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

Table of Contents 3

I Definition of an affine group **17**
1 Motivating discussion . . . 17
2 Some category theory . . . 18
3 Affine groups . . . 21
4 Affine monoids . . . 26
5 Affine supergroups . . . 27
6 Terminology . . . 28
7 Exercises . . . 28

II Affine Groups and Hopf Algebras **29**
1 Algebras . . . 29
2 Coalgebras . . . 30
3 The duality of algebras and coalgebras . . . 31
4 Bi-algebras . . . 32
5 Affine groups and Hopf algebras . . . 34
6 Abstract restatement . . . 36
7 Commutative affine groups . . . 36
8 Quantum groups . . . 36
9 Terminology . . . 37
10 Exercises . . . 37

III Affine Groups and Group Schemes **41**
1 The spectrum of a ring . . . 41
2 Schemes . . . 43
3 Affine groups as affine group schemes . . . 44
4 Summary . . . 45

IV Examples **47**
1 Examples of affine groups . . . 47
2 Examples of homomorphisms . . . 54
3 Appendix: A representability criterion . . . 54

V Some Basic Constructions **57**
1 Products of affine groups . . . 57
2 Fibred products of affine groups . . . 57
3 Limits of affine groups . . . 58

4 Extension of the base ring (extension of scalars) 59
5 Restriction of the base ring (Weil restriction of scalars) 60
6 Transporters 64
7 Galois descent of affine groups 67
8 The Greenberg functor 68
9 Exercises 69

VI Affine groups over fields **71**
1 Affine k-algebras 71
2 Schemes algebraic over a field 71
3 Algebraic groups as groups in the category of affine algebraic schemes . . . 73
4 Terminology 75
5 Homogeneity 75
6 Reduced algebraic groups 76
7 Smooth algebraic schemes 77
8 Smooth algebraic groups 78
9 Algebraic groups in characteristic zero are smooth (Cartier's theorem) . . . 79
10 Smoothness in characteristic $p \neq 0$ 81
11 Appendix: The faithful flatness of Hopf algebras 82

VII Group Theory: Subgroups and Quotient Groups. **87**
1 A criterion to be an isomorphism 87
2 Injective homomorphisms 88
3 Affine subgroups 89
4 Kernels of homomorphisms 90
5 Dense subgroups 92
6 Normalizers; centralizers; centres 97
7 Quotient groups; surjective homomorphisms 100
8 Existence of quotients 105
9 Semidirect products 105
10 Smooth algebraic groups 106
11 Algebraic groups as sheaves 106
12 Terminology 109
13 Exercises 109

VIII Representations of Affine Groups **111**
1 Finite groups 111
2 Definition of a representation 112
3 Terminology 113
4 Comodules 114
5 The category of comodules 117
6 Representations and comodules 118
7 The category of representations of G 123
8 Affine groups are inverse limits of algebraic groups 123
9 Algebraic groups admit finite-dimensional faithful representations 125
10 The regular representation contains all 126
11 Every faithful representation generates $\mathsf{Rep}(G)$ 127
12 Stabilizers of subspaces 130

13 Chevalley’s theorem . . . 132
14 Sub-coalgebras and subcategories . . . 133
15 Quotient groups and subcategories . . . 134
16 Characters and eigenspaces . . . 134
17 Every normal affine subgroup is a kernel . . . 136
18 Variant of the proof of the key Lemma 17.4 . . . 138
19 Applications of Corollary 17.6 . . . 138

IX Group Theory: the Isomorphism Theorems **141**
1 Review of abstract group theory . . . 141
2 The existence of quotients . . . 142
3 The homomorphism theorem . . . 143
4 The isomorphism theorem . . . 144
5 The correspondence theorem . . . 145
6 The Schreier refinement theorem . . . 146
7 The category of commutative algebraic groups . . . 148
8 Exercises . . . 148

X Categories of Representations (Tannaka Duality) **151**
1 Recovering a group from its representations . . . 151
2 Application to Jordan decompositions . . . 154
3 Characterizations of categories of representations . . . 159
4 Homomorphisms and functors . . . 166

XI The Lie Algebra of an Affine Group **169**
1 Definition of a Lie algebra . . . 169
2 The isomorphism theorems . . . 170
3 The Lie algebra of an affine group . . . 171
4 Examples . . . 173
5 Description of Lie(G) in terms of derivations . . . 176
6 Extension of the base field . . . 177
7 The adjoint map Ad: $G \to \mathrm{Aut}(\mathfrak{g})$ . . . 178
8 First definition of the bracket . . . 179
9 Second definition of the bracket . . . 179
10 The functor Lie preserves fibred products . . . 180
11 Commutative Lie algebras . . . 182
12 Normal subgroups and ideals . . . 182
13 Algebraic Lie algebras . . . 182
14 The exponential notation . . . 183
15 Arbitrary base rings . . . 184
16 More on the relation between algebraic groups and their Lie algebras . . . 185

XII Finite Affine Groups **191**
1 Definitions . . . 191
2 Étale affine groups . . . 193
3 Finite flat affine p-groups . . . 197
4 Cartier duality . . . 199
5 Exercises . . . 201

XIII The Connected Components of an Algebraic Group **203**
1 Idempotents and connected components . . . 203
2 Étale subalgebras . . . 206
3 Algebraic groups . . . 208
4 Affine groups . . . 212
5 Exercises . . . 212
6 Where we are . . . 213

XIV Groups of Multiplicative Type; Tori **215**
1 Group-like elements . . . 215
2 The characters of an affine group . . . 216
3 The affine group $D(M)$ . . . 217
4 Diagonalizable groups . . . 219
5 Groups of multiplicative type . . . 223
6 Rigidity . . . 227
7 Smoothness . . . 229
8 Group schemes . . . 230
9 Exercises . . . 230

XV Unipotent Affine Groups **231**
1 Preliminaries from linear algebra . . . 231
2 Unipotent affine groups . . . 232
3 Unipotent affine groups in characteristic zero . . . 237
4 Group schemes . . . 239

XVI Solvable Affine Groups **241**
1 Trigonalizable affine groups . . . 241
2 Commutative algebraic groups . . . 243
3 The derived group of an algebraic group . . . 246
4 Solvable algebraic groups . . . 248
5 Structure of solvable groups . . . 251
6 Split solvable groups . . . 252
7 Tori in solvable groups . . . 252
8 Exercises . . . 253

XVII The Structure of Algebraic Groups **255**
1 Radicals and unipotent radicals . . . 255
2 Definition of semisimple and reductive groups . . . 256
3 The canonical filtration on an algebraic group . . . 258
4 The structure of semisimple groups . . . 259
5 The structure of reductive groups . . . 261
6 Pseudoreductive groups . . . 263
7 Properties of G versus those of $\mathsf{Rep}_k(G)$: a summary . . . 265

XVIII Beyond the basics **267**

Bibliography **269**

Index **273**

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);
$X \stackrel{\text{def}}{=} Y$ 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,

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

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

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

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 $f\colon A \to R$ defines a commutative diagram

$$\begin{array}{ccccccc} h^A(A) & \xrightarrow{h^A(f)} & h^A(R) & \qquad & \mathrm{id}_A & \longmapsto & f \\ \downarrow{\scriptstyle T_A} & & \downarrow{\scriptstyle T_R} & & \downarrow & & \downarrow \\ F(A) & \xrightarrow{F(f)} & F(R) & & a_T & \longmapsto & F(f)(a_T),\ T_R(f). \end{array}$$

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 $A \rightsquigarrow h^A\colon \mathsf{A} \to \mathsf{A}^\vee$ 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

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

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

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

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 $F\colon \mathsf{A} \to \mathsf{Set}$ 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 $T_a\colon h^A \to F$ is an isomorphism. Note that, if F is representable, say $F \approx h^A$, then the choice of an isomorphism $T\colon h^A \to F$ 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

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

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

$$\begin{array}{ccc} G(R) & \xrightarrow{\alpha(R)} & H(R) \\ \downarrow{\scriptstyle G(\phi)} & & \downarrow{\scriptstyle H(\phi)} \\ G(R') & \xrightarrow{\alpha(R')} & H(R') \end{array}$$

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

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

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 $\alpha: h^A \to G$ 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 $G: \mathsf{Alg}_k \to \mathsf{Grp}$ 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

$$\begin{array}{ccc} G_0(R) & \xrightarrow{f_R} & R \\ \downarrow{\scriptstyle G_0(\phi)} & & \downarrow{\scriptstyle \phi} \\ G_0(R') & \xrightarrow{f_{R'}} & R' \end{array}$$

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 $\alpha: h^B \to h^A$ 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 $\Delta: A \to A \otimes A$. Let Δ be a comultiplication on the k-algebra A. For every k-algebra R, the map,

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

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 $G: \mathsf{Alg}_k \to \mathsf{Set}$ be a representable functor, and let $m: G \times G \to G$ be a natural transformation. Let (A, a) represent G, so that $T_a: h^A \simeq G$. 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 $\Delta: A \to A \otimes A$. 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 $G: \mathsf{Alg}_k \to \mathsf{Grp}$ such that the underlying set-valued functor is representable, or
(c) a k-algebra A together with a comultiplication $\Delta: A \to A \otimes A$ 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 $\Delta: A \to A \otimes A$ corresponding (by the Yoneda lemma) to m. To pass from (c) to (a), take G to be h^A endowed with the multiplication $m: G \times G \to G$ 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 $\Delta: k[M] \to k[M] \otimes k[M]$ 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 $\Delta: A \to A \otimes A$ 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 $\epsilon: A \to k$ and $S: A \to A$ 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 $h^{\mathcal{O}(G)}: \mathsf{Alg}_k \to \mathsf{Grp}$ 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 $f_R: G(R) \to R$ (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 $g: A \to R$. 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 $u: G \to H$ defines a homomorphism of k-algebras $u^{\natural}: \mathcal{O}(H) \to \mathcal{O}(G)$. 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:

$$\begin{array}{ccccccc} M_1 & \longrightarrow & \{1\} & \quad & M^\times & \longrightarrow & M_1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle (a,b)\mapsto b} \\ M \times M & \xrightarrow{(a,b)\mapsto ab} & M & & M_1 & \xrightarrow{(a,b)\mapsto a} & M. \end{array}$$

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

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

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

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

and the odd symbols

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

by setting

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

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

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

(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

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

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 $(A, m, e, \Delta, \epsilon)$ 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) $\Delta: A \to A \otimes A$ is a homomorphism of algebras;
(d) $\epsilon: A \to k$ 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 $(A, m, e, \Delta, \epsilon)$ 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 $S: A \to A$ 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

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

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

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

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 $f: A \to A'$,*

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

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:

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

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 $\mathrm{inv}: M \to M$ 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 $S: A \to A$ 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 $f: A \to A'$ 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 $f: A \to A'$ defines a morphism of functors $h^f: G \to G'$. 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 $\Delta: A \to A \otimes A$, 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 (non-commutative) 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:

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

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

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

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

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

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*** $\mathrm{spec}(A)$ 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 $\mathfrak{a}$,

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

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). $\square$

In other words, Spec is an equivalence from $\mathsf{Alg}_{\mathbb{Z}}^{\mathrm{opp}}$ 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). $\square$

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

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

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

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

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.

$\mathsf{Func}(\mathsf{Alg}_k, \mathsf{Set})$	$\xleftarrow{h^A \leftsquigarrow A}$	$\mathsf{Alg}_k^{\mathrm{opp}}$	$\xrightarrow{A \rightsquigarrow \mathrm{Spec}(A)}$	Sch/k
$\left\{\begin{matrix}\text{Representable}\\ \text{functors}\end{matrix}\right\}$	$\sim$	$\mathsf{Alg}_k^{\mathrm{opp}}$	$\sim$	{Affine schemes}
{Affine groups}	$\sim$	{Groups in $\mathsf{Alg}_k^{\mathrm{opp}}$}	$\sim$	$\left\{\begin{matrix}\text{Affine group}\\ \text{schemes}\end{matrix}\right\}$

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

(a) for all k-algebras R, the map $m(R): G(R) \times G(R) \to G(R)$ is a group structure on the set $G(R)$;
(b) there exist natural transformations $e: * \to G$ and $\mathrm{inv}: G \to G$ (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 $\Delta: A \to A \otimes A$ a homomorphism satisfying the equivalent conditions:

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

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

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 $\epsilon: A \to k$ and $S: A \to A$ (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 $m: G \times G \to G$ a morphism satisfying the equivalent conditions:

(a) for all k-algebras R, the map $m(R): G(R) \times G(R) \to G(R)$ is a group structure on the set $G(R)$;
(b) there exist there exist morphisms $e: * \to G$ and $\mathrm{inv}: G \to G$ (necessarily unique) satisfying the conditions of I, 2.7;
(c) for all k-schemes S, the map $m(S): G(S) \times G(S) \to G(S)$ 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 $(X_{ij})_{1\le i,j\le n}$). 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

$$\begin{cases} \Delta x_{ik} = \sum_{j=1,\ldots,n} x_{ij} \otimes x_{jk} \\ \Delta y = y \otimes y \end{cases} \qquad \begin{cases} \epsilon(x_{ii}) = 1 \\ \epsilon(x_{ij}) = 0, \; i \neq j \\ \epsilon(y) = 1 \end{cases} \qquad \begin{cases} S(x_{ij}) = y a_{ji} \\ S(y) = \det(x_{ij}) \end{cases}$$

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

$$\Delta(x) = (x) \otimes (x)$$
$$\epsilon(x) = I$$

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

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

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:

$$\begin{array}{ccccc} F(R) & \to & F'(R_{k'}) & \rightrightarrows & F'(R_{k'} \otimes_R R_{k'}) \\ & & \downarrow\approx & & \downarrow\approx \\ h^A(R) & \to & h^{A'}(R_{k'}) & \rightrightarrows & h^{A'}(R_{k'} \otimes_R R_{k'}). \end{array}$$

□

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

$$F(R) \to \prod_i F(R_{f_i}) \rightrightarrows \prod_{i,j} F(R_{f_i} \otimes_R R_{f_j})$$

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 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 spec(k). A similar statement holds with "Zariski" replaced by "étale".