of multiplicative type and U unipotent because, for any other unipotent affine subgroup U' of G, the map $U' \to G/U \simeq T$ is zero (XV, 2.14), and so $U' \subset U$; similarly any other subgroup T' of multiplicative type is contained in T; therefore T (resp. U) is the largest subgroup of multiplicative type (resp. unipotent subgroup), and so the decomposition is unique if it exists. When G is smooth, this is proved in (2.4). In the general case, one proves, by considering the cases $U = \mathbb{G}_a, \alpha_p, \mathbb{Z}/p\mathbb{Z}$, that the exact sequence

$$1 \to G_s \to G \to U \to 1$$

(over k^{al}) splits (see DG IV, §3, 1.1, p.502). □

ASIDE 2.7 In fact, G_s is characteristic in the strong sense, but this requires a small additional argument (DG IV, §2, 2.4, p. 486; §3, 1.1, p. 501); in general, G_u is not (ibid. IV §3, 1.2).

REMARK 2.8 It is necessary that k be perfect in (b). Let k be a separably closed field of characteristic p, and let $G = (\mathbb{G}_m)_{k'/k}$ where k' is an extension of k of degree p (necessarily purely inseparable). Then G is a commutative smooth connected algebraic group over k. The canonical map $\mathbb{G}_m \to G$ realizes $\mathbb{G}_m$ as G_s, and the quotient $G/\mathbb{G}_m$ is unipotent. Over k^{al}, G decomposes into $(\mathbb{G}_m)_{k^{\mathrm{al}}} \times (G/\mathbb{G}_m)_{k^{\mathrm{al}}}$, and so G is not reductive. However, G contains no unipotent subgroup because $G(k) = k'^{\times}$ has no p-torsion, and so $G_u = 1$. See XVII, 6.1.

NOTES Should complete the proof of (2.6), and derive (2.4) as a corollary.

3 The derived group of an algebraic group

Let G be an algebraic group over a field k.

DEFINITION 3.1 The ***derived group*** $\mathcal{D}G$ (or G' or G^{der}) of G is the intersection of the normal algebraic subgroups N of G such that G/N is commutative.

PROPOSITION 3.2 *The quotient $G/\mathcal{D}G$ is commutative (hence $\mathcal{D}G$ is the smallest normal subgroup with this property).*

PROOF. Because the affine subgroups of G satisfy the descending chain condition (VII, 3.3), $\mathcal{D}G = N_1 \cap \ldots \cap N_r$ for certain normal affine subgroups $N_1, \ldots, N_r$ such that G/N_i is commutative. The canonical homomorphism

$$G \to G/N_1 \times \cdots \times G/N_r$$

has kernel $N_1 \cap \ldots \cap N_r$, and so realizes $G/\mathcal{D}G$ as an affine subgroup of a commutative algebraic group. □

We shall need another description of $\mathcal{D}G$, which is analogous to the description of the derived group as the subgroup generated by commutators. As for abstract groups, there exist maps of functors

$$G^2 \to G^4 \to \cdots \to G^{2n} \to G.$$

Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \to \mathcal{O}(G^{2n})$ of k-algebras (not Hopf algebras) defined by $G^{2n} \to G$. Then

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \cdots$$

and we let $I = \bigcap I_n$.

PROPOSITION 3.3 *The coordinate ring of $\mathcal{D}G$ is $\mathcal{O}(G)/I$.*

PROOF. From the diagram of set-valued functors

$$\begin{tikzcd}
G^{2n} \arrow[d] & \times & G^{2n} \arrow[r] \arrow[d] & G^{4n} \arrow[d] \\
G & \times & G \arrow[r, "\text{mult}"] & G
\end{tikzcd}$$

we get a diagram of k-algebras

$$\begin{tikzcd}
\mathcal{O}(G)/I_n & \otimes & \mathcal{O}(G)/I_n & \arrow[l] \mathcal{O}(G)/I_{2n} \\
\mathcal{O}(G) \arrow[u] & \otimes & \mathcal{O}(G) \arrow[u] & \arrow[l, "\Delta"'] \mathcal{O}(G) \arrow[u]
\end{tikzcd}$$

(because $\mathcal{O}(G)/I_n$ is the image of $\mathcal{O}(G)$ in $\mathcal{O}(G^{4n})$). It follows that

$$\Delta\colon \mathcal{O}(G) \to \mathcal{O}(G)/I \otimes \mathcal{O}(G)/I$$

factors through $\mathcal{O}(G) \to \mathcal{O}(G)/I$, and defines a Hopf algebra structure on $\mathcal{O}(G)/I$, which corresponds to the smallest algebraic subgroup G' of G such that $G'(R)$ contains all the commutators for all R. Clearly, this is also the smallest normal subgroup such that G/G' is commutative. □

COROLLARY 3.4 *For any field $K \supset k$, $\mathcal{D}G_K = (\mathcal{D}G)_K$.*

PROOF. The definition of I commutes with extension of the base field. □

COROLLARY 3.5 *If G is connected (resp. smooth), then $\mathcal{D}G$ is connected (resp. smooth).*

PROOF. The algebraic group G is connected (resp. smooth) if and only if $G_{k^{\mathrm{al}}}$ is connected (resp. smooth), and so we may suppose that k is algebraically closed. Then G is connected (resp. smooth) if and only if $\mathcal{O}(G)$ has no nontrivial idempotents (resp. nilpotents). If $\mathcal{O}(G)/I$ had a nontrivial idempotent (resp. nilpotent), then so would $\mathcal{O}(G)/I_n$ for some n, but (by definition) the homomorphism of k-algebras $\mathcal{O}(G)/I_n \hookrightarrow \mathcal{O}(G^{2n})$ is injective. If G is connected (resp. smooth), then so also is G^{2n}, and so $\mathcal{O}(G^{2n})$ has no nontrivial idempotents (resp. nilpotents). □

COROLLARY 3.6 *Let G be a smooth algebraic group. Then $\mathcal{O}(\mathcal{D}G) = \mathcal{O}(G)/I_n$ for some n, and $(\mathcal{D}G)(k') = \mathcal{D}(G(k'))$ for every separably closed field k' containing k.*

PROOF. We may suppose that G is connected. As G is smooth and connected, so also is G^{2n} (III, 2.2; XIII, 3.9). Therefore, each ideal I_n is prime, and a descending sequence of prime ideals in a noetherian ring terminates. This proves the first part of the statement (CA 16.5).

Let V_n be the image of $G^{2n}(k')$ in $G(k')$. Its closure in $G(k')$ is the zero-set of I_n. Being the image of a regular map, V_n contains a dense open subset U of its closure (CA 12.14). Choose n as in the first part, so that the zero-set of I_n is $\mathcal{D}G(k')$. Then

$$U \cdot U^{-1} \subset V_n \cdot V_n \subset V_{2n} \subset \mathcal{D}(G(k')) = \bigcup\nolimits_m V_m \subset \mathcal{D}G(k').$$

It remains to show that $U \cdot U^{-1} = \mathcal{D}G(k')$. Let $g \in \mathcal{D}G(k')$. Because U is open and dense $\mathcal{D}G(k')$, so is gU^{-1}, which must therefore meet U, forcing g to lie in $U \cdot U$. □

COROLLARY 3.7 *The derived group $\mathcal{D}G$ of a connected algebraic group G is the unique smooth affine subgroup such that $(\mathcal{D}G)(k^{\mathrm{sep}}) = \mathcal{D}(G(k^{\mathrm{sep}}))$.*

PROOF. The derived group has these properties by (3.5) and (3.6), and it is the only affine subgroup with these properties because $(\mathcal{D}G)(k^{\text{sep}})$ is dense in $\mathcal{D}G$. □

☠ 3.8 For an algebraic group G, the group $G(k)$ may have commutative quotients without G having commutative quotients, i.e., we may have $G(k) \neq \mathcal{D}(G(k))$ but $G = \mathcal{D}G$. This is the case for $G = \mathrm{PGL}_n$ over nonperfect separably closed field of characteristic p dividing n.

ASIDE 3.9 For each k-algebra R, the group $(\mathcal{D}G)(R)$ consists of the elements of $G(R)$ that lie in $\mathcal{D}(G(R'))$ for some faithfully flat R-algebra R'.

Commutator groups

For subgroups H_1 and H_2 of an abstract group G, we let (H_1, H_2) denote the subgroup of G generated by the commutators $[h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1}$ with $h_1 \in H_1$ and $h_2 \in H_2$.

PROPOSITION 3.10 *Let H_1 and H_2 be smooth connected affine subgroups of a smooth connected algebraic group G. Then there is a (unique) smooth connected affine subgroup (H_1, H_2) of G such that $(H_1, H_2)(k^{\text{al}}) = (H_1(k^{\text{al}}), H_2(k^{\text{al}}))$.*

PROOF. Consider the natural transformation

$$(h_1, h_2, \ldots; h_1', h_2', \ldots) \mapsto [h_1, h_1'][h_2, h_2'] \cdots : H_1^n \times H_2^n \to G.$$

Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \to \mathcal{O}(H_1^n \times H_2^n)$ of k-algebras defined by the natural transformation, and let $I = \bigcap I_n$. As before, $\mathcal{O}(G)/I$ inherits a Hopf algebra structure from $\mathcal{O}(G)$, and the affine subgroup H of G with $\mathcal{O}(H) = \mathcal{O}(G)/I$ is such that $H(k^{\text{al}}) = (H_1(k^{\text{al}}), H_2(k^{\text{al}}))$. □

ASIDE 3.11 For each k-algebra R, the group $(H_1, H_2)(R)$ consists of the elements of $G(R)$ that lie in $(H_1(R'), H_2(R'))$ for some faithfully flat R-algebra R'.

4 Solvable algebraic groups

Write $\mathcal{D}^2 G$ for the second derived group $\mathcal{D}(\mathcal{D}G)$, $\mathcal{D}^3 G$ for the third derived group $\mathcal{D}(\mathcal{D}^2 G)$, and so on.

DEFINITION 4.1 An algebraic group G is ***solvable*** if the ***derived series***

$$G \supset \mathcal{D}G \supset \mathcal{D}^2 G \supset \cdots$$

terminates with 1.

LEMMA 4.2 *An algebraic group G is solvable if and only if it admits a subnormal series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1 \tag{125}$$

whose quotients G_i / G_{i+1} are commutative.

PROOF. If G is solvable, then the derived series is such a sequence. Conversely, given a sequence as in (125), $G_1 \supset \mathcal{D}G$, so $G_2 \supset \mathcal{D}^2 G, \ldots$, so $G_n \supset \mathcal{D}^n G$. Hence $\mathcal{D}^n G = 1$. □

A sequence of algebraic subgroups (125) such that G_{i+1} is normal in G_i for each i and G_i/G_{i+1} is commutative is called ***solvable series.***

PROPOSITION 4.3 *Subgroups, quotients, and extensions of solvable algebraic groups are solvable.*

PROOF. Obvious. □

EXAMPLE 4.4 Let G be a finite group, and let $(G)_k$ be the algebraic group such that $(G)_k(R) = G$ for all k-algebras R with no nontrivial idempotents. Then $\mathcal{D}(G)_k = (\mathcal{D}G)_k$, $\mathcal{D}^2(G)_k = (\mathcal{D}^2 G)_k$, and so on. Therefore $(G)_k$ is solvable if and only if G is solvable. In particular, the theory of solvable algebraic groups includes the theory of solvable finite groups, which is already quite complicated. For example, all finite groups with no element of order 2 are solvable (Feit-Thompson theorem).

EXAMPLE 4.5 The group $\mathbb{T}_n$ of upper triangular matrices is solvable. For example, the subnormal series

$$\mathbb{T}_3 = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \supset 1$$

has quotients $\mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$, $\mathbb{G}_a \times \mathbb{G}_a$, and $\mathbb{G}_a$.

More generally, the functor

$$R \rightsquigarrow G_0(R) \overset{\text{def}}{=} \{(a_{ij}) \mid a_{ii} = 1 \text{ for all } i\}$$

is an algebraic subgroup of $\mathbb{T}_n$ because it is represented by $\mathcal{O}(\mathbb{T}_n)/(T_{11} - 1, \ldots, T_{nn} - 1)$. Similarly, there is an algebraic subgroup G_r of G_0 of matrices (a_{ij}) such that $a_{ij} = 0$ for $0 < j - i \leq r$. The functor

$$(a_{ij}) \mapsto (a_{1,r+2}, \ldots, a_{i,r+i+1}, \ldots)$$

is a homomorphism from G_r onto $\mathbb{G}_a \times \mathbb{G}_a \times \cdots$ with kernel G_{r+1}. Thus the sequence of algebraic subgroups

$$\mathbb{T}_n \supset G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

exhibits $\mathbb{T}_n$ as a solvable group.

Alternatively, we can work abstractly. A ***flag*** in a vector space V is a set of subspaces of V, distinct from $\{0\}$ and V, ordered by inclusion. When we order the flags in V by inclusion, the maximal flags are the families $\{V_1, \ldots, V_{n-1}\}$ with $\dim V_i = i$, $n = \dim V$, and

$$V_1 \subset \cdots \subset V_{n-1}.$$

For example, if $(e_i)_{1 \leq i \leq n}$ is a basis for V, then we get a maximal flag by taking $V_i = \langle e_1, \ldots, e_i \rangle$.

Let $F = \{V_1, \ldots, V_{n-1}\}$ be a maximal flag in V, and let $\mathbb{T}$ be the algebraic subgroup of GL_V such that $\mathbb{T}(R)$ consists of the automorphisms preserving the flag, i.e., such that

$u(V_i \otimes R) \subset V_i \otimes R$ for all k-algebras R. When we take F to be the maximal flag in k^n defined by the standard basis, $G = \mathbb{T}_n$. Let G_0 be the algebraic subgroup of G of u acting as id on the quotients V_i/V_{i-i}; more precisely,

$$G_0 = \operatorname{Ker}(G \to \prod \mathrm{GL}_{V_i/V_{i-i}}).$$

Then G_0 is a normal algebraic subgroup of $\mathbb{T}$ with quotient isomorphic to $\mathbb{G}_m^n$. Now define G_r to be the algebraic subgroup of G_0 of elements u acting as id on the quotients V_i/V_{i-r-1}. Again, G_{r+1} is a normal algebraic subgroup of G_r with quotient isomorphic to a product of copies of $\mathbb{G}_a$.

EXAMPLE 4.6 The group of $n \times n$ monomial matrices is solvable if and only if $n \le 4$ (because S_n is solvable if and only if $n \le 4$; GT 4.33).

The Lie-Kolchin theorem

THEOREM 4.7 *Let G be a subgroup of GL_V. If G is connected, smooth, and solvable, and k is algebraically closed, then it is trigonalizable.*

PROOF. It suffices to show that there exists a basis for V such that $G(k) \subset \mathbb{T}_n(k)$ (because then $(G \cap \mathbb{T}_n)(k) = G(k)$, and so $G \cap \mathbb{T}_n = G$, which implies that $G \subset \mathbb{T}$). Also, it suffices to show that the elements of $G(k)$ have a common eigenvector, because then we can apply induction on the dimension of V (cf. the proof of 2.1). We prove this by induction on the length of the derived series G. If the derived series has length zero, then G is commutative, and we proved the result in (2.2).

Let $N = \mathcal{D}G$. Its derived series is shorter than that of G, and so we can assume that the elements of N have a common eigenvector, i.e., for some character χ of N, the space V_χ (for N) is nonzero. Therefore the sum W of the nonzero eigenspaces V_χ for N is nonzero. According to (VIII, 16.2), the sum is direct, $W = \bigoplus V_\chi$, and so the set $\{V_\chi\}$ of nonzero eigenspaces for N is finite.

Let x be a nonzero element of V_χ for some χ, and let $g \in G(k)$. For $n \in N(k)$,

$$ngx = g(g^{-1}ng)x = g \cdot \chi(g^{-1}ng)x = \chi(g^{-1}ng) \cdot gx$$

The middle equality used that N is normal in G. Thus, gx lies in the eigenspace for the character $\chi^g = (n \mapsto \chi(g^{-1}ng))$ of N. This shows that $G(k)$ permutes the finite set $\{V_\chi\}$.

Choose a χ such that $V_\chi \neq 0$, and let $H \subset G(k)$ be the stabilizer of V_χ. Then H consists of the $g \in G(k)$ such that $\chi^g = \chi$, i.e., such that

$$\chi(n) = \chi(g^{-1}ng) \text{ for all } n \in N(k). \tag{126}$$

Clearly H is a subgroup of finite index in $G(k)$, and it is closed for the Zariski topology on $G(k)$ because (126) is a polynomial condition on g for each n. Therefore $H = G(k)$, otherwise its cosets would disconnect $G(k)$. This shows that $W = V_\chi$, and so $G(k)$ stabilizes V_χ.

An element $n \in N(k)$ acts on V_χ as the homothety $x \mapsto \chi(n)x$, $\chi(n) \in k$. But each element n of $N(k)$ is a product of commutators $[x,y]$ of elements of $G(k)$ (see 3.6), and so n acts on V_χ as an automorphism of determinant 1. But the determinant of $x \mapsto \chi(n)x$ is $\chi(n)^{\dim V_\chi}$, and so the image of $\chi\colon G \to \mathbb{G}_m$ is finite. Because N is connected, this shows that $N(k)$ in fact acts trivially[2] on V_χ. Hence $G(k)$ acts on V_χ through the quotient $G(k)/N(k)$, which is commutative. In this case, we know there is a common eigenvalue (2.1). □

4.8 All the hypotheses in the theorem are needed (however, if k is algebraically closed and G is solvable, then the theorem applies to G°_{red}, which is a subgroup of G with the same dimension).

CONNECTED: The group G of monomial 2×2 matrices is solvable but not trigonalizable. The only common eigenvectors of $\mathbb{D}_2(k)\subset G(k)$ are $e_1=\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $e_2=\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$, but the monomial matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ interchanges e_1 and e_2, and so there is no common eigenvector for the elements of $G(k)$.

SMOOTH: (Waterhouse 1979, 10, Exercise 3, p. 79.) Let k have characteristic 2, and let G be the affine subgroup of SL_2 of matrices $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ such that $a^2=1=d^2$ and $b^2=0=c^2$. There is an exact sequence

$$0\longrightarrow \mu_2 \xrightarrow{a\mapsto\left(\begin{smallmatrix}a&0\\0&a\end{smallmatrix}\right)} G \xrightarrow{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\mapsto(ab,cd)} u_2\times u_2 \longrightarrow 1.$$

Moreover, $\mu_2\subset ZG$, and so G is connected and solvable (even nilpotent), but no line is fixed in the natural action of G on k^2. Therefore G is not trigonalizable.

SOLVABLE: As $\mathbb{T}_n$ is solvable (4.5) and a subgroup of a solvable group is obviously solvable, this condition is necessary.

k ALGEBRAICALLY CLOSED: If $G(k)\subset\mathbb{T}_n(k)$, then the elements of $G(k)$ have a common eigenvector, namely, $e_1=(1\,0\ldots 0)^t$. Unless k is algebraically closed, an endomorphism need not have an eigenvector, and, for example,

$$\left\{\left(\begin{smallmatrix}a&b\\-b&a\end{smallmatrix}\right)\;\middle|\; a,b\in\mathbb{R},\quad a^2+b^2=1\right\}$$

is an commutative algebraic group over $\mathbb{R}$ that is not trigonalizable over $\mathbb{R}$.

5 Structure of solvable groups

THEOREM 5.1 *Let G be a connected solvable smooth algebraic group over a perfect field k. There exists a unique connected normal affine subgroup G_u of G such that*

(a) *G_u is unipotent, and*
(b) *G/G_u is of multiplicative type.*

The formation of G_u commutes with change of the base field.

PROOF. When G is commutative

$$G=G_u\times G_s$$

where G_u is the largest unipotent affine subgroup of G and G_s is the largest affine subgroup of G of multiplicative type (see 2.4). As G_u is a quotient of G, it is connected, and so this proves the existence of G_u in this case.

[2] In more detail, the argument shows that the character χ takes values in $\mu_m\subset\mathbb{G}_m$ where $m=\dim V_\chi$. If k has characteristic zero, or characteristic p and $p\not| m$, then μ_m is étale, and so, because N is connected, χ is trivial. If $p|m$, the argument only shows that χ takes values in μ_{p^r} for p^r the power of p dividing m. But $\mu_{p^r}(k)=1$, and so the action of $N(k)$ on V is trivial, as claimed.

We next prove the existence of G_u when k is algebraically closed. Embed G into $\mathbb{T}_n$ for some n, and construct

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{U}_n \arrow[r] & \mathbb{T}_n \arrow[r] & \mathbb{D}_n \arrow[r] & 1 \\
1 \arrow[r] & G_u \arrow[r] \arrow[u] & G \arrow[r] \arrow[u] & T \arrow[r] \arrow[u] & 1
\end{tikzcd}$$

where T is the image of G in $\mathbb{D}_n$ and $G_u = \mathbb{U}_n \cap G$. Certainly G_u is a normal affine subgroup of G satisfying (a) and (b), and it remains to show that it is connected. As G/G_u is commutative, $\mathcal{D}G \subset G_u$, and there is an exact sequence

$$1 \to G_u/\mathcal{D}G \to G/\mathcal{D}G \to T \to 1.$$

Clearly, $G_u/\mathcal{D}G \simeq (G/\mathcal{D}G)_u$, and now

$$(G/\mathcal{D}G)_u, \mathcal{D}G \text{ connected} \implies G_u \text{ connected}$$

(XIII, 3.11).

For the uniqueness, use that G_u is the largest unipotent affine subgroup of G: if U is a unipotent affine subgroup of G, then the composite $U \to G \to G/G_u$ is trivial (XV, 2.14), and so $U \subset G_u$.

When k is only perfect, the uniqueness of $(G_{k^{\mathrm{al}}})_u$ implies that it is stable under $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$, and hence arises from a unique algebraic subgroup G_u of G (VII, 5.12), which clearly has the required properties.

The formation of G_u commutes with extension of scalars, because, for any field $k' \supset k$, the affine subgroup $(G_u)_{k'}$ of $G_{k'}$ has all the required properties (XIII, 3.8; XV, 2.8). □

6 Split solvable groups

DEFINITION 6.1 A solvable algebraic group is ***split*** if it admits subnormal series whose quotients are $\mathbb{G}_a$ or $\mathbb{G}_m$.

Such a group is automatically smooth (VII, 10.1) and connected (XIII, 3.11). This agrees with our definition of split unipotent group. Any quotient of a split solvable group is again a split solvable group.

7 Tori in solvable groups

PROPOSITION 7.1 *Let G be a smooth connected solvable group over an algebraically closed field. If T and T' are maximal tori in G, then $T' = gTg^{-1}$ for some $g \in G(k)$.*

PROOF. Omitted for the present (cf. Springer 1998, 6.3.5). □

PROPOSITION 7.2 *The centralizer of any torus in a smooth connected solvable group G is connected.*

PROOF. Omitted for the present (cf. Springer 1998, 6.3.5). □

8 Exercises

EXERCISE XVI-1 Give a geometric proof that G connected implies $\mathcal{D}G$ connected. [Show that the image of connected set under a continuous map is connected (for the Zariski topology, say), the closure of a connected set is connected, and a nested union of connected sets is connected sets is connected; then apply the criterion (XIII, 3.2).]

EXERCISE XVI-2 Show that an algebraic group G is trigonalizable if and only if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of $\mathcal{O}(G)$ by subspaces C_i such that C_0 is spanned by group-like elements, $\bigcup_{r \geq 0} C_r = A$, and $\Delta(C_r) \subset \sum_{0 \leq i \leq r} C_i \otimes C_{r-i}$ (Waterhouse 1979, Chap. 9, Ex. 5, p. 72).

CHAPTER **XVII**

The Structure of Algebraic Groups

Throughout this chapter, k is a field.

1 Radicals and unipotent radicals

Let G be an algebraic group over k.

LEMMA 1.1 *Let N and H be affine subgroups of G with N normal. If H and N are solvable (resp. unipotent, resp. connected, resp. smooth), then HN is solvable (resp. unipotent, resp. connected, resp. smooth).*

PROOF. We use the exact sequence

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] & HN \arrow[r] & HN/N \arrow[r] & 1. \\
 & & & H/H\cap N \arrow[u, "(\mathrm{IX},\ 4.4)", "\simeq"'] &
\end{tikzcd}$$

Because H is solvable, so also is its quotient $H/H\cap N$; hence HN/N is solvable, and HN is solvable because it is an extension of solvable groups (XVI, 4.3). The same argument applies with "solvable" replaced by "unipotent" (use XV, 2.5), or by "connected" (use XIII, 3.11), or by "smooth" (use VII, 10.1). □

PROPOSITION 1.2 *Let G be a smooth algebraic group over a field k.*

(a) *There exists a largest*[1] *smooth connected normal solvable subgroup of G (called the* ***radical*** *RG of G).*

(b) *There exists a largest smooth connected normal unipotent subgroup (called the* ***unipotent radical*** *R_uG of G).*

PROOF. (a) Let R be a maximal smooth connected normal solvable subgroup of G. If H is another such subgroup, then RH is also has these properties (1.1), and so $RH = R$; hence $H \subset R$.

(b) Same as (a). □

[1] Recall that "largest" means "unique maximal".

The formation of the radical and the unipotent radical each commute with separable extensions of the base field: let K be a Galois extension of k with Galois group Γ; by uniqueness, RG_K is stable under the action of Γ, and therefore arises from a subgroup $R'G$ of G (by V, 7.3); now $(RG)_K \subset RG_K$, and so $RG \subset R'G$; as RG is maximal, $RG = R'G$, and so $(RG)_K = (R'G)_K = RG_K$.

PROPOSITION 1.3 *Let G be a smooth algebraic group over a perfect field k. For any extension field K of k,*

$$RG_K = (RG)_K \text{ and } R_u G_K = (R_u G)_K.$$

Moreover, $R_u G = (RG)_u$ (notations as in XVI, 5.1).

PROOF. See the above discussion. □

DEFINITION 1.4 Let G be a smooth algebraic group over a field k. The ***geometric radical*** of G is $RG_{k^{\mathrm{al}}}$, and the ***geometric unipotent radical*** of G is $R_u G_{k^{\mathrm{al}}}$.

2 Definition of semisimple and reductive groups

DEFINITION 2.1 Let G be an algebraic group over a field k.

(a) G is ***semisimple*** if it is smooth and connected and its geometric radical is trivial.
(b) G is ***reductive*** if it is smooth and connected and its geometric unipotent radical is trivial.
(c) G is ***pseudoreductive*** if it is smooth and connected and its unipotent radical is trivial.

Thus

$$\text{semisimple} \implies \text{reductive} \implies \text{pseudoreductive}.$$

For example, SL_n, SO_n, and Sp_n are semisimple, and GL_n is reductive (but not semisimple). When k is perfect, $R_u G_{k^{\mathrm{al}}} = (R_u G)_{k^{\mathrm{al}}}$, and so "reductive" and "pseudoreductive" are equivalent.

PROPOSITION 2.2 *Let G be a smooth connected algebraic group over a perfect field k.*

(a) G is semisimple if and only if $RG = 1$.
(b) G is reductive if and only if $R_u G = 1$ (i.e., G is pseudoreductive).

PROOF. Obvious from (1.3). □

PROPOSITION 2.3 *Let G be a smooth connected algebraic group over a field k.*

(a) If G is semisimple, then every smooth connected normal commutative subgroup is trivial; the converse is true if k is perfect.
(b) If G is reductive, then every smooth connected normal commutative subgroup is a torus; the converse is true if k is perfect.

PROOF. (a) Suppose that G is semisimple, and let H be a smooth connected normal commutative subgroup of G. Then $H_{k^{\mathrm{al}}} \subset RG_{k^{\mathrm{al}}} = 1$, and so $H = 1$. For the converse, we use that RG and $\mathcal{D}G$ are stable for any automorphism of G. This is obvious from their definitions: RG is the largest connected normal solvable algebraic subgroup and $\mathcal{D}G$ is the smallest normal algebraic subgroup such that $G/\mathcal{D}G$ is commutative. Therefore the chain

$$G \supset RG \supset \mathcal{D}(RG) \supset \mathcal{D}^2(RG) \supset \cdots \supset \mathcal{D}^r(RG) \supset 1,$$

is preserved by every automorphism of G, and, in particular, by the inner automorphisms defined by elements of $G(k)$. This remains true over k^{al}, and so the groups are normal in G by (VII, 6.6). As $\mathcal{D}^r(RG)$ is commutative, it is trivial.

(b) Let H be a smooth connected normal commutative subgroup of G; then $H_{k^{\mathrm{al}}} \subset RG_{k^{\mathrm{al}}}$, which has no unipotent subgroup. Therefore H is a torus. For the converse, we consider the chain

$$G \supset R_uG \supset \mathcal{D}(R_uG) \supset \mathcal{D}^2(R_uG) \supset \cdots \supset \mathcal{D}^r(R_uG) \supset 1.$$

Then $\mathcal{D}^r(R_uG)$ is a commutative unipotent subgroup, and so is trivial. □

A smooth connected algebraic group G is pseudoreductive but not reductive if it contains no nontrivial normal smooth unipotent affine subgroup but $G_{k^{\mathrm{al}}}$ does contain such a subgroup.

REMARK 2.4 If one of the conditions, smooth, connected, normal, commutative, is dropped, then a semisimple group may have such a subgroup:

Group	subgroup	smooth?	connected?	normal?	commutative?
SL_2, $\mathrm{char}(k) \neq 2$	$\mathbb{Z}/2\mathbb{Z} = \{\pm I\}$	yes	no	yes	yes
SL_2, $\mathrm{char}(k) = 2$	μ_2	no	yes	yes	yes
SL_2	$\mathbb{U}_2 = \{\left(\begin{smallmatrix}1 & * \\ 0 & 1\end{smallmatrix}\right)\}$	yes	yes	no	yes
$\mathrm{SL}_2 \times \mathrm{SL}_2$	$\{1\} \times \mathrm{SL}_2$	yes	yes	yes	no

In the first two rows, the affine subgroup consists of the diagonal matrices of square 1.

PROPOSITION 2.5 *Let G be a smooth connected algebraic group over a perfect field. The quotient group G/RG is semisimple, and G/R_uG is reductive.*

PROOF. One sees easily that $R(G/RG) = 1$ and $R_u(G/R_uG) = 1$. □

EXAMPLE 2.6 Let G be the group of invertible matrices $\left(\begin{smallmatrix}A & B \\ 0 & C\end{smallmatrix}\right)$ with A of size $m \times m$ and C of size $n \times n$. The unipotent radical of G is the subgroup of matrices $\left(\begin{smallmatrix}I & B \\ 0 & I\end{smallmatrix}\right)$. The quotient of G by R_uG is isomorphic to the reductive group of invertible matrices of the form $\left(\begin{smallmatrix}A & 0 \\ 0 & C\end{smallmatrix}\right)$, i.e., to $\mathrm{GL}_m \times \mathrm{GL}_n$. The radical of this is $\mathbb{G}_m \times \mathbb{G}_m$.

PROPOSITION 2.7 *Let G be a connected algebraic group, and let U be a normal unipotent subgroup of G. Then U acts trivially on every semisimple representation of G.*

PROOF. Let (V,r) be a semisimple representation of G, and let W be the largest subspace of V on which U acts trivially. As U is normal, W is stable under G (VIII, 17.2). Let W' be a G-complement to V. If $W' \neq 0$, then $W'^{U} \neq 0$, and U acts trivially on $W + W'^{U}$, contradicting the maximality of W. Hence $W = V$. □

COROLLARY 2.8 *Let G be a smooth connected algebraic group. If G has a semisimple faithful representation, then it is reductive.*

PROOF. A normal unipotent subgroup of G acts trivially on a faithful representation of G, and therefore is trivial. □

The proposition shows that, for a smooth connected algebraic group G,

$$R_u G \subset \bigcap\nolimits_{(V,r)\text{ semisimple}} \operatorname{Ker}(r).$$

In (5.4) below, we shall prove that, in characteristic zero, $R_u G$ is equal to the intersection of the kernels of the semisimple representations of G; thus G is reductive if and only if $\mathsf{Rep}(G)$ is semisimple. This is false in nonzero characteristic.

ASIDE 2.9 In SGA 3, XIX, it is recalled that the unipotent radical of a smooth connected affine group scheme over an algebraically closed field is the largest smooth connected normal unipotent subgroup of G (ibid. 1.2). A smooth connected affine group scheme over an algebraically closed field is defined to be reductive if its unipotent radical is trivial (ibid. 1.6). A group scheme G over a scheme S is defined to be reductive if it is smooth and affine over S and each geometric fibre of G over S is a connected reductive group (2.7). When S is the spectrum of field, this definition coincides with our definition.

3 The canonical filtration on an algebraic group

THEOREM 3.1 *Let G be an algebraic group over a field k.*

(a) *G contains a unique connected normal subgroup G° such that G/G° is an étale algebraic group.*
(b) *Assume that k is perfect; then G contains a largest smooth subgroup.*
(c) *Assume that k is perfect and that G is smooth and connected; then G contains a unique smooth connected normal solvable subgroup N such that G/N is a semisimple group.*
(d) *Assume that k is perfect and that G is smooth connected and solvable; then G contains a unique connected unipotent subgroup N such that G/N is of multiplicative type.*

PROOF. (a) See XIII, 3.7.

(b) Because k is perfect, there exists a subgroup G_{red} of G with $\mathcal{O}(G_{\text{red}}) = \mathcal{O}(G)/\mathcal{N}$ (see VI, 6.3). This is reduced, and hence smooth (VI, 8.3b). This is the largest smooth subgroup of G because $\mathcal{O}(G_{\text{red}})$ is the largest reduced quotient of $\mathcal{O}(G)$.

(c) The radical RG of G has these properties. Any other smooth connected normal solvable subgroup N of G is contained in RG (by the definition of RG), and if $N \neq RG$ then G/N is not semisimple.

(c) See XVI, 5.1. □

NOTES Perhaps (or perhaps not):

(a) Explain the connected components for a nonaffine algebraic group, at least in the smooth case. Also discuss things over a ring k.

(b) Explain the Barsotti-Chevalley-Rosenlicht theorem.

(c) Explain anti-affine groups.

(d) Explain what is true when you drop "smooth" and "perfect", and maybe even allow a base ring.

4 The structure of semisimple groups

An algebraic group is ***simple*** (resp. ***almost-simple***) if it is smooth, connected, noncommutative, and every proper normal subgroup is trivial (resp. finite). For example, SL_n is almost-simple for $n > 1$, and $\mathrm{PSL}_n = \mathrm{SL}_n / \mu_n$ is simple. A simple algebraic group can not be finite (because smooth connected finite algebraic groups are trivial, hence commutative).

Let N be a smooth subgroup of an algebraic group G. If N is minimal among the nonfinite normal subgroups of G, then it is either commutative or almost-simple; if G is semisimple, then it is almost-simple.

An algebraic group G is said to be the ***almost-direct product*** of its algebraic subgroups $G_1, \ldots, G_r$ if the map

$$(g_1, \ldots, g_r) \mapsto g_1 \cdots g_r \colon G_1 \times \cdots \times G_r \to G$$

is a surjective homomorphism with finite kernel. In particular, this means that the G_i commute and each G_i is normal in G.

PROPOSITION 4.1 *Let G be a simple algebraic group over an algebraically closed field. Then the group of inner automorphisms of G has finite index in the full group of automorphisms of G.*

The usual proof of this shows that $\mathrm{Aut}(G) = \mathrm{Inn}(G) \cdot D$ where D is group of automorphisms leaving stable a maximal torus and a Borel subgroup containing the torus. It uses the conjugacy of Borel subgroups and the conjugacy of maximal tori in solvable groups, and then shows that $D/D \cap \mathrm{Inn}(G)$ is finite by letting it act on the roots. In short, it is not part of the basic theory. Unless, I find a more elementary proof, I'll defer the proof to the next chapter.

THEOREM 4.2 *A semisimple algebraic group G has only finitely many almost-simple normal subgroups $G_1, \ldots, G_r$, and the map*

$$(g_1, \ldots, g_r) \mapsto g_1 \cdots g_r \colon G_1 \times \cdots \times G_r \to G \tag{127}$$

is surjective with finite kernel. Each smooth connected normal algebraic subgroup of G is a product of those G_i that it contains, and is centralized by the remaining ones.

In particular, an algebraic group is semisimple if and only if it is an almost-direct product of almost-simple algebraic groups. The algebraic groups G_i are called the ***almost-simple factors*** of G.

PROOF. When k has characteristic zero, this is proved most easily using Lie algebras (see LAG). In the general case, we let $G_1, G_2, \ldots, G_r$ be distinct smooth subgroups of G, each of which is minimal among the nonfinite normal subgroups of G. For $i \neq j$, (G_i, G_j) is a smooth connected normal subgroup of G contained in each of G_i and G_j (see XVI, 3.10), and so it is trivial. Thus, the map

$$u\colon G_1 \times \cdots \times G_r \to G$$

is a homomorphism of algebraic groups, and $H \overset{\text{def}}{=} G_1 \cdots G_r$ is a smooth connected normal subgroup of G. The kernel of u is finite, and so

$$\dim G \geq \sum\nolimits_{i=1}^{r} \dim G_i .$$

This shows that r is bounded, and we may assume that our family contains them all. It then remains to show that $H = G$. For this we may assume that $k = k^{\mathrm{al}}$. Let $H' = C_G(H)$. The action of G on itself by inner automorphisms defines a homomorphism

$$G(k) \to \mathrm{Aut}(H)$$

whose image contains $\mathrm{Inn}(H)$ and whose kernel is $H'(k)$ (which equals $H'_{\mathrm{red}}(k)$). As $\mathrm{Inn}(H)$ has finite index in $\mathrm{Aut}(H)$ (see 4.1), this shows that $(G/H \cdot H'_{\mathrm{red}})(k)$ is finite, and so the quotient $G/\left(H \cdot H'_{\mathrm{red}}\right)$ is finite. As G is connected and smooth, it is strongly connected, and so $G = H \cdot H'_{\mathrm{red}}$; in fact, $G = H \cdot H'^{\circ}_{\mathrm{red}}$.

Let N be a smooth subgroup of $H'^{\circ}_{\mathrm{red}}$, and assume that N is minimal among the nonfinite normal subgroups of $H'^{\circ}_{\mathrm{red}}$. Then N is normal in G (because $G = H \cdot H'$ and H centralizes H'), and so it equals one of the G_i. This contradicts the definition of H, and we conclude that $H'^{\circ}_{\mathrm{red}} = 1$. □

COROLLARY 4.3 *All nontrivial smooth connected normal subgroups and quotients of a semisimple algebraic group are semisimple.*

PROOF. Any such group is an almost-product of almost-simple algebraic groups. □

COROLLARY 4.4 *If G is semisimple, then $\mathcal{D}G = G$, i.e., a semisimple group has no commutative quotients.*

PROOF. This is obvious for almost-simple algebraic groups, and hence for any almost-product of such algebraic groups. □

Simply connected semisimple groups

(This section need to be rewritten.) An semisimple algebraic group G is ***simply connected*** if every isogeny $G' \to G$ is an isomorphism.

Let G be a simply connected semisimple group over a field k, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Then $G_{k^{\mathrm{sep}}}$ decomposes into a product

$$G_{k^{\mathrm{sep}}} = G_1 \times \cdots \times G_r \tag{128}$$

of its almost-simple subgroups G_i. The set $\{G_1, \ldots, G_r\}$ contains all the almost-simple subgroups of G. When we apply $\sigma \in \Gamma$ to (128), it becomes

$$G_{k^{\mathrm{sep}}} = \sigma G_{k^{\mathrm{sep}}} = \sigma G_1 \times \cdots \times \sigma G_r$$

with $\{\sigma G_1, \ldots, \sigma G_r\}$ a permutation of $\{G_1, \ldots, G_r\}$. Let $H_1, \ldots, H_s$ denote the products of G_i in the different orbits of Γ. Then $\sigma H_i = H_i$, and so H_i is defined over k (V, 7.3), and

$$G = H_1 \times \cdots \times H_s$$

is a decomposition of G into a product of its almost-simple subgroups.

Now suppose that G itself is almost-simple, so that Γ acts transitively on the G_i in (128). Let

$$\Delta = \{\sigma \in \Gamma \mid \sigma G_1 = G_1\},$$

and let $K = (k^{\mathrm{sep}})^{\Delta}$.

PROPOSITION 4.5 *We have $G \simeq (G_1)_{K/k}$ (restriction of base field).*

PROOF. We can rewrite (128) as

$$G_{k^{\mathrm{sep}}} = \prod \sigma G_{1k^{\mathrm{sep}}}$$

where σ runs over a set of cosets for Δ in Γ. On comparing this with (V, 5.7), we see that there is a canonical isomorphism

$$G_{k^{\mathrm{sep}}} \simeq \left((G_1)_{K/k}\right)_{k^{\mathrm{sep}}}.$$

In particular, it commutes with the action of Γ, and so is defined over k (see V, 7.3). □

The group G_1 over K is ***geometrically almost-simple***, i.e., it is almost-simple and remains almost-simple over K^{al}.

PROPOSITION 4.6 *Every representation of a semisimple algebraic group over a field of characteristic zero is semisimple.*

PROOF. Omitted for the moment. □

5 The structure of reductive groups

Recall that every algebraic group G of multiplicative type contains a largest torus G°_{red}. For example, if $G = D(M)$, then $G^{\circ}_{\mathrm{red}} = D(M/\{\text{torsion}\})$. Its formation commutes with extension of the base field:

$$(G^{\circ}_{\mathrm{red}})_{k'} = (G_{k'})^{\circ}_{\mathrm{red}}. \tag{129}$$

THEOREM 5.1 *If G is reductive, then*

(a) *the radical RG of G is a torus, and $(RG)_{k^{\mathrm{al}}} = RG_{k^{\mathrm{al}}}$;*
(b) *the centre ZG of G is of multiplicative type, and $(ZG)^{\circ}_{\mathrm{red}} = RG$;*
(c) *the derived group $\mathcal{D}G$ of G is semisimple;*
(d) *$ZG \cap \mathcal{D}G$ is the (finite) centre of $\mathcal{D}G$, and*

(e) $G = RG \cdot \mathcal{D}G$ *(hence also* $G = (ZG)^{\circ} \cdot \mathcal{D}G$*).*

PROOF. According to (XVI, 2.6), $ZG_{k^{\mathrm{al}}}$ is a product of a group of multiplicative type with a unipotent subgroup, and the decomposition is stable under all automorphisms. As $G_{k^{\mathrm{al}}}$ is reductive, the unipotent subgroup is trivial, and so $ZG_{k^{\mathrm{al}}}$ is of multiplicative type. As $ZG_{k^{\mathrm{al}}} = (ZG)_{k^{\mathrm{al}}}$, ZG is also of multiplicative type.

Because $RG_{k^{\mathrm{al}}}$ is a smooth connected solvable group, it is an extension of a group of multiplicative type by a connected unipotent group (XVI, 5.1). As $G_{k^{\mathrm{al}}}$ is reductive, the latter is trivial, and so $RG_{k^{\mathrm{al}}}$ is of multiplicative type. As $(RG)_{k^{\mathrm{al}}} \subset RG_{k^{\mathrm{al}}}$, RG itself is of multiplicative type, and as it is smooth and connected, it is a torus. Rigidity (XIV, 6.1) implies that the action of G on RG by inner automorphisms is trivial, and so $RG \subset ZG$. Hence $RG \subset (ZG)^{\circ}_{\mathrm{red}}$, but clearly $(ZG)^{\circ}_{\mathrm{red}} \subset RG$, and so

$$RG = (ZG)^{\circ}_{\mathrm{red}}. \tag{130}$$

Now

$$(RG)_{k^{\mathrm{al}}} \overset{(130)}{=} \left((ZG)^{\circ}_{\mathrm{red}}\right)_{k^{\mathrm{al}}} = (ZG_{k^{\mathrm{al}}})^{\circ}_{\mathrm{red}} \overset{(130)}{=} RG_{k^{\mathrm{al}}}.$$

This completes the proof of (a) and (b).

We next show that the algebraic group $ZG \cap \mathcal{D}G$ is finite. For this, we may replace k with its algebraic closure. Choose a faithful representation $G \to \mathrm{GL}_V$, and regard G as an algebraic subgroup of GL_V. Because ZG is diagonalizable, V is a direct sum

$$V = V_1 \oplus \cdots \oplus V_r$$

of eigenspaces for the action of ZG (see XIV, 4.7). When we choose bases for the V_i, then $(ZG)(k)$ consists of the matrices

$$\begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_r \end{pmatrix}$$

with each A_i of the form $\mathrm{diag}(a_i, \ldots, a_i)$, $a_i \neq a_j$ for $i \neq j$, and so its centralizer in GL_V consists of the matrices of this shape but with the A_i arbitrary. Since $(\mathcal{D}G)(k)$ consists of commutators (XVI, 3.6), its elements have determinant 1. But $\mathrm{SL}(V_i)$ contains only finitely many scalar matrices $\mathrm{diag}(a_i, \ldots, a_i)$, and so $(ZG)(k) \cap (\mathcal{D}G)(k)$ is finite. This equals $(ZG \cap \mathcal{D}G)(k)$, and so $ZG \cap \mathcal{D}G$ is finite (XII, 1.6).

Note that $RG \cdot \mathcal{D}G$ is a normal subgroup of G. The quotient $G/(RG \cdot \mathcal{D}G)$ is semisimple because $(G/(RG \cdot \mathcal{D}G))_{k^{\mathrm{al}}}$ is a quotient of $G_{k^{\mathrm{al}}}/RG_{k^{\mathrm{al}}}$ and we can apply (2.5 and 4.3). On the other hand, $G/(RG \cdot \mathcal{D}G)$ is commutative because it is a quotient of $G/\mathcal{D}G$. Therefore it is trivial (4.4),

$$G = RG \cdot \mathcal{D}G.$$

Now the homomorphism

$$\mathcal{D}G \to G/RG$$

is surjective with finite kernel $RG \cap \mathcal{D}G \subset ZG \cap \mathcal{D}G$. As $G/R(G)$ is semisimple, so also is $\mathcal{D}G$.

Certainly $ZG \cap \mathcal{D}G \subset Z(\mathcal{D}G)$, but, because $G = RG \cdot \mathcal{D}G$ and $RG \subset ZG$, $Z(\mathcal{D}G) \subset ZG$. This completes the proof of (c), (d), and (e). □

EXAMPLE 5.2 Let $G = \mathrm{SL}_n$. Let p be the characteristic exponent of k, and set $n = n' \cdot p^r$ with $\gcd(n', p) = 1$. Then $ZG \simeq \mu_n$, $(ZG)^\circ \simeq \mu_{p^r}$, $(ZG)_{\mathrm{red}} \simeq \mu_{n'}$, and $(ZG)^\circ_{\mathrm{red}} = 1 = RG$.

REMARK 5.3 From a reductive group G, we obtain a semisimple group G' (its derived group), a group Z of multiplicative type (its centre), and a homomorphism $\varphi\colon ZG' \to Z$. Moreover, G can be recovered from (G', Z, φ): the map

$$z \mapsto (\varphi(z)^{-1}, z)\colon ZG' \to Z \times G'$$

is an isomorphism from ZG' onto a central subgroup of $Z \times G'$, and the quotient is G. Clearly, every reductive group arises from such a triple (G', Z, φ) (and G' can even be chosen to be simply connected).

Reductive groups in characteristic zero

THEOREM 5.4 *The following conditions on a connected algebraic group G over a field of characteristic zero are equivalent:*

(a) *G is reductive;*
(b) *every finite-dimensional representation of G is semisimple;*
(c) *some faithful finite-dimensional representation of G is semisimple.*

PROOF. (a) $\implies$ (b): If G is reductive, then $G = Z \cdot G'$ where Z is the centre of G (a group of multiplicative type) and G' is the derived group of G (a semisimple group) — see (5.1). Let $G \to \mathrm{GL}_V$ be a representation of G. When regarded as a representation of Z, V decomposes into a direct sum $V = \bigoplus_i V_i$ of simple representations (XIV, 5.10). Because Z and G' commute, each subspace V_i is stable under G'. As a G'-module, V_i decomposes into a direct sum $V_i = \bigoplus_j V_{ij}$ with each V_{ij} simple as a G'-module (4.6). Now $V = \bigoplus_{i,j} V_{ij}$ is a decomposition of V into a direct sum of simple G-modules.

(b) $\implies$ (c): Obvious, because every algebraic group has a faithful finite-dimensional representation (VIII, 9.1).

(c) $\implies$ (a): This is true over any field (see 2.8). □

COROLLARY 5.5 *Over a field of characteristic zero, all finite-dimensional representations of an algebraic group G are semisimple if and only if the identity component G° of G is reductive.*

PROOF. Omitted for the moment. □

6 Pseudoreductive groups

We briefly summarize Conrad, Gabber, and Prasad 2010, which completes earlier work of Tits (Borel and Tits 1978; Tits 1992, 1993; Springer 1998, Chapters 13–15).

6.1 Let k be a separably closed field of characteristic p, and let $G = (\mathbb{G}_m)_{k'/k}$ where k' is an extension of k of degree p (necessarily purely inseparable). Then G is a commutative smooth connected algebraic group over k. The canonical map $\mathbb{G}_m \to G$ realizes $\mathbb{G}_m$ as the largest subgroup of G of multiplicative type, and the quotient $G/\mathbb{G}_m$ is unipotent. Over k^{al}, G decomposes into $(\mathbb{G}_m)_{k^{\mathrm{al}}} \times (G/\mathbb{G}_m)_{k^{\mathrm{al}}}$ (see XVI, 2.4), and so G is not reductive. However, G contains no unipotent subgroup because $G(k) = k'^{\times}$, which has no p-torsion. Therefore G is pseudo-reductive.

6.2 Let k' be a finite field extension of k, and let G be a reductive group over k'. If k' is separable over k, then $(G)_{k'/k}$ is reductive, but otherwise it is only pseudoreductive.

6.3 Let C be a commutative connected algebraic group over k. If C is reductive, then C is a torus, and the tori are classified by the continuous actions of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on free commutative groups of finite rank. By contrast, "it seems to be an impossible task to describe general commutative pseudo-reductive groups over imperfect fields" (Conrad et al. 2010, p. xv).

6.4 Let $k_1,\ldots,k_n$ be finite field extensions of k. For each i, let G_i be a reductive group over k_i, and let T_i be a maximal torus in G_i. Define algebraic groups

$$G \hookleftarrow T \twoheadrightarrow \bar{T}$$

by

$$\begin{aligned} G &= \prod\nolimits_i (G_i)_{k_i/k} \\ T &= \prod\nolimits_i (T_i)_{k_i/k} \\ \bar{T} &= \prod\nolimits_i (T_i/Z(G_i))_{k_i/k}. \end{aligned}$$

Let $\phi: T \to C$ be a homomorphism of commutative pseudoreductive groups that factors through the quotient map $T \to \bar{T}$:

$$T \xrightarrow{\phi} C \xrightarrow{\psi} \bar{T}.$$

Then ψ defines an action of C on G by conjugation, and so we can form the semi-direct product

$$G \rtimes C.$$

The map

$$t \mapsto (t^{-1}, \phi(t)): T \to G \rtimes C$$

is an isomorphism from T onto a central subgroup of $G \rtimes C$, and the quotient $(G \rtimes C)/T$ is a pseudoreductive group over k. The main theorem (5.1.1) of Conrad et al. 2010 says that, except possibly when k has characteristic 2 or 3, every pseudoreductive group over k arises by such a construction (the theorem also treats the exceptional cases).

6.5 The maximal tori in reductive groups are their own centralizers. Any pseudoreductive group with this property is reductive (except possibly in characteristic 2; Conrad et al. 2010, 11.1.1).

6.6 If G is reductive, then $G = \mathcal{D}G \cdot (ZG)^{\circ}$ where $\mathcal{D}G$ is the derived group of G and $(ZG)^{\circ}$ is the largest central connected reductive subgroup of G. This statement becomes false with "pseudoreductive" for "reductive" (Conrad et al. 2010, 11.2.1).

6.7 For a reductive group G, the map

$$RG = (ZG)^\circ \to G/\mathcal{D}G$$

is an isogeny, and G is semisimple if and only if one (hence both) groups are trivial. For a pseudoreductive group, the condition $RG = 1$ does not imply that $G = \mathcal{D}G$. Conrad et al. 2010, 11.2.2, instead adopt the definition: an algebraic group G is ***pseudo-semisimple*** if it is pseudoreductive and $G = \mathcal{D}G$. The derived group of a pseudoreductive group is pseudo-semisimple (ibid. 1.2.6, 11.2.3).

6.8 A reductive group G over any field k is unirational, and so $G(k)$ is dense in G if k is infinite. This fails for pseudoreductive groups: over every nonperfect field k there exists a commutative pseudoreductive group that it not unirational; when k is a nonperfect rational function field $k_0(T)$, such a group G can be chosen so that $G(k)$ is not dense in G (Conrad et al. 2010, 11.3.1).

7 Properties of G versus those of $\mathsf{Rep}_k(G)$: a summary

7.1 An affine group G is finite if and only if there exists a representation (V,r) such that every representation of G is a subquotient of V^n for some $n \geq 0$ (XII, 1.4).

7.2 A affine group G is strongly connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\mathsf{Rep}(G)$ of subquotients of V^n, $n \geq 0$, is not stable under $\otimes$ (apply 7.1). In characteristic zero, a group is strongly connected if and only if it is connected.

7.3 An affine group G is unipotent if and only if every simple representation is trivial (this is essentially the definition XV, 2.1).

7.4 An affine group G is trigonalizable if and only if every simple representation has dimension 1 (this is the definition XVI, 1.1).

7.5 An affine group G is algebraic if and only if $\mathsf{Rep}(G) = \langle V \rangle^{\otimes}$ for some representation (V,r) (VIII, 11.7).

7.6 Let G be a smooth connected algebraic group. If $\mathsf{Rep}(G)$ is semisimple, then G is reductive (2.8), and the converse is true in characteristic zero (II, 5.4).

CHAPTER XVIII

Beyond the basics

Not yet written. It will provide a 50 page summary of the rest of the theory of affine algebraic groups, as developed in detail in LAG and RG.

Bibliography

ABE, E. 1980. Hopf algebras, volume 74 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge. Translated from the Japanese by Hisae Kinoshita and Hiroko Tanaka.

ANDRÉ, Y. 1992. Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part. *Compositio Math.* 82:1–24.

ARTIN, M. 1991. Algebra. Prentice Hall Inc., Englewood Cliffs, NJ.

BARSOTTI, I. 1955a. Structure theorems for group-varieties. *Ann. Mat. Pura Appl. (4)* 38:77–119.

BARSOTTI, I. 1955b. Un teorema di struttura per le varietà gruppali. *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (8)* 18:43–50.

BOREL, A. 1969. Linear algebraic groups. Notes taken by Hyman Bass. W. A. Benjamin, Inc., New York-Amsterdam.

BOREL, A. 1991. Linear algebraic groups. Springer-Verlag, New York.

BOREL, A. AND TITS, J. 1978. Théorèmes de structure et de conjugaison pour les groupes algébriques linéaires. *C. R. Acad. Sci. Paris Sér. A-B* 287:A55–A57.

BOURBAKI, N. A. Algèbre. Éléments de mathématique. Hermann; Masson, Paris.

BOURBAKI, N. LIE. Groupes et Algèbres de Lie. Éléments de mathématique. Hermann; Masson, Paris. Chap. I, Hermann 1960; Chap. II,III, Hermann 1972; Chap. IV,V,VI, Masson 1981;Chap. VII,VIII, Masson 1975; Chap. IX, Masson 1982 (English translation available from Springer).

CARTIER, P. 1962. Groupes algébriques et groupes formels, pp. 87–111. *In* Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962). Librairie Universitaire, Louvain.

CARTIER, P. 2007. A primer of Hopf algebras, pp. 537–615. *In* Frontiers in number theory, physics, and geometry. II. Springer, Berlin. Preprint available at IHES.

CHEVALLEY, C. 1960. Une démonstration d'un théorème sur les groupes algébriques. *J. Math. Pures Appl. (9)* 39:307–317.

CHEVALLEY, C. C. 1951. Théorie des groupes de Lie. Tome II. Groupes algébriques. Actualités Sci. Ind. no. 1152. Hermann & Cie., Paris.

CONRAD, B. 2002. A modern proof of Chevalley's [sic] theorem on algebraic groups. *J. Ramanujan Math. Soc.* 17:1–18.

CONRAD, B., GABBER, O., AND PRASAD, G. 2010. Pseudo-reductive groups, volume 17 of *New Mathematical Monographs*. Cambridge University Press, Cambridge.

DĂSCĂLESCU, S., NĂSTĂSESCU, C., AND RAIANU, Ş. 2001. Hopf algebras: an introduction, volume 235 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York.

DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics 900. Springer-Verlag, Berlin.

DEMAZURE, M. 1972. Lectures on p-divisible groups. Springer-Verlag, Berlin.

DEMAZURE, M. AND GABRIEL, P. 1970. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeur, Paris.

FIEKER, C. AND DE GRAAF, W. A. 2007. Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras. *LMS J. Comput. Math.* 10:271–287.

GREENBERG, M. J. 1961. Schemata over local rings. *Ann. of Math. (2)* 73:624–648.

GREENBERG, M. J. 1963. Schemata over local rings. II. *Ann. of Math. (2)* 78:256–266.

HARTSHORNE, R. 1977. Algebraic geometry. Springer-Verlag, New York.

HOCHSCHILD, G. 1971a. Introduction to affine algebraic groups. Holden-Day Inc., San Francisco, Calif.

HOCHSCHILD, G. 1971b. Note on algebraic Lie algebras. *Proc. Amer. Math. Soc.* 29:10–16.

HOCHSCHILD, G. AND MOSTOW, G. D. 1969. Automorphisms of affine algebraic groups. *J. Algebra* 13:535–543.

HOCHSCHILD, G. P. 1981. Basic theory of algebraic groups and Lie algebras, volume 75 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

HUMPHREYS, J. E. 1975. Linear algebraic groups. Springer-Verlag, New York.

KOHLS, M. 2011. A user friendly proof of Nagata's characterization of linearly reductive groups in positive characteristics. *Linear Multilinear Algebra* 59:271–278.

KOLCHIN, E. R. 1948. On certain concepts in the theory of algebraic matric groups. *Ann. of Math. (2)* 49:774–789.

MACLANE, S. 1971. Categories for the working mathematician. Springer-Verlag, New York. Graduate Texts in Mathematics, Vol. 5.

MATSUMURA, H. AND OORT, F. 1967. Representability of group functors, and automorphisms of algebraic schemes. *Invent. Math.* 4:1–25.

MILNE, J. S. 1980. Etale cohomology, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J.

MUMFORD, D. 1966. Introduction to algebraic geometry. Harvard Notes. (Reprinted, with the introduction of errors, by Springer as The Red Book of Varieties and Schemes, 1999).

MURRE, J. P. 1967. Lectures on an introduction to Grothendieck's theory of the fundamental group. Tata Institute of Fundamental Research, Bombay. Notes by S. Anantharaman, Tata Institute of Fundamental Research Lectures on Mathematics, No 40.

NITSURE, N. 2002. Representability of $\mathrm{G}L_E$. *Proc. Indian Acad. Sci. Math. Sci.* 112:539–542.

NITSURE, N. 2004. Representability of Hom implies flatness. *Proc. Indian Acad. Sci. Math. Sci.* 114:7–14.

NOETHER, E. 1927. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Mathematische Annalen* 96:26–61.

NORI, M. V. 1987. On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$. *Invent. Math.* 88:257–275.

OESTERLÉ, J. 1984. Nombres de Tamagawa et groupes unipotents en caractéristique p. *Invent. Math.* 78:13–88.

OORT, F. 1966. Algebraic group schemes in characteristic zero are reduced. *Invent. Math.* 2:79–80.

PERRIN, D. 1976. Approximation des schémas en groupes, quasi compacts sur un corps. *Bull. Soc. Math. France* 104:323–335.

PINK, R. 2005. Finite group schemes. Available at the author's website www.math.ethz.ch/~pink/.

ROSENLICHT, M. 1956. Some basic theorems on algebraic groups. *Amer. J. Math.* 78:401–443.

RUSSELL, P. 1970. Forms of the affine line and its additive group. *Pacific J. Math.* 32:527–539.

SAAVEDRA RIVANO, N. 1972. Catégories Tannakiennes. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin.

SERRE, J.-P. 1993. Gèbres. *Enseign. Math. (2)* 39:33–85.

SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 1,2. Springer-Verlag, Berlin.

SPRINGER, T. A. 1998. Linear algebraic groups, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA.

SWEEDLER, M. E. 1969. Hopf algebras. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York.

TAKEUCHI, M. 1972. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.* 7:251–270.

TATE, J. 1997. Finite flat group schemes, pp. 121–154. *In* Modular forms and Fermat's last theorem (Boston, MA, 1995). Springer, New York.

TITS, J. 1967. Lectures on Algebraic Groups, fall term 1966–1967, Yale University.

TITS, J. 1992. Théorie des groupes (Course at the Collège de France 1991-92, see Annuaire du Collège de France).

TITS, J. 1993. Théorie des groupes (Course at the Collège de France 1992-93, see Annuaire du Collège de France).

VARADARAJAN, V. S. 2004. Supersymmetry for mathematicians: an introduction, volume 11 of *Courant Lecture Notes in Mathematics*. New York University Courant Institute of Mathematical Sciences, New York.

WATERHOUSE, W. C. 1975. Basically bounded functors and flat sheaves. *Pacific J. Math.* 57:597–610.

WATERHOUSE, W. C. 1979. Introduction to affine group schemes, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

WEIL, A. 1960. Adeles and algebraic groups. Mimeographed Notes of a Seminar at IAS, 1959–1960. Reprinted by Birkhäuser Boston, 1982.

WEIL, A. 1962. Foundations of algebraic geometry. American Mathematical Society, Providence, R.I.

Index