

Algebraic Groups, Lie Groups, and their Arithmetic Subgroups

J.S. Milne



Version 3.00
April 1, 2011

This work is a modern exposition of the theory of algebraic groups (affine group schemes), Lie groups, and their arithmetic subgroups.

BibTeX information:

```
@misc{milneALA,  
author={Milne, James S.},  
title={Algebraic Groups, Lie Groups, and their Arithmetic Subgroups},  
year={2011},  
note={Available at www.jmilne.org/math/}  
}
```

v1.00 April 29, 2009. First version on the web (first two chapters only).

v1.01 May 10, 2009. Minor fixes.

v1.02 June 1, 2009. More minor fixes.

v2.00 April 27, 2010. Posted all 6 chapters (378 pages).

v3.00 April 1, 2011. Revised and expanded (422 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.

Copyright © 2005, 2006, 2009, 2010, 2011 J.S. Milne.

Single paper copies for noncommercial personal use may be made without explicit permission from the copyright holder.

Table of Contents

Table of Contents	3
Preface	5
I Basic Theory of Affine Groups	13
1 Introductory overview	14
2 Definitions	18
3 Examples	29
4 Some basic constructions	34
5 Affine groups and Hopf algebras	41
6 Affine groups and affine group schemes	53
7 Group theory: subgroups and quotient groups.	73
8 Representations of affine groups	94
9 Group theory: the isomorphism theorems	121
10 Recovering a group from its representations; Jordan decompositions	128
11 Characterizations of categories of representations	137
12 Finite flat affine groups	144
13 The connected components of an algebraic group	152
14 Groups of multiplicative type; tori	163
15 Unipotent affine groups	176
16 Solvable affine groups	183
17 The structure of algebraic groups	194
18 Example: the spin groups	203
19 The classical semisimple groups	217
20 The exceptional semisimple groups	232
21 Tannakian categories	233
II Lie Algebras and Algebraic Groups	239
1 The Lie algebra of an algebraic group	239
2 Lie algebras and algebraic groups	255
3 Nilpotent and solvable Lie algebras	264
4 Unipotent algebraic groups and nilpotent Lie algebras	273
5 Semisimple Lie algebras and algebraic groups	277
6 Semisimplicity of representations	287
III The Structure of Semisimple Lie Algebras and Algebraic Groups in Characteristic Zero	295
1 Root systems and their classification	296

2	Structure of semisimple Lie algebras and their representations	305
3	Structure of semisimple algebraic groups and their representations	317
4	Real Lie algebras and real algebraic groups	325
5	Reductive groups	326
IV	Lie groups	327
1	Lie groups	327
2	Lie groups and algebraic groups	328
3	Compact topological groups	331
V	The Structure of Reductive Groups: the split case	333
1	Split reductive groups: the program	333
2	The root datum of a split reductive group	338
3	Borel fixed point theorem and applications	351
4	Parabolic subgroups and roots	363
5	Root data and their classification	366
6	Construction of split reductive groups: the existence theorem	374
7	Construction of isogenies of split reductive groups: the isogeny theorem . .	377
8	Representations of split reductive groups	378
VI	The Structure of Reductive Groups: general case	383
1	The cohomology of algebraic groups; applications	384
2	Classical groups and algebras with involution	394
3	Relative root systems and the anisotropic kernel.	395
VII	Arithmetic Subgroups	397
1	Commensurable groups	397
2	Definitions and examples	398
3	Questions	399
4	Independence of ρ and L	399
5	Behaviour with respect to homomorphisms	400
6	Adèlic description of congruence subgroups	401
7	Applications to manifolds	402
8	Torsion-free arithmetic groups	402
9	A fundamental domain for SL_2	403
10	Application to quadratic forms	404
11	“Large” discrete subgroups	405
12	Reduction theory	406
13	Presentations	408
14	The congruence subgroup problem	409
15	The theorem of Margulis	410
16	Shimura varieties	411
	Bibliography	413
	Index	419

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). Arithmetic groups are groups of matrices with integer entries. They are a basic source of discrete groups acting on manifolds.

The first goal of the present work is to provide a modern exposition of the 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 expositions² do not allow this.³ In recent years, the tannakian duality⁴ 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. **Chapter I** develops the basic theory of algebraic groups, including tannakian duality.

Lie algebras are an essential tool in studying both algebraic groups and Lie groups. In **Chapter II** develops the basic theory of Lie algebras and discusses the functor from algebraic groups to Lie algebras.

As Cartier (1956) noted, the relation between Lie algebras and algebraic groups in characteristic zero is best understood through their categories of representations. In **Chapter III** we review the classification of semisimple Lie algebras and their representations, and we

¹See, 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, and so the intuition provided by group theory is unavailable. Consider, for example, the subgroups $H = SL_p$ and $N = \mathbb{G}_m$ (diagonal) of GL_p over a field of characteristic p . If nilpotents are *not* allowed, then $N \cap H = 1$, and the map $H/H \cap N \rightarrow HN/N$ is the homomorphism $SL_p \rightarrow PGL_p$, which is an inseparable isogeny of degree p ; in particular, it is injective and surjective but not an isomorphism. 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*.

²The only exceptions I know of are Demazure and Gabriel 1970, Waterhouse 1979, and SGA3. While the first two do not treat the classification of semisimple algebraic groups over fields, the third assumes it.

³Worse, 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 the only ones available to him. When he wrote his influential book Borel 1969b, he persisted in using Weil's approach to algebraic geometry, and, with the exceptions noted in the preceding footnote, all subsequent authors have followed him.

⁴Strictly, 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".

exploit tannakian duality to deduce the classification of semisimple algebraic groups and their representations in characteristic zero.⁵ The only additional complication presented by algebraic groups is that of determining the centre of the simply connected algebraic group attached to a semisimple Lie algebra, but this centre can also be seen in the category of representations of the Lie algebra.

Although there are many books on algebraic groups, and even more on Lie groups, there are few that treat both. In fact it is not easy to discover in the expository literature what the precise relation between the two is. In **Chapter IV** we show that all connected complex semisimple Lie groups are algebraic groups,⁶ and that all connected real semisimple Lie groups arise as covering groups of algebraic groups. Thus the reader who understands the theory of algebraic groups and their representations will find that he also understands much of the basic theory of Lie groups. Realizing a Lie group as an algebraic group is the first step towards understanding the discrete subgroups of the Lie group.

In **Chapter V**, which is largely independent of Chapters III and IV, we study split reductive groups over arbitrary fields. It is a remarkable observation of Chevalley that, for reductive groups containing a split maximal torus, the theory is independent of the ground field (and, largely, even of the characteristic of the ground field). We define the root datum of a split reductive and explain how this describes the structure of groups, and we prove the fundamental isogeny theorem following the approach in Steinberg 1999.

In **Chapter VI**, we explain how descent theory and Galois cohomology allow one to extend to study nonsplit reductive groups. In particular, we prove that the list of classical semisimple algebraic groups in Chapter I, §19, is complete, and we include Tits's classification of nonsplit groups (Tits 1966, Selbach 1976).

For an algebraic group G over \mathbb{Q} , any subgroup of $G(\mathbb{Q})$ commensurable with $G(\mathbb{Z})$ is said to be arithmetic. In **Chapter VII**, we show that such a group Γ is discrete in the Lie group $G(\mathbb{R})$ and that the quotient $G(\mathbb{R})/\Gamma$ has finite volume. Selberg conjectured, and Margulis proved, that, except for $\mathrm{SO}(1, n)$ and $\mathrm{SU}(1, n)$, every discrete subgroup of finite covolume in a semisimple Lie group is arithmetic. In combination with the results of Chapter VI and VII, this gives a classification of Riemannian locally symmetric spaces up to finite covers (with a few exceptions).⁷

TERMINOLOGY

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

⁵The classical proof of the classification theorems for semisimple groups in characteristic zero uses the similar theorems for Lie algebras, deduces them for Lie groups, and then passes to algebraic groups (Borel 1975, §1). The only other proof in the expository literature that I know of is that of Chevalley, which works in all characteristics, but is quite long and complicated and requires algebraic geometry. The proof presented here requires neither analysis nor algebraic geometry.

⁶In other words, the convergent power series defining the group can be replaced by polynomials.

⁷Briefly, the universal covering space of such a space X is a Riemannian symmetric space \tilde{X} . The identity component of $\mathrm{Aut}(\tilde{X})$ is a real semisimple Lie group \mathcal{G} , and $X \approx \Gamma \backslash \mathcal{G} / K$ with K a maximal compact subgroup of \mathcal{G} and Γ a discrete subgroup of \mathcal{G} of finite covolume. The pairs (\mathcal{G}, K) can be classified in terms of Dynkin diagrams. Except in $\mathrm{SO}(1, n)$ and $\mathrm{SU}(1, n)$, the group Γ is commensurable with $i(G(\mathbb{Z}))$ where G is an algebraic group over \mathbb{Q} and $i: G(\mathbb{R}) \rightarrow \mathcal{G}$ is a homomorphism of Lie groups with compact kernel and finite cokernel. That a pair (G, i) exists over \mathbb{R} is shown in Chapter III, and the pairs (G, i) over \mathbb{Q} giving rise to a given pair over \mathbb{R} are classified for the classical groups in Chapter VII.

- ◇ We allow our rings to have nilpotents, i.e., we don't require that our algebraic groups be reduced.
- ◇ We **do not** identify an algebraic group G with its points $G(k)$ with in 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.
- ◇ 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.

Beyond its greater simplicity, there is another reason for replacing the old terminology with the new: for the study of group schemes over bases more general than fields there is no old terminology.

0a Notations; terminology

We use the standard (Bourbaki) notations: $\mathbb{N} = \{0, 1, 2, \dots\}$; \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., $p = 2, 3, 5, \dots$

Throughout k is the ground ring (always commutative, and usually 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 $\text{Hom}_{k\text{-lin}}(V, k)$ 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. When F and F' are functors from a category, we say that “a homomorphism $F(a) \rightarrow F'(a)$ is natural in a ” when we have a family of such maps, indexed by the objects a of the category, forming a natural transformation $F \rightarrow F'$. For a natural transformation $\alpha: F \rightarrow F'$, we often write α_R for the morphism $\alpha(R): F(R) \rightarrow F'(R)$. When its action on morphisms is obvious, we usually describe a functor F by giving its action $R \rightsquigarrow F(R)$ on objects. Categories are required to be locally small (i.e., the morphisms between any two objects form a set), except for the category \mathbf{A}^\vee of functors $\mathbf{A} \rightarrow \mathbf{Set}$. A diagram $A \rightarrow B \rightrightarrows C$ is said to be *exact* if the first arrow is the equalizer of the pair of arrows; in particular, this means that $A \rightarrow B$ is a monomorphism (cf. EGA I, Chap. 0, 1.4).

Here is a list of categories:

Category	Objects	Page
Alg_k	commutative k -algebras	
\mathbf{A}^\vee	functors $\mathbf{A} \rightarrow \mathbf{Set}$	
$\text{Comod}_k(C)$	finite-dimensional comodules over C	p. 100
Grp	(abstract) groups	
$\text{Rep}_k(G)$	finite-dimensional representations of G	p. 95
$\text{Rep}_k(\mathfrak{g})$	finite-dimensional representations of \mathfrak{g}	
Set	sets	
Vec_k	finite-dimensional vector spaces over k	

In each case, the morphisms are the usual ones, and composition is the usual composition.

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. 29
algebraic monoid	affine algebraic monoid	p. 29
bialgebra	commutative bi-algebra	p. 51
Hopf algebra	bialgebra with an inversion	p. 51
group scheme	affine group scheme	p. 60
algebraic group scheme	affine algebraic group scheme	p. 60
group variety	affine group variety	p. 60
subgroup	affine subgroup	p. 94
representation	linear representation	p. 97
root system	reduced root system	p. 297

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.

0b 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.

All chapters assume 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.

Chapter IV assumes the analysis usually taught in first-year graduate courses and in some advanced undergraduate courses.

Chapter V assumes some knowledge of algebraic geometry (my notes AG suffice).

Chapter VI assumes familiarity with the main statements of algebraic number theory (including class field theory, e.g., CFT, Chapter I §1; Chapter V).

0c 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 (v5.21, 2011).
CFT Class Field Theory (v4.00, 2008).

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).

Bourbaki TG Bourbaki, Topologie Générale.

DG Demazure and Gabriel, Groupes Algébriques, Tome I, 1970.

EGA Eléments de Géométrie Algébrique, Grothendieck (avec Dieudonné).

SGA Séminaire de Géométrie Algébrique, Grothendieck et al.

monnnnn <http://mathoverflow.net/questions/nnnnn/>

§ Subsection (so II, §3c means Chapter II, Section 3, Subsection c).

0d Sources

I list some of the works that I have found particularly useful in writing this book, and which may be useful also to the reader.

Chapter I: Demazure and Gabriel 1970; Serre 1993; Springer 1998; Waterhouse 1979.

Chapters II, III: Bourbaki LIE; Demazure and Gabriel 1970; Erdmann and Wildon 2006; Humphreys 1972; Serre 1965; Serre 1966.

Chapter IV: Lee 2002.

Chapter V: Conrad et al. 2010, Demazure and Gabriel 1970; SGA3; Springer 1979; Springer 1989; Springer 1998.

Chapter VI: Kneser 1969.

Chapter VII: Borel 1969a.

History: Borel 2001; Hawkins 2000; Helgason 1990, 1994; chapter notes in Springer 1998.

0e 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: Darij Grinberg, Lucio Guerberoff, Florian Herzig, Chu-Wee Lim, Victor Petrov, David Vogan, Xiandong Wang.

DRAMATIS PERSONÆ

JACOBI (1804–1851). In his work on partial differential equations, he discovered the Jacobi identity. Jacobi's work helped Lie to develop an analytic framework for his geometric ideas.

RIEMANN (1826–1866). Defined the spaces whose study led to the introduction of local Lie groups and Lie algebras.

LIE (1842–1899). Founded the subject that bears his name in order to study the solutions of differential equations.

KILLING (1847–1923). He introduced Lie algebras independently of Lie in order to understand the different noneuclidean geometries (manifolds of constant curvature), and he classified the possible Lie algebras over the complex numbers in terms of root systems. Introduced Cartan subalgebras, Cartan matrices, Weyl groups, and Coxeter transformations.

MAURER (1859–1927). His thesis was on linear substitutions (matrix groups). He characterized the Lie algebras of algebraic groups, and essentially proved that group varieties are rational (in characteristic zero).

ENGEL (1861–1941). In collaborating with Lie on the three-volume *Theorie der Transformationsgruppen* and editing Lie's collected works, he helped put Lie's ideas into coherent form and make them more accessible.

E. CARTAN (1869–1951). Corrected and completed the work of Killing on the classification of semisimple Lie algebras over \mathbb{C} , and extended it to give a classification of their representations. He also classified the semisimple Lie algebras over \mathbb{R} , and he used this to classify symmetric spaces.

WEYL (1885–1955). Proved that the finite-dimensional representations of semisimple Lie algebras and Lie groups are semisimple (completely reducible).

NOETHER (1882–1935).

HASSE (1898–1979).

BRAUER (1901–1977).

ALBERT (1905–1972).

They found a classification of semisimple algebras over number fields, which gives a classification of the classical algebraic groups over the same fields.

HOPF (1894–1971). Observed that a multiplication map on a manifold defines a comultiplication map on the cohomology ring, and exploited this to study the ring. This observation led to the notion of a Hopf algebra.

VON NEUMANN (1903–1957). Proved that every closed subgroup of a real Lie group is again a Lie group.

WEIL (1906–1998). Classified classical groups over arbitrary fields in terms of semisimple algebras with involution (thereby winning the all India cocycling championship for 1960).

CHEVALLEY (1909–1984). He proved the existence of the simple Lie algebras and of their representations without using the classification. One of the initiators of the systematic study of algebraic groups over arbitrary fields. Classified the split semisimple algebraic groups over any field, and in the process found new classes of finite simple groups.

KOLCHIN (1916–1991). Obtained the first significant results on matrix groups over *arbitrary* fields as preparation for his work on differential algebraic groups.

IWASAWA (1917–1998). Found the Iwasawa decomposition, which is fundamental for the structure of real semisimple Lie groups.

HARISH-CHANDRA (1923–1983). Independently of Chevalley, he showed the existence of the simple Lie algebras and of their representations without using the classification. With

Borel he proved some basic results on arithmetic groups. Was one of the founders of the theory of infinite-dimensional representations of Lie groups.

BOREL (1923–2003). He introduced algebraic geometry into the study of algebraic groups, thereby simplifying and extending earlier work of Chevalley, who then adopted these methods himself. Borel made many fundamental contributions to the theory of algebraic groups and of their arithmetic subgroups.

TITS (1930–). His theory of buildings gives an geometric approach to the study of algebraic groups, especially the exceptional simple groups. With Bruhat he used them to study the structure of algebraic groups over discrete valuation rings.

MARGULIS (1946–). Proved fundamental results on discrete subgroups of Lie groups.

Basic Theory of Affine Groups

The emphasis in this chapter is on affine algebraic groups over a base field, but, when it requires no extra effort, we often study more general objects: affine groups (not of finite type); base rings rather than fields; affine algebraic monoids rather than groups; affine algebraic supergroups (very briefly); quantum groups (even more briefly). The base field (or ring) is always denoted k , and R is always a commutative k -algebra.

NOTES Most sections in this chapter are complete but need to be revised. The main exceptions are Sections 18 and 19, which need to be completed, and Section 20, which needs to be written.

1	Introductory overview	14
2	Definitions	18
3	Examples	29
4	Some basic constructions	34
5	Affine groups and Hopf algebras	41
6	Affine groups and affine group schemes	53
7	Group theory: subgroups and quotient groups.	73
8	Representations of affine groups	94
9	Group theory: the isomorphism theorems	121
10	Recovering a group from its representations; Jordan decompositions	128
11	Characterizations of categories of representations	137
12	Finite flat affine groups	144
13	The connected components of an algebraic group	152
14	Groups of multiplicative type; tori	163
15	Unipotent affine groups	176
16	Solvable affine groups	183
17	The structure of algebraic groups	194
18	Example: the spin groups	203
19	The classical semisimple groups	217
20	The exceptional semisimple groups	232
21	Tannakian categories	233

1 Introductory overview

Loosely speaking, an algebraic group over a field k is a group defined by polynomials. Before giving the precise definition in the next section, 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,

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

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, 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 $((a_{ij})_{1 \leq i, j \leq n}, d)$ 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.

To simplify the statements, for the remainder of this section, we assume that the base field k has characteristic zero.

1a The building blocks

We now list 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 $\mathrm{GL}_n(k)$. Let σ be a permutation of $\{1, \dots, n\}$ 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 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 k 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 its only finite quotient group is trivial.

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 GL_n for some 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*¹ if its centre Z is finite and G/Z is simple. For example, SL_n is almost-simple for $n > 1$ because its centre

$$Z = \left\{ \begin{pmatrix} \xi & & 0 \\ & \ddots & \\ 0 & & \xi \end{pmatrix} \mid \xi^n = 1 \right\}$$

is finite and the quotient $PSL_n = SL_n/Z$ is simple.

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

$$H_1 \leftarrow G \rightarrow H_2.$$

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 $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$;
- D_n ($n \geq 4$), the special orthogonal group SO_{2n} ;
- 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, \dots, G_r if the map

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G$$

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,

$$G = SL_2 \times SL_2 / N, \quad N = \{(I, I), (-I, -I)\} \quad (1)$$

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. Semisimple algebraic groups will be our main interest.

¹Other authors say “quasi-simple” or “simple”.

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 connected algebraic group of multiplicative type is a **torus**.

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

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

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

1b 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 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 16.31).

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, they are extensions of semisimple groups by tori. For example, GL_n is reductive. It is an extension of the simple group PGL_n by the torus \mathbb{G}_m ,

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

Here $\mathbb{G}_m = \mathrm{GL}_1$ and the map $\mathbb{G}_m \rightarrow \mathrm{GL}_n$ sends it onto the subgroup of nonzero scalar matrices.

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 $\mathrm{diag}(-1, 1, \dots)$ lies in O_n and has determinant -1 , and so O_n is not connected: it contains $\mathrm{SO}_n \stackrel{\mathrm{def}}{=} \mathrm{Ker} \left(\mathrm{O}_n \xrightarrow{\det} \{\pm 1\} \right)$ 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 $\mathrm{diag}(a_1, \dots, a_n)$,

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

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

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

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

1c Summary

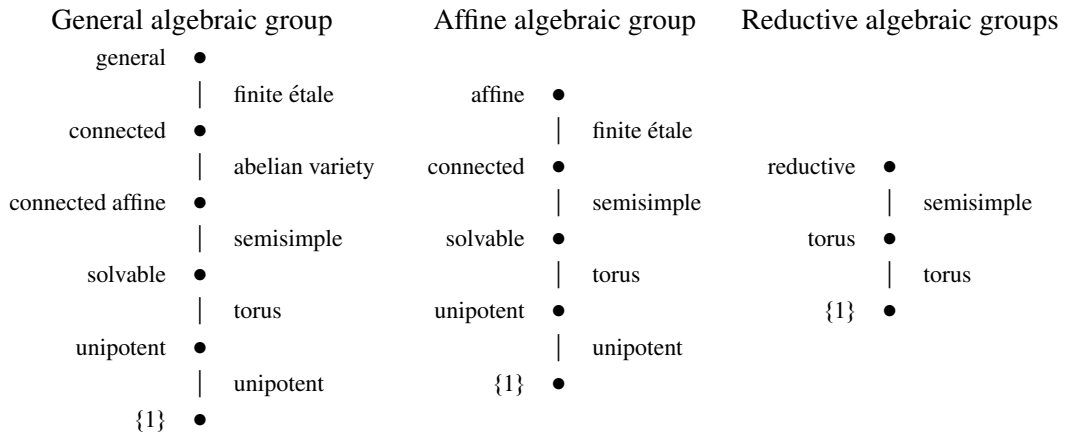
Recall that we are assuming that the base field k has characteristic zero. Every algebraic group has a composition series whose quotients are respectively a finite group, an abelian variety, a semisimple group, a torus, and a unipotent group. More precisely:

- (a) An algebraic group G contains a unique normal connected subgroup G° such that G/G° is a finite étale algebraic group (see 13.17).
- (b) A connected algebraic group G contains a largest² normal connected affine algebraic subgroup N ; the quotient G/N is an abelian variety (Barsotti, Chevalley, Rosenlicht).³
- (c) A connected affine algebraic group G contains a largest normal connected solvable algebraic subgroup N (see §17a); 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 17.2; 16.33).

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

²This means that it contains all other such algebraic subgroups; in particular, it is unique.

³The theorem is proved in Barsotti 1955b and in Rosenlicht 1956. Rosenlicht (ibid.) notes that it had been proved earlier with a different proof by Chevalley in 1953, who only published his proof in Chevalley 1960. A modern proof can be found in Conrad 2002.



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).

1d Exercises

EXERCISE 1-1 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.

EXERCISE 1-2 Let T be a commutative subgroup of $GL(V)$ consisting of diagonalizable endomorphisms. Show that there exists a basis for V relative to which $T \subset \mathbb{D}_n$.

EXERCISE 1-3 Let ϕ be a positive definite bilinear form on a real vector space V , and let $SO(\phi)$ be the algebraic subgroup of $SL(V)$ of maps α such that $\phi(\alpha x, \alpha y) = \phi(x, y)$ for all $x, y \in V$. Show that every element of $SO(\phi)$ is semisimple (but $SO(\phi)$ is not diagonalizable because it is not commutative).

EXERCISE 1-4 Let k be a field of characteristic zero. Show that every element of $GL_n(k)$ of finite order is semisimple. (Hence the group of permutation matrices in $GL_n(k)$ consists of semisimple elements, but it is not diagonalizable because it is not commutative).

2 Definitions

What is an affine algebraic group? For example, what is SL_n ? We know what $SL_n(R)$ 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 $R \rightarrow R'$ of rings defines a homomorphism of groups $SL_n(R) \rightarrow SL_n(R')$. 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 section, k is a commutative ring.

2a Motivating discussion

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

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

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

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

$$\det(X_{ij}) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in k[X_{11}, X_{12}, \dots, X_{nn}]. \quad (4)$$

The condition that G can be defined by polynomials is very strong: it excludes, for example, the functor with

$$G(R) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } R = k \\ \{1\} & \text{otherwise.} \end{cases}$$

Now suppose that k is noetherian, and let S be a subset of $k[X_1, \dots, X_n]$. The ideal \mathfrak{a} generated by S consists of the finite sums

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

Clearly S and \mathfrak{a} have the same zero-sets for any k -algebra R . According to the Hilbert basis theorem (CA 3.6), every ideal in $k[X_1, \dots, X_n]$ can be generated by a finite set of polynomials, and so an affine algebraic group is isomorphic (as a functor to sets) to the functor defined by a *finite* set of polynomials.

We have just observed that an affine algebraic group G is isomorphic to the functor defined by an *ideal* \mathfrak{a} of polynomials in some polynomial ring $k[X_1, \dots, X_n]$. Let $A = k[X_1, \dots, X_n]/\mathfrak{a}$. For any k -algebra R , a homomorphism $A \rightarrow R$ is determined by the images a_i of the X_i , and the n -tuples (a_1, \dots, a_n) that arise from a homomorphism are exactly those in the zero-set of \mathfrak{a} . Therefore the functor $R \mapsto \mathfrak{a}(R)$ sending a k -algebra R to the zero-set of \mathfrak{a} in R^n is canonically isomorphic to the functor

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

Since the k -algebras that can be expressed in the form $k[X_1, \dots, X_n]/\mathfrak{a}$ are exactly the finitely generated k -algebras, we conclude that the functors $\text{Alg}_k \rightarrow \text{Set}$ defined by a set of polynomials in a finite number of symbols are exactly the functors $R \mapsto \text{Hom}_{k\text{-alg}}(A, R)$ defined by a finitely generated k -algebra A .

Before continuing, it is convenient to review some category theory.

2b Some category theory

An object A of a category \mathbf{A} defines a functor

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

A morphism $\alpha: A' \rightarrow A$ of objects defines a map $f \mapsto f \circ \alpha: h^A(R) \rightarrow h^{A'}(R)$ which is natural in R (i.e., it is a natural transformation of functors $h^A \rightarrow h^{A'}$).

THE YONEDA LEMMA

Let $F: \mathbf{A} \rightarrow \mathbf{Set}$ be a functor from \mathbf{A} to the category of sets, and let A be an object of \mathbf{A} . A natural transformation $T: h^A \rightarrow F$ defines an element $a_T = T_A(\text{id}_A)$ of $F(A)$.

2.1 (YONEDA LEMMA) *The map $T \mapsto a_T$ is a bijection*

$$\text{Hom}(h^A, F) \simeq F(A) \tag{5}$$

with inverse $a \mapsto T_a$, where

$$(T_a)_R(f) = F(f)(a), \quad f \in h^A(R) = \text{Hom}(A, R).$$

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

PROOF. Let T be a natural transformation $h^A \rightarrow F$. For any morphism $f: A \rightarrow R$, the commutative diagram

$$\begin{array}{ccc} h^A(A) & \xrightarrow{h^A(f)} & h^A(R) \\ \downarrow T_A & & \downarrow T_R \\ F(A) & \xrightarrow{F(f)} & F(R) \end{array} \quad \begin{array}{ccc} \text{id}_A & \xrightarrow{\quad} & f \\ \downarrow & & \downarrow \\ a_T & \xrightarrow{\quad} & F(f)(a_T) = T_R(f) \end{array}$$

shows that

$$T_R(f) = F(f)(a_T). \tag{6}$$

Therefore T is determined by a_T , and so the map $T \mapsto a_T$ is injective. On the other hand, for $a \in F(A)$,

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

and so the map $T \mapsto a_T$ is surjective.

The proof of the naturality of (5) is left as an (easy) exercise for the reader. \square

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

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

In other words, the contravariant functor $A \rightsquigarrow h^A: \mathbf{A} \rightarrow \mathbf{A}^\vee$ is fully faithful.

REPRESENTABLE FUNCTORS

2.3 A functor $F: \mathbf{A} \rightarrow \mathbf{Set}$ is said to be **representable** if it is isomorphic to h^A for some object A . A pair (A, a) , $a \in F(A)$, is said to **represent** F if $T_a: h^A \rightarrow F$ is an isomorphism. Note that, if F is representable, say $F \approx h^A$, then the choice of an isomorphism $T: h^A \rightarrow F$ determines an element $a_T \in F(A)$ such that (A, a_T) represents F — in fact, $T = T_{a_T}$ — and so we sometimes say that (A, T) represents F .

2.4 Let F_1 and F_2 be functors $\mathbf{A} \rightarrow \mathbf{Set}$. In general, the natural transformations $F_1 \rightarrow F_2$ will form a proper class (not a set), but the Yoneda lemma shows that $\text{Hom}(F_1, F_2)$ is a set if F_1 is representable (because it is isomorphic to a set).

There are similar statements for the contravariant functors $\text{Hom}(-, A)$ defined by objects.

GROUP OBJECTS IN CATEGORIES

Let \mathbf{C} be a category with finite products (including a final object $*$).

2.5 A **group object** in \mathbf{C} is an object G of \mathbf{C} together with a morphism $m: G \times G \rightarrow G$ such that the induced map $G(T) \times G(T) \rightarrow G(T)$ makes $G(T)$ into a group for every T in \mathbf{C} . Here $G(T) = \text{Hom}(T, G)$.

2.6 A pair (G, m) is a group object if and only if there exist maps $e: * \rightarrow G$ and $\text{inv}: G \rightarrow G$ making the diagrams (35) and (36), p. 46, commute. (Exercise!).

2.7 Let (G, m) be a group object in \mathbf{C} . For every map $T \rightarrow T'$ of objects in \mathbf{C} , the map $G(T) \rightarrow G(T')$ is a homomorphism, and so (G, m) defines a functor $\mathbf{C} \rightarrow \mathbf{Grp}$. Conversely, suppose that for each object T in \mathbf{C} we are given a group structure on $G(T)$, and that for each morphism $T \rightarrow T'$ in \mathbf{C} the map $G(T) \rightarrow G(T')$ is a homomorphism of groups. According to the Yoneda lemma, the product maps $G(T) \times G(T) \rightarrow G(T)$ arise from a (unique) morphism $m: G \times G \rightarrow G$, and clearly (G, m) is a group object in \mathbf{C} . We conclude that to give a group object in \mathbf{C} is the same as giving a functor $\mathbf{C} \rightarrow \mathbf{Grp}$ such that the underlying functor to \mathbf{Set} is representable. (For more details, see, for example, Tate 1997, §1.)

2.8 A **monoid object** in \mathbf{C} is an object M of \mathbf{C} together with a morphism $m: M \times M \rightarrow M$ and a map $e: * \rightarrow M$ such that the induced map $G(T) \times G(T) \rightarrow G(T)$ makes $G(T)$ into a monoid with identity element $\text{Im}(e)$ for every T in \mathbf{C} . Remarks similar to (2.6) and (2.7) apply.

2c Definition of an affine (algebraic) group

Recall (CA §8) that the tensor product of two k -algebras A_1 and A_2 is their direct sum in the category Alg_k . In other words, if $f_1: A_1 \rightarrow R$ and $f_2: A_2 \rightarrow R$ are homomorphisms of k -algebras, there is a unique homomorphism $(f_1, f_2): A_1 \otimes A_2 \rightarrow R$ 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 $a_2 \in A_2$:

$$\begin{array}{ccccc}
 A_1 & \longrightarrow & A_1 \otimes A_2 & \longleftarrow & A_2 \\
 & \searrow f_1 & \downarrow (f_1, f_2) & \swarrow f_2 & \\
 & & R & &
 \end{array} \tag{7}$$

Now consider a k -algebra A together with a k -algebra homomorphism $\Delta: A \rightarrow A \otimes A$. For any k -algebra R , the map

$$f_1, f_2 \mapsto f_1 \cdot f_2 \stackrel{\text{def}}{=} (f_1, f_2) \circ \Delta: h^A(R) \times h^A(R) \rightarrow h^A(R), \tag{8}$$

is a binary operation on $h^A(R)$, which is natural in R .

DEFINITION 2.9 An **affine group** over k is a k -algebra A together with a homomorphism Δ such that (8) makes $h^A(R)$ into a group for all R . A **homomorphism of affine groups** $(A, \Delta) \rightarrow (A', \Delta')$ is a homomorphism $\alpha: A' \rightarrow A$ of k -algebras such that $\Delta \circ \alpha = (\alpha \otimes \alpha) \circ \Delta'$:

$$\begin{array}{ccc}
 A & \xleftarrow{\alpha} & A' \\
 \downarrow \Delta & & \downarrow \Delta' \\
 A \otimes A & \xleftarrow{\alpha \otimes \alpha} & A' \otimes A'
 \end{array} \tag{9}$$

Let $G = (A, \Delta)$ be an affine group. The ring A is called the **coordinate ring** (or **coordinate algebra**) of G , and is denoted $\mathcal{O}(G)$, and Δ is called the **comultiplication** of G . When $\mathcal{O}(G)$ is finitely presented⁴, G is called an **affine algebraic group**.

EXAMPLE 2.10 Let $A = k[X]$. Then $h^A(R)$ is isomorphic to R by $f \mapsto f(X)$. Let Δ be the homomorphism $k[X] \rightarrow k[X] \otimes k[X] = k[X \otimes 1, 1 \otimes X]$ such that

$$\Delta(X) = X \otimes 1 + 1 \otimes X.$$

For $f_1, f_2 \in h^A(R)$,

$$(f_1 \cdot f_2)(X) = (f_1, f_2)(X \otimes 1 + 1 \otimes X) = f_1(X) + f_2(X),$$

and so the binary operation on $h^A(R) \simeq R$ defined by Δ is just addition. Hence $(k[X], \Delta)$ is an affine algebraic group, called the **additive group**. It is denoted by \mathbb{G}_a .

EXAMPLE 2.11 Let M be a (multiplicative) commutative group, and let A be its group algebra, so the elements of A are the finite sums

$$\sum_m a_m m, \quad a_m \in k, \quad m \in M,$$

and

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

⁴Recall (CA 3.11) that a k -algebra A is finitely presented if it is isomorphic to the quotient of a polynomial ring $k[X_1, \dots, X_n]$ 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.

Set

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

Then $h^A(R) \simeq \text{Hom}_{\text{group}}(M, R^\times)$ with its natural group structure,

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

2.12 Let $\Delta: A \rightarrow A \otimes A$ be a homomorphism of k -algebras. In (5.15) we shall see that (A, Δ) is an affine group if and only if there exist homomorphism $\epsilon: A \rightarrow k$ and $S: A \rightarrow A$ 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 .

2.13 Let $G = (A, \Delta)$ be an affine algebraic group. Then

$$A \approx k[X_1, \dots, X_m]/(f_1, \dots, f_n)$$

for some m, n . The functor $h^A: \text{Alg}_k \rightarrow \text{Grp}$ is that defined by the set of polynomials $\{f_1, \dots, f_n\}$. The tensor product

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

is a polynomial ring in the symbols $X_1 \otimes 1, \dots, X_n \otimes 1, 1 \otimes X_1, \dots, 1 \otimes X_n$. Therefore Δ , and hence the multiplication on the groups $h^A(R)$, is also described by polynomials, namely, by any set of representatives for the polynomials $\Delta(X_1), \dots, \Delta(X_m)$.

AFFINE GROUPS AS FUNCTORS

Because $A_1 \otimes A_2$ is the direct sum of A_1 and A_2 in Alg_k , we have

$$h^{A_1 \otimes A_2} \simeq h^{A_1} \times h^{A_2}. \quad (10)$$

In particular, $h^{A \otimes A} \simeq h^A \times h^A$, and so we can regard h^Δ , for Δ a homomorphism $A \rightarrow A \otimes A$, as a functor $h^A \times h^A \rightarrow h^A$. When (A, Δ) is an affine group,

$$h^\Delta(R): h^A(R) \times h^A(R) \rightarrow h^A(R)$$

is the group structure in $h^A(R)$ defined by Δ .

For an affine group $G = (A, \Delta)$, we let $G(R) = h^A(R)$ when R a k -algebra. Then $R \rightsquigarrow G(R)$ is a functor $\text{Alg}_k \rightarrow \text{Grp}$.

Let $G' = (A', \Delta')$ be a second affine group, and let $\alpha: (A, \Delta) \rightarrow (A', \Delta')$ be a homomorphism of k -algebras. Because of the Yoneda lemma, the diagram (9) commutes if and only if

$$\begin{array}{ccc} h^A & \xrightarrow{h^\alpha} & h^{A'} \\ \uparrow h^\Delta & & \uparrow h^{\Delta'} \\ h^A \times h^A & \xrightarrow{h^\alpha \times h^\alpha} & h^{A'} \times h^{A'} \end{array} \quad (11)$$

commutes. This says that, under the bijection

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

provided by the Yoneda lemma, homomorphisms of algebraic groups correspond to natural transformations preserving the group structure, i.e., to natural transformations from G to G' as functors to Grp (rather than Set).

THEOREM 2.14 *The functor $A \rightsquigarrow h^A$ defines an equivalence from the category of affine groups over k to the category of functors $G: \text{Alg}_k \rightarrow \text{Grp}$ such that underlying functor to Set is representable. Under the equivalence, affine algebraic groups correspond to functors representable by finitely presented k -algebras.*

PROOF. We have just seen that the functor is fully faithful. Let G_0 be a functor $\text{Alg}_k \rightarrow \text{Set}$. To give a functor $G: \text{Alg}_k \rightarrow \text{Grp}$ such that $G_0 = (\text{forget}) \circ G$ is the same as giving a natural transformation $G_0 \times G_0 \rightarrow G_0$ that makes $G_0(R)$ into a group for all k -algebras R . If G_0 is representable by A , then $G_0 \times G_0$ is representable by $A \otimes A$ (see (10)), and so such a natural transformation corresponds (by the Yoneda lemma) to a homomorphism of k -algebras $\Delta: A \rightarrow A \otimes A$. Hence such a G arises from an affine group (A, Δ) , and so the functor is essentially surjective. This proves the first statement, and the second statement is obvious. \square

We now construct a canonical quasi-inverse to the functor in the theorem. Let \mathbb{A}^1 be the functor sending a k -algebra R to its underlying set,

$$\mathbb{A}^1: \text{Alg}_k \rightarrow \text{Set}, \quad (R, \times, +, 1) \rightsquigarrow R,$$

and let G be a functor from the category of k -algebras to groups,

$$G: \text{Alg}_k \rightarrow \text{Grp}.$$

Let $G_0 = (\text{forget}) \circ G$ be the underlying functor to Set , and let A be the set of natural transformations from G_0 to \mathbb{A}^1 ,

$$A = \text{Hom}(G_0, \mathbb{A}^1).$$

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

$$f_R: G(R) \rightarrow R, \quad R \text{ a } k\text{-algebra},$$

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

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

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

$$\begin{aligned} (f \pm f')_R(g) &= f_R(g) \pm f'_R(g) \\ (ff')_R(g) &= f_R(g) f'_R(g). \end{aligned}$$

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

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

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

PROPOSITION 2.15 *The functor G_0 is a representable if and only if α is an isomorphism.*

PROOF. If α is an isomorphism, then certainly G_0 is representable. Conversely, suppose that G_0 is represented by (B, b) . Then

$$A \stackrel{\text{def}}{=} \text{Hom}(G_0, \mathbb{A}^1) \stackrel{T_b}{\simeq} \text{Hom}(h^B, \mathbb{A}^1) \stackrel{\text{Yoneda}}{\simeq} \mathbb{A}^1(B) \simeq B,$$

where the last isomorphism uses that $\mathbb{A}^1 = h^{k[X]}$. Thus $A \simeq B$, and one checks that $\alpha: h^B \rightarrow h^A$ is the natural transformation defined by this isomorphism; therefore α is an isomorphism. This proves the statement. \square

SUMMARY 2.16 We have shown that it is essentially the same to give

- (a) a k -algebra A together with a homomorphism $\Delta: A \rightarrow A \otimes_k A$ that makes $h^A(R)$ into a group for all R , or
- (b) a functor $G: \text{Alg}_k \rightarrow \text{Grp}$ such that $\text{forget} \circ G$ is representable.

To pass from (a) to (b), take $G = h^A$ endowed with the multiplication $h^\Delta: G \times G \rightarrow G$. To pass from (b) to (a), take $A = \text{Hom}(\mathbb{A}^1, G_0)$ endowed with the homomorphism $A \rightarrow A \otimes A$ corresponding (by the Yoneda lemma) to $G \times G \rightarrow G$.

We adopted (a), rather than (b), as the definition of an affine group because it is more elementary. Throughout, we shall use the two descriptions of an affine algebraic group interchangeably.

Let G be an affine group, and let A be its coordinate ring. When we regard A as $\text{Hom}(G, \mathbb{A}^1)$, an element $f \in A$ is a family of maps $f_R: G(R) \rightarrow R$ (of sets) indexed by the k -algebras R and 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 $g: A \rightarrow R$. The two points of views are related by the equation

$$f_R(g) = g(f), \quad f \in A, \quad g \in G(R). \quad (12)$$

Moreover,

$$(\Delta f)_R(g_1, g_2) = f_R(g_1 \cdot g_2). \quad (13)$$

According to the Yoneda lemma, a homomorphism $\alpha: G \rightarrow H$ defines a homomorphism of rings $\alpha^*: \mathcal{O}(H) \rightarrow \mathcal{O}(G)$. Explicitly,

$$(\alpha^* f)_R(g) = f_R(\alpha_R g), \quad f \in \mathcal{O}(H), \quad g \in G(R). \quad (14)$$

When G is a functor $\text{Alg}_k \rightarrow \text{Grp}$ such that G_0 is representable, we shall loosely refer to any k -algebra A that represents G_0 (with an implicit isomorphism $h^A \simeq G_0$) as the coordinate ring of G , and denote it by $\mathcal{O}(G)$.

NOTES Consider the categories with the following objects and the obvious morphisms:

- (a) a functor $G: \text{Alg}_k \rightarrow \text{Grp}$ together with a representation (A, a) of the underlying functor to Set ;
- (b) a functor $G: \text{Alg}_k \rightarrow \text{Grp}$ such that the underlying functor to Set is representable;
- (c) a k -algebra A together with a homomorphism $\Delta: A \rightarrow A \otimes_k A$ that makes $h^A(R)$ into a group for all k -algebras R .

There are canonical “forgetful” functors $a \rightarrow b$ and $a \rightarrow c$ which are equivalences of categories. There are even canonical quasi-inverse functors $b \rightarrow a$ (take $A = \text{Hom}(G, \mathbb{A}^1) \dots$) and $c \rightarrow a$ (take $G = h^A \dots$). However, the functors are not isomorphisms of categories. In the previous version of the notes, I took (b) as the definition of affine group. In this version, I took (c) as the definition because it more obviously gives a reasonable category (no set theory problems). Perhaps (a) is the best.

2d Affine monoids

Recall that a **monoid** is a set M together with an associative binary operation $M \times M \rightarrow M$ and an identity element (usually denoted 0, 1, or e). In other words, it is a “group without inverses”. A **homomorphism** of monoids is a map $\varphi: M \rightarrow M'$ such that

- (a) $\varphi(e_M) = e_{M'}$, and
- (b) $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in M$.

When M' is a group, (a) holds automatically because a group has only one element such that $ee = e$. For any monoid M , the set M^\times of elements in M with inverses is a group (the largest subgroup of M).

An **affine monoid** is a k -algebra A together with homomorphisms $\Delta: A \rightarrow A \otimes A$ and $\epsilon: A \rightarrow k$ such that Δ makes $h^A(R)$ into a monoid with identity element $A \xrightarrow{\epsilon} k \rightarrow R$ for each k -algebra R . Essentially, this is the same as a functor from the category of k -algebras to monoids that is representable (as a functor to sets). When A is finitely presented, the affine monoid is said to be **algebraic**.

EXAMPLE 2.17 For a k -module V , let End_V be the functor

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

When V is finitely generated and projective, we saw in (3.6) that, as a functor to sets, End_V is represented by $\text{Sym}(V \otimes_k V^\vee)$, and so it is an algebraic monoid. When V is free, the choice of a basis e_1, \dots, 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 $k[X_{11}, X_{12}, \dots, X_{nn}]$.

PROPOSITION 2.18 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:

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

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 §4b below). \square

EXAMPLE 2.19 An associative k -algebra B with identity (not necessarily commutative) defines a functor $R \rightsquigarrow (R \otimes_k B, \times)$ from the category of k -algebras to monoids. When B is finitely generated and projective as a k -module, this is an affine algebraic monoid. For example, if $B = \text{End}_{k\text{-lin}}(V)$, then $\mathbb{G}_m^B = \text{GL}_V$. When B is also free, the choice of a basis for B identifies it (as a functor to sets) with $R \mapsto R^{\dim_k B}$, which is represented by $k[X_1, \dots, X_{\dim_k B}]$. For the general case, see 2.21 or DG II, §1, 2.3, p.149.

We let \mathbb{G}_m^B denote the corresponding affine algebraic group

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

2e 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, 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 $k[X_1, \dots, X_m, Y_1, \dots, Y_n]$ 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, \dots, 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, \dots, X_m , and when $m = 0$, it is the exterior algebra of the vector space with basis $\{Y_1, \dots, Y_n\}$ 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 $\text{GL}_{m|n}$ be the functor

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

It is known that such a matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is invertible (Varadarajan 2004, 3.6.1), and so $\text{GL}_{m|n}$ 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 $k[X_{11}, X_{12}, \dots, X_{m+n, m+n}, Y, Z]$ 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

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

Much of the theory of affine groups extends to affine supergroups (see, for example, Fiorese and Gavarini 2008).

2f A representability criterion

When k is not a field, the following criterion will sometimes be useful in showing that a functor to groups is an affine group.

THEOREM 2.20 *Let $F: \text{Alg}_k \rightarrow \text{Set}$ be a functor. If F is representable, then it satisfies the condition:*

(*) *for every faithfully flat homomorphism $R \rightarrow R'$ of k -algebras, the sequence*

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

is exact (i.e., the first arrow maps $F(R)$ bijectively onto the set on which the pair of arrows coincide).

Conversely, if F satisfies () and there exists a faithfully flat homomorphism $k \rightarrow k'$ such that $F_{k'}$ is representable, then F itself is representable.*

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

$$R \rightarrow R' \rightrightarrows R' \otimes_R R'$$

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

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

is exact, and so F satisfies (*).

Conversely, suppose that F satisfies (*), and let k' be a faithfully flat extension of k . For every k -algebra R , the map $R \rightarrow R_{k'}$ is faithfully flat, and so

$$F(R) \rightarrow F(R_{k'}) \rightrightarrows F(R_{k'} \otimes_R R_{k'})$$

is exact. In particular, F is determined by its restriction $F_{k'}$ to k' -algebras. Now suppose that $F_{k'}$ is representable by a k' -algebra A' . The fact that $F_{k'}$ comes from a functor over k means that it is equipped with a descent datum. This descent datum defines a descent datum on A' , which descent theory shows arises from a k -algebra A , which represents F (Waterhouse 1979, Chapter 17). \square

EXAMPLE 2.21 Let f_1, \dots, f_r be elements of k such that $(f_1, \dots, f_r) = k$. Then $k \rightarrow \prod k_{f_i}$ is faithfully flat because the condition means that no maximal ideal of k contains all f_i . Therefore a functor F satisfying (*) and such that $F_{k_{f_i}}$ is representable for each i is itself representable.

2g Terminology

From now on “algebraic group” will mean “affine algebraic group” and “algebraic monoid” will mean “affine algebraic monoid”.

3 Examples

In this section, we list some examples of affine groups and of homomorphisms of affine groups. Throughout this section, k is a commutative ring.

3a Examples of affine groups

3.1 We can now describe \mathbb{G}_a more simply as the functor $R \rightsquigarrow (R, +)$. It is represented by $k[X]$.

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

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

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 subring of polynomials in X and X^{-1} . The homomorphism

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

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

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

Thus $\mathcal{O}(\mathbb{G}_m) = k[X, X^{-1}]$; for $f \in k[X, X^{-1}]$ and $a \in \mathbb{G}_m(R) = R^\times$,

$$f_R(a) = f(a, a^{-1}).$$

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

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

and so G is an affine algebraic group, called the **trivial algebraic group**. More generally, for any finite group G , let $\mathcal{O}(G) = \prod_{g \in G} k_g$ (product of copies of k indexed by the elements of G). Then $R \rightsquigarrow \text{Hom}_{k\text{-alg}}(\mathcal{O}(G), R)$ is an affine algebraic group $(G)_k$ over k such that $(G)_k(R) = G$ for any k -algebra R with no nontrivial idempotents (see 5.23 below). Such an affine algebraic group is called a **constant finite algebraic group**.

3.4 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,

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

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

3.5 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 field k of characteristic $p \neq 0$,

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

is an additive group, and $R \rightsquigarrow \alpha_p(R)$ is a functor. Moreover,

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

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

3.6 For any k -module V , the functor of k -algebras⁵

$$D_a(V): R \rightsquigarrow \text{Hom}_{k\text{-lin}}(V, R) \quad (\text{additive group}) \quad (15)$$

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

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

(see CA §8). Therefore $D_a(V)$ 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

$$V_a: R \rightsquigarrow R \otimes V \quad (\text{additive group})$$

is not representable unless V is finitely generated and projective.⁶ 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,

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

(CA 10.8). Therefore V_a is an affine algebraic group with coordinate ring $\text{Sym}(V^\vee)$ when V is finitely generated and projective.

When V is finitely generated and free, the canonical maps

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

are obviously isomorphisms, and it follows that they are isomorphisms when V is a finitely generated and projective. Therefore, when V is finitely generated and projective, the functor

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

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

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

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

⁵Notations suggested by those in DG II, §1, 2.1.

⁶This is stated without proof in EGA I (1971) 9.4.10: “on peut montrer en effet que le foncteur $T \mapsto \Gamma(T, \mathcal{E}(T)) \dots$ n’est représentable que si \mathcal{E} est localement libre de rang fini”.

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

$$\det(MN) = \det(M) \cdot \det(N) \quad (16)$$

and

$$\operatorname{adj}(M) \cdot M = \det(M) \cdot I = M \cdot \operatorname{adj}(M) \quad (\text{Cramer's rule}) \quad (17)$$

where I denotes the identity matrix and

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

with M_{ij} the matrix obtained from M by deleting the i th row and the j th 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,

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

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

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

3.8 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 $\operatorname{GL}_n(R)$, and that $R \rightsquigarrow \operatorname{GL}_n(R)$ is a functor. Moreover,

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

and so GL_n is an affine algebraic group with coordinate ring⁷ $\frac{k[X_{11}, X_{12}, \dots, X_{nn}, Y]}{(\det(X_{ij})Y - 1)}$. It is called the **general linear group**. For $f \in \mathcal{O}(\operatorname{GL}_n)$ and $a = (a_{ij}) \in \operatorname{GL}_n(R)$,

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

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

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

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 $A \simeq \mathcal{O}(\operatorname{GL}_n)$.

⁷In other words, $\mathcal{O}(\operatorname{GL}_n)$ is the ring of fractions of $k[X_{11}, X_{12}, \dots, X_{nn}]$ for the multiplicative subset generated by $\det(X_{ij})$,

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

See CA, 6.2.

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

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

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

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

and so

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

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

$$\begin{cases} \det(X_{ij})Y - 1 \\ \sum_{j,k} X_{ji} c_{jk} X_{kl} - c_{il}, \quad i, l = 1, \dots, n. \end{cases}$$

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

3.10 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 $V \times V \rightarrow k$, and let ψ be a nondegenerate alternating form $V \times V \rightarrow k$. 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 (3.7), (3.8), or (3.9), which shows that they are affine algebraic groups in this case. For the general case, use (2.21).

3.11 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 $(\bar{a}, \bar{b}) = (b, a)$.

For an $n \times n$ matrix $A = (a_{ij})$ with entries in K , define \bar{A} to be (\bar{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 $e \in K \setminus k$. 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 $k[\dots, X_{ij}, \dots] \otimes_k k[\dots, Y_{ij}, \dots]$.

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

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

3.12 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

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

and so

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

3.13 Let $k = k_1 \times \cdots \times k_n$, and write $1 = e_1 + \cdots + e_n$. Then $\{e_1, \dots, e_n\}$ 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 . 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

$$G(R) = \prod_i G_i(R_i)$$

for all k -algebras $R = R_1 \times \cdots \times R_n$.

3b Examples of homomorphisms

3.14 The determinant defines a homomorphism of algebraic groups

$$\det: \mathrm{GL}_n \rightarrow \mathbb{G}_m.$$

3.15 The homomorphisms

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

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

4 Some basic constructions

Throughout this section, k is a commutative ring.

4a Products of affine groups

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

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

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

$$\mathcal{O}(G_1 \times G_2) = \mathcal{O}(G_1) \otimes \mathcal{O}(G_2), \quad (18)$$

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

$$\mathrm{Hom}_{k\text{-alg}}(A_1 \otimes_k A_2, R) \simeq \mathrm{Hom}_{k\text{-alg}}(A_1, R) \times \mathrm{Hom}_{k\text{-alg}}(A_2, R) \quad (19)$$

(see (7), p. 22).

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

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

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

4b Fibred products of affine groups

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

$$G_1 \rightarrow H \leftarrow G_2 \quad (20)$$

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

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

Obviously $G_1 \times_H G_2$ is the fibred product of G_1 and G_2 over H in the category of functors from Alg_k to Set .

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

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

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

$$\mathrm{Hom}_{k\text{-alg}}(A_1 \otimes_B A_2, R) \simeq \mathrm{Hom}_{k\text{-alg}}(A_1, R) \times_{\mathrm{Hom}_{k\text{-alg}}(B, R)} \mathrm{Hom}_{k\text{-alg}}(A_2, R). \quad (21)$$

Therefore, if the functors G_1 , G_2 , and H in (20) are represented by k -algebras A_1 , A_2 , and B , then $G_1 \times_H G_2$ is represented by the k -algebra $A_1 \otimes_B A_2$.

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

$$\mathcal{O}(G_1 \times_H G_2) = \mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2). \quad (22)$$

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

For example, let H be an affine group and let $* \rightarrow H$ be the unique homomorphism from the trivial group to H . For any homomorphism $\alpha: G \rightarrow H$,

$$(G \times_H *) (R) = \mathrm{Ker}(\alpha(R): G(R) \rightarrow H(R)).$$

The affine group $(G \times_H *)$ is called the **kernel** of α , and is denoted $\mathrm{Ker}(\alpha)$. Note that

$$\mathcal{O}(\mathrm{Ker}(G \rightarrow H)) = \mathcal{O}(G) \otimes_{\mathcal{O}(H)} k. \quad (23)$$

Similarly, the equalizer of a pair of homomorphisms can be realized as a fibred product. Therefore, all finite direct limits exist in the category of affine groups.

4c Extension of the base ring (extension of scalars)

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

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

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

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

(in (7), take $A_1 = k'$, $A_2 = \mathcal{O}(G)$, and f_1 equal to the given k' -algebra structure on R). The affine group $G_{k'}$ is said to have been obtained from G by **extension of the base ring** or by **extension of scalars**. If G is an algebraic group, so also is $G_{k'}$. Clearly $G \rightsquigarrow G_{k'}$ is a functor.

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

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

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

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

Similarly, if V is finitely generated and projective, then

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

EXAMPLE 4.2 Let G be the unitary group defined by a separable k -algebra K of degree 2 (see 3.11). For any field extension $k \rightarrow k'$, $G_{k'}$ is the unitary group defined by the k' -algebra $K \otimes_k k'$, and so, for example, $G_{k^{\text{al}}} \simeq \text{GL}_n$.

4d Restriction of the base ring (restriction of scalars)

Throughout this subsection, k' is a k -algebra that is finitely generated and projective as a k -module. We shall show that there is a right adjoint to the functor $G \rightsquigarrow G_{k'}$. We first explain this for functors to sets.

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

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

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

$$\text{Hom}(F_{k'}, F') \rightarrow \text{Hom}(F, (F')_{k'/k}).$$

This has an obvious inverse⁸, and so it is a bijection. We have shown that the extension of scalars functor $F \rightsquigarrow F_{k'}$ has a right adjoint $F' \rightsquigarrow (F')_{k'/k}$:

$$\text{Hom}(F_{k'}, F') \simeq \text{Hom}(F, (F')_{k'/k}). \quad (24)$$

Because it is a right adjoint, $F' \rightsquigarrow (F')_{k'/k}$ preserves inverse limits. In particular, it takes (fibred) products to (fibred) products. This can also be checked directly.

LEMMA 4.3 *If $F: \text{Alg}_{k'} \rightarrow \text{Set}$ is represented by a (finitely-presented) k -algebra, then so also is $(F)_{k'/k}$.*

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

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

⁸Given $F \rightarrow (F')_{k'/k}$, we need $F_{k'} \rightarrow F'$. Let R be a k' -algebra, and let R_0 be R regarded as a k -algebra. The given k -algebra map $k' \rightarrow R$ and the identity map $R_0 \rightarrow R$ define a map $k' \otimes_k R_0 \rightarrow R$ (of k' -algebras). Hence we have

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

and $F(R_0) = F_{k'}(R)$.

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

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

and so there is a bijection

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

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

$$a_i = \sum_{j=1}^d b_{ij} e_j, \quad i = 1, \dots, n. \quad (25)$$

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

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

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

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

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

when the a 's and b 's are related by (25). The polynomial g has coefficients in k' , but we can write it (uniquely) as a sum

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

Clearly,

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

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

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

We deduce the general case from the free case by applying Theorem 2.20. For any faithfully flat homomorphism $R \rightarrow R'$ of k -algebras, $R_{k'} \rightarrow R'_{k'}$ is a faithfully flat homomorphism of k' -algebras (CA 9.7), and so

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

is exact. But this equals

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

and so $(F)_{k'/k}$ satisfies the condition (*) of the theorem. According to (CA 10.4), there exist elements f_1, \dots, f_r of k such that $(f_1, \dots, f_r) = k$ and k'_{f_i} is a free k_{f_i} -module for each i . It follows that $((F)_{k'/k})_{k_{f_i}}$ is representable for each i , and so $(F)_{k'/k}$ is representable (cf. Example 2.21). \square

If G is a functor $\text{Alg}_{k'} \rightarrow \text{Grp}$, then $(G)_{k'/k}$ is a functor $\text{Alg}_k \rightarrow \text{Grp}$. The lemma shows that if G is an affine (algebraic) group, then so also is $(G)_{k'/k}$, and (24) shows that the functor $G' \rightsquigarrow (G')_{k'/k}$ is right adjoint to the functor “extension of scalars”:

$$\text{Hom}(G, (G')_{k'/k}) \simeq \text{Hom}(G_{k'}, G').$$

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

PROPERTIES OF THE RESTRICTION OF SCALARS FUNCTOR

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

$$\Pi_{k'/k} \circ \Pi_{k''/k'} \simeq \Pi_{k''/k}.$$

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

$$\begin{aligned} ((\Pi_{k'/k} \circ \Pi_{k''/k'}) (G)) (R) &= (\Pi_{k'/k} (\Pi_{k''/k'} G)) (R) \\ &= G(k'' \otimes_{k'} k' \otimes_k R) \\ &\simeq G(k'' \otimes_k R) \\ &= (\Pi_{k''/k} G) (R) \end{aligned}$$

because $k'' \otimes_{k'} k' \otimes_k R \simeq k'' \otimes_k R$.

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

$$(\Pi_{k'/k} G)_K \simeq \Pi_{k' \otimes_k K/K} (G_K); \quad (26)$$

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

$$(\Pi_{k'/k} G)_K (R) \stackrel{\text{def}}{=} G(k' \otimes_k R) \simeq G(k' \otimes_k K \otimes_K R) \stackrel{\text{def}}{=} \Pi_{k' \otimes_k K/K} (G_K) (R)$$

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

4.6 Let k' be a product of k -algebras, $k' = k_1 \times \cdots \times k_n$, with each k_i finitely generated and projective as a k -module. Let G be the affine group over k' corresponding to a family $(G_i)_i$ of affine groups over the k_i (see 3.13). Then

$$(G)_{k'/k} \simeq (G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}. \quad (27)$$

Indeed, for any k -algebra R ,

$$\begin{aligned} (G)_{k'/k} (R) &\stackrel{\text{def}}{=} G(k' \otimes R) \\ &= G_1(k_1 \otimes R) \times \cdots \times G_n(k_n \otimes R) \\ &\stackrel{\text{def}}{=} ((G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}) (R) \end{aligned}$$

because $k' \otimes R \simeq k_1 \otimes R \times \cdots \times k_n \otimes R$ and G is representable.

4.7 There is a homomorphism $i: G \rightarrow (\Pi_{k'/k}G)_{k'}$ of affine groups over k' such that, for all k' -algebras R , $i(R)$ is the map $G(R) \rightarrow G(k' \otimes R)$ defined by $a \mapsto 1 \otimes a: R \rightarrow k' \otimes R$. Then i is injective (obviously), and has the following universal property: let H be an affine group over k ; then any homomorphism $G \rightarrow H_{k'}$ (over k') factors uniquely through i .

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

$$(\Pi_{k'/k}G)_K \simeq \prod_{\alpha: k' \rightarrow K} G_\alpha$$

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

$$(\Pi_{k'/k}G)_K \stackrel{(26)}{\simeq} \Pi_{k' \otimes K/K} G_K \stackrel{(27)}{\simeq} \prod_{\alpha: k' \rightarrow K} G_\alpha$$

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

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

$$0 \rightarrow V_\alpha \rightarrow (G)_{k'/k} \rightarrow G \rightarrow 0$$

where V is the tangent space to G at 1, i.e., $V = \text{Ker}(G(k[\varepsilon]) \rightarrow G(k))$. This is proved in II, 1.29, below.

4.10 We saw in (4.8) that, when k' is a separable field extension of k , $(G)_{k'/k}$ becomes isomorphic to a product of copies of G over some field containing k' . This is far from true when k'/k is an inseparable field extension. For example, let k be a nonperfect field of characteristic 2, so that there exists a nonsquare a in k , and let $k' = k[\sqrt{a}]$. Then

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

According to (4.5),

$$(\Pi_{k'/k}G)_{k'} \simeq \Pi_{k'[\varepsilon]/k'} G_{k'},$$

which is an extension of $G_{k'}$ by a vector group (4.9).

4e Galois descent of affine groups

In this subsection, k is a field. Let Ω be a Galois extension of the field k , and let $\Gamma = \text{Gal}(\Omega/k)$. When Ω is an infinite extension of k , we endow Γ with the Krull topology. By an *action* of Γ on an Ω -vector space V we mean a homomorphism $\Gamma \rightarrow \text{Aut}_k(V)$ such that each $\sigma \in \Gamma$ acts σ -linearly, i.e., such that

$$\sigma(cv) = \sigma(c) \cdot \sigma(v) \text{ for all } \sigma \in \Gamma, c \in \Omega, \text{ and } v \in V.$$

We say that the action is continuous if every element of V is fixed by an open subgroup of Γ , i.e., if

$$V = \bigcup_{\Gamma'} V^{\Gamma'} \quad (\text{union over the open subgroups } \Gamma' \text{ of } \Gamma).$$

PROPOSITION 4.11 For any Ω -vector space V equipped with a continuous action of Γ , the map

$$\sum_i c_i \otimes v_i \mapsto \sum_i c_i v_i : \Omega \otimes_k V^\Gamma \rightarrow V$$

is an isomorphism.

PROOF. See Chapter VI, 1.2 below or AG, 16.15 (the proof is quite elementary). \square

For any vector space V over k , the group Γ acts continuously on $\Omega \otimes V$ according to rule:

$$\sigma(c \otimes v) = \sigma c \otimes v \text{ for all } \sigma \in \Gamma, c \in \Omega, \text{ and } v \in V.$$

PROPOSITION 4.12 The functor $V \rightsquigarrow \Omega \otimes_k V$ from vector spaces over k to vector spaces over Ω equipped with a continuous action of Γ is an equivalence of categories.

PROOF. When we choose bases for V and V' , then $\text{Hom}_{k\text{-lin}}(V, V')$ and $\text{Hom}_{\Omega\text{-lin}}(\Omega \otimes V, \Omega \otimes V')$ become identified with certain sets of matrices, and the full faithfulness of the functor follows from the fact that $\Omega^\Gamma = k$. That the functor is essentially surjective follows from (4.11). \square

Let G be an affine group over Ω . By a continuous action of Γ on G we mean a continuous action of Γ on $\mathcal{O}(G)$ preserving Δ and the k -algebra structure on A ; thus

$$\left. \begin{aligned} \sigma(f \cdot f') &= \sigma f \cdot \sigma f' \\ \sigma 1 &= 1 \\ (\sigma \otimes \sigma)(\Delta(f)) &= \Delta(\sigma f) \end{aligned} \right\} \text{ for all } \sigma \in \Gamma, f, f' \in A.$$

PROPOSITION 4.13 The functor $G \rightsquigarrow G_\Omega$ from affine groups over k to affine groups over Ω equipped with a continuous action of Γ is an equivalence of categories.

PROOF. Immediate consequence of Proposition 4.12. \square

EXAMPLE 4.14 Let k' be a finite separable field extension of k , and let Ω be a Galois extension of k containing all conjugates of k' . Let $G = (A, \Delta)$ be an affine group over k' , and let

$$G_* = (A_*, \Delta_*) \stackrel{\text{def}}{=} \prod_{\tau: k' \rightarrow \Omega} (\tau A, \tau \Delta)$$

where τ runs over the k -homomorphisms $k' \rightarrow \Omega$. There is an obvious continuous action of $\Gamma \stackrel{\text{def}}{=} \text{Gal}(\Omega/k)$ on G_* , and the corresponding affine group over k is $(G)_{k'/k}$. This is essentially the original construction of $(G)_{k'/k}$ in Weil 1960, 1.3.

4f The Greenberg functor

Let A be a local artinian ring with residue field k . For example, A could be the ring $W_m(k)$ of Witt vectors of length m . In general, A is a $W_m(k)$ -module for some m . For an affine group G over A , consider the functor $\mathcal{G}(G)$:

$$R \rightsquigarrow G(A \otimes_{W_m(k)} W_m(R)).$$

Then $\mathcal{G}(G)$ is an affine group over k . See Greenberg 1961, Greenberg 1963.

4g Exercises

EXERCISE 4-1 Let k' be a finite separable extension of a field k . Let \mathbb{A}^1 be the functor $\text{Alg}_k \rightarrow \text{Set}$ sending R to R , and let $U_i, i \in k$, be the subfunctor of \mathbb{A}^1 such that $U_i(R) = \{a \in R \mid a \neq i\}$. Show that $\mathbb{A}^1 = U_0 \cup U_1$ but $\Pi_{k'/k}\mathbb{A}^1 \neq (\Pi_{k'/k}U_0) \cup (\Pi_{k'/k}U_1)$ if $k' \neq k$.

EXERCISE 4-2 Let k'/k be a finite field extension. Let $\alpha: G_{k'} \rightarrow H$ be a homomorphism of algebraic groups over k' , and let $\beta: G \rightarrow \Pi_{k'/k}H$ be the corresponding homomorphism over k . Show that $\text{Ker}(\beta)$ is the unique affine subgroup of G such that $\text{Ker}(\beta)_{k'} = \text{Ker}(\alpha)$.

5 Affine groups and Hopf algebras

Un principe général: tout calcul relatif aux cogèbres est trivial et incompréhensible.

Serre 1993, p. 39.

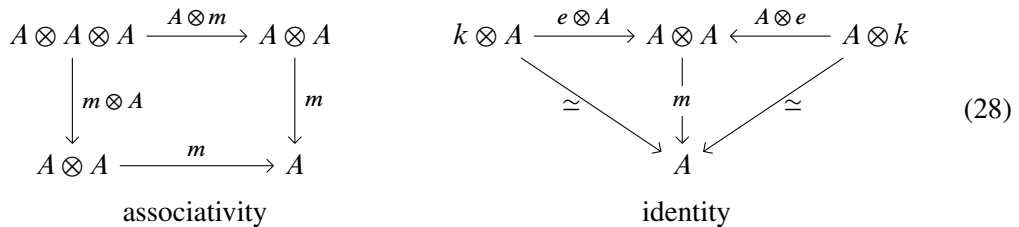
In this section, we examine the extra structure that the coordinate ring of an affine group G acquires from the group structure on G . Throughout k is a commutative ring.

5a Algebras

Recall that an associative algebra over k with identity is a module A over k together with a pair of k -linear maps⁹

$$m: A \otimes A \rightarrow A \quad e: k \rightarrow A$$

such that the following diagrams commute:



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

5b Coalgebras

DEFINITION 5.1 A *co-associative coalgebra* over k *with co-identity* (henceforth, a *coalgebra* over k) is a module C over k together with a pair of k -linear maps

$$\Delta: C \rightarrow C \otimes C \quad \epsilon: C \rightarrow k$$

⁹Warning: I sometimes also use “ e ” for the neutral element of $G(R)$ (a homomorphism $\mathcal{O}(G) \rightarrow R$).

such that the diagrams

$$\begin{array}{ccc}
 C \otimes C \otimes C & \xleftarrow{C \otimes \Delta} & C \otimes C \\
 \uparrow \Delta \otimes C & & \uparrow \Delta \\
 C \otimes C & \xleftarrow{\Delta} & C
 \end{array}
 \qquad
 \begin{array}{ccccc}
 k \otimes C & \xleftarrow{\epsilon \otimes C} & C \otimes C & \xrightarrow{C \otimes \epsilon} & C \otimes k \\
 & \searrow \simeq & \uparrow \Delta & \nearrow \simeq & \\
 & & C & &
 \end{array}
 \quad (29)$$

co-associativity co-identity

commute, i.e., such that

$$\begin{cases}
 (C \otimes \Delta) \circ \Delta = (\Delta \otimes C) \circ \Delta \\
 (C \otimes \epsilon) \circ \Delta = \text{id}_C = (\epsilon \otimes C) \circ \Delta.
 \end{cases}
 \quad (30)$$

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

$$\begin{array}{ccc}
 C \otimes C & \xrightarrow{f \otimes f} & D \otimes D \\
 \uparrow \Delta_C & & \uparrow \Delta_D \\
 C & \xrightarrow{f} & D
 \end{array}
 \qquad
 \begin{array}{ccc}
 C & \xrightarrow{f} & D \\
 \downarrow \epsilon_C & & \downarrow \epsilon_D \\
 k & \xlongequal{\quad} & k
 \end{array}
 \quad (31)$$

commute, i.e., such that

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

5.2 Let S be a set and let C be the k -vector space with basis S (so $C = 0$ if S is empty). Then C becomes a coalgebra over k with Δ and ϵ defined by

$$\left. \begin{aligned}
 \Delta(s) &= s \otimes s \\
 \epsilon(s) &= 1
 \end{aligned} \right\} \text{ all } s \in S.$$

This shows that every vector space admits the structure of a coalgebra.

5.3 Let (C, Δ, ϵ) be a coalgebra over k . A k -subspace 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.

5.4 Let $(C, \Delta_C, \epsilon_C)$ and $(D, \Delta_D, \epsilon_D)$ be coalgebras over k ; define $\Delta_{C \otimes D}$ to be the composite

$$C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes_k D \otimes D \xrightarrow{C \otimes t \otimes D} C \otimes D \otimes_k C \otimes D$$

where t is the **transposition map** $c \otimes d \mapsto d \otimes c$, and define $\epsilon_{C \otimes D}$ to be the composite

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

then $(C \otimes D, \Delta_{C \otimes D}, \epsilon_{C \otimes D})$ is a coalgebra over k . On taking $D = C$, we see that $C \otimes C$ is a coalgebra over k .

5c 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

$$V^\vee \otimes W^\vee \rightarrow (V \otimes W)^\vee \quad (32)$$

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

If (C, Δ, ϵ) is a co-associative coalgebra over k with a co-identity, then C^\vee becomes an associative algebra over k with the multiplication $C^\vee \otimes C^\vee \hookrightarrow (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee$ and the identity $k \simeq k^\vee \xrightarrow{\epsilon^\vee} C^\vee$. Similarly, if (A, m, e) is an associative algebra over k with an identity and A is *finitely generated and projective* as a k -module, then A^\vee becomes a co-associative coalgebra over k with the co-multiplication $A^\vee \xrightarrow{m^\vee} (A \otimes A)^\vee \simeq A^\vee \otimes A^\vee$ 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 (28) or (29).

EXAMPLE 5.5 Let X be a set, and let C be the free k -module with basis X . The k -linear maps

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

endow C with the structure of coalgebra over k . The dual algebra C^\vee can be identified with the k -module of maps $X \rightarrow k$ endowed with the k -algebra structure

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

5d Bi-algebras

For k -algebras A and B , $A \otimes B$ becomes a k -algebra with the maps

$$\begin{aligned} m_{A \otimes B}((a \otimes b) \otimes (a' \otimes b')) &= m_A(a \otimes a') \otimes m_B(b \otimes b') \\ e_{A \otimes B}(c) &= e_A(c) \otimes 1 = 1 \otimes e_B(c). \end{aligned}$$

DEFINITION 5.6 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) $\Delta: A \rightarrow A \otimes A$ is a homomorphism of algebras;
- (d) $\epsilon: A \rightarrow k$ is a homomorphism of algebras.

A **homomorphism** of bi-algebras $(A, m, \dots) \rightarrow (A', m', \dots)$ is a k -linear map $A \rightarrow A'$ 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 5.7 For a quintuple $(A, m, e, \Delta, \epsilon)$ satisfying (a) and (b) of (5.6), the following conditions are equivalent:

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

PROOF Consider the diagrams:

$$\begin{array}{ccccc}
 A \otimes A & \xrightarrow{m} & A & \xrightarrow{\Delta} & A \otimes A \\
 \downarrow \Delta \otimes \Delta & & & & \uparrow m \otimes m \\
 A \otimes A \otimes A \otimes A & \xrightarrow{A \otimes t \otimes A} & A \otimes A \otimes A \otimes A & &
 \end{array}$$

$$\begin{array}{ccc}
 A \otimes A & \xleftarrow{\Delta} & A \\
 \uparrow e \otimes e & & \uparrow e \\
 k \otimes k & \xleftarrow{\cong} & k
 \end{array}
 \quad
 \begin{array}{ccc}
 A \otimes A & \xrightarrow{m} & A \\
 \downarrow \epsilon \otimes \epsilon & & \downarrow \epsilon \\
 k \otimes k & \xrightarrow{\cong} & k
 \end{array}
 \quad
 \begin{array}{ccc}
 & A & \\
 e \nearrow & & \searrow \epsilon \\
 k & \xrightarrow{\text{id}} & k
 \end{array}$$

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. \square

DEFINITION 5.8 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 5.9 An *inversion* (or *antipodal map*¹⁰) for a bi-algebra A is a k -linear map $S: A \rightarrow A$ such that

- (a) the diagram

$$\begin{array}{ccccc}
 A & \xleftarrow{m \circ (S \otimes \text{id})} & A \otimes A & \xrightarrow{m \circ (\text{id} \otimes S)} & A \\
 \uparrow e & & \uparrow \Delta & & \uparrow e \\
 k & \xleftarrow{\epsilon} & A & \xrightarrow{\epsilon} & k
 \end{array} \tag{33}$$

commutes, i.e.,

$$m \circ (S \otimes \text{id}) \circ \Delta = e \circ \epsilon = m \circ (\text{id} \otimes S) \circ \Delta. \tag{34}$$

and

- (b) $S(ab) = S(ba)$ for all $a, b \in A$ and $S(1) = 1$ (so S is a k -algebra homomorphism when A is commutative).

¹⁰Usually shortened to “antipode”.

ASIDE 5.10 In fact, condition (a) implies condition (b) (Dăscălescu et al. 2001, 4.2.6).

EXAMPLE 5.11 Let X be a monoid, and let A be the k -module with basis X . The k -linear maps

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

endow A with the structure of a k -algebra. When combined with the coalgebra structure in (5.5), this makes A into a bi-algebra over k . When X is a group, the map

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

is an inversion.

PROPOSITION 5.12 Let A and A' be bi-algebras over k . If A and A' admit inversions S and S' , then, for any homomorphism $f: A \rightarrow A'$,

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

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 (5.16) below. The general case is proved in Dăscălescu et al. 2001, 4.2.5. \square

DEFINITION 5.13 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.

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 5-1 below before continuing.

ASIDE 5.14 To give a k -bialgebra that is finitely generated and projective as a k -module is the same as giving a pair of finitely generated projective k -algebras A and B together with a nondegenerate k -bilinear pairing

$$\langle \cdot, \cdot \rangle: B \times A \rightarrow k$$

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

5e 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 5.15 (a) Let A be a k -algebra, and let $\Delta: A \rightarrow A \otimes A$ and $\epsilon: A \rightarrow k$ be homomorphisms. The triple (A, Δ, ϵ) 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 $\Delta: A \rightarrow A \otimes A$ be a homomorphism. The pair (A, Δ) is an affine group if and only if there exists a homomorphism $\epsilon: A \rightarrow k$ such that (A, Δ, ϵ) is a Hopf algebra.

PROOF. (a) Let $M = h^A$, and let $m: M \times M \rightarrow M$ and $e: * \rightarrow M$ be the natural transformations defined by Δ and ϵ (here $*$ is the trivial monoid represented by k). Then m and e define a monoid structure on $M(R)$ for each k -algebra R if and only if the diagrams

$$\begin{array}{ccc}
 M \times M \times M & \xrightarrow{\text{id}_M \times m} & M \times M \\
 \downarrow m \times \text{id}_M & & \downarrow m \\
 M \times M & \xrightarrow{m} & M
 \end{array}
 \qquad
 \begin{array}{ccccc}
 * \times M & \xrightarrow{e \times \text{id}_M} & M \times M & \xleftarrow{\text{id}_M \times e} & M \times * \\
 \searrow \simeq & & \downarrow m & & \swarrow \simeq \\
 & & M & &
 \end{array}
 \tag{35}$$

commute. As $A \rightsquigarrow h^A$ sends tensor products to products (10, p. 10), the Yoneda lemma, shows that these diagrams commute if and only if the diagrams (29) commute.

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

$$\begin{array}{ccccc}
 M & \xrightarrow{(\text{inv}, \text{id})} & M \times M & \xleftarrow{(\text{id}, \text{inv})} & M \\
 \downarrow & & \downarrow m & & \downarrow \\
 * & \xrightarrow{e} & M & \xleftarrow{e} & *
 \end{array}
 \tag{36}$$

commutes. Here (id, inv) denotes the morphism whose composites with the projection maps are id and inv . Such a natural transformation corresponds to a k -algebra homomorphism $S: A \rightarrow A$ satisfying (34), i.e., to an inversion for A . \square

Thus, as promised in (2.12), we have shown that a pair (A, Δ) is an affine group if and only if there exist homomorphisms ϵ and S making certain diagrams commute.

PROPOSITION 5.16 *Let A and A' be commutative Hopf algebras over k . A k -algebra homomorphism $f: A \rightarrow A'$ is a homomorphism of Hopf algebras if*

$$(f \otimes f) \circ \Delta = \Delta' \circ f; \tag{37}$$

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

PROOF. According to (5.15b), $G = (A, \Delta)$ and $G' = (A', \Delta')$ are affine groups. A k -algebra homomorphism $f: A \rightarrow A'$ defines a morphism of functors $h^f: G \rightarrow G'$. If (37) 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 $g \mapsto g^{-1}$, $f \circ S = S' \circ f$. \square

COROLLARY 5.17 *For any commutative k -algebra A and homomorphism $\Delta: A \rightarrow A \otimes A$, 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 (5.16) to the identity map. \square

THEOREM 5.18 *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 affine groups over k .*

PROOF. It follows from (5.15b) and (5.17) that the functor is bijective on objects, and it is obviously bijective on morphisms. \square

EXAMPLE 5.19 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 of G into GL_3 . Note that the functor $R \rightsquigarrow R \times R \times R$ also has an obvious commutative group structure (componentwise addition), which shows that the k -algebra $k[X, Y, Z]$ has more than one Hopf algebra structure.

5f Abstract restatement

Let \mathbf{C} be a category with finite products and, in particular, a final object $*$ (the product over the empty set). A **monoid object** in \mathbf{C} is an object M together with morphisms $m: M \times M \rightarrow M$ and $e: * \rightarrow M$ such that the diagrams (35) commute. A **morphism** of monoid objects is a morphism of the objects compatible with the maps m and e .

Let \mathbf{A} be a category, and let \mathbf{A}^\vee be the category of functors $\mathbf{A} \rightarrow \mathbf{Set}$. For any finite family $(F_i)_{i \in I}$ of functors, the functor $A \rightsquigarrow \prod_{i \in I} F_i(A)$ is the product of the F_i , and so \mathbf{A}^\vee has finite products. To give the structure of a monoid object on a functor $M: \mathbf{A} \rightarrow \mathbf{Set}$ is the same as giving a factorization of M through \mathbf{Mon} .

Now assume that \mathbf{A} has finite direct sums. It follows from the definitions of direct sums and products, that the functor $A \rightsquigarrow h^A$ sends direct sums to direct products. According to the Yoneda lemma (2.1), $A \rightsquigarrow h^A: \mathbf{A}^{\mathrm{opp}} \rightarrow \mathbf{A}^\vee$ is fully faithful. Its essential image is (by definition) the subcategory of representable functors. Therefore $A \rightsquigarrow h^A$ is an equivalence from the category of monoid objects in $\mathbf{A}^{\mathrm{opp}}$ to the category of monoid objects in \mathbf{A}^\vee whose underlying functor to sets is representable (equivalently, to the category of functors $\mathbf{A} \rightarrow \mathbf{Mon}$ whose underlying functor to sets is representable).

Now take $\mathbf{A} = \mathbf{Alg}_k$. Tensor products in this category are direct sums (in the sense of category theory), and so the above remarks show that $A \rightsquigarrow h^A$ is an equivalence from the category of monoid objects in $\mathbf{Alg}_k^{\mathrm{opp}}$ to the category of affine monoids over k . On comparing the diagrams (29) and (35), we see that a monoid object in $\mathbf{Alg}_k^{\mathrm{opp}}$ is just a commutative bi-algebra.

Similarly, a **group object** in a category \mathbf{C} with finite products is defined to be an object M together with morphisms $m: M \times M \rightarrow M$, $e: * \rightarrow M$, and $\mathrm{inv}: M \rightarrow M$ such that the diagrams (35) and (36) commute.¹¹ The same arguments as above show that $A \rightsquigarrow h^A$ is an equivalence from the category of group objects in $\mathbf{Alg}_k^{\mathrm{opp}}$ to the category of affine groups over k . Moreover, a group object in $\mathbf{Alg}_k^{\mathrm{opp}}$ is just a commutative bi-algebra with an inversion.

¹¹For any object T of \mathbf{C} , the maps m , e , and inv define a group structure on $\mathrm{Hom}(T, M)$. The Yoneda lemma shows that inv is uniquely determined by m and e . Thus, one can also define a group object to be a monoid object for which there exists a morphism inv such that the diagram (36) commutes.

In summary: the functor $A \rightsquigarrow h^A$ defines an equivalence from the category of commutative bi-algebras (resp. commutative Hopf algebras) to the category of affine monoids (resp. groups). Under the equivalence, finitely presented bi-algebras (resp. Hopf algebras) correspond to algebraic monoids (resp. groups).

5g Explicit description of Δ , ϵ , and S

Let G be an affine group over k . Recall (2.16) that an element f of the coordinate ring $\mathcal{O}(G)$ is a family of functions $f_R: G(R) \rightarrow R$ of sets compatible with homomorphisms of k -algebras. An element $f_1 \otimes f_2$ of $\mathcal{O}(G) \otimes \mathcal{O}(G)$ defines a function $(f_1 \otimes f_2)_R: G(R) \times G(R) \rightarrow R$ by the rule:

$$(f_1 \otimes f_2)_R(a, b) = (f_1)_R(a) \cdot (f_2)_R(b).$$

In this way, $\mathcal{O}(G) \otimes \mathcal{O}(G)$ becomes identified with the coordinate ring of $G \times G$.

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

$$(\Delta f)_R(a, b) = f_R(ab), \quad \text{for all } R \text{ and all } a, b \in G(R). \quad (38)$$

Moreover,

$$\epsilon f = f(1) \text{ (constant function)}, \quad (39)$$

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

$$(Sf)_R(a) = f_R(a^{-1}), \quad \text{for all } R \text{ and all } a \in G(R). \quad (40)$$

EXAMPLE 5.20 Recall (3.1) that \mathbb{G}_a has coordinate ring $k[X]$ 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 $G(R) \times G(R)$. As $(\Delta f)_R(a, b) = f_R(a + b)$ (see (38)), we find that

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

in other words, Δ is the homomorphism of k -algebras $k[X] \rightarrow k[X] \otimes k[X]$ sending X to $X \otimes 1 + 1 \otimes X$. Moreover,

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

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

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

EXAMPLE 5.21 For $G = \mathbb{G}_m$, $\mathcal{O}(G) = k[X, X^{-1}]$, Δ is the homomorphism of k -algebras $k[X, X^{-1}] \rightarrow k[X, X^{-1}] \otimes k[X, X^{-1}]$ sending X to $X \otimes X$, ϵ is the homomorphism $k[X, X^{-1}] \rightarrow k$ sending $f(X, X^{-1})$ to $f(1, 1)$, and S is the homomorphism $k[X, X^{-1}] \rightarrow k[X, X^{-1}]$ sending X to X^{-1} .

EXAMPLE 5.22 For $G = \text{GL}_n$,

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

and

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

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

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

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

$$\begin{aligned} (\Delta x_{ik})_R((a_{ij}), (b_{ij})) &= (x_{ik})_R((a_{ij})(b_{ij})) && \text{definition (38)} \\ &= \sum_j a_{ij} b_{jk} && \text{as } (x_{kl})_R((c_{ij})) = c_{kl} \\ &= (\sum_{j=1, \dots, n} x_{ij} \otimes x_{jk})_R((a_{ij}), (b_{ij})) && \text{as claimed.} \end{aligned}$$

EXAMPLE 5.23 Let F be a finite group, and let A be the set of maps $F \rightarrow k$ with its natural k -algebra structure. Then A is a product of copies of k indexed by the elements of F . More precisely, let e_σ be the function that is 1 on σ and 0 on the remaining elements of F . The e_σ 's are 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 . Let $(F)_k$ be the associated algebraic group, so that

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

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

5h Commutative affine groups

A monoid or group G (resp. an algebra A) is commutative if and only if the diagram at left (resp. the middle diagram) commutes, and a coalgebra or bi-algebra C is said to be **co-commutative** if the diagram at right commutes:

$$\begin{array}{ccc} G \times G & \xrightarrow{t} & G \times G \\ & \searrow m & \swarrow m \\ & & G \end{array} \quad \begin{array}{ccc} A \otimes A & \xrightarrow{t} & A \otimes A \\ & \searrow m & \swarrow m \\ & & A \end{array} \quad \begin{array}{ccc} C \otimes C & \xleftarrow{t} & C \otimes C \\ & \swarrow \Delta & \searrow \Delta \\ & & C \end{array} \tag{41}$$

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.

5i Finite flat algebraic groups; Cartier duality

If $(A, m, e, \Delta, \epsilon)$ is a bi-algebra over k and A is finitely generated and projective as a k -module, then $(A^\vee, \Delta^\vee, \epsilon^\vee, m^\vee, e^\vee)$ is also a k -bialgebra (see §5c and Proposition 5.7). If moreover $(A, m, e, \Delta, \epsilon)$ is commutative (resp. co-commutative), then $(A^\vee, \Delta^\vee, \epsilon^\vee, m^\vee, e^\vee)$ is co-commutative (resp. commutative).

An algebraic group G over k is said to be *finite* (resp. *flat*) if the k -algebra $\mathcal{O}(G)$ is a finite (resp. flat). Thus G is finite and flat if and only if $\mathcal{O}(G)$ is finitely generated and projective as a k -module (CA The coordinate ring $\mathcal{O}(G)$ of a commutative finite flat algebraic monoid is a commutative co-commutative bi-algebra, and so its dual $\mathcal{O}(G)^\vee$ is the coordinate ring of a commutative finite flat algebraic monoid G^\vee , called the *Cartier dual* of G . If $\mathcal{O}(G)$ admits an inversion S , then S^\vee is an algebra homomorphism, and so G^\vee is an algebraic group. To check that S^\vee is an algebra homomorphism, we have to check that $\Delta^\vee \circ (S^\vee \otimes S^\vee) = S^\vee \circ \Delta^\vee$, or, equivalently, that $\Delta \circ S = (S \otimes S) \circ \Delta$. In other words, we have check the diagram at left below commutes. This corresponds (under a category equivalence) to the diagram at right, which commutes precisely because G is commutative (the inverse of a product is the product of the inverses):

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{\Delta} & \mathcal{O}(G) \otimes \mathcal{O}(G) & & G & \xleftarrow{m} & G \times G \\ \downarrow S & & \downarrow S \otimes S & & \uparrow_{\text{inv}} & & \uparrow_{\text{inv} \times \text{inv}} \\ \mathcal{O}(G) & \xrightarrow{\Delta} & \mathcal{O}(G) \otimes \mathcal{O}(G) & & G & \xleftarrow{m} & G \times G. \end{array}$$

Note that $G^{\vee\vee} \simeq G$.

5j 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

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

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 $q \rightarrow 1$. 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 section 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).

5k 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.¹²

5l Exercises

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

EXERCISE 5-1 For a set X , let $R(X)$ be the k -algebra of maps $X \rightarrow k$. 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 $R(X) \otimes R(Y) \rightarrow R(X \times Y)$ 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

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

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 $R(\Gamma) \otimes R(\Gamma)$.

EXERCISE 5-2 We continue the notations of the last exercise. Let Γ be an arbitrary group. From a homomorphism $\rho: \Gamma \rightarrow \mathrm{GL}_n(k)$, we obtain a family of functions $g \mapsto \rho(g)_{i,j}$, $1 \leq i, j \leq n$, 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 5-3 Let G be the constant algebraic group over k defined by a finite commutative group Γ . Let n be the exponent of Γ , and assume that k contains n distinct n th roots of 1 (so, in particular, n is not divisible by the characteristic of k). Show that the Cartier dual of G is the constant algebraic group defined by the dual group $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$.

¹²In 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 5-4 If k has characteristic $p \neq 0$, show that $\alpha_p^\vee \simeq \alpha_p$ and $(\mathbb{Z}/p\mathbb{Z})_k^\vee \simeq \mu_p$ (hence $\mu_p^\vee \simeq (\mathbb{Z}/p\mathbb{Z})_k$) (here $(\mathbb{Z}/p\mathbb{Z})_k$, μ_p , and α_p are the groups in (3.3), (3.4), and (3.5)).

EXERCISE 5-5 Let A be a Hopf algebra. Prove the following statements by interpreting them as statements about affine groups.

- (a) $S \circ S = \text{id}_A$.
- (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 $a \otimes b \mapsto (a \otimes 1)\Delta(b): A \otimes A \rightarrow A \otimes A$ is a homomorphism of k -algebras.

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

EXERCISE 5-6 Show that there is no algebraic group G over k such that $G(R)$ has two elements for every k -algebra R .

EXERCISE 5-7 Verify directly that $\mathcal{O}(\mathbb{G}_a)$ and $\mathcal{O}(\mathbb{G}_m)$ satisfy the axioms to be a Hopf algebra.

EXERCISE 5-8 Verify all the statements in 5.23.

EXERCISE 5-9 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 $C \rightarrow C/V$ is a homomorphism. Show that any homomorphism of k -coalgebras $C \rightarrow D$ whose kernel contains V factors uniquely through $C \rightarrow C/V$.
- (c) Deduce that every homomorphism $f: C \rightarrow D$ of coalgebras induces an isomorphism of k -coalgebras

$$C/\text{Ker}(f) \rightarrow \text{Im}(f).$$

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

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

EXERCISE 5-10 (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 $A \rightarrow A/\mathfrak{a}$ is a homomorphism. Show that any homomorphism of k -bialgebras $A \rightarrow B$ whose kernel contains \mathfrak{a} factors uniquely through $A \rightarrow A/\mathfrak{a}$. 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 $f: A \rightarrow B$ of bialgebras (resp. Hopf algebras) induces an isomorphism of bialgebras (resp. Hopf algebras),

$$A/\text{Ker}(f) \rightarrow \text{Im}(f).$$

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 (5.15).

6 Affine groups and affine group schemes

In the last section, we saw that affine groups over k correspond to group objects in the opposite of the category of k -algebras (see §5f). In this section we interpret this opposite category as the category of affine schemes over k . Thus algebraic groups over k correspond to group objects in the category of affine schemes over k . When k is a field, we use this geometric interpretation to obtain additional insights.

In the first three subsections, k is a commutative ring, but starting in §6d we require it to be a field.

6a Affine schemes

Let A be commutative ring, and let V be the set of prime ideals in A . The *principal open subsets* of V are the sets of the form

$$D(f) = \{\mathfrak{p} \in V \mid f \notin \mathfrak{p}\}, \quad f \in A.$$

They form a base for a topology on V whose closed sets are exactly the sets

$$V(\mathfrak{a}) = \{\mathfrak{p} \in V \mid \mathfrak{p} \supset \mathfrak{a}\}, \quad \mathfrak{a} \text{ an ideal in } A.$$

This is the *Zariski topology*, and the set V endowed with the Zariski topology is the (*prime spectrum*) $\text{spec}(A)$ of A .

Let $\varphi: A \rightarrow B$ be a homomorphism 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

$$\text{spec}(\varphi): \text{spec } B \rightarrow \text{spec } A, \quad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}),$$

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.

Let A be a commutative ring. Let $V = \text{spec } A$, and let \mathcal{B} be the set of principal open subsets. Then \mathcal{B} is closed under finite intersections because

$$D(f_1 \cdots f_r) = D(f_1) \cap \cdots \cap D(f_r).$$

For a principal open subset D of V , define $\mathcal{O}_A(D) = S_D^{-1}A$ where S_D is the multiplicative subset $A \setminus \bigcup_{\mathfrak{p} \in D} \mathfrak{p}$ of A . If $D = D(f)$, then S_D is the smallest saturated multiplicative subset of A containing f , and so $\mathcal{O}_A(D) \simeq A_f$ (see CA 6.12). If $D \supset D'$, then $S_D \subset S_{D'}$, and so there is a canonical “restriction” homomorphism $\mathcal{O}_A(D) \rightarrow \mathcal{O}_A(D')$. These restriction maps make $D \rightsquigarrow \mathcal{O}_A(D)$ into a functor on \mathcal{B} satisfying the sheaf condition: for any covering $D = \bigcup_{i \in I} D_i$ of a principal open subset D by principal open subsets D_i , the sequence

$$\mathcal{O}_A(D) \rightarrow \prod_{i \in I} \mathcal{O}_A(D_i) \rightrightarrows \prod_{(i,j) \in I \times I} \mathcal{O}_A(D_i \cap D_j)$$

is exact.¹³ For an open subset U of V , define $\mathcal{O}_A(U)$ by the exactness of

$$\mathcal{O}_A(U) \rightarrow \prod_{D \in I} \mathcal{O}_A(D) \rightrightarrows \prod_{(D,D') \in I \times I} \mathcal{O}_A(D \cap D') \quad (42)$$

where $I = \{D \in \mathcal{B} \mid D \subset U\}$. Clearly, $U \rightsquigarrow \mathcal{O}_A(U)$ is a functor on the open subsets of V , and it is not difficult to check that it is a sheaf. The set I in (42) can be replaced by any subset of \mathcal{B} covering U without changing $\mathcal{O}_A(U)$. In particular, if $U = D(f)$, then

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

Therefore, the stalk of \mathcal{O}_A at a point $\mathfrak{p} \in V$ is

$$\mathcal{O}_{\mathfrak{p}} \stackrel{\text{def}}{=} \lim_{\rightarrow U \ni \mathfrak{p}} \mathcal{O}_A(U) = \lim_{\rightarrow f \notin \mathfrak{p}} \mathcal{O}_A(D(f)) \simeq \lim_{\rightarrow f \notin \mathfrak{p}} A_f \simeq A_{\mathfrak{p}}$$

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

Thus from A we get a locally ringed space $\text{Spec}(A) = (\text{spec } A, \mathcal{O}_A)$. An *affine scheme* (V, \mathcal{O}_V) is a ringed space isomorphic to $\text{Spec}(A)$ for some commutative ring A . A *morphism* of affine schemes is 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. A homomorphism $A \rightarrow B$ defines a morphism $\text{Spec } B \rightarrow \text{Spec } A$ of affine schemes.

PROPOSITION 6.1 *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. Straightforward. □

We often write V for (V, \mathcal{O}) , and we call $\mathcal{O}(V)$ 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 $\mathcal{O}(V)$.

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

6b Affine groups as affine group schemes

We now fix commutative ring k . An *affine scheme over k* (or an *affine k -scheme*) is an affine scheme V together with a morphism $V \rightarrow \text{Spec } k$. As a k -algebra is a commutative ring together with a homomorphism $k \rightarrow A$, we see that Spec defines a contravariant equivalence from the category of k -algebras to the category of affine k -schemes. For any finite

¹³Recall that this means that the first arrow is the equalizer of the pair of arrows.

family $(A_i)_{i \in I}$ of k -algebras, $\bigotimes_{i \in I} A_i$ is the direct sum of the A_i in the category of k -algebras, and so $\text{Spec}(\bigotimes_{i \in I} A_i)$ is the direct product¹⁴ of the affine k -schemes $\text{Spec}(A_i)$. It follows that finite products exist in the category of affine k -schemes, and so we can define an **affine group scheme over k** to be a group object in this category (see 2.5).

THEOREM 6.2 *The functor Spec defines an equivalence from the category of affine groups over k to the category of affine group schemes over k .*

PROOF. The functor Spec sends a k -algebra A equipped with a homomorphism $\Delta: A \rightarrow A \otimes A$ to an affine k -scheme V equipped with a morphism $m: V \times V \rightarrow V$. The pair (A, Δ) is an affine group if and only if there exist homomorphisms k -algebra $\epsilon: A \rightarrow k$ and $S: A \rightarrow A$ such that the diagrams (29) and (33) commute (see 5.15). But such a pair (ϵ, S) gives rise to morphisms $e: * \rightarrow V$ and $\text{inv}: V \rightarrow V$ such that the diagrams (35) and (36) commute (and conversely).

[Alternatively, the functor Spec maps a pair (A, Δ) , $\Delta: A \rightarrow A \otimes A$, to a pair (V, m) , $m: V \times V \rightarrow V$. As $h^A(B) = (\text{Spec } A)(\text{Spec } B)$, we see that Δ defines a group structure on $h^A(B)$ for all k -algebras B if and only if m defines a group structure on $V(T)$ for all affine k -schemes T . Therefore (A, Δ) is an affine group over k if and only if (V, m) is a group object in the category of affine schemes over k .] \square

We have constructed a realization of the category $(\text{Alg}_k)^{\text{opp}}$, and hence a realization of affine k -groups as groups in a category. This construction has two main applications.

- (a) A **scheme** is defined to be a locally ringed space that admits an open covering by affine schemes, and a **scheme V over k** is a scheme together with a morphism $V \rightarrow \text{Spec } k$. A **group scheme over k** is a group object in the category of schemes over k . Therefore, our construction embeds the category of affine groups over k into the much larger category of group schemes over k . This is important, but will not be pursued here. The interested reader is referred to SGA3.
- (b) When k is a field, the affine scheme attached to an affine algebraic group can be regarded as a variety over k (perhaps with nilpotents in the structure sheaf). This gives us a geometric interpretation of the algebraic group, to which we can apply algebraic geometry. This we explain in the remainder of this section.

6c The topology of an affine scheme

6.3 A topological space V is **noetherian** if every ascending chain of open subsets $U_1 \subset U_2 \subset \dots$ 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 exactly one that is irredundant in the sense that no subset in I contains a second (CA 12.10). The elements of this I are called the **irreducible components** of V .

¹⁴Fibred product over $\text{Spec } k$ in the category of all schemes.

6.4 When A is a noetherian ring, every descending chain of closed subsets in $\text{spec}(A)$ eventually becomes constant, and so $\text{spec}(A)$ is noetherian. Moreover, the map $\mathfrak{a} \mapsto V(\mathfrak{a})$ defines one-to-one correspondences

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

The ideal corresponding to a closed set W is $I(W) = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in W\}$. The nilradical \mathfrak{N} of A is the smallest radical ideal, and so it corresponds to the whole space $\text{spec}(A)$. Therefore $\text{spec}(A)$ is irreducible if and only if \mathfrak{N} is prime.

For the remainder of this section, we assume that k is a field.

6d Affine k -algebras

An **affine k -algebra** is a finitely generated k -algebra A such that $k^{\text{al}} \otimes_k A$ is reduced. If A is affine, then $K \otimes_k A$ is reduced for all fields K containing k ; in particular, A itself is reduced (CA 18.3). When k is perfect, every reduced finitely generated k -algebra is an affine k -algebra (CA 18.1). The tensor product of two affine k -algebras is again an affine k -algebra (CA 18.4).

6e Schemes algebraic over a field

Let k be a field, and let V be an affine k -scheme. When $\mathcal{O}_V(V)$ is a finitely generated k -algebra (resp. an affine k -algebra), V is called an **affine algebraic scheme** over k (resp. an **affine algebraic variety** over k).

For schemes algebraic over a field it is convenient to ignore the nonclosed points and work only with the closed points. What makes this possible is that, for any homomorphism $\varphi: A \rightarrow B$ of algebras finitely generated over a field, Zariski's lemma shows that the pre-image of a maximal ideal in B is a maximal ideal in A .¹⁵

For a finitely generated k -algebra A , define $\text{spm}(A)$ to be the set of maximal ideals in A endowed with the topology for which the closed sets are those of the form

$$V(\mathfrak{a}) \stackrel{\text{def}}{=} \{\mathfrak{m} \text{ maximal} \mid \mathfrak{m} \supset \mathfrak{a}\}, \quad \mathfrak{a} \text{ an ideal in } A.$$

The inclusion map $\text{spm}(A) \hookrightarrow \text{spec}(A)$ identifies $\text{spm}(A)$ with the set of closed points of $\text{spec}(A)$, and the map $S \mapsto S \cap \text{spm}(A)$ is a bijection from the open (resp. closed) subsets of $\text{spec}(A)$ onto the open (resp. closed) subsets of $\text{spm}(A)$. As noted, Zariski's lemma shows that spm is a contravariant functor from the category of finitely generated k -algebras to topological spaces. On $V = \text{spm}(A)$ there is a sheaf \mathcal{O}_V such that $\mathcal{O}_V(D(f)) \simeq A_f$ for

¹⁵Recall (CA 11.1) that Zariski's lemma says that a field K that is finitely generated as an algebra over a subfield k is, in fact, finitely generated as a vector space over k . Let $\varphi: A \rightarrow B$ be a homomorphism of finitely generated k -algebras. For any maximal ideal \mathfrak{m} in B , B/\mathfrak{m} is a field, which Zariski's lemma shows to be finite over k . Therefore the image of A in B/\mathfrak{m} is finite over k . As it is an integral domain, this implies that it is a field, and so $\varphi^{-1}(\mathfrak{m})$ is a maximal ideal.

all $f \in A$. It can be defined the same way as for $\text{spec}(A)$, or as the restriction to $\text{spm}(A)$ of the sheaf on $\text{spec}(A)$. When working with affine algebraic schemes (or varieties), implicitly we use max specs. In other words, all points are closed.

When k is algebraically closed, the definition of an affine algebraic variety over k that we arrive at is essentially the same as that in AG, Chapter 3 — see the next example.

EXAMPLE 6.5 Let k be an algebraically closed field, and endow k^n with the topology for which the closed sets are the zero-sets of families of polynomials. Let V be a closed subset of k^n , let \mathfrak{a} be the set of polynomials that are zero on V , and let

$$k[V] = k[X_1, \dots, X_n]/\mathfrak{a} = k[x_1, \dots, x_n].$$

A pair of elements $g, h \in k[V]$ with $h \neq 0$ defines a function

$$P \mapsto \frac{g(P)}{h(P)}: D(h) \rightarrow k$$

on the open subset $D(h)$ of V where h is nonzero. A function $f: U \rightarrow k$ on an open subset U of V is said to be **regular** if it is of this form in a neighbourhood of each point of U . Let $\mathcal{O}(U)$ be the set of regular functions on U . Then $U \rightsquigarrow \mathcal{O}(U)$ is a sheaf of k -algebras on V , and (V, \mathcal{O}) is an affine algebraic scheme over k with $\mathcal{O}(V) = k[V]$. See AG 3.4 — the map

$$(a_1, \dots, a_n) \mapsto (x_1 - a_1, \dots, x_n - a_n): V \rightarrow \text{spm}(k[V])$$

is a bijection because of the Nullstellensatz. When $V = k^n$, the scheme (V, \mathcal{O}) is **affine n -space** \mathbb{A}^n .

EXAMPLE 6.6 Let k be an algebraically closed field. The affine algebraic scheme $\text{Spm}(k[X, Y]/(Y))$ can be identified with the scheme attached to the closed subset $Y = 0$ of $k \times k$ in (6.5). Now consider $\text{Spm}(k[X, Y]/(Y^2))$. This has the same underlying topological space as before (namely, the x -axis in $k \times k$), but it should now be thought of as having multiplicity 2, or as being a line thickened in another dimension.

6.7 Let K be a field containing k . An affine algebraic scheme V over k defines an affine algebraic scheme V_K over K with $\mathcal{O}(V_K) = K \otimes_k \mathcal{O}(V)$.

6.8 An affine algebraic scheme V over a field k is said to be **reduced** if $\mathcal{O}(V)$ is reduced, and it is said to be **geometrically reduced** if $V_{k^{\text{al}}}$ is reduced. Thus V is geometrically reduced if and only if $\mathcal{O}(V)$ is an affine k -algebra, and so a “geometrically reduced affine algebraic scheme” is another name for an “affine algebraic variety”. Let \mathfrak{N} be the nilradical of $\mathcal{O}(V)$. Then

$$\begin{aligned} V \text{ is reduced} &\iff \mathfrak{N} = 0; \\ V \text{ is irreducible} &\iff \mathfrak{N} \text{ is prime}; \\ V \text{ is reduced and irreducible} &\iff \mathcal{O}(V) \text{ is an integral domain.} \end{aligned}$$

The first statement follows from the definitions, the second statement has already been noted (p. 56), and the third statement follows from the first two.

6.9 Recall (CA 3.12) that the **height** $\text{ht}(\mathfrak{p})$ of a prime ideal \mathfrak{p} in a noetherian ring A is the greatest length d of a chain of distinct prime ideals

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_d,$$

and that the **Krull dimension** of A is

$$\sup\{\text{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \text{spm}(A)\}.$$

6.10 The **dimension** of an affine algebraic scheme V is the Krull dimension of $\mathcal{O}(V)$ — this is finite (CA 13.11). When V is irreducible, the nilradical \mathfrak{N} of $\mathcal{O}(V)$ is prime, and so $\mathcal{O}(V)/\mathfrak{N}$ is an integral domain. In this case, the dimension of V is the transcendence degree over k of the field of fractions of $\mathcal{O}(V)/\mathfrak{N}$, and every maximal chain of distinct prime ideals in $\mathcal{O}(V)$ has length $\dim V$ (CA 13.8). Therefore, every maximal chain of distinct irreducible closed subsets of V has length $\dim V$. For example, the dimension of \mathbb{A}^n is the transcendence degree of $k(X_1, \dots, X_n)$ over k , which is n .

6f Algebraic groups as groups in the category of affine algebraic schemes

Finite products exist in the category of affine algebraic schemes over k . For example, the product of the affine algebraic schemes V and W is $\text{Spec}(\mathcal{O}(V) \otimes \mathcal{O}(W))$, and $*$ = $\text{Spm}(k)$ is a final object. Therefore monoid objects and group objects are defined. A monoid (resp. group) in the category of affine algebraic schemes over k is called an **affine algebraic monoid scheme** (resp. **affine algebraic group scheme**) over k .

As the tensor product of two affine k -algebras is again affine (§6d), the category of affine algebraic varieties also has products. A monoid object (resp. group object) in the category of affine algebraic varieties is called an **affine monoid variety** (resp. **affine group variety**).

An affine algebraic scheme V defines a functor

$$R \rightsquigarrow V(R) \stackrel{\text{def}}{=} \text{Hom}_{k\text{-alg}}(\mathcal{O}(V), R), \quad (43)$$

from k -algebras to sets. For example, $\mathbb{A}^n(R) \simeq R^n$ for all k -algebras R . Let V' be the functor defined by V . It follows from (6.1) and the Yoneda lemma that $V \rightsquigarrow V'$ is an equivalence from the category of algebraic schemes over k to the category of functors from k -algebras to sets representable by finitely generated k -algebras. Group structures on V correspond to factorizations of V' through the category of groups. Thus $V \rightsquigarrow V'$ is an equivalence from the category of affine algebraic group schemes over k to the category of functors $\text{Alg}_k \rightarrow \text{Grp}$ representable by finitely generated k -algebras, with quasi-inverse $G \rightsquigarrow \text{Spm}(\mathcal{O}(G))$.

The functor $V \rightsquigarrow \mathcal{O}(V)$ is an equivalence from the category of algebraic schemes over k to the category of finitely generated k -algebras (cf. 6.1). Group structures on V correspond to Hopf algebra structures on $\mathcal{O}(V)$. Thus $V \rightsquigarrow \mathcal{O}(V)$ is a contravariant equivalence from the category of affine algebraic group schemes over k to the category of finitely generated Hopf algebras over k .

SUMMARY 6.11 Let k be a field. There are canonical equivalences between the following categories:

- (a) the category of affine algebraic groups over k ;

- (b) the category of functors $\text{Alg}_k \rightarrow \text{Grp}$ representable by finitely generated k -algebras;
- (c) the opposite of the category of finitely generated Hopf algebras over k ;
- (d) the category of affine algebraic group schemes over k .

There is a similar statement with “group” and “Hopf algebra” replaced by “monoid” and “bi-algebra”.

For an affine algebraic group G , we let $(|G|, \mathcal{O}(G))$, or just $|G|$, denote the corresponding affine group scheme (or group variety); thus $|G| = \text{Spm}(\mathcal{O}(G))$. The *dimension* of an algebraic group G is defined to be the Krull dimension of $\mathcal{O}(G)$. When $\mathcal{O}(G)$ is an integral domain, this is equal to the transcendence degree of $\mathcal{O}(G)$ over k (CA 13.8).

IS THE SET $|G|$ A GROUP?

Not usually. The problem is that the functor spm does not send sums to products. For example, when k_1 and k_2 are finite field extensions of k , the set $\text{spm}(k_1 \otimes_k k_2)$ may have several points¹⁶ whereas $\text{spm}(k_1) \times \text{spm}(k_2)$ has only one. For an algebraic group G , there is a canonical map $|G \times G| \rightarrow |G| \times |G|$, but the map

$$|G \times G| \rightarrow |G|$$

defined by m need not factor through it.

However, $|G|$ is a group when k is algebraically closed. Then the Nullstellensatz shows that $|G| \simeq G(k)$, and so $|G|$ inherits a group structure from $G(k)$. To put it another way, for finitely generated algebras A_1 and A_2 over an algebraically closed field k ,

$$\text{spm}(A_1 \otimes A_2) \simeq \text{spm}(A_1) \times \text{spm}(A_2) \quad (44)$$

(as sets, not as topological spaces¹⁷), and so the forgetful functor $(V, \mathcal{O}) \rightsquigarrow V$ sending an affine algebraic scheme over k to its underlying set preserves finite products, and hence also monoid objects and group objects.

Assume k is perfect, and let $\Gamma = \text{Gal}(k^{\text{al}}/k)$. Then $|G| \simeq \Gamma \backslash G(k^{\text{al}})$ and $G(k) \simeq G(k^{\text{al}})^{\Gamma}$. In other words, $|G|$ can be identified with the set of Γ -orbits in $G(k^{\text{al}})$ and $G(k)$ with the set of Γ -orbits consisting of a single point. While the latter inherits a group structure from $G(k)$, the former need not.

The situation is worse with spec . For example, (44) fails for spec even when k is algebraically closed.

¹⁶For example, if k_1/k is separable, then

$$k_1 = k[a] \simeq k[X]/(f)$$

for a suitable element a and its minimum polynomial f . Let $f = f_1 \cdots f_r$ be the factorization of f into its irreducible factors in k_2 (they are distinct because k_1/k is separable). Now

$$k_1 \otimes_k k_2 \simeq k_2[X]/(f_1 \cdots f_r) \simeq \prod_{i=1}^r k_2[X]/(f_i)$$

by the Chinese remainder theorem. Therefore $\text{spm}(k_1 \otimes_k k_2)$ has r points.

¹⁷When regarded as a functor to topological spaces, $(V, \mathcal{O}) \rightsquigarrow V$ does not preserve finite products: the topology on $V \times W$ is not the product topology. For an affine algebraic group G , the map $m: |G| \times |G| \rightarrow |G|$ is not usually continuous relative to the product topology, and so $|G|$ is not a topological group for the Zariski topology.

6g Terminology

From now on “group scheme” and “algebraic group scheme” will mean “affine group scheme” and “affine algebraic group scheme”; similarly for “group variety”, “monoid variety”, “monoid scheme” and “algebraic monoid scheme”.

6h Homogeneity

Let G be an algebraic group over a field k . An element a of $G(k)$ defines an element of $G(R)$ for each k -algebra R , which we denote a_R (or just a). Let e denote the identity element of $G(k)$.

PROPOSITION 6.12 For each $a \in G(k)$, the natural map

$$L_a: G(R) \rightarrow G(R), \quad g \mapsto a_R g,$$

is an isomorphism of set-valued functors. Moreover,

$$L_e = \text{id}_G \text{ and } L_a \circ L_b = L_{ab}, \quad \text{all } a, b \in G(k).$$

Here e is the neutral element in $G(k)$.

PROOF. The second statement is obvious, and the first follows from it, because the equalities

$$L_a \circ L_{a^{-1}} = L_e = \text{id}_G$$

show that L_a is an isomorphism. □

The homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(G)$ defined by L_a is the composite of the homomorphisms

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{a \otimes \mathcal{O}(G)} k \otimes \mathcal{O}(G) \simeq \mathcal{O}(G). \quad (45)$$

For $a \in G(k)$, we let \mathfrak{m}_a denote the kernel of $a: \mathcal{O}(G) \rightarrow k$; thus

$$\mathfrak{m}_a = \{f \in \mathcal{O}(G) \mid f_k(a) = 0\}$$


(see the notations 2.16). Then $\mathcal{O}(G)/\mathfrak{m}_a \simeq k$, and so \mathfrak{m}_a is a maximal ideal in $\mathcal{O}(G)$. Note that $\mathcal{O}(G)_{\mathfrak{m}_a}$ is the ring of fractions obtained from $\mathcal{O}(G)$ by inverting the elements of the multiplicative set $\{f \in \mathcal{O}(G) \mid f_k(a) \neq 0\}$.

PROPOSITION 6.13 For each $a \in G(k)$, $\mathcal{O}(G)_{\mathfrak{m}_a} \simeq \mathcal{O}(G)_{\mathfrak{m}_e}$.

PROOF. The isomorphism $\ell_a: \mathcal{O}(G) \rightarrow \mathcal{O}(G)$ corresponding (by the Yoneda lemma) to L_a is defined by $\ell_a(f)_R(g) = f_R(a_R g)$, all $g \in G(R)$. Therefore, $\ell_a^{-1} \mathfrak{m}_e = \mathfrak{m}_a$, and so ℓ_a extends to an isomorphism $\mathcal{O}(G)_{\mathfrak{m}_a} \rightarrow \mathcal{O}(G)_{\mathfrak{m}_e}$ (because of the universal property of rings of fractions; CA 6.1). □

COROLLARY 6.14 When k is algebraically closed, the local rings $\mathcal{O}(G)_{\mathfrak{m}}$ at maximal ideals \mathfrak{m} of $\mathcal{O}(G)$ are all isomorphic.

PROOF. When k is algebraically closed, the Nullstellensatz (CA 11.6) shows that all maximal ideals in $\mathcal{O}(G)$ are of the form \mathfrak{m}_a for some $a \in G(k)$. \square

 6.15 The corollary fails when k is not algebraically closed. For example, for the algebraic group μ_3 over \mathbb{Q} ,

$$\mathcal{O}(\mu_3) = \frac{k[X]}{X^3 - 1} \simeq \frac{k[X]}{X - 1} \times \frac{k[X]}{X^2 + X + 1} \simeq \mathbb{Q} \times \mathbb{Q}[\sqrt{-3}],$$


and so the local rings are \mathbb{Q} and $\mathbb{Q}[\sqrt{-3}]$.

6i Reduced algebraic groups

An algebraic group G is **reduced** if $|G|$ is reduced, i.e., if $\mathcal{O}(G)$ has no nilpotents.

PROPOSITION 6.16 *Let G be a reduced algebraic group over a field k . If $G(K) = \{1\}$ for some algebraically closed field K containing k , then G is the trivial algebraic group, i.e., $\mathcal{O}(G) = k$.*

PROOF. Every maximal ideal of $\mathcal{O}(G)$ arises as the kernel of a homomorphism $\mathcal{O}(G) \rightarrow K$ (Nullstellensatz, CA 11.5), and so $\mathcal{O}(G)$ has only one maximal ideal \mathfrak{m} . As $\mathcal{O}(G)$ is reduced, the intersection of its maximal ideals is zero (CA 11.8), and so $\mathfrak{m} = 0$. Therefore $\mathcal{O}(G)$ is a field. It contains k , and the identity element in G is a homomorphism $\mathcal{O}(G) \rightarrow k$, and so $\mathcal{O}(G) = k$. \square

6.17 The proposition is false for nonreduced groups. For example, $\alpha_p(K) = \{1\}$ for every field K containing k , but α_p is not the trivial group. 

PROPOSITION 6.18 *Let G be an algebraic group over a perfect field k , and let \mathfrak{N} be the nilradical of $\mathcal{O}(G)$. There is a unique Hopf algebra structure on $\mathcal{O}(G)/\mathfrak{N}$ such that $\mathcal{O}(G) \rightarrow \mathcal{O}(G)/\mathfrak{N}$ is a homomorphism of Hopf algebras. Let $G_{\text{red}} \rightarrow G$ be the corresponding homomorphism of algebraic groups. Every homomorphism $H \rightarrow G$ with H a reduced algebraic group factors uniquely through $G_{\text{red}} \rightarrow G$.*

PROOF. Let $A = \mathcal{O}(G)$ and $A_{\text{red}} = \mathcal{O}(G)/\mathfrak{N}$. Then A_{red} is a finitely generated reduced algebra over a perfect field, and so it is an affine k -algebra (§6d). Hence $A_{\text{red}} \otimes_k A_{\text{red}}$ is also an affine k -algebra. In particular, it is reduced, and so the map

$$A \xrightarrow{\Delta} A \otimes A \rightarrow A_{\text{red}} \otimes A_{\text{red}}$$

factors through A_{red} . Similarly, S and ϵ are defined on A_{red} , and it follows that there exists a unique structure of a Hopf algebra on A_{red} such that $A \rightarrow A_{\text{red}}$ is a homomorphism of Hopf algebras. Every homomorphism from A to a reduced k -algebra factors uniquely through $A \rightarrow A_{\text{red}}$, from which the final statement follows. \square

The algebraic group G_{red} is called the **reduced algebraic group attached to G** .

6.19 When k is not perfect, a Hopf algebra structure on A need not pass to the quotient A/\mathfrak{N} . For example, let k be a field of characteristic 2, and let a be a nonsquare in k . Then $R \rightsquigarrow G(R) = \{x \in R \mid x^4 = ax^2\}$ is an additive commutative algebraic group, but $\mathcal{O}(G)/\mathfrak{N}$ is not a Hopf algebra quotient of $\mathcal{O}(G)$ (see Exercise 13-7 below). ✎

NOTES G_{red} is an affine subgroup of G if $A_{\text{red}} \otimes A_{\text{red}}$ is reduced.

6j Smooth algebraic schemes

We review some definitions and results in commutative algebra.

6.20 Let \mathfrak{m} be a maximal ideal of a noetherian ring A , and let $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$ be the maximal ideal of the local ring $A_{\mathfrak{m}}$; for all natural numbers $r \leq s$, the map

$$a + \mathfrak{m}^s \mapsto a + \mathfrak{n}^s: \mathfrak{m}^r/\mathfrak{m}^s \rightarrow \mathfrak{n}^r/\mathfrak{n}^s$$

is an isomorphism (CA 6.7).

6.21 Let A be a local noetherian ring with maximal ideal \mathfrak{m} and residue field k . Then $\mathfrak{m}/\mathfrak{m}^2$ is a k -vector space of dimension equal to the minimum number of generators of \mathfrak{m} (Nakayama's lemma, CA 3.9). Moreover, $\text{ht}(\mathfrak{m}) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ (CA 16.5), and when equality holds A is said to be **regular**. Every regular noetherian local ring is an integral domain (CA 17.3).

6.22 A point \mathfrak{m} of an affine algebraic scheme V is said to be **regular** if the local ring $\mathcal{O}(V)_{\mathfrak{m}}$ is regular, and V is said to be **regular** if all of its closed points are regular.¹⁸ A regular affine algebraic scheme is reduced. To see this, let f be a nilpotent element of $\mathcal{O}(V)$; as f maps to zero in $\mathcal{O}(V)_{\mathfrak{m}}$, $sf = 0$ for some $s \in \mathcal{O}(V) \setminus \mathfrak{m}$; therefore the annihilator of f is an ideal $\mathcal{O}(V)$ not contained in any maximal ideal, and so it equals $\mathcal{O}(V)$.

6.23 An affine algebraic scheme V over k is said to be **smooth** if $V_{k^{\text{al}}}$ is regular. If V is smooth, then V_K is regular for all fields K containing k ; in particular, V itself is regular (CA 18.14). If V is smooth, then it follows from (6.22) that $\mathcal{O}(V)$ is an affine k -algebra, and so V is an algebraic variety. Every affine algebraic variety contains a regular point (CA 18.15).

6k Smooth algebraic groups

An algebraic group G is said to be **smooth** if $|G|$ is smooth, and it is **connected** if $|G|$ is connected (as a topological space).

PROPOSITION 6.24 *Let H be an algebraic subgroup of an algebraic group G . Then $\dim H \leq \dim G$, and $\dim H < \dim G$ if G is smooth and connected and $H \neq G$.*

PROOF. Because $\mathcal{O}(H)$ is a quotient of $\mathcal{O}(G)$, $\dim(\mathcal{O}(H)) \leq \dim(\mathcal{O}(G))$. If G is smooth and connected, then $\mathcal{O}(G)$ is an integral domain; if $H \neq G$, then $\dim H < \dim G$ by (CA 13.3). □

¹⁸This then implies that local ring at every (not necessarily closed) point is regular (for a noetherian ring A , if $A_{\mathfrak{m}}$ is regular for all maximal ideals, then $A_{\mathfrak{p}}$ is regular for all prime ideals (CA 17.5a).

PROPOSITION 6.25 *An algebraic group G over an algebraically closed field k is smooth if and only if $\mathcal{O}(G)_{\mathfrak{m}_e}$ is regular, where $\mathfrak{m}_e = \text{Ker}(\epsilon: \mathcal{O}(G) \rightarrow k)$.*

PROOF. If $\mathcal{O}(G)_{\mathfrak{m}}$ is regular for $\mathfrak{m} = \mathfrak{m}_e$, then $\mathcal{O}(G)_{\mathfrak{m}}$ is regular for all \mathfrak{m} by homogeneity (6.13). Hence G is smooth. \square

PROPOSITION 6.26 (a) *An algebraic group G is smooth if and only if $|G|$ is geometrically reduced (i.e., an algebraic variety).*

(b) *An algebraic group G over a perfect field is smooth if and only if $|G|$ is reduced.*

PROOF. (a) If G is smooth, then $|G|$ is an algebraic variety by (6.23). For the converse, we have to show that $G_{k^{\text{al}}}$ is regular. According to (6.23), $G_{k^{\text{al}}}$ has a regular point, and so, by homogeneity (6.13), all of its points are regular.

(b) When k is perfect, a finitely generated k -algebra A is reduced if and only if $k^{\text{al}} \otimes A$ is reduced (see CA 18.1). Thus (b) follows from (a). \square

COROLLARY 6.27 *An algebraic group G over an algebraically closed field k is smooth if every nilpotent element of $\mathcal{O}(G)$ is contained in \mathfrak{m}_e^2 .*

PROOF. Let \bar{G} be the reduced algebraic group attached to G (see 6.18), and let \bar{e} be the neutral element of $\bar{G}(k)$. By definition, $\mathcal{O}(\bar{G}) = \mathcal{O}(G)/\mathfrak{N}$ where \mathfrak{N} is the nilradical of $\mathcal{O}(G)$. Every prime ideal of $\mathcal{O}(G)$ contains \mathfrak{N} , and so the prime ideals of $\mathcal{O}(G)$ and $\mathcal{O}(\bar{G})$ are in natural one-to-one correspondence. Therefore \mathfrak{m}_e and $\mathfrak{m}_{\bar{e}}$ have the same height, and so

$$\dim \mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}} = \dim \mathcal{O}(G)_{\mathfrak{m}_e}$$

(Krull dimensions). The hypothesis on $\mathcal{O}(G)$ implies that

$$\mathfrak{m}_e/\mathfrak{m}_e^2 \rightarrow \mathfrak{m}_{\bar{e}}/\mathfrak{m}_{\bar{e}}^2$$


is an isomorphism of k -vector spaces. Because $|\bar{G}|$ is a reduced, \bar{G} is smooth (6.26); in particular, $\mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}}$ is regular, and so

$$\dim_k(\mathfrak{m}_{\bar{e}}/\mathfrak{m}_{\bar{e}}^2) = \dim \mathcal{O}(\bar{G})_{\mathfrak{m}_{\bar{e}}}.$$

Therefore

$$\dim_k(\mathfrak{m}_e/\mathfrak{m}_e^2) = \dim \mathcal{O}(G)_{\mathfrak{m}_e},$$

and so $\mathcal{O}(G)_{\mathfrak{m}_e}$ is regular. This implies that G is smooth (6.25). \square

6.28 A reduced algebraic group over a nonperfect field need not be smooth. For example, let k be such a field, so that $\text{char}(k) = p \neq 0$ and there exists an element a of k that is not a p th power. Then the subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $Y^p = aX^p$ is reduced but not smooth. Indeed, 

$$\mathcal{O}(G) = k[X, Y]/(Y^p - aX^p),$$

which is an integral domain because $Y^p - aX^p$ is irreducible in $k[X, Y]$, but

$$\mathcal{O}(G_{k^{\text{al}}}) = k^{\text{al}}[X, Y]/(Y^p - aX^p) = k^{\text{al}}[x, y]$$

contains the nilpotent element $y - a^{\frac{1}{p}}x$. The reduced subgroup $(G_{k^{\text{al}}})_{\text{red}}$ of $G_{k^{\text{al}}}$ is the subgroup of $\mathbb{G}_a \times \mathbb{G}_a$ is defined by $Y = a^{\frac{1}{p}}X$, which is not defined over k (as a subgroup of $\mathbb{G}_a \times \mathbb{G}_a$).

Note that G is the kernel of $(x, y) \mapsto y^p - ax^p: \mathbb{G}_a \times \mathbb{G}_a \xrightarrow{\alpha} \mathbb{G}_a$. Therefore, although $\text{Ker}(\alpha_{k^{\text{al}}})$ is (of course) defined over k , $\text{Ker}(\alpha_{k^{\text{al}}})_{\text{red}}$ is not.

61 Algebraic groups in characteristic zero are smooth (Cartier's theorem)

We first prove two lemmas.

LEMMA 6.29 *Let V and V' be vector spaces over a field,¹⁹ and let W be a subspace of V . For $x \in V, y \in V'$,*

$$x \otimes y \in W \otimes V' \iff x \in W \text{ or } y = 0.$$

PROOF. The element $x \otimes y$ lies in $W \otimes V'$ if and only if its image in $V \otimes V' / W \otimes V'$ is zero. But

$$V \otimes V' / W \otimes V' \simeq (V/W) \otimes V',$$

and the image $\bar{x} \otimes y$ of $x \otimes y$ in $(V/W) \otimes V'$ is zero if and only if $\bar{x} = 0$ or $y = 0$. \square

LEMMA 6.30 *Let (A, Δ, ϵ) be a Hopf algebra over k , and let $I = \text{Ker}(\epsilon)$.*

- (a) *As a k -vector space, $A = k \oplus I$.*
- (b) *For any $a \in I$,*

$$\Delta(a) = a \otimes 1 + 1 \otimes a \pmod{I \otimes I}.$$

PROOF. (a) The maps $k \rightarrow A \xrightarrow{\epsilon} k$ are k -linear, and compose to the identity. Therefore $A = k \oplus I$ and $a \in A$ decomposes as $a = \epsilon(a) + (a - \epsilon(a)) \in k \oplus I$.

(b) For $a \in A$, write $a = a' + a''$ with $a' = \epsilon(a) \in k$ and $a'' \in I$. Let

$$\Delta(a) = \sum b \otimes c, \quad b, c \in A.$$

From the commutativity of the second diagram in (29), p. 42, we find that

$$\begin{aligned} 1 \otimes a &= \sum b' \otimes c && \text{in } k \otimes A \\ a \otimes 1 &= \sum b \otimes c' && \text{in } A \otimes k. \end{aligned}$$

Therefore

$$\begin{aligned} \Delta(a) - a \otimes 1 - 1 \otimes a &= \sum (b \otimes c - b' \otimes c - b \otimes c') \\ &= \sum (b'' \otimes c'' - b' \otimes c') \\ &\equiv -\sum b' \otimes c' \pmod{I \otimes I}. \end{aligned}$$

Now

$$\begin{aligned} ((\epsilon, \epsilon) \circ \Delta)(a) &= (\epsilon, \epsilon)(\sum b \otimes c) = \sum b' \otimes c' \\ ((\epsilon, \epsilon) \circ \Delta)(a) &= (\epsilon \cdot \epsilon)(a) = \epsilon(a) \quad (\text{as } \epsilon \cdot \epsilon \stackrel{\text{def}}{=} (\epsilon, \epsilon) \circ \Delta, (8), \text{ p. 22}), \end{aligned}$$

and so $\sum b' \otimes c' = 0$ if $a \in I$. \square

¹⁹It suffices to require V and V' to be modules over a ring with V' faithfully flat.

THEOREM 6.31 (CARTIER 1962) *Every algebraic group over a field of characteristic zero is smooth.*

PROOF. We may replace k with its algebraic closure. Thus, let G be an algebraic group over an algebraically closed field k of characteristic zero, and let $A = \mathcal{O}(G)$. Let $\mathfrak{m} = \mathfrak{m}_e = \text{Ker}(\epsilon)$. Let a be a nilpotent element of A ; according to (6.27), it suffices to show that a lies in \mathfrak{m}^2 .

If a maps to zero in $A_{\mathfrak{m}}$, then it maps to zero in $A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2$, and therefore in A/\mathfrak{m}^2 by (6.20), and so $a \in \mathfrak{m}^2$. Thus, we may suppose that there exists an $n \geq 2$ such that $a^n = 0$ in $A_{\mathfrak{m}}$ but $a^{n-1} \neq 0$ in $A_{\mathfrak{m}}$. Now $sa^n = 0$ in A for some $s \notin \mathfrak{m}$. On replacing a with sa , we find that $a^n = 0$ in A but $a^{n-1} \neq 0$ in $A_{\mathfrak{m}}$.

Now $a \in \mathfrak{m}$ (because $A/\mathfrak{m} = k$ has no nilpotents), and so (see 6.30)

$$\Delta(a) = a \otimes 1 + 1 \otimes a + y \quad \text{with} \quad y \in \mathfrak{m} \otimes_k \mathfrak{m}.$$

Because Δ is a homomorphism of k -algebras,

$$0 = \Delta(a^n) = (\Delta a)^n = (a \otimes 1 + 1 \otimes a + y)^n. \quad (46)$$

When expanded, the right hand side becomes a sum of terms

$$a^n \otimes 1, \quad n(a^{n-1} \otimes 1) \cdot (1 \otimes a + y), \quad (a \otimes 1)^h (1 \otimes a)^i y^j \quad (h+i+j=n, i+j \geq 2).$$

As $a^n = 0$ and the terms with $i+j \geq 2$ lie in $A \otimes \mathfrak{m}^2$, equation (46) shows that

$$na^{n-1} \otimes a + n(a^{n-1} \otimes 1)y \in A \otimes \mathfrak{m}^2,$$

and so

$$na^{n-1} \otimes a \in a^{n-1}\mathfrak{m} \otimes A + A \otimes \mathfrak{m}^2 \quad (\text{inside } A \otimes_k A).$$

In the quotient $A \otimes (A/\mathfrak{m}^2)$ this becomes

$$na^{n-1} \otimes \bar{a} \in a^{n-1}\mathfrak{m} \otimes A/\mathfrak{m}^2 \quad (\text{inside } A \otimes A/\mathfrak{m}^2). \quad (47)$$

Note that $a^{n-1} \notin a^{n-1}\mathfrak{m}$, because if $a^{n-1} = a^{n-1}m$ with $m \in \mathfrak{m}$, then $(1-m)a^{n-1} = 0$ and, as $1-m$ is a unit in $A_{\mathfrak{m}}$, this would imply $a^{n-1} = 0$ in $A_{\mathfrak{m}}$, which is a contradiction. Moreover n is a unit in A because it is a nonzero element of k . We conclude that $na^{n-1} \notin a^{n-1}\mathfrak{m}$, and so (see 6.29) $\bar{a} = 0$. In other words, $a \in \mathfrak{m}^2$, as required. \square

COROLLARY 6.32 *Let G be an algebraic group over a field of characteristic zero. If $G(K) = \{1\}$ for some algebraically closed field K , then G is the trivial algebraic group.*

PROOF. According to the theorem, G is reduced, and so we can apply Proposition 6.16. \square

ASIDE 6.33 Let k be an arbitrary commutative ring. A functor $F: \text{Alg}_k \rightarrow \text{Set}$ is said to be **formally smooth** if, for any k -algebra A and nilpotent ideal \mathfrak{n} in A , the map $F(A) \rightarrow F(A/\mathfrak{n})$ is surjective. A k -scheme X is **smooth** over k if it is locally of finite presentation and the functor $A \rightsquigarrow X(A) \stackrel{\text{def}}{=} \text{Hom}_k(\text{Spec } A, X)$ is formally smooth. There is the following criterion (SGA1, II):

a finitely presented morphism is smooth if it is flat and its geometric fibres are nonsingular algebraic varieties.

Therefore, when the ring k contains a field of characteristic zero, Cartier's theorem (6.31) shows that every flat affine group scheme of finite presentation over k is smooth.

6m Smoothness in characteristic $p \neq 0$

THEOREM 6.34 *An algebraic group G over an algebraically closed field k of characteristic $p \neq 0$ is smooth if $\mathcal{O}(G)$ has the following property:*

$$a \in \mathcal{O}(G), \quad a^p = 0 \implies a = 0. \quad (48)$$

PROOF. Let a be a nilpotent element of $\mathcal{O}(G)$. As in the proof of Theorem 6.31, we may suppose that $a^n = 0$ in $\mathcal{O}(G)$ but $a^{n-1} \neq 0$ in $\mathcal{O}(G)_{\mathfrak{m}_e}$. If $p|n$, then $(a^{\frac{n}{p}})^p = 0$, and so $a^{\frac{n}{p}} = 0$, which is a contradiction. Therefore n is nonzero in k , and the argument in the proof of Theorem 6.31 shows that $a \in \mathfrak{m}_e^2$. \square

COROLLARY 6.35 *For all $r \geq 1$, the image of $a \mapsto a^{p^r} : \mathcal{O}(G) \rightarrow \mathcal{O}(G)$ is a Hopf subalgebra of $\mathcal{O}(G)$, and for all sufficiently large r , it is a reduced Hopf algebra.*

PROOF. Let k be a field of characteristic $p \neq 0$. For a k -algebra R , we let f_R denote the homomorphism $a \mapsto a^p : R \rightarrow R$. When $R = k$, we omit the subscript. We let ${}_f R$ denote the ring R regarded as a k -algebra by means of the map $k \xrightarrow{f} k \rightarrow R$. Let G be an algebraic group over k , and let $G^{(p)}$ be the functor $R \rightsquigarrow G({}_f R)$. This is represented by $k \otimes_{f,k} \mathcal{O}(G)$ (tensor product of $\mathcal{O}(G)$ with k relative to the map $f : k \rightarrow k$),

$$\begin{array}{ccc}
 & & R \\
 & \nearrow & \nearrow \\
 \mathcal{O}(G) & \longrightarrow & k \otimes_{f,k} \mathcal{O}(G) \\
 \uparrow & & \uparrow \\
 k & \xrightarrow{f} & k
 \end{array}$$

and so it is again an algebraic group. The k -algebra homomorphism $f_R : R \rightarrow {}_f R$ defines a homomorphism $G(R) \rightarrow G^{(p)}(R)$, which is natural in R , and so arises from a homomorphism $F : G \rightarrow G^{(p)}$ of algebraic groups. This homomorphism corresponds to the homomorphism of Hopf algebras

$$c \otimes a \mapsto ca^p : \mathcal{O}(G^{(p)}) \rightarrow \mathcal{O}(G).$$

When k is perfect, this has image $\mathcal{O}(G)^p$, which is therefore a Hopf subalgebra of $\mathcal{O}(G)$ (Exercise 5-10). On repeating this argument with f and F replaced by f^r and F^r , we find that $\mathcal{O}(G)^{p^r}$ is a Hopf subalgebra of $\mathcal{O}(G)$.

Concerning the second part of the statement, because the nilradical \mathfrak{N} of $\mathcal{O}(G)$ is finitely generated, there exists an exponent n such that $a^n = 0$ for all $a \in \mathfrak{N}$. Let r be such that $p^r \geq n$; then $a^{p^r} = 0$ for all $a \in \mathfrak{N}$. With this r , $\mathcal{O}(G)^{p^r}$ satisfies (48). As it is a Hopf algebra, it is reduced. \square

NOTES The first part of (6.35) only requires that k be perfect (probably the same is true of the remaining statements).

6n Transporters

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

$$(g, x) \mapsto gx: G \times X \rightarrow X$$

such that

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

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

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

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

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

THEOREM 6.36 *Let $G \times X \rightarrow X$ be an action of an affine monoid G on a functor X , and let Z and Y be subfunctors of X such that Z is closed in X . If Y is representable, then $T_G(Y, Z)$ is represented by a quotient of $\mathcal{O}(G)$.*

CLOSED SUBFUNCTORS

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

$$(Z \times_Y h^A)(R) = \{\varphi: A \rightarrow R \mid \varphi(\alpha) \in Z(A)\}.$$

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

$$R \rightsquigarrow \{\varphi: A \rightarrow R \mid \varphi(\alpha) \in Z(A)\}$$

is represented by a quotient of A ; i.e., there exists an ideal $\mathfrak{a} \subset A$ such that, for a homomorphism $\varphi: A \rightarrow R$ of k -algebras,

$$\alpha_R \in Z(R) \iff \varphi(\mathfrak{a}) = 0,$$

where α_R is the image of α under $Y(A) \rightarrow Y(R)$.

EXAMPLE 6.37 Let Z be a subfunctor of $Y = h^B$ for some k -algebra B . For the identity map $h^B \rightarrow Y$, the functor $Z \times_Y h^B = Z$. Therefore, if Z is closed in h^B , then it is represented by a quotient of B . Conversely, let $Z \subset h^B$ be the functor defined by an ideal $\mathfrak{b} \subset B$, i.e.,

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

Then Z is closed because, for any $\alpha: B \rightarrow A$, the functor $Z \times_{h^B} h^A$ is

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

which is represented by $A/\alpha(\mathfrak{b})$.²⁰

EXAMPLE 6.38 Let Y be the functor $\mathbb{A}^n = (R \rightsquigarrow R^n)$. A subfunctor of \mathbb{A}^n is closed if and if it is defined by a finite set of polynomials in $k[X_1, \dots, X_n]$ in the sense of §2a. This is the special case $B = k[X_1, \dots, X_n]$ of Example 6.37.

For a k -algebra B and functor $X: \text{Alg}_B \rightarrow \text{Set}$, we let $\Pi_{B/k} X$ denote the functor $R \rightsquigarrow X(B \otimes R)$ (cf. §4d).

LEMMA 6.39 *If Z is a closed subfunctor of X , then, for any k -algebra B , $\Pi_{B/k} Z$ is a closed subfunctor of $\Pi_{B/k} X$.*

PROOF. Let A be a k -algebra, and $\alpha \in X(B \otimes A)$. To prove that $\Pi_{B/k} Z$ is closed in $\Pi_{B/k} X$ we have to show that there exists an ideal $\mathfrak{a} \subset A$ such that, for every homomorphism $\varphi: A \rightarrow R$ of k -algebras,

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

Because Z is closed in X , there exists an ideal $\mathfrak{b} \subset B \otimes A$ such that

$$(B \otimes \varphi)(\alpha) \in Z(B \otimes R) \iff (B \otimes \varphi)(\mathfrak{b}) = 0. \quad (49)$$

Choose a basis $(e_i)_{i \in I}$ for B as k -vector space. Each element b of $B \otimes A$ can be expressed uniquely as $b = \sum_{i \in I} e_i \otimes b_i$, $b_i \in A$, and we let \mathfrak{a} be the ideal in A generated by the coordinates b_i of the elements $b \in \mathfrak{b}$. Then $\mathfrak{b} \subset B \otimes \mathfrak{a}$, and \mathfrak{a} is the smallest ideal in A with this property, i.e.,

$$\mathfrak{a} \subset \mathfrak{a}' \iff \mathfrak{b} \subset B \otimes \mathfrak{a}' \quad (\mathfrak{a}' \text{ an ideal in } A). \quad (50)$$

On applying (50) with $\mathfrak{a}' = \text{Ker } \varphi$, we see that

$$\mathfrak{a} \subset \text{Ker}(\varphi) \iff \mathfrak{b} \subset B \otimes \text{Ker}(\varphi) = \text{Ker}(B \otimes \varphi).$$

Combined with (49), this shows that \mathfrak{a} has the required property. \square

LEMMA 6.40 *If Z is a closed subfunctor of X , then, for any map $T \rightarrow X$ of functors, $T \times_X Z$ is a closed subfunctor of T .*

PROOF. Let $h^A \rightarrow T$ be a map of functors. Then $h^A \times_T T \times_X Z \simeq h^A \times_X Z$, and so the statement is obvious. \square

LEMMA 6.41 *Let Z and Y be subfunctors of a functor X , and let $G \times X \rightarrow X$ be an action of an affine monoid G on X . Assume $Y = h^B$. For a k -algebra R , let $y_R \in Y(R \otimes B)$ be the homomorphism $b \mapsto 1 \otimes b: B \rightarrow R \otimes B$. Then*

$$T_G(Y, Z)(R) = \{g \in G(R) \mid g y_R \in Z(R \otimes B)\}.$$

²⁰More generally, if Y is the functor of k -algebras defined by a scheme Y' , then the closed subfunctors of Y are exactly those defined by closed subschemes of Y' .

PROOF. Certainly, $\text{LHS} \supset \text{RHS}$. For the reverse inclusion, let R' be an R -algebra, and let $\alpha \in Y(R') = \text{Hom}(B, R')$. Then y_R maps to α under the map $Y(R \otimes B) \rightarrow Y(R')$ defined by $R \rightarrow R'$ and $B \xrightarrow{\alpha} R'$, and so

$$gy_R \in Z(R \otimes B) \implies g\alpha \in Z(R'). \quad \square$$

We now prove Theorem 6.36. We may suppose that $Y = h^B$. Lemma 6.41 shows that

$$T_G(Y, Z) \simeq G \times_{\Pi_{B/k} X} \Pi_{B/k} Z,$$

where $G \rightarrow \Pi_{B/k} X$ is the natural transformation $g \mapsto gy_R: G(R) \rightarrow X(R \otimes B)$. Lemma 6.39 shows that $\Pi_{B/k} Z$ is a closed subfunctor of $\Pi_{B/k} X$, and so it follows from (6.40) that $T_G(Y, Z)$ is a closed subfunctor of h^G . This means that it is represented by a quotient of $\mathcal{O}(G)$.

ASIDE 6.42 The assumption that k is a field was used in this subsection only to deduce in the proof of Lemma 6.39 that B is free as a k -module. Thus Theorem 6.36 is true over a commutative ring k when Y is representable by a k -algebra B that is free as a k -module (or, more generally, locally free; cf. DG I, §2, 7.7, p. 65).

60 Appendix: The faithful flatness of Hopf algebras

In this subsection, we prove the following very important technical result.

THEOREM 6.43 *For any Hopf algebras $A \subset B$ over a field k , B is faithfully flat over A .*

For any field $k' \supset k$, the homomorphism $A \rightarrow k' \otimes A$ is faithfully flat, and so it suffices to show that $k' \otimes B$ is faithfully flat over $k' \otimes A$ (CA 9.4). Therefore we may suppose that k is algebraically closed.

Let $\varphi: H \rightarrow G$ be a homomorphism of affine groups such that $\mathcal{O}(H \rightarrow G) = B \leftarrow A$.

CASE THAT A IS REDUCED AND A AND B ARE FINITELY GENERATED.

We begin with a remark. Let V be an algebraic scheme over an algebraically closed field. Then V is a finite union $V = V_1 \cup \dots \cup V_r$ of its irreducible components (6c). Assume that V is homogeneous, i.e., for any pair (a, b) of points of V , there exists an isomorphism $V \rightarrow V$ sending a to b . Then V is a disjoint union of the V_i . As each V_i is closed, this means that the V_i are the connected components of V . In particular, they are open. When V_i is reduced, the ring $\mathcal{O}(V_i)$ is an integral domain.

We now regard H and G as algebraic group schemes, i.e., we write H and G for $|H|$ and $|G|$. Then H and G are disjoint unions of their connected components, say $H = \bigsqcup_{i \in I} H_i$ and $G = \bigsqcup_{j \in J} G_j$. Because G is reduced, each ring $\mathcal{O}(G_j)$ is an integral domain, and $\mathcal{O}(G) = \prod_{j \in J} \mathcal{O}(G_j)$. Each connected component H_i of H maps into a connected component $G_{j(i)}$ of G . The map $i \mapsto j(i): I \rightarrow J$ is surjective, because otherwise $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ would not be injective (any $f \in \mathcal{O}(G)$ such that $f|_{G_j} = 0$ for $j \neq j_0$ would have $f \circ \alpha = 0$).

Let H° and G° be the connected components of H and G containing the identity elements. Then H° maps into G° . Because G is reduced, $\mathcal{O}(G^\circ)$ is an integral domain, and so the generic flatness theorem (CA 9.12; CA 16.9) shows that there exists a $b \in H^\circ$ such that

$\mathcal{O}(H)_{\mathfrak{m}_b}$ is faithfully flat over $\mathcal{O}(H)_{\mathfrak{m}_{\varphi(b)}}$. Homogeneity, more precisely, the commutative diagrams

$$\begin{array}{ccc} H & \xrightarrow{L_b} & H & & \mathcal{O}(H)_{\mathfrak{m}_e} & \xleftarrow{\simeq} & \mathcal{O}(H)_{\mathfrak{m}_b} \\ \downarrow & & \downarrow & & \uparrow & & \uparrow \\ G & \xrightarrow{L_a} & G & & \mathcal{O}(G)_{\mathfrak{m}_e} & \xleftarrow{\simeq} & \mathcal{O}(G)_{\mathfrak{m}_a} \end{array}$$

(see §6h), now implies that $\mathcal{O}(H)_{\mathfrak{m}_b}$ is faithfully flat over $\mathcal{O}(G)_{\mathfrak{m}_{\varphi(b)}}$ for all $b \in H$. Hence $\mathcal{O}(H)$ is flat over $\mathcal{O}(G)$ (CA 9.9), and it remains to show that the map (of sets) $\varphi: H \rightarrow G$ is surjective (CA 9.10c). According to (CA 12.14), the image of $H \rightarrow G$ contains a nonempty open subset U of G° . For any $g \in G^\circ$, the sets U^{-1} and Ug^{-1} have nonempty intersection. This means that there exist $u, v \in U$ such that $u^{-1} = vg^{-1}$, and so $g = uv \in U$. Thus the image of φ contains G° , and the translates of G° by points in the image cover G (because I maps onto J).

CASE THAT THE AUGMENTATION IDEAL OF A IS NILPOTENT

We begin with a remark. For any homomorphism $\alpha: H \rightarrow G$ of abstract groups, the map

$$(n, h) \mapsto (nh, h): \text{Ker}(\alpha) \times H \rightarrow H \times_G H \quad (51)$$

is a bijection — this just says that two elements of H with the same image in G differ by an element of the kernel. Similarly, for any homomorphism $\alpha: H \rightarrow G$ of affine groups, there is an isomorphism

$$\text{Ker}(\alpha) \times H \rightarrow H \times_G H \quad (52)$$

which becomes the map (51) for each k -algebra R . Because of the correspondence between affine groups and Hopf algebras, this implies that, for any homomorphism $A \rightarrow B$ of Hopf algebras, there is a canonical isomorphism

$$b_1 \otimes b_2 \mapsto (\Delta b_1)(1 \otimes b_2): B \otimes_A B \rightarrow (B/I_A B) \otimes_k B \quad (53)$$

where I_A is the augmentation ideal $\text{Ker}(A \xrightarrow{\epsilon} k)$ of A .

Let $I = I_A$, and assume that I is nilpotent, say $I^n = 0$. Choose a family $(e_j)_{j \in J}$ of elements in B whose image in B/IB is a k -basis and consider the map

$$(a_j)_{j \in J} \mapsto \sum_j a_j e_j: A^{(J)} \rightarrow B \quad (54)$$

where $A^{(J)}$ is a direct sum of copies of A indexed by J . We shall show that (54) is an isomorphism (hence B is even free as an A -module).

Let C be the cokernel of (54). A diagram chase in

$$\begin{array}{ccccccc} A^{(J)} & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ \downarrow & & \downarrow & & & & \\ (A/I)^{(J)} & \xrightarrow{\text{onto}} & B/IB & & & & \end{array}$$

shows that every element of C is the image of an element of B mapping to zero in B/IB , i.e., lying in IB . Hence $C = IC$, and so $C = IC = I^2C = \dots = I^n C = 0$. Hence $A^{(J)} \rightarrow B$ is surjective.

For the injectivity, consider diagrams

$$\begin{array}{ccccc}
 A^{(J)} & \xrightarrow{\text{onto}} & B & & k^{(J)} & \xrightarrow{\simeq} & B/IB \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 B^{(J)} & \xrightarrow{\text{onto}} & B \otimes_A B & & (B/IB)^{(J)} & \xrightarrow{\simeq} & (B/IB) \otimes_k (B/IB)
 \end{array}$$

in which the bottom arrows are obtained from the top arrows by tensoring on the left with B and B/IB respectively. If $b \in B^{(J)}$ maps to zero in $B \otimes_A B$, then it maps to zero in $B/IB \otimes_k B/IB$, which implies that it maps to zero in $(B/IB)^{(J)}$. Therefore the kernel M of $B^{(J)} \rightarrow B \otimes_A B$ is contained in $(IB)^{(J)} = I \cdot B^{(J)}$.

Recall (53) that

$$B \otimes_A B \simeq B \otimes_k B/IB.$$

As B/IB is free as a k -module (k is a field), $B \otimes_k B/IB$ is free as a left B -module, and so $B \otimes_A B$ is free (hence projective) as a left B -module. Therefore there exists a B -submodule N of $B^{(J)}$ mapping isomorphically onto $B \otimes_A B$, and

$$B^{(J)} = M \oplus N \text{ (direct sum of } B\text{-submodules).}$$

We know that

$$M \subset I \cdot B^{(J)} = IM \oplus IN,$$

and so $M \subset IM$. Hence $M \subset IM \subset I^2M = \dots = 0$. We have shown that $B^{(J)} \rightarrow B \otimes_A B$ is injective, and this implies that $A^{(J)} \rightarrow B$ is injective because $A^{(J)} \subset B^{(J)}$.

CASE THAT A AND B ARE FINITELY GENERATED

We begin with a remark. For any homomorphisms of abstract groups

$$\begin{array}{ccc}
 H & & \\
 \downarrow \beta & & \\
 G & \xrightarrow{\alpha} & G',
 \end{array}$$

the map

$$(n, h) \mapsto (n \cdot \beta(h), h): \text{Ker}(\alpha) \times H \rightarrow G \times_{G'} H$$

is a bijection. This implies a similar statement for affine groups:

$$\text{Ker}(G \rightarrow G') \times H \simeq G \times_{G'} H. \quad (55)$$

After Theorem 6.31, we may suppose that k has characteristic $p \neq 0$. According to (6.35), there exists an n such that $\mathcal{O}(G)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(G)$. Let G' be the algebraic group such that $\mathcal{O}(G') = \mathcal{O}(G)^{p^n}$, and consider the diagrams

$$\begin{array}{ccccccc}
 1 & \longrightarrow & N & \longrightarrow & H & \longrightarrow & G' & & \mathcal{O}(N) & \longleftarrow & \mathcal{O}(H) & \xleftarrow[\text{flat}]{\text{faithfully}} & \mathcal{O}(G') \\
 & & \downarrow & & \downarrow & & \parallel & & \uparrow & & \uparrow \text{injective} & & \parallel \\
 1 & \longrightarrow & M & \longrightarrow & G & \longrightarrow & G' & & \mathcal{O}(M) & \longleftarrow & \mathcal{O}(G) & \longleftarrow & \mathcal{O}(G')
 \end{array}$$

where N and M are the kernels of the homomorphisms $H \rightarrow G'$ and $G \rightarrow G'$ respectively. Because $\mathcal{O}(G')$ is reduced, the homomorphism $\mathcal{O}(G') \rightarrow \mathcal{O}(H)$ is faithfully flat, and so

$$\mathcal{O}(G) \rightarrow \mathcal{O}(H) \text{ injective} \implies (\mathcal{O}(G) \rightarrow \mathcal{O}(H)) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) \text{ injective.}$$

As k is a direct summand of $\mathcal{O}(H)$, this implies that $(\mathcal{O}(G) \rightarrow \mathcal{O}(H)) \otimes_{\mathcal{O}(G')} k$ is injective. From the diagram

$$\begin{array}{ccc} \mathcal{O}(N) & \xrightarrow{(23)} & \mathcal{O}(H) \otimes_{\mathcal{O}(G')} k \\ \uparrow & & \uparrow \\ \mathcal{O}(M) & \xrightarrow{(23)} & \mathcal{O}(G) \otimes_{\mathcal{O}(G')} k \end{array}$$

we see that $\mathcal{O}(M) \rightarrow \mathcal{O}(N)$ is injective, and hence is faithfully flat (because the augmentation ideal of $\mathcal{O}(M)$ is nilpotent). From the diagrams

$$\begin{array}{ccccc} N \times H & \xrightarrow{(52)} & H \times_{G'} H & \mathcal{O}(N) \otimes \mathcal{O}(H) & \simeq & \mathcal{O}(H) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) \\ \downarrow & & \downarrow & \uparrow & & \uparrow \\ M \times H & \xrightarrow{(55)} & G \times_{G'} H & \mathcal{O}(M) \otimes \mathcal{O}(H) & \simeq & \mathcal{O}(G) \otimes_{\mathcal{O}(G')} \mathcal{O}(H). \end{array}$$

we see that $(\mathcal{O}(G) \rightarrow \mathcal{O}(H)) \otimes_{\mathcal{O}(G')} \mathcal{O}(H)$ is faithfully flat. As $\mathcal{O}(G') \rightarrow \mathcal{O}(H)$ is faithfully flat, this implies that $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is faithfully flat (CA 9.4).

GENERAL CASE

We show in (8.25) below that A and B are directed unions of finitely generated Hopf subalgebras A_i and B_i such that $A_i \subset B_i$. As B_i is flat as an A_i -module for all i , B is flat as an A -module (CA 9.13). For the faithful flatness, we use the statement (CA 9.10b):

$$A \rightarrow B \text{ faithfully flat} \Leftrightarrow \mathfrak{m}B \neq B, \text{ all maximal ideals } \mathfrak{m} \subset A \Leftrightarrow \mathfrak{a}B \neq B, \text{ all proper ideals } \mathfrak{a} \subset A.$$

Let \mathfrak{m} be a maximal ideal in A . If $1 \in \mathfrak{m}B$, then $1 \in (\mathfrak{m} \cap A_i)B_i$ for some i . But $\mathfrak{m} \cap A_i \neq A_i$, and so this contradicts the faithful flatness of B_i over A_i . Hence $\mathfrak{m}B \neq B$, and B is faithfully flat over A .

COROLLARY 6.44 *Let $A \subset B$ be Hopf algebras with B an integral domain, and let $K \subset L$ be their fields of fractions. Then $B \cap K = A$; in particular, $A = B$ if $K = L$.*

PROOF. Because B is faithfully flat over A , $cB \cap A = cA$ for any $c \in A$. Therefore, if $a/c \in B$, $a, c \in A$, then $a \in cB \cap A = cA$, and so $a/c \in A$. \square

ASIDE 6.45 Some statements have easy geometric proofs for smooth algebraic groups. In extending the proof to all algebraic groups, one often has to make a choice between a nonelementary (sometimes difficult) proof using algebraic geometry, and an elementary but uninformative proof using Hopf algebras. In general, we sketch the easy geometric proof for smooth algebraic groups, and give the elementary Hopf algebra proof in detail.

NOTES In most of the literature, for example, Borel 1991, Humphreys 1975, and Springer 1998, ‘‘algebraic group’’ means ‘‘smooth algebraic group’’ in our sense. Our approach is similar to that in Demazure and Gabriel 1970 and Waterhouse 1979. The important Theorem 6.31 was announced in a footnote to Cartier 1962; the direct proof presented here follows Oort 1966. Theorem 6.43 is proved entirely in the context of Hopf algebras in Takeuchi 1972; the proof presented here follows Waterhouse 1979, Chapter 14.

7 Group theory: subgroups and quotient groups.

In this section and in Section 9, we show how the basic definitions and theorems in the theory of abstract groups can be extended to affine groups. Throughout, k is a field.

7a A criterion to be an isomorphism

PROPOSITION 7.1 *A homomorphism of affine groups $\alpha: H \rightarrow G$ is an isomorphism if and only if*

- (a) *the map $\alpha(R): H(R) \rightarrow G(R)$ is injective for all k -algebras R , and*
- (b) *the homomorphism $\alpha^*: \mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is injective.*

PROOF. The conditions are obviously necessary. For the sufficiency, note that the maps

$$H \times_G H \rightrightarrows H \xrightarrow{\alpha} G$$

give rise to homomorphisms of Hopf algebras

$$\mathcal{O}(G) \rightarrow \mathcal{O}(H) \rightrightarrows \mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H).$$

In particular, the homomorphisms

$$\left. \begin{array}{l} x \mapsto x \otimes 1 \\ x \mapsto 1 \otimes x \end{array} \right\} : \mathcal{O}(H) \rightarrow \mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H) \quad (56)$$

agree on $\mathcal{O}(G)$, and so define elements of $H(\mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H))$ mapping to the same element in $G(\mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H))$. Now,

- ◇ condition (a) with $R = \mathcal{O}(H) \otimes_{\mathcal{O}(G)} \mathcal{O}(H)$ implies that the two homomorphisms (56) are equal, and
- ◇ condition (b) implies that $\mathcal{O}(H)$ is a faithfully flat $\mathcal{O}(G)$ -algebra (see 6.43), and so the subset of $\mathcal{O}(H)$ on which the two homomorphisms (56) agree is $\alpha^*(\mathcal{O}(G))$ by (CA 9.6).

On combining these statements, we find that α^* is surjective, and so it is an isomorphism. \square

7b Injective homomorphisms

DEFINITION 7.2 A homomorphism $H \rightarrow G$ of affine groups is *injective* if the map $H(R) \rightarrow G(R)$ is injective for all k -algebras R . An injective homomorphism is also called an *embedding*.

PROPOSITION 7.3 *A homomorphism $\alpha: H \rightarrow G$ of affine groups is injective if and only if the map $\alpha^*: \mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is surjective.*

In other words, $\alpha: H \rightarrow G$ is injective if and only if the map $|\alpha|: |H| \rightarrow |G|$ of affine schemes is a closed immersion.

PROOF. \Rightarrow : The homomorphism α^* factors into homomorphisms of Hopf algebras

$$\mathcal{O}(G) \rightarrow \alpha^*(\mathcal{O}(G)) \hookrightarrow \mathcal{O}(H)$$

(see Exercise 5-10). Let H' be the affine group whose Hopf algebra is $\alpha^*(\mathcal{O}(G))$. Then α factors into

$$H \rightarrow H' \rightarrow G,$$

and the injectivity of α implies that $H(R) \rightarrow H'(R)$ is injective for all k -algebras R . Because $\mathcal{O}(H') \rightarrow \mathcal{O}(H)$ is injective, Proposition 7.1 shows that the map $H \rightarrow H'$ is an isomorphism, and so $\alpha^*(\mathcal{O}(G)) = \mathcal{O}(H)$.

\Leftarrow : If α^* is surjective, then any two homomorphisms $\mathcal{O}(H) \rightarrow R$ that become equal when composed with α^* must already be equal, and so $H(R) \rightarrow G(R)$ is injective. \square

PROPOSITION 7.4 *Let $\alpha: H \rightarrow G$ be a homomorphism of affine groups. If α is injective, then so also is $\alpha_{k'}: H_{k'} \rightarrow G_{k'}$ for any field k' containing k . Conversely, if $\alpha_{k'}$ is injective for one field k' containing k , then α is injective.*

PROOF. For any field k' containing k , the map $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is surjective if and only if the map $k' \otimes_k \mathcal{O}(G) \rightarrow k' \otimes_k \mathcal{O}(H)$ is surjective (this is simply a statement about vector spaces over fields). \square

7.5

When k is a perfect field, G_{red} is an affine subgroup of G (see 6.18). However, it need not be normal. For example, over a field k of characteristic 3, let $G = \mu_3 \rtimes (\mathbb{Z}/2\mathbb{Z})_k$ for the nontrivial action of $(\mathbb{Z}/2\mathbb{Z})_k$ on μ_3 ; then $G_{\text{red}} = (\mathbb{Z}/2\mathbb{Z})_k$, which is not normal in G (see SGA3 VI_A 0.2).

7c Affine subgroups

DEFINITION 7.6 An *affine subgroup* (resp. *normal affine subgroup*) of an affine group G is a closed subfunctor H of G such that $H(R)$ is a subgroup (resp. normal subgroup) of $G(R)$ for all R .

In other words, a subfunctor H of an affine group G is an affine subgroup of G if

- ◇ $H(R)$ is a subgroup of $G(R)$ for all k -algebras R , and
- ◇ H is representable (in which case it is represented by a quotient of $\mathcal{O}(G)$ — see 7.3).

REMARK 7.7 An affine subgroup H of an algebraic group G is an algebraic group, because $\mathcal{O}(H)$ is a quotient of the finitely generated k -algebra $\mathcal{O}(G)$.

PROPOSITION 7.8 *The affine subgroups of an affine group G are in natural one-to-one correspondence with the Hopf ideals on $\mathcal{O}(G)$.*

PROOF. For an affine subgroup H of G ,

$$I(H) = \{f \in \mathcal{O}(G) \mid f_R(h) = 1 \text{ for all } h \in H(R) \text{ and all } R\}$$

is a Hopf ideal in G (it is the kernel of $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$; see Exercise 5-10). Conversely, if \mathfrak{a} is a Hopf ideal in G , then the functor

$$R \rightsquigarrow \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \mathfrak{a}\}$$

is an affine subgroup $G(\mathfrak{a})$ of $\mathcal{O}(G)$ (it is represented by $\mathcal{O}(G)/\mathfrak{a}$). The maps $H \mapsto I(H)$ and $\mathfrak{a} \mapsto G(\mathfrak{a})$ are inverse. \square

COROLLARY 7.9 *Every set of affine subgroups of an algebraic group G has a minimal element (therefore every descending chain of affine subgroups becomes stationary).*

PROOF. The ring $\mathcal{O}(G)$ is noetherian (Hilbert basis theorem, CA 3.6). \square

PROPOSITION 7.10 *For any affine subgroup H of an algebraic group G , the algebraic scheme $|H|$ is closed in $|G|$.*

PROOF. If \mathfrak{a} is the kernel of $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$, then $|H|$ is the subspace $V(\mathfrak{a}) \stackrel{\text{def}}{=} \{\mathfrak{m} \mid \mathfrak{m} \supset \mathfrak{a}\}$ of $|G|$. \square

PROPOSITION 7.11 *For any family $(H_j)_{j \in J}$ of affine subgroups of an affine group G , the functor*

$$R \rightsquigarrow \bigcap_{j \in J} H_j(R) \quad (\text{intersection inside } G(R))$$

is an affine subgroup $\bigcap_{j \in J} H_j$ of G , with coordinate ring $\mathcal{O}(G)/I$ where I is the ideal generated by the ideals $I(H_j)$.

PROOF. We have

$$H_j(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in I(H_j)\}.$$

Therefore,

$$\begin{aligned} H(R) &= \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \bigcup I(H_j)\} \\ &= \text{Hom}(\mathcal{O}(G)/I, R). \end{aligned} \quad \square$$

EXAMPLE 7.12 The intersection of the affine subgroups SL_n and \mathbb{G}_m (scalar matrices) of GL_n is μ_n (matrices $\text{diag}(c, \dots, c)$ with $c^n = 1$).

We sometimes loosely refer to an injective homomorphism $\alpha: H \rightarrow G$ as an affine subgroup of G .

DEFINITION 7.13 An affine subgroup H of algebraic group G is said to be **characteristic** if, for all k -algebras R and all automorphisms α of G_R , $\alpha(H_R) = H_R$ (cf. DG II, §1, 3.9). If the condition holds only when R is a field, we say that H is **characteristic in the weak sense**.

Both conditions are stronger than requiring that $\alpha(H) = H$ for all automorphisms of G (see 16.15).

7.14 In the realm of not necessarily affine group schemes over a field, there can exist non-affine (necessarily nonclosed) subgroup schemes of an affine algebraic group. For example, the constant subgroup scheme $(\mathbb{Z})_k$ of \mathbb{G}_a over \mathbb{Q} is neither closed nor affine. Worse, the (truly) constant subfunctor $R \rightsquigarrow \mathbb{Z} \subset R$ of \mathbb{G}_a is not representable. Over an algebraically closed field k consider the discrete (nonaffine) group scheme with underlying set k ; the obvious map $k \rightarrow \mathbb{G}_a$ of nonaffine group schemes is a homomorphism, and it is both mono and epi, but it is not an isomorphism.

7.14

7d Kernels of homomorphisms

The *kernel* of a homomorphism $\alpha: H \rightarrow G$ of affine groups is the functor

$$R \rightsquigarrow N(R) \stackrel{\text{def}}{=} \text{Ker}(\alpha(R): H(R) \rightarrow G(R)).$$

Let $\epsilon: \mathcal{O}(G) \rightarrow k$ be the identity element of $G(k)$. Then an element $h: \mathcal{O}(H) \rightarrow R$ of $H(R)$ lies in $N(R)$ if and only if its composite with $\alpha^*: \mathcal{O}(G) \rightarrow \mathcal{O}(H)$ factors through ϵ :

$$\begin{array}{ccc} \mathcal{O}(H) & \xleftarrow{\alpha^*} & \mathcal{O}(G) \\ \downarrow h & & \downarrow \epsilon \\ R & \xleftarrow{\quad\quad\quad} & k. \end{array}$$

Let I_G be the kernel of $\epsilon: \mathcal{O}(G) \rightarrow k$ (this is called the *augmentation ideal*), and let $I_G \cdot \mathcal{O}(H)$ denote the ideal generated by its image in $\mathcal{O}(H)$. Then the elements of $N(R)$ correspond to the homomorphisms $\mathcal{O}(H) \rightarrow R$ that are zero on $I_G \cdot \mathcal{O}(H)$, i.e.,

$$N(R) = \text{Hom}_{k\text{-alg}}(\mathcal{O}(H)/I_G \mathcal{O}(H), R).$$

We have proved:

PROPOSITION 7.15 For any homomorphism $H \rightarrow G$ of affine groups, there is an affine subgroup N of H (called the *kernel* of the homomorphism) such that

$$N(R) = \text{Ker}(H(R) \rightarrow G(R))$$

for all R ; its coordinate ring is $\mathcal{O}(H)/I_G \mathcal{O}(H)$.

Alternatively, note that the kernel of α is the fibred product of $H \rightarrow G \leftarrow *$, and so it is an algebraic group with coordinate ring

$$\mathcal{O}(H) \otimes_{\mathcal{O}(G)} (\mathcal{O}(G)/I_G) \simeq \mathcal{O}(H)/I_G \mathcal{O}(H)$$

(see §4b).

EXAMPLE 7.16 Consider the map $g \mapsto g^n: \mathbb{G}_m \rightarrow \mathbb{G}_m$. This corresponds to the map on Hopf algebras $Y \mapsto X^n: k[Y, Y^{-1}] \rightarrow k[X, X^{-1}]$ because

$$X^n(g) = g^n = Y(g^n)$$

(cf. (14), p.25). The map $\epsilon: k[Y, Y^{-1}] \rightarrow k$ sends $f(Y)$ to $f(1)$, and so the augmentation ideal for \mathbb{G}_m is $(Y - 1)$. Thus, the kernel has coordinate ring

$$k[X, X^{-1}]/(X^n - 1) \simeq k[X]/(X^n - 1).$$

In other words, the kernel is the algebraic group μ_n , as we would expect.

EXAMPLE 7.17 Let N be the kernel of the determinant map $\det: \mathrm{GL}_n \rightarrow \mathbb{G}_m$. This corresponds to the map on Hopf algebras

$$X \mapsto \det(X_{ij}): k[X, X^{-1}] \rightarrow k[\dots, X_{ij}, \dots, \det(X_{ij})^{-1}]$$

because

$$\det(X_{ij})(a_{ij}) = \det(a_{ij}) = X(\det(a_{ij})).$$


As we just noted, the augmentation ideal for \mathbb{G}_m is $(X - 1)$, and so

$$\mathcal{O}(N) = \frac{k[\dots, X_{ij}, \dots, \det(X_{ij})^{-1}]}{(\det(X_{ij}) - 1)} \simeq \frac{k[\dots, X_{ij}, \dots]}{(\det(X_{ij}) - 1)}.$$

In other words, the kernel of \det is the algebraic group SL_n , as we would expect.

PROPOSITION 7.18 When k has characteristic zero, a homomorphism $G \rightarrow H$ is injective if and only if $G(k^{\mathrm{al}}) \rightarrow H(k^{\mathrm{al}})$ is injective.

PROOF. If $G(k^{\mathrm{al}}) \rightarrow H(k^{\mathrm{al}})$ is injective, the kernel N of the homomorphism has the property that $N(k^{\mathrm{al}}) = 0$, and so it is the trivial algebraic group (by 6.32). \square

7.19 Proposition 7.18 is false for fields k of characteristic $p \neq 0$. For example, the homomorphism $x \mapsto x^p: \mathbb{G}_a \rightarrow \mathbb{G}_a$ has kernel α_p , and so it is not injective, but the map $x \mapsto x^p: \mathbb{G}_a(R) \rightarrow \mathbb{G}_a(R)$ is injective for every reduced k -algebra R . 

REMARK 7.20 Let A be an object of some category \mathcal{A} . A morphism $u: S \rightarrow A$ is a **monomorphism** if $f \mapsto u \circ f: \mathrm{Hom}(T, S) \rightarrow \mathrm{Hom}(T, A)$ is injective for all objects T . Two monomorphisms $u: S \rightarrow A$ and $u': S' \rightarrow A$ are said to be **equivalent** if each factors through the other. This is an equivalence relation on the monomorphisms with target A , and an equivalence class of monomorphisms is called a **subobject** of A .

A homomorphism of affine groups is a injective if and only if it is a monomorphism in the category of affine groups. To see this, let $\alpha: H \rightarrow G$ be a homomorphism of affine groups. If α is injective and the homomorphisms $\beta, \gamma: H' \rightarrow H$ agree when composed with α , then (7.1a) with $R = \mathcal{O}(H')$ shows that $\beta = \gamma$. Suppose, on the other hand, that α is not injective, so that its kernel N is nontrivial. Then the homomorphisms $n \mapsto 1$, $n \mapsto n: N \rightarrow N$ are distinct, but they agree when composed with α , and so α is not a monomorphism.

Let G be an affine group. Two monomorphisms $u: H \rightarrow G$ and $u': H' \rightarrow G$ are equivalent if and only if $\mathrm{Im}(u_R) = \mathrm{Im}(u'_R)$ for all k -algebras R . It follows that, in each equivalence class of monomorphisms with target G , there is exactly one with H an affine subgroup of G and with u the inclusion map.

ASIDE 7.21 In any category, the equalizer of a pair of morphisms is a monomorphism. A monomorphism that arises in this way is said to be *regular*. In Grp, every monomorphism is regular (see, for example, van Oosten, Basic Category Theory, Exercise 42, p.21). For example, the centralizer of an element a of a group A (which is not a normal subgroup in general) is the equalizer of the homomorphisms $x \mapsto x, x \mapsto axa^{-1}: A \rightarrow A$. Is it true that every monomorphism in the category of affine (or algebraic) groups is regular?

7e Dense subgroups

Let G be an algebraic group over a field k . By definition, a point $a \in G(k)$ is a homomorphism $\mathcal{O}(G) \rightarrow k$, whose kernel we denote \mathfrak{m}_a (a maximal ideal in $\mathcal{O}(G)$). As we discussed §6f, the map $a \mapsto \mathfrak{m}_a: G(k) \rightarrow |G|$ is injective with image the set of maximal ideals \mathfrak{m} of $\mathcal{O}(G)$ such that $\mathcal{O}(G)/\mathfrak{m} = k$. We endow $G(k)$ with the subspace topology.

PROPOSITION 7.22 *Let G be an algebraic group over a field k , and let Γ be a subgroup of $G(k)$. There exists an affine subgroup H of G such that $H(k) = \Gamma$ if and only if Γ is closed, in which case there exists a unique smallest H with this property. When k is algebraically closed, every smooth affine subgroup of G arises in this way.*

PROOF. If $\Gamma = H(k)$ for an affine subgroup H of G , then $\Gamma = |H| \cap G(k)$, which is closed by (7.10). Conversely, let Γ be a closed subgroup of $G(k)$. Each $f \in \mathcal{O}(G)$ defines a function $\Gamma \rightarrow k$, and, for $x, y \in \Gamma$, $(\Delta f)(x, y) = f(x \cdot y)$ (see (13), p. 25). Therefore, when we let $R(\Gamma)$ denote the k -algebra of maps $\Gamma \rightarrow k$ and define $\Delta_\Gamma: R(\Gamma) \times R(\Gamma) \rightarrow R(\Gamma \times \Gamma)$ as in Exercise 5-1, we obtain a commutative diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{\Delta_G} & \mathcal{O}(G) \otimes \mathcal{O}(G) \\ \downarrow & & \downarrow \\ R(\Gamma) & \xrightarrow{\Delta_\Gamma} & R(\Gamma \times \Gamma), \end{array}$$

which shows that Δ_Γ maps into $R(\Gamma) \otimes R(\Gamma)$, and so $(R(\Gamma), \Delta_\Gamma)$ is a Hopf algebra (ibid.). Because Γ is closed, it is the zero set of the ideal

$$\mathfrak{a} \stackrel{\text{def}}{=} \text{Ker}(\mathcal{O}(G) \rightarrow R(\Gamma)),$$

which is a Hopf ideal because $(\mathcal{O}(G), \Delta_G) \rightarrow (R(\Gamma), \Delta_\Gamma)$ is a homomorphism of Hopf algebras (5.16). The affine subgroup H of G with $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a} \subset R(\Gamma)$ has $H(k) = \Gamma$. Clearly, it is the smallest subgroup of G with this property. When k is algebraically closed and H is a smooth subgroup of G , then the group attached to $\Gamma = H(k)$ is H itself. \square

REMARK 7.23 For any subgroup Γ of $G(k)$, the closure $\bar{\Gamma}$ of Γ in $G(k) \subset |G|$ is a closed subgroup of $G(k)$.²¹ The smallest affine subgroup H of G such that $H(k) = \bar{\Gamma}$ is often called the “Zariski closure” of Γ in G .

²¹It is a general fact that the closure of a subgroup Γ of a topological group is a subgroup. To see this, note that for a fixed $c \in \Gamma$, the maps $x \mapsto cx$ and $x \mapsto x^{-1}$ are continuous, and hence are homeomorphisms because they have inverses of the same form. For $c \in \Gamma$, we have $\Gamma c = \Gamma$, and so $\bar{\Gamma} c = \bar{\Gamma}$. As c is arbitrary, this says that $\bar{\Gamma} \cdot \Gamma = \bar{\Gamma}$. For $d \in \bar{\Gamma}$, $d\Gamma \subset \bar{\Gamma}$, and so $d\bar{\Gamma} \subset \bar{\Gamma}$. We have shown that $\bar{\Gamma} \cdot \bar{\Gamma} \subset \bar{\Gamma}$. Because $x \mapsto x^{-1}$ is a homeomorphism, it maps $\bar{\Gamma}$ onto $(\Gamma^{-1})^-$. Therefore $\bar{\Gamma}^{-1} = (\Gamma^{-1})^- = \bar{\Gamma}$.

REMARK 7.24 When k is not algebraically closed, not every smooth algebraic subgroup of G arises from a closed subgroup of $G(k)$. Consider, for example, the algebraic subgroup $\mu_n \subset \mathbb{G}_m$ over \mathbb{Q} . If n is odd, then $\mu_n(\mathbb{Q}) = \{1\}$, and the algebraic group attached to $\{1\}$ is the trivial group.

REMARK 7.25 It is obvious from its definition that $R(\Gamma)$ has no nonzero nilpotents. Therefore the affine subgroup attached to a closed subgroup Γ of $G(k)$ is reduced, and hence smooth if k is perfect. In particular, no nonsmooth subgroup arises in this way.

DEFINITION 7.26 Let G be an algebraic group over a field k , and let k' be a field containing k . We say that a subgroup Γ of $G(k')$ is *dense* in G if the only affine subgroup H of G such that $H(k') \supset \Gamma$ is G itself.

7.27 If $\Gamma \subset G(k')$ is dense in G , then, for any field $k'' \supset k'$, $\Gamma \subset G(k'')$ is dense in G .

7.28 If $G(k)$ is dense in G , then G is reduced, hence smooth if k is perfect (see 7.25).

7.29 It follows from the proof of (7.22) that $G(k)$ is dense in G if and only if

$$f \in \mathcal{O}(G), f(P) = 0 \text{ for all } P \in G(k) \implies f = 0. \quad (57)$$

In other words, $G(k)$ is dense in G if and only if no nonzero element of $\mathcal{O}(G)$ maps to zero under all homomorphisms of k -algebras $\mathcal{O}(G) \rightarrow k$:

$$\bigcap_{\alpha: \mathcal{O}(G) \rightarrow k} \text{Ker}(\alpha) = 0.$$

7.30 For an affine algebraic variety V over a field k , any $f \in \mathcal{O}(V)$ such that $f(P) = 0$ for all $V(k^{\text{al}})$ is zero (Nullstellensatz; CA 11.5); better, any $f \in \mathcal{O}(V)$ such that $f(P) = 0$ for all $P \in V(k^{\text{sep}})$ is zero (AG 11.15). Therefore, if G is smooth, then $G(k^{\text{sep}})$ (a fortiori, $G(k^{\text{al}})$) is dense in G .

7.31 If $G(k)$ is finite, for example, if the field k is finite, and $\dim G > 0$, then $G(k)$ is never dense in G .

PROPOSITION 7.32 *If k is infinite, then $G(k)$ is dense in G when $G = \mathbb{G}_a, \text{GL}_n$, or SL_n .*

PROOF. We use the criterion (7.29). Because k is infinite, no nonzero polynomial in $k[X_1, \dots, X_n]$ can vanish on all of k^n (FT, proof of 5.18). This implies that no nonzero polynomial f can vanish on a set of the form

$$D(h) \stackrel{\text{def}}{=} \{a \in k^n \mid h(a) \neq 0\}, \quad h \neq 0,$$

because otherwise hf would vanish on k^n . As

$$\text{GL}_n(k) = \{a \in k^{n^2} \mid \det(a) \neq 0\},$$

this proves the proposition for GL_n .

The proposition is obvious for \mathbb{G}_a , and it can be proved for SL_n by realizing $\mathcal{O}(\mathrm{SL}_n)$ as a subalgebra of $\mathcal{O}(\mathrm{GL}_n)$. Specifically, the natural bijection

$$A, r \mapsto A \cdot \mathrm{diag}(r, 1, \dots, 1): \mathrm{SL}_n(R) \times \mathbb{G}_m(R) \rightarrow \mathrm{GL}_n(R)$$

(of set-valued functors) defines an isomorphism of k -algebras

$$\mathcal{O}(\mathrm{GL}_n) \simeq \mathcal{O}(\mathrm{SL}_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

and the algebra on the right contains $\mathcal{O}(\mathrm{SL}_n)$. Hence

$$\bigcap_{\alpha: \mathcal{O}(\mathrm{SL}_n) \rightarrow k} \mathrm{Ker}(\alpha) \subset \bigcap_{\alpha: \mathcal{O}(\mathrm{GL}_n) \rightarrow k} \mathrm{Ker}(\alpha) = 0. \quad \square$$

PROPOSITION 7.33 *Let G be an algebraic group over a perfect field k , and let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. Then Γ acts on $G(k^{\mathrm{al}})$, and $H \leftrightarrow H(k^{\mathrm{al}})$ is a one-to-one correspondence between the smooth subgroups of G and the closed subgroups of $G(k^{\mathrm{al}})$ stable under Γ .*

PROOF. Combine (7.22) with (4.13). (More directly, both correspond to radical Hopf ideals \mathfrak{a} in the k^{al} -bialgebra $k^{\mathrm{al}} \otimes \mathcal{O}(G)$ stable under the action of Γ ; see AG 16.7, 16.8). \square

ASIDE 7.34 Let k be an infinite field. We say that a finitely generated k -algebra has “enough maps to k ” if $\bigcap_{\alpha: A \rightarrow k} \mathrm{Ker}(\alpha) = 0$ (intersection over k -algebra homomorphisms $A \rightarrow k$). We saw in the proof of (7.32) that $k[X_1, \dots, X_n]_h$ has enough maps to k for any $h \neq 0$. Obviously, any subalgebra of an algebra having enough maps to k also has enough maps to k . In particular, any subalgebra of $k[X_1, \dots, X_n]_h$ has enough maps to k . A connected affine variety V is said to be **unirational** if $\mathcal{O}(V)$ can be realized as a subalgebra $k[X_1, \dots, X_n]_h$ in such a way that the extension of the fields of fractions is finite. Geometrically, this means that there is a finite map from an open subvariety of \mathbb{A}^n onto an open subvariety of V . Clearly, if V is unirational, then $\mathcal{O}(V)$ has enough maps to k . Therefore, if a connected algebraic group G is unirational, then $G(k)$ is dense in G . So which algebraic groups are unirational? In SGA3, XIV 6.11 we find:

One knows (Rosenlicht) examples of forms of \mathbb{G}_a over a nonperfect field, which have only finitely many rational points, and therefore a fortiori are not unirational. Moreover Chevalley has given an example of a torus over a field of characteristic zero which is not a rational variety. On the other hand, it follows from the Chevalley’s theory of semisimple groups that over an algebraically closed field, every smooth connected affine algebraic group is a rational variety.

Borel 1991, 18.2, proves that a connected smooth algebraic group G is unirational if k is perfect or if G is reductive. For a nonunirational nonconnected algebraic group, Rosenlicht gives the example of the group of matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ over \mathbb{R} with $a^2 + b^2 = \pm 1$. For a nonunirational connected algebraic group, Rosenlicht gives the example of the subgroup of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $Y^p - Y = tX^p$ over the field $k = k_0(t)$ (t transcendental). On the other hand, if $k[\sqrt{a}, \sqrt{b}]$ has degree 4 over k , then the norm torus²² associated with this extension is a three-dimensional torus that is not a rational variety. Proofs of these statements will be given in a future version of the notes.

²²Let $T = (\mathbb{G}_m)_{k[\sqrt{a}, \sqrt{b}]/k}$. The norm map defines a homomorphism $T \rightarrow \mathbb{G}_m$, and the norm torus is the kernel of this homomorphism.

ASIDE 7.35 (mo56192) Rosenlicht's subgroup $Y^p - Y = tX^p$ of $\mathbb{G}_a \times \mathbb{G}_a$ ($p \neq 2$) and the subgroup $Y^p = tX^p$ of $\mathbb{G}_a \times \mathbb{G}_a$ are examples of algebraic groups G over k such that $G(k)$ is not dense in G (the first is smooth; the second is reduced but not smooth).

A smooth, connected unipotent group is said to be k -split if there is a filtration by k -subgroups for which the successive quotients are isomorphic to \mathbb{G}_a . The examples in the above paragraph are non-split unipotent groups. Any smooth connected k -split unipotent group U is even a rational variety (in fact, k -isomorphic as a variety to \mathbb{A}^n), and so it is clear that $U(k)$ is Zariski dense in U when k is infinite. More generally, let G be a smooth connected affine algebraic group over k and assume that the unipotent radical of $G_{k^{\text{al}}}$ is defined and split over k (both of these conditions can fail). Then as a k -variety, G is just the product of its reductive quotient ($G/R_u G$) and its unipotent radical (result of Rosenlicht). In particular, G is unirational, and if k is infinite, then $G(k)$ is dense in G (George McNinch)

A necessary condition when k is imperfect: if $G(k)$ is dense in G , then G_{red} is a smooth algebraic group over k . Proof: the regular locus of G_{red} is open and non-empty, so contains a rational point. This point is then smooth. By translation, G_{red} is smooth at origin, hence smooth everywhere. This implies that it is an algebraic group because it is geometrically reduced (Qing Liu).

ASIDE 7.36 Let k be a commutative ring. Waterhouse 1979, 1.2, p. 5 defines an *affine group scheme* to be representable functor from k -algebras to groups. He defines an affine group scheme to be *algebraic* if its representing algebra is finitely generated (ibid. 3.3, p. 24). Now assume that k is a field. He defines an *algebraic matrix group* over k to be a Zariski-closed subgroup of $\text{SL}_n(k)$ for some n (ibid., 4.2, p. 29), and he defines an *affine algebraic group* to be a closed subset of k^n some n with a group law on it for which the multiplication and inverse are polynomial maps (ibid. 4.2, p. 29). Algebraic matrix groups and affine algebraic groups define (essentially the same) affine group schemes.

Waterhouse 1979	This work
affine group scheme	affine group
algebraic affine group scheme	affine algebraic group (or just algebraic group)
algebraic matrix group	affine subgroup G of $\text{GL}_{n,k}$ such that $G(k)$ is dense in G
affine algebraic group	algebraic group G such that $G(k)$ is dense in G .

We shall sometimes use *algebraic matrix group* to mean an affine subgroup G of $\text{GL}_{n,k}$ such that $G(k)$ is dense in G .

ASIDE 7.37 Before Borel introduced algebraic geometry into the theory of algebraic groups in a more systematic way, Chevalley defined algebraic groups to be closed subsets of k^n endowed with a group structure defined by polynomial maps. In other words, he studied affine algebraic groups and algebraic matrix groups in the above sense. Hence, effectively he studied reduced algebraic groups G with the property that $G(k)$ is dense in G .

ASIDE 7.38 In the literature one finds statements:

When k is perfect, any algebraic subgroup of GL_n defined by polynomials with coefficients in k is automatically defined over k (e.g., Borel 1991, Humphreys 1975).

What is meant is the following:

When k is perfect, any smooth algebraic subgroup G of $\text{GL}_{n,k^{\text{al}}}$ such the subset $G(k^{\text{al}})$ of $\text{GL}_n(k^{\text{al}})$ is defined by polynomials with coefficients in k arises from a smooth algebraic subgroup of $\text{GL}_{n,k}$.

From our perspective, the condition on $G(k^{\text{al}})$ (always) implies that G arises from a reduced algebraic subgroup of $\text{GL}_{n,k}$, which is smooth if k is perfect.

7f Normalizers; centralizers; centres

For a subgroup H of an abstract group G , we let $N_G(H)$ (resp. $C_G(H)$) denote the normalizer (resp. centralizer) of H in G , and we let $Z(G)$ denote the centre of G . In this subsection, we extend these notions to an affine subgroup H of an affine group G over a field k .

For $g \in G(R)$, let ${}^g H$ be the functor of R -algebras

$$R' \rightsquigarrow g \cdot H(R') \cdot g^{-1} \quad (\text{subset of } G(R')).$$

Define N to be the functor of k -algebras

$$R \rightsquigarrow \{g \in G(R) \mid {}^g H = H\}.$$

Thus, for any k -algebra R ,

$$\begin{aligned} N(R) &= \{g \in G(R) \mid g \cdot H(R') \cdot g^{-1} = H(R') \text{ for all } R\text{-algebras } R'\} \\ &= G(R) \cap \bigcap_{R'} N_{G(R')}(H(R')). \end{aligned}$$

PROPOSITION 7.39 *The functor N is an affine subgroup of G .*

PROOF. Clearly $N(R)$ is a subgroup of $G(R)$, and so it remains to show that N is representable by a quotient of $\mathcal{O}(G)$. Clearly

$$g \cdot H(R') \cdot g^{-1} = H(R') \iff g \cdot H(R') \cdot g^{-1} \subset H(R') \text{ and } g^{-1} \cdot H(R') \cdot g \subset H(R'),$$

and so, when we let G act on itself by conjugation,

$$N = T_G(H, H) \cap T_G(H, H)^{-1}$$

(notations as in §6n). Proposition 6.36 shows that $T_G(H, H)$ is representable, and it follows from (7.11) that N is representable by a quotient of $\mathcal{O}(G)$. \square

The affine subgroup N of G is called the **normalizer** $N_G(H)$ of H in G . It is obvious from its definition that the formation of $N_G(H)$ commutes with extension of the base field: for any field $k' \supset k$,

$$N_G(H)_{k'} \simeq N_{G_{k'}}(H_{k'}).$$

PROPOSITION 7.40 *If H is an affine subgroup of an algebraic group G , and $H(k')$ is dense in H for some field $k' \supset k$, then*

$$N_G(H)(k) = G(k) \cap N_{G(k')}(H(k')).$$

PROOF. Let $g \in G(k) \cap N_{G(k')}(H(k'))$. Because $g \in G(k)$, ${}^g H$ is an algebraic subgroup of G , and so ${}^g H \cap H$ is an algebraic subgroup of H . Because $g \in N_{G(k')}(H(k'))$,

$$({}^g H)(k') = H(k'),$$

and so $({}^g H \cap H)(k') = H(k')$. As $H(k')$ is dense in H , this implies that ${}^g H \cap H = H$, and so ${}^g H = H$. \square

COROLLARY 7.41 *Let H be a smooth affine subgroup of a smooth algebraic group G . If $H(k^{\text{sep}})$ is normal in $G(k^{\text{sep}})$, then H is normal in G .*

PROOF. Because H is smooth, $H(k^{\text{sep}})$ is dense in H , and so (7.40) shows that $N_G(H)(k^{\text{sep}}) = G(k^{\text{sep}})$, and so $N_G(H) = G$. \square



7.42 The corollary is false without the smoothness assumptions, even with k^{al} for k^{sep} . For example, let H be the subgroup of SL_2 in characteristic $p \neq 0$ such that

$$H(R) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid pa = 0 \right\}$$

(so $H \simeq \alpha_p$). Then $H(k^{\text{al}}) = 1$, but H is not normal in SL_2 .

PROPOSITION 7.43 *Let H be an affine subgroup of an algebraic group G .*

- (a) H is normal in G if and only if $N_G(H) = G$.
- (b) Let i_g denote the inner automorphism of G defined by $g \in G(k)$; if $G(k)$ is dense in G and $i_g(H) = H$ for all $g \in G(k)$, then H is normal in G .

PROOF. (a) This is obvious from the definitions.

(b) Let $N = N_G(H) \subset G$. If $i_g(H) = H$, then $g \in N(k)$. The hypotheses imply that $G(k) \subset N(k)$, and so $N = G$. \square

Let H be an affine subgroup of an affine group G , and let N be the normalizer of H . Each $n \in N(R)$ defines a natural transformation i_n

$$h \mapsto nhn^{-1}: H(R') \rightarrow H(R')$$

of H regarded as a functor from the category of R -algebras to sets, and we define C to be the functor of k -algebras

$$R \rightsquigarrow \{n \in N(R) \mid i_n = \text{id}_H\}.$$

Thus,

$$C(R) = G(R) \cap \bigcap_{R'} C_{G(R')}(H(R')).$$

PROPOSITION 7.44 *The functor C is an affine subgroup of G .*

PROOF. We have to show that C is representable. Let G act on $G \times G$ by

$$g(g_1, g_2) = (g_1, gg_2g^{-1}), \quad g, g_1, g_2 \in G(R),$$

and embed H diagonally in $G \times G$,

$$H \rightarrow G \times G, \quad h \mapsto (h, h) \text{ for } h \in H(R).$$

Then

$$C = T_{G \times G}(H, H),$$

which is representable by (6.36). \square

The affine subgroup C of G is called the **centralizer** $C_G(H)$ of H in G . It is obvious from its definition that the formation of $C_G(H)$ commutes with extension of the base field: for any field $k' \supset k$,

$$C_G(H)_{k'} \simeq C_{G_{k'}}(H_{k'}).$$

PROPOSITION 7.45 *If H is an affine subgroup of an algebraic group G , and $H(k')$ is dense in H for some field $k' \supset k$, then*

$$C_G(H)(k) = G(k) \cap C_{G(k')}(H(k')).$$

PROOF. Let $n \in G(k) \cap C_{G(k')}(H(k'))$. According to (7.40), $n \in N_G(H)(k)$. The maps i_n and id_H coincide on an affine subgroup of H , which contains $H(k')$, and so equals H . Therefore $n \in C_G(H)(k)$. \square

COROLLARY 7.46 *Let H be a smooth affine subgroup of a smooth algebraic group G . If $H(k^{\text{sep}})$ is central in $G(k^{\text{sep}})$, then H is central in G .*

PROOF. Because H is smooth, $H(k^{\text{sep}})$ is dense in H , and so (7.45) shows that $C_G(H)(k^{\text{sep}}) = G(k^{\text{sep}})$, and so $C_G(H) = G$. \square

The **centre** $Z(G)$ of an affine group G is defined to be $C_G(G)$. It is an affine subgroup of G , and if G is algebraic and $G(k')$ is dense in G , then

$$Z(G)(k) = G(k) \cap Z(G(k')).$$

7.47 Even when G and H are smooth, $C_G(H)$ need not be smooth. For example, it is possible for $C_G(H)$ to be nontrivial but for $C_G(H)(k')$ to be trivial for all fields $k' \supset k$. To see this, let G be the functor

$$R \rightsquigarrow R \times R^\times$$

with the multiplication $(a, u)(b, v) = (a + bu^p, uv)$; here $0 \neq p = \text{char}(k)$. This is an algebraic group because, as a functor to sets, it is isomorphic to $\mathbb{G}_a \times \mathbb{G}_m$. For a pair $(a, u) \in R \times R^\times$, $(a, u)(b, v) = (b, v)(a, u)$ for all (b, v) if and only if $u^p = 1$. Therefore, the centre of G is μ_p , and so $Z(G)(k') = 1$ for all fields k' containing k . Another example is provided by SL_p over a field of characteristic p . The centre of SL_p is μ_p , which is not smooth.

EXAMPLE 7.48 For a k -algebra R , the usual argument shows that the centre of $\text{GL}_n(R)$ is the group of nonzero diagonal matrices. Therefore

$$Z(\text{GL}_n) = \mathbb{G}_m \quad (\text{embedded diagonally}).$$

More abstractly, for any finite-dimensional vector space V ,

$$Z(\text{GL}_V) = \mathbb{G}_m \quad (a \in \mathbb{G}_m(R) \text{ acts on } V_R \text{ as } v \mapsto av).$$

EXAMPLE 7.49 Let $G = \text{GL}_n$ over a field k . For an integer N , let H_N be the subfunctor

$$R \rightsquigarrow H_N(R) = \{\text{diag}(a_1, \dots, a_n) \in \text{GL}_n(R) \mid a_1^N = \dots = a_n^N = 1\}.$$

of G . Then $H_N \simeq (\mu_N)^n$, and so it is an affine subgroup of G . For N sufficiently large

$$C_G(H_N) = \mathbb{D}_n$$

(group of diagonal matrices) (see (14.35)). We consider two cases.

(a) $k = \mathbb{Q}$ and N odd. Then $H_N(k) = \{1\}$, and

$$C_{G(k)}(H_N(k)) = \mathrm{GL}_n(k) \neq \mathbb{D}_n(k) = C_G(H_N)(k).$$

(b) k is algebraically closed of characteristic $p \neq 0$ and N is a power of p . Then $H_N(k) = 1$ and

$$C_{G(k)}(H_N(k)) = \mathrm{GL}_n(k) \neq \mathbb{D}_n(k) = C_G(H_N)(k).$$

An affine subgroup H of an affine group G is said to **normalize** (resp. **centralize**) an affine subgroup N of G if $H(R)$ normalizes (resp. centralizes) $N(R)$ for all k -algebras R ; equivalently, if $H \subset N_G(N)$ (resp. $H \subset C_G(N)$).

7g Quotient groups; surjective homomorphisms

What does it mean for a homomorphism of algebraic groups $G \rightarrow Q$ to be surjective? One might guess that it means that $G(R) \rightarrow Q(R)$ is surjective for all R , but this condition is too stringent. For example, it would say that $x \mapsto x^n: \mathbb{G}_m \rightarrow \mathbb{G}_m$ is not surjective even though $x \mapsto x^n: \mathbb{G}_m(k) \rightarrow \mathbb{G}_m(k)$ is surjective whenever k is algebraically closed. In fact, $\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$ is surjective according to the following definition.

DEFINITION 7.50 A homomorphism $G \rightarrow Q$ is said to be **surjective** (and Q is called a **quotient** of G) if for every k -algebra R and $q \in Q(R)$, there exists a faithfully flat R -algebra R' and a $g \in G(R')$ mapping to the image of q in $Q(R')$:

$$\begin{array}{ccc} G(R') & \longrightarrow & Q(R') & \quad \exists g \longmapsto * \\ \downarrow & & \downarrow & \quad \uparrow \\ G(R) & \longrightarrow & Q(R) & \quad q. \end{array}$$

In other words, a homomorphism $G \rightarrow Q$ is surjective if every $q \in Q(R)$ lifts to G after a faithfully flat extension. A surjective homomorphism is also called a **quotient map**.

THEOREM 7.51 A homomorphism $G \rightarrow Q$ is surjective if and only if $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is injective.

PROOF. \Rightarrow : Consider the “universal” element $\mathrm{id}_{\mathcal{O}(Q)} \in Q(\mathcal{O}(Q))$. If $G \rightarrow Q$ is surjective, there exists a $g \in G(R')$ with R' faithfully flat over $\mathcal{O}(Q)$ such that g and $\mathrm{id}_{\mathcal{O}(Q)}$ map to the same element of $Q(R')$, i.e., such that the diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \longleftarrow & \mathcal{O}(Q) \\ \downarrow g & & \downarrow \mathrm{id}_{\mathcal{O}(Q)} \\ R' & \xleftarrow{\text{faithfully flat}} & \mathcal{O}(Q) \end{array}$$

commutes. The map $\mathcal{O}(Q) \rightarrow R'$, being faithfully flat, is injective (CA 9.6), which implies that $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is injective.

\Leftarrow : According to (6.43) $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is faithfully flat. Let $q \in Q(R)$. Regard q as a homomorphism $\mathcal{O}(Q) \rightarrow R$, and form the tensor product $R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R$:

$$\begin{array}{ccc}
 \mathcal{O}(G) & \xleftarrow{\text{faithfully flat}} & \mathcal{O}(Q) \\
 \downarrow g = 1 \otimes q & \swarrow q' & \downarrow q \\
 R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R & \xleftarrow{\quad} & R
 \end{array} \tag{58}$$

Then R' is a faithfully flat R -algebra because $\mathcal{O}(G)$ is a faithfully flat $\mathcal{O}(H)$ -algebra (apply CA 9.7). The commutativity of the square in (58) means that $g \in G(R')$ maps to the image q' of q in $Q(R')$. \square

PROPOSITION 7.52 *Let $\alpha: H \rightarrow G$ be a homomorphism of affine groups. If α is surjective, then so also is $\alpha_{k'}: H_{k'} \rightarrow G_{k'}$ for any field k' containing k . Conversely, if $\alpha_{k'}$ is surjective for one field k' containing k , then α is surjective.*

PROOF. Because $k \rightarrow k'$ is faithfully flat, the map $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is injective if and only if $k' \otimes_k \mathcal{O}(G) \rightarrow k' \otimes_k \mathcal{O}(H)$ is injective (see CA 9.2). \square

PROPOSITION 7.53 *A homomorphism of affine groups that is both injective and surjective is an isomorphism.*

PROOF. The map on coordinate rings is both surjective and injective, and hence is an isomorphism. \square

PROPOSITION 7.54 *Let $G \rightarrow Q$ be a homomorphism of algebraic groups. If $G \rightarrow Q$ is a quotient map, then $G(k^{\text{al}}) \rightarrow Q(k^{\text{al}})$ is surjective; the converse is true if Q is smooth.*

PROOF. Let $q \in Q(k^{\text{al}})$. For some finitely generated k^{al} -algebra R , the image of q in $Q(R)$ lifts to an element g of $G(R)$. Zariski's lemma (CA 11.1) shows that there exists a k^{al} -algebra homomorphism $R \rightarrow k^{\text{al}}$, and the image of g in $G(k^{\text{al}})$ maps to $q \in Q(k^{\text{al}})$:


$$\begin{array}{ccc}
 G(R) & \longrightarrow & G(k^{\text{al}}) \\
 \downarrow & & \downarrow \\
 Q(k^{\text{al}}) & \longrightarrow & Q(R) \longrightarrow Q(k^{\text{al}})
 \end{array}
 \quad
 \begin{array}{ccc}
 g & \longmapsto & g_{k^{\text{al}}} \\
 \downarrow & & \downarrow \\
 q & \longmapsto & q_R \longmapsto q
 \end{array}$$

$$\begin{array}{ccc}
 & \text{id} & \\
 & \curvearrowright & \\
 k^{\text{al}} & \longrightarrow & R \longrightarrow k^{\text{al}}
 \end{array}$$

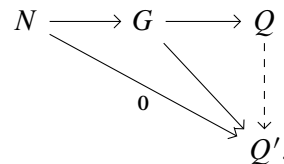
For the converse, we may suppose that k is algebraically closed. Recall (2.16) that an element f of $\mathcal{O}(Q)$ is a family $(f_R)_R$ with f_R a map $Q(R) \rightarrow R$. Because Q is

smooth, $\mathcal{O}(Q)$ is reduced, and so f is determined by f_k (CA 11.8). As $G(k) \rightarrow Q(k)$ is surjective, f is determined by the composite $G(k) \rightarrow Q(k) \xrightarrow{f_k} k$, and so $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is injective. \square

More generally, a homomorphism $\alpha: G \rightarrow H$ of algebraic groups is surjective if, for some field k' containing k , the image of $G(k')$ in $H(k')$ is dense in H (see 9.8 below).

7.55 The smoothness condition in the second part of the proposition is necessary. Let k be a field of characteristic $p \neq 0$, and consider the homomorphism $1 \rightarrow \alpha_p$ where 1 denotes the trivial algebraic group. The map $1(k^{\text{al}}) \rightarrow \alpha_p(k^{\text{al}})$ is $\{1\} \rightarrow \{1\}$, which is surjective, but $1 \rightarrow \alpha_p$ is not a quotient map because the map on coordinate rings is $k[X]/(X^p) \rightarrow k$, which is not injective. 

THEOREM 7.56 *Let $G \rightarrow Q$ be a quotient map with kernel N . Then any homomorphism $G \rightarrow Q'$ whose kernel contains N factors uniquely through Q :*



PROOF. Note that, if g and g' are elements of $G(R)$ with the same image in $Q(R)$, then $g^{-1}g'$ lies in N and so maps to 1 in $Q'(R)$. Therefore g and g' have the same image in $Q'(R)$. This shows that the composites of the homomorphisms

$$G \times_Q G \rightrightarrows G \rightarrow Q'$$

are equal. Therefore, the composites of the homomorphisms

$$\mathcal{O}(G) \otimes_{\mathcal{O}(Q)} \mathcal{O}(G) \rightrightarrows \mathcal{O}(G) \leftarrow \mathcal{O}(Q')$$

are equal. The subring of $\mathcal{O}(G)$ on which the two maps coincide is $\mathcal{O}(Q)$ (CA 9.6), and so the map $\mathcal{O}(Q') \rightarrow \mathcal{O}(G)$ factors through uniquely through $\mathcal{O}(Q) \hookrightarrow \mathcal{O}(G)$. Therefore $G \rightarrow Q'$ factors uniquely through $G \rightarrow Q$. \square

COROLLARY 7.57 *If $\theta: G \rightarrow Q$ and $\theta': G \rightarrow Q'$ are quotient maps with the same kernel, then there is a unique homomorphism $\alpha: Q \rightarrow Q'$ such that $\alpha \circ \theta = \theta'$; moreover, α is an isomorphism.*

PROOF. From the theorem, there are unique homomorphisms $\alpha: Q \rightarrow Q'$ and $\alpha': Q' \rightarrow Q$ such that $\alpha \circ \theta = \theta'$ and $\alpha' \circ \theta' = \theta$. Now $\alpha' \circ \alpha = \text{id}_Q$, because both have the property that $\beta \circ \theta = \theta$. Similarly, $\alpha \circ \alpha' = \text{id}_{Q'}$, and so α and α' are inverse isomorphisms. \square

DEFINITION 7.58 A surjective homomorphism $G \rightarrow Q$ with kernel N is called the **quotient of G by N** , and Q is denoted by G/N .

When it exists, the quotient is uniquely determined up to a unique isomorphism by the universal property in (7.56). We shall see later (8.77) that quotients by normal subgroups always exist.

DEFINITION 7.59 A sequence

$$1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$$

is *exact* if $G \rightarrow Q$ is a quotient map with kernel N .

PROPOSITION 7.60 If

$$1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$$

is exact, then

$$\dim G = \dim N + \dim Q.$$

PROOF. For any homomorphism $\alpha: G \rightarrow Q$ of abstract groups, the map

$$(n, g \mapsto (ng, g): \text{Ker}(\alpha) \times G \rightarrow G \times_Q G$$

is a bijection — this just says that two elements of G with the same image in Q differ by an element of the kernel. In particular, for any homomorphism $\alpha: G \rightarrow Q$ of affine groups and k -algebra R , there is a bijection

$$\text{Ker}(\alpha)(R) \times G(R) \rightarrow (G \times_Q G)(R),$$

which is natural in R . Therefore $N \times G \simeq G \times_Q G$,²³ and so

$$\mathcal{O}(N) \otimes \mathcal{O}(G) \simeq \mathcal{O}(G \times_Q G).$$

Recall that the dimension of an algebraic group G has the following description: according to the Noether normalization theorem (CA 5.11), there exists a finite set S of elements in $\mathcal{O}(G)$ such that $k[S]$ is a polynomial ring in the elements of S and $\mathcal{O}(G)$ is finitely generated as a $k[S]$ -module; the cardinality of S is $\dim G$. Since $\mathcal{O}(G \times_Q G) = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} \mathcal{O}(G)$, it follows from this description that

$$\dim(G \times_Q G) = 2 \dim G - \dim Q.$$

Therefore $2 \dim G - \dim Q = \dim N + \dim G$, from which the assertion follows. \square

ASIDE 7.61 Proposition 7.60 can also be proved geometrically. First make a base extension to k^{al} . For a surjective map $\varphi: G \rightarrow Q$ of irreducible algebraic schemes, the dimension of the fibre over a closed point P of Q is equal $\dim(G) - \dim Q$ for P in a nonempty open subset of Q (cf. AG 10.9b). Now use homogeneity (I, §6h) to see that, when $G \rightarrow Q$ is a homomorphism of algebraic group schemes, all the fibres have the same dimension.

²³This duplicates (52), p. 70.

ASIDE 7.62 A morphism $u: A \rightarrow B$ in a category \mathbf{A} is said to be an **epimorphism** if $\text{Hom}(B, T) \rightarrow \text{Hom}(A, T)$ is injective for all objects T .

It is obvious from Theorem 7.51 that a surjective homomorphism of affine groups is an epimorphism. The converse is true for groups (MacLane 1971, Exercise 5 to I 5), but it is false for affine groups. For example, the embedding

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \hookrightarrow \left\{ \begin{pmatrix} * & * \\ * & * \end{pmatrix} \right\} = \text{GL}_2$$

is a nonsurjective epimorphism (any two homomorphisms from GL_2 that agree on B are equal).²⁴

7h Existence of quotients

PROPOSITION 7.63 *Let G be an algebraic group, and let H be an affine subgroup of G . There exists a surjective homomorphism $G \rightarrow Q$ containing H in its kernel and universal among homomorphisms with this property.*

PROOF. For any finite family $(G \xrightarrow{q_i} Q_i)_{i \in I}$ of surjective morphisms such that $H \subset \text{Ker}(q_i)$ all i , let $H_I = \bigcap_{i \in I} \text{Ker}(q_i)$. According to (7.9), there exists a family for which H_I is minimal. For such a family, I claim that the map from G to the image of $(q_i): G \rightarrow \prod_{i \in I} Q_i$ is universal. If it isn't, then there exists a homomorphism $q: G \rightarrow Q$ containing H in its kernel but not H_I . But then $H_{I \cup \{q\}} = H_I \cap \text{Ker}(q)$ is properly contained in H_I . \square

Later (8.70), we shall show that, when H is normal, the kernel of the universal homomorphism $G \rightarrow Q$ is exactly H .

7i Semidirect products

DEFINITION 7.64 An affine group G is said to be a **semidirect product** of its affine subgroups N and Q , denoted $G = N \rtimes Q$, if N is normal in G and the map $(n, q) \mapsto nq: N(R) \times Q(R) \rightarrow G(R)$ is a bijection of sets for all k -algebras R .

In other words, G is a semidirect product of its affine subgroups N and Q if $G(R)$ is a semidirect product of its subgroups $N(R)$ and $Q(R)$ for all k -algebras R (cf. GT 3.7).

For example, let \mathbb{T}_n be the algebraic group of upper triangular matrices, so

$$\mathbb{T}_n(R) = \{(a_{ij}) \in \text{GL}_n(R) \mid a_{ij} = 0 \text{ for } i > j\}.$$

Then \mathbb{T}_n is the semidirect product of its (normal) subgroup \mathbb{U}_n and its subgroup \mathbb{D}_n .

PROPOSITION 7.65 *Let N and Q be affine subgroups of an affine group G . Then G is the semidirect product of N and Q if and only if there exists a homomorphism $G \rightarrow Q$ whose restriction to Q is the identity map and whose kernel is N .*

²⁴This follows from the fact that $\text{GL}_2/B \simeq \mathbb{P}^1$. Let f, f' be two homomorphisms $\text{GL}_2 \rightarrow G$. If $f|_B = f'|_B$, then $g \mapsto f'(g) \cdot f(g)^{-1}$ defines a map $\mathbb{P}^1 \rightarrow G$, which has image 1_G because G is affine and \mathbb{P}^1 is complete (see AG 7.5).

Alternatively, in characteristic zero, one can show that any homomorphism of $B \cap \text{SL}_2$ has at most one extension to SL_2 because any finite dimensional representation of \mathfrak{sl}_2 can be reconstructed from the operators h and y . Specifically, if $hv = mv$ and $y^{m+1}v = 0$, then $xv = 0$; if $hv = mv$ and $u = y^n v$, then $xy^n v$ can be computed as usual using that $[x, y] = h$.

PROOF. \Rightarrow : By assumption, the product map is a bijection of functors $N \times Q \rightarrow G$. The composite of the inverse of this map with the projection $N \times Q \rightarrow Q$ has the required properties.

\Leftarrow : Let $\varphi: G \rightarrow Q$ be the given homomorphism. For each k -algebra R , $\varphi(R)$ realizes $G(R)$ as a semidirect product $G(R) = N(R) \rtimes Q(R)$ of its subgroups $N(R)$ and $Q(R)$. \square

Let G be an affine group and X a functor from the category of k -algebras to sets. Recall §6n that an action of G on X is a natural transformation $\theta: G \times X \rightarrow X$ such that each map $G(R) \times X(R) \rightarrow X(R)$ is an action of the group $G(R)$ on the set $X(R)$. Now let N and Q be algebraic groups and suppose that there is given an action of Q on N

$$(q, n) \mapsto \theta_R(q, n): Q(R) \times N(R) \rightarrow N(R)$$

such that, for each q , the map $n \mapsto \theta_R(q, n)$ is a group homomorphism. Then the functor

$$R \rightsquigarrow N(R) \rtimes_{\theta_R} Q(R)$$

(cf. GT 3.9) is an affine group because, as a functor to sets, it is $N \times Q$, which is represented by $\mathcal{O}(N) \otimes \mathcal{O}(Q)$. We denote it by $N \rtimes_{\theta} Q$, and call it the *semidirect product of N and Q defined by θ* .

7j Smooth algebraic groups

PROPOSITION 7.66 *Quotients and extensions of smooth algebraic groups are smooth.*

PROOF. Let Q be the quotient of G by the affine subgroup N . Then $Q_{k^{\text{al}}}$ is the quotient of $G_{k^{\text{al}}}$ by $N_{k^{\text{al}}}$. If G is smooth, $\mathcal{O}(G_{k^{\text{al}}})$ is reduced; as $\mathcal{O}(Q_{k^{\text{al}}}) \subset \mathcal{O}(G_{k^{\text{al}}})$, it also is reduced, and so Q is smooth. For extensions, we (at present) appeal to algebraic geometry: let $W \rightarrow V$ be a regular map of algebraic varieties; if V is smooth and the fibres of the map are smooth subvarieties of W with constant dimension, then W is smooth (?; tba). \square



7.67 The kernel of a homomorphism of smooth algebraic groups need not be smooth. For example, in characteristic p , the kernels of $x \mapsto x^p: \mathbb{G}_m \rightarrow \mathbb{G}_m$ and $x \mapsto x^p: \mathbb{G}_a \rightarrow \mathbb{G}_a$ are not smooth (they are μ_p and α_p respectively).

7k Algebraic groups as sheaves

Some of the above discussion simplifies when regard affine groups as sheaves.

PROPOSITION 7.68 *Let F be a functor from the category of k -algebras to sets. If F is representable, then*

- (F1) *for every finite family of k -algebras $(R_i)_{i \in I}$, the canonical map $F(\prod_i R_i) \rightarrow \prod_i F(R_i)$ is bijective;*
- (F2) *for every faithfully flat homomorphism $R \rightarrow R'$ of k -algebras, the sequence*

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

is exact (i.e., the first arrow realizes $F(R)$ as the equalizer of the pair of arrows).

PROOF. (F1). For any k -algebra A , it follows directly from the definition of product that

$$\mathrm{Hom}(A, \prod_{i \in I} R_i) \simeq \prod_{i \in I} \mathrm{Hom}(A, R_i),$$

(F2). If $R \rightarrow R'$ is faithfully flat, then it is injective, and so

$$\mathrm{Hom}(A, R) \rightarrow \mathrm{Hom}(A, R')$$

is injective for any k -algebra A . According to (CA 9.5), the sequence

$$R \rightarrow R' \rightrightarrows R' \otimes_R R'$$

is exact, and it follows that

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

is exact. □

A functor satisfying the conditions (F1) and (F2) is said to be a *sheaf for the flat topology*²⁵.

PROPOSITION 7.69 *A functor $F: \mathrm{Alg}_k \rightarrow \mathrm{Set}$ is a sheaf if and only if it satisfies the following condition:*

(S) *for every k -algebra R and finite family $(R_i)_{i \in I}$ of k -algebras such that $R \rightarrow \prod_i R_i$ is faithfully flat, the sequence*

$$F(R) \rightarrow \prod_{i \in I} F(R_i) \rightrightarrows \prod_{(i, i') \in I \times I} F(R_i \otimes_k R_{i'})$$

is exact.

PROOF. Easy exercise (cf. Milne 1980, II 1.5). □

We sometimes use (S1) to denote the condition that $F(R) \rightarrow \prod_{i \in I} F(R_i)$ is injective and (S2) for the condition that its image is subset on which the pair of maps agree.

PROPOSITION 7.70 *For any functor $F: \mathrm{Alg}_k \rightarrow \mathrm{Set}$, there exists a sheaf aF and a natural transformation $F \rightarrow aF$ that is universal among natural transformations from F to sheaves.*

PROOF. For $a, b \in F(R)$, set $a \sim b$ if a and b have the same image in $F(R')$ for some faithfully flat R -algebra R' . Then \sim is an equivalence relation on $F(R)$, and the functor $R \rightsquigarrow F(R)/\sim$ satisfies (S1). Moreover, any natural transformation from F to a sheaf will factor uniquely through $F \rightarrow F/\sim$.

Now let F be a functor satisfying (S1). For any k -algebra R , define

$$F'(R) = \varinjlim \mathrm{Ker}(F(R') \rightrightarrows F(R' \otimes_R R')).$$

where R' runs over the faithfully flat R -algebras. One checks easily that F' is a sheaf, and that any natural transformation from F to a sheaf factors uniquely through $F \rightarrow F'$. □

²⁵Strictly, for the fpqc (fidèlement plat quasi-compacte) topology.

The sheaf aF is called the *associated sheaf* of F .

PROPOSITION 7.71 *Let S be a sheaf, and let F be a subfunctor of S . If*

$$S(R) = \bigcup_{R' \text{ a faithfully flat } R\text{-algebra}} (S(R) \cap F(R'))$$

(intersection inside $S(R')$), then S is the sheaf associated with F .

PROOF. Obviously any natural transformation $F \rightarrow F'$ with F' a sheaf extends uniquely to S . □

Let \mathbf{P} be the category of functors $\text{Alg}_k \rightarrow \text{Set}$, and let \mathbf{S} be the full subcategory of \mathbf{P} consisting of the sheaves.

PROPOSITION 7.72 *The inclusion functor $i: \mathbf{S} \rightarrow \mathbf{P}$ preserves inverse limits; the functor $a: \mathbf{P} \rightarrow \mathbf{S}$ preserves direct limits and finite inverse limits.*

PROOF. By definition $\text{Hom}(a(-), -) \simeq \text{Hom}(-, i(-))$, and so a and i are adjoint functors. This implies (immediately) that i preserves inverse limits and a preserves direct limits. To show that a preserves finite inverse limits, it suffices to show that it preserves finite products and equalizers, which follows from the construction of a . □

PROPOSITION 7.73 *Let $G \rightarrow Q$ be a surjective homomorphism of affine groups with kernel N . Then Q represents the sheaf associated with the functor*

$$R \rightsquigarrow G(R)/N(R).$$

PROOF. Let P be the functor $R \rightsquigarrow G(R)/N(R)$. Then P commutes with products, and we shall show:

- (a) For any injective homomorphism $R \rightarrow R'$ of k -algebras, the map $P(R) \rightarrow P(R')$ is injective.
- (b) Let

$$P'(R) = \lim_{\substack{\longrightarrow \\ R'}} \text{Ker}(P(R') \rightrightarrows P(R' \otimes_R R'))$$

where the limit is over all faithfully flat R -algebras; then $P' \simeq Q$.

For (a), we have to prove that

$$N(R) = N(R') \cap G(R) \quad (\text{intersection inside } G(R')).$$

For some index set I , $N(R)$ is the subset of R^I defined by some polynomial conditions

$$f_j(\dots, X_i, \dots) = 0$$

and $N(R')$ is the subset of R'^I defined by the same polynomial conditions. But if an element of R^I satisfies the conditions when regarded as an element of R'^I , then it already satisfies the conditions in R^I (because $R \rightarrow R'$ is injective).

For (b), consider the diagram

$$\begin{array}{ccccc} K(R') & \rightarrow & P(R') & \rightrightarrows & P(R' \otimes_R R') \\ & & \downarrow & & \downarrow \\ Q(R) & \rightarrow & Q(R') & \rightrightarrows & Q(R' \otimes_R R') \end{array}$$

where $K(R')$ is the equalizer of the top pair of maps — we know that $Q(R)$ is the equalizer of the bottom pair of maps. For any k -algebra R' , the map $P(R') \rightarrow Q(R')$ is injective, and so the two vertical arrows induce an injective homomorphism $K(R') \rightarrow Q(R)$. When we pass to the limit over R' , it follows directly from the definition of “surjective” (see 7.50) that this map becomes surjective. \square

NOTES (a) Explain why it is useful to regard the affine groups as sheaves rather than presheaves.

(b) Explain the set-theoretic problems with (7.70) (limit over a proper class), and why we don’t really need the result (or, at least, we can avoid the problems). See Waterhouse 1975.

71 Limits of affine groups

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

THEOREM 7.74 *Let F be a functor from a small category I to the category of affine groups over k ; then the functor*

$$R \rightsquigarrow \varprojlim F(R) \tag{59}$$

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

PROOF. Denote the functor (59) by \underline{F} ; thus $\underline{F}(R)$ is the inverse limit of the functor $i \rightsquigarrow F_i(R)$ from I to the category of (abstract) groups. It is easy to see that $\underline{F} = \varprojlim F$ in the category of functors from k -algebras to groups, and it will follow that \underline{F} is the inverse limit in the category of affine groups once we show that it is an affine group. But \underline{F} is equal to the equalizer of two homomorphisms

$$\prod_{i \in \text{ob}(I)} F_i \rightrightarrows \prod_{u \in \text{ar}(I)} F_{\text{target}(u)} \tag{60}$$

(MacLane 1971, V 2 Theorem 2, p.109). Both products are affine groups, and we saw in (§4b) that equalizers exist in the category of affine groups. \square

In particular, inverse limits of algebraic groups exist as affine groups. Later (8.23) we shall see that every affine group arises in this way.

THEOREM 7.75 *Let F be a functor from a finite category I to the category of algebraic groups over k ; then the functor*

$$R \rightsquigarrow \varprojlim F_i(R) \tag{61}$$

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

PROOF. Both products in (60) are algebraic groups. \square

Direct limits, even finite direct limits, are more difficult. For example, the sum of two groups is their free product, but when G_1 and G_2 are algebraic groups, the functor $R \rightsquigarrow G_1(R) * G_2(R)$ will generally be far from being an algebraic group. Moreover, the functor $R \rightsquigarrow \varinjlim F_i(R)$ need not be a sheaf. Roughly speaking, when the direct limit of a system of affine groups exists, it can be constructed by forming the naive direct limit in the category of functors, and then forming the associated sheaf. For example, when N is a normal subgroup of an affine group G , the quotient affine group G/N is the sheaf associated with the functor $R \rightsquigarrow G(R)/N(R)$ (cf. 7.73).

7m Terminology

From now on, “subgroup” of an affine group will mean “affine subgroup”. Thus, if G is an affine (or algebraic) group, a subgroup H of G is again an affine (or algebraic) group, whereas a subgroup H of $G(k)$ is an abstract group.

7n Exercises

EXERCISE 7-1 Let A and B be subgroups of the affine group G , and let AB be the sheaf associated with the subfunctor $R \rightsquigarrow A(R) \cdot B(R)$ of G .

- Show that AB is representable by $\mathcal{O}(G)/\mathfrak{a}$ where \mathfrak{a} is the kernel of homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(A) \otimes \mathcal{O}(B)$ defined by the map $a, b \mapsto ab: A \times B \rightarrow G$ (of set-valued functors).
- Show that, for any k -algebra R , an element $G(R)$ lies in $(AB)(R)$ if and only if its image in $G(R')$ lies in $A(R') \cdot B(R')$ for some faithfully flat R -algebra R' , i.e.,

$$(AB)(R) = \bigcap_{R'} G(R) \cap (A(R') \cdot B(R')).$$

- Show that AB is a subgroup of G if B normalizes A .

EXERCISE 7-2 Let A, B, C be subgroups of an affine group G such that A is a normal subgroup of B . Show:

- $C \cap A$ is a normal subgroup of $C \cap B$;
- CA is a normal subgroup of CB .

EXERCISE 7-3 (Dedekind’s modular laws). Let A, B, C be subgroups of an affine group G such that A is a subgroup of B . Show:

- $B \cap AC = A(B \cap C)$;
- if $G = AC$, then $B = A(B \cap C)$.

8 Representations of affine groups

One of the main results in this section is that all algebraic groups can be realized as subgroups of GL_n for some n . At first sight, this is a surprising result, because it says that all possible multiplications in algebraic groups are just matrix multiplication in disguise.

In this section, we often work with algebraic monoids rather than groups since this forces us to distinguish between “left” and “right” correctly. Note that for a commutative ring R , the only difference between a left module and a right module is one of notation: it

is simply a question of whether we write rm or mr (or better $\overset{r}{m}$). In this section, it will sometimes be convenient to regard R -modules as right modules, and write $V \otimes_k R$ instead of $R \otimes_k V$. Throughout, k is a field.

8a Finite groups

We first look at how to realize a finite group G as a matrix group. A representation of G on a k -vector space V is a homomorphism of groups $G \rightarrow \text{Aut}_{k\text{-lin}}(V)$, or, in other words, an action $G \times V \rightarrow V$ of G on V in which each $\gamma \in G$ acts k -linearly. Let $X \times G \rightarrow X$ be a right action of G on a finite set X . Define V to be the k -vector space of maps $X \rightarrow k$, and let G act on V according to the rule:

$$(gf)(x) = f(xg) \quad \text{for } g \in G, f \in V, x \in X.$$

This defines a representation of G on V , which is faithful if G acts effectively on X . The vector space V has a canonical basis consisting of the maps that send one element of X to 1 and the remainder to 0, and so this gives a homomorphism $G \rightarrow \text{GL}_n(k)$ where n is the order of X . For example, for the symmetric group S_n acting on $\{1, 2, \dots, n\}$, this gives the map $\sigma \mapsto I(\sigma): S_n \rightarrow \text{GL}_n(k)$ in (§1a). When we take $X = G$, the vector space V is the k -algebra $\mathcal{O}(G)$ of maps $G \rightarrow k$, and the representation is called the **regular representation**.

8b Definition of a representation

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

$$\begin{aligned} V(R) &= V \otimes R, & (R\text{-module}) \\ \text{End}_V(R) &= \text{End}_{R\text{-lin}}(V(R)), & (\text{monoid under composition}) \\ \text{Aut}_V(R) &= \text{Aut}_{R\text{-lin}}(V(R)), & (\text{group under composition}). \end{aligned}$$

Then $R \rightsquigarrow \text{End}_V(R)$ is a functor from the category of k -algebras to monoids and $R \rightsquigarrow \text{Aut}_V(R)$ is a functor from the category of k -algebras to groups. With the terminology of (2.18), $\text{Aut}_V = \text{End}_V^\times$.

Let G be an affine monoid or group over k . A **linear representation** of G on a k -vector space V is a natural transformation $r: G \rightarrow \text{End}_V$ of functors $\text{Alg}_k \rightarrow \text{Mon}$. In other words, it is a family of homomorphisms of monoids

$$r_R: G(R) \rightarrow \text{End}_{R\text{-lin}}(V(R)), \quad R \text{ a } k\text{-algebra}, \quad (62)$$

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

$$\begin{array}{ccc} G(R) & \xrightarrow{r_R} & \text{End}_{R\text{-lin}}(V(R)) \\ \downarrow & & \downarrow \\ G(R') & \xrightarrow{r_{R'}} & \text{End}_{R'\text{-lin}}(V(R')) \end{array}$$

commutes. When G is an affine group, r takes values in Aut_V and is a natural transformation of group-valued functors. A linear representation is said to be **finite-dimensional** if V is finite-dimensional as a k -vector space, and it is **faithful** if all the homomorphisms r_R are injective. A subspace W of V is a **subrepresentation** if $r_R(g)(W(R)) \subset W(R)$ for all k -algebras R and all $g \in G(R)$.

A **homomorphism of linear representations** $(V, r) \rightarrow (V', r')$ is a k -linear map $\alpha: V \rightarrow V'$ such that

$$\begin{array}{ccc} V(R) & \xrightarrow{\alpha(R)} & V'(R) \\ \downarrow r_R(g) & & \downarrow r'_R(g) \\ V(R) & \xrightarrow{\alpha(R)} & V'(R) \end{array}$$

commutes for all $g \in G(R)$ and all k -algebras R .

We write V also for the functor $R \rightsquigarrow V(R)$ defined by V . Then a linear representation of G on V can also be defined as an action of G on V ,

$$G \times V \rightarrow V, \quad (63)$$

such that each $g \in G(R)$ acts R -linearly on $V(R)$.

When $V = k^n$, End_V is the monoid $R \rightsquigarrow (M_n(R), \times)$ and $\text{Aut}_V = \text{GL}_n$. A linear representation of an affine monoid (resp. group) G on V is a homomorphism $G \rightarrow (M_n, \times)$ (resp. $G \rightarrow \text{GL}_n$).

EXAMPLE 8.1 Let $G = \mathbb{G}_a$. Let V be a finite-dimensional k -vector space, and let $\rho_0, \dots, \rho_i, \dots$ be a sequence of endomorphisms V such that all but a finite number are zero. For $t \in R$, let

$$r_R(t) = \sum_{i \geq 0} \rho_i t^i \in \text{End}(V(R))$$

(so $r_R(t)(v \otimes c) = \sum \rho_i(v) \otimes ct^i$). If

$$\begin{cases} \rho_0 = \text{id}_V \\ \rho_i \circ \rho_j = \binom{i+j}{i} \rho_{i+j} \end{cases} \quad \text{all } i, j \geq 0, \quad (64)$$

then

$$r_R(t + t') = r_R(t) + r_R(t') \quad \text{for all } t, t' \in R,$$

and so r_R is a representation. We shall see later (8.15) that all finite-dimensional representations of \mathbb{G}_a are of this form. Note that (64) implies that $\rho_i \circ \rho_1 = (i+1)\rho_{i+1}$, and so $\rho_1^n = n!\rho_n$. When k has characteristic zero, this implies that ρ_1 is nilpotent and that $\rho_n = \rho_1^n/n!$, and so

$$r_R(t) = \sum (\rho_1 t)^n / n! = \exp(\rho_1 t).$$

When k has nonzero characteristic, there are more possibilities. See Abe 1980, p. 185.

EXAMPLE 8.2 Let $G = \text{GL}_n$, and let M_n denote the vector space of all $n \times n$ matrices with entries in k . The actions

$$(P, A) \mapsto PAP^{-1}: G(R) \times M_n(R) \rightarrow M_n(R)$$

define a linear representation of G on M_n . The orbits of $G(k)$ acting on $M_n(k)$ are the similarity classes, which are represented by the Jordan matrices when k is algebraically closed.

EXAMPLE 8.3 There is a unique linear representation r of G on $\mathcal{O}(G)$ (regarded as a k -vector space) such that

$$(gf)_R(x) = f_R(xg), \quad \text{for all } g \in G(R), f \in \mathcal{O}(G), x \in G(R). \quad (65)$$

This is called the **regular representation**. In more detail: the formula (65) defines a map $G(R) \times \mathcal{O}(G) \rightarrow R \otimes \mathcal{O}(G)$, which extends by linearity to a map $G(R) \times R \otimes \mathcal{O}(G) \rightarrow R \otimes \mathcal{O}(G)$.

8c Terminology

From now on, “representation” will mean “linear representation”.

8d Comodules

Let (A, m, e) be a k -algebra, not necessarily commutative. Recall that a left A -module is a k -vector space V together with a k -linear map $\mu: A \otimes V \rightarrow V$ such that the diagrams

$$\begin{array}{ccc}
 V & \xleftarrow{\mu} & A \otimes V \\
 \uparrow \mu & & \uparrow m \otimes V \\
 A \otimes V & \xleftarrow{A \otimes \mu} & A \otimes A \otimes V
 \end{array}
 \qquad
 \begin{array}{ccc}
 V & \xleftarrow{\mu} & A \otimes V \\
 \parallel & & \uparrow e \otimes V \\
 V & \xleftarrow{\simeq} & k \otimes V
 \end{array}
 \tag{66}$$

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

DEFINITION 8.4 Let (C, Δ, ϵ) be a k -coalgebra. A **right C -comodule**²⁶ is a k -linear map $\rho: V \rightarrow V \otimes C$ (called the **coaction** of C on V) such that the diagrams

$$\begin{array}{ccc}
 V & \xrightarrow{\rho} & V \otimes C \\
 \downarrow \rho & & \downarrow V \otimes \Delta \\
 V \otimes C & \xrightarrow{\rho \otimes C} & V \otimes C \otimes C
 \end{array}
 \qquad
 \begin{array}{ccc}
 V & \xrightarrow{\rho} & V \otimes C \\
 \parallel & & \downarrow V \otimes \epsilon \\
 V & \xrightarrow{\simeq} & V \otimes k
 \end{array}
 \tag{67}$$

commute, i.e., such that

$$\begin{cases}
 (V \otimes \Delta) \circ \rho = (\rho \otimes C) \circ \rho \\
 (V \otimes \epsilon) \circ \rho = V.
 \end{cases}$$

A **homomorphism** $\alpha: (V, \rho) \rightarrow (V', \rho')$ of C -comodules is a k -linear map $\alpha: V \rightarrow V'$ such that the diagram

$$\begin{array}{ccc}
 V & \xrightarrow{\alpha} & V' \\
 \downarrow \rho & & \downarrow \rho' \\
 V \otimes C & \xrightarrow{\alpha \otimes C} & V' \otimes C
 \end{array}$$

commutes. A comodule is said to be **finite-dimensional** if it is finite-dimensional as a k -vector space.

EXAMPLE 8.5 (a) The pair (C, Δ) is a right C -comodule (compare (29), p. 42, with (67)). More generally, for any k -vector space V ,

$$V \otimes \Delta: V \otimes C \rightarrow V \otimes C \otimes C$$

²⁶It would be more natural to consider left comodules, except that it is *right* comodules that correspond to *left* representations of monoids. Because we consider right comodules we are more-or-less forced to write $V \otimes R$ where elsewhere we write $R \otimes V$.

is a right C -comodule (called the **free comodule on V**). The choice of a basis for V realizes this as a direct sum of copies of (C, Δ) :

$$\begin{array}{ccc} V \otimes C & \xrightarrow{V \otimes \Delta} & V \otimes C \otimes C \\ \downarrow \approx & & \downarrow \approx \\ C^n & \xrightarrow{\Delta^n} & (C \otimes C)^n. \end{array}$$

(b) Let (V_1, ρ_1) and (V_2, ρ_2) be comodules over coalgebras C_1 and C_2 respectively. The map

$$V_1 \otimes V_2 \xrightarrow{\rho_1 \otimes \rho_2} V_1 \otimes C_1 \otimes V_2 \otimes C_2 \simeq V_1 \otimes V_2 \otimes C_1 \otimes C_2$$

provides $V_1 \otimes V_2$ with the structure of a $C_1 \otimes C_2$ -comodule.

(c) Let (V, ρ) be a right C -comodule, and let $\alpha: C \rightarrow C'$ be a homomorphism of coalgebras. The map

$$V \xrightarrow{\rho} V \otimes C \xrightarrow{V \otimes \alpha} V \otimes C'$$

provides V with the structure of a right C' -comodule.

(d) Let V be a k -vector space, and let $\rho: V \rightarrow V \otimes C$ be a k -linear map. Choose a basis $(e_i)_{i \in I}$ for V , and write

$$\rho(e_j) = \sum_{i \in I} e_i \otimes c_{ij}, \quad c_{ij} \in C, \quad (68)$$

(finite sum, so, for each j , almost all c_{ij} 's are zero). Then (V, ρ) is a right comodule if and only if²⁷

$$\left. \begin{array}{l} \Delta(c_{ij}) = \sum_{k \in I} c_{ik} \otimes c_{kj} \\ \epsilon(c_{ij}) = \delta_{ij} \end{array} \right\} \quad \text{all } i, j \in I. \quad (69)$$

For a module V over an algebra A , there is a smallest quotient of A , namely, the image of A in $\text{End}_k(V)$, through which the action of A on V factors. In the next remark, we show that for a comodule V over a coalgebra C , there is a smallest subcoalgebra C_V of C through which the co-action of C on V factors.

REMARK 8.6 Let (V, ρ) be a C -comodule.

(a) When we choose a k -basis $(e_i)_{i \in I}$ for V , the equations (69) show that the k -subspace spanned by the c_{ij} is a subcoalgebra of C , which we denote C_V . Clearly, C_V is the smallest subspace of C such that $\rho(V) \subset V \otimes C_V$, and so it is independent of the choice of the basis. When V is finite dimensional over k , so also is C_V .

(b) Recall that for a finite-dimensional k -vector space V ,

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

If $\rho \leftrightarrow \rho'$ under this isomorphism, then

$$\rho(v) = \sum_{i \in I} e_i \otimes c_i \implies \rho'(v \otimes f) = \sum_{i \in I} f(e_i) c_i.$$

²⁷The first equality can be written symbolically as

$$(\Delta(c_{ij})) = (c_{ik}) \otimes (c_{kj}).$$

In particular, $\rho'(e_j \otimes e_i^\vee) = c_{ij}$ (notation as in (68)). Therefore C_V is the image of $\rho': V \otimes V^\vee \rightarrow C$.

(c) If (V, ρ) is a sub-comodule of (C, Δ) , then $V \subset C_V$. To see this, note that the restriction of the co-identity ϵ of C to V is an element ϵ_V of V^\vee and that $\rho'(v \otimes \epsilon_V) = v$ for all $v \in V$ because

$$\begin{aligned} \rho'(e_j \otimes \epsilon_V) &= \sum_{i \in I} \epsilon(e_j) c_{ij} \\ &= (\epsilon \otimes \text{id}_C) \Delta(e_j) \\ &= (\text{id}_C \otimes \epsilon) \Delta(e_j) && \text{(by (29), p. 42)} \\ &= \sum_{i \in I} e_j \epsilon(c_{ij}) \\ &= e_j && \text{(by (69)).} \end{aligned}$$

REMARK 8.7 Recall (§5c) that the linear dual of a coalgebra (C, Δ, ϵ) is an algebra $(C^\vee, \Delta^\vee, \epsilon^\vee)$ (associative with identity). Let V be a k -vector space, and let $\rho: V \rightarrow V \otimes C$ be a k -linear map. Define μ to be the composite of

$$C^\vee \otimes V \xrightarrow{C^\vee \otimes \rho} C^\vee \otimes V \otimes C \simeq V \otimes C^\vee \otimes C \xrightarrow{V \otimes \text{ev}} V \otimes k \simeq V$$

where $\text{ev}: C^\vee \otimes C \rightarrow k$ is the evaluation map. One can check that (V, ρ) is a right C -comodule if and only if (V, μ) is a left C^\vee -module. When C and V are finite-dimensional, $\rho \mapsto \mu$ is a bijection

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

and so there is a one-to-one correspondence between the right C -comodule structures on V and the left C^\vee -module structures on V . In the general case, not every C^\vee -module structure arises from a C -comodule structure, but it is known which do (Dăscălescu et al. 2001, 2.2; Sweedler 1969, 2.1).

A k -subspace W of V is a **subcomodule** if $\rho(W) \subset W \otimes C$. Then $(W, \rho|_W)$ is itself a C -comodule.

PROPOSITION 8.8 *Every comodule (V, ρ) is a filtered union of its finite-dimensional sub-comodules.*

PROOF. As a finite sum of (finite-dimensional) sub-comodules is a (finite-dimensional) sub-comodule, it suffices to show that each element v of V is contained in a finite-dimensional sub-comodule. Let $(e_i)_{i \in I}$ be a basis for C as a k -vector space, and let

$$\rho(v) = \sum_i v_i \otimes e_i, \quad v_i \in V,$$

(finite sum, i.e., only finitely many v_i are nonzero). Write

$$\Delta(e_i) = \sum_{j,k} r_{ijk} (e_j \otimes e_k), \quad r_{ijk} \in k.$$

We shall show that

$$\rho(v_k) = \sum_{i,j} r_{ijk} (v_i \otimes e_j) \tag{70}$$

from which it follows that the k -subspace of V spanned by v and the v_i is a subcomodule containing v . Recall from (67) that

$$(V \otimes \Delta) \circ \rho = (\rho \otimes C) \circ \rho.$$

On applying each side of this equation to v , we find that

$$\sum_{i,j,k} r_{ijk}(v_i \otimes e_j \otimes e_k) = \sum_k \rho(v_k) \otimes e_k \quad (\text{inside } V \otimes C \otimes C).$$

On comparing the coefficients of $1 \otimes 1 \otimes e_k$ in these two expressions, we obtain (70). \square

COROLLARY 8.9 *A coalgebra C is a union of its sub-coalgebras C_V , where V runs over the finite-dimensional sub-comodules of C .*

PROOF. For any finite-dimensional sub-comodule V of C ,

$$V \subset C_V \subset C$$

(see 8.6), and so this follows from the proposition. \square

ASIDE 8.10 The main definitions in this subsection require only that k be a commutative ring. When k is noetherian, every comodule over a k -coalgebra C is a filtered union of finitely generated subcoalgebras (Serre 1993, 1.4).

8e The category of comodules

Let (C, Δ, ϵ) be a coalgebra over k . With the obvious definitions, the standard isomorphism theorems (cf. 9.1, 9.2, 9.3, 9.4 below) hold for comodules over C . For example, if (W, ρ_W) is a sub-comodule of (V, ρ_V) , then the quotient vector space V/W has a (unique) comodule structure $\rho_{V/W}$ for which $(V, \rho_V) \rightarrow (V/W, \rho_{V/W})$ is a homomorphism. In particular, the sub-comodules are exactly the kernels of homomorphism of comodules. The category of comodules over C is abelian and the forgetful functor to k -vector spaces is exact.

A bialgebra structure (m, e) on C defines a tensor product structure on the category of comodules over C : when (V_1, ρ_1) and (V_2, ρ_2) are C -comodules, $V_1 \otimes V_2$ has a natural structure of a $C \otimes C$ -comodule (see 8.5b), and the homomorphism of coalgebras $m: C \otimes C \rightarrow C$ turns this into a C -comodule structure (see 8.5c). The tensor product of the empty family of comodules is the **trivial comodule** $(k, k \xrightarrow{e} C \simeq k \otimes C)$. The forgetful functor preserves tensor products.

Assume that V is finite dimensional. Under the canonical isomorphisms

$$\text{Hom}_{k\text{-lin}}(V, V \otimes C) \simeq \text{Hom}_{k\text{-lin}}(V \otimes V^\vee, C) \simeq \text{Hom}_{k\text{-lin}}(V^\vee, C \otimes V^\vee), \quad (71)$$

a right coaction ρ on V corresponds to left coaction ρ' on V^\vee . When C is a Hopf algebra, the inversion can be used to turn ρ' into a right coaction ρ^\vee : define ρ^\vee to be the composite

$$V^\vee \xrightarrow{\rho'} A \otimes V^\vee \xrightarrow{t} V^\vee \otimes A \xrightarrow{V^\vee \otimes S} V^\vee \otimes A. \quad (72)$$

The pair (V^\vee, ρ^\vee) is called the **dual** or **contragredient** of (V, ρ) . The forgetful functor preserves duals.

SUMMARY 8.11 Let C be a k -coalgebra.

- ◇ The finite-dimensional comodules over C form an abelian category $\text{Comod}(C)$.
- ◇ A bialgebra structure on C provides $\text{Comod}(C)$ with a tensor product structure.
- ◇ A Hopf algebra structure on C provides $\text{Comod}(C)$ with a tensor product structure and duals.

8f Representations and comodules

A *comodule over a bialgebra* $(A, m, e, \Delta, \epsilon)$ is defined to be a comodule over the coalgebra (A, Δ, ϵ) .

PROPOSITION 8.12 *Let G be an affine monoid over k . For any k -vector space V , there is a natural one-to-one correspondence between the linear representations of G on V and the $\mathcal{O}(G)$ -comodule structures on V .*

We first describe the correspondence in the case that V is finite dimensional. The choice of a basis $(e_i)_{i \in I}$ for V identifies End_V with M_n , and morphisms $r: G \rightarrow \text{End}_V$ of set-valued functors with the matrices $(r_{ij})_{(i,j) \in I \times I}$ of regular functions on G ,

$$r_R(g) = \left(\begin{array}{c} \\ (r_{ij})_R(g) \\ \end{array} \right)_{i,j \in I}.$$

The map r is a morphism of affine monoids if and only if $(r_{ij})_R(1) = \delta_{ij}$ ($i, j \in I$) and

$$(r_{ij})_R(gg') = \sum_{k \in I} (r_{ik})_R(g) \cdot (r_{kj})_R(g'), \quad \text{all } g, g' \in G(R), \quad i, j \in I. \quad (73)$$

On the other hand, to give a k -linear map $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ is the same as giving a matrix $(r_{ij})_{i,j \in I}$ of elements of $\mathcal{O}(G)$,

$$\rho(e_j) = \sum_{i \in I} e_i \otimes r_{ij},$$

and ρ is a co-action if and only if $\epsilon(r_{ij}) = \delta_{ij}$ ($i, j \in I$) and

$$\Delta(r_{ij}) = \sum_{k \in I} r_{ik} \otimes r_{kj}, \quad \text{all } i, j \in I, \quad (74)$$

(see (69), p. 98). But

$$\Delta(r_{ij})_R(g, g') = (r_{ij})_R(g \cdot g')$$

and

$$\left(\sum_{k \in I} r_{ik} \otimes r_{kj} \right)_R(g, g') = \sum_{k \in I} (r_{ik})_R(g) \cdot (r_{kj})_R(g')$$

(cf. §5g), and so (73) holds if and only if (74) holds. Therefore

$$r \leftrightarrow (r_{ij}) \leftrightarrow \rho$$

gives a one-to-one correspondence between the linear representations of G on V and the $\mathcal{O}(G)$ -comodule structures on V .

SUMMARY 8.13 Let $V = k^n$ with its canonical basis $(e_i)_{i \in I}$; a matrix $(r_{ij})_{i,j \in I}$ of elements of $\mathcal{O}(G)$ satisfying

$$\left. \begin{array}{l} \Delta(r_{ij}) = \sum_{k \in I} r_{ik} \otimes r_{kj} \\ \epsilon(r_{ij}) = \delta_{ij} \end{array} \right\} \quad \text{all } i, j \in I,$$

defines a coaction of $\mathcal{O}(G)$ on V by

$$\rho(e_j) = \sum_{i \in I} e_i \otimes r_{ij},$$

and a homomorphism $r: G \rightarrow \text{GL}_n$ by

$$r(g) = (r_{ij}(g))_{i,j \in I},$$

which corresponds to the homomorphism $\mathcal{O}(\text{GL}_n) \rightarrow \mathcal{O}(G)$ sending X_{ij} to r_{ij} .

In the more formal proof of Proposition 8.12 below, we construct a *canonical* correspondence between the representations and the comodule structures, and in Proposition 8.18 we show that, once a basis has been chosen, the correspondence becomes that described above.

PROOF (OF PROPOSITION 8.12) Let $A = \mathcal{O}(G)$. We prove the following more precise result:

Let $r: G \rightarrow \text{End}_V$ be a representation; the “universal” element $u = \text{id}_A$ in $G(A) \simeq \text{Hom}_{k\text{-alg}}(A, A)$ maps to an element of $\text{End}_V(A) \stackrel{\text{def}}{=} \text{End}_{A\text{-lin}}(V(A))$ whose restriction to $V \subset V(A)$ is a comodule structure $\rho: V \rightarrow V \otimes A$ on V . Conversely, a comodule structure ρ on V determines a representation r such that, for R a k -algebra and $g \in G(R)$, the restriction of $r_R(g): V(R) \rightarrow V(R)$ to $V \subset V(R)$ is

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{V \otimes g} V \otimes R.$$

These operations are inverse.

Let V be a vector space over k , and let $r: G \rightarrow \text{End}_V$ be a natural transformation of *set*-valued functors. Let $g \in G(R) = \text{Hom}_{k\text{-alg}}(A, R)$, and consider the diagram:

$$\begin{array}{ccccc} V & \xrightarrow{v \mapsto v \otimes 1} & V \otimes A & \xrightarrow{V \otimes g} & V \otimes R \\ & \searrow \rho \stackrel{\text{def}}{=} r_A(u)|_V & \downarrow r_A(u) & & \downarrow r_R(g) \\ & & V \otimes A & \xrightarrow{V \otimes g} & V \otimes R \end{array}$$

The k -linear map ρ determines $r_R(g)$ because $r_A(u)$ is the unique A -linear extension of ρ to $V \otimes A$ and $r_R(g)$ is the unique R -linear map making the right hand square commute. Thus the map ρ determines the natural transformation r . Moreover, the diagram can be used to extend any k -linear map $\rho: V \rightarrow V \otimes A$ to a natural transformation r of set-valued functors, namely, for $g \in G(R) = \text{Hom}_{k\text{-alg}}(A, R)$ and define $r_R(g)$ to be the linear map $V(R) \rightarrow V(R)$ whose restriction to V is $(V \otimes g) \circ \rho$. Thus,

$$r_R(g)(v \otimes c) = (V \otimes g)(c\rho(v)), \quad \text{for all } g \in G(R), v \in V, c \in R. \quad (75)$$

In this way, we get a one-to-one correspondence $r \leftrightarrow \rho$ between natural transformations of set-valued functors r and k -linear maps ρ , and it remains to show that r is a representation of G if and only if ρ is a comodule structure on V .

Recall that the identity element $1_{G(k)}$ of $G(k)$ is $A \xrightarrow{\epsilon} k$. To say that $r_k(1_{G(k)}) = \text{id}_{V \otimes k}$ means that the following diagram commutes,

$$\begin{array}{ccccc} & & v \mapsto v \otimes 1 & & \\ & \searrow & & \searrow & \\ V & \xrightarrow{v \mapsto v \otimes 1} & V \otimes A & \xrightarrow{V \otimes \epsilon} & V \otimes k \\ & \searrow \rho & & & \downarrow V \otimes k \\ & & V \otimes A & \xrightarrow{V \otimes \epsilon} & V \otimes k \end{array}$$

i.e., that the right hand diagram in (67) commutes.

Next consider the condition that $r_R(g)r_R(h) = r_R(gh)$ for $g, h \in G(R)$. By definition (see (8)), gh is the map

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{(g,h)} R,$$

and so $r_R(gh)$ acts on V as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{V \otimes \Delta} V \otimes A \otimes A \xrightarrow{V \otimes (g,h)} V \otimes R. \quad (76)$$

On the other hand, $r_R(g)r_R(h)$ acts as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{V \otimes h} V \otimes R \xrightarrow{\rho \otimes R} V \otimes A \otimes R \xrightarrow{V \otimes (g,\text{id})} V \otimes R,$$

i.e., as

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{\rho \otimes A} V \otimes A \otimes A \xrightarrow{V \otimes (g,h)} V \otimes R. \quad (77)$$

The maps (76) and (77) agree for all g, h if and only if the first diagram in (67) commutes. \square

EXAMPLE 8.14 Recall (8.5) that, for any k -bialgebra A , the map $\Delta: A \rightarrow A \otimes A$ is a comodule structure on A . When $A = \mathcal{O}(G)$, this comodule structure on A corresponds to the regular representation of G on $\mathcal{O}(G)$ (8.3).

EXAMPLE 8.15 Let $\rho: V \rightarrow V \otimes \mathcal{O}(\mathbb{G}_a)$ be a finite-dimensional $\mathcal{O}(\mathbb{G}_a)$ -comodule. The k -vector space $\mathcal{O}(\mathbb{G}_a) \simeq k[X]$ has basis $1, X, X^2, \dots$ and so we can write

$$\rho(v) = \sum_{i \geq 0} \rho_i(v) \otimes X^i, \quad v \in V.$$

As ρ is k -linear, so also is each map $v \mapsto \rho_i(v)$, and as the sum is finite, for each v , $\rho_i(v)$ is zero except for a finite number of i . As V is finite-dimensional, this means that only finitely many of the ρ_i are nonzero. It follows that the representations constructed in (8.1) form a complete set.

PROPOSITION 8.16 Let $r: G \rightarrow \text{End}_V$ be the representation corresponding to a comodule (V, ρ) . A subspace W of V is a subrepresentation if and only if it is a subcomodule.

PROOF. Routine checking. \square

PROPOSITION 8.17 Every representation of G is a union of its finite-dimensional subrepresentations.

PROOF. In view of (8.12) and (8.16), this is simply a restatement of Proposition 8.8. \square

PROPOSITION 8.18 Let $r: G \rightarrow \text{End}_V$ be the representation corresponding to a comodule (V, ρ) . Choose a basis $(e_i)_{i \in I}$ for V , and write

$$\rho(e_j) = \sum_i e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G). \quad (78)$$

Then, for each $g \in G(R)$,

$$r_R(g)(e_j \otimes 1) = \sum_{i \in I} e_i \otimes g(a_{ij}) = \sum_{i \in I} e_i \otimes a_{ijR}(g) \quad (79)$$

(equality in $V(R)$; recall that a_{ijR} is a map $G(R) \rightarrow R$ and that $r_R(g)$ is a map $V(R) \rightarrow V(R)$).

PROOF. According to (75),

$$\begin{aligned} r_R(g)(e_j \otimes 1) &= (\text{id}_V \otimes g)(\rho(e_j)) \\ &= (\text{id}_V \otimes g)(\sum_i e_i \otimes a_{ij}) \\ &= \sum_i e_i \otimes g(a_{ij}) \\ &= \sum_i e_i \otimes a_{ij}R(g). \end{aligned}$$

In the last step, we used that $g(f) = f_R(g)$ for $f \in \mathcal{O}(G)$ and $g \in G(R)$ (see 2.16). \square

COROLLARY 8.19 *Let (G, r) be the representation corresponding to a comodule (V, ρ) . Choose a basis $(e_i)_{i \in I}$ for V . Then $\mathcal{O}(\text{End}_V)$ is a polynomial ring in variables X_{ij} ($i, j \in I$) where X_{ij} acts by sending an endomorphism of V to its (i, j) th matrix entry. The homomorphism $\mathcal{O}(\text{End}_V) \rightarrow \mathcal{O}(G)$ defined by r sends X_{ij} to a_{ij} where a_{ij} is given by (78).*

PROOF. Restatement of the proposition. \square

COROLLARY 8.20 *Let $r: G \rightarrow \text{End}_V$ be the representation corresponding to a comodule (V, ρ) . Let H be a subgroup of G , and let $\mathfrak{a} = \mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a}$. The following conditions on a vector $v \in V$ are equivalent:*

- (a) for all k -algebras R and all $g \in H(R)$, $r_R(g)(v_R) = v_R$;
- (b) $\rho(v) \equiv v \otimes 1 \pmod{V \otimes \mathfrak{a}}$.

PROOF. We may suppose that $v \neq 0$, and so is part of a basis $(e_i)_{i \in I}$ for V , say $v = e_j$. Let $(a_{ij})_{i, j \in I}$ be as in (78); then (b) holds for e_j if and only if $a_{ij} - \delta_{ij} \in \mathfrak{a}$ for all i . On the other hand, (79) shows that (a) holds for e_j if and only if the same condition holds on (a_{ij}) . \square

We say that $v \in V$ is **fixed** by H if it satisfies the equivalent conditions of the corollary, and we let V^H denote the subspace of fixed vectors in V . If $H(k)$ is dense in H , then $v \in V^H$ if and only if $r(g)v = v$ for all $g \in H(k)$ (because there is a largest subgroup of G fixing v).

LEMMA 8.21 *Let G, r, V, ρ , and H be as in the corollary, and let R be a k -algebra. The following submodules of $V(R)$ are equal:*

- (a) $V^H \otimes R$;
- (b) $\{v \in V(R) \mid r_{R'}(g)(v_{R'}) = v_{R'} \text{ for all } R\text{-algebras } R' \text{ and } g \in H(R')\}$;
- (c) $\{v \in V(R) \mid \rho(v) \equiv v \otimes 1 \pmod{V \otimes \mathfrak{a} \otimes R}\}$.

PROOF. Nothing in this subsection requires that k be a field (provided one assumes V to be free). Therefore the equality of the sets in (b) and (c) follows by taking $k = R$ in Corollary 8.20. The condition

$$\rho(v) \equiv v \otimes 1 \pmod{V \otimes \mathfrak{a}}$$

is linear in v , and so if W is the solution space over k , then $W \otimes_k R$ is the solution space over R . This proves the equality of the sets in (a) and (c). \square

8g The category of representations of G

Let G be an affine monoid over k , and let $\text{Rep}(G)$ be the category of representations of G on finite-dimensional k -vector spaces. As this is essentially the same as the category of finite-dimensional $\mathcal{O}(G)$ -comodules (see 8.12), it is an abelian category and the forgetful functor to k -vector spaces is exact and faithful.

The **tensor product** of two representations (V, r) and (V', r') is defined to be $(V \otimes V', r \otimes r')$ where $(r \otimes r')_R(g) = r_R(g) \otimes r'_R(g)$.

When G is a group, the **contragredient** (or **dual**) of a representation (V, r) is defined to be (V^\vee, r^\vee) where,

$$(r^\vee_R(g)(f))(v) = f(r_R(g^{-1})v), \quad g \in G(R), \quad f \in V^\vee(R), \quad v \in V(R)$$

(more succinctly, $(gf)(v) = f(g^{-1}v)$).

PROPOSITION 8.22 *Let (V, r) and (V', r') be representations of G , and let ρ and ρ' be the corresponding comodule structures on V and V' . The comodule structures on $V \otimes V'$ and V^\vee defined by $r \otimes r'$ and r^\vee are those described in §8e.*

PROOF. Easy exercise for the reader. □

8h Affine groups are inverse limits of algebraic groups

It is convenient at this point to prove the following theorem.

THEOREM 8.23 *Every affine monoid (resp. group) is an inverse limit of its algebraic quotients.*

In particular, every affine monoid (resp. group) is an inverse limit of algebraic monoids (resp. groups) in which the transition maps are quotient maps.

We prove Theorem 8.23 in the following equivalent form.

THEOREM 8.24 *Every bialgebra (resp. Hopf algebra) over k is a directed union of its finitely generated sub-bialgebras (resp. Hopf subalgebras) over k .*

PROOF. Let A be a k -bialgebra. By (8.8), every finite subset of A is contained in a finite-dimensional k -subspace V such that $\Delta(V) \subset V \otimes A$. Let (e_i) be a basis for V , and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. Then $\Delta(a_{ij}) = \sum_k a_{ik} \otimes a_{kj}$ (see (69), p. 98), and the subspace L of A spanned by the e_i and a_{ij} satisfies $\Delta(L) \subset L \otimes L$. The k -subalgebra A' generated by L satisfies $\Delta(A') \subset A' \otimes A'$, and so it is a finitely generated sub-bialgebra of A . It follows that A is the directed union $A = \bigcup A'$ of its finitely generated sub-bialgebras.

Suppose that A has an inversion S . If $\Delta(a) = \sum b_i \otimes c_i$, then $\Delta(Sa) = \sum S c_i \otimes S b_i$ (Exercise 5-5b). Therefore, the k -subalgebra A' generated by L and SL satisfies $S(A') \subset A'$, and so it is a finitely generated Hopf subalgebra of A . It follows that A is the directed union of its finitely generated Hopf subalgebras. □

COROLLARY 8.25 *Let A be a Hopf subalgebra of the Hopf algebra B . Then A and B are directed unions of finitely generated Hopf subalgebras A_i and B_i such that $A_i \subset B_i$.*

PROOF. Since each finitely generated Hopf subalgebra of A is contained in a finitely generated Hopf subalgebra of B , this follows easily from the theorem. \square

COROLLARY 8.26 *Let A be a Hopf algebra over a field k . If A is an integral domain and its field of fractions is finitely generated (as a field) over k , then A is finitely generated.*

PROOF. Any finite subset S of A is contained in a finitely generated Hopf subalgebra A' of A . When S is chosen to generate the field of fractions of A , then A' and A have the same field of fractions, and so they are equal (6.44). \square

COROLLARY 8.27 *A Hopf algebra whose augmentation ideal is finitely generated is itself finitely generated.*

PROOF. Let A be a Hopf algebra. If I_A is finitely generated, then there exists a finitely generated Hopf subalgebra A' of A containing a set of generators for I_A . The inclusion $A' \rightarrow A$ corresponds to a quotient map $G \rightarrow G'$ whose kernel has Hopf algebra $A \otimes_{A'} A'/I_{A'} \simeq A/I_{A'}A = A/I_A \simeq k$. Proposition 7.1 shows that $G \simeq G'$, and so $A' \simeq A$. \square

PROPOSITION 8.28 *Every quotient of an algebraic group is itself an algebraic group.*

PROOF. We have to show that a Hopf subalgebra A of a finitely generated Hopf algebra B is finitely generated. Because B is noetherian, the ideal $I_A B$ is finitely generated, and because B is flat over A , the map $I_A \otimes_A B \rightarrow A \otimes_A B \simeq B$ is an isomorphism of $I_A \otimes_A B$ onto $I_A B$. Therefore $I_A \otimes B$ is a finitely generated B -module, and as B is faithfully flat over A , this implies that I_A is finitely generated.²⁸ \square

ASIDE 8.29 Proposition 8.28 is *not* obvious because subalgebras of finitely generated k -algebras need not be finitely generated. For example, the subalgebra $k[X, XY, XY^2, \dots]$ of $k[X, Y]$ is not even noetherian. There are even subfields K of $k(X_1, \dots, X_n)$ containing k such that $K \cap k[X_1, \dots, X_n]$ is not finitely generated as a k -algebra (counterexamples to Hilbert's fourteenth problem; Nagata and others).

ASIDE 8.30 Theorem 8.23 is also true for nonaffine group schemes: every quasicompact group scheme over a field k is a filtered inverse limit of group schemes of finite type over k (Perrin 1976).

8i Algebraic groups admit finite-dimensional faithful representations

In fact, every sufficiently large finite-dimensional subrepresentation of the regular representation will be faithful.

THEOREM 8.31 *For any algebraic group G , the regular representation of G has faithful finite-dimensional subrepresentations; in particular, the regular representation itself is faithful.*

²⁸As a B -module, $I_A \otimes_A B$ has a finite set of generators $\{c_1 \otimes b_1, \dots, c_m \otimes b_m\}$, and the map

$$(a_1, \dots, a_m) \mapsto \sum a_i c_i: A^m \rightarrow I_A$$

is surjective because it becomes surjective when tensored with B .

PROOF. Let $A = \mathcal{O}(G)$, and let V be a finite-dimensional submodule of A containing a set of generators for A as a k -algebra. Let $(e_i)_{1 \leq i \leq n}$ be a basis for V , and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. According to (8.19), the image of $\mathcal{O}(\mathrm{GL}_V) \rightarrow A$ contains the a_{ij} . But, because $\epsilon: A \rightarrow k$ is a co-identity (see (29), p. 42),

$$e_j = (\epsilon \otimes \mathrm{id}_A)\Delta(e_j) = \sum_i \epsilon(e_i)a_{ij},$$

and so the image contains V ; it therefore equals A . We have shown that $\mathcal{O}(\mathrm{GL}_V) \rightarrow A$ is surjective, which means that $G \rightarrow \mathrm{GL}_V$ is injective (7.2). [Variant: $A_V \supset V$ (see 8.6c), and so $A_V = A$; this implies that the representation on V is faithful.] \square

COROLLARY 8.32 *Every affine group admits a faithful family of finite-dimensional representations.*

PROOF. Write G as an inverse limit $G = \varprojlim_{i \in I} G_i$ of algebraic groups, and, for each $i \in I$, choose a faithful finite-dimensional representation (V_i, r_i) of G_i . Each (V_i, r_i) can be regarded as a representation of G , and the family is faithful. \square

The theorem says that every algebraic group can be realized as an algebraic subgroup of GL_n for some n . This does *not* mean that we should consider only subgroups of GL_n because realizing an algebraic group in this way involves many choices.

PROPOSITION 8.33 *Let (V, r) be a faithful representation of an algebraic group G . Then V is a union of its finite-dimensional faithful subrepresentations.*

PROOF. Let $(e_i)_{i \in I}$ be a basis for V , and write $\rho(e_j) = \sum_{i \in I} e_i \otimes a_{ij}$, $a_{ij} \in A$. Because (V, r) is faithful, the k -algebra A is generated by the a_{ij} (8.19). Because A is finitely generated as a k -algebra, only finitely many a_{ij} 's are need to generate it, and so there exists a finite subset J of I such that the a_{ij} 's appearing in $\rho(e_j)$ for some $j \in J$ generate A . Every finite-dimensional subrepresentation of (V, r) containing $\{e_j \mid j \in J\}$ is faithful. \square

ASIDE 8.34 Does every affine group of finite type over a commutative ring admit an injective homomorphism into GL_n for some n ? Apparently, this is not known even when k is the ring of dual numbers over a field and G is smooth (mo22078, Brian Conrad). Using (8.10), one sees by the above arguments that an affine group scheme G of finite type over a noetherian ring k has a faithful representation on a finitely generated submodule M of the regular representation. If M is flat over k , then it is projective, and hence a direct summand of a free finitely generated k -module L , and so $G \hookrightarrow \mathrm{GL}_{\mathrm{rank}(L)}$. When k is a Dedekind domain and G is flat, the module M is torsion-free, and hence automatically flat. Thus, every flat affine group scheme of finite type over a Dedekind domain admits an embedding into GL_n for some n . As every split reductive group scheme over a ring k arises by base change from a similar group over \mathbb{Z} (Chevalley), such group schemes admit embeddings into GL_n . Since every reductive group splits over a finite étale extension of the base ring (SGA3), an argument using restriction of scalars proves the statement for every reductive group (mo22078).

8j The regular representation contains all

Let (V, r_V) be a representation of G . For $v \in V(R)$ and $u \in V^\vee(R)$, let $\langle u, v \rangle = u(v) \in R$. For a fixed $v \in V$ and $u \in V^\vee$, the maps

$$x \mapsto \langle u, r_V(x)v \rangle: G(R) \rightarrow R$$

are natural in R , and so define an element of $\mathcal{O}(G)$, i.e., there exists a $\phi_u(v) \in \mathcal{O}(G)$ such that

$$\phi_u(v)_R(x) = \langle u, r_V(x)v \rangle \text{ (in } R) \text{ for all } x \in G(R).$$

Let $A = \mathcal{O}(G)$, and let r_A be the regular representation of G on A .

PROPOSITION 8.35 *The map ϕ_u is a homomorphism of representations $(V, r_V) \rightarrow (A, r_A)$.*

PROOF. We have to show that

$$(\phi_u)_R \circ r_V(g) = r_A(g) \circ (\phi_u)_R$$

for all k -algebras R and all $g \in G(R)$. For any $v \in V(R)$ and $x \in G(R)$,

$$\begin{aligned} (\text{LHS}(v))(x) &= \phi_u(r_V(g)v)_R(x) \\ &= \langle u, r_V(x)r_V(g)v \rangle \quad (\text{definition of } \phi_u) \\ &= \langle u, r_V(xg)v \rangle \quad (r_V \text{ is a homomorphism}) \\ &= \phi_u(v)_R(xg) \quad (\text{definition of } \phi_u) \\ &= (r_A(g)\phi_u(v))_R(x) \quad ((65), \text{ p. 96}) \\ &= (\text{RHS}(v))(x), \end{aligned}$$

as required. □

PROPOSITION 8.36 *If u_1, \dots, u_n span V^\vee , then the k -linear map*

$$v \mapsto (\phi_{u_1}(v), \dots, \phi_{u_n}(v)): V \rightarrow A^n \quad (80)$$

is injective.

PROOF. Note that $\phi_u(v)(1) = \langle u, v \rangle$, and so the composite

$$V(R) \rightarrow A^n(R) \rightarrow R^n$$

of (80) with the map ‘‘evaluate at 1’’ is

$$v \mapsto (\langle u_1, v \rangle, \dots, \langle u_n, v \rangle),$$

which is injective by our choice of the u_i 's. □

Thus, V embeds into a finite sum of copies of the regular representation. We give a second proof of this.

PROPOSITION 8.37 *Let (V, ρ) be a finite-dimensional representation of G . Let V_0 denote V regarded as a vector space, and let $V_0 \otimes \mathcal{O}(G)$ be the free comodule on V_0 (see 8.5). Then*

$$\rho: V \rightarrow V_0 \otimes \mathcal{O}(G)$$

is an injective homomorphism of representations.

PROOF. The coaction on $V_0 \otimes \mathcal{O}(G)$ is

$$V_0 \otimes \Delta: V_0 \otimes \mathcal{O}(G) \rightarrow V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G).$$

The commutative diagram (see (67), p. 97)

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V_0 \otimes \mathcal{O}(G) \\ \downarrow \rho & & \downarrow V_0 \otimes \Delta \\ V \otimes \mathcal{O}(G) & \xrightarrow{\rho \otimes \mathcal{O}(G)} & V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G) \end{array}$$

says exactly that the map $\rho: V \rightarrow V_0 \otimes \mathcal{O}(G)$ is a homomorphism of comodules. It is obviously injective. \square

8k Every faithful representation generates $\text{Rep}(G)$

Let (C, Δ, ϵ) be a coalgebra over k , and let (V, ρ) be a comodule over C . Recall (8.6) that C_V denotes the smallest subspace of C such that $\rho(V) \subset V \otimes C_V$. The space C_V is a sub-coalgebra of C , and, for any basis $(e_i)_{i \in I}$ of V , it is spanned by the elements c_{ij} determined by the equation

$$\rho(e_j) = \sum_{i \in I} e_i \otimes c_{ij}.$$

Note that

$$C_{\oplus V_i} = \sum_i C_{V_i} \quad (\text{sum of subspaces of } C).$$

Any C_V -comodule (W, ρ_W) can be regarded as a C -comodule with the coaction

$$W \xrightarrow{\rho_W} W \otimes C_V \subset W \otimes C.$$

LEMMA 8.38 *Let (V, ρ) be a finite dimensional C -comodule. Every finite-dimensional C_V -comodule (considered as a C -comodule) is isomorphic to a quotient of a sub-comodule of V^n for some n .*

PROOF. We may replace C with C_V , and so assume that C is finite dimensional. Let $A = C^\vee$. Because of the correspondence between right C -comodule structures and left A -module structures (8.7), it suffices to prove the following statement:

let A be a finite k -algebra and let V be a finite-dimensional faithful left A -module; then every finite-dimensional A -module W is isomorphic to a quotient of a submodule of V^n for some n .

Every module W is isomorphic to a quotient of the free module A^m for some m , and so it suffices to prove that A itself is isomorphic to a submodule of V^n for some n . But if e_1, \dots, e_n span V as a k -vector space, then $a \mapsto (ae_1, \dots, ae_n): A \rightarrow V^n$ is injective because V is faithful. \square

Now assume that A is a bialgebra over k . Then the tensor product of two A -comodules has a natural A -comodule structure (§8e).

LEMMA 8.39 *Let A be a bialgebra over k , and let V and V' be finite-dimensional A -comodules. Then $A_{V \otimes V'} = A_V \cdot A_{V'}$.*

PROOF. Choose k -bases $(e_i)_{i \in I}$ and $(e'_i)_{i \in I'}$ for V and V' , and write

$$\rho_V(e_j) = \sum_{i \in I} e_i \otimes a_{ij}, \quad \rho_{V'}(e'_j) = \sum_{i \in I'} e'_i \otimes a'_{ij}.$$

Then $(e_i \otimes e_{i'})_{(i,i') \in I \otimes I'}$ is a basis for $V \otimes_k V'$, and

$$\rho_{V \otimes V'}(e_j \otimes e_{j'}) = \sum_{i,i'} (e_i \otimes e_{i'}) \otimes (a_{ij} \cdot a'_{i'j'})$$

(see §8e). As

$$\begin{aligned} A_V &= \langle a_{ij} \mid i, j \in I \rangle \\ A_{V'} &= \langle a_{ij} \mid i, j \in I' \rangle \\ A_{V \otimes V'} &= \langle a_{ij} \cdot a'_{i'j'} \mid i, j \in I, \quad i', j' \in I' \rangle, \end{aligned}$$

the statement is clear. (Alternatively, note that $A_V \otimes A_{V'}$ is the sub-coalgebra attached to the $A \otimes A$ -comodule $V \otimes V'$, and that $A_{V \otimes V'}$ is the image of this by the multiplication map $m: A \otimes A \rightarrow A$.) \square

Now assume that A is a Hopf algebra over k . Then the dual of an A -comodule has a natural A -comodule structure (§8e).

LEMMA 8.40 *Let A be a Hopf algebra over k , and let $S: A \rightarrow A$ be its inversion. For any finite-dimensional A -comodule (V, ρ) , $A_{V^\vee} = SA_V$.*

PROOF. Under the isomorphisms (71), the right co-action $\rho: V \rightarrow V \otimes A$ corresponds to a left co-action $\rho': V^\vee \rightarrow A \otimes V^\vee$, and A_V is also the smallest subspace of A such that $\rho'(V^\vee) \subset A_V \otimes V^\vee$. It follows from the definition of ρ^\vee (see (72)) that SA_V is the smallest subspace of A such that $\rho^\vee(V^\vee) \subset V^\vee \otimes A$. \square

LEMMA 8.41 *Let V be a finite-dimensional comodule over a k -bialgebra A . Then*

$$A(V) \stackrel{\text{def}}{=} \sum_{n \geq 0} A_{V^{\otimes n}} \subset A$$

is the smallest sub-bialgebra of A containing A_V and 1.

PROOF. It follows from Lemma 8.39 that

$$A_{V^{\otimes n}} = A_V \cdots A_V \quad (n \text{ factors}),$$

and so it is clear that $A(V)$ is the subalgebra of A generated by A_V and 1. \square

Note that $A = \bigcup_V A(V)$ because $A = \bigcup_V A_V$ (see 8.9).

LEMMA 8.42 *Let V be a finite-dimensional comodule over a Hopf k -algebra A . Then $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing A_V and 1 and stable under S (in other words, it is the smallest Hopf subalgebra of A containing A_V and 1).*

PROOF. From Lemma 8.41, $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing $A_{V \oplus V^\vee}$ and 1. But

$$A_{V \oplus V^\vee} = A_V + A_{V^\vee} \stackrel{8.40}{=} A_V + SA_V,$$

and so it is the smallest sub-bialgebra of A containing A_V , SA_V , and 1. \square

Let G be an algebraic group over k , and let $A = \mathcal{O}(G)$.

LEMMA 8.43 *Let (V, r) be a finite-dimensional representation of G , and let (V, ρ) be the corresponding A -comodule. The representation r is faithful if and only if $A(V \oplus V^\vee) = A$.*

PROOF. Choose a basis $(e_i)_{i \in I}$ for V , and write $\rho(e_j) = \sum e_i \otimes a_{ij}$. Then $A(V \oplus V^\vee)$ is the smallest sub-bialgebra of A containing the a_{ij} and 1 and stable under S (by 8.42). On the other hand, the image of $\mathcal{O}(\mathrm{GL}_V) \rightarrow \mathcal{O}(G) = A$ is the k -subalgebra generated by the a_{ij} (8.19). As this image is a sub-bialgebra stable under S , we see that $\mathcal{O}(\mathrm{GL}_V) \rightarrow \mathcal{O}(G)$ is surjective (so r is faithful) if and only if $A(V \oplus V^\vee) = A$. \square

THEOREM 8.44 *Let $G \rightarrow \mathrm{GL}_V$ be a representation of G . If V is faithful, then every finite-dimensional representation of G is isomorphic to a quotient of a sub-representation of a direct sum of representations $\bigotimes^n (V \oplus V^\vee)$.*

PROOF. Let W be the direct sum of the representations $\bigotimes^n (V \oplus V^\vee)$. By definition, $A(V \oplus V^\vee) = A_W$. According to Lemma 8.38, every finite-dimensional A_W -comodule is isomorphic to a quotient of a sub-comodule of W . When V is faithful, $A_W = A$. \square

COROLLARY 8.45 *Every simple G -module is a Jordan-Hölder quotient of $\bigotimes^n (V \oplus V^\vee)$ for some n .*

PROOF. Immediate consequence of the theorem. \square

We close this subsection with some remarks.

8.46 When M is an affine monoid with coordinate ring $\mathcal{O}(M) = A$, we let M_V denote the quotient affine monoid of M with coordinate ring $A(V)$. Similarly, when G is an affine group, we let G_V denote the quotient affine group of G with coordinate ring $A(V \oplus V^\vee)$. Both M_V and G_V act faithfully on V . Moreover,

$$M = \varprojlim M_V, \quad G = \varprojlim G_V$$

because $A = \bigcup A(V)$.

8.47 Let (V, ρ) be a finite-dimensional comodule over a Hopf k -algebra A . Choose a basis $(e_i)_{i \in I}$ for V and define the matrix (a_{ij}) by $\rho(e_j) = \sum_{i \in I} e_i \otimes a_{ij}$. Let $\delta_V = \det(a_{ij})$. Then δ_V is an invertible element of A , contained in $A(V)$, and

$$A(V \oplus V^\vee) = A(V) \left[\frac{1}{\delta_V} \right].$$

8.48 The quotient M_V of M is the smallest affine submonoid of End_V containing the image of r , and the quotient G_V of G is the smallest affine subgroup of GL_V containing the image of r .

8.49 Let $\det(V) = \bigwedge^{\dim V} V$. Then every simple G -module is a Jordan-Hölder quotient of $\bigotimes^n V \otimes \bigotimes^m \det(V)^\vee$ for some m, n .

8.50 It sometimes happens that $\mathcal{O}(G_V)$ is a quotient of $\mathcal{O}(\text{End}_V)$ (and not just of $\mathcal{O}(\text{GL}_V)$), i.e., that $A(V) = A(V \oplus V^\vee)$. This is the case, for example, if G_V is contained in SL_V . In this case, Theorem 8.44 and its corollary simplify: the tensor powers of $V \oplus V^\vee$ can be replaced by those of V .

ASIDE 8.51 Our exposition of Theorem 8.44 follows Serre 1993.

81 Stabilizers of subspaces

PROPOSITION 8.52 Let $G \rightarrow \text{GL}_V$ be a representation of G , and let W be a subspace of V . The functor

$$R \rightsquigarrow \{g \in G(R) \mid gW_R = W_R\}$$

is a subgroup of G (denoted G_W , and called the *stabilizer* of W in G).

PROOF. Let $(e_i)_{i \in J}$ be a basis for W , and extend it to a basis $(e_i)_{i \in J \sqcup I}$ for V . Write

$$\rho(e_j) = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

Let $g \in G(R) = \text{Hom}_{k\text{-alg}}(\mathcal{O}(G), R)$. Then (see 8.18)

$$ge_j = \sum_{i \in J \sqcup I} e_i \otimes g(a_{ij}).$$

Thus, $g(W \otimes R) \subset W \otimes R$ if and only if $g(a_{ij}) = 0$ for $j \in J, i \in I$. As $g(a_{ij}) = (a_{ij})_R(g)$ (see 2.16), this shows that the functor is represented by the quotient of $\mathcal{O}(G)$ by the ideal generated by $\{a_{ij} \mid j \in J, i \in I\}$. \square

We say that an affine subgroup H of G *stabilizes* W if $H \subset G_W$, i.e., if $hW_R = W_R$ for all k -algebras R and $h \in H(R)$.

COROLLARY 8.53 Let H be an algebraic subgroup of G such that $H(k)$ is dense in H . If $hW = W$ for all $h \in H(k)$, then H stabilizes W .

PROOF. As $hW = W$ for all $h \in H(k)$, we have $(H \cap G_W)(k) = H(k)$, and so $H \cap G_W = H$. \square

PROPOSITION 8.54 Let G act on V and V' , and let W and W' be nonzero subspaces of V and V' . Then the stabilizer of $W \otimes W'$ in $V \otimes V'$ is $G_W \cap G_{W'}$.

PROOF. Clearly $G_W \cap G_{W'} \subset G_{W \otimes W'}$. Conversely, if g is an element of $G(R)$ not in $G_W(R)$, then there exists a nonzero $w \in W$ such that $gw \notin W_R$. For any nonzero element w' of W' , the element $g(w \otimes w') = gw \otimes gw'$ of $V_R \otimes V'_R$ is not in $W_R \otimes W'_R$,²⁹ and so $g \notin G_{W \otimes W'}(R)$. \square

PROPOSITION 8.55 Let $G \rightarrow \mathrm{GL}_V$ be a representation of G , and let $v \in V$. The functor

$$R \rightsquigarrow G_v(R) \stackrel{\mathrm{def}}{=} \{g \in G(R) \mid g(v \otimes 1) = v \otimes 1 \text{ (in } V_R)\}$$

is a subgroup of G (denoted G_v , and called the *isotropy* or *stability group* of v in G).

PROOF. If $v = 0$, then $G_v = G$ and there is nothing to prove. Otherwise, choose a basis $(e_i)_{i \in I}$ for V with $e_{i_0} = v$ for some $i_0 \in I$. Write

$$\rho(e_j) = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

An element $g \in G(R)$ fixes $v \otimes 1$ if and only if

$$g(a_{ii_0}) = \begin{cases} 1 & \text{if } i = i_0 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore G_v is represented by the quotient of $\mathcal{O}(G)$ by the ideal generated by $\{a_{ii_0} - \delta_{ii_0} \mid i \in I\}$. \square

DEFINITION 8.56 For a representation $r: G \rightarrow \mathrm{GL}_V$ of G ,

$$V^G = \{v \in V \mid gv = v \text{ (in } V_R) \text{ for all } k\text{-algebras } R \text{ and } g \in G(R)\}.$$

It is largest subspace of V on which the action of G is trivial. If ρ denotes the corresponding coaction, then

$$V^G = \{v \in V \mid \rho(v) = v \otimes 1\}.$$

8m Chevalley's theorem

THEOREM 8.57 (CHEVALLEY) Every subgroup of an algebraic group G is the stabilizer of a one-dimensional subspace in a finite-dimensional representation of G .

PROOF. Let H be a subgroup of G , and let \mathfrak{a} be the kernel of $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$. According to (8.8), there exists a finite-dimensional k -subspace V of $\mathcal{O}(G)$ containing a generating set of \mathfrak{a} as an ideal and such that

$$\Delta(V) \subset V \otimes \mathcal{O}(G).$$

²⁹Let e and e' be nonzero elements of V and V' ; if $e \otimes e' \in W_R \otimes W'_R$ for some k -algebra R , then $e \in W$ and $e' \in W'$. To see this, write $V = W \oplus W_1$, so that

$$V \otimes V' = W \otimes V' \oplus W_1 \otimes V'.$$

Let $e = e_0 + e_1$ with $e_0 \in W$ and $e_1 \in W_1$. If $e_1 \neq 0$, then $e_1 \otimes e' \neq 0$ in $W_1 \otimes V' \subset (W_1 \otimes V')_R$, and so $e \otimes e' \notin (W \otimes V')_R$.

Let $W = \mathfrak{a} \cap V$ in V . Let $(e_i)_{i \in J}$ be a basis for W , and extend it to a basis $(e_i)_{J \sqcup I}$ for V . Let

$$\Delta e_j = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

As in the proof of 8.52, G_W is represented by the quotient of $\mathcal{O}(G)$ by the ideal \mathfrak{a}' generated by $\{a_{ij} \mid j \in J, i \in I\}$. Because $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is a homomorphism of coalgebras³⁰

$$\begin{aligned} \Delta(\mathfrak{a}) &\subset \text{Ker}(\mathcal{O}(G) \otimes \mathcal{O}(G) \rightarrow \mathcal{O}(H) \otimes \mathcal{O}(H)) = \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G), \\ \epsilon(\mathfrak{a}) &= 0. \end{aligned}$$

The first of these applied to e_j , $j \in J$, shows that $\mathfrak{a}' \subset \mathfrak{a}$, and the second shows that

$$e_j = (\epsilon, \text{id})\Delta(e_j) = \sum_{i \in I} \epsilon(e_i) a_{ij}.$$

As the e_j , $j \in J$, generate \mathfrak{a} (as an ideal), so do the a_{ij} , $j \in J$, and so $\mathfrak{a}' = \mathfrak{a}$. Thus $H = G_W$. The next (elementary) lemma shows that W can be taken to be one-dimensional. \square

LEMMA 8.58 *Let W be a finite-dimensional subspace of a vector space V , and let $D = D = \bigwedge^{\dim W} W \subset \bigwedge^{\dim W} V$. Let α be an automorphism of V_R for some k -algebra R . Then $\alpha W_R = W_R$ if and only if $\alpha D_R = D_R$.*

PROOF. Let $(e_j)_{j \in J}$ be a basis for W , and extend it to a basis $(e_i)_{J \sqcup I}$ of V . Let $w = \bigwedge_{j \in J} e_j$. For any k -algebra R ,

$$W_R = \{v \in V_R \mid v \wedge w = 0 \text{ (in } \bigwedge^{d+1} V_R)\}.$$

To see this, let $v \in V_R$ and write $v = \sum_{i \in J \sqcup I} a_i e_i$, $a_i \in R$. Then

$$v \wedge w = \sum_{i \in I} a_i e_1 \wedge \cdots \wedge e_d \wedge e_i.$$

As the elements $e_1 \wedge \cdots \wedge e_d \wedge e_i$, $i \in I$, are linearly independent in $\bigwedge^{d+1} V$, we see that

$$v \wedge w = 0 \iff a_i = 0 \text{ for all } i \in I.$$

Let $\alpha \in \text{GL}(V_R)$. If $\alpha W_R = W_R$, then obviously $(\bigwedge^d \alpha)(D_R) = D_R$. Conversely, suppose that $(\bigwedge^d \alpha)(D_R) = D_R$, so that $(\bigwedge^d \alpha)w = cw$ for some $c \in R^\times$. When $v \in W_R$, $v \wedge w = 0$, and so

$$0 = (\bigwedge^{d+1} \alpha)(v \wedge w) = \alpha v \wedge (\bigwedge^d \alpha)w = c((\alpha v) \wedge w),$$

which implies that $\alpha v \in W_R$. \square

COROLLARY 8.59 *A subgroup H of an algebraic group G is the subgroup of G fixing a vector in some faithful finite-dimensional representation of G in each of the following two cases:*

- (a) *all the representations of H are semisimple;*

³⁰We use the following elementary fact: for any subspace W of a vector space V , the kernel of $V \otimes V \rightarrow V/W \otimes V/W$ is $V \otimes W + W \otimes V$. To prove this, write $V = W \oplus W'$.

- (b) a nonzero multiple of each character of H defined over k extends to a similar character of G .

PROOF. According to Chevalley's theorem, H is the stabilizer of a line D in a finite-dimensional representation V of G . Let D^\vee be the dual of D with H acting contragrediently. If we can find a representation V' of G containing D^\vee as an H -stable subspace, then H will be the subgroup of G fixing any nonzero vector in $D \otimes D^\vee \subset V \otimes V'$.³¹

Certainly D^\vee occurs as a quotient of V^\vee , and so, in case (a), it also occurs as a direct summand of V^\vee (regarded as an H -module). In this case, we can take $V' = V^\vee$.

The action of H on D defines a character of H , which in case (b) extends to a character of G . In this case, we can take $V' = D^\vee$. \square

8n Sub-coalgebras and subcategories

Let C be a coalgebra over k . As before, $\text{Comod}(C)$ denotes the category of finite-dimensional right C -comodules. Let D be a sub-coalgebra of C . Any D -comodule (V, ρ) becomes a C -comodule with the coaction

$$V \xrightarrow{\rho} V \otimes D \subset V \otimes C.$$

In this way, we get an exact fully faithful functor $\text{Comod}(D) \rightarrow \text{Comod}(C)$. We let D^\vee denote the full subcategory of $\text{Comod}(C)$ whose objects are isomorphic to a comodule in the image of this functor.

DEFINITION 8.60 A full subcategory of an abelian category is *replete* if it is closed under the formation of finite direct sums, subobjects, and quotient objects.

In particular, every object isomorphic to an object in a replete subcategory also lies in the subcategory. A replete subcategory is an abelian category, and the inclusion functor is exact.

THEOREM 8.61 *The map $D \mapsto D^\vee$ is a bijection from the set of sub-coalgebras of C onto the set of replete subcategories of $\text{Comod}(C)$.*

PROOF. It is obvious that D^\vee is replete. Let \mathbf{S} be a replete subcategory of $\text{Comod}(C)$, and let

$$C(\mathbf{S}) = \sum_{V \in \mathbf{S}} C_V \quad (\text{sub-coalgebra of } C).$$

To prove the theorem, we have to show that:

- ◇ $C(D^\vee) = D$ for all sub-coalgebras D of C , and
- ◇ $C(\mathbf{S})^\vee = \mathbf{S}$ for all replete subcategories \mathbf{S} of $\text{Comod}(C)$. \square

The first statement follows from Corollary 8.9, and the second follows from Lemma 8.38.

³¹Let v be a nonzero vector in D . Then

$$H \subset G_{v \otimes v^\vee} \subset G_{D \otimes D^\vee} = G_D \cap G_{D^\vee} = G_D = H.$$

PROPOSITION 8.62 *Let A be a bialgebra over k .*

- (a) *A sub-coalgebra D of A is a sub-bialgebra of A if and only if D^\vee is stable under tensor products and contains the trivial comodule.*
- (b) *Assume A has an inversion S . A sub-bialgebra D is stable under S if and only if D^\vee is stable under the contragredient functor.*

PROOF. (a) If D is a sub-bialgebra of A , then certainly D^\vee is stable under tensor products and contains the trivial comodule (see §8e). For the converse, recall that $D = \bigcup D_V$ and that $D_V \cdot D_{V'} = D_{V \otimes V'}$ (see 8.39), and so D is closed under products. Because D^\vee contains $V_0 = k$, D contains $D_{V_0} = k$.

(b) Use the formula $A_{V^\vee} = SA_V$ (8.40). □

8o Quotient groups and subcategories

For an affine group G over k , $\text{Rep}(G)$ denotes the category of finite-dimensional G -modules. Let $G \rightarrow Q$ be a quotient of G . A representation $r: Q \rightarrow \text{GL}_V$ defines a representation $G \rightarrow Q \xrightarrow{r} \text{GL}_V$ of G . We get in this way an exact fully faithful functor $\text{Rep}(Q) \rightarrow \text{Rep}(G)$. The essential image of the functor consists of the representations of G containing $\text{Ker}(G \rightarrow Q)$ in their kernel. We let Q^\vee denote this subcategory of $\text{Rep}(G)$.

THEOREM 8.63 *The map $Q \mapsto Q^\vee$ is a bijection from the set of isomorphism classes of quotients of G to the set of replete subcategories of $\text{Rep}(G)$ closed under the formation of tensor products (including the empty tensor product) and under passage to the contragredient.*

PROOF. Obvious from (8.61), (8.62), and the dictionary between Hopf algebras and their comodules and affine groups and their representations. □

8p Characters and eigenspaces

A **character** of an affine group G is a homomorphism $G \rightarrow \mathbb{G}_m$. As $\mathcal{O}(\mathbb{G}_m) = k[X, X^{-1}]$ and $\Delta(X) = X \otimes X$, we see that to give a character χ of G is the same as giving an invertible element $a = a(\chi)$ of $\mathcal{O}(G)$ such that $\Delta(a) = a \otimes a$; such an element is said to be **group-like**. A one-dimensional representation L of G defines a character of G (because $\text{GL}_L \simeq \mathbb{G}_m$).

A character $\chi: G \rightarrow \mathbb{G}_m$ defines a representation of G on any finite-dimensional space V : let $g \in G(R)$ act on V_R as multiplication by $\chi(g) \in R^\times$. For example, χ defines a representation of G on $V = k^n$ by

$$g \mapsto \begin{pmatrix} \chi(g) & & 0 \\ & \ddots & \\ 0 & & \chi(g) \end{pmatrix}, \quad g \in G(R).$$

Let $r: G \rightarrow \text{GL}_V$ be a representation of G . We say that G acts on V **through a character** χ if

$$r(g)v = \chi(g)v \quad \text{all } g \in G(R), v \in V_R.$$

More precisely, this means that the image of r is contained in the centre \mathbb{G}_m of GL_V and is the composite of

$$T \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V. \quad (81)$$

More generally, we say that G acts on a subspace W of V **through a character** χ if W is stable under G and G acts on W through χ . Note that this means, in particular, that the elements of W are common eigenvectors for the $g \in G(k)$: if $w \in W$, then for every $g \in G(k)$, $r(g)w$ is a scalar multiple of w . If G acts on subspaces W and W' through a character χ , then it acts on $W + W'$ through χ . Therefore, there is a largest subspace V_χ of V on which G acts through χ , called the **eigenspace for G with character χ** .

LEMMA 8.64 *Let (V, r) be a representation of G , and let (V, ρ) be the corresponding co-module. For any character χ of G ,*

$$V_\chi = \{v \in V \mid \rho(v) = v \otimes a(\chi)\}.$$

PROOF. Let W be a subspace of V . Then G acts on W through χ if and only if $\rho|_W$ factors as

$$W \xrightarrow{w \mapsto w \otimes X} W \otimes \mathcal{O}(\mathbb{G}_m) \xrightarrow{w \otimes X \mapsto w \otimes a(\chi)} W \otimes \mathcal{O}(G). \quad \square$$

THEOREM 8.65 *Let $r: G \rightarrow \mathrm{GL}(V)$ be a representation of an algebraic group on a vector space V . If V is a sum of eigenspaces, $V = \sum_{\chi \in \mathcal{E}} V_\chi$, then it is a direct sum of the eigenspaces*

$$V = \bigoplus_{\chi \in \mathcal{E}} V_\chi.$$

PROOF. We first prove this when G is smooth. We may replace k with a larger field, and so assume that k is algebraically closed. If the sum is not direct, there exists a finite subset $\{\chi_1, \dots, \chi_m\}$, $m \geq 2$, of \mathcal{E} and a relation

$$v_1 + \dots + v_m = 0, \quad v_i \in V_{\chi_i}, \quad v_i \neq 0. \quad (82)$$

On applying $g \in G(k)$ to (82), we get a relation

$$\chi_1(g)v_1 + \dots + \chi_{m-1}(g)v_{m-1} + \chi_m(g)v_m = 0. \quad (83)$$

As $\chi_m \neq \chi_{m-1}$ and G is smooth, there exists a $g \in G(k)$ such that $\chi_m(g) \neq \chi_{m-1}(g)$. Multiply (83) by $\chi_m(g)^{-1}$ and subtract it from (82). This will give us a new relation of the same form but with fewer terms. Continuing in this fashion, we arrive at a contradiction.

For the proof of the general case, we shall make use of the elementary lemma 14.2, which says that any set of units a in $\mathcal{O}(G)$ satisfying $\Delta(a) = a \otimes a$ is linearly independent. From the relation (82), we get a relation

$$0 = \sum_{i \in J} \rho(v_i) = \sum_{i \in J} v_i \otimes a(\chi_i)$$

which contradicts the linear independence of the $a(\chi_i)$. □

In §14 we shall show that when G is a split torus, V is always a sum of the eigenspaces V_χ . In general, this will be far from true. For example, SL_n has no nontrivial characters.

8q Every normal affine subgroup is a kernel

LEMMA 8.66 *Let v and w be nonzero vectors in vector spaces V and W respectively, and let α and β be endomorphisms of V_R and W_R for some k -algebra R . If $v \otimes w$ is fixed by $\alpha \otimes \beta$, then there exists a $c \in R^\times$ such that $\alpha(v) = cv$ and $\beta(w) = c^{-1}w$.*

PROOF. Write

$$V = \langle v \rangle \oplus V', \quad W = \langle w \rangle \oplus W'.$$

Then

$$V \otimes W = \langle v \otimes w \rangle \oplus \langle v \rangle \otimes W' \oplus V' \otimes \langle w \rangle \oplus V' \otimes W',$$

where $\langle v \otimes w \rangle = \langle v \rangle \otimes \langle w \rangle \neq 0$. Write

$$\alpha v = av + v', \quad \beta w = bw + w', \quad a, b \in R, \quad v' \in V'_R, \quad w' \in W'_R.$$

Then

$$(\alpha \otimes \beta)(v \otimes w) = ab(v \otimes w) + av \otimes w' + v' \otimes bw + v' \otimes w'.$$

If $(\alpha \otimes \beta)(v \otimes w) = v \otimes w$, then $ab = 1$ and

$$a(v \otimes w') = 0 = b(v' \otimes w).$$

As $a, b \in R^\times$ and $v \neq 0 \neq w$, this implies that $w' = 0 = v'$, as required. \square

LEMMA 8.67 *For any normal subgroup N of an affine group G and representation (V, r) of G , the subspace V^N is stable under G .*

PROOF. Let $w \in (V^N)_R$ and let $g \in G(R)$ for some k -algebra R . For any R -algebra R' and $n \in N(R')$

$$r(n)(r(g)w) = r(ng)w = r(gn')w = r(g)r(n')w = r(g)w,$$

because $n' = g^{-1}ng \in N(R')$. Therefore, $r(g)w \in (V^N)_R$, as required. \square

LEMMA 8.68 *Let G be an affine group over k , and let (V, r) be a representation of G . If V is a sum of simple subrepresentations, say $V = \sum_{i \in I} S_i$ (the sum need not be direct), then for any subrepresentation W of V , there is a subset J of I such that*

$$V = W \oplus \bigoplus_{i \in J} S_i.$$

In particular, V is semisimple.

PROOF. Let J be maximal among the subsets of I such the sum $S_J \stackrel{\text{def}}{=} \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). For this, it suffices to show that each S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals S_i or 0. In the first case, $S_i \subset W + S_J$, and in the second $S_J \cap S_i = 0$ and $W \cap (S_J + S_i) = 0$, contradicting the definition of I . \square

LEMMA 8.69 *Suppose that k is algebraically closed. Every normal subgroup of an algebraic group G over k occurs as the kernel of representation of G .*

PROOF. Let N be a normal subgroup of G . According to Chevalley's theorem 8.57, N is the stabilizer of a line L in a representation V of G . Let N act on L through the character χ . After possibly replacing (V, L) with a second pair, we shall find a G -module U and a line L' in U such that N acts on L' through χ and L' is a direct summand of U as an N -module. Then U^\vee contains a line L^\vee on which N acts through the character χ^{-1} , and $L \otimes L^\vee \subset (V \otimes U^\vee)^N$. If an element α of $G(R)$ acts trivially on $(V \otimes U^\vee)_R^N$, then it acts trivially on $(L \otimes L^\vee)_R$, and so it stabilizes L_R in V_R (by 8.66); hence $\alpha \in N(R)$. Therefore N is the kernel of the representation of G on $(V \otimes U^\vee)^N$.

It remains to construct U . Suppose first that G is smooth. In this case, we take U to be the smallest G -stable subspace of V containing L . The subspace $\sum_{g \in G(k)} gL$ of V is stable under $G(k)$, hence under G (8.53), and so equals U . According to Lemma 8.68, U decomposes into a direct sum $U = \bigoplus_{i \in I} L_i$ of lines L_i stable under N , one of which can be taken to be L .

If G is not smooth, then the characteristic of k is $p \neq 0$, and there exists an n such that $\mathcal{O}(G)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(G)$ (see 6.35). In this case, we replace V by $V^{\otimes p^n}$ and L by $L^{\otimes p^n}$ — Proposition 8.54 shows that N is still the stabilizer of L . Let G' be the quotient of G such that $\mathcal{O}(G') = \mathcal{O}(G)^{p^n}$. Choose a basis $(e_i)_{i \in I}$ for V containing a nonzero element e of L . Write

$$\rho(e) = e \otimes a + \sum_{e_i \neq e} e_i \otimes a_i, \quad a_{i1} \in \mathfrak{a} = \text{Ker}(\mathcal{O}(G) \rightarrow \mathcal{O}(N)). \quad (84)$$

In replacing L with $L^{\otimes p^n}$, we replaced the original a with a^{p^n} , which now lies in $\mathcal{O}(G')$. Let $L' = \langle a \rangle \subset \mathcal{O}(G')$, and consider the representation

$$G \rightarrow G' \rightarrow \text{GL}_{\mathcal{O}(G')}$$

of G on $\mathcal{O}(G')$. The character χ of N corresponds to the element \bar{a} of $\mathcal{O}(N)$, where \bar{a} is the image of a in $\mathcal{O}(N) = \mathcal{O}(G)/\mathfrak{a}$ (see (84)). As

$$\Delta(a) \equiv a \otimes a \pmod{\mathcal{O}(G) \otimes \mathcal{O}(G)/\mathfrak{a}},$$

N acts on the line L' through the same character χ . Because G' is smooth, we can take U to be the smallest G' -stable subspace of $\mathcal{O}(G')$ containing L' , as in the paragraph above. \square

THEOREM 8.70 *Let N be a normal subgroup of an algebraic group G . The universal surjective homomorphism $G \rightarrow Q$ containing N in its kernel (see 7.63) has kernel exactly N .*

PROOF. Lemma 8.69 shows that, over some finite extension k' of k , there exists a homomorphism $G_{k'} \rightarrow H$ with kernel $N_{k'}$. The kernel of $G \rightarrow \Pi_{k'/k} H$ is N . From the universal property of $G \rightarrow Q$, we see that $\text{Ker}(G \rightarrow Q) \subset N$, and hence the two are equal. \square

COROLLARY 8.71 *For any distinct normal subgroups $N \subset N'$ of an affine group G , there exists a representation of G on which N acts trivially but N' acts nontrivially.*

PROOF. Let $Q = G/N$ be the quotient of G by N , and let $Q \rightarrow \text{GL}_V$ be a faithful representation of Q . The composite $G \rightarrow Q \rightarrow \text{GL}_V$ is the required representation. \square

8r Variant of the proof of the key Lemma 8.69

LEMMA 8.72 *Let (V, r) be a finite-dimensional faithful representation of an algebraic group G , and let N be the kernel of the representation of G on $V^\vee \otimes V$. Then*

$$N(R) = \{\alpha \in G(R) \mid \text{there exists a } c \in R \text{ such that } \alpha x = cv \text{ for all } v \in V\}.$$

In other words, for any subgroup G of GL_V , the subgroup of G acting trivially on $V^\vee \otimes V$ is the subgroup acting on V by scalars.

PROOF. Let $(e_i)_{1 \leq i \leq n}$ be a basis for V , and let $e_{ij} = e_i^\vee \otimes e_j$. Let α be endomorphism of V_R for some k -algebra R . A direct calculation shows that $\alpha(e_{ij}) = e_{ij}$ for all i, j if and only if there exists a $c \in R$ such that $\alpha e_i = c e_i$ for all i . \square

LEMMA 8.73 *Let G be an algebraic group, and let H be a subgroup of G . The following are equivalent:*

- (a) H is normal in G ;
- (b) for each representation V of G and k -character χ of H , the subspace V^χ of V on which H acts through χ is stable under G ;
- (c) every H -isotypic component of a representation of G is stable under G .

PROOF. See André 1992, Lemma 1. (We sketch the proof of (a) \implies (b). For any $g \in G(k)$, $gV^\chi = V^{g\chi}$, but the action of G on the set of k -characters of H is trivial, because G is connected and the set is discrete. When G is smooth, this is shown in the proof of (16.31).) \square

We now prove that every normal subgroup N of a connected algebraic group G occurs as the kernel of a representation of G (without assumption on the field k). Let L be a line in a representation V of G such that $G_L = N$. Then N acts on L through a character χ . Let W be the smallest G -stable subspace of V containing L . Then $W \subset V^\chi$ by (8.73), and so N is contained in the kernel H of $G \rightarrow \text{GL}_{W^\vee \otimes W}$. According to (8.72), H acts on W through a k -character. In particular, it stabilizes L , and so $H \subset N$.

8s Applications of Corollary 8.71

LEMMA 8.74 *Let N_1 and N_2 be normal subgroups of an affine group G . If $\text{Rep}(G)^{N_1} = \text{Rep}(G)^{N_2}$ then $N_1 = N_2$.*

PROOF. If $N_1 \neq N_2$, then Corollary 8.71 shows that there exists a representation (V, r) of G and a $v \in V$ fixed by N_1 but not by $N_1 N_2$. Then V^{N_1} is an object of $\text{Rep}(G)^{N_1}$ but not of $\text{Rep}(G)^{N_2}$, which contradicts the hypothesis. \square

THEOREM 8.75 *Let N be a normal subgroup of an affine group G , and let Q be a quotient of G . Then $N = \text{Ker}(G \rightarrow Q)$ if and only if $\text{Rep}(G)^N = Q^\vee$.*

PROOF. \implies : According to Theorem 7.56, a representation $r: G \rightarrow \text{GL}_V$ factors through Q (and so lies in Q^\vee) if and only if r maps N to 1 (and so (V, r) lies in $\text{Rep}(G)^N$).

\impliedby : Let N' be the kernel of $G \rightarrow Q$. Then $\text{Rep}(G)^{N'} = Q^\vee$, and so $\text{Rep}(G)^N = \text{Rep}(G)^{N'}$. This implies that $N = N'$. \square

COROLLARY 8.76 *The map $N \mapsto \text{Rep}(G)^N$ is a bijection from the set of normal subgroups of G to the set of replete subcategories of $\text{Rep}(G)$ closed under tensor products and passage to the contragredient.*

PROOF. Let \mathbf{S} be a replete subcategory of $\text{Rep}(G)$ closed under tensor products and passage to the contragredient. The $\mathbf{S} = Q^\vee$ for some quotient Q of G , well-defined up to isomorphism, and the kernel N of $G \rightarrow Q$ is a normal subgroup of G . The maps $\mathbf{S} \mapsto N$ and $N \mapsto \text{Rep}(G)^N$ are inverse. \square

THEOREM 8.77 *For any normal subgroup N of an affine group G , there exists a quotient map with kernel N .*

PROOF. The subcategory $\text{Rep}(G)^N$ of $\text{Rep}(G)$ is replete and closed under tensor products and passage to the contragredient. Therefore $\text{Rep}(G)^N = Q^\vee$ for some quotient Q of G , and the Theorem 8.75 implies that N is the kernel of $G \rightarrow Q$. \square

NOTES Add a discussion of the correspondence between normal subgroups of an affine group G and the normal Hopf ideals in $\mathcal{O}(G)$ (Abe 1980, p. 179), and also of the correspondence between normal Hopf ideals and Hopf subalgebras (ibid. 4.4.7, p. 207, in the case that k is algebraically closed and the Hopf algebras are assumed to be reduced).

NOTES Add a discussion of the general theorem on the existence of quotients of group schemes over artinian rings (SGA3, VI_A).

9 Group theory: the isomorphism theorems

In this section, we show that the (Noether) isomorphism theorems in abstract group theory hold also for affine groups.

9a Review of abstract group theory

For a group G (in the usual sense), we have the notions of subgroup, a normal subgroup, an embedding (injective homomorphism), and of a quotient map (surjective homomorphism). Moreover, there are the following basic results, which are often referred to collectively as the isomorphisms theorems.³²

9.1 (Existence of quotients). The kernel of a quotient map $G \rightarrow Q$ is a normal subgroup of G , and every normal subgroup N of G arises as the kernel of a quotient map $G \rightarrow G/N$.

9.2 (Homomorphism theorem). The image of a homomorphism $\alpha: G \rightarrow G'$ is a subgroup αG of G' , and α defines an isomorphism from $G/\text{Ker}(\alpha)$ onto αG ; in particular, every homomorphism is the composite of a quotient map and an embedding.

³²Statements (9.2), (9.3), and (9.4) are sometimes called the first, second, and third isomorphism theorems, but the numbering varies. In Noether 1927, the first isomorphism theorem is (9.4) and the second is (9.3).

9.3 (Isomorphism theorem). Let H and N be subgroups of G such that H normalizes N ; then HN is a subgroup of G , N is a normal subgroup of HN , $H \cap N$ is a normal subgroup of H , and the map

$$h(H \cap N) \mapsto hN: H/H \cap N \rightarrow HN/N$$

is an isomorphism.

9.4 (Correspondence theorem). Let N be a normal subgroup of G . The map $H \mapsto H/N$ defines a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N . A subgroup H of G containing N is normal if and only if H/N is normal in G/N , in which case the map

$$G/H \rightarrow (G/N)/(H/N)$$

defined by the quotient map $G \rightarrow G/N$ is an isomorphism.

In this section, we shall see that, appropriately interpreted, all these notions and statements extend to affine groups (in particular, to algebraic groups).

9b The existence of quotients

See Theorem 8.70.

EXAMPLE 9.5 Let PGL_n be the quotient of GL_n by its centre, and let PSL_n be the quotient of SL_n by its centre:

$$\mathrm{PGL}_n = \mathrm{GL}_n / \mathbb{G}_m, \quad \mathrm{PSL}_n = \mathrm{SL}_n / \mu_n.$$

The homomorphism $\mathrm{SL}_n \rightarrow \mathrm{GL}_n \rightarrow \mathrm{PGL}_n$ contains μ_n in its kernel, and so defines a homomorphism

$$\mathrm{PSL}_n \rightarrow \mathrm{PGL}_n. \quad (85)$$

Is this an isomorphism? Note that

$$\mathrm{SL}_n(k) / \mu_n(k) \rightarrow \mathrm{GL}_n(k) / \mathbb{G}_m(k) \quad (86)$$

is injective, but not in general surjective: not every invertible $n \times n$ matrix can be written as the product of a matrix with determinant 1 and a scalar matrix (such a matrix has determinant in $k^{\times n}$). Nevertheless, I claim that (85) is an isomorphism of algebraic groups. In characteristic zero, this follows from the fact that (86) is an isomorphism when $k = k^{\mathrm{al}}$ (apply 7.18 and 7.54). In the general case, we have to check the conditions (7.2a) and (7.50).

Let $q \neq 1 \in \mathrm{PSL}_n(R)$. For some faithfully flat R -algebra R' , there exists a $g \in \mathrm{SL}_n(R')$ mapping to q in $\mathrm{PSL}_n(R')$. The image of g in $\mathrm{GL}_n(R')$ is not in $\mathbb{G}_m(R')$ (because $q \neq 1$); therefore, the image of g in $\mathrm{PGL}_n(R')$ is $\neq 1$, which implies that the image of q in $\mathrm{PGL}_n(R)$ is $\neq 1$:

$$\begin{array}{ccc} \mathrm{PSL}_n(R') & \longrightarrow & \mathrm{PGL}_n(R') \\ \uparrow & & \uparrow \text{injective} \\ \mathrm{PSL}_n(R) & \longrightarrow & \mathrm{PGL}_n(R). \end{array}$$

We have checked condition (7.2a).

Let $q \in \mathrm{PGL}_n(R)$. For some faithfully flat R -algebra R' , there exists a $g \in \mathrm{GL}_n(R')$ mapping to q . If $a \stackrel{\mathrm{def}}{=} \det(g)$ is an n th power, say $a = t^n$, then $g = g_0 t$ with $\det(g_0) = 1$, and the image of g in $\mathrm{GL}_n(R')/\mathbb{G}_m(R')$ is in the image of $\mathrm{SL}_n(R')/\mu_n(R')$. Hence, the image of q in $\mathrm{PGL}_n(R')$ is in the image of $\mathrm{PSL}_n(R')$. If a is not an n th power in R' , we replace R' by the faithfully flat (even free) algebra $R'[T]/(T^n - a)$ in which it does become an n th power. We have checked condition (7.50).

9c The homomorphism theorem

A homomorphism $\alpha: G \rightarrow G'$ of affine groups defines a homomorphism $\alpha^*: \mathcal{O}(G') \rightarrow \mathcal{O}(G)$ of Hopf algebras, whose kernel \mathfrak{a} is a Hopf ideal in $\mathcal{O}(G')$.³³ Thus

$$\mathfrak{a} = \{f \in \mathcal{O}(G') \mid f_R(\alpha_R(P)) = 0 \text{ for all } k\text{-algebras } R \text{ and all } P \in G(R)\}.$$

The subgroup H of G' corresponding to \mathfrak{a} (see 7.8) is called the **image** of α (and often denoted αG). Thus

$$H(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for } f \in \mathfrak{a}\}.$$

THEOREM 9.6 (Homomorphism theorem) *For any homomorphism $\alpha: G \rightarrow G'$ of affine groups, the kernel N of α is a normal subgroup of G , the image αG of α is a subgroup of G' , and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & G' \\ \text{surjective} \downarrow & & \uparrow \text{injective} \\ G/N & \xrightarrow{\text{isomorphism}} & \alpha G. \end{array}$$

If G is an algebraic group, then so also are G/N and αG .

PROOF. The factorization

$$\mathcal{O}(G) \leftarrow \mathcal{O}(G')/\mathfrak{a} \leftarrow \mathcal{O}(G')$$

of α^* defines a factorization

$$G \rightarrow \alpha G \rightarrow G'$$

of α into a surjection followed by an injection. As $G \rightarrow G/N$ and $G \rightarrow \alpha G$ are both quotient maps with kernel N , there is a unique isomorphism $G/N \rightarrow \alpha G$ such that the composite

$$G \rightarrow G/N \rightarrow \alpha G$$

is $G \xrightarrow{\alpha} \alpha G$ (apply 7.57).

The final statement follows from (8.28). □

³³In fact, we don't need to use that \mathfrak{a} is a Hopf ideal, just that it is an ideal.

COROLLARY 9.7 For any k -algebra R ,

$$(\alpha G)(R) = \bigcup_{R'} G(R) \cap \text{Im} \alpha(R') \quad (R' \text{ runs over the } R\text{-algebras}).$$

Therefore αG represents the sheaf associated with

$$R \rightsquigarrow \text{Im}(\alpha(R)).$$

Moreover, αG is the intersection of the subgroups H of G' with the property that $\text{Im} \alpha(R) \subset H(R)$ for all k -algebras R .

PROOF. The map $G \rightarrow \alpha G$ is a quotient map, and so the first statement follows from (7.73). If H is a subgroup of G' such that $H(R) \supset \text{Im} \alpha(R)$ for all k -algebras R , then, for any fixed k -algebra R ,

$$H(R) \supset \bigcup_{R'} G(R) \cap \text{Im} \alpha(R') = (\alpha G)(R),$$

and so $H \supset \alpha G$. □

COROLLARY 9.8 A homomorphism $\alpha: G \rightarrow G'$ of algebraic groups is surjective if, for some field K containing k , the image of $G(K)$ in $G'(K)$ is dense in G' .

PROOF. As $\alpha(G(K)) \subset (\alpha G)(K) \subset G'(K)$, the condition implies that $\alpha G = G$. □

Let $\alpha: G \rightarrow G'$ be a homomorphism of algebraic groups. Then $G(k^{\text{al}}) \rightarrow (\alpha G)(k^{\text{al}})$ is surjective (see 7.54), and so

$$\begin{aligned} (\alpha G)(k) &= G'(k) \cap (\alpha G)(k^{\text{al}}) \\ &= G'(k) \cap \text{Im}(G(k^{\text{al}}) \xrightarrow{\alpha(k^{\text{al}})} G'(k^{\text{al}})). \end{aligned}$$

9d The isomorphism theorem

Let H and N be algebraic subgroups of G such that H normalizes N . The natural action of $H(R)$ on $N(R)$ defines an action θ of H on N by group homomorphisms, and multiplication defines a homomorphism

$$N \rtimes_{\theta} H \rightarrow G.$$

We define $NH = HN$ to be the image of this homomorphism. The following statements are obvious from §9c.

9.9 For any k -algebra R , $(HN)(R)$ consists of the elements of $G(R)$ that lie in $H(R')N(R')$ for some finitely generated faithfully flat R -algebra R' . Therefore NH represents the sheaf associated with the functor

$$R \rightsquigarrow H(R) \cdot N(R) \subset G(R).$$

Moreover, NH is the intersection of the subgroups G' of G such that, for all k -algebras R , $G'(R)$ contains both $H(R)$ and $N(R)$.

9.10 We have

$$(HN)(k^{\text{al}}) = H(k^{\text{al}}) \cdot N(k^{\text{al}}),$$

and so

$$(HN)(k) = G(k) \cap (H(k^{\text{al}}) \cdot N(k^{\text{al}})).$$

9.11 It is not true that $(HN)(R) = H(R)N(R)$ for all k -algebras R . For example, consider the algebraic subgroups SL_n and \mathbb{G}_m (nonzero scalar matrices) of GL_n . Then $\text{GL}_n = \text{SL}_n \cdot \mathbb{G}_m$, but a matrix $A \in \text{GL}_n(R)$ whose determinant is not an n th power is not the product of a scalar matrix with a matrix of determinant 1.

THEOREM 9.12 (Isomorphism theorem) Let H and N be algebraic subgroups of the algebraic group G such that H normalizes N . The natural map

$$H/H \cap N \rightarrow HN/N \tag{87}$$

is an isomorphism.

PROOF. We have an isomorphism of group-valued functors

$$H(R)/(H \cap N)(R) \rightarrow H(R)N(R)/N(R) \subset (HN)(R)/N(R).$$

The statement now follows from (7.73), or by passing to the associated sheaves. \square

EXAMPLE 9.13 Let $G = \text{GL}_n$, $H = \text{SL}_n$, and $N = \mathbb{G}_m$ (scalar matrices in G). Then $N \cap H = \mu_n$ (obviously), $HN = \text{GL}_n$ (by the arguments in 9.5), and (87) becomes the isomorphism

$$\text{SL}_n / \mu_n \rightarrow \text{GL}_n / \mathbb{G}_m.$$

9e The correspondence theorem

THEOREM 9.14 (Correspondence theorem). Let N be a normal algebraic subgroup of G . The map $H \mapsto H/N$ defines a one-to-one correspondence between the set of algebraic subgroups of G containing N and the set of algebraic subgroups of G/N . An algebraic subgroup H of G containing N is normal if and only if H/N is normal in G/N , in which case the map

$$G/H \rightarrow (G/N)/(H/N) \tag{88}$$

defined by the quotient map $G \rightarrow G/N$ is an isomorphism.

PROOF. The first statement follows from the fact that the analogous statement holds for Hopf algebras (cf. Exercise 5-10). For the second statement, note that the map

$$G(R)/H(R) \rightarrow (G(R)/N(R))/(H(R)/N(R))$$

defined by the quotient map $G(R) \rightarrow G(R)/N(R)$ is an isomorphism. This isomorphism is natural in R , and when we pass to the associated sheaves, we obtain the isomorphism (88). \square

ASIDE 9.15 Let $q: G \rightarrow G/N$ be the quotient map. For any subgroup H of G , qH is a subgroup of G/N , which corresponds to H/N . Deduce that if H' is normal in H , then $H'N$ is normal in HN .

NOTES Need to discuss how much of the isomorphism theorems hold for smooth groups. Should move the smoothness part of (17.1) here.

9f The Schreier refinement theorem

LEMMA 9.16 (BUTTERFLY LEMMA) *Let $H_1 \supset N_1$ and $H_2 \supset N_2$ be algebraic subgroups of an algebraic group G with N_1 and N_2 normal in H_1 and H_2 . Then $N_1(H_1 \cap H_2)$ and $N_2(N_1 \cap H_2)$ are normal algebraic subgroups of the algebraic groups $N_1(H_1 \cap H_2)$ and $N_2(H_2 \cap H_1)$ respectively, and there is a canonical isomorphism of algebraic groups*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}$$

PROOF. The algebraic group $H_1 \cap H_2$ is normal in $H_1 \cap H_2$ and so $N_1(H_1 \cap H_2)$ is normal in $N_1(H_1 \cap H_2)$ (see Exercise 7-2). Similarly, $N_2(H_2 \cap N_1)$ is normal in $N_2(H_2 \cap H_1)$.

The subgroup $H_1 \cap H_2$ of G normalizes $N_1(H_1 \cap N_2)$, and so the isomorphism Theorem 9.12 shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \simeq \frac{(H_1 \cap H_2) \cdot N_1(H_1 \cap N_2)}{N_1(H_1 \cap N_2)}. \quad (89)$$

As $H_1 \cap N_2 \subset H_1 \cap H_2$, we have that $H_1 \cap H_2 = (H_1 \cap H_2)(H_1 \cap N_2)$, and so

$$N_1 \cdot (H_1 \cap H_2) = N_1 \cdot (H_1 \cap H_2) \cdot (H_1 \cap N_2).$$

The first of Dedekind's modular laws (Exercise 7-3a) with $A = H_1 \cap N_2$, $B = H_1 \cap H_2$, and $C = N_1$ becomes

$$\begin{aligned} (H_1 \cap H_2) \cap N_1(H_1 \cap N_2) &= (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) \\ &= (H_1 \cap N_2)(N_1 \cap H_2). \end{aligned}$$

Therefore (89) is an isomorphism

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}.$$

A symmetric argument shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)},$$

and so

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)}. \quad \square$$

A **subnormal series** in an affine group G is a finite sequence of subgroups, beginning with G and ending with 1 , such that each subgroup is normal in the preceding subgroup.

PROPOSITION 9.17 *Let H be a subgroup of an affine group G . If*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

is a subnormal series for G , then

$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_s = \{1\}$$

is a subnormal series for H , and

$$H \cap G_i / H \cap G_{i+1} \hookrightarrow G_i / G_{i+1}.$$

PROOF. Obvious. □

Two subnormal sequences

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\}$$

are said to be **equivalent** if $s = t$ and there is a permutation π of $\{1, 2, \dots, s\}$ such that $G_i/G_{i+1} \approx H_{\pi(i)}/H_{\pi(i)+1}$.

THEOREM 9.18 *Any two subnormal series in an algebraic group have equivalent refinements.*

PROOF. Let $G_{ij} = G_{i+1}(H_j \cap G_i)$ and let $H_{ji} = H_{j+1}(G_i \cap H_j)$. According to the butterfly lemma

$$G_{ij}/G_{i,j+1} \simeq H_{ji}/H_{j,i+1},$$

and so the refinement (G_{ij}) of (G_i) is equivalent to the refinement (H_{ji}) of (H_i) . □

A subnormal series is a **composition series** if no quotient group G_i has a proper nontrivial normal subgroup.

THEOREM 9.19 *For any two composition series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\},$$

$s = t$ and there is a permutation π of $\{1, 2, \dots, s\}$ such that G_i/G_{i+1} is isomorphic to $H_{\pi(i)}/H_{\pi(i)+1}$ for each i .

PROOF. Use that, for each i , only one of the quotients $G_{i+1}(H_j \cap G_i)/G_{i+1}(H_{j+1} \cap G_i)$ is nontrivial □

An algebraic group is **strongly connected** if it has no finite quotient. An algebraic group G with $\dim G > 0$ is **almost-simple** if for any proper normal subgroup N we have $\dim N < \dim G$. An almost-simple group is strongly connected.

THEOREM 9.20 *Let G be a strongly connected algebraic group. There exists a subnormal sequence*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

such that each G_i is strongly connected and G_i/G_{i+1} is almost-simple. If

$$G = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\}$$

is a second such sequence, then $s = t$ and there is a permutation π of $\{1, 2, \dots, s\}$ such that G_i/G_{i+1} is isogenous to $H_{\pi(i)}/H_{\pi(i)+1}$ for each i .

9g The category of commutative algebraic groups

THEOREM 9.21 *The commutative algebraic groups over a field form an abelian category.*

PROOF. The Hom sets are commutative groups, and the composition of morphisms is bilinear. Moreover, the product $G_1 \times G_2$ of two commutative algebraic groups is both a product and a sum of G_1 and G_2 . Thus the category of commutative algebraic groups over a field is additive. Every morphism in the category has both a kernel and cokernel (7.15; 8.70), and the canonical morphism from the coimage of the morphism to its image is an isomorphism (homomorphism theorem, 9.6). Therefore the category is abelian. \square

COROLLARY 9.22 *The finitely generated co-commutative Hopf algebras over a field form an abelian category.*

ASIDE 9.23 Theorem 9.21 is generally credited to Grothendieck but, as we have seen, it is a fairly direct consequence of allowing the coordinate rings to have nilpotent elements. See SGA3, VI_A, 5.4; DG III §3, 7.4, p. 355.

Corollary 9.22 is proved purely in the context of Hopf algebras in Sweedler 1969, Chapter XVI, for finite-dimensional co-commutative Hopf algebras, and in Takeuchi 1972, 4.16, for finitely generated co-commutative Hopf algebras.

9h Exercises

EXERCISE 9-1 Let H and N be subgroups of the algebraic group G such that H normalizes N . Show that the kernel of $\mathcal{O}(G) \rightarrow \mathcal{O}(HN)$ is equal to the kernel of the composite

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes_k \mathcal{O}(G) \rightarrow \mathcal{O}(H) \otimes_k \mathcal{O}(N).$$

ASIDE 9.24 As noted earlier, in much of the expository literature (e.g., Borel 1991, Humphreys 1975, Springer 1998), “algebraic group” means “smooth algebraic group”. With this terminology, many of the results in this section become false.^{34,35} Fortunately, because of Theorem 6.31, this is only a problem in nonzero characteristic. The importance of allowing nilpotents was pointed out by Cartier (1962) more than forty years ago, but, except for Demazure and Gabriel 1970 and Waterhouse 1979, this point-of-view has not been adopted in the expository literature. Contrast our statement and treatment of the isomorphism theorems and the Schreier refinement theorem with those in Barsotti 1955a and Rosenlicht 1956.

10 Recovering a group from its representations; Jordan decompositions

By a character of a topological group, I mean a continuous homomorphism from the group to the circle group $\{z \in \mathbb{C} \mid z\bar{z} = 1\}$. A finite commutative group G can be recovered

³⁴For example, in the category of smooth groups, the homomorphism $H/H \cap N \rightarrow HN/N$ is a purely inseparable isogeny of degree q where q is the multiplicity of $H \cap N$ in the intersection product $H \bullet N$.

³⁵The situation is even worse, because these books use a terminology based on Weil’s Foundations, which sometimes makes it difficult to understand their statements. For example, in Humphreys 1975, p. 218, one finds the following statement: “for a homomorphism $\varphi: G \rightarrow G'$ of k -groups, the kernel of φ need not be defined over k .” By this, he means the following: form the kernel N of $\varphi_{k^{\text{al}}}: G_{k^{\text{al}}} \rightarrow G'_{k^{\text{al}}}$ (in our sense); then N_{red} need not arise from a smooth algebraic group over k . Of course, with our (or any reasonable) definitions, the kernel of a homomorphism of algebraic groups over k is certainly an algebraic group over k .

from its group G^\vee of characters because the canonical homomorphism $G \rightarrow G^{\vee\vee}$ is an isomorphism.

More generally, a locally compact commutative topological group G can be recovered from its character group because, again, the canonical homomorphism $G \rightarrow G^{\vee\vee}$ is an isomorphism (Pontryagin duality). Moreover, the dual of a compact commutative group is a discrete commutative group, and so, the study of compact commutative topological groups is equivalent to that of discrete commutative groups.

Clearly, “commutative” is required in the above statements, because any character will be trivial on the derived group. However, Tannaka showed that it is possible to recover a compact noncommutative group from its category of unitary representations.

In this section, we prove the analogue of this for algebraic groups. Initially, k is allowed to be a commutative ring.

10a Recovering a group from its representations

Let G be an affine monoid with coordinate ring A , and let $r_A: G \rightarrow \text{End}_A$ be the regular representation. Recall that $g \in G(R)$ acts on $f \in A$ according to the rule:

$$(gf)_R(x) = f_R(x \cdot g) \text{ all } x \in G(R). \quad (90)$$

LEMMA 10.1 *Let G be an affine monoid over a ring k , and let $A = \mathcal{O}(G)$. Let α be an endomorphism of A (as a k -algebra) such that the diagram*

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \downarrow \alpha & & \downarrow 1 \otimes \alpha \\ A & \xrightarrow{\Delta} & A \otimes A \end{array}$$

commutes. Then there exists a unique $g \in G(k)$ such that $\alpha = r_A(g)$.

PROOF. According to the Yoneda lemma, there exists morphism $\phi: G \rightarrow G$ of set-valued functors such that

$$(\alpha f)_R(x) = f_R(\phi_R x) \text{ all } f \in A, x \in G(R). \quad (91)$$

The commutativity of the diagram says that, for $f \in A$,

$$(\Delta \circ \alpha)(f) = ((1 \otimes \alpha) \circ \Delta)(f).$$

Recall that $(\Delta f)_R(x, y) = f_R(x \cdot y)$ for $f \in A$ (see (38), p. 48). Therefore, for $x, y \in G(R)$,

$$\begin{aligned} (\text{LHS})_R(x, y) &= (\alpha f)_R(x \cdot y) = f_R(\phi_R(x \cdot y)) \\ (\text{RHS})_R(x, y) &= (\Delta f)_R(x, \phi_R y) = f_R(x \cdot \phi_R y).^{36} \end{aligned}$$

Hence

$$\phi_R(x \cdot y) = x \cdot \phi_R(y), \quad \text{all } x, y \in G(R).$$

On setting $y = e$ in the last equation, we find that $\phi_R(x) = x \cdot g$ with $g = \phi_R(e)$. Therefore, for $f \in A$ and $x \in G(R)$,

$$(\alpha f)_R(x) \stackrel{(91)}{=} f_R(x \cdot g) \stackrel{(90)}{=} (gf)_R(x).$$

Hence $\alpha = r_A(g)$.

The uniqueness of g follows from the faithfulness of the regular representation (8.31). \square

THEOREM 10.2 *Let G be an affine monoid (or group) over a field k , and let R be a k -algebra. Suppose that we are given, for each finite-dimensional representation $r_V: G \rightarrow \text{End}_V$ of G , an R -linear map $\lambda_V: V_R \rightarrow V_R$. If the family (λ_V) satisfies the conditions,*

(a) *for all representations V, W ,*

$$\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W,$$

(b) *$\lambda_{\mathbf{1}}$ is the identity map (here $\mathbf{1} = k$ with the trivial action)*

(c) *for all G -equivariant maps $\alpha: V \rightarrow W$,*

$$\lambda_W \circ \alpha_R = \alpha_R \circ \lambda_V,$$

then there exists a unique $g \in G(R)$ such that $\lambda_V = r_V(g)$ for all V .

PROOF. Recall (8.17) that every representation of G is a filtered union of finite-dimensional representations. It follows from (c) that, for each representation $r_V: G \rightarrow \text{GL}_V$ of G (possibly infinite dimensional), there exists a unique R -linear endomorphism λ_V of V_R such that $\lambda_V|_W = \lambda_W$ for each finite-dimensional subrepresentation $W \subset V$. The conditions (a,b,c) will continue to hold for the enlarged family.

Let $A = \mathcal{O}(G)_R$, and let $\lambda_A: A \rightarrow A$ be the R -linear map corresponding to the regular representation r of G on $\mathcal{O}(G)$. The map $m: A \otimes A \rightarrow A$ is equivariant for the representations $r \otimes r$ and r ,³⁷ and so the first two diagrams in (10.1) commute with α and $\alpha \otimes \alpha$ replaced by λ_A and $\lambda_{A \otimes A} = \lambda_A \otimes \lambda_A$ respectively. Similarly, the map $\Delta: A \rightarrow A \otimes A$ is

³⁶In detail, let $\Delta f = \sum f_i \otimes g_i$; then

$$\begin{aligned} (\text{RHS})_R(x, y) &= (\sum_i f_i \otimes \alpha g_i)_R(x, y) \\ &= \sum_i f_{iR}(x) \cdot (\alpha g_i)_R(y) \\ &= \sum_i f_{iR}(x) \cdot g_{iR}(\phi_R y) \\ &= (\sum_i f_i \otimes g_i)_R(x, \phi_R y) \\ &= (\Delta f)_R(x, \phi_R y). \end{aligned}$$

³⁷We check that, for $x \in G(R)$,

$$\begin{aligned} (r(g) \circ m)(f \otimes f')(x) &= (r(g)(ff'))(x) = (ff')(xg) = f(xg) \cdot f'(xg) \\ (m \circ r(g) \otimes r(g))(f \otimes f')(x) &= ((r(g)f) \cdot (r(g)f'))(x) = f(xg) \cdot f'(xg). \end{aligned}$$

equivariant for the representation $1 \otimes r$ on $A \otimes A$, and so the third diagram in (10.1) commutes with α replaced by λ_A . Now Lemma 10.1, applied to the affine monoid G_R over R , shows that there exists a $g \in G(R)$ such $\lambda_A = r(g)$.

Let (V, r_V) be a finite-dimensional representation of G . For any $u \in V^\vee$, the linear map $\phi_u: V \rightarrow A$ is equivariant (see 8.35), and so

$$\phi_u \circ \lambda_V = \lambda_A \circ \phi_u = r(g) \circ \phi_u = \phi_u \circ r_V(g).$$

As the family of maps ϕ_u ($u \in V^\vee$) is injective (8.36), this implies that $\lambda_V = r_V(g)$.

This proves the existence of g , and the uniqueness follows the fact that G admits a faithful family of finite-dimensional representations (see 8.32). \square

We close this subsection with a series of remarks.

10.3 Each $g \in G(R)$ of course defines such a family. Thus, from the category $\text{Rep}(G)$ of representations of G on finite-dimensional k -vector spaces we can recover $G(R)$ for any k -algebra R , and hence the group G itself. For this reason, Theorem 10.2 is often called the *reconstruction theorem*.

10.4 Let (λ_V) be a family satisfying the conditions (a,b,c) of Theorem 10.4. When G is an affine group (rather than just a monoid), each λ_V is an isomorphism, and the family satisfies the condition $\lambda_{V^\vee} = (\lambda_V)^\vee$ (because this is true of the family $(r_V(g))$).

10.5 Let ω_R be the forgetful functor $\text{Rep}_R(G) \rightarrow \text{Mod}_R$, and let $\text{End}^\otimes(\omega_R)$ be the set of natural transformations $\lambda: \omega_R \rightarrow \omega_R$ commuting with tensor products — the last condition means that λ satisfies conditions (a) and (b) of the theorem. The theorem says that the canonical map $G(R) \rightarrow \text{End}^\otimes(\omega_R)$ is an isomorphism. Now let $\underline{\text{End}}^\otimes(\omega)$ denote the functor $R \mapsto \text{End}^\otimes(\omega_R)$; then $G \simeq \underline{\text{End}}^\otimes(\omega)$. When G is a group, this can be written $G \simeq \underline{\text{Aut}}^\otimes(\omega)$.

10.6 Suppose that k is algebraically closed and that G is reduced, so that $\mathcal{O}(G)$ can be identified with a ring of k -valued functions on $G(k)$. It is possible to give an explicit description of $\mathcal{O}(G)$ in terms of the representations of G . For each representation (V, r_V) of G (over k) and $u \in V^\vee$, we have a function ϕ_u on $G(k)$,

$$\phi_u(g) = \langle u, r_V(g) \rangle \in k.$$

Then $\phi_u \in \mathcal{O}(G)$, and every element of $\mathcal{O}(G)$ arises in this way (cf. Springer 1998, p.39, and Exercise 5-2).

10.7 Let H be a subgroup of an algebraic group G . For each k -algebra R , let $H'(R)$ be the subgroup of $G(R)$ fixing all tensors in all representations of G fixed by H . The functor $R \rightsquigarrow H'(R)$ is representable by a subgroup H' of G , which clearly contains H . It follows from the theorem that $H' = H$.

10.8 In (10.7), instead of all representations of G , it suffices to choose a faithful representation V and take all quotients of subrepresentations of a direct sum of representations of the form $\otimes^n(V \oplus V^\vee)$ (by 8.44).

10.9 In general, we can't omit "quotients of" from (10.8).³⁸ However, we can omit it if some nonzero multiple of every homomorphism $H \rightarrow \mathbb{G}_m$ extends to a homomorphism $G \rightarrow \mathbb{G}_m$ (8.59).

10.10 Lemma 10.1 and its proof are valid with k a commutative ring. Therefore (using 8.10), one sees that Theorem 10.2 holds with k a noetherian ring and $\text{Rep}_k(G)$ the category of representations of G on finitely generated k -modules, or with k a Dedekind domain, G a flat group scheme, and $\text{Rep}_k(G)$ the category of representations of G on finitely generated projective k -modules (or even finitely generated free k -modules).

10b Application to Jordan decompositions

We now require k to be a field.

THE JORDAN DECOMPOSITION OF A LINEAR MAP

In this subsection, we review some linear algebra.

Recall that an endomorphism α of a vector space V is *diagonalizable* if V has a basis of eigenvectors for α , and that it is *semisimple* if it becomes diagonalizable after an extension of the base field k . For example, the linear map $x \mapsto Ax: k^n \rightarrow k^n$ defined by an $n \times n$ matrix A is diagonalizable if and only if there exists an invertible matrix P with entries in k such that PAP^{-1} is diagonal, and it is semisimple if and only if there exists such a matrix P with entries in some field containing k .

From linear algebra, we know that α is semisimple if and only if its minimum polynomial $m_\alpha(T)$ has distinct roots; in other words, if and only if the subring $k[\alpha] \simeq k[T]/(m_\alpha(T))$ of $\text{End}_k(V)$ generated by α is separable.

Recall that an endomorphism α of a vector space V is *nilpotent* if $\alpha^m = 0$ for some $m > 0$, and that it is *unipotent* if $\text{id}_V - \alpha$ is nilpotent. Clearly, if α is nilpotent, then its minimum polynomial divides T^m for some m , and so the eigenvalues of α are all zero, even in k^{al} . From linear algebra, we know that the converse is also true, and so α is unipotent if and only if its eigenvalues in k^{al} all equal 1.

Let α be an endomorphism of a finite-dimensional vector space V over k . We say that α *has all of its eigenvalues* in k if the characteristic polynomial $P_\alpha(T)$ of α splits in $k[X]$:

$$P_\alpha(T) = (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}, \quad a_i \in k.$$

For each eigenvalue a of α in k , the *generalized eigenspace* is defined to be:

$$V_a = \{v \in V \mid (\alpha - a)^N v = 0, \quad N \text{ sufficiently divisible}^{39}\}.$$

³⁸Consider for example, the subgroup $B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ of GL_2 acting on $V = k \times k$ and suppose that a vector $v \in (V \oplus V^\vee)^{\otimes n}$ is fixed by B . Then $g \mapsto gv$ is a regular map $\text{GL}_2/B \rightarrow (V \oplus V^\vee)^{\otimes n}$ of algebraic varieties (not affine). But $\text{GL}_2/B \simeq \mathbb{P}^1$, and so any such map is trivial. Therefore, v is fixed by GL_2 , and so $B' = B$. Cf 7.62.

³⁹By this I mean that there exists an N_0 such that the statement holds for all positive integers divisible by N_0 , i.e., that N is sufficiently large for the partial ordering

$$M \leq N \iff M \text{ divides } N.$$

PROPOSITION 10.11 *If α has all of its eigenvalues in k , then V is a direct sum of its generalized eigenspaces:*

$$V = \bigoplus_i V_{a_i}.$$

PROOF. Let $P(T)$ be a polynomial in $k[T]$ such that $P(\alpha) = 0$, and suppose that $P(T) = Q(T)R(T)$ with Q and R relatively prime. Then there exist polynomials $a(T)$ and $b(T)$ such that

$$a(T)Q(T) + b(T)R(T) = 1.$$

For any $v \in V$,

$$a(\alpha)Q(\alpha)v + b(\alpha)R(\alpha)v = v, \quad (92)$$

which implies immediately that $\text{Ker}(Q(\alpha)) \cap \text{Ker}(R(\alpha)) = 0$. Moreover, because $Q(\alpha)R(\alpha) = 0$, (92) expresses v as the sum of an element of $\text{Ker}(R(\alpha))$ and an element of $\text{Ker}(Q(\alpha))$. Thus, V is the direct sum of $\text{Ker}(Q(\alpha))$ and $\text{Ker}(R(\alpha))$.

On applying this remark repeatedly, we find that

$$V = \text{Ker}(T - a_1)^{n_1} \oplus \text{Ker}((T - a_2)^{n_2} \cdots (T - a_r)^{n_r}) = \cdots = \bigoplus_i \text{Ker}(T - a_i)^{n_i},$$

as claimed. \square

THEOREM 10.12 *Let V be a finite-dimensional vector space over a perfect field. For any automorphism α of V , there exist unique automorphisms α_s and α_u of V such that*

- (a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, and
- (b) α_s is semisimple and α_u is unipotent.

Moreover, each of α_s and α_u is a polynomial in α .

PROOF. Assume first that α has all of its eigenvalues in k , so that V is a direct sum of the generalized eigenspaces of α , say, $V = \bigoplus_{1 \leq i \leq m} V_{a_i}$ where the a_i are the distinct roots of P_α . Define α_s to be the automorphism of V that acts as a_i on V_{a_i} for each i . Then α_s is a semisimple automorphism of V , and $\alpha_u \stackrel{\text{def}}{=} \alpha \circ \alpha_s^{-1}$ commutes with α_s (because it does on each V_{a_i}) and is unipotent (because its eigenvalues are 1). Thus α_s and α_u satisfy (a) and (b).

Because the polynomials $(T - a_i)^{n_i}$ are relatively prime, the Chinese remainder theorem shows that there exists a $Q(T) \in k[T]$ such that

$$Q(T) \equiv a_i \pmod{(T - a_i)^{n_i}}, \quad i = 1, \dots, m.$$

Then $Q(\alpha)$ acts as a_i on V_{a_i} for each i , and so $\alpha_s = Q(\alpha)$, which is a polynomial in α . Similarly, $\alpha_s^{-1} \in k[\alpha]$, and so $\alpha_u \stackrel{\text{def}}{=} \alpha \circ \alpha_s^{-1} \in k[\alpha]$.

It remains to prove the uniqueness of α_s and α_u . Let $\alpha = \beta_s \circ \beta_u$ be a second decomposition satisfying (a) and (b). Then β_s and β_u commute with α , and therefore also with α_s and α_u (because they are polynomials in α). It follows that $\beta_s^{-1}\alpha_s$ is semisimple and that $\alpha_u\beta_u^{-1}$ is unipotent. Since they are equal, both must equal 1. This completes the proof in this case.

In the general case, because k is perfect, there exists a finite Galois extension k' of k such that α has all of its eigenvalues in k' . Choose a basis for V , and use it to attach matrices to endomorphisms of V and $k' \otimes_k V$. Let A be the matrix of α . The first part of

the proof allows us to write $A = A_s A_u = A_u A_s$ with A_s a semisimple matrix and A_u a unipotent matrix with entries in k' ; moreover, this decomposition is unique.

Let $\sigma \in \text{Gal}(k'/k)$, and for a matrix $B = (b_{ij})$, define σB to be (σb_{ij}) . Because A has entries in k , $\sigma A = A$. Now

$$A = (\sigma A_s)(\sigma A_u)$$

is again a decomposition of A into commuting semisimple and unipotent matrices. By the uniqueness of the decomposition, $\sigma A_s = A_s$ and $\sigma A_u = A_u$. Since this is true for all $\sigma \in \text{Gal}(K/k)$, the matrices A_s and A_u have entries in k . Now $\alpha = \alpha_s \circ \alpha_u$, where α_s and α_u are the endomorphisms with matrices A_s and A_u , is a decomposition of α satisfying (a) and (b).

Finally, the first part of the proof shows that there exist $a_i \in k'$ such that

$$A_s = a_0 + a_1 A + \cdots + a_{n-1} A^{n-1} \quad (n = \dim V).$$

The a_i are unique, and so, on applying σ , we find that they lie in k . Therefore,

$$\alpha_s = a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \in k[\alpha].$$

Similarly, $\alpha_u \in k[\alpha]$. □

The automorphisms α_s and α_u are called the *semisimple* and *unipotent parts* of α , and

$$\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$$

is the (*multiplicative*) *Jordan decomposition* of α .

PROPOSITION 10.13 *Let α and β be automorphisms of vector spaces V and W over a perfect field, and let $\varphi: V \rightarrow W$ be a linear map. If $\varphi \circ \alpha = \beta \circ \varphi$, then $\varphi \circ \alpha_s = \beta_s \circ \varphi$ and $\varphi \circ \alpha_u = \beta_u \circ \varphi$.*

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k . Recall that α_s acts on each generalized eigenspace V_a , $a \in k$, as multiplication by a . As φ obviously maps V_a into W_a , it follows that $\varphi \circ \alpha_s = \beta_s \circ \varphi$. Similarly, $\varphi \circ \alpha_s^{-1} = \beta_s^{-1} \circ \varphi$, and so $\varphi \circ \alpha_u = \beta_u \circ \varphi$. □

COROLLARY 10.14 *Every subspace W of V stable under α is stable under α_s and α_u , and $\alpha|_W = \alpha_s|_W \circ \alpha_u|_W$ is the Jordan decomposition of $\alpha|_W$.*

PROOF. It follows from the proposition that W is stable under α_s and α_u , and it is obvious that the decomposition $\alpha|_W = \alpha_s|_W \circ \alpha_u|_W$ has the properties to be the Jordan decomposition. □

PROPOSITION 10.15 *For any automorphisms α and β of vector spaces V and W over a perfect field,*

$$\begin{aligned} (\alpha \otimes \beta)_s &= \alpha_s \otimes \beta_s \\ (\alpha \otimes \beta)_u &= \alpha_u \otimes \beta_u. \end{aligned}$$

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k . For any $a, b \in k$, $V_a \otimes_k W_b \subset (V \otimes_k W)_{ab}$, and so $\alpha_s \otimes \beta_s$ and $(\alpha \otimes \beta)_s$ both act on $V_a \otimes_k W_b$ as multiplication by ab . This shows that $(\alpha \otimes \beta)_s = \alpha_s \otimes \beta_s$. Similarly, $(\alpha_s^{-1} \otimes \beta_s^{-1}) = (\alpha \otimes \beta)_s^{-1}$, and so $(\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u$. \square

10.16 Let k be a nonperfect field of characteristic 2, so that there exists an $a \in k$ that is not a square in k , and let $M = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$. In $k[\sqrt{a}]$, M has the Jordan decomposition

$$M = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & 1/\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix}.$$

These matrices do not have coefficients in k , and so, if M had a Jordan decomposition in $M_2(k)$, it would have two distinct Jordan decompositions in $M_2(k[\sqrt{a}])$, contradicting the uniqueness.

INFINITE-DIMENSIONAL VECTOR SPACES

Let V be a vector space, possibly infinite dimensional, over a perfect field k . An endomorphism α of V is **locally finite** if V is a union of finite-dimensional subspaces stable under α . A locally finite endomorphism is **semisimple** (resp. **locally nilpotent**, **locally unipotent**) if its restriction to each stable finite-dimensional subspace is semisimple (resp. nilpotent, unipotent).

Let α be a locally finite automorphism of V . By assumption, every $v \in V$ is contained in a finite-dimensional subspace W stable under α , and we define $\alpha_s(v) = (\alpha|_W)_s(v)$. According to (10.12), this is independent of the choice of W , and so in this way we get a semisimple automorphism of V . Similarly, we can define α_u . Thus:

THEOREM 10.17 *For any locally finite automorphism α of V , there exist unique automorphisms α_s and α_u such that*

- (a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, and
- (b) α_s is semisimple and α_u is locally unipotent.

For any finite-dimensional subspace W of V stable under α ,

$$\alpha|_W = (\alpha_s|_W) \circ (\alpha_u|_W) = (\alpha_u|_W) \circ (\alpha_s|_W)$$

is the Jordan decomposition of $\alpha|_W$.

JORDAN DECOMPOSITIONS IN ALGEBRAIC GROUPS

Finally, we are able to prove the following important theorem.

THEOREM 10.18 *Let G be an algebraic group over a perfect field k . For any $g \in G(k)$ there exist unique elements $g_s, g_u \in G(k)$ such that, for all representations (V, r_V) of G , $r_V(g_s) = r_V(g)_s$ and $r_V(g_u) = r_V(g)_u$. Furthermore,*

$$g = g_s g_u = g_u g_s. \tag{93}$$

PROOF. In view of (10.13) and (10.15), the first assertion follows immediately from (10.2) applied to the families $(r_V(g)_s)_V$ and $(r_V(g)_u)_V$. Now choose a faithful representation r_V . Because

$$r_V(g) = r_V(g_s)r_V(g_u) = r_V(g_u)r_V(g_s),$$

(93) follows. □

The elements g_s and g_u are called the *semisimple* and *unipotent parts* of g , and $g = g_s g_u$ is the *Jordan decomposition* of g .

10.19 To check that a decomposition $g = g_s g_u$ is the Jordan decomposition, it suffices to check that $r(g) = r(g_s)r(g_u)$ is the Jordan decomposition of $r(g)$ for a single faithful representation of G .

10.20 Homomorphisms of groups preserve Jordan decompositions. To see this, let $\alpha: G \rightarrow G'$ be a homomorphism and let $g = g_s g_u$ be a Jordan decomposition in $G(k)$. For any representation $\varphi: G' \rightarrow \mathrm{GL}_V$, $\varphi \circ \alpha$ is a representation of G , and so $(\varphi \circ \alpha)(g) = ((\varphi \circ \alpha)(g_s)) \cdot ((\varphi \circ \alpha)(g_u))$ is the Jordan decomposition in $\mathrm{GL}(V)$. If we choose φ to be faithful, this implies that $\alpha(g) = \alpha(g_s) \cdot \alpha(g_u)$ is the Jordan decomposition of $\alpha(g)$.

NOTES Our proof of the existence of Jordan decompositions (Theorem 10.18) is the standard one, except that we have made Lemma 10.1 explicit. As Borel has noted (1991, p. 88; 2001, VIII 4.2, p. 169), the result essentially goes back to Kolchin 1948, 4.7.

10c Homomorphisms and functors

NOTES This section needs to be reworked. The proof of 10.22 requires the semisimplicity of the category of representations of a reductive group in characteristic zero, and so needs to be moved.

Throughout this subsection, k is a field.

PROPOSITION 10.21 *Let $f: G \rightarrow G'$ be a homomorphism of affine groups over k , and let ω^f be the corresponding functor $\mathrm{Rep}_k(G') \rightarrow \mathrm{Rep}_k(G)$.*

- (a) *f is faithfully flat if and only if ω^f is fully faithful and every subobject of $\omega^f(X)$, for $X' \in \mathrm{ob}(\mathrm{Rep}_k(G))$, is isomorphic to the image of a subobject of $\omega^f(X')$.*
- (b) *f is a closed immersion if and only if every object of $\mathrm{Rep}_k(G)$ is isomorphic to a subquotient of an object of the form of $\omega^f(X')$, $X' \in \mathrm{ob}(\mathrm{Rep}_k(G'))$.*

PROOF. (a) If $G \xrightarrow{f} G'$ is faithfully flat, and therefore an epimorphism, then $\mathrm{Rep}_k(G')$ can be identified with the subcategory of $\mathrm{Rep}_k(G)$ of representations $G \rightarrow \mathrm{GL}(W)$ factoring through G' . It is therefore obvious that ω^f has the stated properties. Conversely, if ω^f is fully faithful, it defines an equivalence of $\mathrm{Rep}_k(G')$ with a full subcategory of $\mathrm{Rep}_k(G)$, and the second condition shows that, for $X' \in \mathrm{ob}(\mathrm{Rep}_k(G'))$, $\langle X' \rangle$ is equivalent to $\langle \omega^f(X) \rangle$. Let $G = \mathrm{Spec} B$ and $G' = \mathrm{Spec} B'$; then (§11c) shows that

$$B' = \varinjlim \mathrm{End}(\omega^f|_{\langle X' \rangle})^\vee = \varinjlim \mathrm{End}(\omega^f|_{\langle \omega^f(X') \rangle})^\vee \subset \varinjlim \mathrm{End}(\omega|_{\langle X \rangle})^\vee = B,$$

and $B \rightarrow B'$ being injective implies that $G \rightarrow G'$ is faithfully flat (6.43).

(b) Let \mathbf{C} be the strictly full subcategory of $\text{Rep}_k(G)$ whose objects are isomorphic to subquotients of objects of the form $\omega^f(X')$. The functors

$$\text{Rep}_k(G') \rightarrow \mathbf{C} \rightarrow \text{Rep}_k(G)$$

correspond to homomorphisms of k -coalgebras

$$B' \rightarrow B'' \rightarrow B$$

where $G = \text{Spec } B$ and $G' = \text{Spec } B'$. An argument as in the above proof shows that $B'' \rightarrow B$ is injective. Moreover, for $X' \in \text{ob}(\text{Rep}_k(G'))$, $\text{End}(\omega|\langle\omega^f(X)\rangle) \rightarrow \text{End}(\omega|\langle X'\rangle)$ is injective, and so $B' \rightarrow B''$ is surjective. If f is a closed immersion, then $B' \rightarrow B$ is surjective and it follows that $B'' \xrightarrow{\sim} B$, and $\mathbf{C} = \text{Rep}_k(G)$. Conversely, if $\mathbf{C} = \text{Rep}_k(G)$, $B'' = B$ and $B' \rightarrow B$ is surjective. [Take a faithful representation of G' ; it is also a faithful representation of G , etc..] \square

PROPOSITION 10.22 *Let G and G' be algebraic groups over a field k of characteristic zero, and assume G° is reductive. Let $f: G \rightarrow G'$ be a homomorphism, and let $\omega^f: \text{Rep}(G') \rightarrow \text{Rep}(G)$ be the functor $(r, V) \mapsto (r \circ \lambda, V)$. Then:*

- (a) f is a quotient map if and only if ω^f is fully faithful;
- (b) f is an embedding if and if every object of $\text{Rep}_k(G)$ is isomorphic to a direct factor of an object of the form $\omega^f(V)$.

PROOF. Omitted for the present (Deligne and Milne 1982, 2.21, 2.29). \square

11 Characterizations of categories of representations

Pontryagin duality has two parts. First it shows that a locally compact abelian group G can be recovered from its dual G^\vee . This it does by showing that the canonical map $G \rightarrow G^{\vee\vee}$ is an isomorphism. Secondly, it characterizes the abelian groups that arise as dual groups. For example, it shows that the duals of discrete abelian groups are exactly the compact abelian groups, and that the duals of locally compact abelian groups are exactly the locally compact abelian groups.

In §10 we showed how to recover an algebraic group G from its “dual” $\text{Rep}(G)$ (reconstruction theorem). In this section, we characterize the categories that arise as the category of representations of an algebraic or affine group (*description theorem*).

Throughout, k is a field. In Theorems 11.1, 11.5, 11.13, and 11.14, \mathbf{C} is a small category (or, at least, admits a *set* of representatives for its isomorphism classes of objects).

11a Categories of comodules

An additive category \mathbf{C} is said to be k -**linear** if the Hom sets are k -vector spaces and composition is k -bilinear. Functors of k -linear categories are required to be k -linear, i.e., the maps $\text{Hom}(a, b) \rightarrow \text{Hom}(Fa, Fb)$ defined by F are required to be k -linear. Recall that Vec_k denotes the category of *finite-dimensional* vector spaces over k .

THEOREM 11.1 *Let \mathbf{C} be a k -linear abelian category, and let $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ be an exact faithful k -linear functor. Then there exists a coalgebra C such that \mathbf{C} is equivalent to the category of C -comodules of finite dimension.*

The proof will occupy the rest of this subsection.

For an object X in \mathbf{C} , $\omega(\text{id}_X) = \omega(0)$ if and only if $\text{id}_X = 0$. Therefore, X is the zero object if and only if $\omega(X)$ is the zero object. It follows that, if $\omega(\alpha)$ is a monomorphism (resp. an epimorphism, resp. an isomorphism), then so also is α . For objects X, Y of \mathbf{C} , $\text{Hom}(X, Y)$ is a subspace of $\text{Hom}(\omega X, \omega Y)$, and hence has finite dimension.

For monomorphisms $X \xrightarrow{x} Y$ and $X' \xrightarrow{x'} Y$ with the same target, write $x \leq x'$ if there exists a morphism $X \rightarrow X'$ (necessarily unique) giving a commutative triangle. The lattice of subobjects of Y is obtained from the collection of monomorphisms by identifying two monomorphisms x and x' if $x \leq x'$ and $x' \leq x$. The functor ω maps the lattice of subobjects of Y injectively⁴⁰ to the lattice of subspaces of ωY . Hence X has finite length.

Similarly ω maps the lattice of quotient objects of Y injectively to the lattice of quotient spaces of ωY .

For X in \mathbf{C} , we let $\langle X \rangle$ denote the full subcategory of \mathbf{C} whose objects are the quotients of subobjects of direct sums of copies of X . For example, if \mathbf{C} is the category of finite-dimensional comodules over a coalgebra C , and then $\langle V \rangle = \text{Comod}(C_V)$ for any comodule V (see 8.38).

Let X be an object of \mathbf{C} . For any subset S of $\omega(X)$, there exists a smallest subobject Y of X such that $\omega(Y) \supset S$, namely, the intersection of all such subobjects, which we call the subobject of X **generated** by S :

$$Y \subset X \quad \longrightarrow \quad S \subset \omega(Y) \subset \omega(X).$$

An object Y is **monogenic** if it is generated by a single element, i.e., there exists a $y \in \omega(Y)$ such that the only subobject Y' of Y such $y \in \omega(Y')$ is Y itself.

PROOF IN THE CASE THAT \mathbf{C} IS GENERATED BY A SINGLE OBJECT

In the next three lemmas, we assume that $\mathbf{C} = \langle X \rangle$ for an object X , and we let $n = \dim_k \omega(X)$.

LEMMA 11.2 *For any monogenic object Y of \mathbf{C} ,*

$$\dim_k \omega(Y) \leq n^2.$$

PROOF. By hypothesis, $Y = Y_1/Y_2$ where Y_1 is isomorphic to a subobject of X^m for some m . Let $y \in \omega(Y)$ generate Y , and let y_1 be an element of $\omega(Y_1)$ whose image in $\omega(Y)$ is y . Let Z be the subobject of Y_1 generated by y_1 . The image of Z in $Y = Y_1/Y_2$ is Y , and so it suffices to prove the lemma for Z , i.e., we may suppose that $Y \subset X^m$ for some m . We shall show that it is possible to take $m \leq n$, from which the statement follows.

Suppose that $m > n$. We have $y \in \omega(Y) \subset \omega(X^m) = \omega(X)^m$. Let $y = (y_1, \dots, y_m)$ in $\omega(X)^m$. Since $m > n$, there exist $a_i \in k$, not all zero, such that $\sum a_i y_i = 0$. The a_i define a surjective morphism $X^m \rightarrow X$ whose kernel N is isomorphic to X^{m-1} .⁴¹ As $y \in \omega(N)$,

⁴⁰If $\omega(X) = \omega(X')$, then the kernel of

$$\begin{pmatrix} x \\ x' \end{pmatrix}: X \times X' \rightarrow Y$$

projects isomorphically onto each of X and X' (because it does after ω has been applied).

⁴¹Let A be an $(m-1) \times m$ matrix such that $\begin{pmatrix} a_1 & \dots & a_m \\ A \end{pmatrix}$ is invertible. Then $A: X^m \rightarrow X^{m-1}$ defines an isomorphism of N onto X^{m-1} (because $\omega(A)$ does).

we have $Y \subset N$. We have shown that Y embeds into X^{m-1} . Continue in this fashion until $Y \subset X^m$ with $m \leq n$. \square

As $\dim_k \omega(Y)$ can take only finitely many values when Y is monogenic, there exists a monogenic P for which $\dim_k \omega(P)$ has its largest possible value. Let $p \in \omega(P)$ generate P .

LEMMA 11.3 (a) *The pair (P, p) represents the functor ω .*
 (b) *The object P is a projective generator⁴² for \mathbf{C} .*

PROOF. (a) Let X be an object of \mathbf{C} , and let $x \in \omega(X)$; we have to prove that there exists a unique morphism $f: P \rightarrow X$ such that $\omega(f)$ sends p to x . The uniqueness follows from the fact p generates P . To prove the existence, let Q be the smallest subobject of $P \times X$ such that $\omega(Q)$ contains (p, x) . The morphism $Q \rightarrow P$ defined by the projection map is surjective because P is generated by p . Therefore,

$$\dim_k \omega(Q) \geq \dim_k \omega(P),$$

but because $\dim_k(\omega(P))$ is maximal, equality must hold, and so $Q \rightarrow P$ is an isomorphism. The composite of its inverse with the second projection $Q \rightarrow X$ is a morphism $P \rightarrow X$ sending p to x .

(b) The object P is projective because ω is exact, and it is a generator because ω is faithful. \square

Let $A = \text{End}(P)$ — it is a k -algebra of finite dimension as a k -vector space (not necessarily commutative) — and let h^P be the functor $X \rightsquigarrow \text{Hom}(P, X)$.

LEMMA 11.4 *The functor h^P is an equivalence from \mathbf{C} to the category of right A -modules of finite dimension over k . Its composite with the forgetful functor is canonically isomorphic to ω .*

PROOF. Because P is a generator, the h^P is fully faithful, and because P is projective, it is exact. It remains to prove that it is essentially surjective.

Let M be a finite-dimensional right A -module, and choose a finite presentation for M ,

$$A^m \xrightarrow{\alpha} A^n \rightarrow M \rightarrow 0$$

where α is an $m \times n$ matrix with coefficients in A . This matrix defines a morphism $P^m \rightarrow P^n$ whose cokernel X has the property that $h^P(X) \simeq M$.

For the second statement,

$$\omega(X) \simeq \text{Hom}(P, X) \simeq \text{Hom}(h^P(P), h^P(X)) = \text{Hom}(A, h^P(X)) \simeq h^P(X). \quad \square$$

As A is a finite k -algebra, its linear dual $C = A^\vee$ is a k -coalgebra, and to give a right A -module structure on a k -vector space is the same as giving a left C -comodule structure (see 8.7). Together with (11.4), this completes the proof in the case that $\mathbf{C} = \langle X \rangle$. Note that

$$A \stackrel{\text{def}}{=} \text{End}(P) \simeq \text{End}(h^P) \simeq \text{End}(\omega),$$

and so

$$C \simeq \text{End}(\omega)^\vee.$$

⁴²An object P of a category is a **generator** of the category if the functor $\text{Hom}(P, -)$ is faithful, and an object P of an abelian category is **projective** if $\text{Hom}(P, -)$ is exact.

PROOF IN THE GENERAL CASE

We now consider the general case. For an object X of \mathbf{C} , let A_X be the algebra of endomorphisms of $\omega|\langle X \rangle$, and let $C_X = A_X^\vee$. For each Y in $\langle X \rangle$, A_X acts on $\omega(Y)$ on the left, and so $\omega(Y)$ is a right C -comodule; moreover, $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories

$$\langle X \rangle \rightarrow \text{Comod}(C_X).$$

Define a partial ordering on the set of isomorphism classes of objects in \mathbf{C} by the rule:

$$[X] \leq [Y] \text{ if } \langle X \rangle \subset \langle Y \rangle.$$

Note that $[X], [Y] \leq [X \oplus Y]$, so that we get a directed set, and that if $[X] \leq [Y]$, then restriction defines a homomorphism $A_Y \rightarrow A_X$. When we pass to the limit over the isomorphism classes, we obtain the following more precise form of the theorem.

THEOREM 11.5 *Let \mathbf{C} be a k -linear abelian category and let $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ be a k -linear exact faithful functor. Let $C = \varinjlim \text{End}(\omega|\langle X \rangle)^\vee$. For each object Y in \mathbf{C} , the vector space $\omega(Y)$ has a natural structure of right C -comodule, and the functor $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories $\mathbf{C} \rightarrow \text{Comod}(C)$.*

EXAMPLE 11.6 Let A be a finite k -algebra (not necessarily commutative). Because A is finite, its dual A^\vee is a coalgebra (§5c), and we saw in (8.7) that left A -module structures on k -vector space correspond to right A^\vee -comodule structures. If we take \mathbf{C} to be $\text{Mod}(A)$, ω to the forgetful functor, and X to be ${}_A A$ in the above discussion, then

$$\text{End}(\omega|\langle X \rangle)^\vee \simeq A^\vee,$$

and the equivalence of categories $\mathbf{C} \rightarrow \text{Comod}(A^\vee)$ in (11.5) simply sends an A -module V to V with its canonical A^\vee -comodule structure.

ASIDE 11.7 Let \mathbf{C} be a k -linear abelian category with a tensor product structure (see 11.13). A **coalgebra in \mathbf{C}** is an object C of \mathbf{C} together with morphisms $\Delta: C \rightarrow C \otimes C$ and $\epsilon: C \rightarrow k$ such that the diagrams (29) commute. Similarly, it is possible to define the notion of **C -comodule in \mathbf{C}** . Assume that there exists an exact faithful k -linear functor preserving tensor products. Then there exists a coalgebra C in \mathbf{C} together with a coaction of C on each object of \mathbf{C} such that, for every exact faithful k -linear functor ω to Vec_k preserving tensor products, $\omega(C) \simeq \varinjlim \text{End}(\omega|\langle X \rangle)^\vee$ (as coalgebras) and ω preserves the comodule structures. Moreover, the tensor product makes C into a bialgebra in \mathbf{C} , and if \mathbf{C} has duals, then \mathbf{C} is a Hopf algebra.

ASIDE 11.8 For the proof of Theorem 11.5, we have followed Serre 1993, 2.5. For a slightly different proof, see Deligne and Milne 1982, §2, or Saavedra Rivano 1972. It is also possible to use Grothendieck's theorem that a right exact functor is pro-representable. Let P pro-represent ω , and let A be the endomorphism ring of P .

11b Categories of comodules over a bialgebra

Let C be a coalgebra over k . We saw in (§8e), that a bialgebra structure on C defines a tensor product structure on $\text{Comod}(C)$, and that an inversion on C defines duals. In this section we prove the converse: a tensor product structure on $\text{Comod}(C)$ defines a bialgebra structure on C , and the existence of duals implies the existence of an inversion.

11.9 Let A be a finite k -algebra (not necessarily commutative), and let R be a commutative k -algebra. Consider the functors

$$\text{Mod}(A) \xrightarrow[\text{forget}]{\omega} \text{Vec}(k) \xrightarrow[V \mapsto R \otimes_k V]{\phi_R} \text{Mod}(R).$$

For $M \in \text{ob}(\text{Mod}(A))$, let $M_0 = \omega(M)$. An element λ of $\text{End}(\phi_R \circ \omega)$ is a family of R -linear maps

$$\lambda_M: R \otimes_k M_0 \rightarrow R \otimes_k M_0,$$

functorial in M . An element of $R \otimes_k A$ defines such a family, and so we have a map

$$\alpha: R \otimes_k A \rightarrow \text{End}(\phi_R \circ \omega),$$

which we shall show to be an isomorphism by defining an inverse β . Let $\beta(\lambda) = \lambda_A(1 \otimes 1)$. Clearly $\beta \circ \alpha = \text{id}$, and so we only have to show $\alpha \circ \beta = \text{id}$. The A -module $A \otimes_k M_0$ is a direct sum of copies of A , and the additivity of λ implies that $\lambda_{A \otimes_k M_0} = \lambda_A \otimes \text{id}_{M_0}$. The map $a \otimes m \mapsto am: A \otimes_k M_0 \rightarrow M$ is A -linear, and hence

$$\begin{array}{ccc} R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M \\ \downarrow \lambda_A \otimes \text{id}_{M_0} & & \downarrow \lambda_M \\ R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M \end{array}$$

commutes. Therefore

$$\lambda_M(1 \otimes m) = \lambda_A(1) \otimes m = (\alpha \circ \beta(\lambda))_M(1 \otimes m) \text{ for } 1 \otimes m \in R \otimes M,$$

i.e., $\alpha \circ \beta = \text{id}$.

11.10 Let C be a k -coalgebra, and let ω_C be the forgetful functor on $\text{Comod}(C)$. Then

$$C \simeq \varinjlim \text{End}(\omega_C|_{\langle X \rangle})^\vee. \quad (94)$$

For a finite k -algebra A , (11.9) says that $A \simeq \text{End}(\omega)$. Therefore, for any finite k -coalgebra C , we have $C \simeq \text{End}(\omega_C)^\vee$. On passing to the limit, we get (94).

Let $\alpha: C \rightarrow C'$ be a homomorphism of k -coalgebras. A coaction $V \rightarrow V \otimes C$ defines a coaction $V \rightarrow V \otimes C'$ by composition with $\text{id}_V \otimes \alpha$. Thus, α defines a functor $F: \text{Comod}(C) \rightarrow \text{Comod}(C')$ such that

$$\omega_{C'} \circ F = \omega_C. \quad (95)$$

LEMMA 11.11 *Every functor $F: \text{Comod}(C) \rightarrow \text{Comod}(C')$ satisfying (95) arises, as above, from a unique homomorphism of k -coalgebras $C \rightarrow C'$.*

PROOF. The functor F defines a homomorphism

$$\varinjlim \text{End}(\omega_{C'}|_{\langle FX \rangle}) \rightarrow \varinjlim \text{End}(\omega_C|_{\langle X \rangle}),$$

and $\varinjlim \text{End}(\omega_{C'}|_{\langle FX \rangle})$ is a quotient of $\varinjlim \text{End}(\omega_{C'}|_{\langle X \rangle})$. On passing to the duals, we get a homomorphism

$$\varinjlim \text{End}(\omega_C|_{\langle X \rangle})^\vee \rightarrow \varinjlim \text{End}(\omega_{C'}|_{\langle X \rangle})^\vee$$

and hence a homomorphism $C \rightarrow C'$. This has the required property. \square

Again, let C be a coalgebra over k . Recall (5.4) that $C \otimes C$ is again a coalgebra over k . A coalgebra homomorphism $m: C \otimes C \rightarrow C$ defines a functor

$$\phi^m: \text{Comod}(C) \times \text{Comod}(C) \rightarrow \text{Comod}(C)$$

sending (V, W) to $V \otimes W$ with the coaction

$$V \otimes W \xrightarrow{\rho_V \otimes \rho_W} V \otimes C \otimes W \otimes C \simeq V \otimes W \otimes C \otimes C \xrightarrow{V \otimes W \otimes m} V \otimes W \otimes C$$

(cf. 8.5b, §8e).

PROPOSITION 11.12 *The map $m \mapsto \phi^m$ defines a one-to-one correspondence between the set of k -coalgebra homomorphisms $m: C \otimes C \rightarrow C$ and the set of k -bilinear functors*

$$\phi: \text{Comod}(C) \times \text{Comod}(C) \rightarrow \text{Comod}(C)$$

such that $\phi(V, W) = V \otimes W$ as k -vector spaces.

- (a) *The homomorphism m is associative (i.e., the left hand diagram in (28) commutes) if and only if the canonical isomorphisms of vector spaces*

$$u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w: U \otimes (V \otimes W) \rightarrow (U \otimes V) \otimes W$$

are isomorphisms of C -comodules for all C -comodules U, V, W .

- (b) *The homomorphism m is commutative (i.e., $m(a, b) = m(b, a)$ for all $a, b \in C$) if and only if the canonical isomorphisms of vector spaces*

$$v \otimes w \mapsto w \otimes v: V \otimes W \rightarrow W \otimes V$$

are isomorphisms of C -comodules for all C -comodules W, V .

- (c) *There is an identity map $e: k \rightarrow C$ (i.e., a k -linear map such that the right hand diagram in (28) commutes) if and only if there exists a C -comodule U with underlying vector space k such that the canonical isomorphisms of vector spaces*

$$U \otimes V \simeq V \simeq V \otimes U$$

are isomorphisms of C -comodules for all C -comodules V .

PROOF. The pair $(\text{Comod}(C) \times \text{Comod}(C), \omega \otimes \omega)$, with $(\omega \otimes \omega)(X, Y) = \omega(X) \otimes \omega(Y)$ (as a k -vector space), satisfies the conditions of (11.5), and $\lim_{\rightarrow} \text{End}(\omega \otimes \omega | \langle (X, Y) \rangle)^\vee = C \otimes C$. Thus the first statement of the proposition follows from (11.11). The remaining statements are easy. \square

Let $\omega: A \rightarrow B$ be a faithful functor. We say that a morphism $\omega X \rightarrow \omega Y$ *lives in* A if it lies in $\text{Hom}(X, Y) \subset \text{Hom}(\omega X, \omega Y)$.

For k -vector spaces U, V, W , there are canonical isomorphisms

$$\begin{aligned} \phi_{U, V, W}: U \otimes (V \otimes W) &\rightarrow (U \otimes V) \otimes W, & u \otimes (v \otimes w) &\mapsto (u \otimes v) \otimes w \\ \phi_{U, V}: U \otimes V &\rightarrow V \otimes U, & u \otimes v &\mapsto v \otimes u. \end{aligned}$$

THEOREM 11.13 *Let C be a k -linear abelian category, and let $\otimes: C \times C \rightarrow C$ be k -bilinear functor. Let $\omega: C \rightarrow \text{Vec}_k$ be a k -linear exact faithful functor such that*

- (a) $\omega(X \otimes Y) = \omega(X) \otimes \omega(Y)$ for all X, Y ;
 (b) the isomorphisms $\phi_{\omega X, \omega Y, \omega Z}$ and $\phi_{\omega X, \omega Y}$ live in \mathbf{C} for all X, Y, Z ;
 (c) there exists an (identity) object $\mathbf{1}$ in \mathbf{C} such that $\omega(\mathbf{1}) = k$ and the canonical isomorphisms

$$\omega(\mathbf{1}) \otimes \omega(X) \simeq \omega(X) \simeq \omega(X) \otimes \omega(\mathbf{1})$$

live in \mathbf{C} .

Let $B = \lim \overrightarrow{\text{End}(\omega|_{\langle X \rangle})}^\vee$, so that ω defines an equivalence of categories $\mathbf{C} \rightarrow \text{Comod}(B)$ (Theorem 11.5). Then B has a unique structure (m, e) of a commutative k -bialgebra such that $\otimes = \phi^m$ and $\omega(\mathbf{1}) = (k \xrightarrow{e} B \simeq k \otimes B)$.

PROOF. To give a bi-algebra structure on a coalgebra (A, Δ, ϵ) , one has to give coalgebra homomorphisms (m, e) that make A into an algebra (5.7), and a bialgebra is a commutative bi-algebra (§5k). Thus, the statement is an immediate consequence of Proposition 11.12. \square

11c Categories of representations of affine groups

THEOREM 11.14 Let \mathbf{C} be a k -linear abelian category, let $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ be a k -bilinear functor. Let ω be an exact faithful k -linear functor $\mathbf{C} \rightarrow \text{Vec}_k$ satisfying the conditions (a), (b), and (c) of (11.13). For each k -algebra R , let $G(R)$ be the set of families

$$(\lambda_V)_{V \in \text{ob}(\mathbf{C})}, \quad \lambda_V \in \text{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

- ◇ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ for all $V, W \in \text{ob}(\mathbf{C})$,
- ◇ $\lambda_{\mathbf{1}} = \text{id}_{\omega(\mathbf{1})}$ for every identity object of $\mathbf{1}$ of \mathbf{C} , and
- ◇ $\lambda_W \circ \omega(\alpha)_R = \omega(\alpha)_R \circ \lambda_V$ for all arrows α in \mathbf{C} .

Then G is an affine monoid over k , and ω defines an equivalence of tensor categories over k ,

$$\mathbf{C} \rightarrow \text{Rep}(G).$$

When ω satisfies the following condition, G is an affine group:

- (d) for any object X such that $\omega(X)$ has dimension 1, there exists an object X^{-1} in \mathbf{C} such that $X \otimes X^{-1} \approx \mathbf{1}$.

PROOF. Theorem 11.13 allows us to assume that $\mathbf{C} = \text{Comod}(B)$ for B a k -bialgebra, and that \otimes and ω are the natural tensor product structure and forgetful functor. Let G be the monoid corresponding to B . Using (11.9) we find that, for any k -algebra R ,

$$\underline{\text{End}}(\omega)(R) \stackrel{\text{def}}{=} \text{End}(\phi_R \circ \omega) = \lim_{\leftarrow} \text{Hom}_{k\text{-lin}}(B_X, R) = \text{Hom}_{k\text{-lin}}(B, R).$$

An element $\lambda \in \text{Hom}_{k\text{-lin}}(B_X, R)$ corresponds to an element of $\underline{\text{End}}(\omega)(R)$ commuting with the tensor structure if and only if λ is a k -algebra homomorphism; thus

$$\underline{\text{End}}^\otimes(\omega)(R) = \text{Hom}_{k\text{-alg}}(B, R) = G(R).$$

We have shown that $\underline{\text{End}}^\otimes(\omega)$ is representable by an affine monoid $G = \text{Spec } B$ and that ω defines an equivalence of tensor categories

$$\mathbf{C} \rightarrow \text{Comod}(B) \rightarrow \text{Rep}_k(G).$$

On applying (d) to the highest exterior power of an object of \mathbf{C} , we find that $\underline{\text{End}}^\otimes(\omega) = \underline{\text{Aut}}^\otimes(\omega)$, which completes the proof. \square

REMARK 11.15 Let (G, ω) be $(\text{Rep}_k(G), \text{forget})$. On following through the proof of (11.14) in this case one recovers Theorem 10.2: $\underline{\text{Aut}}^\otimes(\omega^G)$ is represented by G .

NOTES Add discussion of how much of this section extends to base rings k . (Cf. mo3131.)

12 Finite flat affine groups

In this section, we allow k to be a commutative ring, but we emphasise the case of a field. As usual, unadorned tensor products are over k . In the remainder of this chapter, we shall need to use only the results on étale affine groups over a field.

12a Definitions

Let k be a commutative ring. Recall (CA 10.4) that the following conditions on a k -module M are equivalent: M is finitely generated and projective; M is “locally free” over k (ibid. (b) or (c)); M is finitely presented and flat.

DEFINITION 12.1 A **finite flat** affine group over k is an affine group G such that $\mathcal{O}(G)$ satisfies these equivalent conditions.^{43,44} For such an affine group, the function

$$\mathfrak{p} \mapsto \dim_{k(\mathfrak{p})} M \otimes k(\mathfrak{p}): \text{Spec}(k) \rightarrow \mathbb{N}$$

is locally constant; here $k(\mathfrak{p})$ is the field of fractions of k/\mathfrak{p} . It is called the **order** of G over k .

When k is a field, the flatness is automatic, and we usually simply speak of a finite affine group over k . Thus a finite affine group over k is an affine group such that $\dim_k \mathcal{O}(G)$ is finite (and $\dim_k \mathcal{O}(G)$ is then the order of G over k). We say that an affine group is an affine **p -group** if it is finite and its order is a power of p .

12b Étale affine groups

ÉTALE k -ALGEBRAS (k A FIELD)

Let k be a field, and let A be a finite k -algebra. For any finite set S of maximal ideals in A , the Chinese remainder theorem (CA 2.12) says that the map $A \rightarrow \prod_{\mathfrak{m} \in S} A/\mathfrak{m}$ is surjective with kernel $\bigcap_{\mathfrak{m} \in S} \mathfrak{m}$. In particular, $|S| \leq [A:k]$, and so A has only finitely many maximal ideals. If S is the set of all maximal ideals in A , then $\bigcap_{\mathfrak{m} \in S} \mathfrak{m}$ is the nilradical \mathfrak{N} of A (CA 11.8), and so A/\mathfrak{N} is a finite product of fields.

PROPOSITION 12.2 *The following conditions on a finite k -algebra A are equivalent:*

- (a) A is a product of separable field extensions of k ;
- (b) $A \otimes k^{\text{al}}$ is a product of copies of k^{al} ;

⁴³A finite flat group scheme over a ring is affine, and so

$$\text{finite flat affine group} = \text{finite flat group scheme.}$$

⁴⁴One can define a finite affine group G over k to be an affine group such that $\mathcal{O}(G)$ is of finite presentation, but these groups are of little interest.

(c) $A \otimes k^{\text{al}}$ is reduced.

PROOF. (a) \Rightarrow (b). We may suppose that A itself is a separable field extension of k . From the primitive element theorem (FT 5.1), we know that $A = k[\alpha]$ for some α . Because $k[\alpha]$ is separable over k , the minimum polynomial $f(X)$ of α is separable, which means that

$$f(X) = \prod (X - \alpha_i), \quad \alpha_i \neq \alpha_j \text{ for } i \neq j,$$

in $k^{\text{al}}[X]$. Now

$$A \otimes_k k^{\text{al}} \simeq (k[X]/(f)) \otimes k^{\text{al}} \simeq k^{\text{al}}[X]/(f),$$

and, according to the Chinese remainder theorem (CA 2.12),

$$k^{\text{al}}[X]/(f) \simeq \prod_i k^{\text{al}}[X]/(X - \alpha_i) \simeq k^{\text{al}} \times \cdots \times k^{\text{al}}.$$

(b) \Rightarrow (c). Obvious.

(c) \Rightarrow (a). The map $a \mapsto a \otimes 1: A \rightarrow A \otimes_k k^{\text{al}}$ is injective, and so A is reduced. Therefore the above discussion shows that it is a finite product of fields. Let k' one of the factors of A . If k' is not separable over k , then k has characteristic $p \neq 0$ and there exists an element α of k' whose minimum polynomial is of the form $f(X^p)$ with $f \in k[X]$ (see FT 3.6, et seq.). Now

$$k[\alpha] \otimes k^{\text{al}} \simeq (k[X]/(f(X^p))) \otimes k^{\text{al}} \simeq k^{\text{al}}[X]/(f(X^p)),$$

which is not reduced because $f(X^p)$ is a p th power in $k^{\text{al}}[X]$. Hence $A \otimes k^{\text{al}}$ is not reduced. \square

DEFINITION 12.3 A k -algebra is *étale* if it is finite and it satisfies the equivalent conditions of the proposition.⁴⁵

PROPOSITION 12.4 *Finite products, tensor products, and quotients of étale k -algebras are étale.*

PROOF. This is obvious from the condition (b). \square

COROLLARY 12.5 *The composite of any finite set of étale subalgebras of a k -algebra is étale.*

PROOF. Let A_i be étale subalgebras of B . Then $A_1 \cdots A_n$ is the image of the map

$$a_1 \otimes \cdots \otimes a_n \mapsto a_1 \cdots a_n: A_1 \otimes \cdots \otimes A_n \rightarrow B,$$

and so is a quotient of $A_1 \otimes \cdots \otimes A_n$. \square

PROPOSITION 12.6 *If A is étale over k , then $A \otimes_k k'$ is étale over k' for any field extension k' of k .*

⁴⁵This agrees with Bourbaki's terminology (Bourbaki A, V §6): Let A be an algebra over a field k . We say that A is *diagonalizable* if there exists an integer $n \geq 0$ such that A is isomorphic to the product algebra k^n . We say that A is *étale* if there exists an extension L of k such that the algebra $L \otimes_k A$ deduced from A by extension of scalars is diagonalizable.

PROOF. Let k'^{al} be an algebraic closure of k' , and let k^{al} be the algebraic closure of k in k'^{al} . Then

$$\begin{array}{ccc} k' & \longrightarrow & k'^{\text{al}} \\ \uparrow & & \uparrow \\ k & \longrightarrow & k^{\text{al}} \end{array}$$

is commutative, and so

$$\begin{aligned} (A \otimes_k k') \otimes_{k'} k'^{\text{al}} &\simeq (A \otimes_k k^{\text{al}}) \otimes_{k^{\text{al}}} k'^{\text{al}} \\ &\simeq (k^{\text{al}} \times \cdots \times k^{\text{al}}) \otimes_{k^{\text{al}}} k'^{\text{al}} \\ &\simeq k'^{\text{al}} \times \cdots \times k'^{\text{al}}. \end{aligned} \quad \square$$

CLASSIFICATION OF ÉTALE k -ALGEBRAS (k A FIELD)

Let k^{sep} be the composite of the subfields k' of k^{al} separable over k . If k is perfect, for example, of characteristic zero, then $k^{\text{sep}} = k^{\text{al}}$. Let Γ be the group of k -automorphisms of k^{sep} . For any subfield K of k^{sep} , finite and Galois over k , an easy Zorn's lemma argument⁴⁶ shows that

$$\sigma \mapsto \sigma|_K: \Gamma \rightarrow \text{Gal}(K/k)$$

is surjective. Let X be a finite set with an action of Γ ,

$$\Gamma \times X \rightarrow X.$$

We say that the action is⁴⁷ continuous if it factors through $\Gamma \rightarrow \text{Gal}(K/k)$ for some subfield K of k^{sep} finite and Galois over k .

For an étale k -algebra A , let

$$F(A) = \text{Hom}_{k\text{-alg}}(A, k^{\text{al}}) = \text{Hom}_{k\text{-alg}}(A, k^{\text{sep}}).$$

Then Γ acts on $F(A)$ through its action on k^{sep} :

$$(\sigma f)(a) = \sigma(f(a)), \quad \sigma \in \Gamma, f \in F(A), a \in A.$$

The images of all homomorphisms $A \rightarrow k^{\text{sep}}$ will lie in some finite Galois extension of k , and so the action of Γ on $F(A)$ is continuous.

THEOREM 12.7 *The map $A \rightsquigarrow F(A)$ defines a contravariant equivalence from the category étale k -algebras to the category of finite sets with a continuous action of Γ .*

PROOF. This is a restatement of the fundamental theorem of Galois theory (FT §3), and is left as an exercise to the reader (the indolent may see Waterhouse 1979, 6.3). \square

⁴⁶Let $\sigma_0 \in \text{Gal}(K/k)$. Apply Zorn's lemma to the set of all pairs (E, α) where E is a subfield of k^{sep} containing k and α is homomorphism $E \rightarrow k^{\text{sep}}$ whose restriction to K is σ_0 .

⁴⁷Equivalently, the action is continuous relative to the discrete topology on X and the Krull topology on Γ (FT §7).

12.8 We explain the theorem in more detail. Let $\bar{k} = k^{\text{sep}}$, and let $\Gamma = \text{Gal}(\bar{k}/k)$. Then Γ acts on $F(A) \stackrel{\text{def}}{=} \text{Hom}_{k\text{-alg}}(A, \bar{k})$ through its action on \bar{k} :

$$\gamma\sigma = \gamma \circ \sigma \text{ for } \gamma \in \Gamma, \sigma \in F(A).$$

For any étale k -algebra A , there is a canonical isomorphism

$$a \otimes c \mapsto (\sigma a \cdot c)_{\sigma \in F(A)}: A \otimes \bar{k} \rightarrow \bar{k}^{F(A)}, \quad (96)$$

where

$$\bar{k}^{F(A)} \stackrel{\text{def}}{=} \text{Hom}(F(A), \bar{k}) = \prod_{\sigma \in F(A)} k_{\sigma}, \quad k_{\sigma} = \bar{k}.$$

In other words, $\bar{k}^{F(A)}$ is a product of copies of \bar{k} indexed by the elements of $F(A)$. When we let Γ act on $A \otimes \bar{k}$ through its action of \bar{k} and on $\bar{k}^{F(A)}$ through its actions on both \bar{k} and $F(A)$,

$$(\gamma f)(\sigma) = \gamma(f(\gamma^{-1}\sigma)), \quad \gamma \in \Gamma, \quad f: F(A) \rightarrow \bar{k}, \quad \sigma \in F(A),$$

then the (96) becomes equivariant. Now:

(a) for any étale k -algebra A ,

$$A = (A \otimes \bar{k})^{\Gamma};$$

(b) for any finite set S with a continuous action of Γ , $(\bar{k}^S)^{\Gamma}$ is an étale k -subalgebra of \bar{k}^S , and

$$F((\bar{k}^S)^{\Gamma}) \simeq S.$$

Therefore, $A \rightsquigarrow F(A)$ is an equivalence of categories with quasi-inverse $S \mapsto (\bar{k}^S)^{\Gamma}$.

12.9 Suppose that A is generated by a single element, say, $A = k[\alpha] \simeq k[X]/(f(X))$. Then A is étale if and only if $f(X)$ has distinct roots in k^{al} . Assume this, and choose $f(X)$ to be monic. A k -algebra homomorphism $A \rightarrow k^{\text{sep}}$ is determined by the image of α , which can be any root of f in k^{sep} . Therefore, $F(A)$ can be identified with the set of roots of f in k^{sep} . Suppose $F(A)$ decomposes into r orbits under the action of Γ , and let f_1, \dots, f_r be the monic polynomials whose roots are the orbits. Then each f_i is stable under Γ , and so has coefficients in k (FT 7.8). It follows that $f = f_1 \cdots f_r$ is the decomposition of f into its irreducible factors over k , and that

$$A \simeq \prod_{1 \leq i \leq r} k[X]/(f_i(X))$$

is the decomposition of A into a product of fields.

ÉTALE AFFINE GROUPS OVER A FIELD

Let k be a field. An affine group G over k is *étale* if $\mathcal{O}(G)$ is an étale k -algebra; in particular, an étale affine group is finite (hence algebraic).⁴⁸

⁴⁸Algebraic geometers will recognize that an affine group G is étale if and only if the morphism of schemes $|G| \rightarrow \text{Spec} k$ is étale.

REMARK 12.10 Recall (6.26) that an algebraic group G over k is smooth if and only if $\mathcal{O}(G) \otimes k^{\text{al}}$ is reduced. Therefore, a finite affine group G over k is étale if and only if it is smooth. If k has characteristic zero, then every finite affine group is étale (6.31). If k is perfect of characteristic $p \neq 0$, then $\mathcal{O}(G)^{p^r}$ is a reduced Hopf algebra for some r (6.35); as the kernel of the map $x \mapsto x^{p^r} : \mathcal{O}(G) \rightarrow \mathcal{O}(G)^{p^r}$ has dimension a power of p , we see that a finite affine group of order n is étale if p does not divide n .

Let \mathcal{A} be the category of étale k -algebras. The functor $G \rightsquigarrow \mathcal{O}(G)$ is an equivalence from the category of étale affine groups over k to the category of group objects in the category \mathcal{A}^{opp} (see §5f). As $G(k^{\text{sep}}) = \text{Hom}_{k\text{-alg}}(\mathcal{O}(G), k^{\text{sep}})$, when we combine this statement with Theorem 12.7, we obtain the following theorem.

THEOREM 12.11 *The functor $G \rightsquigarrow G(k^{\text{sep}})$ is an equivalence from the category of étale algebraic groups over k to the category of finite groups endowed with a continuous action of Γ .*

Let K be a subfield of k^{sep} containing k , and let Γ' be the subgroup of Γ consisting of the σ fixing the elements of K . Then K is the subfield of k^{sep} of elements fixed by Γ' (see FT 7.10), and it follows that $G(K)$ is the subgroup $G(k^{\text{sep}})$ of elements fixed by Γ' .

EXAMPLES

For an étale algebraic group G , the order of G is the order of the (abstract) group $G(k^{\text{al}})$.

Since $\text{Aut}(X) = 1$ when X is a group of order 1 or 2, there is exactly one étale algebraic group of order 1 and one of order 2 over k (up to isomorphism).

Let X be a group of order 3. Such a group is cyclic and $\text{Aut}(X) = \mathbb{Z}/2\mathbb{Z}$. Therefore the étale algebraic groups of order 3 over k correspond to homomorphisms $\Gamma \rightarrow \mathbb{Z}/2\mathbb{Z}$ factoring through $\text{Gal}(K/k)$ for some finite Galois extension K of k . A separable quadratic extension K of k defines such a homomorphism, namely,

$$\sigma \mapsto \sigma|_K : \Gamma \rightarrow \text{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$$

and all nontrivial such homomorphisms arise in this way (see FT §7). Thus, up to isomorphism, there is exactly one étale algebraic group G^K of order 3 over k for each separable quadratic extension K of k , plus the constant group G_0 . For G_0 , $G_0(k)$ has order 3. For G^K , $G^K(k)$ has order 1 but $G^K(K)$ has order 3. There are infinitely many distinct quadratic extensions of \mathbb{Q} , for example, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, ..., $\mathbb{Q}[\sqrt{p}]$, Since $\mu_3(\mathbb{Q}) = 1$ but $\mu_3(\mathbb{Q}[\sqrt[3]{1}]) = 3$, μ_3 must be the group corresponding to $\mathbb{Q}[\sqrt[3]{1}]$.

FINITE ÉTALE AFFINE GROUPS OVER RING

DEFINITION 12.12 A k -algebra A is *étale* if it is flat of finite presentation over k and $A \otimes k(\mathfrak{p})$ is étale over the field $k(\mathfrak{p})$ for all prime ideals \mathfrak{p} in k .

Assume that $\text{Spec } k$ is connected, and let x be a homomorphism from k into an algebraically closed field Ω . For a finite étale k -algebra A , let $F(A)$ denote the set $\text{Hom}_{k\text{-alg}}(A, \Omega)$. Then $A \rightsquigarrow F(A)$ is a functor, and we let Γ be its automorphism group. Then Γ is a profinite group, which is called the *fundamental group* $\pi_1(\text{Spec } k, x)$ of $\text{Spec } k$. It acts on each

set $F(A)$, and the functor F is a contravariant equivalence from the category of finite étale k -algebras to the category of finite sets with a continuous action of Γ .

An affine group G over k is *étale* if $\mathcal{O}(G)$ is an étale k -algebra. As in the case that k is a field, the functor

$$G \rightsquigarrow G(\Omega)$$

is an equivalence from the category of étale affine groups over k to the category of finite groups endowed with a continuous action of Γ .

12c Finite flat affine groups in general

Recall that the augmentation ideal I_G of an affine group G is the kernel of $\epsilon: \mathcal{O}(G) \rightarrow k$.

PROPOSITION 12.13 *Let G be a finite affine group over a field k of characteristic $p \neq 0$, and suppose that $x^p = 0$ for all $x \in I_G$. For any basis x_1, \dots, x_r of I_G/I_G^2 , the monomials*

$$x_1^{m_1} \cdots x_r^{m_r}, \quad 0 \leq m_i < p$$

form a basis for $\mathcal{O}(G)$ as a k -vector space (and so $[\mathcal{O}(G):k] = p^r$).

PROOF. Omitted for the moment (see Waterhouse 1979, 11.4). □

The proposition says that $\mathcal{O}(G) \simeq k[X_1, \dots, X_r]/(X_1^p, \dots, X_r^p)$. This generalizes.

THEOREM 12.14 *Let G be a finite group scheme over a perfect field k of characteristic $p \neq 0$ such that $|G|$ is connected. For any basis x_1, \dots, x_r of I_G/I_G^2 , there exist integers $e_1, \dots, e_r \geq 1$ such that*

$$\mathcal{O}(G) \simeq k[X_1, \dots, X_r]/(X_1^{p^{e_1}}, \dots, X_r^{p^{e_r}}).$$

PROOF. Omitted for the moment (see Waterhouse 1979, 14.4). □

Let k be nonperfect, and let $a \in k \setminus k^p$. The subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equations $x^{p^2} = 0$, $y^p = ax^p$ is finite and connected, but $\mathcal{O}(G)$ is not a truncated polynomial algebra, i.e., (12.14) fails for G (Waterhouse 1979, p. 113).

CLASSIFICATION OF FINITE COMMUTATIVE AFFINE GROUPS OVER A PERFECT FIELD (DIEUDONNÉ MODULES)

Let k be a perfect field of characteristic p . A finite group scheme over k of order prime to p is étale, which can be understood in terms of the Galois group of k , and so it remains to classify the p -groups.

Let W be the ring of Witt vectors with entries in k . Thus W is a complete discrete valuation ring with maximal ideal generated by $p = p1_W$ and residue field k . For example, if $k = \mathbb{F}_p$, then $W = \mathbb{Z}_p$. The Frobenius automorphism σ of W is the unique automorphism such that $\sigma a \equiv a^p \pmod{p}$.

THEOREM 12.15 *There exists a contravariant equivalence $G \rightsquigarrow M(G)$ from the category of commutative finite affine p -groups to the category of triples (M, F, V) in which M is a W -module of finite length and F and V are endomorphisms of M satisfying the following conditions ($c \in W, m \in M$):*

$$\begin{aligned} F(c \cdot m) &= \sigma c \cdot Fm \\ V(\sigma c \cdot m) &= c \cdot Vm \\ FV &= p \cdot \text{id}_M = VF. \end{aligned}$$

The order of G is $p^{\text{length}(M(G))}$. For any perfect field k' containing k , there is functorial isomorphism

$$M(G_{k'}) \simeq W(k') \otimes_{W(k)} M(G).$$

PROOF. The proof is quite long, and will not be included. See Demazure 1972, Chap. III, or Pink 2005. \square

For example:

$$\begin{aligned} M(\mathbb{Z}/p\mathbb{Z}) &= W/pW, & F &= 1, & V &= 0; \\ M(\mu_p) &= W/pW, & F &= 0, & V &= p; \\ M(\alpha_p) &= W/pW, & F &= 0, & V &= 0. \end{aligned}$$

The module $M(G)$ is called the **Dieudonné module** of G .

The theorem is very important since it reduces the study of commutative affine p -groups over perfect fields to semi-linear algebra. There are important generalizations of the theorem to discrete valuation, and other, rings.

12d Cartier duality

In this subsection, we allow k to be a ring.

Let G be a finite flat commutative affine group with bialgebra $(\mathcal{O}(G), m, e, \Delta, \epsilon)$. Recall (§5i) that the Cartier dual G^\vee of G is the affine group with bialgebra $(\mathcal{O}(G)^\vee, \Delta^\vee, \epsilon^\vee, m^\vee, e^\vee)$. The functor $G \rightsquigarrow G^\vee$ is a contravariant equivalence of the category of finite flat commutative affine groups with itself, and $(G^\vee)^\vee \simeq G$. Our goal in this subsection is to describe the affine group G^\vee as a functor.

For k -algebra R , let $\underline{\text{Hom}}(G, \mathbb{G}_m)(R)$ be the set of homomorphisms of $\alpha: G_R \rightarrow \mathbb{G}_{mR}$ of affine groups over R . This becomes a group under the multiplication

$$(\alpha_1 \cdot \alpha_2)(g) = \alpha_1(g) \cdot \alpha_2(g), \quad g \in G(R'), \quad R' \text{ an } R\text{-algebra.}$$

In this way,

$$R \rightsquigarrow \underline{\text{Hom}}(G, \mathbb{G}_m)(R)$$

becomes a functor $\text{Alg}_k \rightarrow \text{Grp}$.

THEOREM 12.16 *There is a canonical isomorphism*

$$G^\vee \simeq \underline{\text{Hom}}(G, \mathbb{G}_m)$$

of functors $\text{Alg}_k \rightarrow \text{Grp}$.

PROOF. Let R be a k -algebra. We have

$$G(R) = \text{Hom}_{R\text{-alg}}(\mathcal{O}(G), R) \hookrightarrow \text{Hom}_{R\text{-lin}}(\mathcal{O}(G), R) = \mathcal{O}(G^\vee)_R. \quad (97)$$

The multiplication in $\mathcal{O}(G)$ corresponds to comultiplication in $\mathcal{O}(G^\vee)$, from which it follows that the image of (97) consists of the group-like elements in $\mathcal{O}(G^\vee)_R$. On the other hand, we know that $\text{Hom}(G_R^\vee, \mathbb{G}_m)$ also consists of the group-like elements in $\mathcal{O}(G^\vee)_R$. Thus,

$$G(R) \simeq \underline{\text{Hom}}(G^\vee, \mathbb{G}_m)(R).$$

This isomorphism is natural in R , and so we have shown that $G \simeq \underline{\text{Hom}}(G^\vee, \mathbb{G}_m)$. To obtain the required isomorphism, replace G with G^\vee and use that $(G^\vee)^\vee \simeq G$. \square

NOTES For more on Cartier duality, see Pink 2005, §24, and the notes on Cartier duality on Ching-Li Chai's website

EXAMPLE 12.17 Let $G = \alpha_p$, so that $\mathcal{O}(G) = k[X]/(X^p) = k[x]$. Let $1, y, y_2, \dots, y_{p-1}$ be the basis of $\mathcal{O}(G^\vee) = \mathcal{O}(G)^\vee$ dual to $1, x, \dots, x^{p-1}$. Then $y^i = i!y_i$; in particular, $y^p = 0$. In fact, $G^\vee \simeq \alpha_p$, and the pairing is

$$a, b \mapsto \exp(ab): \alpha_p(R) \times \alpha_p(R) \rightarrow R^\times$$

where

$$\exp(ab) = 1 + \frac{ab}{1!} + \frac{(ab)^2}{2!} + \cdots + \frac{(ab)^{p-1}}{(p-1)!}.$$

ASIDE 12.18 The theory of finite flat affine groups, or finite flat group schemes to use the more common term, is extensive. See Tate 1997 for a short introduction.

PROPOSITION 12.19 *An algebraic group G over a field is finite if and only if there exists a representation (V, r) such that every representation of G is a subquotient⁴⁹ of V^n for some $n \geq 0$.*

PROOF. If G is finite, then the regular representation X of G is finite-dimensional, and (8.36) says that it has the required property. Conversely if, with the notations of (§11a), $\text{Rep}_k(G) = \langle X \rangle$, then $G = \text{Spec } B$ where B is the linear dual of the finite k -algebra A_X . \square

12e Exercises

EXERCISE 12-1 Show that A is étale if and only if there are no nonzero k -derivations $D: A \rightarrow k$. [Regard A as a left A -module by left multiplication. Let A be a k -algebra and M an A -module. A k -**derivation** is a k -linear map $D: A \rightarrow M$ such that

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad (\text{Leibniz rule}).]$$

EXERCISE 12-2 How many finite algebraic groups of orders 1, 2, 3, 4 are there over \mathbb{R} (up to isomorphism)?

⁴⁹Here V^n is a direct sum of n copies of V , and subquotient means any representation isomorphic to a subrepresentation of a quotient (equivalently, to a quotient of a subrepresentation).

EXERCISE 12-3 (Waterhouse 1979, Exercise 9, p. 52). Let G be a finite group scheme. Show that the following are equivalent:

- (a) $\mathcal{O}(G_{\text{red}})$ is étale;
- (b) G_{red} is a subgroup of G ;
- (c) G is isomorphic to the semi-direct product of G° and $\pi_0 G$.

13 The connected components of an algebraic group

Recall that a topological space X is connected if it is not the union of two disjoint nonempty open subsets. This amounts to saying that, apart from X itself and the empty set, there is no subset of X that is both open and closed. For each point x of X , the union of the connected subsets of X containing x is again connected, and so it is the largest connected subset containing x — it is called the connected component of x . The set of the connected components of the points of X is a partition of X by closed subsets. Write $\pi_0(X)$ for the set of connected components of X .

In a topological group G , the connected component of the neutral element is a closed normal connected subgroup G° of G , called the neutral (or identity) component of G . Therefore, the quotient $\pi_0(G) = G/G^\circ$ is a separated topological group. For example, $\text{GL}_2(\mathbb{R})$ has two connected components, namely, the identity component consisting of the matrices with determinant > 0 and another connected component consisting of the matrices with determinant < 0 .

In this section, we discuss the identity component G° of an affine group and the (étale) quotient group $\pi_0(G)$ of its connected components. Throughout, k is a field.

13a Some commutative algebra

Throughout this subsection, A is a commutative ring. An element e of A is *idempotent* if $e^2 = e$. For example, 0 and 1 are both idempotents — they are called the *trivial idempotents*. Idempotents e_1, \dots, e_n are *orthogonal* if $e_i e_j = 0$ for $i \neq j$. Any sum of orthogonal idempotents is again idempotent. A finite set $\{e_1, \dots, e_n\}$ of orthogonal idempotents is *complete* if $e_1 + \dots + e_n = 1$. Any finite set of orthogonal idempotents $\{e_1, \dots, e_n\}$ can be completed by adding the idempotent $e = 1 - (e_1 + \dots + e_n)$.

If $A = A_1 \times \dots \times A_n$ (direct product of rings), then the elements

$$e_1 = (1, 0, \dots), e_2 = (0, 1, 0, \dots), \dots, e_n = (0, \dots, 0, 1)$$

form a complete set of orthogonal idempotents. Conversely, if $\{e_1, \dots, e_n\}$ is a complete set of orthogonal idempotents in A , then Ae_i becomes a ring with the addition and multiplication induced by that of A (but with the identity element e_i), and $A \simeq Ae_1 \times \dots \times Ae_n$.

LEMMA 13.1 *The space $\text{spec } A$ is disconnected if and only if A contains a nontrivial idempotent.*

PROOF. Let e be a nontrivial idempotent, and let $f = 1 - e$. For a prime ideal \mathfrak{p} , the map $A \rightarrow A/\mathfrak{p}$ must send exactly one of e or f to a nonzero element. This shows that $\text{spec } A$ is a disjoint union of the sets⁵⁰ $D(e)$ and $D(f)$, each of which is open. If $D(e) = \text{spec } A$,

⁵⁰The set $D(e)$ consists of the prime ideals of A not containing e , and $V(\mathfrak{a})$ consists of all prime ideals containing \mathfrak{a} .

then e would be a unit (CA 2.2), and hence can be cancelled from $ee = e$ to give $e = 1$. Therefore $D(e) \neq \text{spec } A$, and similarly, $D(f) \neq \text{spec } A$.

Conversely, suppose that $\text{spec } A$ is disconnected, say, the disjoint union of two nonempty closed subsets $V(\mathfrak{a})$ and $V(\mathfrak{b})$. Because the union is disjoint, no prime ideal contains both \mathfrak{a} and \mathfrak{b} , and so $\mathfrak{a} + \mathfrak{b} = A$. Thus $a + b = 1$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. As $ab \in \mathfrak{a} \cap \mathfrak{b}$, all prime ideals contain ab , which is therefore nilpotent (CA 2.5), say $(ab)^m = 0$. Any prime ideal containing a^m contains a ; similarly, any prime ideal containing b^m contains b ; thus no prime ideal contains both a^m and b^m , which shows that $(a^m, b^m) = A$. Therefore, $1 = ra^m + sb^m$ for some $r, s \in A$. Now

$$\begin{aligned}(ra^m)(sb^m) &= rs(ab)^m = 0, \\ (ra^m)^2 &= (ra^m)(1 - sb^m) = ra^m, \\ (sb^m)^2 &= sb^m \\ ra^m + sb^m &= 1,\end{aligned}$$

and so $\{ra^m, sb^m\}$ is a complete set of orthogonal idempotents. Clearly $V(\mathfrak{a}) \subset V(ra^m)$ and $V(\mathfrak{b}) \subset V(sb^m)$. As $V(ra^m) \cap V(sb^m) = \emptyset$, we see that $V(\mathfrak{a}) = V(ra^m)$ and $V(\mathfrak{b}) = V(sb^m)$, and so each of ra^m and sb^m is a nontrivial idempotent. \square

PROPOSITION 13.2 *Let $\{e_1, \dots, e_n\}$ be a complete set of orthogonal idempotents in A . Then*

$$\text{spec } A = D(e_1) \sqcup \dots \sqcup D(e_n)$$

is a decomposition of $\text{spec } A$ into a disjoint union of open subsets. Moreover, every such decomposition arises in this way.

PROOF. Let \mathfrak{p} be a prime ideal in A . Because A/\mathfrak{p} is an integral domain, exactly one of the e_i 's maps to 1 in A/\mathfrak{p} and the remainder map to zero. This proves that $\text{spec } A$ is the disjoint union of the sets $D(e_i)$.

Now consider a decomposition

$$\text{spm } A = U_1 \sqcup \dots \sqcup U_n$$

each U_i open. We use induction on n to show that it arises from a complete set of orthogonal idempotents. When $n = 1$, there is nothing to prove, and when $n \geq 2$, we write

$$\text{spm } A = U_1 \sqcup (U_2 \sqcup \dots \sqcup U_n).$$

The proof of the lemma shows that there exist orthogonal idempotents $e_1, e'_1 \in A$ such that $e_1 + e'_1 = 1$ and

$$\begin{aligned}U_1 &= D(e_1) \\ U_2 \sqcup \dots \sqcup U_n &= D(e'_1) = \text{spec } Ae'_1.\end{aligned}$$

By induction, there exist orthogonal idempotents e_2, \dots, e_n in Ae'_1 such that $e_2 + \dots + e_n = e'_1$ and $U_i = D(e_i)$ for $i = 2, \dots, n$. Now $\{e_1, \dots, e_n\}$ is a complete set of orthogonal idempotents in A such that $U_i = D(e_i)$ for all i . \square

13.3 Recall that a ring A is said to be Jacobson if every prime ideal is an intersection of maximal ideals, and that every finitely generated algebra over a field is Jacobson (see CA 12.3 et seq.). In a Jacobson ring, the nilradical is an intersection of maximal ideals. When A is Jacobson, “prime ideal” can be replaced by “maximal ideal” and “spec” with “spm” in the above discussion. In particular, for a Jacobson ring A , there are natural one-to-one correspondences between

- ◇ the decompositions of $\text{spm}(A)$ into a finite disjoint union of open subspaces,
- ◇ the decompositions of A into a finite direct products of rings, and
- ◇ the complete sets of orthogonal idempotents in A .

Now consider a ring $A = k[X_1, \dots, X_n]/\mathfrak{a}$. When k is algebraically closed

$$\text{spm } A \simeq \text{the zero set of } \mathfrak{a} \text{ in } k^n$$

as topological spaces (Nullstellensatz, CA 11.6), and so $\text{spm } A$ is connected if and only if the zero set of \mathfrak{a} in k^n is connected.

LEMMA 13.4 *Let A be a finitely generated algebra over a separably closed field k . The number of connected components of $\text{spm } A$ is equal to the largest degree of an étale k -subalgebra of A (and both are finite).*

PROOF. Because $\text{spm } A$ is noetherian, it is a finite disjoint union of its connected components, each of which is open (CA 12.12). Let E be an étale k -subalgebra of A . Because k is separably closed, E is a product of copies of k . A decomposition of E corresponds to a complete set $(e_i)_{1 \leq i \leq m}$ of orthogonal idempotents in E , and $m = [E:k]$. Conversely, a complete set $(e_i)_{1 \leq i \leq m}$ of orthogonal idempotents in A defines an étale k -subalgebra of A of degree m , namely, $\sum k e_i$. Thus the statement follows from the above remark. \square

LEMMA 13.5 *Let A be a finitely generated k -algebra. Assume that k is algebraically closed, and let K be an algebraically closed field containing k . If $\text{spm } A$ is connected, so also is $\text{spm } A_K$.*

PROOF. Write $A = k[X_1, \dots, X_n]/\mathfrak{a}$, so that $A_K = K[X_1, \dots, X_n]/\mathfrak{b}$ where \mathfrak{b} is the ideal generated by \mathfrak{a} . By assumption, the zero set $V(\mathfrak{a})$ of \mathfrak{a} in k^n is connected. As the closure of a connected set is connected, it suffices to show that the zero set $V(\mathfrak{b})$ of \mathfrak{b} in K^n is the Zariski closure of $V(\mathfrak{a})$. Let $f \in K[X_1, \dots, X_n]$ be zero on $V(\mathfrak{a})$. Choose a basis $(a_i)_{i \in I}$ for K over k , and write

$$f = \sum_i a_i f_i \quad (f_i \in k[X_1, \dots, X_n], \text{ finite sum}).$$

As f is zero on $V(\mathfrak{a})$, so also is each f_i . By the Strong Nullstellensatz (CA 11.7), this implies that each f_i lies in the radical of \mathfrak{a} , which implies that f is zero on $V(\mathfrak{b})$. \square

LEMMA 13.6 *Let A and B be finitely generated algebras over an algebraically closed field k . If $\text{spm } A$ and $\text{spm } B$ are connected, then so also is $\text{spm } A \otimes B$.*

PROOF. Because of the Nullstellensatz, we can identify $\text{spm } A \otimes B$ with $\text{spm } A \times \text{spm } B$ (as a set). Let $\mathfrak{m}_1 \in \text{spm } A$. The k -algebra homomorphisms

$$B \simeq (A/\mathfrak{m}_1) \otimes B \leftarrow A \otimes B$$

give continuous maps

$$\mathfrak{n} \mapsto (\mathfrak{m}_1, \mathfrak{n}): \text{spm}(B) \simeq \text{spm}(A/\mathfrak{m}_1 \otimes B) \xrightarrow{\text{closed}} \text{spm}(A \otimes B).$$

Similarly, for $\mathfrak{n}_2 \in \text{spm } B$, we have

$$\mathfrak{m} \mapsto (\mathfrak{m}, \mathfrak{n}_2): \text{spm}(A) \simeq \text{spm}(A \otimes B/\mathfrak{n}_2) \xrightarrow{\text{closed}} \text{spm}(A \otimes B).$$

As $\text{spm } A$ and $\text{spm } B$ are connected, this shows that $(\mathfrak{m}_1, \mathfrak{n}_1)$ and $(\mathfrak{m}_2, \mathfrak{n}_2)$ lie in the same connected component of $\text{spm } A \times \text{spm } B$ for every $\mathfrak{n}_1 \in \text{spm } B$ and $\mathfrak{m}_2 \in \text{spm } A$. \square

ASIDE 13.7 On \mathbb{C}^n there are two topologies: the Zariski topology, whose closed sets are the zero sets of collections of polynomials, and the complex topology. Clearly Zariski-closed sets are closed for the complex topology, and so the complex topology is the finer than the Zariski topology. It follows that a subset of \mathbb{C}^n that is connected in the complex topology is connected in the Zariski topology. The converse is false. For example, if we remove the real axis from \mathbb{C} , the resulting space is not connected for the complex topology but it is connected for the topology induced by the Zariski topology (a nonempty Zariski-open subset of \mathbb{C} can omit only finitely many points). Thus the next result is a surprise:

If $V \subset \mathbb{C}^n$ is closed and irreducible for the Zariski topology, then it is connected for the complex topology.

For the proof, see Shafarevich 1994, VII 2.

13b Étale subalgebras

Let A be a finitely generated k -algebra. An étale k -subalgebra of A will give an étale k^{al} -subalgebra of the same degree of $A_{k^{\text{al}}}$, and so its degree is bounded by the number of connected components of $\text{spm } A_{k^{\text{al}}}$ (13.4). The composite of two étale subalgebras of A is étale (12.5), and so there is a largest étale k -subalgebra $\pi_0(A)$ of A , containing all other étale subalgebras.

Let K be a field containing k . Then $\pi_0(A) \otimes_k K$ is an étale subalgebra of $A \otimes_k K$ (see 12.6). We shall need to know that it is the largest étale subalgebra.

PROPOSITION 13.8 *Let A be a finitely generated k -algebra, and let K be a field containing k . Then*

$$\pi_0(A) \otimes_k K = \pi_0(A \otimes_k K).$$

PROOF. If $\pi_0(A) \otimes K$ is not the largest étale subalgebra of $A \otimes K$, then $\pi_0(A) \otimes L$ will not be the largest étale subalgebra in $A \otimes L$ for any field L containing K . Therefore, it suffices to prove the proposition for a field L containing K .

We first prove the statement with $K = k^{\text{sep}}$. It follows from (12.8) that the étale k -algebras in A are in canonical one-to-one correspondence with the étale k^{sep} -algebras in $A \otimes k^{\text{sep}}$ stable under the action of $\Gamma = \text{Gal}(k^{\text{sep}}/k)$ (acting on the second factor). Because

it is the (unique) largest étale k^{sep} -algebra in $A \otimes k^{\text{sep}}$, $\pi_0(A \otimes k^{\text{sep}})$ is stable under the action of Γ . Under the correspondence

$$\begin{aligned}\pi_0(A \otimes k^{\text{sep}}) &\leftrightarrow \pi_0(A \otimes k^{\text{sep}})^{\Gamma} \\ \pi_0(A) \otimes k^{\text{sep}} &\leftrightarrow \pi_0(A).\end{aligned}$$

As $\pi_0(A) \otimes k^{\text{sep}} \subset \pi_0(A \otimes k^{\text{sep}})$, we have $\pi_0(A) \subset \pi_0(A \otimes k^{\text{sep}})^{\Gamma}$. But $\pi_0(A)$ is the largest étale k -algebra in A , and so $\pi_0(A) = \pi_0(A \otimes k^{\text{sep}})^{\Gamma}$. Therefore $\pi_0(A) \otimes k^{\text{sep}} = \pi_0(A \otimes k^{\text{sep}})$.

We next prove the statement when $k = k^{\text{sep}}$ and $K = k^{\text{al}}$. If $K \neq k$, then k has characteristic $p \neq 0$ and K is purely inseparable over it. Let e_1, \dots, e_m be a basis of idempotents for $\pi_0(A \otimes K)$. Write $e_j = \sum a_i \otimes c_i$ with $a_i \in A$ and $c_i \in K$. For some r , all the elements $c_i^{p^r}$ lie in k , and then $e_j^{p^r} = \sum a_i^{p^r} \otimes c_i^{p^r} \in A$. But $e_j = e_j^{p^r}$, and so $\pi_0(A \otimes K)$ has a basis in A .

Finally, we prove the statement when k and K are both algebraically closed. We may suppose that A is not a product of k -algebras, and so has no nontrivial idempotents. We have to show that then $A \otimes K$ also has no nontrivial idempotents, but this follows from 13.5. \square

COROLLARY 13.9 *Let A be a finitely generated k -algebra. The degree $[\pi_0(A):k]$ of $\pi_0(A)$ is equal to the number of connected components of $\text{spm}(A \otimes k^{\text{al}})$.*

PROOF. We have

$$[\pi_0(A):k] = [\pi_0(A) \otimes k^{\text{al}}:k^{\text{al}}] = [\pi_0(A \otimes k^{\text{al}}):k^{\text{al}}],$$

and so this follows from 13.4. \square

Let A and A' be finitely generated k -algebras. Then $\pi_0(A) \otimes \pi_0(A')$ is an étale subalgebra of $A \otimes A'$ (see 12.4). We shall need to know that it is the largest étale subalgebra.

PROPOSITION 13.10 *Let A and A' be finitely generated k -algebras. Then*

$$\pi_0(A \otimes A') = \pi_0(A) \otimes \pi_0(A').$$

PROOF. As $\pi_0(A) \otimes \pi_0(A') \subset \pi_0(A \otimes A')$, we may suppose that k is algebraically closed (13.8), and we may replace each of A and A' with a direct factor and so suppose that $\pi_0(A) = 1 = \pi_0(A')$. We then have to show that $\pi_0(A \otimes A') = 1$, but this follows from 13.6. \square

ASIDE 13.11 Let V be an algebraic variety over a field k , and let $\pi_0(V_{k^{\text{sep}}})$ be the set of connected components of V over k^{sep} . Then $\pi_0(V_{k^{\text{sep}}})$ is a finite set with an action of $\text{Gal}(k^{\text{sep}}/k)$, and so defines an étale k -algebra B . Let $\pi_0(V) = \text{spm } B$. Then $\pi_0(V)$ is an algebraic variety, (finite and) étale over k , and there is a canonical morphism $V \rightarrow \pi_0(V)$ of algebraic varieties whose fibres are connected.⁵¹ For a projective variety, this is the Stein factorization of the morphism $V \rightarrow \text{Spm } k$ (cf. Hartshorne 1977, III, 11.5). For an affine variety $V = \text{spm } A$, $\pi_0(V) = \text{spm}(\pi_0(A))$.

⁵¹More precisely, let \mathfrak{m} be a point of $\text{spm}(\pi_0(V))$, and let $k(\mathfrak{m})$ be the residue field at \mathfrak{m} (finite extension of k). Then the fibre over \mathfrak{m} is a geometrically connected algebraic variety over $k(\mathfrak{m})$.

13c Algebraic groups

Let G be an algebraic group with coordinate ring $A = \mathcal{O}(G)$. The map $\Delta: A \rightarrow A \otimes A$ is a k -algebra homomorphism, and so sends $\pi_0(A)$ into $\pi_0(A \otimes A) \stackrel{13.10}{=} \pi_0(A) \otimes \pi_0(A)$. Similarly, $S: A \rightarrow A$ sends $\pi_0(A)$ into $\pi_0(A)$, and we can define ϵ on $\pi_0(A)$ to be the restriction of ϵ on A . Therefore $\pi_0(A)$ is a Hopf subalgebra of A .

DEFINITION 13.12 Let G be an algebraic group over a field k .

- (a) The **group of connected components** $\pi_0(G)$ of G is the quotient algebraic group corresponding to the Hopf subalgebra $\pi_0(\mathcal{O}(G))$ of $\mathcal{O}(G)$.
- (b) The **identity component** G° of G is the kernel of the homomorphism $G \rightarrow \pi_0(G)$.

PROPOSITION 13.13 *The following four conditions on an algebraic group G are equivalent:*

- (a) *the étale affine group $\pi_0(G)$ is trivial;*
- (b) *the topological space $\text{spm}(\mathcal{O}(G))$ is connected;*
- (c) *the topological space $\text{spm}(\mathcal{O}(G))$ is irreducible;*
- (d) *the ring $\mathcal{O}(G)/\mathfrak{N}$ is an integral domain.*

PROOF. (b) \Rightarrow (a). Remark 13.3 implies that $\pi_0(\mathcal{O}(G))$ has no nontrivial idempotents, and so is a field. The existence of the k -algebra homomorphism $\epsilon: \mathcal{O}(G) \rightarrow k$ implies that $\pi_0(\mathcal{O}(G)) = k$.

(c) \Rightarrow (b). Trivial.

(d) \Leftrightarrow (c). In general, $\text{spm } A$ is irreducible if and only if the nilradical of A is prime (see §6.4).

(a) \Rightarrow (d). If $\pi_0(G)$ is trivial, so also is $\pi_0(G_{k^{\text{al}}})$ (Lemma 13.8). Write $\text{spm } \mathcal{O}(G_{k^{\text{al}}})$ as a union of its irreducible components. No irreducible component is contained in the union of the remainder. Therefore, there exists a point that lies on exactly one irreducible component. By homogeneity (6.12), all points have this property, and so the irreducible components are disjoint. As $\text{spm } \mathcal{O}(G_{k^{\text{al}}})$ is connected, there must be only one, and so $G_{k^{\text{al}}}$ is irreducible. Let \mathfrak{N}' be the nilradical of $\mathcal{O}(G_{k^{\text{al}}}) = k^{\text{al}} \otimes_k \mathcal{O}(G)$ — we have shown that $\mathcal{O}(G_{k^{\text{al}}})/\mathfrak{N}'$ is an integral domain. As the canonical map $\mathcal{O}(G)/\mathfrak{N} \rightarrow \mathcal{O}(G_{k^{\text{al}}})/\mathfrak{N}'$ is injective, we obtain (d). \square

PROPOSITION 13.14 *The fibres of the map $|G| \rightarrow |\pi_0(G)|$ are the connected components of the topological space $|G|$.*

PROOF. The connected components of $|G|$ and the points of $|\pi_0(G)|$ are both indexed by the elements of a maximal complete set of orthogonal idempotents. \square

PROPOSITION 13.15 *Every homomorphism from G to an étale algebraic group factors uniquely through $G \rightarrow \pi_0(G)$.*

PROOF. Let $G \rightarrow H$ be a homomorphism from G to an étale algebraic group H . The image of $\mathcal{O}(H)$ in $\mathcal{O}(G)$ is étale (see 12.4), and so is contained in $\pi_0(\mathcal{O}(G)) \stackrel{\text{def}}{=} \mathcal{O}(\pi_0 G)$. \square

PROPOSITION 13.16 *The subgroup G° of G is connected, and every homomorphism from a connected algebraic group to G factors through $G^\circ \rightarrow G$.*

PROOF. The homomorphism of k -algebras $\epsilon: \mathcal{O}(\pi_0 G) \rightarrow k$ decomposes $\mathcal{O}(\pi_0 G)$ into a direct product

$$\mathcal{O}(\pi_0 G) = k \times B.$$

Let $e = (1, 0)$. Then the augmentation ideal of $\mathcal{O}(\pi_0 G)$ is $(1 - e)$, and

$$\mathcal{O}(G) = e\mathcal{O}(G) \times (1 - e)\mathcal{O}(G)$$

with $e\mathcal{O}(G) \simeq \mathcal{O}(G)/(1 - e)\mathcal{O}(G) = \mathcal{O}(G^\circ)$ (see 7.15). Clearly, $k = \pi_0(e\mathcal{O}(G)) \simeq \pi_0(\mathcal{O}(G^\circ))$. Therefore $\pi_0 G^\circ = 1$, which implies that G° is connected.

If H is connected, then the composite $H \rightarrow G \rightarrow \pi_0(G)$ has trivial image. \square

PROPOSITION 13.17 *The subgroup G° is the unique connected normal affine subgroup of G such that G/G° is étale.*

PROOF. The subgroup G° is normal with étale quotient by definition, and we have shown it to be connected. Suppose that H is a second normal algebraic subgroup of G . If G/H is étale, then (by (a)) the homomorphism $G \rightarrow G/H$ factors through $\pi_0(G)$, and so we get a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & G^\circ & \longrightarrow & G & \longrightarrow & \pi_0 G & \longrightarrow & 1 \\ & & \downarrow & & \parallel & & \downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 1 \end{array}$$

with exact rows. The similar diagram with each $*$ replaced with $*(R)$ gives, for each k -algebra R , an exact sequence

$$1 \rightarrow G^\circ(R) \rightarrow H(R) \rightarrow (\pi_0 G)(R). \quad (98)$$

Since this functorial in R , it gives a sequence of algebraic groups

$$1 \rightarrow G^\circ \rightarrow H \rightarrow \pi_0 G.$$

The exactness of (98) shows that G° is the kernel of $H \rightarrow \pi_0 G$. This map factors through $\pi_0 H$, and so if $\pi_0 H = 1$, its kernel is H : therefore $G^\circ \simeq H$. \square

Proposition 13.17 says that, for any algebraic group G , there is a unique exact sequence

$$1 \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow 1$$

such that G° is connected and $\pi_0(G)$ is étale. This is sometimes called the **connected-étale exact sequence**.

The next proposition says that the functors $G \rightsquigarrow \pi_0 G$ and $G \rightsquigarrow G^\circ$ commute with extension of the base field.

PROPOSITION 13.18 For any field extension $k' \supset k$,

$$\begin{aligned}\pi_0(G_{k'}) &\simeq \pi_0(G)_{k'} \\ (G_{k'})^\circ &\simeq (G^\circ)_{k'}.\end{aligned}$$

In particular, G is connected if and only if $G_{k'}$ is connected.

PROOF. As $\mathcal{O}(G_{k'}) \simeq \mathcal{O}(G) \otimes_k k'$, this follows from (13.8). \square

PROPOSITION 13.19 For any algebraic groups G and G' ,

$$\begin{aligned}\pi_0(G \times G') &\simeq \pi_0(G) \times \pi_0(G') \\ (G \times G')^\circ &\simeq G^\circ \times G'^\circ.\end{aligned}$$

In particular, $G \times G'$ is connected if and only if both G and G' are connected.

PROOF. The coordinate ring $\mathcal{O}(G \times G') \simeq \mathcal{O}(G) \otimes \mathcal{O}(G')$, and so this follows from (13.10). \square

REMARK 13.20 Let G be an algebraic group over k . For any field k' containing k , Proposition 13.18 shows that G is connected if and only if $G_{k'}$ is connected. In particular, if an algebraic group G over a field is connected, then so also is $G_{k^{\text{al}}}$. In other words, a connected algebraic group is geometrically connected. This is false for algebraic varieties: for example,

$$X^2 + Y^2 = 0$$

is connected over \mathbb{R} (even irreducible), but becomes a disjoint union of the two lines

$$X + \pm iY = 0$$

over \mathbb{C} — the ring $\mathbb{R}[X, Y]/(X^2 + Y^2)$ is an integral domain, but

$$\mathbb{C}[X, Y]/(X^2 + Y^2) \simeq \mathbb{C}[X, Y]/(X + iY) \times \mathbb{C}[X, Y]/(X - iY).$$

The reason for the difference is the existence of the homomorphism $\epsilon: \mathcal{O}(G) \rightarrow k$ (the neutral element of $G(k)$). An integral affine algebraic variety V over a field k is geometrically connected if and only if k is algebraically closed in $\mathcal{O}(V)$, which is certainly the case if there exists a k -algebra homomorphism $\mathcal{O}(V) \rightarrow k$ (AG 11.5).

PROPOSITION 13.21 Let

$$1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$$

be an exact sequence of algebraic groups. If N and Q are connected, so also is G ; conversely, if G is connected, so also is Q .

PROOF. Assume N and Q are connected. Then N is contained in the kernel of $G \rightarrow \pi_0(G)$, so this map factors through $G \rightarrow Q$ (see 7.56), and therefore has image $\{1\}$. Conversely, since G maps onto $\pi_0(Q)$, it must be trivial if G is connected. \square

EXAMPLES

13.22 Let G be finite. When k has characteristic zero, G is étale, and so $G = \pi_0(G)$ and $G^\circ = 1$. Otherwise, there is an exact sequence

$$1 \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow 1.$$

When k is perfect, the homomorphism $G \rightarrow \pi_0(G)$ has a section, and so G is a semidirect product

$$G = G^\circ \rtimes \pi_0(G).$$

To see this, note that the homomorphism $G_{\text{red}} \rightarrow \pi_0(G)$ is an isomorphism because both groups are smooth, and it is an isomorphism on k^{al} -points:

$$G_{\text{red}}(k^{\text{al}}) = G(k^{\text{al}}) \xrightarrow{\cong} \pi_0(G)(k^{\text{al}}).$$

13.23 The groups \mathbb{G}_a , GL_n , \mathbb{T}_n (upper triangular), \mathbb{U}_n (strictly upper triangular), \mathbb{D}_n are connected because in each case $\mathcal{O}(G)$ is an integral domain. For example,

$$k[\mathbb{T}_n] = k[\text{GL}_n]/(X_{ij} \mid i > j),$$

which is isomorphic to the polynomial ring in the symbols X_{ij} , $1 \leq i \leq j \leq n$, with the product $X_{11} \cdots X_{nn}$ inverted.

13.24 For the group G of monomial matrices (3.12), $\pi_0(\mathcal{O}(G))$ is a product of copies of k indexed by the elements of S_n . Thus, $\pi_0 G = S_n$ (regarded as a constant algebraic group (5.23)), and $G^\circ = \mathbb{D}_n$.

13.25 The group SL_n is connected. As we noted in the proof of (7.32), the natural isomorphism

$$A, r \mapsto A \cdot \text{diag}(r, 1, \dots, 1): \text{SL}_n(R) \times \mathbb{G}_m(R) \rightarrow \text{GL}_n(R)$$

(of set-valued functors) defines an isomorphism of k -algebras

$$\mathcal{O}(\text{GL}_n) \simeq \mathcal{O}(\text{SL}_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

and the algebra on the right contains $\mathcal{O}(\text{SL}_n)$. In particular, $\mathcal{O}(\text{SL}_n)$ is a subring of $\mathcal{O}(\text{GL}_n)$, and so is an integral domain.

13.26 Assume $\text{char}(k) \neq 2$. For any nondegenerate quadratic space (V, q) , the algebraic group $\text{SO}(q)$ is connected. It suffices to prove this after replacing k with k^{al} , and so we may suppose that q is the standard quadratic form $X_1^2 + \cdots + X_n^2$, in which case we write $\text{SO}(q) = \text{SO}_n$. The latter is shown to be connected in Exercise 13-4 below.

The determinant defines a quotient map $\mathcal{O}(q) \rightarrow \{\pm 1\}$ with kernel $\text{SO}(q)$. Therefore $\mathcal{O}(q)^\circ = \text{SO}(q)$ and $\pi_0(\mathcal{O}(q)) = \{\pm 1\}$ (constant algebraic group).

13.27 The symplectic group Sp_{2n} is connected (for some hints on how to prove this, see Springer 1998, 2.2.9).

ASIDE 13.28 According to (13.7) and (13.13), an algebraic group G over \mathbb{C} is connected if and only if $G(\mathbb{C})$ is connected for the complex topology. Thus, we could for example deduce that GL_n is a connected algebraic group from knowing that $\mathrm{GL}_n(\mathbb{C})$ is connected for the complex topology. However, it is easier to deduce that $\mathrm{GL}_n(\mathbb{C})$ is connected from knowing that GL_n is connected (of course, this requires the serious theorem stated in (13.7)).

13.29 An algebraic group G over \mathbb{R} may be connected without $G(\mathbb{R})$ being connected, and conversely. For example, GL_2 is connected as an algebraic group, but $\mathrm{GL}_2(\mathbb{R})$ is not connected for the real topology, and μ_3 is not connected as an algebraic group, but $\mu_3(\mathbb{R}) = \{1\}$ is certainly connected for the real topology.

13d Affine groups

Let G be an affine group, and write $G = \varprojlim_{i \in I} G_i$ where $(G_i)_{i \in I}$ is the family of algebraic quotients of G (see 8.23). Define

$$G^\circ = \varprojlim_{i \in I} G_i^\circ,$$

$$\pi_0 G = \varprojlim_{i \in I} \pi_0 G_i.$$

PROPOSITION 13.30 *Assume k has characteristic zero. An algebraic group G is connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\mathrm{Rep}(G)$ of subquotients of V^n , $n \geq 0$, is not stable under \otimes .*

PROOF. In characteristic zero, all finite groups are étale. Therefore, a group G is connected if and only if there is no non-trivial epimorphism $G \rightarrow G'$ with G' finite. According to (8.63), this is equivalent to $\mathrm{Rep}_k(G)$ having no non-trivial subcategory of the type described in (12.19). \square

NOTES Discuss connectedness over a base ring (or scheme). Not of much interest. More important is to look at the connectedness of the fibres. The strong connectedness condition is that the geometric fibres are connected, i.e., that for an algebraic group G over a commutative ring R , the algebraic group G_K is connected for every homomorphism $R \rightarrow K$ from R into an algebraically closed field K .

13e Exercises

EXERCISE 13-1 Show that if $1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$ is exact, so also is $\pi_0(N) \rightarrow \pi_0(G) \rightarrow \pi_0(Q) \rightarrow 1$ (in an obvious sense). Give an example to show that $\pi_0(N) \rightarrow \pi_0(G)$ need not be injective.

EXERCISE 13-2 What is the map $\mathcal{O}(\mathrm{SL}_n) \rightarrow \mathcal{O}(\mathrm{GL}_n)$ defined in example 13.25?

EXERCISE 13-3 Prove directly that $\pi_0(\mathcal{O}(\mathrm{O}_n)) = k \times k$.

EXERCISE 13-4 (Springer 1998, 2.2.2). Assume k has characteristic $\neq 2$. For any k -algebra R , let $V(R)$ be the set of skew-symmetric matrices, i.e., the matrices A such that $A^t = -A$.

- (a) Show that the functor $R \mapsto V(R)$ is represented by a finitely generated k -algebra A , and that A is an integral domain.
- (b) Show that $A \mapsto (I_n + A)^{-1}(I_n - A)$ defines a bijection from a nonempty open subset of $\mathrm{SO}_n(k^{\mathrm{al}})$ onto an open subset of $V(k^{\mathrm{al}})$.
- (c) Deduce that SO_n is connected.

EXERCISE 13-5 Let A be a product of copies of k indexed by the elements of a finite set S . Show that the k -bialgebra structures on A are in natural one-to-one correspondence with the group structures on S .

EXERCISE 13-6 Let G be a finite affine group. Show that the following conditions are equivalent:

- (a) the k -algebra $\mathcal{O}(G_{\mathrm{red}})$ is étale;
- (b) $\mathcal{O}(G_{\mathrm{red}}) \otimes \mathcal{O}(G_{\mathrm{red}})$ is reduced;
- (c) G_{red} is a subgroup of G ;
- (d) G is isomorphic to the semi-direct product of G° and $\pi_0 G$.

EXERCISE 13-7 Let k be a nonperfect field of characteristic 2, so that there exists an $a \in k$ that is not a square. Show that the functor $R \rightsquigarrow G(R) \stackrel{\mathrm{def}}{=} \{x \in R \mid x^4 = ax^2\}$ becomes a finite commutative algebraic group under addition. Show that $G(k)$ has only one element but $\pi_0(G)$ has two. Deduce that G is not isomorphic to the semi-direct product of G° and $\pi_0(G)$. (Hence 13-6 shows that $\mathcal{O}(G)/\mathfrak{M}$ is not a Hopf algebra.)

EXERCISE 13-8 Let k be a field of characteristic p . Show that the extensions

$$0 \rightarrow \mu_p \rightarrow G \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$$

with G a finite commutative algebraic group are classified by the elements of $k^\times/k^{\times p}$ (the split extension $G = \mu_p \times \mathbb{Z}/p\mathbb{Z}$ corresponds to the trivial element in $k^\times/k^{\times p}$). Show that G_{red} is not a subgroup of G unless the extension splits.

13f Where we are

As discussed in the first section, every affine algebraic group has a composition series with the quotients listed at right:

$$\begin{array}{rcl}
 \text{affine} & G & \\
 & | & \text{finite étale} \\
 \text{connected} & G^\circ & \\
 & | & \text{semisimple} \\
 \text{solvable} & \bullet & \\
 & | & \text{torus} \\
 \text{unipotent} & \bullet & \\
 & | & \text{unipotent} \\
 & \{1\} &
 \end{array}$$

We have constructed the top segment of this picture. Next we look at tori and unipotent groups. Then we study the most interesting groups, the semisimple ones, and finally, we put everything together.

14 Groups of multiplicative type; tori

In this section we study the affine groups that become diagonalizable over an extension field. Through k is a field.

We state for reference:

$$\begin{aligned} \mathbb{G}_m(R) &= R^\times & \mathcal{O}(\mathbb{G}_m) &= k[X, X^{-1}] & \Delta(X) &= X \otimes X & \epsilon(X) &= 1 & S(X) &= X^{-1} \\ \mu_n(R) &= \{\zeta \in R \mid \zeta^n = 1\} & \mathcal{O}(\mu_n) &= \frac{k[X]}{(X^n - 1)} = k[x] & \Delta(x) &= x \otimes x & \epsilon(x) &= 1 & S(x) &= x^{n-1} \end{aligned}$$

14a Group-like elements

DEFINITION 14.1 Let $A = (A, \Delta, \epsilon)$ be a k -coalgebra. An element a of A is **group-like** if $\Delta(a) = a \otimes a$ and $\epsilon(a) = 1$.

LEMMA 14.2 *The group-like elements in A are linearly independent.*

PROOF. If not, it will be possible to express one group-like element e as a linear combination of other group-like elements $e_i \neq e$:

$$e = \sum_i c_i e_i, \quad c_i \in k. \quad (99)$$

We may even suppose that the e_i occurring in the sum are linearly independent. Now

$$\begin{aligned} \Delta(e) &= e \otimes e \stackrel{(99)}{=} \sum_{i,j} c_i c_j e_i \otimes e_j \\ \Delta(e) &\stackrel{(99)}{=} \sum_i c_i \Delta(e_i) = \sum_i c_i e_i \otimes e_i. \end{aligned}$$

The $e_i \otimes e_j$ are also linearly independent, and so this implies that

$$\begin{cases} c_i c_i = c_i & \text{all } i \\ c_i c_j = 0 & \text{if } i \neq j. \end{cases}$$

We also know that

$$\begin{aligned} \epsilon(e) &= 1 \\ \epsilon(e) &= \sum c_i \epsilon(e_i) = \sum c_i. \end{aligned}$$

On combining these statements, we see that the c_i form a complete set of orthogonal idempotents in the field k , and so one of them equals 1 and the remainder are zero, which contradicts our assumption that e is not equal to any of the e_i . \square

Let A be a k -bialgebra. If a and b are group-like elements in A , then

$$\begin{aligned} \Delta(ab) &= \Delta(a)\Delta(b) = (a \otimes a)(b \otimes b) = ab \otimes ab \\ \epsilon(ab) &= \epsilon(a)\epsilon(b) = 1 \end{aligned}$$

because Δ and ϵ are k -algebra homomorphisms. Therefore the group-like elements form a submonoid of (A, \times) .

Let A be a Hopf algebra, and let $a \in A$. If a is group-like, then

$$1 = (e \circ \epsilon)(a) \stackrel{(34)}{=} (\text{mult} \circ (S \otimes \text{id}_A) \circ \Delta)(a) = S(a)a,$$

and so a is a unit in A with $a^{-1} = S(a)$. Conversely, if a is a unit in A such that $\Delta(a) = a \otimes a$, then

$$a \stackrel{(30)}{=} ((\epsilon, \text{id}_A) \circ \Delta)(a) = \epsilon(a)a,$$

and so $\epsilon(a) = 1$. Thus the group-like elements of A are exactly the units such that $\Delta(a) = a \otimes a$.

14b The characters of an affine group

Recall that a character of an affine group G is a homomorphism $\chi: G \rightarrow \mathbb{G}_m$. To give a character χ of G is the same as giving a homomorphism of k -algebras $\mathcal{O}(\mathbb{G}_m) \rightarrow \mathcal{O}(G)$ respecting the comultiplications, and this is the same as giving a unit $a(\chi)$ of $\mathcal{O}(G)$ (the image of X) such that $\Delta(a(\chi)) = a(\chi) \otimes a(\chi)$. Therefore, $\chi \leftrightarrow a(\chi)$ is a one-to-one correspondence between the characters of G and the group-like elements of $\mathcal{O}(G)$.

For characters χ, χ' , define

$$\chi + \chi': G(R) \rightarrow R^\times$$

by

$$(\chi + \chi')(g) = \chi(g) \cdot \chi'(g).$$

Then $\chi + \chi'$ is again a character, and the set of characters is an abelian group, denoted $X(G)$. The correspondence $\chi \leftrightarrow a(\chi)$ between characters and group-like elements has the property that

$$a(\chi + \chi') = a(\chi) \cdot a(\chi').$$

ASIDE 14.3 Recall (2.16) that an element f of $\mathcal{O}(G)$ can be regarded as a natural transformation $f: G \rightarrow \mathbb{A}^1$. Suppose that

$$\begin{cases} f(1_G) = 1, & \text{for } 1_G \text{ the identity element in } G(R), \text{ and} \\ f(xy) = f(x)f(y), & \text{for } x, y \in G(R), R \text{ a } k\text{-algebra.} \end{cases} \quad (100)$$

Then $f(R)$ takes values in $R^\times \subset \mathbb{A}^1(R)$ and is a homomorphism $G(R) \rightarrow R^\times$. In other words, f is a character of G . One can see directly from the definitions that the condition (100) holds if and only if f is group-like.

14c The affine group $D(M)$

Let M be a commutative group (written multiplicatively), and let $k[M]$ be the k -vector space with basis M . Thus, the elements of $k[M]$ are finite sums

$$\sum_i a_i m_i, \quad a_i \in k, \quad m_i \in M.$$

When we endow $k[M]$ with the multiplication extending that on M ,

$$\left(\sum_i a_i m_i \right) \left(\sum_j b_j n_j \right) = \sum_{i,j} a_i b_j m_i n_j,$$

then $k[M]$ becomes a k -algebra, called the **group algebra** of M . It becomes a Hopf algebra when we set

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1} \quad (m \in M)$$

because, for m an element of the basis M ,

$$\begin{aligned}(\mathrm{id} \otimes \Delta)(\Delta(m)) &= m \otimes (m \otimes m) = (m \otimes m) \otimes m = (\Delta \otimes \mathrm{id})(\Delta(m)), \\(\epsilon \otimes \mathrm{id})(\Delta(m)) &= 1 \otimes m, \quad (\mathrm{id} \otimes \epsilon)(\Delta(m)) = m \otimes 1, \\(\mathrm{mult} \circ (S \otimes \mathrm{id}))(m \otimes m) &= 1 = (\mathrm{mult} \circ (\mathrm{id} \otimes S))(m \otimes m).\end{aligned}$$

Note that $k[M]$ is generated as a k -algebra by any set of generators for M , and so it is finitely generated if M is finitely generated.

EXAMPLE 14.4 Let M be a cyclic group, generated by e .

- (a) Case e has infinite order. Then the elements of $k[M]$ are the finite sums $\sum_{i \in \mathbb{Z}} a_i e^i$ with the obvious addition and multiplication, and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, $S(e) = e^{-1}$. Therefore, $k[M] \simeq k[\mathbb{G}_m]$.
- (b) Case e is of order n . Then the elements of $k[M]$ are sums $a_0 + a_1 e + \cdots + a_{n-1} e^{n-1}$ with the obvious addition and multiplication (using $e^n = 1$), and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, and $S(e) = e^{n-1}$. Therefore, $k[M] \simeq k[\mu_n]$.

EXAMPLE 14.5 Recall that if W and V are vector spaces with bases $(e_i)_{i \in I}$ and $(f_j)_{j \in J}$, then $W \otimes_k V$ is a vector space with basis $(e_i \otimes f_j)_{(i,j) \in I \times J}$. Therefore, if M_1 and M_2 are commutative groups, then

$$(m_1, m_2) \leftrightarrow m_1 \otimes m_2 : k[M_1 \times M_2] \leftrightarrow k[M_1] \otimes k[M_2]$$

is an isomorphism of k -vector spaces, and one checks easily that it respects the Hopf k -algebra structures.

PROPOSITION 14.6 For any commutative group M , the functor $D(M)$

$$R \rightsquigarrow \mathrm{Hom}(M, R^\times) \quad (\text{homomorphisms of abelian groups})$$

is an affine group, with coordinate ring $k[M]$. When M is finitely generated, the choice of a basis for M determines an isomorphism of $D(M)$ with a finite product of copies of \mathbb{G}_m and various μ_n 's.

PROOF. To give a k -linear map $k[M] \rightarrow R$ is the same as giving a map $M \rightarrow R$. The map $k[M] \rightarrow R$ is a k -algebra homomorphism if and only if $M \rightarrow R$ is a homomorphism from M into R^\times . This shows that $D(M)$ is represented by $k[M]$, and it is therefore an algebraic group.

A decomposition of commutative groups

$$M \approx \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

defines a decomposition of k -bialgebras

$$k[M] \approx k[\mathbb{G}_m] \otimes \cdots \otimes k[\mathbb{G}_m] \otimes k[\mu_{n_1}] \otimes \cdots \otimes k[\mu_{n_r}]$$

(14.4,14.5). Since every finitely generated commutative group M has such a decomposition, this proves the second statement. \square

LEMMA 14.7 *The group-like elements of $k[M]$ are exactly the elements of M .*

PROOF. Let $e \in k[M]$ be group-like. Then

$$e = \sum c_i e_i \text{ for some } c_i \in k, e_i \in M.$$

The argument in the proof of Lemma 14.2 shows that the c_i form a complete set of orthogonal idempotents in k , and so one of them equals 1 and the remainder are zero. Therefore $e = e_i$ for some i . \square

Thus

$$X(D(M)) \simeq M.$$

The character of $D(M)$ corresponding to $m \in M$ is

$$D(M)(R) \stackrel{\text{def}}{=} \text{Hom}(M, R^\times) \xrightarrow{f \mapsto f(m)} R^\times \stackrel{\text{def}}{=} \mathbb{G}_m(R).$$

SUMMARY 14.8 Let p be the characteristic exponent of k . Then:

$D(M)$ is algebraic	\iff	M is finitely generated
$D(M)$ is connected	\iff	M has only p -torsion
$D(M)$ is algebraic and smooth	\iff	M is finitely generated and has no p -torsion
$D(M)$ is algebraic, smooth, and connected	\iff	M is free and finitely generated.

14d Diagonalizable groups

DEFINITION 14.9 An affine group G is **diagonalizable** if the group-like elements in $\mathcal{O}(G)$ span it as a k -vector space.

THEOREM 14.10 *An affine group G is diagonalizable if and only if it is isomorphic to $D(M)$ for some commutative group M .*

PROOF. The group-like elements of $k[M]$ span it by definition. Conversely, suppose the group-like elements M span $\mathcal{O}(G)$. Lemma 14.2 shows that they form a basis for $\mathcal{O}(G)$ (as a k -vector space), and so the inclusion $M \hookrightarrow \mathcal{O}(G)$ extends to an isomorphism $k[M] \rightarrow \mathcal{O}(G)$ of vector spaces. That this isomorphism is compatible with the bialgebra structures (m, e, Δ, ϵ) can be checked on the basis elements $m \in M$, where it is obvious. \square

ASIDE 14.11 When we interpret the characters of G as elements of $\mathcal{O}(G)$ satisfying (100), we can say that G is diagonalizable if and only if $\mathcal{O}(G)$ is spanned by characters.

THEOREM 14.12 (a) *The functor $M \rightsquigarrow D(M)$ is a contravariant equivalence from the category of commutative groups to the category of diagonalizable affine groups (with quasi-inverse $G \rightsquigarrow X(G)$).*

(b) *If*

$$1 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 1$$

is an exact sequence of commutative groups, then

$$1 \rightarrow D(M'') \rightarrow D(M) \rightarrow D(M') \rightarrow 1$$

is an exact sequence of affine groups.

(c) *Subgroups and quotient groups of diagonalizable affine groups are diagonalizable.*

PROOF. (a) Certainly, we have a contravariant functor

$$D: \{\text{commutative groups}\} \rightsquigarrow \{\text{diagonalizable groups}\}.$$

We first show that D is fully faithful, i.e., that

$$\text{Hom}(M, M') \rightarrow \text{Hom}(D(M'), D(M)) \tag{101}$$

is an isomorphism for all M, M' . It sends direct limits to inverse limits and direct sums to products, and so it suffices to prove that (101) is an isomorphism when M, M' are cyclic. If, for example, M and M' are both infinite cyclic groups, then

$$\begin{aligned} \text{Hom}(M, M') &= \text{Hom}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}, \\ \text{Hom}(D(M'), D(M)) &= \text{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \{X^i \mid i \in \mathbb{Z}\} \simeq \mathbb{Z}, \end{aligned}$$

and (101) is an isomorphism. The remaining cases are similarly easy.

Theorem 14.10 shows that the functor is essentially surjective, and so it is an equivalence.

(b) The map $k[M'] \rightarrow k[M]$ is injective, and so $D(M) \rightarrow D(M')$ is a quotient map (by definition). Its kernel is represented by $k[M]/I_{k[M']}$, where $I_{k[M']}$ is the augmentation ideal of $k[M']$ (see 7.15). But $I_{k[M']}$ is the ideal generated the elements $m - 1$ for $m \in M'$, and so $k[M]/I_{k[M']}$ is the quotient ring obtained by putting $m = 1$ for all $m \in M'$. Therefore $M \rightarrow M''$ defines an isomorphism $k[M]/I_{k[M']} \rightarrow k[M'']$.

(c) If H is a subgroup of G , then $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is surjective, and so if the group-like elements of $\mathcal{O}(G)$ span it, the same is true of $\mathcal{O}(H)$.

Let $D(M) \rightarrow Q$ be a quotient map, and let H be its kernel. Then $H = D(M'')$ for some quotient M'' of M . Let M' be the kernel of $M \rightarrow M''$. Then $D(M) \rightarrow D(M')$ and $D(M) \rightarrow Q$ are quotient maps with the same kernel, and so are isomorphic (7.57). \square

ASIDE 14.13 Our definition of a diagonalizable group agrees with that in SGA3, VIII 1.1: a group scheme is diagonalizable if it is isomorphic to a scheme of the form $D(M)$ for some commutative group M .

DIAGONALIZABLE REPRESENTATIONS

DEFINITION 14.14 A representation of an affine group is **diagonalizable** if it is a sum of one-dimensional representations. (According to 8.68, it is then a direct sum of one-dimensional representations.)

Recall that \mathbb{D}_n is the group of invertible diagonal $n \times n$ matrices; thus

$$\mathbb{D}_n \simeq \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n \text{ copies}} \simeq D(\mathbb{Z}^n).$$

A finite-dimensional representation (V, r) of an affine group G is diagonalizable if and only if there exists a basis for V such that $r(G) \subset \mathbb{D}_n$. In more down-to-earth terms, the representation defined by an inclusion $G \subset \text{GL}_n$ is diagonalizable if and only if there exists an invertible matrix P in $M_n(k)$ such that, for all k -algebras R and all $g \in G(R)$,

$$PgP^{-1} \in \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}.$$

A character $\chi: G \rightarrow \mathbb{G}_m$ defines a representation of G on any finite-dimensional space V : let $g \in G(R)$ act on V_R as multiplication by $\chi(g) \in R^\times$. For example, χ defines a representation of G on k^n by

$$g \mapsto \begin{pmatrix} \chi(g) & & 0 \\ & \ddots & \\ 0 & & \chi(g) \end{pmatrix}.$$

Let (V, r) be a representation of G . We say that G **acts on V through χ** if

$$r(g)v = \chi(g)v \text{ all } g \in G(R), v \in V_R.$$

This means that the image of r is contained in the centre \mathbb{G}_m of GL_V and that r is the composite of

$$G \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V.$$

Let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be the coaction defined by r . Then G acts on V through the character χ if and only if

$$\rho(v) = v \otimes a(\chi), \quad \text{all } v \in V.$$

When V is 1-dimensional, $\mathrm{GL}_V = \mathbb{G}_m$, and so G always acts on V through some character.

Let (V, r) be a representation of G . If G acts on subspaces W and W' through the character χ , then it acts on $W + W'$ through the character χ . Therefore, for each $\chi \in X(G)$, there is a largest subspace V_χ (possibly zero) such that G acts on V_χ through χ . We have (8.64)

$$V_\chi = \{v \in V \mid \rho(v) = v \otimes a(\chi)\}.$$

THEOREM 14.15 *The following conditions on an affine group G are equivalent:*

- (a) G is diagonalizable;
- (b) every finite-dimensional representation of G is diagonalizable;
- (c) every representation of G is diagonalizable;
- (d) for every representation (V, r) of G ,

$$V = \bigoplus_{\chi \in X(T)} V_\chi.$$

PROOF. (a) \Rightarrow (c): Let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be the comodule corresponding to a representation of G (see 8.12). We have to show that V is a sum of one-dimensional representations or, equivalently, that V is spanned by vectors u such that $\rho(u) \in \langle u \rangle \otimes \mathcal{O}(G)$.

Let $v \in V$. As the group-like elements form a basis $(e_i)_{i \in I}$ for $\mathcal{O}(G)$, we can write

$$\rho(v) = \sum_{i \in I} u_i \otimes e_i, \quad u_i \in V.$$

On applying the identities (p. 97)

$$\begin{cases} (\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_A) \circ \rho \\ (\mathrm{id}_V \otimes \epsilon) \circ \rho = \mathrm{id}_V. \end{cases}$$

to v , we find that

$$\begin{aligned} \sum_i u_i \otimes e_i \otimes e_i &= \sum_i \rho(u_i) \otimes e_i \\ v &= \sum u_i. \end{aligned}$$

The first equality shows that

$$\rho(u_i) = u_i \otimes e_i \in \langle u_i \rangle \otimes_k A,$$

and the second shows that the set of u_i 's arising in this way span V .

(c) \Rightarrow (a): In particular, the regular representation of G is diagonalizable, and so $\mathcal{O}(G)$ is spanned by its eigenvectors. Let $f \in \mathcal{O}(G)$ be an eigenvector for the regular representation, and let χ be the corresponding character. Then

$$f(hg) = f(h)\chi(g) \quad \text{for } h, g \in G(R), R \text{ a } k\text{-algebra.}$$

In particular, $f(g) = f(e)\chi(g)$, and so f is a multiple of χ . Hence $\mathcal{O}(G)$ is spanned by its characters.

(b) \Rightarrow (c): As every representation is a sum of finite-dimensional subrepresentations (8.33), (b) implies that every representation is a sum of one-dimensional subrepresentations.

(c) \Rightarrow (b): Trivial.

(c) \Rightarrow (d): Certainly, (c) implies that $V = \sum_{\chi \in X(G)} V_\chi$, and Theorem 8.65 implies that the sum is direct.

(d) \Rightarrow (c): Clearly each space V_χ is a sum of one-dimensional representations. \square

NOTES Part of this subsection duplicates §7p.

NOTES Explain that to give a representation of $D(M)$ on V is the same as giving a gradation (grading) on V (for a base ring, see CGP A.8.8.) Better, $\text{Rep}(D(M)) = \dots$

SPLIT TORI

14.16 A **split torus** is an algebraic group isomorphic to a finite product of copies of \mathbb{G}_m . Equivalently, it is a connected diagonalizable algebraic group. Under the equivalence of categories $M \rightsquigarrow D(M)$ (see 14.12a), the split tori correspond to free abelian groups M of finite rank. A quotient of a split torus is again a split torus (because it corresponds to a subgroup of a free abelian group of finite rank), but a subgroup of a split torus need not be a split torus. For example, μ_n is a subgroup of \mathbb{G}_m (the map $\mu_n \rightarrow \mathbb{G}_m$ corresponds to $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$).

EXAMPLE 14.17 Let T be the split torus $\mathbb{G}_m \times \mathbb{G}_m$. Then $X(T) \simeq \mathbb{Z} \oplus \mathbb{Z}$, and the character corresponding to $(m_1, m_2) \in \mathbb{Z} \oplus \mathbb{Z}$ is

$$(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2}: T(R) \rightarrow \mathbb{G}_m(R).$$

A representation V of T decomposes into a direct sum of subspaces $V_{(m_1, m_2)}$, $(m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}$, such that $(t_1, t_2) \in T(k)$ acts on $V_{(m_1, m_2)}$ as $t_1^{m_1} t_2^{m_2}$. In this way, the category $\text{Rep}(T)$ acquires a gradation by the group $\mathbb{Z} \times \mathbb{Z}$.

14e Groups of multiplicative type

DEFINITION 14.18 An affine group G is of **multiplicative type** if $G_{k^{\text{sep}}}$ is diagonalizable.

Let M be an abelian group, and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. A *continuous action* of Γ on M is a homomorphism $\Gamma \rightarrow \text{Aut}(M)$ such that every element of M is fixed by an open subgroup of Γ , i.e.,

$$M = \bigcup_K M^{\text{Gal}(k^{\text{sep}}/K)}$$

where K runs through the finite Galois extensions of k contained in k^{sep} .

For an affine group G , we define

$$X^*(G) = \text{Hom}(G_{k^{\text{sep}}}, \mathbb{G}_m).$$

LEMMA 14.19 *The canonical action of Γ on $X^*(G)$ is continuous.*

PROOF. When G is algebraic, $X^*(G)$ is finitely generated, and each of its generators is defined over a finite separable extension of k ; therefore the action factors through $\text{Gal}(K/k)$ for some finite Galois extension K of k . In the general case, every homomorphism $G_{k^{\text{sep}}} \rightarrow \mathbb{G}_m$ factors through an algebraic quotient of G , and so $X^*(G) = \bigcup X^*(Q)$ with Q algebraic. \square

THEOREM 14.20 *The functor X^* is a contravariant equivalence from the category of affine groups of multiplicative type over k to the category of commutative groups with a continuous action of Γ . Under the equivalence, short exact sequences correspond to short exact sequences.*

PROOF. To give a continuous semilinear action of Γ on $k^{\text{sep}}[M]$ is the same as giving a continuous action of Γ on M (because M is the set of group-like elements in $k^{\text{sep}}[M]$ and M is a k^{sep} -basis for $k^{\text{sep}}[M]$), and so this follows from Theorem 14.12 and Proposition 4.13. \square

Let G be a group of multiplicative type over k . For any $K \subset k^{\text{sep}}$,

$$G(K) = \text{Hom}(X^*(G), k^{\text{sep}\times})^{\Gamma_K}$$

where Γ_K is the subgroup of Γ of elements fixing K , and the notation means the $G(K)$ equals the group of homomorphisms $X^*(G) \rightarrow k^{\text{sep}\times}$ commuting with the actions of Γ_K .

EXAMPLE 14.21 Take $k = \mathbb{R}$, so that Γ is cyclic of order 2, and let $X^*(G) = \mathbb{Z}$. Then $\text{Aut}(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$, and so there are two possible actions of Γ on $X^*(G)$.

- (a) Trivial action. Then $G(\mathbb{R}) = \mathbb{R}^\times$, and $G \simeq \mathbb{G}_m$.
- (b) The generator ι of Γ acts on \mathbb{Z} as $m \mapsto -m$. Then $G(\mathbb{R}) = \text{Hom}(\mathbb{Z}, \mathbb{C}^\times)^{\Gamma}$ consists of the elements of \mathbb{C}^\times fixed under the following action of ι ,

$$\iota z = \bar{z}^{-1}.$$

Thus $G(\mathbb{R}) = \{z \in \mathbb{C}^\times \mid z\bar{z} = 1\}$, which is compact.

EXAMPLE 14.22 Let K be a finite separable extension of k , and let T be the functor $R \rightsquigarrow (R \otimes_k K)^\times$. Then T is the group of multiplicative type corresponding to the Γ -module $\mathbb{Z}^{\text{Hom}_k(K, k^{\text{sep}})}$ (families of elements of \mathbb{Z} indexed by the k -homomorphisms $K \rightarrow k^{\text{sep}}$).

ASIDE 14.23 SGA3, IX 1.1, defines a group scheme to be of multiplicative type if it is locally diagonalizable group for the flat (fpqc) topology. Over a field k , this amounts to requiring the group scheme to become diagonalizable over some field extension of k . Because of Theorem 14.28 below, this is equivalent to our definition.

TORI

DEFINITION 14.24 A **torus** is an algebraic group T such that $T_{k^{\text{sep}}}$ is a split torus.

In other words, the tori are the algebraic groups T of multiplicative type such that $X^*(T)$ is torsion free.

PROPOSITION 14.25 For a torus T , there exist (unique) subtori T_1, \dots, T_r such that

- ◊ $T = T_1 \cdots T_r$,
- ◊ $T_i \cap T_j$ is finite for all $i \neq j$, and
- ◊ $X^*(T_i)_{\mathbb{Q}}$ is a simple Γ -module for all i .

PROOF. Let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. Because $X^*(T)$ is finitely generated, Γ acts on it through a finite quotient. Therefore Maschke's theorem (GT 7.4) shows that $X^*(T)_{\mathbb{Q}}$ is a direct sum of simple Γ -modules, say,

$$X^*(T)_{\mathbb{Q}} = V_1 \oplus \cdots \oplus V_r.$$

Let M_i be the image of $X^*(T)$ in V_i . Then there is an exact sequence

$$0 \rightarrow X^*(T) \rightarrow M_1 \times \cdots \times M_r \rightarrow F \rightarrow 0$$

of continuous Γ -modules with F finite. On applying the functor D , we get an exact sequence of algebraic groups of multiplicative type

$$0 \rightarrow D(F) \rightarrow D(M_1) \times \cdots \times D(M_r) \rightarrow T \rightarrow 0.$$

Take $T_i = D(M_i)$. □

A torus is **anisotropic** if $X(T) = 0$, i.e., $X^*(T)^{\Gamma} = 0$.

COROLLARY 14.26 Every torus has a largest split subtorus T_s and a largest anisotropic subtorus T_a . The intersection $T_s \cap T_a$ is finite and $T_s \cdot T_a = T$.

PROOF. In fact T_s is the product of the T_i in the proposition such that Γ act trivially on $X^*(T_i)$ and T_a is the product of the remainder. □

REPRESENTATIONS OF A GROUP OF MULTIPLICATIVE TYPE

When G is a diagonalizable affine group, $\text{Rep}(G)$ is a semisimple abelian category whose simple objects are in canonical one-to-one correspondence with the characters of G . When G is of multiplicative type, the description of $\text{Rep}(G)$ is only a little more complicated.

Let k^{sep} be a separable closure of k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$.

THEOREM 14.27 Let G be an affine group of multiplicative type. Then $\text{Rep}(G)$ is a semisimple abelian category whose simple objects are in canonical one-to-one correspondence with the orbits of Γ acting on $X^*(G)$.

PROOF. It suffices to prove this in the case that G is algebraic, and so is split by a finite Galois extension Ω of k with Galois group $\bar{\Gamma}$. Let $\bar{\Gamma}$ act on $\mathcal{O}(G_\Omega) \simeq \Omega \otimes \mathcal{O}(G)$ through its action on Ω . By a semilinear action of $\bar{\Gamma}$ on a representation (V, r) of G_Ω , we mean a semilinear action of $\bar{\Gamma}$ on V such that $\gamma\rho = \rho$ where ρ is the coaction of $\mathcal{O}(G)$ on V . It follows from Proposition 4.12 that the functor $V \rightsquigarrow V_\Omega$ from $\text{Rep}_k(G)$ to the category of objects of $\text{Rep}_\Omega(G_\Omega)$ equipped with a semilinear action of $\bar{\Gamma}$ is an equivalence of categories.

Let V be a finite-dimensional representation of G_Ω equipped with a semilinear action of $\bar{\Gamma}$. Then

$$V = \bigoplus_{\chi \in X(G_\Omega)} V_\chi.$$

An element γ of Γ acts on V by mapping V_χ isomorphically onto $V_{\gamma\chi}$. Therefore, as a representation of G_Ω equipped with a semilinear action of $\bar{\Gamma}$, V decomposes into a direct sum of simple objects corresponding to the orbits of $\bar{\Gamma}$ acting on $X(G_\Omega)$. As these are also the orbits of Γ acting on $X^*(G_{k^{\text{sep}}}) \simeq X(G_\Omega)$, the statement follows. \square

CRITERIA FOR AN AFFINE GROUP TO BE OF MULTIPLICATIVE TYPE

Recall that if C is a finite-dimensional cocommutative coalgebra over k , then its linear dual C^\vee is a commutative algebra over k (§5c). We say that C is *coétale* if C^\vee is étale. More generally, we say that a cocommutative coalgebra over k is *coétale* if every finite-dimensional subcoalgebra is coétale (cf. 8.9).

THEOREM 14.28 *The following conditions on an affine group G over k are equivalent:*

- (a) G is of multiplicative type (i.e., G becomes diagonalizable over k^{sep});
- (b) G becomes diagonalizable over some field $K \supset k$;
- (c) G is commutative and $\text{Hom}(G, \mathbb{G}_a) = 0$;
- (d) G is commutative and $\mathcal{O}(G)$ is coétale.

PROOF. (a) \Rightarrow (b): Trivial.

(b) \Rightarrow (c): Clearly

$$\text{Hom}(G, \mathbb{G}_a) \simeq \{f \in \mathcal{O}(G) \mid \Delta(f) = f \otimes 1 + 1 \otimes f\}.$$

The condition on f is linear, and so, for any field $K \supset k$,

$$\text{Hom}(G_K, \mathbb{G}_{aK}) \simeq \text{Hom}(G, \mathbb{G}_a) \otimes K.$$

Thus, we may suppose that G is diagonalizable. If $\alpha: G \rightarrow \mathbb{G}_a$ is a nontrivial homomorphism, then

$$g \mapsto \begin{pmatrix} 1 & \alpha(g) \\ 0 & 1 \end{pmatrix}$$

is a nonsemisimple representation of G , which contradicts (14.15).

(c) \Rightarrow (d): We may assume that k is algebraically closed. Let C be finite-dimensional subcoalgebra of $\mathcal{O}(G)$, i.e., a finite-dimensional k -subspace such that $\Delta(C) \subset C \otimes C$. Let $A = C^\vee$. Then A is a finite product of local Artin rings with residue field k (CA 15.7). If one of these local rings is not a field, then there exists a surjective homomorphism of k -algebras

$$A \rightarrow k[\varepsilon], \quad \varepsilon^2 = 0.$$

This can be written $x \mapsto \langle x, a \rangle + \langle x, b \rangle \varepsilon$ for some $a, b \in C$ with $b \neq 0$. For $x, y \in A$,

$$\langle xy, a \rangle + \langle xy, b \rangle \varepsilon = \langle xy, \Delta a \rangle + \langle x \otimes y, \Delta b \rangle \varepsilon$$

and

$$\begin{aligned} (\langle x, a \rangle + \langle x, b \rangle \varepsilon)(\langle y, a \rangle + \langle y, b \rangle \varepsilon) &= \langle x, a \rangle \langle y, a \rangle + (\langle x, a \rangle \langle y, b \rangle + \langle x, b \rangle \langle y, a \rangle) \varepsilon \\ &= \langle x \otimes y, a \rangle + \langle x \otimes y, a \otimes b + b \otimes a \rangle \varepsilon. \end{aligned}$$

It follows that

$$\begin{aligned} \Delta a &= a \otimes a \\ \Delta b &= a \otimes b + b \otimes a. \end{aligned}$$

On the other hand, the structure map $k \rightarrow A$ is $(\varepsilon|_C)^\vee$, and so $\varepsilon(a) = 1$. Therefore a is a group-like element of $\mathcal{O}(G)$, and so it is a unit (see §14a). Now

$$\begin{aligned} \Delta(ba^{-1}) &= \Delta b \cdot \Delta a^{-1} = (a \otimes b + b \otimes a)(a^{-1} \otimes a^{-1}) \\ &= 1 \otimes ba^{-1} + ba^{-1} \otimes 1, \end{aligned}$$

and so $\text{Hom}(G, \mathbb{G}_a) \neq 0$, which contradicts (c). Therefore A is a product of fields.

(d) \Rightarrow (a): We may suppose that k is separably closed. Let C be a finite-dimensional subcoalgebra of $\mathcal{O}(G)$, and let $A = C^\vee$. By assumption, A is a product of copies of k . Let a_1, \dots, a_n be elements of C such that

$$x \mapsto (\langle x, a_1 \rangle, \dots, \langle x, a_n \rangle): A \rightarrow k^n$$

is an isomorphism. Then $\{a_1, \dots, a_n\}$ spans C and the argument in the above step shows that each a_i is a group-like element of C . As $\mathcal{O}(G)$ is a union of its finite-dimensional subcoalgebras (8.9), this shows that $\mathcal{O}(G)$ is spanned by its group-like elements. \square

COROLLARY 14.29 *An affine group G is of multiplicative type if and only if $G_{k^{\text{al}}}$ is diagonalizable.*

PROOF. Certainly, $G_{k^{\text{al}}}$ is diagonalizable if G is of multiplicative type, and the converse follows the theorem. \square

COROLLARY 14.30 *A commutative affine group G is of multiplicative type if and only if $\text{Rep}(G)$ is semisimple.*

PROOF. We saw in 14.27 that $\text{Rep}(G)$ is semisimple if G is of multiplicative type. Conversely, if $\text{Rep}(G)$ is semisimple, then $\text{Hom}(G, \mathbb{G}_a) = 0$, and so G is of multiplicative type. \square

ASIDE 14.31 In nonzero characteristic, the groups of multiplicative type are the *only* algebraic groups whose representations are all semisimple.⁵² In characteristic zero, the reductive groups also have semisimple representations (see II, 5).

⁵²More precisely, for an algebraic group over a field k of characteristic $p \neq 0$, $\text{Rep}(G)$ is semisimple if and only if G° is of multiplicative type and G/G° has order prime to p (Nagata's theorem, DG IV §3.6, p. 509).

14f Rigidity

Later we shall need the following result.

THEOREM 14.32 *Every action of a connected affine group G on an algebraic group H of multiplicative type is trivial.*

Clearly, it suffices to prove the theorem for an algebraically closed base field k .

PROOF OF THE THEOREM WHEN H IS FINITE.

When $H = \mu_n$, an action of G on M defines a map

$$G \rightarrow \underline{\text{Aut}}(\mu_n) \subset \underline{\text{Hom}}(\mu_n, \mu_n) \simeq \underline{\text{Hom}}(\mu_n, \mathbb{G}_m) \simeq \mathbb{Z}/n\mathbb{Z}$$

(see §12d), which is trivial, because G is connected. A similar argument proves the theorem when H is finite (hence a finite product of groups of the form μ_n).

PROOF OF THE THEOREM IN THE CASE THAT G IS SMOOTH.

We shall use that $G(k)$ is dense in G . We may suppose that H is a torus T . The kernel of $x \mapsto x^m: T \rightarrow T$ is a product of copies of μ_m , and so G acts trivially on it. Because of the category equivalence $T \rightsquigarrow X(T)$, it suffices to show that $g \in G(k)$ acts trivially on the $X(T)$, and because g acts trivially on the kernel of $m: T \rightarrow T$ it acts trivially on $X(T)/mX(T)$. We can now apply the following elementary lemma.

LEMMA 14.33 *Let M be a finitely generated commutative group, and let $\alpha: M \rightarrow M$ be a homomorphism such that*

$$\begin{array}{ccc} M & \longrightarrow & M \\ \downarrow & & \downarrow \\ M/mM & \xrightarrow{\text{id}} & M/mM \end{array}$$

commutes for all m . Then $\alpha = \text{id}$.

PROOF. We may suppose that M is torsion-free. Choose a basis e_i for M , and write $\alpha(e_j) = \sum_i a_{ij} e_i$, $a_{ij} \in \mathbb{Z}$. The hypothesis is that, for every integer m ,

$$(a_{ij}) \equiv I_n \pmod{m},$$

i.e., that $m|a_{ij}$ for $i \neq j$ and $m|a_{ii} - 1$. Clearly, this implies that $(a_{ij}) = I_n$. □

PROOF OF THE THEOREM IN THE GENERAL CASE.

This doesn't use the smooth case.

LEMMA 14.34 *Let V be a k -vector space, and let M be a finitely generated commutative group. Then the family of homomorphisms*

$$V \otimes k[M] \rightarrow V \otimes k[M/nM], \quad n \geq 2,$$

is injective.

PROOF. An element f of $V \otimes k[M]$ can be written uniquely in the form

$$f = \sum_{m \in M} f_m \otimes m, \quad f_m \in V.$$

Assume $f \neq 0$, and let $I = \{m \in M \mid f_m \neq 0\}$. As I is finite, for some n , the elements of I will remain distinct in M/nM , and for this n , the image of f in $V \otimes_k k[M/nM]$ is nonzero. \square

As k is algebraically closed, the group H is diagonalizable. We saw above, that G acts trivially on H_n for all n . Let $H = D(M)$ with M a finitely generated abelian group. Then $\mathcal{O}(H) = k[M]$ and $\mathcal{O}(H_n) = k[M/nM]$. Let

$$\rho: k[M] \rightarrow \mathcal{O}(G) \otimes k[M]$$

give the action. We have to show that $\rho(x) = 1 \otimes x$ for each $x \in k[M]$, but this follows from the fact that G acts trivially on H_n for all $n \geq 2$, and the family of maps

$$\mathcal{O}(G) \otimes_k k[M] \rightarrow \mathcal{O}(G) \otimes_k k[M/nM], \quad n \geq 2,$$

is injective.

DENSITY OF THE TORSION POINTS

PROPOSITION 14.35 *Let T be an algebraic group of multiplicative type, and let T_n be the kernel of $n: T \rightarrow T$. Let $\alpha: T \rightarrow T$ be a homomorphism whose restriction to T_n is the identity map for all n . Then α is the identity map.*

PROOF. It suffices to show that $X^*(\alpha): X^*(T) \rightarrow X^*(T)$ is the identity map, but the hypothesis says that $X^*(\alpha)$ induces the identity map on the quotient $X^*(T)/nX^*(T) = X^*(T_n)$ for all n , and so this follows from Lemma 14.33. \square

14g Exercises

EXERCISE 14-1 Show that the functor

$$C \rightsquigarrow \{\text{group-like elements in } C \otimes k^{\text{sep}}\}$$

is an equivalence from the category of coétale finite cocommutative k -coalgebras to the category of finite sets with a continuous action of $\text{Gal}(k^{\text{sep}}/k)$. (Hint: use 12.7.)

EXERCISE 14-2 Show that $\underline{\text{Aut}}(\mu_m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (constant group defined by the group of invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$). Hint: To recognize the elements of $\underline{\text{Aut}}(\mu_m)(R)$ as complete systems of orthogonal idempotents, see the proof of (14.2).

EXERCISE 14-3 Let k'/k be a cyclic Galois extension of degree n with Galois group Γ generated by σ , and let $G = (\mathbb{G}_m)_{k'/k}$.

- Show that $X^*(G) \simeq \mathbb{Z}[\Gamma]$ (group algebra $\mathbb{Z} + \mathbb{Z}\sigma + \cdots + \mathbb{Z}\sigma^{n-1}$ of Γ).
- Show that

$$\text{End}_\Gamma(X^*(G)) = \left\{ \left(\begin{array}{cccc} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{array} \right) \middle| a_i \in \mathbb{Z} \right\}.$$

15 Unipotent affine groups

Recall that an endomorphism of a finite-dimensional vector space V is unipotent if its characteristic polynomial is $(T - 1)^{\dim V}$. For such an endomorphism, there exists a basis of V relative to which its matrix lies in

$$\mathbb{U}_n(k) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}.$$

Let G be an algebraic group over a perfect field k . We say that $g \in G(k)$ is unipotent if $r(g)$ is unipotent for all finite-dimensional representations (V, r) of G . It suffices to check that $r(g)$ is unipotent for some faithful representation (V, r) , or that $g = g_u$ (see 10.18).

By definition, a smooth algebraic group G over a field k is unipotent if the elements of $G(k^{\text{al}})$ are all unipotent. However, not all unipotent groups are smooth, and so we adopt a different definition equivalent to requiring that the group be isomorphic to a subgroup of \mathbb{U}_n .

Throughout this section, k is a field.

15a Preliminaries from linear algebra

LEMMA 15.1 *Let $G \rightarrow \text{GL}(W)$ be a simple linear representation of an abstract group G on a finite-dimensional vector space W over an algebraically closed field k . Let G act on $\text{End}(W)$ by the rule:*

$$(gf)(w) = g(f(w)), \quad g \in G, \quad f \in \text{End}(W), \quad w \in W.$$

Then every nonzero G -subspace X of $\text{End}(W)$ contains an element $f_0: W \rightarrow W$ such that $f_0(W)$ has dimension one.

PROOF. We may suppose that X is simple. Then the k -algebra of G -endomorphisms of X is a division algebra, and hence equals k (Schur's lemma, GT 7.24, 7.29). For any $w \in W$, the map φ_w ,

$$f \mapsto f(w): X \rightarrow W$$

is a G -homomorphism. As $X \neq 0$, there exists an $f \in X$ and a $w_0 \in W$ such that $f(w_0) \neq 0$. Then $\varphi_{w_0} \neq 0$, and so it is an isomorphism (because X and W are simple). Let $f_0 \in X$ be such that $\varphi_{w_0}(f_0) = w_0$.

Let $w \in W$. Then $\varphi_{w_0}^{-1} \circ \varphi_w$ is a G -endomorphism of X , and so $\varphi_w = c(w)\varphi_{w_0}$ for some $c(w) \in k$. On evaluating this at f_0 , we find that $f_0(w) = c(w)w_0$, and so $f_0(W) \subset \langle w_0 \rangle$. \square

PROPOSITION 15.2 *Let V be a finite-dimensional vector space, and let G be a subgroup of $\text{GL}(V)$ consisting of unipotent endomorphisms. Then there exists a basis of V for which G is contained in \mathbb{U}_n .*

PROOF. It suffices to show that $V^G \neq 0$, because then we can apply induction on the dimension of V to obtain a basis of V with the required property⁵³.

Choose a basis $(e_i)_{1 \leq i \leq n}$ for V . The condition that a vector $v = \sum a_i e_i$ be fixed by all $g \in G$ is linear in the a_i , and so has a solution in k^n if and only if it has a solution in $(k^{\text{al}})^n$.⁵⁴ Therefore we may suppose that k is algebraically closed.

Let W be a nonzero subspace of V of minimal dimension among those stable under G . Clearly W is simple. For each $g \in G$, $\text{Tr}_W(g) = \dim W$, and so

$$\text{Tr}_W(g(g' - 1)) = \text{Tr}_W(gg') - \text{Tr}_W(g) = 0.$$

Let $U = \{f \in \text{End}(W) \mid \text{Tr}_W(gf) = 0 \text{ for all } g \in G\}$. If G acts nontrivially on W , then U is nonzero because $(g' - 1)|_W \in U$ for all $g' \in G$. The lemma then shows that U contains an element f_0 such that $f_0(W)$ has dimension one. Such an f_0 has $\text{Tr}_W f_0 \neq 0$, which contradicts the fact that $f_0 \in U$. We conclude that G acts trivially on W . \square

15b Unipotent affine groups

DEFINITION 15.3 An affine group G is **unipotent** if every nonzero representation of G has a nonzero fixed vector (i.e., a nonzero $v \in V$ such that $\rho(v) = v \otimes 1$ when V is regarded as a $\mathcal{O}(G)$ -comodule).

Equivalently, G is unipotent if every simple object in $\text{Rep}(G)$ is trivial. We shall see that the unipotent algebraic groups are exactly the algebraic groups isomorphic to affine subgroups of \mathbb{U}_n for some n . For example, \mathbb{G}_a and its subgroups are unipotent.

PROPOSITION 15.4 An algebraic group G is unipotent if and only if, for every finite-dimensional representation (V, r) of G , there exists a basis of V for which the image of G is contained in \mathbb{U}_n .

PROOF. \Rightarrow : This can be proved by induction on the dimension of V (see footnote 53).

\Leftarrow : If e_1, \dots, e_n is such a basis, then $\langle e_1 \rangle$ is fixed by G . \square

DEFINITION 15.5 A Hopf algebra A is said to be **coconnected** if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \dots$ of A by subspaces C_i such that⁵⁵

$$C_0 = k, \bigcup_{r \geq 0} C_r = A, \text{ and } \Delta(C_r) \subset \sum_{0 \leq i \leq r} C_i \otimes C_{r-i}. \quad (102)$$

⁵³We use induction on the dimension of V . Let e_1, \dots, e_m be a basis for V^G . The induction hypothesis applied to G acting on V/V^G shows that there exists a basis $\bar{e}_{m+1}, \dots, \bar{e}_n$ for V/V^G such that

$$\alpha(\bar{e}_{m+i}) = c_{1,i} \bar{e}_{m+1} + \dots + c_{i-1,i} \bar{e}_{m+i-1} + \bar{e}_{m+i} \text{ for all } i \leq n - m.$$

Let $\bar{e}_{m+i} = e_{m+i} + V^G$ with $e_{m+i} \in V$. Then e_1, \dots, e_n is a basis for V relative to which $G \subset \mathbb{U}_n(k)$.

⁵⁴For any representation (V, r) of an abstract group G , the subspace V^G of V is the intersection of the kernels of the linear maps

$$v \mapsto gv - v: V \rightarrow V, \quad g \in G.$$

It follows that $(V \otimes \bar{k})^{G_{\bar{k}}} \simeq V^G \otimes \bar{k}$, and so

$$(V \otimes \bar{k})^{G_{\bar{k}}} \neq 0 \implies V^G \neq 0.$$

⁵⁵This definition is probably as mysterious to the reader as it is to the author. Basically, it is the condition you arrive at when looking at Hopf algebras with only one group-like element (so the corresponding affine group has only one character). See Sweedler, Moss Eisenberg. Hopf algebras with one grouplike element. Trans. Amer. Math. Soc. 127 1967 515–526.

THEOREM 15.6 *The following conditions on an algebraic group G are equivalent:*

- (a) G is unipotent;
- (b) G is isomorphic to an algebraic subgroup of \mathbb{U}_n for some n ;
- (c) the Hopf algebra $\mathcal{O}(G)$ is coconnected.

PROOF. (a) \Rightarrow (b). Apply Proposition 15.4 to a faithful finite-dimensional representation of G (which exists by 8.31).

(b) \Rightarrow (c). Any quotient of a coconnected Hopf algebra is coconnected (the image of a filtration satisfying (102) will still satisfy (102)), and so it suffices to show that $\mathcal{O}(\mathbb{U}_n)$ is coconnected. Recall that $\mathcal{O}(\mathbb{U}_n) \simeq k[X_{ij} \mid i < j]$, and that

$$\Delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \sum_{i < r < j} X_{ir} \otimes X_{rj}.$$

Assign a weight of $j - i$ to X_{ij} , so that a monomial $\prod X_{ij}^{n_{ij}}$ will have weight $\sum n_{ij}(j - i)$, and let C_r be the subspace spanned by the monomials of weight $\leq r$. Clearly, $C_0 = k$, $\bigcup_{r \geq 0} C_r = A$, and $C_i C_j \subset C_{i+j}$. It suffices to check the third condition in (102) on the monomials. For the X_{ij} it is obvious. We proceed by induction on weight of a monomial. If the condition holds for monomials P, Q of weights r, s , then $\Delta(PQ) = \Delta(P)\Delta(Q)$ lies in

$$\begin{aligned} \left(\sum C_i \otimes C_{r-i} \right) \left(\sum C_j \otimes C_{s-j} \right) &\subset \sum (C_i C_j \otimes C_{r-i} C_{s-j}) \\ &\subset \sum C_{i+j} \otimes C_{r+s-i-j}. \end{aligned}$$

(c) \Rightarrow (a). Now assume that $\mathcal{O}(G)$ is a coconnected Hopf algebra, and let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be a comodule. Then V is a union of the subspaces

$$V_r = \{v \in V \mid \rho(v) \in V \otimes C_r\}.$$

If V_0 contains a nonzero vector v , then $\rho(v) = v' \otimes 1$ for some vector v' ; on applying ϵ , we find that $v = v'$, and so v is fixed. We complete the proof by showing that

$$V_r = 0 \implies V_{r+1} = 0.$$

By definition, $\rho(V_{r+1}) \subset V \otimes C_{r+1}$, and so

$$(\text{id} \otimes \Delta)\rho(V_{r+1}) \subset V \otimes \sum_i C_i \otimes C_{r-i}.$$

Hence V_{r+1} maps to zero in $V \otimes A/C_r \otimes A/C_r$. We now use that $(\text{id} \otimes \Delta) \circ \rho = (\rho \otimes \text{id}) \circ \rho$. The map $V \rightarrow V \otimes A/C_r$ defined by ρ is injective because $V_r = 0$, and on applying $\rho \otimes \text{id}$ we find that $V \rightarrow (V \otimes A/C_r) \otimes A/C_r$ is injective. Hence $V_{r+1} = 0$. \square

NOTES The exposition of 15.6 follows Waterhouse 1979, 8.3.

COROLLARY 15.7 *Subgroups, quotients, and extensions of unipotent groups are unipotent.*

PROOF. If G is isomorphic to a subgroup of \mathbb{U}_n , then so also is a subgroup of G .

A representation of a quotient of G can be regarded as a representation of G , and so has a nonzero fixed vector if it is nontrivial and G is unipotent.

Suppose that G contains a normal subgroup N such that both N and G/N are unipotent. For any representation (V, r) of G , the subspace V^N is stable under G (see 8.67), and so it defines a representation of G/N . If $V \neq 0$, then $V^N \neq 0$, and so $V^G = (V^N)^{G/N} \neq 0$. \square

COROLLARY 15.8 *Let G be an algebraic group. If G is unipotent, then all elements of $G(k)$ are unipotent, and the converse is true when $G(k)$ is dense in G .*

PROOF. Let G be unipotent, and let (V, r) be a finite-dimensional representation of V . For some basis of V , the $r(G) \subset \mathbb{U}_n$ and so $r(G(k)) \subset \mathbb{U}_n(k)$; in particular, the elements of $r(G(k))$ are unipotent. For the converse, choose a faithful representation $G \rightarrow \mathrm{GL}_V$ of G and let $n = \dim V$. According to Proposition 15.2, there exists a basis of V for which $G(k) \subset \mathbb{U}_n(k)$. Because $G(k)$ is dense in G , this implies that $G \subset \mathbb{U}_n$. \square

15.9 For an algebraic group G , even over an algebraically closed field k , it is possible for all elements of $G(k)$ to be unipotent without G being unipotent. For example, in characteristic p , the algebraic group μ_p has $\mu_p(k^{\mathrm{al}}) = 1$, but it is not unipotent. \otimes

COROLLARY 15.10 *Let k' be a field containing k . An algebraic group G over k is unipotent if and only if $G_{k'}$ is unipotent.*

PROOF. If G is unipotent, then $\mathcal{O}(G)$ is coconnected. But then $k' \otimes \mathcal{O}(G)$ is obviously coconnected, and so $G_{k'}$ unipotent. Conversely, suppose that $G_{k'}$ is unipotent. For any representation (V, r) of G , the subspace V^G of V is the kernel of the linear map

$$v \mapsto \rho(v) - v \otimes 1: V \rightarrow V \otimes \mathcal{O}(G).$$

It follows that

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k',$$

and so

$$(V \otimes k')^{G_{k'}} \neq 0 \implies V^G \neq 0. \quad \square$$

EXAMPLE 15.11 Let k be a nonperfect field of characteristic $p \neq 0$, and let $a \in k \setminus k^p$. The affine subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^p = X - aX^p$$

becomes isomorphic to \mathbb{G}_a over $k[a^{\frac{1}{p}}]$, but it is not isomorphic to \mathbb{G}_a over k . To see this, let C be the complete regular curve with function field $k(C)$ the field of fractions of $\mathcal{O}(G)$. Then $G \subset C$, and one checks that the complement consists of a single point whose residue field is $k[a^{\frac{1}{p}}]$. The inclusion $G \subset C$ is canonical, and if $G \simeq \mathbb{G}_a$, then the complement would consist of a single point with residue field k .

COROLLARY 15.12 *A smooth algebraic group G is unipotent if $G(k^{\mathrm{al}})$ consists of unipotent elements.*

PROOF. If $G(k^{\text{al}})$ consists of unipotent elements, then $G_{k^{\text{al}}}$ is unipotent (15.8), and so G is unipotent (15.10). \square



15.13 A unipotent group need not be smooth. For example, in characteristic p , the subgroup of \mathbb{U}_2 consisting of matrices $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ with $a^p = 0$ is not smooth (it is isomorphic to α_p).

COROLLARY 15.14 *An algebraic group is unipotent if and only if it admits a subnormal series whose quotients are isomorphic to affine subgroups of \mathbb{G}_a .*

PROOF. The group \mathbb{U}_n has a subnormal series whose quotients are isomorphic to \mathbb{G}_a — for example, the following subnormal series

$$\mathbb{U}_4 = \left\{ \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \supset 1$$

has quotients $\mathbb{G}_a \times \mathbb{G}_a \times \mathbb{G}_a$, $\mathbb{G}_a \times \mathbb{G}_a$, \mathbb{G}_a . Therefore any affine subgroup of \mathbb{U}_n has a subnormal series whose quotients are isomorphic to affine subgroups of \mathbb{G}_a (see 9.17). For the converse, note that \mathbb{G}_a is unipotent, and so we can apply (15.7). \square

COROLLARY 15.15 *Every homomorphism from a unipotent algebraic group to an algebraic group of multiplicative type is trivial.*

PROOF. A nontrivial homomorphism $U \rightarrow H$ over k gives rise to a nontrivial homomorphism over k^{al} . Over an algebraically closed field, every algebraic group H of multiplicative type is a subgroup of \mathbb{G}_m^n for some n (because every finitely generated commutative group is a quotient of \mathbb{Z}^n for some n), and so it suffices to show that $\text{Hom}(U, \mathbb{G}_m) = 0$ when U is unipotent. But a homomorphism $U \rightarrow \mathbb{G}_m$ is a one-dimensional representation of G , which is trivial by definition. \square

COROLLARY 15.16 *The intersection of a unipotent affine subgroup of an algebraic group with a subgroup of multiplicative type is trivial.*

PROOF. The intersection is unipotent (15.7), and so the inclusion of the intersection into the group of multiplicative type is trivial. \square

For example, $\mathbb{U}_n \cap \mathbb{D}_n = 1$ (which, of course, is obvious).

PROPOSITION 15.17 *An algebraic group G is unipotent if and only if every nontrivial affine subgroup of it admits a nonzero homomorphism to \mathbb{G}_a .*

PROOF. We use the criterion (15.14). Assume that G is unipotent. Then G has a subnormal series

$$G \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$$

whose quotients G_i/G_{i+1} are isomorphic to affine subgroups of \mathbb{G}_a . Let H be a nontrivial affine subgroup of G . As $H \neq 1$, there exists an i such that $H \subset G_i$ but $H \not\subset G_{i+1}$. Now

$$H \rightarrow G_i/G_{i+1} \hookrightarrow \mathbb{G}_a$$

is a nontrivial homomorphism.⁵⁶

For the converse, let G_1 be the kernel of a nontrivial homomorphism $G \rightarrow \mathbb{G}_a$. If $G_1 \neq 1$, let G_2 be the kernel of a nontrivial homomorphism $G_1 \rightarrow \mathbb{G}_a$. Continuing in this fashion, we obtain a subnormal series whose quotients are affine subgroups of \mathbb{G}_a (the series terminates in 1 because the topological space $|G|$ is noetherian and only finitely many G_i can have the same underlying topological space). \square

COROLLARY 15.18 *Every homomorphism from a group of multiplicative type to a unipotent algebraic group is trivial.*

PROOF. Let $\alpha: T \rightarrow U$ be such a homomorphism. If $\alpha T \neq 1$, then it admits a nontrivial homomorphism to \mathbb{G}_a , but this contradicts the fact that αT is of multiplicative type (14.28). \square

EXAMPLE 15.19 Let k be a nonperfect field characteristic p . For any finite sequence a_0, \dots, a_m of elements of k with $a_0 \neq 0$ and $n \geq 1$, the affine subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^{p^n} = a_0X + a_1X^p + \dots + a_mX^{p^m}$$

is a form of \mathbb{G}_a , and every form of \mathbb{G}_a arises in this way (Russell 1970, 2.1; or apply 15.24). Note that G is the fibred product

$$\begin{array}{ccc} G & \longrightarrow & \mathbb{G}_a \\ \downarrow & & \downarrow a_0F + \dots + a_mF^{p^m} \\ \mathbb{G}_a & \xrightarrow{F^n} & \mathbb{G}_a. \end{array}$$

In particular, G is an extension of \mathbb{G}_a by a finite subgroup of \mathbb{G}_a (so it does satisfy 15.14). There is a criterion for when two forms are isomorphic (ibid. 2.3). In particular, any form becomes isomorphic to \mathbb{G}_a over a purely inseparable extension of k .

DEFINITION 15.20 A unipotent algebraic group is said to be *split* if it admits a subnormal series whose quotients are isomorphic to \mathbb{G}_a (and not just subgroups of \mathbb{G}_a).⁵⁷

Such a group is automatically smooth (7.66) and connected (13.21).

⁵⁶Alternatively, use that every algebraic subgroup H of G is unipotent. Therefore H contains a normal affine subgroup N such that H/N is isomorphic to a subgroup of \mathbb{G}_a . Now the composite

$$H \rightarrow H/N \rightarrow \mathbb{G}_a$$

is a nontrivial homomorphism from N to \mathbb{G}_a .

⁵⁷Cf. SGA3, XVII, 5.10: Let k be a field and G an algebraic k -group. Following the terminology introduced by Rosenlicht (*Questions of rationality for solvable algebraic groups over nonperfect fields*. Ann. Mat. Pura Appl. (4) 61 1963 97–120), we say that G is “ k -résoluble” if G has a composition series whose successive quotients are isomorphic to \mathbb{G}_a . . .

PROPOSITION 15.21 *Every smooth connected unipotent algebraic group over a perfect field is split.*

PROOF. tba (cf. Borel 1991, 15.5(ii)). □

In particular, every smooth connected unipotent algebraic group splits over a purely inseparable extension.

Although the definition of “unipotent” applies to all affine groups, we have stated most of the above results for algebraic groups. The next statement shows how to extend them to affine groups.

PROPOSITION 15.22 (a) *An inverse limit of unipotent affine groups is unipotent.*

(b) *An affine group is unipotent if and only if all of its algebraic quotients are unipotent.*

PROOF. Obvious from the definitions. □

ASIDE 15.23 The unipotent algebraic groups over a field of characteristic zero are classified by their Lie algebras; more precisely, over a field k of characteristic zero, the functor $G \rightsquigarrow \text{Lie}(G)$ is an equivalence from the category of unipotent algebraic groups over k to the category of nilpotent Lie algebras over k (see II, 4.7, or DG IV §2 4.5, p. 499).

ASIDE 15.24 The unipotent algebraic groups over a field of characteristic $p \neq 0$ are more complicated than in characteristic zero. However, those isomorphic to a subgroup of \mathbb{G}_a^n for some n are classified by the finite-dimensional $k[F]$ -modules (polynomial ring with $Fa = a^p F$). See DG IV §3, 6.6 et seq., p. 521.

ASIDE 15.25 We compare the different definitions of unipotent in the literature.

- (a) In SGA3, XVII 1.3, an algebraic group scheme G over a field k is defined to be unipotent if there exists an algebraically closed field \bar{k} containing k such that $G_{\bar{k}}$ admits a composition series whose quotients are isomorphic to algebraic subgroups of \mathbb{G}_a . It is proved *ibid.* 2.1 that such a group is affine, and so 15.10 and 15.14 show that this definition is equivalent to our definition.
- (b) In DG IV, §2, 2.1, p. 485, a group scheme G over a field is defined to be unipotent if it is affine and, for every nontrivial affine subgroup H , there exists a nontrivial homomorphism $H \rightarrow \mathbb{G}_a$. Statement 15.17 shows that this is equivalent to our definition. (They remark that an algebraic group scheme satisfying the second condition is automatically affine. However, the constant group scheme $(\mathbb{Z})_k$ satisfies the second condition but is not affine.)
- (c) In Conrad et al. 2010, A.1.3, p. 393, a group scheme U over a field is defined to be unipotent if it is affine of finite type and $U_{k^{\text{al}}}$ admits a finite composition series over k^{al} with successive quotients isomorphic to a k^{al} -subgroup of \mathbb{G}_a . This is equivalent to our definition, except that we don’t require the group scheme to be algebraic.
- (d) In Springer 1998, p. 36, a linear algebraic group is defined to be unipotent if all its elements are unipotent. Implicitly, the group G is assumed to be a smooth affine algebraic group over an algebraically closed field, and the condition is that all the elements of $G(k)$ are unipotent. For such groups, this is equivalent to our definition because of (15.8) (but note that not all unipotent groups are smooth).

ASIDE 15.26 Unipotent groups are extensively studied in Tits 1967. For summaries of his results, see Oesterlé 1984, Chap. V, and Conrad et al. 2010 IV Appendix B. (A unipotent group is said to be *wound* if every map of varieties $\mathbb{A}^1 \rightarrow G$ is constant. Every smooth unipotent algebraic group G has unique largest split affine subgroup G_s , called the *split part* of G . It is normal in G , and the quotient G/G_s is wound. The formation of G_s commutes with separable extensions.)

16 Solvable affine groups

Let G be an abstract group. Recall that the commutator of $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1} = (xy)(yx)^{-1}.$$

Thus, $[x, y] = 1$ if and only if $xy = yx$, and G is commutative if and only if every commutator equals 1. The (*first*) *derived group* G' (or $\mathcal{D}G$) of G is the subgroup generated by commutators. Every automorphism of G maps commutators to commutators, and so G' is a characteristic subgroup of G (in particular, it is normal). In fact, it is the smallest normal subgroup such that G/G' is commutative.

The map (not a group homomorphism)

$$(x_1, y_1, \dots, x_n, y_n) \mapsto [x_1, y_1] \cdots [x_n, y_n]: G^{2n} \rightarrow G$$

has image the set of elements of G that can be written as a product of at most n commutators, and so $\mathcal{D}G$ is the union of the images of these maps. Note that the map $G^{2n-2} \rightarrow G$ factors through $G^{2n} \rightarrow G$,

$$(x_1, y_1, \dots, x_{n-1}, y_{n-1}) \mapsto (x_1, y_1, \dots, x_{n-1}, y_{n-1}, 1, 1) \mapsto [x_1, y_1] \cdots [x_{n-1}, y_{n-1}].$$

A group G is said to be *solvable* if the *derived series*

$$G \supset \mathcal{D}G \supset \mathcal{D}^2G \supset \cdots$$

terminates with 1. For example, if $n \geq 5$, then S_n (symmetric group on n letters) is not solvable because its derived series $S_n \supset A_n$ terminates with A_n .

In this section we extend this theory to algebraic groups. Throughout, k is a field.

16a Trigonalizable affine groups

DEFINITION 16.1 An affine group G is *trigonalizable*⁵⁸ if every nonzero representation of G has a one-dimensional subrepresentation (i.e., there exists a nonzero $v \in V$ such that $\rho(v) = v \otimes a$, $a \in \mathcal{O}(G)$).

Equivalently, G is trigonalizable if every simple object in $\text{Rep}(G)$ is one-dimensional. We shall see that the trigonalizable algebraic groups are exactly the algebraic groups isomorphic to affine subgroups of \mathbb{T}_n for some n . Diagonalizable and unipotent groups are both trigonalizable, and every trigonalizable group is an extension of one by the other.

PROPOSITION 16.2 *An algebraic group G is trigonalizable if and only if, for every finite-dimensional representation (V, ρ) of G , there exists a basis of V for which the image of G is contained in \mathbb{T}_n .*

⁵⁸I follow Borel 1991, p. 203, and DG IV §2 3.1. Other names: triangulable (Waterhouse 1979, p. 72); trigonalizable.

PROOF. \Rightarrow : This can be proved by induction on the dimension of V .

\Leftarrow : If e_1, \dots, e_n is such a basis, then $\langle e_1 \rangle$ is stable by G . \square

THEOREM 16.3 *The following conditions on an algebraic group G are equivalent:*

- (a) G is trigonalizable;
- (b) G is isomorphic to an algebraic subgroup of \mathbb{T}_n for some n ;
- (c) there exists a normal unipotent affine subgroup U of G such that G/U is diagonalizable.

PROOF. (a) \Rightarrow (b). Apply Proposition 16.2 to a faithful finite-dimensional representation of G (which exists by 8.31).

(b) \Rightarrow (c). Embed G into \mathbb{T}_n , and let $U = \mathbb{U}_n \cap G$.

(c) \Rightarrow (a). Let U be as in (c), and let (V, r) be a representation of G . The subspace V^U is stable under U (8.67), and so it defines a representation of G/U . If $V \neq 0$, then $V^U \neq 0$, and so it contains a stable line. \square

COROLLARY 16.4 *Subgroups and quotients of trigonalizable algebraic groups are trigonalizable.*

PROOF. If G is isomorphic to a subgroup of \mathbb{T}_n , then so also is every affine subgroup of G . If every nontrivial representation of G has a stable line, then the same is true of every quotient of G (because a representation of the quotient can be regarded as a representation of G). \square

COROLLARY 16.5 *If an algebraic group G over a field k is trigonalizable, then so also is $G_{k'}$ for any extension field k' .*

PROOF. If $G \subset \mathbb{T}_n$, then the same is true of $G_{k'}$. \square

PROPOSITION 16.6 (a) *An inverse limit of trigonalizable affine groups is trigonalizable.*

(b) *An affine group is trigonalizable if and only if all of its algebraic quotients are trigonalizable.*

PROOF. Obvious from the definitions. \square

THEOREM 16.7 *Let G be a trigonalizable algebraic group, and let U be a normal unipotent subgroup such that G/U is diagonalizable. Then the exact sequence*

$$1 \rightarrow U \rightarrow G \rightarrow G/U \rightarrow 1$$

splits in each of the following cases: k is algebraically closed; k has characteristic zero; k is perfect and G/U is connected; U is split.

PROOF. See DG IV §2 3.5, p. 494; SGA3, XVII, 5.1.1. \square

ASIDE 16.8 In DG IV §3 3.1, a group scheme G over a field is defined to be trigonalizable if it is affine and has a normal unipotent subgroup U such that G/U is diagonalizable. Because of Theorem 16.3, this is equivalent to our definition.

16b Commutative algebraic groups

SMOOTH COMMUTATIVE ALGEBRAIC GROUPS ARE GEOMETRICALLY TRIGONALIZABLE

Let α be an endomorphism of a finite-dimensional vector space V over k . If all the eigenvalues of α lie in k , then there exists a basis for V relative to which the matrix of α lies in

$$\mathbb{T}_n(k) = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\}$$

We extend this elementary statement to sets of commuting endomorphisms.

LEMMA 16.9 *Let V be a finite-dimensional vector space over an algebraically closed field k , and let S be a set of commuting endomorphisms of V . There exists a basis of V for which S is contained in the group of upper triangular matrices, i.e., a basis e_1, \dots, e_n such that*

$$\alpha(\langle e_1, \dots, e_i \rangle) \subset \langle e_1, \dots, e_i \rangle \text{ for all } i. \quad (103)$$

In more down-to-earth terms, let S be a set of commuting $n \times n$ matrices; then there exists an invertible matrix P such that PAP^{-1} is upper triangular for all $A \in S$.

PROOF. We prove this by induction on the dimension of V . If every $\alpha \in S$ is a scalar multiple of the identity map, then there is nothing to prove. Otherwise, there exists an $\alpha \in S$ and an eigenvalue a for α such that the eigenspace $V_a \neq V$. Because every element of S commutes with α , V_a is stable under the action of the elements of S : for $\beta \in S$ and $x \in V_a$,

$$\alpha(\beta x) = \beta(\alpha x) = \beta(ax) = a(\beta x).$$

The induction hypothesis applied to S acting on V_a and V/V_a shows that there exist bases e_1, \dots, e_m for V_a and $\bar{e}_{m+1}, \dots, \bar{e}_n$ for V/V_a such that

$$\begin{aligned} \alpha(\langle e_1, \dots, e_i \rangle) &\subset \langle e_1, \dots, e_i \rangle \quad \text{for all } i \leq m \\ \alpha(\langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle) &\subset \langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle \quad \text{for all } i \leq n - m. \end{aligned}$$

Let $\bar{e}_{m+i} = e_{m+i} + V_a$ with $e_{m+i} \in V$. Then e_1, \dots, e_n is a basis for V satisfying (103). \square

PROPOSITION 16.10 *Let V be a finite-dimensional vector space over an algebraically closed field k , and let G be a smooth commutative affine subgroup of GL_V . Then there exists a basis of V for which G is contained in \mathbb{T}_n .*

PROOF. According to the lemma, there exists a basis of V for which $G(k) \subset \mathbb{T}_n(k)$. Now $G \cap \mathbb{T}_n$ is a subgroup of G such that $(G \cap \mathbb{T}_n)(k) = G(k)$. As $G(k)$ is dense in G (see 7.30), this implies that $G \cap \mathbb{T}_n = G$, and so $G \subset \mathbb{T}_n$. \square

DECOMPOSITION OF A SMOOTH COMMUTATIVE ALGEBRAIC GROUP

DEFINITION 16.11 Let G be an algebraic group over a perfect field k . An element g of $G(k)$ is *semisimple* (resp. *unipotent*) if $g = g_s$ (resp. $g = g_u$) with the notations of 10.18.

Thus, g is semisimple (resp. unipotent) if $r(g)$ is semisimple (resp. unipotent) for one faithful representation (V, r) of G , in which case $r(g)$ is semisimple (resp. unipotent) for all representations r of G .

Theorem 10.18 shows that

$$G(k) = G(k)_s \times G(k)_u \text{ (cartesian product of sets)} \quad (104)$$

where $G(k)_s$ (resp. $G(k)_u$) is the set of semisimple (resp. unipotent) elements in $G(k)$. However, this will not in general be a decomposition of groups, because Jordan decompositions do not respect products, for example, $(gh)_u \neq g_u h_u$ in general. However, if G is commutative, then

$$G \times G \xrightarrow{\text{multiplication}} G$$

is a homomorphism of groups, and so it does respect the Jordan decompositions (10.20). Thus, in this case (104) realizes $G(k)$ as a product of subgroups. We can do better.

PROPOSITION 16.12 *Every smooth commutative algebraic group G over a perfect field is a direct product of two algebraic subgroups*

$$G \simeq G_s \times G_u$$

such that $G_s(k^{\text{al}}) = G(k^{\text{al}})_s$ and $G_u(k^{\text{al}}) = G(k^{\text{al}})_u$. The decomposition is unique.

PROOF. The uniqueness allows us to assume that $k = k^{\text{al}}$. First note that the subgroups \mathbb{D}_n and \mathbb{U}_n of \mathbb{T}_n have trivial intersection, because

$$\mathbb{D}_n(R) \cap \mathbb{U}_n(R) = \{I_n\} \quad (\text{inside } \mathbb{T}_n(R))$$

for all R (alternatively, apply 15.16).

On applying (16.10) to a faithful representation of G , we obtain an embedding $G \hookrightarrow \mathbb{T}_n$ for some n . Let $G_s = G \cap \mathbb{D}_n$ and $G_u = G \cap \mathbb{U}_n$. Because G is commutative,

$$G_s \times G_u \rightarrow G \quad (105)$$

is a homomorphism with kernel $G_s \cap G_u$. Because $\mathbb{D}_n \cap \mathbb{U}_n = 1$ as algebraic groups, $G_s \cap G_u = 1$, and so (105) is injective; because $G_s(k)G_u(k) = G(k)$ and G is smooth, (105) is surjective (7.54); therefore it is an isomorphism. The uniqueness is obvious. \square

REMARK 16.13 Let G be a smooth algebraic group over an algebraically closed field k (not necessarily commutative). In general, $G(k)_s$ will not be closed for the Zariski topology. However, $G(k)_u$ is closed. To see this, embed G in GL_n for some n . A matrix A is unipotent if and only if its characteristic polynomial is $(T - 1)^n$. But the coefficients of the characteristic polynomial of A are polynomials in the entries of A , and so this is a polynomial condition.

DECOMPOSITION OF A COMMUTATIVE ALGEBRAIC GROUP

THEOREM 16.14 *Let G be a commutative algebraic group over a field k .*

- (a) *There exists a largest affine subgroup G_s of G of multiplicative type; this is a characteristic subgroup (in the weak sense) of G , and the quotient G/G_s is unipotent.*
- (b) *If k is perfect, there exists a largest unipotent affine subgroup G_u of G , and $G = G_s \times G_u$. This decomposition is unique.*

PROOF. (a) Let G_s be the intersection of the affine subgroups H of G such that G/H is unipotent. Then $G/G_s \rightarrow \prod G/H$ is injective, and so G/G_s is unipotent (15.7). A nontrivial homomorphism $G_s \rightarrow \mathbb{G}_a$ would have a kernel H such that G/H is unipotent (15.7) but $G_s \not\subset H$, contradicting the definition of G_s . Therefore G_s is of multiplicative type (14.28). If H is a second affine subgroup of G of multiplicative type, then the map $H \rightarrow G/G_s$ is zero (15.18), and so $H \subset G_s$. Therefore G_s is the largest affine subgroup of G of multiplicative type. From this description, it is clear that $\alpha G_s = G_s$ for any automorphism α of G .

(b) Assume k is perfect. Then it suffices to show that $G = T \times U$ with T of multiplicative type and U unipotent because, for any other unipotent affine subgroup U' of G , the map $U' \rightarrow G/U \simeq T$ is zero (15.15), and so $U' \subset U$; similarly any other subgroup T' of multiplicative type is contained in T ; therefore T (resp. U) is the largest subgroup of multiplicative type (resp. unipotent subgroup), and so the decomposition is unique. \square

ASIDE 16.15 In fact, G_s is characteristic in the strong sense, but this requires a small additional argument (DG IV, §2, 2.4, p. 486; §3, 1.1, p. 501); in general, G_u is not (ibid. IV §3, 1.2).

REMARK 16.16 It is necessary that k be perfect in (b). Let k be a separably closed field of characteristic p , and let $G = (\mathbb{G}_m)_{k'/k}$ where k' is an extension of k of degree p (necessarily purely inseparable). Then G is a commutative smooth connected algebraic group over k . The canonical map $\mathbb{G}_m \rightarrow G$ realizes \mathbb{G}_m as G_s , and the quotient G/\mathbb{G}_m is unipotent. Over k^{al} , G decomposes into $(\mathbb{G}_m)_{k^{\text{al}}} \times (G/\mathbb{G}_m)_{k^{\text{al}}}$, and so G is not reductive. However, G contains no unipotent subgroup because $G(k) = k'^{\times}$ has no p -torsion, and so $G_u = 1$. See 17.22.

16c The derived group of algebraic group

Let G be an algebraic group over a field k .

DEFINITION 16.17 The **derived group** DG (or G' or G^{der}) of G is the intersection of the normal algebraic subgroups N of G such that G/N is commutative.

PROPOSITION 16.18 *The quotient G/DG is commutative (hence DG is the smallest normal subgroup with this property).*

PROOF. For any normal affine subgroups N_1, \dots, N_r of G , the canonical homomorphism

$$G \rightarrow G/N_1 \times \cdots \times G/N_r$$

has kernel $N_1 \cap \cdots \cap N_r$. Therefore, if each of the algebraic groups G/N_i is commutative, so also is $G/(N_1 \cap \cdots \cap N_r)$. \square

We shall need another description of $\mathcal{D}G$, which is analogous to the description of the derived group as the subgroup generated by commutators. As for abstract groups, there exist maps of functors

$$G^2 \rightarrow G^4 \rightarrow \dots \rightarrow G^{2^n} \rightarrow G.$$

Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(G^{2^n})$ of k -algebras (not Hopf algebras) defined by $G^{2^n} \rightarrow G$. Then

$$I_1 \supset I_2 \supset \dots \supset I_n \supset \dots$$

and we let $I = \bigcap I_n$.

PROPOSITION 16.19 *The coordinate ring of $\mathcal{D}G$ is $\mathcal{O}(G)/I$.*

PROOF. From the diagram of set-valued functors

$$\begin{array}{ccccc} G^{2^n} & \times & G^{2^n} & \longrightarrow & G^{4n} \\ \downarrow & & \downarrow & & \downarrow \\ G & \times & G & \xrightarrow{\text{mult}} & G \end{array}$$

we get a diagram of k -algebras

$$\begin{array}{ccccc} \mathcal{O}(G)/I_n & \otimes & \mathcal{O}(G)/I_n & \leftarrow & \mathcal{O}(G)/I_{2n} \\ \uparrow & & \uparrow & & \uparrow \\ \mathcal{O}(G) & \otimes & \mathcal{O}(G) & \xleftarrow{\Delta} & \mathcal{O}(G) \end{array}$$

(because $\mathcal{O}(G)/I_n$ is the image of $\mathcal{O}(G)$ in $\mathcal{O}(G^{4n})$). It follows that

$$\Delta: \mathcal{O}(G) \rightarrow \mathcal{O}(G)/I \otimes \mathcal{O}(G)/I$$

factors through $\mathcal{O}(G) \rightarrow \mathcal{O}(G)/I$, and defines a Hopf algebra structure on $\mathcal{O}(G)/I$, which corresponds to the smallest algebraic subgroup G' of G such that $G'(R)$ contains all the commutators for all R . Clearly, this is also the smallest normal subgroup such that G/G' is commutative. □

COROLLARY 16.20 *For any field $K \supset k$, $\mathcal{D}G_K = (\mathcal{D}G)_K$.*

PROOF. The definition of I commutes with extension of the base field. □

COROLLARY 16.21 *If G is connected (resp. smooth), then $\mathcal{D}G$ is connected (resp. smooth).*

PROOF. Recall that an algebraic group G is connected (resp. smooth) if and only if $\mathcal{O}(G)$ has no nontrivial idempotents (resp. nilpotents). If $\mathcal{O}(G)/I$ had a nontrivial idempotent (resp. nilpotent), then so would $\mathcal{O}(G)/I_n$ for some n , but (by definition) the homomorphism of k -algebras $\mathcal{O}(G)/I_n \hookrightarrow \mathcal{O}(G^{2^n})$ is injective. If G is connected (resp. smooth), then so also is G^{2^n} , and so $\mathcal{O}(G^{2^n})$ has no nontrivial idempotents (resp. nilpotents). □

COROLLARY 16.22 *Let G be a smooth connected algebraic group. Then $\mathcal{O}(\mathcal{D}G) = \mathcal{O}(G)/I_n$ for some n , and $(\mathcal{D}G)(k^{\text{al}}) = \mathcal{D}(G(k^{\text{al}}))$.*

PROOF. As G is smooth and connected, so also is G^{2n} (6.1, 13.19). Therefore, each ideal I_n is prime, and a descending sequence of prime ideals in a noetherian ring terminates. This proves the first part of the statement (CA 16.5).


Let V_n be the image of $G^{2n}(k^{\text{al}})$ in $G(k^{\text{al}})$. Its closure in $G(k^{\text{al}})$ is the zero-set of I_n . Being the image of a regular map, V_n contains a dense open subset U of its closure (CA 12.14). Choose n as in the first part, so that the zero-set of I_n is $\mathcal{D}G(k^{\text{al}})$. Then

$$U \cdot U^{-1} \subset V_n \cdot V_n \subset V_{2n} \subset \mathcal{D}(G(k^{\text{al}})) = \bigcup_m V_m \subset \mathcal{D}G(k^{\text{al}}).$$

It remains to show that $U \cdot U^{-1} = \mathcal{D}G(k^{\text{al}})$. Let $g \in \mathcal{D}G(k^{\text{al}})$. Because U is open and dense $\mathcal{D}G(k^{\text{al}})$, so is gU^{-1} , which must therefore meet U , forcing g to lie in $U \cdot U$. \square

COROLLARY 16.23 *The derived group $\mathcal{D}G$ of a smooth algebraic group G is the unique smooth affine subgroup such that $(\mathcal{D}G)(k^{\text{al}}) = \mathcal{D}(G(k^{\text{al}}))$.*

PROOF. The derived group has these properties by (16.21) and (16.22), and it is the only affine subgroup with these properties because $(\mathcal{D}G)(k^{\text{al}})$ is dense in $\mathcal{D}G$. \square

16.24 For an algebraic group G , the group $G(k)$ may have commutative quotients without G having commutative quotients, i.e., we may have $G(k) \neq \mathcal{D}(G(k))$ but $G = \mathcal{D}G$. This is the case for $G = \text{PGL}_n$ over nonperfect separably closed field of characteristic p dividing n . 

16d Solvable algebraic groups

Write \mathcal{D}^2G for the second derived group $\mathcal{D}(\mathcal{D}G)$, \mathcal{D}^3G for the third derived group $\mathcal{D}(\mathcal{D}^2G)$, and so on.

DEFINITION 16.25 An algebraic group G is *solvable* if the *derived series*

$$G \supset \mathcal{D}G \supset \mathcal{D}^2G \supset \dots$$

terminates with 1.

LEMMA 16.26 *An algebraic group G is solvable if and only if it admits a subnormal series*

$$G = G_0 \supset G_1 \supset \dots \supset G_n = 1 \tag{106}$$

whose quotients G_i/G_{i+1} are commutative.

PROOF. If G is solvable, then the derived series is such a sequence. Conversely, given a sequence as in (106), $G_1 \supset \mathcal{D}G$, so $G_2 \supset \mathcal{D}^2G$, \dots , so $G_n \supset \mathcal{D}^nG$. Hence $\mathcal{D}^nG = 1$. \square

A sequence of algebraic subgroups (106) such that G_{i+1} is normal in G_i for each i and G_i/G_{i+1} is commutative is called *solvable series*.

PROPOSITION 16.27 *Subgroups, quotients, and extensions of solvable algebraic groups are solvable.*

PROOF. Obvious. □

EXAMPLE 16.28 Let G be a finite group, and let $(G)_k$ be the algebraic group such that $(G)_k(R) = G$ for all k -algebras R with no nontrivial idempotents. Then $\mathcal{D}(G)_k = (\mathcal{D}G)_k$, $\mathcal{D}^2(G)_k = (\mathcal{D}^2G)_k$, and so on. Therefore $(G)_k$ is solvable if and only if G is solvable. In particular, the theory of solvable algebraic groups includes the theory of solvable finite groups, which is already quite complicated. For example, all finite groups with no element of order 2 are solvable.

EXAMPLE 16.29 The group \mathbb{T}_n of upper triangular matrices is solvable. For example, the subnormal series

$$\mathbb{T}_3 = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \supset 1$$

has quotients $\mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$, $\mathbb{G}_a \times \mathbb{G}_a$, and \mathbb{G}_a .

More generally, the functor

$$R \rightsquigarrow G_0(R) \stackrel{\text{def}}{=} \{(a_{ij}) \mid a_{ii} = 1 \text{ for all } i\}$$

is an algebraic subgroup of \mathbb{T}_n because it is represented by $\mathcal{O}(\mathbb{T}_n)/(T_{11} - 1, \dots, T_{nn} - 1)$. Similarly, there is an algebraic subgroup G_r of G_0 of matrices (a_{ij}) such that $a_{ij} = 0$ for $0 < j - i \leq r$. The functor

$$(a_{ij}) \mapsto (a_{1,r+2}, \dots, a_{i,r+i+1}, \dots)$$

is a homomorphism from G_r onto $\mathbb{G}_a \times \mathbb{G}_a \times \dots$ with kernel G_{r+1} . Thus the sequence of algebraic subgroups

$$\mathbb{T}_n \supset G_0 \supset G_1 \supset \dots \supset G_n = \{1\}$$

exhibits \mathbb{T}_n as a solvable group.

Alternatively, we can work abstractly. A **flag** in a vector space V is a set of subspaces of V , distinct from $\{0\}$ and V , ordered by inclusion. When we order the flags in V by inclusion, the maximal flags are the families $\{V_1, \dots, V_{n-1}\}$ with $\dim V_i = i$, $n = \dim V$, and

$$V_1 \subset \dots \subset V_{n-1}.$$

For example, if $(e_i)_{1 \leq i \leq n}$ is a basis for V , then we get a maximal flag by taking $V_i = \langle e_1, \dots, e_i \rangle$.

Let $F = \{V_1, \dots, V_{n-1}\}$ be a maximal flag in V , and let \mathbb{T} be the algebraic subgroup of GL_V such that $\mathbb{T}(R)$ consists of the automorphisms preserving the flag, i.e., such that $\alpha(V_i \otimes R) \subset V_i \otimes R$ for all k -algebras R . When we take F to be the maximal flag in k^n defined by the standard basis, $G = \mathbb{T}_n$. Let G_0 be the algebraic subgroup of G of α acting as id on the quotients V_i/V_{i-1} ; more precisely,

$$G_0 = \text{Ker}(G \rightarrow \prod \text{GL}_{V_i/V_{i-1}}).$$

Then G_0 is a normal algebraic subgroup of \mathbb{T} with quotient isomorphic to \mathbb{G}_m^n . Now define G_r to be the algebraic subgroup of G_0 of elements α acting as id on the quotients V_i/V_{i-r-1} . Again, G_{r+1} is a normal algebraic subgroup of G_r with quotient isomorphic to a product of copies of \mathbb{G}_a .

EXAMPLE 16.30 The group of $n \times n$ monomial matrices is solvable if and only if $n \leq 4$ (because S_n is solvable if and only if $n \leq 4$; GT 4.33).

THE LIE-KOLCHIN THEOREM

THEOREM 16.31 *Let G be a subgroup of GL_V . If G is connected, smooth, and solvable, and k is algebraically closed, then it is trigonalizable.*

PROOF. It suffices to show that there exists a basis for V such that $G(k) \subset \mathbb{T}_n(k)$ (because then $(G \cap \mathbb{T}_n)(k) = G(k)$, and so $G \cap \mathbb{T}_n = G$, which implies that $G \subset \mathbb{T}$). Also, it suffices to show that the elements of $G(k)$ have a common eigenvector, because then we can apply induction on the dimension of V (cf. the proof of 16.9). We prove this by induction on the length of the derived series G . If the derived series has length zero, then G is commutative, and we proved the result in (16.10). Let $N = \mathcal{D}G$. Its derived series is shorter than that of G , and so we can assume that the elements of N have a common eigenvector, i.e., for some character χ of N , the space V_χ (for N) is nonzero.

Let W be the sum of the nonzero eigenspaces V_χ for N . According to (8.65), the sum is direct, $W = \bigoplus V_\chi$, and so the set $\{V_\chi\}$ of nonzero eigenspaces for N is finite.

Let x be a nonzero element of V_χ for some χ , and let $g \in G(k)$. For $n \in N(k)$,

$$ngx = g(g^{-1}ng)x = g \cdot \chi(g^{-1}ng)x = \chi(g^{-1}ng) \cdot gx$$

For the middle equality we used that N is normal in G . Thus, gx lies in the eigenspace for the character $\chi^g = (n \mapsto \chi(g^{-1}ng))$ of N . This shows that $G(k)$ permutes the finite set $\{V_\chi\}$.

Choose a χ and let $H \subset G(k)$ be the stabilizer of V_χ , so H consists of the $g \in G(k)$ such that

$$\chi(n) = \chi(g^{-1}ng) \text{ for all } n \in N(k). \quad (107)$$

Then, H is a subgroup of finite index in $G(k)$, and it is closed for the Zariski topology on $G(k)$ because (107) is a polynomial condition on g for each n . Therefore $H = G(k)$, otherwise its cosets would disconnect $G(k)$. This shows that $W = V_\chi$, and so $G(k)$ stabilizes V_χ .

An element $n \in N(k)$ acts on V_χ as the homothety $x \mapsto \chi(n)x$, $\chi(n) \in k$. But each element n of $N(k)$ is a product of commutators $[x, y]$ of elements of $G(k)$ (see 16.22), and so n acts on V_χ as an automorphism of determinant 1. This shows that $\chi(n)^{\dim V_\chi} = 1$, and so the image of $\chi: G \rightarrow \mathbb{G}_m$ is finite. Because N is connected, this shows that $N(k)$ in fact acts trivially⁵⁹ on V_χ . Hence $G(k)$ acts on V_χ through the quotient $G(k)/N(k)$, which is commutative. In this case, we know there is a common eigenvalue (16.9). \square

⁵⁹In more detail, the argument shows that the character χ takes values in $\mu_m \subset \mathbb{G}_m$ where $m = \dim V_\chi$. If k has characteristic zero, or characteristic p and $p \nmid m$, then μ_m is étale, and so, because N is connected, χ is trivial. If $p|m$, the argument only shows that χ takes values in μ_{p^r} for p^r the power of p dividing m . But $\mu_{p^r}(k) = 1$, and so the action of $N(k)$ on V is trivial, as claimed.

16.32 All the hypotheses in the theorem are needed (however, if k is algebraically closed and G is solvable, then the theorem applies to G_{red}° , which is a subgroup of G with the same dimension).

CONNECTED: The group G of monomial 2×2 matrices is solvable but not trigonalizable.

The only common eigenvectors of $\mathbb{D}_2(k) \subset G(k)$ are $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, but the monomial matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ interchanges e_1 and e_2 , and so there is no common eigenvector for the elements of $G(k)$.

SMOOTH: (Waterhouse 1979, 10, Exercise 3, p. 79.) Let k have characteristic 2, and let G be the affine subgroup of SL_2 of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a^2 = 1 = d^2$ and $b^2 = 0 = c^2$. There is an exact sequence

$$0 \longrightarrow \mu_2 \xrightarrow{a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}} G \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (ab, cd)} \alpha_2 \times \alpha_2 \longrightarrow 1.$$

Moreover, $\mu_2 \subset Z(G)$, and so G is connected and solvable (even nilpotent), but no line is fixed in the natural action of G on k^2 . Therefore G is not trigonalizable.

SOLVABLE: As \mathbb{T}_n is solvable (16.29) and a subgroup of a solvable group is obviously solvable, this condition is necessary.

k ALGEBRAICALLY CLOSED: If $G(k) \subset \mathbb{T}_n(k)$, then the elements of $G(k)$ have a common eigenvector, namely, $e_1 = (1 \ 0 \ \dots \ 0)^t$. Unless k is algebraically closed, an endomorphism need not have an eigenvector, and, for example,

$$\left\{ \begin{pmatrix} -a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, \quad a^2 + b^2 = 1 \right\}$$

is an commutative algebraic group over \mathbb{R} that is not trigonalizable over \mathbb{R} .

16e Structure of solvable groups

THEOREM 16.33 *Let G be a connected solvable smooth group over a perfect field k . There exists a unique connected normal algebraic subgroup G_u of G such that*

- (a) G_u is unipotent;
- (b) G/G_u is of multiplicative type.

The formation of G_u commutes with change of the base field.

PROOF. We first prove this when $k = k^{\text{al}}$. Embed G into \mathbb{T}_n for some n , and construct

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{U}_n & \longrightarrow & \mathbb{T}_n & \longrightarrow & \mathbb{D}_n & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & G_u & \longrightarrow & G & \longrightarrow & T & \longrightarrow & 1 \end{array}$$

where T is the image of G in \mathbb{D}_n and $G_u = \mathbb{U}_n \cap G$. Certainly G_u is a normal algebraic subgroup of G satisfying (a) and (b). We next prove that G_u is connected.

Let $Q = G/\mathcal{D}G$. It is commutative, so that (16.12)

$$Q \simeq Q_u \times Q_s.$$

This shows that Q_u is connected (if it had an étale quotient, so would Q). As G/G_u is commutative, $\mathcal{D}G \subset G_u$, and the diagram

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \mathcal{D}G & \longrightarrow & G_u & \longrightarrow & \pi_0(G_u) \longrightarrow 1 \\
 & & \parallel & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathcal{D}G & \longrightarrow & G & \longrightarrow & Q \longrightarrow 1 \\
 & & & & \downarrow & & \downarrow \\
 & & & & T & \longrightarrow & Q/\pi G_u \\
 & & & & \downarrow & & \downarrow \\
 & & & & 1 & & 1
 \end{array}$$

shows that $T \simeq Q/\pi_0(G_u)$. Since $\pi(G_u) \subset Q_u$, this shows that $\pi_0(G_u) = Q_u$, and so (13.21)

$$Q_u, \mathcal{D}G \text{ connected} \implies G_u \text{ connected.}$$

For the uniqueness, note that G_u is the largest connected normal unipotent subgroup of G , or that $G_u(k^{\text{al}})$ consists of the unipotent elements of $G(k^{\text{al}})$ (and apply a previous result).

When k is only perfect, the uniqueness of $(G_{k^{\text{al}}})_u$ implies that it is stable under $\Gamma = \text{Gal}(k^{\text{al}}/k)$, and hence arises from a unique algebraic subgroup G_u of G (7.33), which clearly has the required properties. \square

16f Split solvable groups

DEFINITION 16.34 A solvable algebraic group is *split* if it admits subnormal series whose quotients are \mathbb{G}_a or \mathbb{G}_m .

Such a group is automatically smooth (7.66) and connected (13.21). This agrees with our definition of split unipotent group. Any quotient of a split solvable group is again a split solvable group.

16g Tori in solvable groups

PROPOSITION 16.35 Let G be a connected smooth solvable group over an algebraically closed field. If T and T' are maximal tori in G , then $T' = gTg^{-1}$ for some $g \in G(k)$.

PROOF. Omitted for the present (cf. Springer 1998, 6.3.5). \square

PROPOSITION 16.36 The centralizer of any torus in a connected smooth solvable group G is connected.

PROOF. Omitted for the present (cf. Springer 1998, 6.3.5). \square

16h Exercises

EXERCISE 16-1 Give a geometric proof that G connected implies $\mathcal{D}G$ connected. [Show that the image of connected set under a continuous map is connected (for the Zariski topology, say), the closure of a connected set is connected, and a nested union of connected sets is connected; then apply the criterion (13.13).]

EXERCISE 16-2 Show that an algebraic group G is trigonalizable if and only if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \dots$ of $\mathcal{O}(G)$ by subspaces C_i such that C_0 is spanned by group-like elements, $\bigcup_{r \geq 0} C_r = A$, and $\Delta(C_r) \subset \sum_{0 \leq i \leq r} C_i \otimes C_{r-i}$ (Waterhouse 1979, Chap. 9, Ex. 5, p. 72).

17 The structure of algebraic groups

Throughout this section, k is a field.

17a Radicals and unipotent radicals

LEMMA 17.1 *Let N and H be algebraic subgroups of G with N normal. If H and N are solvable (resp. unipotent, resp. connected, resp. smooth), then HN is solvable (resp. unipotent, resp. connected, resp. smooth).*

PROOF. We use the exact sequence

$$\begin{array}{ccccccc}
 1 & \longrightarrow & N & \longrightarrow & HN & \longrightarrow & HN/N & \longrightarrow & 1. \\
 & & & & & & \uparrow \simeq & & \\
 & & & & & & (9.12) & & \\
 & & & & & & H/H \cap N & &
 \end{array}$$

Because H is solvable, so also is its quotient $H/H \cap N$; hence HN/N is solvable, and HN is solvable because it is an extension of solvable groups (16.27). The same argument applies with “solvable” replaced by “unipotent” (use 15.7), or by “connected” (use 13.21), or by “smooth” (use 7.66). □

PROPOSITION 17.2 *Let G be a smooth algebraic group over a field k .*

- (a) *There exists a largest⁶⁰ smooth connected normal solvable subgroup of G (called the **radical** RG of G).*
- (b) *There exists a largest smooth connected normal unipotent subgroup (called the **unipotent radical** R_uG of G).*

PROOF. Immediate consequence of the lemma. □

The formation of the radical and the unipotent radical each commute with separable extensions of the base field: let K be a Galois extension of k with Galois group Γ ; by uniqueness, RG_K is stable under the action of Γ , and therefore arises from a subgroup $R'G$ of G (by 4.13); now $(RG)_K \subset RG_K$, and so $RG \subset R'G$; as RG is maximal, $RG = R'G$, and so $(RG)_K = (R'G)_K = RG_K$.

⁶⁰Recall that “largest” means “unique maximal”.

PROPOSITION 17.3 *Let G be a smooth algebraic group over a perfect field k . For any extension field K of k ,*

$$RG_K = (RG)_K \text{ and } R_u G_K = (R_u G)_K.$$

Moreover, $R_u G = (RG)_u$ (notations as in 16.33).

PROOF. See the above discussion. □

DEFINITION 17.4 Let G be a smooth algebraic group over a field k . The **geometric radical** of G is $RG_{k^{\text{al}}}$, and the **geometric unipotent radical** of G is $R_u G_{k^{\text{al}}}$.

17b Definition of semisimple and reductive groups

DEFINITION 17.5 Let G be an algebraic group over a field k .

- (a) G is **semisimple** if it is smooth and connected and its geometric radical is trivial.
- (b) G is **reductive** if it is smooth and connected and its geometric unipotent radical is trivial.
- (c) G is **pseudoreductive** if it is smooth and connected and its unipotent radical is trivial.

Thus

$$\text{semisimple} \implies \text{reductive} \implies \text{pseudoreductive}.$$

For example, SL_n , SO_n , and Sp_n are semisimple, and GL_n is reductive (but not semisimple). When k is perfect, $R_u G_{k^{\text{al}}} = (R_u G)_{k^{\text{al}}}$, and so reductive and pseudoreductive are equivalent.

PROPOSITION 17.6 *Let G be a smooth connected algebraic group over a perfect field k .*

- (a) G is semisimple if and only if $RG = 1$.
- (b) G is reductive if and only if $R_u G = 1$ (i.e., G is pseudoreductive).

PROOF. Obvious from (17.3). □

PROPOSITION 17.7 *Let G be a smooth connected algebraic group over a field k .*

- (a) *If G is semisimple, then every smooth connected normal commutative subgroup is trivial; the converse is true if k is perfect.*
- (b) *If G is reductive, then every smooth connected normal commutative subgroup is a torus; the converse is true if k is perfect.*

PROOF. (a) Suppose that G is semisimple, and let H be a smooth connected normal commutative subgroup of G . Then $H_{k^{\text{al}}} \subset RG_{k^{\text{al}}} = 1$, and so $H = 1$. For the converse, we use that RG and DG are stable for any automorphism of G . This is obvious from their definitions: RG is the largest connected normal solvable algebraic subgroup and DG is the smallest normal algebraic subgroup such that G/DG is commutative. Therefore the chain

$$G \supset RG \supset \mathcal{D}(RG) \supset \mathcal{D}^2(RG) \supset \cdots \supset \mathcal{D}^r(RG) \supset 1,$$

is preserved by every automorphism of G , and, in particular, by the inner automorphisms defined by elements of $G(k)$. This remains true over k^{al} , and so the groups are normal in G by (7.43). As $\mathcal{D}^r(RG)$ is commutative, it is trivial.

(b) Let H be a smooth connected normal commutative subgroup of G ; then $H_{k^{\text{al}}} \subset RG_{k^{\text{al}}}$, which has no unipotent subgroup. Therefore H is a torus. For the converse, we consider the chain

$$G \supset R_u G \supset \mathcal{D}(R_u G) \supset \mathcal{D}^2(R_u G) \supset \cdots \supset \mathcal{D}^r(R_u G) \supset 1.$$

Then $\mathcal{D}^r(R_u G)$ is a commutative unipotent subgroup, and so is trivial. □

A smooth connected algebraic group G is pseudoreductive but not reductive if it contains no nontrivial normal smooth unipotent affine subgroup but $G_{k^{\text{al}}}$ does contain such a subgroup.

REMARK 17.8 If one of the conditions, smooth, connected, normal, commutative, is dropped, then a semisimple group may have such a subgroup:

Group	subgroup	smooth?	connected?	normal?	commutative?
$\text{SL}_2, \text{char}(k) \neq 2$	$\{\pm I\}$	yes	no	yes	yes
SL_2	$\mathbb{U}_2 = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$	yes	yes	no	yes
$\text{SL}_2 \times \text{SL}_2$	$\{1\} \times \text{SL}_2$	yes	yes	yes	no
$\text{SL}_2, \text{char}(k) = 2$	μ_p	no	yes	yes	yes

PROPOSITION 17.9 Let G be a smooth connected algebraic group over a perfect field. The quotient group G/RG is semisimple, and $G/R_u G$ is reductive.

PROOF. One sees easily that $R(G/RG) = 1$ and $R_u(G/R_u G) = 1$. □

EXAMPLE 17.10 Let G be the group of invertible matrices $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ with A of size $m \times m$ and C of size $n \times n$. The unipotent radical of G is the subgroup of matrices $\begin{pmatrix} I & B \\ 0 & I \end{pmatrix}$. The quotient of G by $R_u G$ is isomorphic to the reductive group of invertible matrices of the form $\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$, i.e., to $\text{GL}_m \times \text{GL}_n$. The radical of this is $\mathbb{G}_m \times \mathbb{G}_m$.

PROPOSITION 17.11 Let G be a connected algebraic group, and let N be a normal unipotent subgroup of G . Then N acts trivially on every semisimple representation of G .

PROOF. Let N be a normal affine subgroup of G , and let (V, r) be a semisimple representation of G . I claim that $(V, r|_N)$ is also semisimple. To prove this, it suffices to show that $(V, r|_N)$ is a sum of simple representations of N (8.68). We may suppose that V is simple as a representation of G . Let S be an N -simple subrepresentation of $(V, r|_N)$, and let W be the sum of all subrepresentations of $(V, r|_N)$ isomorphic to S (i.e., W is the N -isotypic component of V of type S). Then W is stable under G (see 8.73), and so equals V . This proves the claim (in characteristic zero, the proof is simpler — see II, 6.15). If N is unipotent, then every semisimple representation is trivial (by definition 15.3). This proves the proposition. □

COROLLARY 17.12 *Let G be a smooth connected algebraic group. If $\text{Rep}(G)$ is semisimple, then G is reductive.*

PROOF. Apply the proposition to $N = R_u G$ and to a faithful representation of G . \square

The proposition shows that, for a smooth connected algebraic group G ,

$$R_u G \subset \bigcap_{(V,r) \text{ semisimple}} \text{Ker}(r).$$

In Chapter II, we shall prove that, in characteristic zero, $R_u G$ is equal to the intersection of the kernels of the semisimple representations of G ; thus G is reductive if and only if $\text{Rep}(G)$ is semisimple. This is false in nonzero characteristic.

ASIDE 17.13 In SGA3, XIX, it is recalled that the unipotent radical of a smooth connected affine group scheme over an algebraically closed field is the largest smooth connected normal unipotent subgroup of G (ibid. 1.2). A smooth connected affine group scheme over an algebraically closed field is defined to be reductive if its unipotent radical is trivial (ibid. 1.6). A group scheme G over a scheme S is defined to be reductive if it is smooth and affine over S and each geometric fibre of G over S is a connected reductive group (2.7). When S is the spectrum of field, this definition coincides with our definition.

17c The canonical filtration on an algebraic group

THEOREM 17.14 *Let G be an algebraic group over a field k .*

- (a) *G contains a unique connected normal subgroup G° such that G/G° is an étale algebraic group.*
- (b) *Assume that k is perfect; then G contains a largest smooth subgroup.*
- (c) *Assume that k is perfect and that G is smooth and connected; then G contains a unique smooth connected normal solvable subgroup N such that G/N is a semisimple group.*
- (d) *Assume that k is perfect and that G is smooth connected and solvable; then G contains a unique connected unipotent subgroup N such that G/N is of multiplicative type.*

PROOF. (a) See 13.17.

(b) Because k is perfect, there exists a subgroup G_{red} of G with $\mathcal{O}(G_{\text{red}}) = \mathcal{O}(G)/\mathcal{N}$ (see 6.18). This is reduced, and hence smooth (6.26b). This is the largest smooth subgroup of G because $\mathcal{O}(G_{\text{red}})$ is the largest reduced quotient of $\mathcal{O}(G)$.

(c) The radical RG of G has these properties. Any other smooth connected normal solvable subgroup N of G is contained in RG (by the definition of RG), and if $N \neq RG$ then G/N is not semisimple.

(c) See 16.33. \square

NOTES Perhaps (or perhaps not):

- (a) Explain the connected components for a nonaffine algebraic group, at least in the smooth case. Also discuss things over a ring k .
- (b) Explain the Barsotti-Chevalley-Rosenlicht theorem.
- (c) Explain anti-affine groups.
- (d) Explain what is true when you drop “smooth” and “perfect”, and maybe even allow a base ring.

17d Semisimple groups

An algebraic group G is *simple* if it is connected, noncommutative, and its only proper normal subgroups is 1, and it is *almost-simple* if it is connected, noncommutative, and all its proper normal subgroups are finite. Thus, for $n > 1$, SL_n is almost-simple and $\mathrm{PSL}_n = \mathrm{SL}_n / \mu_n$ is simple. A subgroup N of an algebraic group G that is minimal among the nonfinite normal subgroups of G is either commutative or almost-simple; if G is semisimple, then it is almost-simple.

An algebraic group G is said to be the *almost-direct product* of its algebraic subgroups G_1, \dots, G_r if the map

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G$$

is a surjective homomorphism with finite kernel. In particular, this means that the G_i commute and each G_i is normal in G .

PROPOSITION 17.15 *Let G be a simple algebraic group over an algebraically closed field. Then the group of inner automorphisms of G has finite index in the full group of automorphisms of G .*

Alas, the usual proof of this shows that $\mathrm{Aut}(G) = \mathrm{Inn}(G) \cdot D$ where D is group of automorphisms leaving stable a maximal torus and a Borel subgroup containing the torus, uses the conjugacy of Borel subgroups and the conjugacy of maximal tori in solvable groups, and then shows that $D/D \cap \mathrm{Inn}(G)$ is finite by letting it act on the roots. Unless, we can find a more elementary proof, we shall include a reference to Chapter III for the characteristic zero case, and to Chapter V for the general case.

THEOREM 17.16 *A semisimple algebraic group G has only finitely many almost-simple normal subgroups G_1, \dots, G_r , and the map*

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G \tag{108}$$

is surjective with finite kernel. Each connected normal algebraic subgroup of G is a product of those G_i that it contains, and is centralized by the remaining ones.

In particular, an algebraic group is semisimple if and only if its an almost-direct product of almost-simple algebraic groups. The algebraic groups G_i are called the *almost-simple factors* of G .

PROOF. (This proof needs to be rewritten.) When k has characteristic zero, this is proved in II, 5.31 using Lie algebras. We give the proof for a general field assuming (17.15).

Let G_1, G_2, \dots, G_r be distinct minimal smooth connected normal subgroups of G . For $i \neq j$, (G_i, G_j) is a connected normal subgroup contained in both G_i and G_j (tba), and so it is trivial. Thus, the map

$$\alpha: G_1 \times \cdots \times G_r \rightarrow G$$

is a homomorphism of algebraic groups, and $H \stackrel{\mathrm{def}}{=} G_1 \cdots G_r$ is a connected normal subgroup of G (hence semisimple). The kernel of α is finite, and so

$$\dim G \geq \dim H = \sum \dim G_i.$$

This shows that r is bounded, and we may assume that our family contains them all.

It remains to show that $H = G$. For this we may assume that $k = k^{\text{al}}$. Let $H' = C_G(H)_{\text{red}}^\circ$. Then $C_G(H)(k)$ is the kernel of

$$G(k) \rightarrow \text{Aut}(H),$$

and its image is $\text{Inn}(H)$. As $\text{Inn}(H)$ has finite index in $\text{Aut}(H)$ (see 17.15), it follows that $H \cdot H'$ has finite index in G , and hence equals G because G is connected. As H' is normal in G , it is also semisimple. A minimal smooth connected normal subgroup of H' is a minimal smooth connected normal subgroup of G (because $G = H \cdot H'$ and H centralizes H'). A nontrivial such group would contradict the definition of H — we deduce that $H' = 1$. \square

COROLLARY 17.17 *All nontrivial connected normal subgroups and quotients of a semisimple algebraic group are semisimple.*

PROOF. Any such group is an almost-product of almost-simple algebraic groups. \square

COROLLARY 17.18 *If G is semisimple, then $\mathcal{D}G = G$, i.e., a semisimple group has no commutative quotients.*

PROOF. This is obvious for almost-simple algebraic groups, and hence for any almost-product of such algebraic groups. \square

SIMPLY CONNECTED SEMISIMPLE GROUPS

(This section need to be rewritten.) An semisimple algebraic group G is **simply connected** if every isogeny $G' \rightarrow G$ is an isomorphism.

Let G be a simply connected semisimple group over a field k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. Then $G_{k^{\text{sep}}}$ decomposes into a product

$$G_{k^{\text{sep}}} = G_1 \times \cdots \times G_r \tag{109}$$

of its almost-simple subgroups G_i . The set $\{G_1, \dots, G_r\}$ contains all the almost-simple subgroups of G . When we apply $\sigma \in \Gamma$ to (109), it becomes

$$G_{k^{\text{sep}}} = \sigma G_{k^{\text{sep}}} = \sigma G_1 \times \cdots \times \sigma G_r$$

with $\{\sigma G_1, \dots, \sigma G_r\}$ a permutation of $\{G_1, \dots, G_r\}$. Let H_1, \dots, H_s denote the products of G_i in the different orbits of Γ . Then $\sigma H_i = H_i$, and so H_i is defined over k (I, 4.13), and

$$G = H_1 \times \cdots \times H_s$$

is a decomposition of G into a product of its almost-simple subgroups.

Now suppose that G itself is almost-simple, so that Γ acts transitively on the G_i in (109). Let

$$\Delta = \{\sigma \in \Gamma \mid \sigma G_1 = G_1\},$$

and let $K = (k^{\text{sep}})^\Delta$.

PROPOSITION 17.19 We have $G \simeq (G_1)_{K/k}$ (restriction of base field).

PROOF. We can rewrite (109) as

$$G_{k^{\text{sep}}} = \prod \sigma G_{1k^{\text{sep}}}$$

where σ runs over a set of cosets for Δ in Γ . On comparing this with (4.8), we see that there is a canonical isomorphism

$$G_{k^{\text{sep}}} \simeq ((G_1)_{K/k})_{k^{\text{sep}}}.$$

In particular, it commutes with the action of Γ , and so is defined over k (see 4.13). \square

The group G_1 over K is *geometrically almost-simple*, i.e., it is almost-simple and remains almost-simple over K^{al} .

17e Reductive groups

THEOREM 17.20 If G is reductive, then the derived group $\mathcal{D}G$ of G is semisimple, the connected centre $Z(G)^\circ$ of G is a torus, and $Z(G) \cap \mathcal{D}G$ is the (finite) centre of $\mathcal{D}G$; moreover,

$$G = Z(G)^\circ \cdot \mathcal{D}G.$$

PROOF. It suffices to prove this with $k = k^{\text{al}}$. By definition, $(RG)_u = 0$, and so (16.33) shows that RG is a torus T . Rigidity (14.32) implies that the action of G on RG by inner automorphisms is trivial, and so $RG \subset Z(G)^\circ$. Since the reverse inclusion always holds, this shows that

$$R(G) = Z(G)^\circ = \text{torus}.$$

We next show that $Z(G)^\circ \cap \mathcal{D}G$ is finite. Choose an embedding $G \hookrightarrow \text{GL}_V$, and write V as a direct sum

$$V = V_1 \oplus \cdots \oplus V_r$$

of eigenspaces for the action of $Z(G)^\circ$ (see 14.15). When we choose bases for the V_i , then $Z(G)^\circ(k)$ consists of the matrices

$$\begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_r \end{pmatrix}$$

with each A_i nonzero and scalar,⁶¹ and so its centralizer in GL_V consists of the matrices of this shape with the A_i arbitrary. Since $(\mathcal{D}G)(k)$ consists of commutators (16.22), it consists of such matrices with determinant 1. As $\text{SL}(V_i)$ contains only finitely many scalar matrices, this shows that $Z(G)^\circ \cap \mathcal{D}G$ is finite.

Note that $Z(G)^\circ \cdot \mathcal{D}G$ is a normal algebraic subgroup of G such that $G/(Z(G)^\circ \cdot \mathcal{D}G)$ is commutative (being a quotient of $G/\mathcal{D}G$) and semisimple (being a quotient of $G/R(G)$). Hence⁶²

$$G = Z(G)^\circ \cdot G^{\text{der}}.$$

⁶¹That is, of the form $\text{diag}(a, \dots, a)$ with $a \neq 0$.

⁶²Because $G = \mathcal{D}G$ if G is semisimple. In other words, a semisimple group has no commutative quotients. At the moment this is only proved at the end of II, §4.

Therefore

$$G^{\text{der}} \rightarrow G/R(G)$$

is surjective with finite kernel. As $G/R(G)$ is semisimple, so also is G^{der} .

Certainly $Z(G) \cap G^{\text{der}} \subset Z(G^{\text{der}})$, but, because $G = Z(G)^\circ \cdot G^{\text{der}}$ and $Z(G)^\circ$ is commutative, $Z(G^{\text{der}}) \subset Z(G)$. \square

REMARK 17.21 From a reductive group G , we obtain a semisimple group G' (its derived group), a group Z of multiplicative type (its centre), and a homomorphism $\varphi: Z(G') \rightarrow Z$. Moreover, G can be recovered from (G', Z, φ) : the map

$$z \mapsto (\varphi(z)^{-1}, z): Z(G') \rightarrow Z \times G'$$

is an isomorphism from $Z(G')$ onto a central subgroup of $Z \times G'$, and the quotient is G . Clearly, every reductive group arises from such a triple (G', Z, φ) (and G' can even be chosen to be simply connected).

17f Pseudoreductive groups

We briefly summarize Conrad, Gabber, and Prasad 2010.

17.22 Let k be a separably closed field of characteristic p , and let $G = (\mathbb{G}_m)_{k'/k}$ where k' is an extension of k of degree p (necessarily purely inseparable). Then G is a commutative smooth connected algebraic group over k . The canonical map $\mathbb{G}_m \rightarrow G$ realizes \mathbb{G}_m as the largest subgroup of G of multiplicative type, and the quotient G/\mathbb{G}_m is unipotent. Over k^{al} , G decomposes into $(\mathbb{G}_m)_{k^{\text{al}}} \times (G/\mathbb{G}_m)_{k^{\text{al}}}$ (see 16.12), and so G is not reductive. However, G contains no unipotent subgroup because $G(k) = k'^{\times}$, which has no p -torsion. Therefore G is pseudo-reductive.

17.23 Let k' be a finite field extension of k , and let G be a reductive group over k' . If k' is separable over k , then $(G)_{k'/k}$ is reductive, but otherwise it is only pseudoreductive.

17.24 Let C be a commutative connected algebraic group over k . If C is reductive, then C is a torus, and the tori are classified by the continuous actions of $\text{Gal}(k^{\text{sep}}/k)$ on free abelian groups of finite rank. By contrast, “it seems to be an impossible task to describe general commutative pseudo-reductive groups over imperfect fields” (Conrad et al. 2010, p. xv).

17.25 Let k_1, \dots, k_n be finite field extensions of k . For each i , let G_i be a reductive group over k_i , and let T_i be a maximal torus in G_i . Define algebraic groups

$$G \leftrightarrow T \twoheadrightarrow \bar{T}$$

by

$$\begin{aligned} G &= \prod_i (G_i)_{k_i/k} \\ T &= \prod_i (T_i)_{k_i/k} \\ \bar{T} &= \prod_i (T_i/Z(G_i))_{k_i/k}. \end{aligned}$$

Let $\phi: T \rightarrow C$ be a homomorphism of commutative pseudoreductive groups that factors through the quotient map $T \rightarrow \bar{T}$:

$$T \xrightarrow{\phi} C \xrightarrow{\psi} \bar{T}.$$

Then ψ defines an action of C on G by conjugation, and so we can form the semi-direct product

$$G \rtimes C.$$

The map

$$t \mapsto (t^{-1}, \phi(t)): T \rightarrow G \rtimes C$$

is an isomorphism from T onto a central subgroup of $G \rtimes C$, and the quotient $(G \rtimes C)/T$ is a pseudoreductive group over k . The main theorem (5.1.1) of Conrad et al. 2010 says that, except possibly when k has characteristic 2 or 3, every pseudoreductive group over k arises by such a construction (the theorem also treats the exceptional cases).

17.26 The maximal tori in reductive groups are their own centralizers. Any pseudoreductive group with this property is reductive (except possibly in characteristic 2; Conrad et al. 2010, 11.1.1).

17.27 If G is reductive, then $G = \mathcal{D}G \cdot Z(G)^\circ$ where $\mathcal{D}G$ is the derived group of G and $Z(G)^\circ$ is the largest central connected reductive subgroup of G . This statement becomes false with “pseudoreductive” for “reductive” (Conrad et al. 2010, 11.2.1).

17.28 For a reductive group G , the map

$$RG = Z(G)^\circ \rightarrow G/\mathcal{D}G$$

is an isogeny, and G is semisimple if and only if one (hence both) groups are trivial. For a pseudoreductive group, the condition $RG = 1$ does not imply that $G = \mathcal{D}G$. Conrad et al. 2010, 11.2.2, instead adopt the definition: an algebraic group G is *pseudo-semisimple* if it is pseudoreductive and $G = \mathcal{D}G$. The derived group of a pseudoreductive group is pseudo-semisimple (ibid. 1.2.6, 11.2.3).

17.29 A reductive group G over any field k is unirational, and so $G(k)$ is dense in G if k is infinite. This fails for pseudoreductive groups: over every nonperfect field k there exists a commutative pseudoreductive group that is not unirational; when k is a nonperfect rational function field $k_0(T)$, such a group G can be chosen so that $G(k)$ is not dense in G (Conrad et al. 2010, 11.3.1).

17g Properties of G versus those of $\text{Rep}_k(G)$

We summarize.

17.30 An affine group G is finite if and only if there exists a representation (r, V) such that every representation of G is a subquotient of V^n for some $n \geq 0$ (12.19).

17.31 An affine group G is strongly connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\text{Rep}(G)$ of subquotients of V^n , $n \geq 0$, is not stable under \otimes (apply 17.30). In characteristic zero, a group is strongly connected if and only if it is connected.

17.32 An affine group G is unipotent if and only if every simple representation is trivial (this is essentially the definition 15.3).

17.33 An affine group G is trigonalizable if and only if every simple representation has dimension 1 (this is the definition 16.1).

17.34 An affine group G is algebraic if and only if $\text{Rep}(G) = \langle V \rangle^{\otimes}$ for some representation (V, r) (8.44).

17.35 Let G be a smooth connected algebraic group. If $\text{Rep}(G)$ is semisimple, then G is reductive (17.12), and the converse is true in characteristic zero (II, 6.14).

18 Example: the spin groups

Let ϕ be a nondegenerate bilinear form on a k -vector space V . The special orthogonal group $\text{SO}(\phi)$ is connected and almost-simple, and it has a 2-fold covering $\text{Spin}(\phi)$ which we now construct.

Throughout this section, k is a field not of characteristic 2 and “ k -algebra” means “associative (not necessarily commutative) k -algebra containing k in its centre”. For example, the $n \times n$ matrices with entries in k become such a k -algebra $M_n(k)$ once we identify an element c of k with the scalar matrix cI_n .

NOTES This section is OK as far as it goes, but it needs to be revised and completed. Also, should explain in more detail that not all representations of \mathfrak{so}_n come from SO_n , but they do from some semisimple algebraic group.

18a Quadratic spaces

Let k be a field not of characteristic 2, and let V be a finite-dimensional k -vector space. A **quadratic form** on V is a mapping

$$q: V \rightarrow k$$

such that $q(x) = \phi_q(x, x)$ for some symmetric bilinear form $\phi_q: V \times V \rightarrow k$. Note that

$$q(x + y) = q(x) + q(y) + 2\phi_q(x, y), \quad (110)$$

and so ϕ_q is uniquely determined by q . A **quadratic space** is a pair (V, q) consisting of a finite-dimensional vector space and a quadratic form q . Often I'll write ϕ (rather than ϕ_q) for the associated symmetric bilinear form and denote (V, q) by (V, ϕ_q) or (V, ϕ) . A nonzero vector x in V is **isotropic** if $q(x) = 0$ and **anisotropic** if $q(x) \neq 0$. Note that q is zero (i.e., $q(V) = 0$) if and only if ϕ is zero (i.e., $\phi(V, V) = 0$).

The **discriminant** of (V, q) is the determinant of the matrix $(\phi(e_i, e_j))$ where e_1, \dots, e_n is a basis of V . The choice of a different basis multiplies $\det(\phi(e_i, e_j))$ by a nonzero square, and so the discriminant is an element of $k/k^{\times 2}$.

Let (V_1, q_1) and (V_2, q_2) be quadratic spaces. An **isometry** is an injective k -linear map $\sigma: V_1 \rightarrow V_2$ such that $q_2(\sigma x) = q_1(x)$ for all $x \in V$ (equivalently, $\phi(\sigma x, \sigma y) = \phi(x, y)$ for all $x, y \in V$). By $(V_1, q_1) \oplus (V_2, q_2)$ we mean the quadratic space (V, q) with

$$V = V_1 \oplus V_2$$

$$q(x_1 + x_2) = q(x_1) + q(x_2), \quad x_1 \in V_1, \quad x_2 \in V_2.$$

Let (V, q) be quadratic space. A basis e_1, \dots, e_n for V is said to be **orthogonal** if $\phi(e_i, e_j) = 0$ for all $i \neq j$.

PROPOSITION 18.1 *Every quadratic space has an orthogonal basis (and so is an orthogonal sum of quadratic spaces of dimension 1).*

PROOF. If $q(V) = 0$, then every basis is orthogonal. Otherwise, let $e \in V$ be such that $q(e) \neq 0$, and extend it to a basis e, e_2, \dots, e_n for V . Then

$$e, e_2 - \frac{\phi(e, e_2)}{q(e)}e, \dots, e_n - \frac{\phi(e, e_n)}{q(e)}e$$

is again a basis for V , and the last $n - 1$ vectors span a subspace W for which $\phi(e, W) = 0$. Apply induction to W . \square

An orthogonal basis defines an isometry $(V, q) \xrightarrow{\approx} (k^n, q')$, where

$$q'(x_1, \dots, x_n) = c_1 x_1^2 + \dots + c_n x_n^2, \quad c_i = q(e_i) \in k.$$

If every element of k is a square, for example, if k is algebraically closed, we can even scale the e_i so that each c_i is 0 or 1.

18b Theorems of Witt and Cartan-Dieudonné

A quadratic space (V, q) is said to be **regular**⁶³ (or **nondegenerate**,...) if for all $x \neq 0$ in V , there exists a y such that $\phi(x, y) \neq 0$. Otherwise, it is **singular**. Also, (V, q) is

- ◇ **isotropic** if it contains an isotropic vector, i.e., if $q(x) = 0$ for some $x \neq 0$,
- ◇ **totally isotropic** if every nonzero vector is isotropic, i.e., if $q(x) = 0$ for all x , and
- ◇ **anisotropic** if it is not isotropic, i.e., if $q(x) = 0$ implies $x = 0$.

Let (V, q) be a regular quadratic space. Then for any nonzero $a \in V$,

$$\langle a \rangle^\perp \stackrel{\text{def}}{=} \{x \in V \mid \phi(a, x) = 0\}$$

is a hyperplane in V (i.e., a subspace of dimension $\dim V - 1$). For an anisotropic $a \in V$, the **reflection in the hyperplane orthogonal** to a is defined to be

$$R_a(x) = x - \frac{2\phi(a, x)}{q(a)}a.$$

Then R_a sends a to $-a$ and fixes the elements of $W \stackrel{\text{def}}{=} \langle a \rangle^\perp$. Moreover,

$$q(R_a(x)) = q(x) - 2\frac{2\phi(a, x)}{q(a)}\phi(a, x) + \frac{4\phi(a, x)^2}{q(a)^2}q(a) = q(x),$$

and so R_a is an isometry. Finally, relative to a basis a, e_2, \dots, e_n with e_2, \dots, e_n a basis for W , its matrix is $\text{diag}(-1, 1, \dots, 1)$, and so $\det(R_a) = -1$.

⁶³With the notations of the last paragraph, (V, q) is regular if $c_1 \dots c_n \neq 0$.

THEOREM 18.2 *Let (V, q) be a regular quadratic space, and let σ be an isometry from a subspace W of V into V . Then there exists a composite of reflections $V \rightarrow V$ extending σ .*

PROOF. Suppose first that $W = \langle x \rangle$ with x anisotropic, and let $\sigma x = y$. Geometry in the plane suggests that we should reflect in the line $x + y$. In the plane this is the line orthogonal to $x - y$, and, if $x - y$ is anisotropic, then

$$R_{x-y}(x) = y$$

as required. To see this, note that

$$\phi(x - y, x) = -\phi(x - y, y)$$

because $q(x) = q(y)$, and so

$$\begin{aligned}\phi(x - y, x + y) &= 0 \\ \phi(x - y, x - y) &= 2\phi(x - y, x);\end{aligned}$$

hence

$$R_{x-y}(x) = x - \frac{2\phi(x - y, x)}{\phi(x - y, x - y)}(x - y) = x - (x - y) = y.$$

If $x - y$ is isotropic, then

$$4q(x) = q(x + y) + q(x - y) = q(x + y)$$

and so $x + y$ is anisotropic. In this case,

$$R_{x+y} \circ R_x(x) = R_{x-(-y)}(-x) = y.$$

We now proceed⁶⁴ by induction on

$$m(W) = \dim W + 2 \dim(W \cap W^\perp).$$

CASE W NOT TOTALLY ISOTROPIC: In this case, the argument in the proof of (18.1) shows that there exists an anisotropic vector $x \in W$, and we let $W' = \langle x \rangle^\perp \cap W$. Then, for $w \in W$, $w - \frac{\phi(w, x)}{q(x)}x \in W'$, and so $W = \langle x \rangle \oplus W'$ (orthogonal decomposition). As $m(W') = m(W) - 1$, we can apply induction to obtain a composite Σ' of reflections such that $\Sigma'|W' = \sigma|W'$. From the definition of W' , we see that $x \in W'^\perp$; moreover, for any $w' \in W'$,

$$\phi(\Sigma'^{-1}\sigma x, w') = \phi(x, \sigma^{-1}\Sigma'w') = \phi(x, w') = 0,$$

and so $y \stackrel{\text{def}}{=} \Sigma'^{-1}\sigma x \in W'^\perp$. By the argument in the first paragraph, there exist reflections (one or two) of the form R_z , $z \in W'^\perp$, whose composite Σ'' maps x to y . Because Σ'' acts as the identity on W' , $\Sigma' \circ \Sigma''$ is the map sought:

$$(\Sigma' \circ \Sigma'')(cx + w') = \Sigma'(cy + w') = c\sigma x + \sigma w'.$$

CASE W TOTALLY ISOTROPIC: Let $V^\vee = \text{Hom}_{k\text{-lin}}(V, k)$ be the dual vector space, and consider the surjective map

$$\alpha: V \xrightarrow{x \mapsto \phi(x, -)} V^\vee \xrightarrow{f \mapsto f|W} W^\vee$$

⁶⁴Following Scharlau 1985, Chapter 1, 5.5.

(so $x \in V$ is sent to the map $y \mapsto \phi(x, y)$ on W). Let W' be a subspace of V mapped isomorphically onto W^\vee . Then $W \cap W' = \{0\}$ and we claim that $W + W'$ is a regular subspace of V . Indeed, if $x + x' \in W + W'$ with $x' \neq 0$, then there exists a $y \in W$ such that

$$0 \neq \phi(x', y) = \phi(x + x', y);$$

if $x \neq 0$, there exists a $y \in W'$ such that $\phi(x, y) \neq 0$.

Endow $W \oplus W^\vee$ with the symmetric bilinear form

$$(x, f), (x', f') \mapsto f(x') + f'(x).$$

Relative to this bilinear form, the map

$$x + x' \mapsto (x, \alpha(x')): W + W' \rightarrow W \oplus W^\vee \quad (111)$$

is an isometry.

The same argument applied to σW gives a subspace W'' and an isometry

$$x + x'' \mapsto (x, \dots): \sigma W + W'' \rightarrow \sigma W \oplus (\sigma W)^\vee. \quad (112)$$

Now the map

$$W + W' \xrightarrow{(111)} W \oplus W^\vee \xrightarrow{\sigma \oplus \sigma^{\vee-1}} \sigma W \oplus (\sigma W)^\vee \xrightarrow{(112)} \sigma W + W'' \subset V$$

is an isometry extending σ . As

$$m(W \oplus W') = 2 \dim W < 3 \dim W = m(W)$$

we can apply induction to complete the proof. \square

COROLLARY 18.3 *Every isometry of (V, q) is a composite of reflections.*

PROOF. This is the special case of the theorem in which $W = V$. \square

COROLLARY 18.4 (WITT CANCELLATION) *Suppose (V, q) has orthogonal decompositions*

$$(V, q) = (V_1, q_1) \oplus (V_2, q_2) = (V'_1, q'_1) \oplus (V'_2, q'_2)$$

with (V_1, q_1) and (V'_1, q'_1) regular and isometric. Then (V_2, q_2) and (V'_2, q'_2) are isometric.

PROOF. Extend an isometry $V_1 \rightarrow V'_1 \subset V$ to an isometry of V . It will map $V_2 = V_1^\perp$ isometrically onto $V'_2 = V_1'^\perp$. \square

COROLLARY 18.5 *All maximal totally isotropic subspace of (V, q) have the same dimension.*

PROOF. Let W_1 and W_2 be maximal totally isotropic subspaces of V , and suppose that $\dim W_1 \leq \dim W_2$. Then there exists an injective linear map $\sigma: W_1 \rightarrow W_2 \subset V$, which is automatically an isometry. Therefore, by Theorem 18.2 it extends to an isometry $\sigma: V \rightarrow V$. Now $\sigma^{-1}W_2$ is a totally isotropic subspace of V containing W_1 . Because W_1 is maximal, $W_1 = \sigma^{-1}W_2$, and so $\dim W_1 = \dim \sigma^{-1}W_2 = \dim W_2$. \square

REMARK 18.6 In the situation of Theorem 18.2, Witt's theorem says simply that there exists an isometry extending σ to V (not necessarily a composite of reflections), and the Cartan-Dieudonné theorem says that every isometry is a composite of at most $\dim V$ reflections. When V is anisotropic, the proof of Theorem 18.2 shows this, but the general case is considerably more difficult — see Artin 1957.

DEFINITION 18.7 The (*Witt index*) of a regular quadratic space (V, q) is the maximum dimension of a totally isotropic subspace of V .

DEFINITION 18.8 A quadratic space (V, q) is a *hyperbolic plane* if it satisfies one of the following equivalent conditions:

- (a) (V, q) is regular and isotropic of dimension 2;
- (b) for some basis of V , the matrix of the form is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;
- (c) V has dimension 2 and the discriminant of q is -1 (modulo squares).

THEOREM 18.9 (WITT DECOMPOSITION) A regular quadratic space (V, q) with Witt index m has an orthogonal decomposition

$$V = H_1 \oplus \cdots \oplus H_m \oplus V_a \quad (113)$$

with the H_i hyperbolic planes and V_a anisotropic; moreover, V_a is uniquely determined up to isometry.

PROOF. Let W be a maximal isotropic subspace of V , and let e_1, \dots, e_m be a basis for W . One easily extends the basis to a linearly independent set $e_1, \dots, e_m, e_{m+1}, \dots, e_{2m}$ such that $\phi(e_i, e_{m+j}) = \delta_{ij}$ (Kronecker delta) and $q(e_{m+i}) = 0$ for $i \leq m$. Then V decomposes as (113) with⁶⁵ $H_i = \langle e_i, e_{m+i} \rangle$ and $V_a = \langle e_1, \dots, e_{2m} \rangle^\perp$. The uniqueness of V_a follows from the Witt cancellation theorem (18.4). \square

18c The orthogonal group

Let (V, q) be a regular quadratic space. Define $O(q)$ to be the group of isometries of (V, q) . Relative to a basis for V , $O(q)$ consists of the *automorphs* of the matrix $M = (\phi(e_i, e_j))$, i.e., the matrices T such that

$$T^t \cdot M \cdot T = M.$$

Thus, $O(q)$ is an algebraic subgroup of GL_V (see 3.9), called the *orthogonal group* of q (it is also called the orthogonal group of ϕ , and denoted $O(\phi)$).

Let $T \in O(q)$. As $\det M \neq 0$, $\det(T)^2 = 1$, and so $\det(T) = \pm 1$. The subgroup of isometries with $\det = +1$ is an algebraic subgroup of SL_V , called the *special orthogonal group* $SO(q)$.

⁶⁵We often write $\langle S \rangle$ for the k -space spanned by a subset S of a vector space V .

18d Super algebras

Recall (§2e) that a **superalgebra** (or $\mathbb{Z}/2\mathbb{Z}$ -**graded algebra**) over k is k -algebra C together with a decomposition $C = C_0 \oplus C_1$ of C as a k -vector space such that

$$k \subset C_0, \quad C_0 C_0 \subset C_0, \quad C_0 C_1 \subset C_1, \quad C_1 C_0 \subset C_1, \quad C_1 C_1 \subset C_0.$$

Note that C_0 is a k -subalgebra of C . A **homomorphism** of super k -algebras is a homomorphism $\varphi: C \rightarrow D$ of algebras such that $\varphi(C_i) \subset D_i$ for $i = 0, 1$.

EXAMPLE 18.10 Let $c_1, \dots, c_n \in k$. Define $C(c_1, \dots, c_n)$ to be the k -algebra with generators e_1, \dots, e_n and relations

$$e_i^2 = c_i, \quad e_j e_i = -e_i e_j \quad (i \neq j).$$

As a k -vector space, $C(c_1, \dots, c_n)$ has basis $\{e_1^{i_1} \dots e_n^{i_n} \mid i_j \in \{0, 1\}\}$, and so has dimension 2^n . When we set C_0 and C_1 equal to the subspaces

$$\begin{aligned} C_0 &= \langle e_1^{i_1} \dots e_n^{i_n} \mid i_1 + \dots + i_n \text{ even} \rangle \\ C_1 &= \langle e_1^{i_1} \dots e_n^{i_n} \mid i_1 + \dots + i_n \text{ odd} \rangle, \end{aligned}$$

of $C(c_1, \dots, c_n)$, then it becomes a superalgebra.

Let $C = C_0 \oplus C_1$ and $D = D_0 \oplus D_1$ be two super k -algebras. The **super tensor product** of C and D , $C \hat{\otimes} D$, is defined to be the k -vector space $C \otimes_k D$ endowed with the superalgebra structure

$$\begin{aligned} (C \hat{\otimes} D)_0 &= (C_0 \otimes D_0) \oplus (C_1 \otimes D_1) \\ (C \hat{\otimes} D)_1 &= (C_0 \otimes D_1) \oplus (C_1 \otimes D_0) \\ (c_i \otimes d_j)(c'_k \otimes d'_l) &= (-1)^{jk} (c_i c'_k \otimes d_j d'_l) \quad c_i \in C_i, d_j \in D_j \text{ etc..} \end{aligned}$$

The maps

$$\begin{aligned} i_C: C &\rightarrow C \hat{\otimes} D, \quad c \mapsto c \otimes 1 \\ i_D: D &\rightarrow C \hat{\otimes} D, \quad d \mapsto 1 \otimes d \end{aligned}$$

have the following universal property: for any homomorphisms of k -superalgebras

$$f: C \rightarrow T, \quad g: D \rightarrow T$$

whose images anticommute in the sense that

$$f(c_i)g(d_j) = (-1)^{ij} g(d_j)f(c_i), \quad c_i \in C_i, d_j \in D_j,$$

there is a unique superalgebra homomorphism $h: C \hat{\otimes} D \rightarrow T$ such that $f = h \circ i_C$, $g = h \circ i_D$.

EXAMPLE 18.11 As a k -vector space, $C(c_1) \hat{\otimes} C(c_2)$ has basis $1 \otimes 1, e \otimes 1, 1 \otimes e, e \otimes e$, and

$$\begin{aligned} (e \otimes 1)^2 &= e^2 \otimes 1 = c_1 \cdot 1 \otimes 1 \\ (1 \otimes e)^2 &= 1 \otimes e^2 = c_2 \cdot 1 \otimes 1 \\ (e \otimes 1)(1 \otimes e) &= e \otimes e = -(1 \otimes e)(e \otimes 1). \end{aligned}$$

Therefore,

$$\begin{aligned} C(c_1) \hat{\otimes} C(c_2) &\simeq C(c_1, c_2) \\ e \otimes 1 &\leftrightarrow e_1 \\ 1 \otimes e &\leftrightarrow e_2. \end{aligned}$$

Similarly,

$$C(c_1, \dots, c_{i-1}) \hat{\otimes} C(c_i) \simeq C(c_1, \dots, c_i),$$

and so, by induction,

$$C(c_1) \hat{\otimes} \dots \hat{\otimes} C(c_n) \simeq C(c_1, \dots, c_n).$$

EXAMPLE 18.12 Every k -algebra A can be regarded as a k -superalgebra by setting $A_0 = A$ and $A_1 = 0$. If A, B are both k -algebras, then $A \otimes_k B = A \hat{\otimes}_k B$.

EXAMPLE 18.13 Let X be a manifold. Then $H(X) \stackrel{\text{def}}{=} \bigoplus_i H^i(X, \mathbb{R})$ becomes an \mathbb{R} -algebra under cup-product, and even a superalgebra with $H(X)_0 = \bigoplus_i H^{2i}(X, \mathbb{R})$ and $H(X)_1 = \bigoplus_i H^{2i+1}(X, \mathbb{R})$. If Y is a second manifold, the Künneth formula says that

$$H(X \times Y) = H(X) \hat{\otimes} H(Y)$$

(super tensor product).

18e Brief review of the tensor algebra

Let V be a k -vector space. The *tensor algebra* of V is $T(V) = \bigoplus_{n \geq 0} V^{\otimes n}$, where

$$\begin{aligned} V^{\otimes 0} &= k, \\ V^{\otimes 1} &= V, \\ V^{\otimes n} &= V \otimes \dots \otimes V \text{ (} n \text{ copies of } V \text{)} \end{aligned}$$

with the algebra structure defined by juxtaposition, i.e.,

$$(v_1 \otimes \dots \otimes v_m) \cdot (v_{m+1} \otimes \dots \otimes v_{m+n}) = v_1 \otimes \dots \otimes v_{m+n}.$$

It is a k -algebra.

If V has a basis e_1, \dots, e_m , then $T(V)$ is the k -algebra of noncommuting polynomials in e_1, \dots, e_m .

There is a k -linear map $V \rightarrow T(V)$, namely, $V = V^{\otimes 1} \hookrightarrow \bigoplus_{n \geq 0} V^{\otimes n}$, and any other k -linear map from V to a k -algebra R extends uniquely to a k -algebra homomorphism $T(V) \rightarrow R$.

18f The Clifford algebra

Let (V, q) be a quadratic space, and let ϕ be the corresponding bilinear form on V .

DEFINITION 18.14 The *Clifford algebra* $C(V, q)$ is the quotient of the tensor algebra $T(V)$ of V by the two-sided ideal $I(q)$ generated by the elements $x \otimes x - q(x)$ ($x \in V$).

Let $\rho: V \rightarrow C(V, q)$ be the composite of the canonical map $V \rightarrow T(V)$ and the quotient map $T(V) \rightarrow C(V, q)$. Then ρ is k -linear, and⁶⁶

$$\rho(x)^2 = q(x), \text{ all } x \in V. \quad (114)$$

Note that if x is anisotropic in V , then $\rho(x)$ is invertible in $C(V, q)$, because (114) shows that

$$\rho(x) \cdot \frac{\rho(x)}{q(x)} = 1.$$

EXAMPLE 18.15 If V is one-dimensional with basis e and $q(e) = c$, then $T(V)$ is a polynomial algebra in one symbol e , $T(V) = k[e]$, and $I(q) = (e^2 - c)$. Therefore, $C(V, q) \approx C(c)$.

EXAMPLE 18.16 If $q = 0$, then $C(V, q)$ is the exterior algebra on V , i.e., $C(V, q)$ is the quotient of $T(V)$ by the ideal generated by all squares x^2 , $x \in V$. In $C(V, q)$,

$$0 = (\rho(x) + \rho(y))^2 = \rho(x)^2 + \rho(x)\rho(y) + \rho(y)\rho(x) + \rho(y)^2 = \rho(x)\rho(y) + \rho(y)\rho(x)$$

and so $\rho(x)\rho(y) = -\rho(y)\rho(x)$.

PROPOSITION 18.17 Let r be a k -linear map from V to a k -algebra D such that $r(x)^2 = q(x)$. Then there exists a unique homomorphism of k -algebras $\bar{r}: C(V, q) \rightarrow D$ such that $\bar{r} \circ \rho = r$:

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C(V, q) \\ & \searrow r & \downarrow \bar{r} \\ & & D. \end{array}$$

PROOF. According to the universal property of the tensor algebra, r extends uniquely to a homomorphism of k -algebras $r': T(V) \rightarrow D$, namely,

$$r'(x_1 \otimes \cdots \otimes x_n) = r(x_1) \cdots r(x_n).$$

As

$$r'(x \otimes x - q(x)) = r(x)^2 - q(x) = 0,$$

r' factors uniquely through $C(V, q)$. □

As usual, $(C(V, q), \rho)$ is uniquely determined up to a unique isomorphism by the universal property in the proposition.

⁶⁶For a k -algebra R , we are regarding k as a subfield of R . When one regards a k -algebra R as a ring with a $k \rightarrow R$, it is necessary to write (114) as

$$\rho(x)^2 = q(x) \cdot 1_{C(V, q)}.$$

THE MAP $C(c_1, \dots, c_n) \rightarrow C(V, q)$

Because ρ is linear,

$$\rho(x + y)^2 = (\rho(x) + \rho(y))^2 = \rho(x)^2 + \rho(x)\rho(y) + \rho(y)\rho(x) + \rho(y)^2.$$

On comparing this with

$$\rho(x + y)^2 \stackrel{(114)}{=} q(x + y) = q(x) + q(y) + 2\phi(x, y),$$

we find that

$$\rho(x)\rho(y) + \rho(y)\rho(x) = 2\phi(x, y). \quad (115)$$

In particular, if f_1, \dots, f_n is an orthogonal basis for V , then

$$\rho(f_i)^2 = q(f_i), \quad \rho(f_j)\rho(f_i) = -\rho(f_i)\rho(f_j) \quad (i \neq j).$$

Let $c_i = q(f_i)$. Then there exists a surjective homomorphism

$$e_i \mapsto \rho(f_i): C(c_1, \dots, c_n) \rightarrow C(V, \phi). \quad (116)$$

THE GRADATION (SUPERSTRUCTURE) ON THE CLIFFORD ALGEBRA

Decompose

$$\begin{aligned} T(V) &= T(V)_0 \oplus T(V)_1 \\ T(V)_0 &= \bigoplus_{m \text{ even}} V^{\otimes m} \\ T(V)_1 &= \bigoplus_{m \text{ odd}} V^{\otimes m}. \end{aligned}$$

As $I(q)$ is generated by elements of $T(V)_0$,

$$I(q) = (I(q) \cap T(V)_0) \oplus (I(q) \cap T(V)_1),$$

and so

$$C(V, q) = C_0 \oplus C_1 \quad \text{with} \quad C_i = T(V)_i / (I(q) \cap T(V)_i).$$

Clearly this decomposition makes $C(V, q)$ into a super algebra.

In more down-to-earth terms, C_0 is spanned by products of an even number of vectors from V , and C_1 is spanned by products of an odd number of vectors.

THE BEHAVIOUR OF THE CLIFFORD ALGEBRA WITH RESPECT TO DIRECT SUMS

Suppose

$$(V, q) = (V_1, q_1) \oplus (V_2, q_2).$$

Then the k -linear map

$$\begin{aligned} V &= V_1 \oplus V_2 & \xrightarrow{r} & C(V_1, q_1) \hat{\otimes} C(V_2, q_2) \\ x &= (x_1, x_2) & \mapsto & \rho_1(x_1) \otimes 1 + 1 \otimes \rho_2(x_2). \end{aligned}$$

has the property that

$$\begin{aligned} r(x)^2 &= (\rho_1(x_1) \otimes 1 + 1 \otimes \rho_2(x_2))^2 \\ &= (q(x_1) + q(x_2))(1 \otimes 1) \\ &= q(x), \end{aligned}$$

because

$$(\rho_1(x_1) \otimes 1)(1 \otimes \rho_2(x_2)) = \rho_1(x_1) \otimes \rho_2(x_2) = -(1 \otimes \rho_2(x_2))(\rho_1(x_1) \otimes 1).$$

Therefore, it factors uniquely through $C(V, q)$:

$$C(V, q) \rightarrow C(V_1, q_1) \hat{\otimes} C(V_2, q_2). \quad (117)$$

EXPLICIT DESCRIPTION OF THE CLIFFORD ALGEBRA

THEOREM 18.18 *Let (V, q) a quadratic space of dimension n .*

- (a) *For every orthogonal basis for (V, q) , the homomorphism (116)*

$$C(c_1, \dots, c_n) \rightarrow C(V, q)$$

is an isomorphism.

- (b) *For every orthogonal decomposition $(V, q) = (V_1, q_1) \oplus (V_2, q_2)$, the homomorphism (117)*

$$C(V, q) \rightarrow C(V_1, q_1) \hat{\otimes} C(V_2, q_2)$$

is an isomorphism.

- (c) *The dimension of $C(V, q)$ as a k -vector space is 2^n .*

PROOF. If $n = 1$, all three statements are clear from (18.15). Assume inductively that they are true for $\dim(V) < n$. Certainly, we can decompose $(V, q) = (V_1, q_1) \oplus (V_2, q_2)$ in such a way that $\dim(V_i) < n$. The homomorphism (117) is surjective because its image contains $\rho_1(V_1) \otimes 1$ and $1 \otimes \rho_2(V_2)$ which generate $C(V_1, q_1) \hat{\otimes} C(V_2, q_2)$, and so

$$\dim(C(V, q)) \geq 2^{\dim(V_1)} 2^{\dim(V_2)} = 2^n.$$

From an orthogonal basis for (V, q) , we get a surjective homomorphism (116). Therefore,

$$\dim(C(V, q)) \leq 2^n.$$

It follows that $\dim(C(V, q)) = 2^n$. By comparing dimensions, we deduce that the homomorphisms (116) and (117) are isomorphisms. \square

COROLLARY 18.19 *The map $\rho: V \rightarrow C(V, q)$ is injective.*

From now on, we shall regard V as a subset of $C(V, q)$ (i.e., we shall omit ρ).

REMARK 18.20 Let L be a field containing k . Then ϕ extends uniquely to an L -bilinear form

$$\phi': V' \times V' \rightarrow L, \quad V' = L \otimes_k V,$$

and

$$C(V', q') \simeq L \otimes_k C(V, q)$$

where q' is quadratic form defined by ϕ' .

THE CENTRE OF THE CLIFFORD ALGEBRA

Assume that (V, q) is regular, and that $n = \dim V > 0$. Let e_1, \dots, e_n be an orthogonal basis for (V, q) , and let $q(e_i) = c_i$. Let

$$\Delta = (-1)^{\frac{n(n-1)}{2}} c_1 \cdots c_n = (-1)^{\frac{n(n-1)}{2}} \det(\phi(e_i, e_j)).$$

We saw in (18.18) that

$$C(c_1, \dots, c_n) \simeq C(V, q).$$

Note that, in $C(c_1, \dots, c_n)$, $(e_1 \cdots e_n)^2 = \Delta$. Moreover,

$$\begin{aligned} e_i \cdot (e_1 \cdots e_n) &= (-1)^{i-1} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n) \\ (e_1 \cdots e_n) \cdot e_i &= (-1)^{n-i} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n). \end{aligned}$$

Therefore, $e_1 \cdots e_n$ lies in the centre of $C(V, q)$ if and only if n is odd.

PROPOSITION 18.21 (a) *If n is even, the centre of $C(V, q)$ is k ; if n is odd, it is of degree 2 over k , generated by $e_1 \cdots e_n$. In particular, $C_0 \cap \text{Centre}(C(V, q)) = k$.*

(b) *No nonzero element of C_1 centralizes C_0 .*

PROOF. First show that a linear combination of reduced monomials is in the centre (or centralizes C_0) if and only if each monomial does, and then find the monomials that centralize the e_i (or the $e_i e_j$). \square

In Scharlau 1985, Chapter 9, 2.10, there is the following description of the complete structure of $C(V, q)$:

If n is even, $C(V, q)$ is a central simple algebra over k , isomorphic to a tensor product of quaternion algebras. If n is odd, the centre of $C(V, q)$ is generated over k by the element $e_1 \cdots e_n$ whose square is Δ , and, if Δ is not a square in k , then $C(V, q)$ is a central simple algebra over the field $k[\sqrt{\Delta}]$.

THE INVOLUTION *

An **involution** of a k -algebra D is a k -linear map $*$: $D \rightarrow D$ such that $(ab)^* = b^* a^*$ and $a^{**} = 1$. For example, $M \mapsto M^t$ (transpose) is an involution of $M_n(k)$.

Let $C(V, q)^{\text{opp}}$ be the **opposite** k -algebra to $C(V, q)$, i.e., $C(V, q)^{\text{opp}} = C(V, q)$ as a k -vector space but

$$ab \text{ in } C(V, q)^{\text{opp}} = ba \text{ in } C(V, q).$$

The map $\rho: V \rightarrow C(V, q)^{\text{opp}}$ is k -linear and has the property that $\rho(x)^2 = q(x)$. Thus, there exists an isomorphism $*$: $C(V, q) \rightarrow C(V, q)^{\text{opp}}$ inducing the identity map on V , and which therefore has the property that

$$(x_1 \cdots x_r)^* = x_r \cdots x_1$$

for $x_1, \dots, x_r \in V$. We regard $*$ as an involution of A . Note that, for $x \in V$, $x^* x = q(x)$.

18g The Spin group

Initially we define the spin group as an abstract group.

DEFINITION 18.22 The group $\text{Spin}(q)$ consists of the elements t of $C_0(V, q)$ such that

- (a) $t^*t = 1$,
- (b) $tVt^{-1} = V$,
- (c) the map $x \mapsto txt^{-1}: V \rightarrow V$ has determinant 1.

REMARK 18.23 (a) The condition (a) implies that t is invertible in $C_0(V, q)$, and so (b) makes sense.

(b) We shall see in (18.27) below that the condition (c) is implied by (a) and (b).

THE MAP $\text{Spin}(q) \rightarrow \text{SO}(q)$

Let t be an invertible element of $C(V, q)$ such that $tVt^{-1} = V$. Then the mapping $x \mapsto txt^{-1}: V \rightarrow V$ is an isometry, because

$$q(txt^{-1}) = (txt^{-1})^2 = tx^2t^{-1} = tq(x)t^{-1} = q(x).$$

Therefore, an element $t \in \text{Spin}(q)$ defines an element $x \mapsto txt^{-1}$ of $\text{SO}(q)$.

THEOREM 18.24 *The homomorphism*

$$\text{Spin}(q) \rightarrow \text{SO}(q)$$

just defined has kernel of order 2, and it is surjective if k is algebraically closed.

PROOF. The kernel consists of those $t \in \text{Spin}(q)$ such that $txt^{-1} = x$ for all $x \in V$. As V generates $C(V, q)$, such a t must lie in the centre of $C(V, q)$. Since it is also in C_0 , it must lie in k . Now the condition $t^*t = 1$ implies that $t = \pm 1$.

For an anisotropic $a \in V$, let R_a be the reflection in the hyperplane orthogonal to a . According to Theorem 18.2, each element σ of $\text{SO}(q)$ can be expressed $\sigma = R_{a_1} \cdots R_{a_m}$ for some a_i . As $\det(R_{a_1} \cdots R_{a_m}) = (-1)^m$, we see that m is even, and so $\text{SO}(q)$ is generated by elements $R_a R_b$ with a, b anisotropic elements of V . If k is algebraically closed, we can even scale a and b so that $q(a) = 1 = q(b)$.

Now

$$\begin{aligned} axa^{-1} &= (-xa + 2\phi(a, x))a^{-1} && \text{as } (ax + xa = 2\phi(a, x), \text{ see (115)}) \\ &= -\left(x - \frac{2\phi(a, x)}{q(a)}a\right) && \text{as } a^2 = q(a) \\ &= -R_a(x). \end{aligned}$$

Moreover,

$$(ab)^*ab = baab = q(a)q(b).$$

Therefore, if $q(a)q(b) = 1$, then $R_a R_b$ is in the image of $\text{Spin}(q) \rightarrow \text{SO}(q)$. As we noted above, such elements generate $\text{SO}(q)$ when k is algebraically closed. \square

In general, the homomorphism is not surjective. For example, if $k = \mathbb{R}$, then $\text{Spin}(q)$ is connected but $\text{SO}(q)$ will have two connected components when ϕ is indefinite. In this case, the image is the identity component of $\text{SO}(q)$.

18h The Clifford group

Write γ for the automorphism of $C(V, q)$ that acts as 1 on $C_0(V, q)$ and as -1 on $C_1(V, q)$.

DEFINITION 18.25 The *Clifford group* is

$$\Gamma(q) = \{t \in C(V, q) \mid t \text{ invertible and } \gamma(t)Vt^{-1} = V\}.$$

For $t \in \Gamma(q)$, let $\alpha(t)$ denote the homomorphism $x \mapsto \gamma(t)xt^{-1}: V \rightarrow V$.

PROPOSITION 18.26 For all $t \in \Gamma(q)$, $\alpha(t)$ is an isometry of V , and the sequence

$$1 \rightarrow k^\times \rightarrow \Gamma(q) \xrightarrow{\alpha} \text{O}(q) \rightarrow 1$$

is exact (no condition on k).

PROOF. Let $t \in \Gamma(q)$. On applying γ and $*$ to $\gamma(t)V = Vt$, we find that $\gamma(t^*)V = Vt^*$, and so $t^* \in \Gamma(q)$. Now, because $*$ and γ act as 1 and -1 on V ,

$$\gamma(t) \cdot x \cdot t^{-1} = -\gamma(\gamma(t) \cdot x \cdot t^{-1})^* = -\gamma(t^{*-1}x\gamma(t^*)) = \gamma(t^{*-1})xt^*,$$

and so

$$\gamma(t^*)\gamma(t)x = xt^*t. \quad (118)$$

We use this to prove that $\alpha(t)$ is an isometry:

$$q(\alpha(t)(x)) = (\alpha(t)(x))^* \cdot (\alpha(t)(x)) = t^{*-1}x\gamma(t)^* \cdot \gamma(t)xt^{-1} \stackrel{(118)}{=} t^{*-1}xxt^*tt^{-1} = q(x).$$

As k is in the centre of $\Gamma(q)$, k^\times is in the kernel of α . Conversely, let $t = t_0 + t_1$ be an invertible element of $C(V, q)$ such that $\gamma(t)xt^{-1} = x$ for all $x \in V$, i.e., such that

$$t_0x = xt_0, \quad t_1x = -xt_1$$

for all $x \in V$. As V generates $C(V, q)$ these equations imply that t_0 lies in the centre of $C(V, q)$, and hence in k (18.21a), and that t_1 centralizes C_0 , and hence is zero (18.21b). We have shown that

$$\text{Ker}(\alpha) = k^\times.$$

It remains to show that α is surjective. For $t \in V$, $\alpha(t)(y) = -tyt^{-1}$ and so (see the proof of (18.24)), $\alpha(t) = R_t$. Therefore the surjectivity follows from Theorem 18.2. \square

COROLLARY 18.27 For an invertible element t of $C_0(V, q)$ such that $tVt^{-1} = V$, the determinant of $x \mapsto txt^{-1}: V \rightarrow V$ is one.

PROOF. According to the proposition, every element $t \in \Gamma(q)$ can be expressed in the form

$$t = ca_1 \cdots a_m$$

with $c \in k^\times$ and the a_i anisotropic elements of V . Such an element acts as $R_{a_1} \cdots R_{a_m}$ on V , and has determinant $(-1)^m$. If $t \in C_0(V, q)$, then m is even, and so $\det(t) = 1$. \square

Hence, the condition (c) in the definition of $\text{Spin}(q)$ is superfluous.

18i Action of $O(q)$ on $\text{Spin}(q)$

18.28 An element σ of $O(q)$ defines an automorphism of $C(V, q)$ as follows. Consider $\rho \circ \sigma: V \rightarrow C(V, q)$. Then $(\rho(\sigma(x)))^2 = \phi(\sigma(x)) \cdot 1 = \phi(x) \cdot 1$ for every $x \in V$. Hence, by the universal property, there is a unique homomorphism $\tilde{\sigma}: C(V, q) \rightarrow C(V, q)$ rendering

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C(V, q) \\ \downarrow \sigma & & \downarrow \tilde{\sigma} \\ V & \xrightarrow{\rho} & C(V, q) \end{array}$$

commutative. Clearly $\widetilde{\sigma_1 \circ \sigma_2} = \tilde{\sigma}_1 \circ \tilde{\sigma}_2$ and $\widetilde{\text{id}} = \text{id}$, and so $\widetilde{\sigma^{-1}} = \tilde{\sigma}^{-1}$, and so $\tilde{\sigma}$ is an automorphism. If $\sigma \in SO(\phi)$, it is known that $\tilde{\sigma}$ is an inner automorphism of $C(V, q)$ by an invertible element of $C^+(V, q)$.

18j Restatement in terms of algebraic groups

Let (V, q) be quadratic space over k , and let q_K be the unique extension of q to a quadratic form on $K \otimes_k V$. As we noted in (18.20), $C(V, q_K) = K \otimes_k C(V, q)$.

THEOREM 18.29 *There exists a naturally defined algebraic group $\underline{\text{Spin}}(q)$ over k such that*

$$\underline{\text{Spin}}(q)(K) \simeq \text{Spin}(q_K)$$

for all fields K containing k . Moreover, there is a homomorphism of algebraic groups

$$\underline{\text{Spin}}(q) \rightarrow \text{SO}(q)$$

giving the homomorphism in (18.24) for each field K containing k . Finally, the action of $O(q)$ on $C(V, q)$ described in (18.24) defines an action of $O(q)$ on $\underline{\text{Spin}}(q)$.

PROOF. Show that, when k is infinite, the algebraic group attached to the subgroup $\text{Spin}(q)$ of $\text{GL}(V)$ (see 7.22) has these properties. Alternatively, define a functor $R \rightsquigarrow \text{Spin}(q_R)$ that coincides with the previous functor when R is a field. \square

In future, we shall write $\text{Spin}(q)$ for the algebraic group $\underline{\text{Spin}}(q)$.

ASIDE 18.30 A representation of a semisimple algebraic group G gives rise to a representation of its Lie algebra \mathfrak{g} , and all representations of \mathfrak{g} arise from G only if G has the largest possible centre. “When E. Cartan classified the simple representations of all simple Lie algebras, he discovered a new representation of the orthogonal Lie algebra [not arising from the orthogonal group]. But he did not give a specific name to it, and much later, he called the elements on which this new representation operates *spinors*, generalizing the terminology adopted by physicists in a special case for the rotation group of the three dimensional space” (C. Chevalley, *The Construction and Study of Certain Important Algebras*, 1955, III 6). This explains the origin and name of the Spin group.

19 The classical semisimple groups

Over an algebraically closed field, the classical semisimple algebraic groups are those whose almost-simple factors are isogenous to a group on the following list: SL_{n+1} ($n \geq 1$), SO_{2n+1} ($n \geq 2$), Sp_{2n} ($n \geq 3$), SO_{2n} ($n \geq 4$); these are said to be, respectively, of type A_n , B_n , C_n , or D_n . Over an arbitrary field k , they are the semisimple algebraic groups that become classical over k^{al} . We shall call A_n , B_n , C_n , and D_n the classical types.

In this section, we describe the classical semisimple groups over a field k in terms of the semisimple algebras with involution over k .⁶⁷ Then we explain how class field theory allows us describe the semisimple algebras over the algebraic number fields (e.g., \mathbb{Q}), the p -adic fields (e.g., \mathbb{Q}_p), and \mathbb{R} .

In this section, by a k -algebra A , we mean a ring (not necessarily commutative) containing k in its centre and of finite dimension as a k -vector space (the dimension is called the *degree* $[A:k]$ of A). Throughout this section, vector spaces and modules are finitely generated.

Throughout this section, k is a field. In the second part of the section, k is assumed to have characteristic zero.

NOTES This section is OK as far as it goes, but needs to be completed (proofs added; condition on the characteristic removed). I think it can be made elementary (no root systems etc.) except that we need to know what the groups of outer automorphisms are — in particular, that they are finite mod inner automorphisms (perhaps this can be proved directly case by case).

19a Nonabelian cohomology

Let Γ be a group. A Γ -set is a set A with an action

$$(\sigma, a) \mapsto \sigma a: \Gamma \times A \rightarrow A$$

of Γ on A (so $(\sigma\tau)a = \sigma(\tau a)$ and $1a = a$). If, in addition, A has the structure of a group and the action of Γ respects this structure (i.e., $\sigma(aa') = \sigma a \cdot \sigma a'$), then we say A is a Γ -group.

DEFINITION OF $H^0(\Gamma, A)$

For a Γ -set A , $H^0(\Gamma, A)$ is defined to be the set A^Γ of elements left fixed by the operation of Γ on A , i.e.,

$$H^0(\Gamma, A) = A^\Gamma = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in \Gamma\}.$$

If A is a Γ -group, then $H^0(\Gamma, A)$ is a group.

DEFINITION OF $H^1(\Gamma, A)$

Let A be a Γ -group. A mapping $\sigma \mapsto a_\sigma$ of Γ into A is said to be a *crossed homomorphism* or a *1-cocycle* Γ in A if the relation $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ holds for all $\sigma, \tau \in \Gamma$. Two 1-cocycles (a_σ) and (b_σ) are said to be *equivalent* if there exists a $c \in A$ such that

$$b_\sigma = c^{-1} \cdot a_\sigma \cdot \sigma c \quad \text{for all } \sigma \in \Gamma.$$

⁶⁷Except for the algebraic groups of type 3D_4 , which seem to be neither classical nor exceptional.

This is an equivalence relation on the set of 1-cocycles of Γ in A , and $H^1(\Gamma, A)$ is defined to be the set of equivalence classes of 1-cocycles.

In general $H^1(\Gamma, A)$ is not a group unless A is commutative, but it has a distinguished element, namely, the class of 1-cocycles of the form $\sigma \mapsto b^{-1} \cdot \sigma b$, $b \in A$ (the *principal 1-cocycles*).

COMPATIBLE HOMOMORPHISMS

Let Δ be a second group. Let A be Γ -group and B an Δ -group. Two homomorphisms $f: A \rightarrow B$ and $g: \Delta \rightarrow \Gamma$ are said to be *compatible* if

$$f(g(\sigma)a) = \sigma(f(a)) \text{ for all } \sigma \in \Delta, a \in A.$$

If (a_σ) is a 1-cocycle for A , then

$$b_\sigma = f(a_{g(\sigma)})$$

is a 1-cocycle of Δ in B , and this defines a mapping $H^1(\Gamma, A) \rightarrow H^1(\Delta, B)$, which is a homomorphism if A and B are commutative.

When $\Delta = \Gamma$, a homomorphism $f: A \rightarrow B$ compatible with the identity map, i.e., such that

$$f(\sigma a) = \sigma(f(a)) \text{ for all } \sigma \in \Gamma, a \in A,$$

f is said to be a Γ -*homomorphism* (or be Γ -*equivariant*).

EXACT SEQUENCES

PROPOSITION 19.1 *An exact sequence*

$$1 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 1$$

of Γ -groups gives rise to an exact sequence of cohomology sets

$$1 \rightarrow H^0(\Gamma, A') \rightarrow H^0(\Gamma, A) \rightarrow H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A') \rightarrow H^1(\Gamma, A) \rightarrow H^1(\Gamma, A'')$$

Exactness at $H^0(\Gamma, A'')$ means that the fibres of the map $H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A')$ are the orbits of the group $H^0(\Gamma, A)$ acting on $H^0(\Gamma, A'')$. Exactness at $H^1(\Gamma, A')$ means that fibre of $H^1(\Gamma, A') \rightarrow H^1(\Gamma, A)$ over the distinguished element is the image of $H^0(\Gamma, A'')$.

We now define the boundary map $H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A')$. For simplicity, regard A' as a subgroup of A with quotient A'' . Let a'' be an element of A'' fixed by Γ , and choose an a in A mapping to it. Because a'' is fixed by Γ , $a^{-1} \cdot \sigma a$ is an element of A' , which we denote a_σ . The map $\sigma \mapsto a_\sigma$ is a 1-cocycle whose class in $H^1(\Gamma, A')$ is independent of the choice of a . To define the remaining maps and check the exactness is now very easy.

PROFINITE GROUPS

For simplicity, we now assume k to be perfect. Let $\Gamma = \text{Gal}(k^{\text{al}}/k)$ where k^{al} is the algebraic closure of k . For any subfield K of k^{al} finite over k , we let

$$\Gamma_K = \{\sigma \in \Gamma \mid \sigma x = x \text{ for all } x \in K\}.$$

We consider only Γ -groups A for which

$$A = \bigcup A^{\Gamma_K} \tag{119}$$

and we define $H^1(\Gamma, A)$ to be the set of equivalence classes of 1-cocycles that factor through $\text{Gal}(K/k)$ for some subfield K of k^{al} finite and Galois over k . With these definitions,⁶⁸

$$H^1(\Gamma, A) = \varinjlim H^1(\text{Gal}(K/k), A^{\Gamma_K}) \quad (120)$$

where K runs through the subfields K of k^{al} finite and Galois over k .

THE GALOIS COHOMOLOGY OF ALGEBRAIC GROUPS

When G is an algebraic group over k ,

$$G(k^{\text{al}}) = \bigcup G(K), \quad G(K) = G(k^{\text{al}})^{\Gamma_K},$$

and so $G(k^{\text{al}})$ satisfies (119). We write $H^i(k, G)$ for $H^i(\text{Gal}(k^{\text{al}}/k), G(k^{\text{al}}))$.

An exact sequence

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

of algebraic groups over k gives rise to an exact sequence

$$1 \rightarrow G'(R) \rightarrow G(R) \rightarrow G''(R)$$

for any k -algebra R ; when $R = k^{\text{al}}$, we get a short exact sequence

$$1 \rightarrow G'(k^{\text{al}}) \rightarrow G(k^{\text{al}}) \rightarrow G''(k^{\text{al}}) \rightarrow 1$$

(7.54), and hence (19.1) an exact sequence

$$1 \rightarrow G'(k) \rightarrow G(k) \rightarrow G''(k) \rightarrow H^1(k, G') \rightarrow H^1(k, G) \rightarrow H^1(k, G'').$$

CLASSIFYING VECTOR SPACES WITH TENSORS

Let K be a finite Galois extension of k with Galois group Γ . Let V be a finite-dimensional K -vector space. A **semi-linear action** of Γ on V is a homomorphism $\Gamma \rightarrow \text{Aut}_{k\text{-lin}}(V)$ such that

$$\sigma(cv) = \sigma c \cdot \sigma v \quad \text{all } \sigma \in \Gamma, c \in K, v \in V.$$

If $V = K \otimes_k V_0$, then there is a unique semi-linear action of Γ on V for which $V^\Gamma = 1 \otimes V_0$, namely,

$$\sigma(c \otimes v) = \sigma c \otimes v \quad \sigma \in \Gamma, c \in K, v \in V.$$

PROPOSITION 19.2 *The functor $V \mapsto K \otimes_k V$ from k -vector spaces to K -vector spaces endowed with a semi-linear action of Γ is an equivalence of categories with quasi-inverse $V \mapsto V^\Gamma$.*

PROOF. The proof is elementary. See AG 16.14. □

⁶⁸Equivalently, we consider only Γ -groups A for which the pairing $\Gamma \times A \rightarrow A$ is continuous relative to the Krull topology on Γ and the discrete topology on A , and we require that the 1-cocycles be continuous for the same topologies.

BILINEAR FORMS AND COHOMOLOGY SETS

Let V_0 be a k -vector space equipped with a bilinear form $\phi_0: V \times V \rightarrow k$, and write $(V_0, \phi_0)_K$ for the pair over K obtained from (V_0, ϕ_0) by extension of scalars. Let $\mathcal{A}(K)$ denote the set of automorphisms of $(V_0, \phi_0)_K$.⁶⁹

THEOREM 19.3 *The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K .*

PROOF. Suppose $(V, \phi)_K \approx (V_0, \phi_0)_K$, and choose an isomorphism

$$f: (V_0, \phi_0)_K \rightarrow (V, \phi)_K.$$

Let

$$a_\sigma = f^{-1} \circ \sigma f.$$

Then

$$\begin{aligned} a_\sigma \cdot \sigma a_\tau &= (f^{-1} \circ \sigma f) \circ (\sigma f^{-1} \circ \sigma \tau f) \\ &= a_{\sigma\tau}, \end{aligned}$$

and so $a_\sigma(f)$ is a 1-cocycle. Moreover, any other isomorphism $f': (V_0, \phi_0)_K \rightarrow (V, \phi)_K$ differs from f by a $g \in \mathcal{A}(K)$, and

$$a_\sigma(f \circ g) = g^{-1} \cdot a_\sigma(f) \cdot \sigma g.$$

Therefore, the cohomology class of $a_\sigma(f)$ depends only on (V, ϕ) . It is easy to see that, in fact, it depends only on the isomorphism class of (V, ϕ) , and that two pairs (V, ϕ) and (V', ϕ') giving rise to the same class are isomorphic. It remains to show that every cohomology class arises from a pair (V, ϕ) . Let $(a_\sigma)_{\sigma \in \Gamma}$ be a 1-cocycle, and use it to define a new action of Γ on $V_K \stackrel{\text{def}}{=} K \otimes_k V$:

$${}^\sigma x = a_\sigma \cdot \sigma x, \quad \sigma \in \Gamma, \quad x \in V_K.$$

Then

$${}^\sigma(cv) = \sigma c \cdot {}^\sigma v, \text{ for } \sigma \in \Gamma, c \in K, v \in V,$$

and

$${}^\sigma({}^\tau v) = {}^\sigma(a_\tau \tau v) = a_\sigma \cdot \sigma a_\tau \cdot \sigma \tau v = {}^{\sigma\tau} v,$$

and so this is a semilinear action. Therefore,

$$V_1 \stackrel{\text{def}}{=} \{x \in V_K \mid {}^\sigma x = x\}$$

is a subspace of V_K such that $K \otimes_k V_1 \simeq V_K$ (by 19.2). Because ϕ_{0K} arises from a pairing over k ,

$$\phi_{0K}(\sigma x, \sigma y) = \sigma \phi(x, y), \quad \text{all } x, y \in V_K.$$

Therefore (because $a_\sigma \in \mathcal{A}(K)$),

$$\phi_{0K}({}^\sigma x, {}^\sigma y) = \phi_{0K}(\sigma x, \sigma y) = \sigma \phi_{0K}(x, y).$$

If $x, y \in V_1$, then $\phi_{0K}({}^\sigma x, {}^\sigma y) = \phi_{0K}(x, y)$, and so $\phi_{0K}(x, y) = \sigma \phi_{0K}(x, y)$. By Galois theory, this implies that $\phi_{0K}(x, y) \in k$, and so ϕ_{0K} induces a k -bilinear pairing on V_1 . \square

⁶⁹In more detail: $(V_0, \phi_0)_K = (V_{0K}, \phi_{0K})$ where $V_{0K} = K \otimes_k V_0$ and ϕ_{0K} is the unique K -bilinear map $V_{0K} \times V_{0K} \rightarrow K$ extending ϕ_0 ; an element of $\mathcal{A}(K)$ is a K -linear isomorphism $\alpha: V_{0K} \rightarrow V_{0K}$ such that $\phi_{0K}(\alpha x, \alpha y) = \phi_{0K}(x, y)$ for all $x, y \in V_{0K}$.

APPLICATIONS

Again let K be a finite Galois extension of k with Galois group Γ .

PROPOSITION 19.4 For all n , $H^1(\Gamma, \mathrm{GL}_n(K)) = 1$.

PROOF. Apply Theorem 19.3 with $V_0 = k^n$ and ϕ_0 the zero form. It shows that $H^1(\Gamma, \mathrm{GL}_n(K))$ classifies the isomorphism classes of k -vector spaces V such that $K \otimes_k V \approx K^n$. But such k -vector spaces have dimension n , and therefore are isomorphic. \square

PROPOSITION 19.5 For all n , $H^1(\Gamma, \mathrm{SL}_n(K)) = 1$

PROOF. Because the determinant map $\det: \mathrm{GL}_n(K) \rightarrow K^\times$ is surjective,

$$1 \rightarrow \mathrm{SL}_n(K) \rightarrow \mathrm{GL}_n(K) \xrightarrow{\det} K^\times \rightarrow 1$$

is an exact sequence of Γ -groups. It gives rise to an exact sequence

$$\mathrm{GL}_n(k) \xrightarrow{\det} k^\times \rightarrow H^1(\Gamma, \mathrm{SL}_n) \rightarrow H^1(\Gamma, \mathrm{GL}_n)$$

from which the statement follows. \square

PROPOSITION 19.6 Let ϕ_0 be a nondegenerate alternating bilinear form on V_0 , and let Sp be the associated symplectic group⁷⁰. Then $H^1(\Gamma, \mathrm{Sp}(K)) = 1$.

PROOF. According to Theorem 19.3, $H^1(\Gamma, \mathrm{Sp}(K))$ classifies isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K . But this condition implies that ϕ is a nondegenerate alternating form and that $\dim V = \dim V_0$. All such pairs (V, ϕ) are isomorphic. \square

REMARK 19.7 Let ϕ_0 be a nondegenerate bilinear symmetric form on V_0 , and let O be the associated orthogonal group. Then $H^1(\Gamma, \mathrm{O}(K))$ classifies the isomorphism classes of quadratic spaces over k that become isomorphic to (V, ϕ) over K . This can be a very large set.

19b Classifying the forms of an algebraic group (overview)

Again let K be a finite Galois extension of k with Galois group Γ . Let G_0 be an algebraic group over k , and let $\mathcal{A}(K)$ be the group of automorphisms of $(G_0)_K$. Then Γ acts on $\mathcal{A}(K)$ in a natural way:

$$\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}, \quad \sigma \in \Gamma, \quad \alpha \in \mathcal{A}(K).$$

THEOREM 19.8 The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of algebraic groups G over k that become isomorphic to G_0 over K .

⁷⁰So $\mathrm{Sp}(R) = \{a \in \mathrm{End}_{R\text{-lin}}(R \otimes_k V) \mid \phi(ax, ay) = \phi(x, y)\}$

PROOF. Let G be such an algebraic group over k , choose an isomorphism

$$f: G_{0K} \rightarrow G_K,$$

and write

$$a_\sigma = f^{-1} \circ \sigma f.$$

As in the proof of Theorem 19.3, $(a_\sigma)_{\sigma \in \Gamma}$ is a 1-cocycle, and the map

$$G \mapsto \text{class of } (a_\sigma)_{\sigma \in \Gamma} \text{ in } H^1(\Gamma, A(K))$$

is well-defined and its fibres are the isomorphism classes.

In proving that the map is surjective, it is useful to identify $\mathcal{A}(K)$ with the automorphism group of the Hopf algebra $\mathcal{O}(G_{0K}) = K \otimes_k \mathcal{O}(G_0)$. Let $A_0 = \mathcal{O}(G_0)$ and $A = K \otimes_k A_0$. As in the proof of Theorem 19.3, we use a 1-cocycle $(a_\sigma)_{\sigma \in \Gamma}$ to twist the action of Γ on A ; specifically, we define

$${}^\sigma a = a_\sigma \circ \sigma a, \quad \sigma \in \Gamma, \quad a \in A.$$

Proposition 19.2 in fact holds for infinite dimensional vector spaces V with the same proof, and so the k -subspace

$$B = \{a \in A \mid {}^\sigma a = a\}$$

of A has the property that

$$K \otimes_k B \simeq A.$$

It remains to show that the Hopf algebra structure on A induces a Hopf algebra structure on B . Consider for example the comultiplication. The k -linear map

$$\Delta_0: A_0 \rightarrow A_0 \otimes_k A_0$$

has a unique extension to a K -linear map

$$\Delta: A \rightarrow A \otimes_K A.$$

This map commutes with the action of Γ :

$$\Delta(\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Because a_σ is a Hopf algebra homomorphism,

$$\Delta(a_\sigma a) = a_\sigma \Delta(a), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Therefore,

$$\Delta({}^\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

In particular, we see that Δ maps B into $(A \otimes_K A)^\Gamma$, which equals $B \otimes_k B$ because the functor in (19.2) preserves tensor products. Similarly, all the maps defining the Hopf algebra structure on A preserve B , and therefore define a Hopf algebra structure on B . Finally, one checks that the 1-cocycle attached to B and the given isomorphism $K \otimes_k B \rightarrow A$ is (a_σ) . \square

EXAMPLES

19.9 For all n , $H^1(k, \mathrm{GL}_n) = 1$.

This follows from (19.4) and (120).

19.10 For all n , $H^1(k, \mathrm{SL}_n) = 1$.

19.11 For all n , $H^1(k, \mathrm{Sp}_n) = 1$.

19.12 Let (V, ϕ) be a nondegenerate quadratic space over k . Then $H^1(k, \mathcal{O}(\phi))$ classifies the isomorphism classes of quadratic spaces over k with the same dimension as V .

PROOF. Over k^{al} , all nondegenerate quadratic spaces of the same dimension are isomorphic. □

19.13 Let G be an algebraic group of k . The isomorphism classes of algebraic groups over k that become isomorphic to $G_{k^{\mathrm{al}}}$ over k^{al} are classified by $H^1(\Gamma, \mathcal{A}(k^{\mathrm{al}}))$. Here $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$ and $\mathcal{A}(k^{\mathrm{al}})$ is the automorphism group of $G_{k^{\mathrm{al}}}$.

This can be proved by passing to the limit in (19.8) over all $K \subset k^{\mathrm{al}}$ that are finite and Galois over k , or by rewriting the proof of (19.8) for infinite extensions.

19.14 Let $G_* = (G)_{K/k}$. We have

$$H^i(k, G_*) \simeq H^i(K, G) \text{ for } i = 0, 1 \text{ (and for all } i \geq 0 \text{ when } G \text{ is commutative).}$$

PROOF. Combine (186) with Shapiro's lemma (CFT II, 1.11 for the commutative case; need to add the proof for the noncommutative case). □

An algebraic group G over a field k is said to be **geometrically almost-simple** (or **absolutely almost-simple**) if it is almost-simple, and remains almost-simple over k^{al} .⁷¹

From now on, **we assume that k has characteristic zero.**

Every semisimple algebraic group over a field k has a finite covering by a simply connected semisimple algebraic group over k ; moreover, every simply connected semisimple algebraic group over k is a direct product of almost-simple algebraic groups over k (when G is simply connected, the map in (17.16) is an isomorphism); finally, every simply connected almost-simple group over k is of the form $(G)_{K/k}$ where G is geometrically almost-simple over K (17.19). Thus, to some extent, the problem of listing all semisimple algebraic groups comes down to the problem of listing all simply connected, geometrically almost-simple, algebraic groups.

A semisimple group G over a field k is said to be **split** if it contains a split torus T such that $T_{k^{\mathrm{al}}}$ is maximal in $G_{k^{\mathrm{al}}}$.

⁷¹The term "absolutely almost-simple" is more common, but I prefer "geometrically almost-simple".

SIMPLY CONNECTED, GEOMETRICALLY ALMOST-SIMPLE, ALGEBRAIC GROUPS

For an algebraic group G , let $G^{\text{ad}} = G/Z(G)$. We shall need a description of the full automorphism group of G . This is provided by the following statement, which will be proved in a later chapter.

19.15 *Let G be a simply connected semisimple group G , and let $\mathcal{A}(k^{\text{al}})$ be the group of automorphisms of $G_{k^{\text{al}}}$. There is an exact sequence*

$$1 \rightarrow G^{\text{ad}}(k^{\text{al}}) \rightarrow \mathcal{A}(k^{\text{al}}) \rightarrow \text{Sym}(D) \rightarrow 1$$

where $\text{Sym}(D)$ is the (finite) group of symmetries of the Dynkin diagram of G . When G is split, Γ acts trivially on $\text{Sym}(D)$, and the sequence is split, i.e., there is a subgroup of $\mathcal{A}(k^{\text{al}})$ on which Γ acts trivially and which maps isomorphically onto $\text{Sym}(D)$.

An element of $G^{\text{ad}}(k^{\text{al}}) = G(k^{\text{al}})/Z(k^{\text{al}})$ acts on $G_{k^{\text{al}}}$ by an inner automorphism. The Dynkin diagrams of almost-simple groups don't have many symmetries: for D_4 the symmetry group is S_3 (symmetric group on 3 letters), for A_n , D_n , and E_6 it has order 2, and otherwise it is trivial. Later in this section, we shall explicitly describe the outer automorphisms arising from these symmetries.

19.16 For each classical type and field k , we shall write down a split, geometrically almost-simple, algebraic group G over k such that $G_{k^{\text{al}}}$ is of the given type (in fact, G is unique up to isomorphism). We know (19.13) that the isomorphism classes of algebraic groups over k becoming isomorphic to G over k^{al} are classified by $H^1(k, \mathcal{A}(k^{\text{al}}))$ where $\mathcal{A}(k^{\text{al}})$ is the automorphism group of $G_{k^{\text{al}}}$. The Galois group Γ acts trivially on $X^*(Z(G))$; for the form G' of G defined by a 1-cocycle (a_σ) , $Z(G')_{k^{\text{al}}} = Z(G)_{k^{\text{al}}}$ but with Γ acting through a_σ .

For example, for A_n , the split group is SL_n . This has centre μ_n , which is the group of multiplicative type corresponding to $\mathbb{Z}/n\mathbb{Z}$ with the trivial action of Γ . Let G_0 and G be groups over k , and let $f: G_0_{k^{\text{al}}} \rightarrow G_{k^{\text{al}}}$ be an isomorphism over k^{al} . Write $a_\sigma = f^{-1} \circ \sigma f$. Then f defines an isomorphism

$$f: Z_0(k^{\text{al}}) \rightarrow Z(k^{\text{al}})$$

on the points of their centres, and

$$f(a_\sigma \sigma x) = \sigma(f(x)).$$

When we use f to identify $Z_0(k^{\text{al}})$ with $Z(k^{\text{al}})$, this says that Γ acts on $Z(k^{\text{al}})$ by the twisted action ${}^\sigma x = a_\sigma \sigma x$.

REMARK 19.17 Let G_0 be the split simply connected group of type X_y , and let G be a form of G_0 . Let c be its cohomology class. If $c \in H^1(k, G^{\text{ad}})$, then G is called an **inner form** of G . In general, c will map to a nontrivial element of

$$H^1(k, \text{Sym}(D)) = \text{Hom}_{\text{continuous}}(\Gamma, \text{Sym}(D)).$$

Let Δ be the kernel of this homomorphism, and let L be the corresponding extension field of k . Let $z = (\Gamma: \Delta)$. Then we say G is of type ${}^z X_y$. For example, if G is of type ${}^3 D_4$, then it becomes an inner form of the split form over a

19c The forms of $M_n(k)$

DEFINITION 19.18 A k -algebra A is **central** if its centre is k , and it is **simple** if it has no 2-sided ideals (except 0 and A). If all nonzero elements have inverses, it is called a **division algebra** (or **skew field**).

EXAMPLE 19.19 (a) The ring $M_n(k)$ is central and simple.

(b) For any $a, b \in k^\times$, the quaternion algebra $\mathbb{H}(a, b)$ is central and simple. It is either a division algebra, or it is isomorphic to $M_2(k)$.

THEOREM 19.20 (WEDDERBURN) For any division algebra D over k , $M_n(D)$ is a simple k -algebra, and every simple k -algebra is of this form.

PROOF. See GT 7.22 or CFT, IV 1.9. □

COROLLARY 19.21 When k is algebraically closed, the only central simple algebras over k are the matrix algebras $M_n(k)$.

PROOF. Let D be a division algebra over k , and let $\alpha \in D$. Then $k[\alpha]$ is a commutative integral domain of finite dimension over k , and so is a field. As k is algebraically closed, $k[\alpha] = k$. □

PROPOSITION 19.22 The k -algebras becoming isomorphic to $M_n(k)$ over k^{al} are the central simple algebras over k of degree n^2 .

PROOF. Let A be a central simple algebra over k of degree n^2 . Then $k^{\text{al}} \otimes_k A$ is again central simple (CFT IV, 2.15), and so is isomorphic to $M_n(k)$ by (19.21). Conversely, if A is a k -algebra that becomes isomorphic to $M_n(k)$ over k^{al} , then it is certainly central and simple, and has degree n^2 . □

PROPOSITION 19.23 All automorphisms of the k -algebra $M_n(k)$ are inner, i.e., of the form $X \mapsto YXY^{-1}$ for some Y .

PROOF. Let S be k^n regarded as an $M_n(k)$ -module. It is simple, and every simple $M_n(k)$ -module is isomorphic to it (see AG 16.12). Let α be an automorphism of $M_n(k)$, and let S' denote S , but with $X \in M_n(k)$ acting as $\alpha(X)$. Then S' is a simple $M_n(k)$ -module, and so there exists an isomorphism of $M_n(k)$ -modules $f: S \rightarrow S'$. Then

$$\alpha(X)f\vec{x} = fX\vec{x}, \quad \text{all } X \in M_n(k), \vec{x} \in S.$$

Therefore,

$$\alpha(X)f = fX, \quad \text{all } X \in M_n(k).$$

As f is k -linear, it is multiplication by an invertible matrix Y , and so this equation shows that

$$\alpha(X) = YXY^{-1}. \quad \square$$

COROLLARY 19.24 *The isomorphism classes of k -algebras becoming isomorphic to $M_n(k)$ over k^{al} are classified by $H^1(k, \text{PGL}_n)$.*

PROOF. The proposition shows that

$$\text{Aut}_{k^{\text{al}}\text{-alg}}(M_n(k^{\text{al}})) = \text{PGL}_n(k^{\text{al}}).$$

Let A be a k -algebra for which there exists an isomorphism $f: M_n(k^{\text{al}}) \rightarrow k^{\text{al}} \otimes_k A$, and let

$$a_\sigma = f^{-1} \circ \sigma f.$$

Then a_σ is a 1-cocycle, depending only on the k -isomorphism class of A .

Conversely, given a 1-cocycle, define

$$\sigma X = a_\sigma \cdot \sigma X, \quad \sigma \in \Gamma, X \in M_n(k^{\text{al}}).$$

This defines an action of Γ on $M_n(k^{\text{al}})$ and $M_n(k^{\text{al}})^\Gamma$ is a k -algebra becoming isomorphic to $M_n(k)$ over k^{al} (cf. the proof of 19.3). \square

REMARK 19.25 Let A be a central simple algebra over k . For some n , there exists an isomorphism $f: k^{\text{al}} \otimes_k A \rightarrow M_n(k^{\text{al}})$, unique up to an inner automorphism (19.22, 19.23). Let $a \in A$, and let $\text{Nm}(a) = \det(f(a))$. Then $\text{Nm}(a)$ does not depend on the choice of f . Moreover, it is fixed by Γ , and so lies in k . It is called the *reduced norm* of a .

19d The inner forms of SL_n

Consider

$$X \mapsto X: \text{SL}_n(k^{\text{al}}) \rightarrow M_n(k^{\text{al}}).$$

The action of $\text{PGL}_n(k^{\text{al}})$ on $M_n(k^{\text{al}})$ by inner automorphisms preserves $\text{SL}_n(k^{\text{al}})$, and is the full group of inner automorphisms of SL_n .

THEOREM 19.26 *The inner forms of SL_n are the groups $\text{SL}_m(D)$ for D a division algebra of degree n/m .*

PROOF. The inner forms of SL_n and the forms of $M_n(k)$ are both classified by $H^1(k, \text{PGL}_n)$, and so correspond. The forms of $M_n(k)$ are the k -algebras $M_m(D)$ (by 19.22, 19.20), and the form of SL_n is related to it exactly as SL_n is related to M_n . \square

Here $\text{SL}_m(D)$ is the group

$$R \mapsto \{a \in M_m(R \otimes_k D) \mid \text{Nm}(a) = 1\}.$$

19e Involutions of k -algebras

DEFINITION 19.27 Let A be a k -algebra. An *involution* of k is a k -linear map $a \mapsto a^*: A \rightarrow A$ such that

$$\begin{aligned}(ab)^* &= b^*a^* \quad \text{all } a, b \in A, \\ a^{**} &= a.\end{aligned}$$

The involution is said to be of the *first* or *second kind* according as it acts trivially on the elements of the centre of k or not.

EXAMPLE 19.28 (a) On $M_n(k)$ there is the standard involution $X \mapsto X^t$ (transpose) of the first kind.

(b) On a quaternion algebra $\mathbb{H}(a, b)$, there is the standard involution $i \mapsto -i$, $j \mapsto -j$ of the first kind.

(c) On a quadratic field extension K of k , there is a unique nontrivial involution (of the second kind).

LEMMA 19.29 Let $(A, *)$ be an k -algebra with involution. An inner automorphism $x \mapsto axa^{-1}$ commutes with $*$ if and only if a^*a lies in the centre of A .

PROOF. To say that $\text{inn}(a)$ commutes with $*$ means that the two maps

$$\begin{aligned}x \mapsto axa^{-1} &\mapsto (a^*)^{-1}x^*a^* \\ x \mapsto x^* &\mapsto ax^*a^{-1}\end{aligned}$$

coincide, i.e., that

$$x^* = (a^*a)x^*(a^*a)^{-1}$$

for all $x \in A$. As $x \mapsto x^*$ is bijective, this holds if and only if a^*a lies in the centre of a . \square

REMARK 19.30 Let A have centre k . We can replace a with ca , $c \in k^\times$, without changing $\text{inn}(a)$. This replaces a^*a with $c^*c \cdot a^*a$. When $*$ is of the first kind, $c^*c = c^2$. Therefore, when k is algebraically closed, we can choose c to make $a^*a = 1$.

19f The outer forms of SL_n

According to (19.15), there is an exact sequence

$$1 \rightarrow \text{PGL}_n(k^{\text{al}}) \rightarrow \text{Aut}(\text{SL}_n k^{\text{al}}) \rightarrow \text{Sym}(D) \rightarrow 1,$$

and $\text{Sym}(D)$ has order 2. In fact, $X \mapsto (X^{-1})^t = (X^t)^{-1}$ is an outer automorphism of SL_n .

Now consider the k -algebra with involution of the second kind

$$M_n(k) \times M_n(k), \quad (X, Y)^* = (Y^t, X^t).$$

Every automorphism of $M_n(k) \times M_n(k)$ is either inner, or is the composite of an inner automorphism with $(X, Y) \mapsto (Y, X)$.⁷² According to (19.29), the inner automorphism by

⁷²This isn't obvious, but follows from the fact that the two copies of $M_n(k)$ are the *only* simple subalgebras of $M_n(k) \times M_n(k)$ (see Farb and Dennis, *Noncommutative algebra*, GTM 144, 1993, 1.13, for a more general statement).

$a \in A$ commutes with $*$ if and only if $a^*a \in k \times k$. But $(a^*a)^* = a^*a$, and so $a^*a \in k$. When we work over k^{al} , we can scale a so that $a^*a = 1$ (19.30): if $a = (X, Y)$, then

$$1 = a^*a = (Y^t X, X^t Y),$$

and so $a = (X, (X^t)^{-1})$. Thus, the automorphisms of $(M_n(k^{\text{al}}) \times M_n(k^{\text{al}}), *)$ are the inner automorphisms by elements $(X, (X^t)^{-1})$ and composites of such automorphisms with $(X, Y) \mapsto (Y, X)$. When we embed

$$X \mapsto (X, (X^t)^{-1}): \text{SL}_n(k^{\text{al}}) \hookrightarrow M_n(k^{\text{al}}) \times M_n(k^{\text{al}}), \quad (121)$$

the image it is stable under the automorphisms of $(M_n(k^{\text{al}}) \times M_n(k^{\text{al}}), *)$, and this induces an isomorphism

$$\text{Aut}(M_n(k^{\text{al}}) \times M_n(k^{\text{al}}), *) \simeq \text{Aut}(\text{SL}_n k^{\text{al}}).$$

Thus, the forms of SL_n correspond to the forms of $(M_n(k) \times M_n(k), *)$. Such a form is a simple algebra A over k with centre K of degree 2 over k and an involution $*$ of the second kind.

The map (121) identifies $\text{SL}_n(k^{\text{al}})$ with the subgroup of $M_n(k^{\text{al}}) \times M_n(k^{\text{al}})$ of elements such that

$$a^*a = 1, \quad \text{Nm}(a) = 1.$$

Therefore, the form of SL_n attached to the form $(A, *)$ is the group G such that $G(R)$ consists of the $a \in R \otimes_k A$ such that

$$a^*a = 1, \quad \text{Nm}(a) = 1.$$

There is a commutative diagram

$$\begin{array}{ccc} \text{Aut}(\text{SL}_n \bar{k}) & \longrightarrow & \text{Sym}(D) \\ \parallel & & \parallel \\ \text{Aut}(M_n(\bar{k}) \times M_n(\bar{k}), *) & \longrightarrow & \text{Aut}_{k\text{-alg}}(\bar{k} \times \bar{k}). \end{array}$$

The centre K of A is the form of $k^{\text{al}} \times k^{\text{al}}$ corresponding to the image of the cohomology class of G in $\text{Sym}(D)$. Therefore, we see that G is an outer form if and only if K is a field.

19g The forms of Sp_{2n}

Here we use the k -algebra with involution of the first kind

$$M_{2n}(k), \quad X^* = SX^t S^{-1}, \quad S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The inner automorphism defined by an invertible matrix U commutes with $*$ if and only if $U^*U \in k$ (see 19.29). When we pass to k^{al} , we may suppose $U^*U = I$, i.e., that

$$SU^t S^{-1}U = I.$$

Because $S^{-1} = -S$, this says that

$$U^t S U = S$$

i.e., that $U \in \mathrm{Sp}_{2n}(k^{\mathrm{al}})$. Since there are no symmetries of the Dynkin diagram C_n , we see that the inclusion

$$X \mapsto X : \mathrm{Sp}_{2n}(k^{\mathrm{al}}) \hookrightarrow M_{2n}(k^{\mathrm{al}}) \quad (122)$$

induces an isomorphism

$$\mathrm{Aut}(\mathrm{Sp}_{2n k^{\mathrm{al}}}) \simeq \mathrm{Aut}(M_{2n}(k^{\mathrm{al}}), *).$$

Therefore, the forms of Sp_{2n} correspond to the forms of $(M_{2n}(k), *)$. Such a form is a central simple algebra A over k with an involution $*$ of the first kind.

The map (122) identifies $\mathrm{Sp}_{2n}(k^{\mathrm{al}})$ with the subgroup of $M_{2n}(k^{\mathrm{al}})$ of elements such that

$$a^* a = 1.$$

Therefore, the form of Sp_{2n} attached to $(A, *)$ is the group G such that $G(R)$ consists of the $a \in R \otimes_k A$ for which

$$a^* a = 1.$$

19h The forms of $\mathrm{Spin}(\phi)$

Let (V, ϕ) be a nondegenerate quadratic space over k with largest possible Witt index. The action of $O(\phi)$ on itself preserves $\mathrm{SO}(\phi)$, and there is also an action of $O(\phi)$ on $\mathrm{Spin}(\phi)$ (see §18i). These actions are compatible with the natural homomorphism

$$\mathrm{Spin}(\phi) \rightarrow \mathrm{SO}(\phi)$$

and realize $O(\phi)$ modulo its centre as the automorphism group of each. Therefore, the forms of $\mathrm{Spin}(\phi)$ are exactly the double covers of the forms of $\mathrm{SO}(\phi)$.

The determination of the forms of $\mathrm{SO}(\phi)$ is very similar to the last case. Let M be the matrix of ϕ relative to some basis for V . We use the k -algebra with involution of the first kind

$$M_n(k), \quad X^* = M X^t M^{-1}.$$

The automorphism group of $(M_n(k), *)$ is $O(\phi)$ modulo its centre, and so the forms of $\mathrm{SO}(\phi)$ correspond to the forms of $(M_{2n}(k), *)$. Such a form is a central simple algebra A over k with an involution $*$ of the first kind, and the form of $\mathrm{SO}(\phi)$ attached to $(A, *)$ is the group G such that $G(R)$ consists of the $a \in R \otimes_k A$ for which

$$a^* a = 1.$$

19i Algebras admitting an involution

To continue, we need a description of the algebras with involution over a field k . For an arbitrary field, there is not much one can say, but for one important class of fields there is a great deal.

PROPOSITION 19.31 *If a central simple algebra A over k admits an involution of the first kind, then*

$$A \otimes_k A \approx M_{n^2}(k), \quad n^2 = [A:k]. \quad (123)$$

PROOF. Recall that the opposite algebra A^{opp} of A equals A as a k -vector space but has its multiplication reversed:

$$a^{\text{opp}}b^{\text{opp}} = (ba)^{\text{opp}}.$$

Let A_0 denote A regarded as a k -vector space. There are commuting left actions of A and A^{opp} on A_0 , namely, A acts by left multiplication and A^{opp} by right multiplication, and hence a homomorphism

$$A \otimes_k A^{\text{opp}} \rightarrow \text{End}_{k\text{-lin}}(A_0).$$

This is injective, and the source and target have the same dimension as k -vector spaces, and so the map is an isomorphism. Since an involution on A is an isomorphism $A \rightarrow A^{\text{opp}}$, the proposition follows from this. \square

Over all fields, matrix algebras and quaternion algebras admit involutions. For many important fields, these are essentially the only such algebras. Consider the following condition on a field k :

19.32 *The only central division algebras over k or a finite extension of k satisfying (123) are the quaternion algebras and the field itself (i.e., they have degree 4 or 1).*

THEOREM 19.33 *The following fields satisfy (19.32): algebraically closed fields, finite fields, \mathbb{R} , \mathbb{Q}_p and its finite extensions, and \mathbb{Q} and its finite extensions.*

PROOF. The proofs become successively more difficult: for algebraically closed fields there is nothing to prove (19.21); for \mathbb{Q} it requires the full force of class field theory (CFT). \square

19j The involutions on an algebra

Given a central simple algebra admitting an involution, we next need to understand the set of all involutions of it.

THEOREM 19.34 (NOETHER-SKOLEM) *Let A be a central simple algebra over K , and let $*$ and \dagger be involutions of A that agree on K ; then there exists an $a \in A$ such that*

$$x^* = ax^\dagger a^{-1}, \quad \text{all } x \in A. \quad (124)$$

PROOF. See CFT IV, 2.10. \square

Let \dagger be an involution (of the first kind, and so fixing the elements of K , or of the second kind, and so fixing the elements of a subfield k of K such that $[K:k] = 2$). For which invertible a in A does (124) define an involution?

Note that

$$x^{**} = (a^\dagger a^{-1})^{-1} x (a^\dagger a^{-1})$$

and so $a^\dagger a^{-1} \in K$, say

$$a^\dagger = ca, \quad c \in K.$$

Now,

$$a^{\dagger\dagger} = c(c^\dagger a^\dagger) = cc^\dagger \cdot a$$

and so

$$cc^\dagger = 1.$$

If \dagger is of the first kind, this implies that $c^2 = 1$, and so $c = \pm 1$.

If \dagger is of the second kind, this implies that $c = d/d^\dagger$ for some $d \in K$ (Hilbert's theorem 90, FT 5.24). Since $*$ is unchanged when we replace a with a/d , we see that in this case (124) holds with a satisfying $a^\dagger = a$.

19k Hermitian and skew-hermitian forms

We need some definitions. Let

- ◇ $(D, *)$ be a division algebra with an involution $*$,
- ◇ V be a left vector space over D , and
- ◇ $\phi: V \times V \rightarrow D$ a form on V that is semilinear in the first variable and linear in the second (so

$$\phi(ax, by) = a^* \phi(x, y)b, \quad a, b \in D).$$

Then ϕ is said to *hermitian* if

$$\phi(x, y) = \phi(y, x)^*, \quad x, y \in V,$$

and *skew hermitian* if

$$\phi(x, y) = -\phi(y, x)^*, \quad x, y \in V.$$

EXAMPLE 19.35 (a) Let $D = k$ with $*$ = id_k . In this case, the hermitian and skew hermitian forms are, respectively, symmetric and skew symmetric forms.

(b) Let $D = \mathbb{C}$ with $*$ = complex conjugation. In this case, the hermitian and skew hermitian forms are the usual objects.

To each hermitian or skew-hermitian form, we attach the group of automorphisms of (V, ϕ) , and the special group of automorphisms of ϕ (the automorphisms with determinant 1, if this is not automatic).

19l The groups attached to algebras with involution

We assume that the ground field k satisfies the condition (19.32), and compute the groups attached to the various possible algebras with involution.

CASE $A = M_n(k)$; INVOLUTION OF THE FIRST KIND.

In this case, the involution $*$ is of the form

$$X^* = aX^t a^{-1}$$

where $a^t = ca$ with $c = \pm 1$. Recall that the group attached to $(M_n(k), *)$ consists of the matrices X satisfying

$$X^* X = I, \quad \det(X) = 1,$$

i.e.,

$$aX^t a^{-1} X = I, \quad \det(X) = 1,$$

or,

$$X^t a^{-1} X = a^{-1}, \quad \det(X) = 1.$$

Thus, when $c = +1$, we get the special orthogonal group for the symmetric bilinear form attached to a^{-1} , and when $c = -1$, we get the symplectic group attached to the skew symmetric bilinear form attached to a^{-1} .

CASE $A = M_n(K)$; INVOLUTION OF THE SECOND KIND

Omitted for the present.

CASE $A = M_n(D)$; D A QUATERNION DIVISION ALGEBRA.

Omitted for the present.

19m Conclusion.

Let k be a field satisfying the condition (19.32). Then the absolutely almost-simple, simply connected, classical groups over k are the following:

- (A) The groups $SL_m(D)$ for D a central division algebra over k (the inner forms of SL_n); the groups attached to a hermitian form for a quadratic field extension K of k (the outer forms of SL_n).
- (BD) The spin groups of quadratic forms, and the spin groups of skew hermitian forms over quaternion division algebras.
- (C) The symplectic groups, and unitary groups of hermitian forms over quaternion division algebras.

It remains to classify the quaternion algebras and the various hermitian and skew hermitian forms. For the algebraically closed fields, the finite fields, \mathbb{R} , \mathbb{Q}_p , \mathbb{Q} and their finite extensions, this has been done, but for \mathbb{Q} and its extensions it is an application of class field theory.

20 The exceptional semisimple groups

Let k be an algebraically closed field. Beyond the four infinite families of classical algebraic groups described in the last section, there are five exceptional algebraic groups, namely, the groups of type F_4 , E_6 , E_7 , E_8 , and G_2 . In this section, I should describe them explicitly, even over arbitrary fields. However, it is unlikely that this section will ever consist of more than a survey, for the following reasons:

- (a) This is at least as difficult for exceptional groups as for the classical groups, but there are only five exceptional families whereas there are four infinite classical families.
- (b) As for the classical groups, the exceptional groups can be constructed from their Lie algebras (characteristic zero) or from their root systems (all characteristics).
- (c) Traditionally, results have been proved case by case for the classical groups; in extending the result to all groups a uniform proof involving roots and weights has been found. So perhaps one shouldn't learn explicit descriptions of the exceptional groups for fear that one will be tempted to prove all results by case by case arguments.

20a The group G_2

Let k be a field of characteristic zero. A **Hurwitz algebra** over k is a finite k -algebra A (not necessarily commutative) together with a nondegenerate quadratic form $N: A \rightarrow k$ such that

$$N(xy) = N(x)N(y) \text{ for all } x, y \in A.$$

The possible dimensions of A are 1, 2, 4, and 8. A Hurwitz algebra of dimension 8 is also known as an octonion or Cayley algebra. For such an algebra A , the functor

$$R \rightsquigarrow \text{Aut}_k(R \otimes_k A)$$

is an algebraic group over k of type G_2 . (To be continued).

21 Tannakian categories

In the first subsection, we define the abstract notion of a category with a tensor product structure. If the tensor category admits a fibre functor, it is a neutral Tannakian category. In the third subsection, we explain how to interpret the centre of the affine group attached to a fibre functor on Tannakian category in terms of the gradations on the category. This will be used in Chapter III to compute the centre of the algebraic group attached to a semisimple Lie algebra.

21a Tensor categories

21.1 A **k -linear category** is an additive category in which the Hom sets are finite-dimensional k -vector spaces and composition is k -bilinear. Functors between such categories are required to be k -linear, i.e., induce k -linear maps on the Hom sets.

21.2 A **tensor category** over k is a k -linear category together with a k -bilinear functor $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ and compatible associativity and commutativity constraints ensuring that the tensor product of any unordered finite set of objects is well-defined up to a well-defined isomorphism. An associativity constraint is a natural isomorphism

$$\phi_{U,V,W}: U \otimes (V \otimes W) \rightarrow (U \otimes V) \otimes W, \quad U, V, W \in \text{ob}(\mathbf{C}),$$

and a commutativity constraint is a natural isomorphism

$$\psi_{V,W}: V \otimes W \rightarrow W \otimes V, \quad V, W \in \text{ob}(\mathbf{C}).$$

Compatibility means that certain diagrams, for example,

$$\begin{array}{ccccc} U \otimes (V \otimes W) & \xrightarrow{\phi_{U,V,W}} & (U \otimes V) \otimes W & \xrightarrow{\psi_{U \otimes V, W}} & W \otimes (U \otimes V) \\ \downarrow \text{id}_U \otimes \psi_{V,W} & & & & \downarrow \phi_{W,U,V} \\ U \otimes (W \otimes V) & \xrightarrow{\phi_{U,W,V}} & (U \otimes W) \otimes V & \xrightarrow{\psi_{U,W} \otimes \text{id}_V} & (W \otimes U) \otimes V, \end{array}$$

commute, and that there exists a neutral object (tensor product of the empty set), i.e., an object U together with an isomorphism $u: U \rightarrow U \otimes U$ such that $V \mapsto V \otimes U$ is an equivalence of categories. For a complete definition, see Deligne and Milne 1982, §1. We use $\mathbf{1}$ to denote a neutral object of \mathbf{C} .

21.3 An object of a tensor category is *trivial* if it is isomorphic to a direct sum of neutral objects.

EXAMPLE 21.4 The category of finitely generated modules over a ring R becomes a tensor category with the usual tensor product and the constraints

$$\left. \begin{aligned} u \otimes (v \otimes w) &\mapsto (u \otimes v) \otimes w: & U \otimes (V \otimes W) &\rightarrow (U \otimes V) \otimes W \\ v \otimes w &\rightarrow w \otimes v: & V \otimes W &\rightarrow W \otimes V. \end{aligned} \right\} \quad (125)$$

Any free R -module U of rank one together with an isomorphism $U \rightarrow U \otimes U$ (equivalently, the choice of a basis for U) is a neutral object. It is trivial to check the compatibility conditions for this to be a tensor category.

EXAMPLE 21.5 The category of finite-dimensional representations of a Lie algebra or of an algebraic (or affine) group G with the usual tensor product and the constraints (125) is a tensor category. The required commutativities follow immediately from (21.4).

21.6 Let (\mathbf{C}, \otimes) and (\mathbf{C}', \otimes) be tensor categories over k . A *tensor functor* $\mathbf{C} \rightarrow \mathbf{C}'$ is a pair (F, c) consisting of a functor $F: \mathbf{C} \rightarrow \mathbf{C}'$ and a natural isomorphism $c_{V,W}: F(V) \otimes F(W) \rightarrow F(V \otimes W)$ compatible the associativity and commutativity constraints and sending neutral objects to a neutral objects. Then F commutes with finite tensor products up to a well-defined isomorphism. See Deligne and Milne 1982, 1.8.

21.7 Let \mathbf{C} be a tensor category over k , and let V be an object of \mathbf{C} . A pair

$$(V^\vee, V^\vee \otimes V \xrightarrow{\text{ev}} \mathbf{1})$$

is called a *dual* of V if there exists a morphism $\delta_V: \mathbf{1} \rightarrow V \otimes V^\vee$ such that the composites

$$\begin{array}{ccccc} V & \xrightarrow{\delta_V \otimes V} & V \otimes V^\vee \otimes V & \xrightarrow{V \otimes \text{ev}} & V \\ V^\vee & \xrightarrow{V^\vee \otimes \delta_V} & V^\vee \otimes V \otimes V^\vee & \xrightarrow{\text{ev} \otimes V^\vee} & V^\vee \end{array}$$

are the identity morphisms on V and V^\vee respectively. Then δ_V is uniquely determined, and the dual (V^\vee, ev) of V is uniquely determined up to a unique isomorphism. For example, a finite-dimensional k -vector space V has as dual $V^\vee \stackrel{\text{def}}{=} \text{Hom}_k(V, k)$ with $\text{ev}(f \otimes v) = f(v)$ — here δ_V is the k -linear map sending 1 to $\sum e_i \otimes f_i$ for any basis (e_i) for V and its dual basis (f_i) . More generally, a module M over a ring admits a dual if and only if M is finitely generated and projective (CA 10.9, 10.10). Similarly, the contragredient of a representation of a Lie algebra or of an algebraic group is a dual of the representation.

21.8 A tensor category is *rigid* if every object admits a dual. For example, the category Vec_k of finite-dimensional vector spaces over k and the category of finite-dimensional representations of a Lie algebra (or an algebraic group) are rigid.

21b Neutral tannakian categories

21.9 A *neutral tannakian category* over k is an abelian k -linear category \mathbf{C} endowed with a rigid tensor structure for which there exists an exact tensor functor $\omega: \mathbf{C} \rightarrow \mathbf{Vec}_k$. Such a functor ω is called a *fibre functor* over k .

We refer to a pair (\mathbf{C}, ω) consisting of a tannakian category over k and a fibre functor over k as a neutral tannakian category.

THEOREM 21.10 *Let (\mathbf{C}, ω) be a neutral tannakian category over k . For each k -algebra R , let $G(R)$ be the set of families*

$$\lambda = (\lambda_V)_{V \in \text{ob}(\mathbf{C})}, \quad \lambda_V \in \text{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

- ◇ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ for all $V, W \in \text{ob}(\mathbf{C})$,
- ◇ $\lambda_{\mathbf{1}} = \text{id}_{\omega(\mathbf{1})}$ for every neutral object of $\mathbf{1}$ of \mathbf{C} , and
- ◇ $\lambda_W \circ \alpha_R = \alpha_R \circ \lambda_V$ for all arrows $\alpha: V \rightarrow W$ in \mathbf{C} .

Then $R \rightsquigarrow G(R)$ is an affine group over k , and ω defines an equivalence of tensor categories over k ,

$$\mathbf{C} \rightarrow \text{Rep}(G).$$

PROOF. This is a restatement of Theorem 11.14. □

21.11 Let ω_R be the functor $V \rightsquigarrow \omega(V) \otimes R$; then $G(R)$ consists of the natural transformations $\lambda: \omega_R \rightarrow \omega_R$ such that the following diagrams commute

$$\begin{array}{ccc} \omega_R(V) \otimes \omega_R(W) & \xrightarrow{c_{V,W}} & \omega_R(V \otimes W) & \omega_R(\mathbf{1}) & \xrightarrow{\omega_R(u)} & \omega_R(\mathbf{1} \otimes \mathbf{1}) \\ \downarrow \lambda_V \otimes \lambda_W & & \downarrow \lambda_{V \otimes W} & \downarrow \lambda_{\mathbf{1}} & & \downarrow \lambda_{\mathbf{1} \otimes \mathbf{1}} \\ \omega_R(V) \otimes \omega_R(W) & \xrightarrow{c_{V,W}} & \omega_R(V \otimes W) & \omega_R(\mathbf{1}) & \xrightarrow{\omega_R(u)} & \omega_R(\mathbf{1} \otimes \mathbf{1}) \end{array}$$

for all objects V, W of \mathbf{C} and all identity objects $(\mathbf{1}, u)$.

21.12 I explain the final statement of (21.10). For each V in \mathbf{C} , there is a representation $r_V: G \rightarrow \text{GL}_{\omega(V)}$ defined by

$$r_V(g)v = \lambda_V(v) \text{ if } g = (\lambda_V) \in G(R) \text{ and } v \in V(R).$$

The functor sending V to $\omega(V)$ endowed with this action of G is an equivalence of categories $\mathbf{C} \rightarrow \text{Rep}(G)$.

21.13 A tannakian category \mathbf{C} is said to be *algebraic* if there exists an object V such that every other object is a subquotient of $P(V, V^\vee)$ for some $P \in \mathbb{N}[X, Y]$. If G is an algebraic group, then (8.31) and (8.44) show that $\text{Rep}(G)$ is algebraic. Conversely, if $\text{Rep}(G)$ is algebraic, with generator V , then G is algebraic because $G \subset \text{GL}_V$.

21.14 It is usual to write $\underline{\text{Aut}}^{\otimes}(\omega)$ (functor of tensor automorphisms of ω) for the affine group G attached to the neutral tannakian category (\mathbf{C}, ω) — we call it the *Tannaka dual* or *Tannaka group* of (\mathbf{C}, ω) . We sometimes denote it by $\pi(\mathbf{C}, \omega)$.

EXAMPLE 21.15 If \mathbf{C} is the category of finite-dimensional representations of an algebraic group H over k and ω is the forgetful functor, then $G(R) \simeq H(R)$ by (10.2), and $\mathbf{C} \rightarrow \text{Rep}(G)$ is the identity functor.

EXAMPLE 21.16 Let N be a normal subgroup of an algebraic group G , and let \mathbf{C} be the subcategory of $\text{Rep}(G)$ consisting of the representations of G on which N acts trivially. The group attached to \mathbf{C} and the forgetful functor is G/N (alternatively, this can be used as a definition of G/N).

21.17 Let (\mathbf{C}, ω) and (\mathbf{C}', ω') be neutral tannakian categories with Tannaka duals G and G' . An exact tensor functor $F: \mathbf{C} \rightarrow \mathbf{C}'$ such that $\omega' \circ F = \omega$ defines a homomorphism $G' \rightarrow G$, namely,

$$(\lambda_V)_{V \in \text{ob}(\mathbf{C}')} \mapsto (\lambda_{FV})_{V \in \text{ob}(\mathbf{C})}: G'(R) \rightarrow G(R).$$

21.18 Let $\mathbf{C} = \text{Rep}(G)$ for some algebraic group G .

- (a) For an algebraic subgroup H of G , let \mathbf{C}^H denote the full subcategory of \mathbf{C} whose objects are those on which H acts trivially. Then \mathbf{C}^H is a neutral tannakian category whose Tannaka dual is G/N where N is the smallest normal algebraic subgroup of G containing H (intersection of the normal algebraic subgroups containing H).
- (b) (*Tannaka correspondence.*) For a collection S of objects of $\mathbf{C} = \text{Rep}(G)$, let $H(S)$ denote the largest subgroup of G acting trivially on all V in S ; thus

$$H(S) = \bigcap_{V \in S} \text{Ker}(r_V: G \rightarrow \text{Aut}(V)).$$

Then the maps $S \mapsto H(S)$ and $H \mapsto \mathbf{C}^H$ form a Galois correspondence

$$\{\text{subsets of } \text{ob}(\mathbf{C})\} \rightleftarrows \{\text{algebraic subgroups of } G\},$$

i.e., both maps are order reversing and $\mathbf{C}^{H(S)} \supset S$ and $H(\mathbf{C}^H) \supset H$ for all S and H . It follows that the maps establish a one-to-one correspondence between their respective images. In this way, we get a natural one-to-one order-reversing correspondence

$$\{\text{tannakian subcategories of } \mathbf{C}\} \xleftrightarrow{1:1} \{\text{normal algebraic subgroups of } G\}$$

(a tannakian subcategory is a full subcategory closed under the formation of duals, tensor products, direct sums, and subquotients).

21c Gradations on tensor categories

21.19 Let M be a finitely generated abelian group. An M -*gradation* on an object X of an abelian category is a family of subobjects $(X^m)_{m \in M}$ such that $X = \bigoplus_{m \in M} X^m$. An M -*gradation* on a tensor category \mathbf{C} is an M -gradation on each object X of \mathbf{C} compatible with all arrows in \mathbf{C} and with tensor products in the sense that $(X \otimes Y)^m = \bigoplus_{r+s=m} X^r \otimes Y^s$.

Let (\mathbf{C}, ω) be a neutral tannakian category, and let G be its Tannaka dual. To give an M -gradation on \mathbf{C} is the same as to give a central homomorphism $D(M) \rightarrow G(\omega)$: a homomorphism corresponds to the M -gradation such that X^m is the subobject of X on which $D(M)$ acts through the character m (Saavedra Rivano 1972; Deligne and Milne 1982, §5).

21.20 Let \mathbf{C} be a semisimple k -linear tensor category such that $\text{End}(X) = k$ for every simple object X in \mathbf{C} , and let $I(\mathbf{C})$ be the set of isomorphism classes of simple objects in \mathbf{C} . For elements x, x_1, \dots, x_m of $I(\mathbf{C})$ represented by simple objects X, X_1, \dots, X_m , write $x < x_1 \otimes \dots \otimes x_m$ if X is a direct factor of $X_1 \otimes \dots \otimes X_m$. The following statements are obvious.

- (a) Let M be a commutative group. To give an M -gradation on \mathbf{C} is the same as to give a map $f: I(\mathbf{C}) \rightarrow M$ such that

$$x < x_1 \otimes x_2 \implies f(x) = f(x_1) + f(x_2).$$

A map from $I(\mathbf{C})$ to a commutative group satisfying this condition will be called a **tensor map**. For such a map, $f(\mathbb{1}) = 0$, and if X has dual X^\vee , then $f([X^\vee]) = -f([X])$.

- (b) Let $M(\mathbf{C})$ be the free abelian group with generators the elements of $I(\mathbf{C})$ modulo the relations: $x = x_1 + x_2$ if $x < x_1 \otimes x_2$. The obvious map $I(\mathbf{C}) \rightarrow M(\mathbf{C})$ is a universal tensor map, i.e., it is a tensor map, and every other tensor map $I(\mathbf{C}) \rightarrow M$ factors uniquely through it. Note that $I(\mathbf{C}) \rightarrow M(\mathbf{C})$ is surjective.

21.21 Let (\mathbf{C}, ω) be a neutral tannakian category such that \mathbf{C} is semisimple and $\text{End}(V) = k$ for every simple object in \mathbf{C} . Let Z be the centre of $G \stackrel{\text{def}}{=} \underline{\text{Aut}}^\otimes(\omega)$. Because \mathbf{C} is semisimple, G° is reductive (II, 6.17), and so Z is of multiplicative type. Assume (for simplicity) that Z is split, so that $Z = D(N)$ with N the group of characters of Z . According to (21.19), to give an M -gradation on \mathbf{C} is the same as giving a homomorphism $D(M) \rightarrow Z$, or, equivalently, a homomorphism $N \rightarrow M$. On the other hand, (21.20) shows that to give an M -gradation on \mathbf{C} is the same as giving a homomorphism $M(\mathbf{C}) \rightarrow M$. Therefore $M(\mathbf{C}) \simeq N$. In more detail: let X be an object of \mathbf{C} ; if X is simple, then Z acts on X through a character n of Z , and the tensor map $[X] \mapsto n: I(\mathbf{C}) \rightarrow N$ is universal.

21.22 Let (\mathbf{C}, ω) be as in (21.21), and define an equivalence relation on $I(\mathbf{C})$ by

$$a \sim a' \iff \text{there exist } x_1, \dots, x_m \in I(\mathbf{C}) \text{ such that } a, a' < x_1 \otimes \dots \otimes x_m.$$

A function f from $I(\mathbf{C})$ to a commutative group defines a gradation on \mathbf{C} if and only if $f(a) = f(a')$ whenever $a \sim a'$. Therefore, $M(\mathbf{C}) \simeq I(\mathbf{C})/\sim$.

ASIDE 21.23 Discuss the prehistory: Tannaka (cf. Serre 1973, p. 71, remark), Krein (cf. Breen), Chevalley (book), Hochschild and Mostow 1969, §4 (AJM 91, 1127–1140).

EXERCISES

EXERCISE 21-1 Use the criterion (12.19) to show that the centralizer of a torus in a connected algebraic group is connected.

Lie Algebras and Algebraic Groups

The Lie algebra of an algebraic group is the (first) linear approximation to the group. The study of Lie algebras is much more elementary than that of algebraic groups. For example, most of the results on Lie algebras that we shall need are proved already in the undergraduate text Erdmann and Wildon 2006.

Throughout this chapter k is a field.

NOTES Most sections in this chapter are complete, but need to be revised (especially Section 4, which, however, can be skipped).

1	The Lie algebra of an algebraic group	239
2	Lie algebras and algebraic groups	255
3	Nilpotent and solvable Lie algebras	264
4	Unipotent algebraic groups and nilpotent Lie algebras	273
5	Semisimple Lie algebras and algebraic groups	277
6	Semisimplicity of representations	287

1 The Lie algebra of an algebraic group

An algebraic group is a functor $R \rightsquigarrow G(R): \text{Alg}_k \rightarrow \text{Grp}$. The Lie algebra of G depends only on the value of the functor on the k -algebra of dual numbers, but it nevertheless contains a surprisingly large amount of information about the group, especially in characteristic zero.

1a Lie algebras: basic definitions

DEFINITION 1.1 A *Lie algebra*¹ over a field k is a vector space \mathfrak{g} over k together with a k -bilinear map

$$[\ , \]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$$

(called the *bracket*) such that

¹Bourbaki LIE, Historical Notes to Chapter I to III writes:

The term “Lie algebra” was introduced by H. Weyl in 1934; in his work of 1925, he had used the expression “infinitesimal group”. Earlier mathematicians had spoken simply of the “infinitesimal transformations $X_1 f, \dots, X_r f$ ” of the group, which Lie and Engel frequently abbreviated by saying “the group $X_1 f, \dots, X_r f$ ”.

- (a) $[x, x] = 0$ for all $x \in \mathfrak{g}$,
 (b) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in \mathfrak{g}$.

A **homomorphism of Lie algebras** is a k -linear map $\alpha: \mathfrak{g} \rightarrow \mathfrak{g}'$ such that

$$\alpha([x, y]) = [\alpha(x), \alpha(y)] \quad \text{for all } x, y \in \mathfrak{g}.$$

A **Lie subalgebra** of a Lie algebra \mathfrak{g} is a k -subspace \mathfrak{s} such that $[x, y] \in \mathfrak{s}$ whenever $x, y \in \mathfrak{s}$ (i.e., such that $[\mathfrak{s}, \mathfrak{s}] \subset \mathfrak{s}$).

Condition (b) is called the **Jacobi identity**. Note that (a) applied to $[x + y, x + y]$ shows that the Lie bracket is skew-symmetric,

$$[x, y] = -[y, x], \text{ for all } x, y \in \mathfrak{g}, \quad (126)$$

and that (126) allows the Jacobi identity to be rewritten as

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]] \quad (127)$$

or

$$[[x, y], z] = [x, [y, z]] - [y, [x, z]] \quad (128)$$

An injective homomorphism is sometimes called an **embedding**, and a surjective homomorphism is sometimes called a **quotient map**.

We shall be mainly concerned with finite-dimensional Lie algebras.

EXAMPLE 1.2 For any associative k -algebra A , the bracket $[a, b] = ab - ba$ is k -bilinear. It makes A into a Lie algebra because $[a, a]$ is obviously 0 and the Jacobi identity can be proved by a direct calculation. In fact, on expanding out the left side of the Jacobi identity for a, b, c one obtains a sum of 12 terms, 6 with plus signs and 6 with minus signs; by symmetry, each permutation of a, b, c must occur exactly once with a plus sign and exactly once with a minus sign. When A is the endomorphism ring $\text{End}_{k\text{-lin}}(V)$ of a k -vector space V , this Lie algebra is denoted \mathfrak{gl}_V , and when $A = M_n(k)$, it is denoted \mathfrak{gl}_n . Let e_{ij} be the matrix with 1 in the ij th position and 0 elsewhere. These matrices form a basis for \mathfrak{gl}_n , and

$$[e_{ij}, e_{i'j'}] = \delta_{ji'}e_{ij'} - \delta_{ij'}e_{i'j} \quad (\delta_{ij} = \text{Kronecker delta}).$$

EXAMPLE 1.3 Let A be a k -algebra (not necessarily associative). A **derivation** of A is a k -linear map $D: A \rightarrow A$ such that

$$D(ab) = D(a)b + aD(b) \text{ for all } a, b \in A.$$

The composite of two derivations need not be a derivation, but their bracket

$$[D, E] \stackrel{\text{def}}{=} D \circ E - E \circ D$$

is, and so the set of k -derivations $A \rightarrow A$ is a Lie subalgebra $\text{Der}_k(A)$ of \mathfrak{gl}_A .

EXAMPLE 1.4 For $x \in \mathfrak{g}$, let $\text{ad}_{\mathfrak{g}} x$ (or $\text{ad} x$) denote the map $y \mapsto [x, y]: \mathfrak{g} \rightarrow \mathfrak{g}$. Then $\text{ad}_{\mathfrak{g}} x$ is a k -derivation because (127) can be rewritten as

$$\text{ad}(x)[y, z] = [\text{ad}(x)y, z] + [y, \text{ad}(x)z].$$

In fact, $\text{ad}_{\mathfrak{g}}$ is a homomorphism of Lie algebras $\mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$ because (128) can be rewritten as

$$\text{ad}([x, y])z = \text{ad}(x)(\text{ad}(y)z) - \text{ad}(y)(\text{ad}(x)z).$$

The kernel of $\text{ad}_{\mathfrak{g}}: \mathfrak{g} \rightarrow \text{Der}_k(\mathfrak{g})$ is the *centre* of \mathfrak{g} ,

$$z(\mathfrak{g}) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid [x, \mathfrak{g}] = 0\}.$$

The derivations of \mathfrak{g} of the form $\text{ad} x$ are said to be *inner* (by analogy with the automorphisms of a group of the form $\text{inn } g$).

1b The isomorphism theorems

An *ideal* in a Lie algebra \mathfrak{g} is a subspace \mathfrak{a} such that $[x, a] \in \mathfrak{a}$ for all $x \in \mathfrak{g}$ and $a \in \mathfrak{a}$ (i.e., such that $[\mathfrak{g}, \mathfrak{a}] \subset \mathfrak{a}$). When \mathfrak{a} is an ideal, the quotient vector space $\mathfrak{g}/\mathfrak{a}$ becomes a Lie algebra with the bracket

$$[x + \mathfrak{a}, y + \mathfrak{a}] = [x, y] + \mathfrak{a}.$$

The following statements are straightforward consequences of the similar statements for vector spaces.

1.5 (Existence of quotients). The kernel of a homomorphism $\mathfrak{g} \rightarrow \mathfrak{q}$ of Lie algebras is an ideal, and every ideal \mathfrak{a} is the kernel of a quotient map $\mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{a}$.

1.6 (Homomorphism theorem). The image of a homomorphism $\alpha: \mathfrak{g} \rightarrow \mathfrak{g}'$ of Lie algebras is a Lie subalgebra $\alpha\mathfrak{g}$ of \mathfrak{g}' , and α defines an isomorphism of $\mathfrak{g}/\text{Ker}(\alpha)$ onto $\alpha\mathfrak{g}$; in particular, every homomorphism of Lie algebras is the composite of a surjective homomorphism with an injective homomorphism.

1.7 (Isomorphism theorem). Let \mathfrak{h} and \mathfrak{a} be Lie subalgebras of \mathfrak{g} such that $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$; then $\mathfrak{h} + \mathfrak{a}$ is a Lie subalgebra of \mathfrak{g} , $\mathfrak{h} \cap \mathfrak{a}$ is an ideal in \mathfrak{h} , and the map

$$x + \mathfrak{h} \cap \mathfrak{a} \mapsto x + \mathfrak{a}: \mathfrak{h}/\mathfrak{h} \cap \mathfrak{a} \rightarrow (\mathfrak{h} + \mathfrak{a})/\mathfrak{a}$$

is an isomorphism.

1.8 (Correspondence theorem). Let \mathfrak{a} be an ideal in a Lie algebra \mathfrak{g} . The map $\mathfrak{h} \mapsto \mathfrak{h}/\mathfrak{a}$ is a one-to-one correspondence between the set of Lie subalgebras of \mathfrak{g} containing \mathfrak{a} and the set of Lie subalgebras of $\mathfrak{g}/\mathfrak{a}$. A Lie subalgebra \mathfrak{h} containing \mathfrak{a} is an ideal if and only if $\mathfrak{h}/\mathfrak{a}$ is an ideal in $\mathfrak{g}/\mathfrak{a}$, in which case the map

$$\mathfrak{g}/\mathfrak{h} \rightarrow (\mathfrak{g}/\mathfrak{a})/(\mathfrak{h}/\mathfrak{a})$$

is an isomorphism

1c The Lie algebra of an algebraic group

Let G be an algebraic group over a field k , and let $k[\varepsilon]$ be the ring of *dual numbers*:

$$k[\varepsilon] \stackrel{\text{def}}{=} k[X]/(X^2).$$

Thus $k[\varepsilon] = k \oplus k\varepsilon$ as a k -vector space and $\varepsilon^2 = 0$. There is a homomorphism

$$\pi: k[\varepsilon] \longrightarrow k, \quad \pi(a + \varepsilon b) = a.$$

DEFINITION 1.9 For an algebraic group G over k ,

$$\text{Lie}(G) = \text{Ker}(G(k[\varepsilon]) \xrightarrow{\pi} G(k)).$$

Following a standard convention, we often write \mathfrak{g} for $\text{Lie}(G)$, \mathfrak{h} for $\text{Lie}(H)$, and so on.

EXAMPLE 1.10 Let $G = \text{GL}_n$, and let I_n be the identity $n \times n$ matrix. An $n \times n$ matrix A gives an element $I_n + \varepsilon A$ of $M_n(k[\varepsilon])$, and

$$(I_n + \varepsilon A)(I_n - \varepsilon A) = I_n;$$

therefore $I_n + \varepsilon A \in \text{Lie}(\text{GL}_n)$. Clearly every element of $\text{Lie}(\text{GL}_n)$ is of this form, and so the map

$$A \mapsto E(A) \stackrel{\text{def}}{=} I_n + \varepsilon A: M_n(k) \rightarrow \text{Lie}(\text{GL}_n)$$

is a bijection. Note that

$$\begin{aligned} E(A)E(B) &= (I_n + \varepsilon A)(I_n + \varepsilon B) \\ &= I_n + \varepsilon(A + B) \\ &= E(A + B). \end{aligned}$$

In the language of algebraic geometry, $\text{Lie}(G)$ is the tangent space to $|G|$ at 1_G (see CA §18).

PROPOSITION 1.11 Let I_G be the augmentation ideal in $\mathcal{O}(G)$, i.e., $I_G = \text{Ker}(\epsilon: \mathcal{O}(G) \rightarrow k)$. Then

$$\text{Lie}(G) \simeq \text{Hom}_{k\text{-lin}}(I_G/I_G^2, k). \quad (129)$$

PROOF. By definition, an element x of $\text{Lie}(G)$ gives a commutative diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{x} & k[\varepsilon] \\ \downarrow \epsilon & & \downarrow \pi \\ k & \xlongequal{\quad} & k, \end{array}$$

and hence a homomorphism $I_G \rightarrow \text{Ker}(\pi) \simeq k$ on the kernels. That this induces an isomorphism (129) is proved in CA 18.9. \square

From (129), we see that $\text{Lie}(G)$ has the structure of k -vector space, and that Lie is a functor from the category of algebraic groups over k to k -vector spaces.

THEOREM 1.12 *There is a unique way of making $G \rightsquigarrow \text{Lie}(G)$ into a functor to Lie algebras such that $\text{Lie}(\text{GL}_n) = \mathfrak{gl}_n$ (as Lie algebras).*

Without the condition on $\text{Lie}(\text{GL}_n)$, we could, for example, take the bracket to be zero. It is clear from the definition of the Lie algebra that an embedding of algebraic groups $G \hookrightarrow H$ defines an injection $\text{Lie } G \rightarrow \text{Lie } H$ of k -vector spaces. On applying this remark to an embedding of G into GL_n , we obtain the uniqueness assertion. The existence assertion will be proved later in this section.

REMARK 1.13 If $a \neq 0$, then $a + b\varepsilon = a(1 + \frac{b}{a}\varepsilon)$ has inverse $a^{-1}(1 - \frac{b}{a}\varepsilon)$ in $k[\varepsilon]$, and so

$$k[\varepsilon]^\times = \{a + b\varepsilon \mid a \neq 0\}.$$

An element of $\text{Lie}(G)$ is a k -algebra homomorphism $\alpha: \mathcal{O}(G) \rightarrow k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0$ is ϵ . Therefore, elements of $\mathcal{O}(G)$ not in the kernel \mathfrak{m} of ϵ map to units in $k[\varepsilon]$, and so α factors uniquely through the local ring $\mathcal{O}(G)_{\mathfrak{m}}$. This shows that $\text{Lie}(G)$ depends only on $\mathcal{O}(G)_{\mathfrak{m}}$. In particular, $\text{Lie}(G^\circ) \simeq \text{Lie}(G)$.

REMARK 1.14 There is a more direct way of defining the action of k on $\text{Lie}(G)$: an element $c \in k$ defines a homomorphism of k -algebras

$$u_c: k[\varepsilon] \rightarrow k[\varepsilon], \quad u_c(a + \varepsilon b) = a + c\varepsilon b$$

such that $\pi \circ u_c = \pi$, and hence a commutative diagram

$$\begin{array}{ccc} G(k[\varepsilon]) & \xrightarrow{G(u_c)} & G(k[\varepsilon]) \\ \downarrow G(\pi) & & \downarrow G(\pi) \\ G(k) & \xrightarrow{\text{id}} & G(k), \end{array}$$

which induces a homomorphism of groups $\text{Lie}(G) \rightarrow \text{Lie}(G)$. For example, when $G = \text{GL}_n$,

$$G(u_c)E(A) = G(u_c)(I_n + \varepsilon A) = I_n + c\varepsilon A = E(cA).$$

This defines a k -vector space structure on $\text{Lie } G$, which agrees that given by (129).

NOTES The definition (1.9) is valid for any functor $G: \text{Alg}_k \rightarrow \text{Grp}$. See DG II, §4, 1.

1d Examples

1.15 By definition

$$\text{Lie}(\text{SL}_n) = \{I + A\varepsilon \in M_n(k[\varepsilon]) \mid \det(I + A\varepsilon) = 1\}.$$

When we expand $\det(I + \varepsilon A)$ as a sum of $n!$ products, the only nonzero term is

$$\prod_{i=1}^n (1 + \varepsilon a_{ii}) = 1 + \varepsilon \sum_{i=1}^n a_{ii},$$

because every other term includes at least two off-diagonal entries. Hence

$$\det(I + \varepsilon A) = 1 + \varepsilon \text{trace}(A)$$

and so

$$\begin{aligned}\mathfrak{sl}_n &\stackrel{\text{def}}{=} \text{Lie}(\text{SL}_n) = \{I + \varepsilon A \mid \text{trace}(A) = 0\} \\ &\simeq \{A \in M_n(k) \mid \text{trace}(A) = 0\}.\end{aligned}$$

For $n \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$,

$$\text{trace}(AB) = \sum_{1 \leq i, j \leq n} a_{ij} b_{ji} = \text{trace}(BA). \quad (130)$$

Therefore $[A, B] = AB - BA$ has trace zero, and \mathfrak{sl}_n is a Lie subalgebra of \mathfrak{gl}_n .

1.16 Recall (I, §1) that \mathbb{T}_n (resp. \mathbb{U}_n , resp. \mathbb{D}_n) is the group of upper triangular (resp. upper triangular with 1s on the diagonal, resp. diagonal) invertible matrices. As

$$\text{Lie}(\mathbb{T}_n) = \left\{ \begin{pmatrix} 1 + \varepsilon c_{11} & \varepsilon c_{12} & \cdots & \varepsilon c_{1n-1} & \varepsilon c_{1n} \\ 0 & 1 + \varepsilon c_{22} & \cdots & \varepsilon c_{2n-1} & \varepsilon c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 + \varepsilon c_{n-1n-1} & \varepsilon c_{n-1n} \\ 0 & 0 & \cdots & 0 & 1 + \varepsilon c_{nn} \end{pmatrix} \right\},$$

we see that

$$\mathfrak{b}_n \stackrel{\text{def}}{=} \text{Lie}(\mathbb{T}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i > j\} \quad (\text{upper triangular matrices}).$$

Similarly,

$$\mathfrak{n}_n \stackrel{\text{def}}{=} \text{Lie}(\mathbb{U}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\} \quad (\text{strictly upper triangular matrices})$$

$$\mathfrak{d}_n \stackrel{\text{def}}{=} \text{Lie}(\mathbb{D}_n) \simeq \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \neq j\} \quad (\text{diagonal matrices}).$$

These are Lie subalgebras of \mathfrak{gl}_n .

1.17 Assume that the characteristic $\neq 2$, and let O_n be orthogonal group:

$$O_n = \{A \in \text{GL}_n \mid A^t \cdot A = I\} \quad (A^t = \text{transpose of } A).$$

For $I + \varepsilon A \in M_n(k[\varepsilon])$,

$$(I + \varepsilon A)^t \cdot (I + \varepsilon A) = (I + \varepsilon A^t) \cdot (I + \varepsilon A) = I + \varepsilon A^t + \varepsilon A,$$

and so

$$\begin{aligned}\text{Lie}(O_n) &= \{I + \varepsilon A \in M_n(k[\varepsilon]) \mid A^t + A = 0\} \\ &\simeq \{A \in M_n(k) \mid A \text{ is skew symmetric}\}.\end{aligned}$$

Similarly, $\text{Lie}(\text{SO}_n)$ consists of the skew symmetric matrices with trace zero, but obviously the second condition is redundant, and so

$$\text{Lie}(\text{SO}_n) = \text{Lie}(O_n).$$

This also follows from the fact that $\text{SO}_n = O_n^\circ$ (see 1.13).

1.18 Let G be a finite étale algebraic group. Then $\mathcal{O}(G)$ is a separable k -algebra, and every quotient of $\mathcal{O}(G)$ is separable (I, 12.4). The only separable subalgebra of $k[\varepsilon]$ is k , and so $G(k[\varepsilon]) = G(k)$ and $\text{Lie}(G) = 0$. This also follows from the fact that

$$\text{Lie}(G) = \text{Lie}(G^\circ) = \text{Lie}(1) = 0$$

(see 1.13).

1.19 Let k have characteristic $p \neq 0$, and let $G = \alpha_p$, so that $\alpha_p(R) = \{r \in R \mid r^p = 0\}$ (see I, 3.5). Then $\alpha_p(k) = \{0\}$ and $\alpha_p(k[\varepsilon]) = \{a\varepsilon \mid a \in k\}$. Therefore,

$$\text{Lie}(\alpha_p) = \{a\varepsilon \mid a \in k\} \simeq k.$$

Similarly,

$$\text{Lie}(\mu_p) = \{1 + a\varepsilon \mid a \in k\} \simeq k.$$

As the bracket on a one-dimensional Lie algebra must be trivial, this shows that α_p and μ_p have the same Lie algebra.

1.20 Let V be a vector space over k . Every element of $V(\varepsilon) \stackrel{\text{def}}{=} k[\varepsilon] \otimes_k V$ can be written uniquely in the form $x + \varepsilon y$ with $x, y \in V$, i.e., $V(\varepsilon) = V \oplus \varepsilon V$. The $k[\varepsilon]$ -linear maps $V(\varepsilon) \rightarrow V(\varepsilon)$ are the maps $\alpha + \varepsilon\beta$, $\alpha, \beta \in \text{End}_{k\text{-lin}}(V)$, where

$$(\alpha + \varepsilon\beta)(x + \varepsilon y) = \alpha(x) + \varepsilon(\alpha(y) + \beta(x)). \quad (131)$$

To see this, note that $\text{End}_{k\text{-lin}}(V(\varepsilon)) \simeq M_2(\text{End}_{k\text{-lin}}(V))$, and that ε acts as $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\text{End}_k(V))$. Thus

$$\begin{aligned} \text{End}_{k[\varepsilon]\text{-lin}}(V(\varepsilon)) &= \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\text{End}_k(V)) \mid \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} \alpha & 0 \\ \beta & \alpha \end{pmatrix} \in M_2(\text{End}_k(V)) \right\}. \end{aligned}$$

It follows that

$$\text{GL}_V(k[\varepsilon]) = \{\alpha + \varepsilon\beta \mid \alpha \text{ invertible}\}$$

and that

$$\text{Lie}(\text{GL}_V) = \{\text{id}_V + \varepsilon\alpha \mid \alpha \in \text{End}(V)\} \simeq \text{End}(V) = \mathfrak{gl}_V.$$

1.21 Let V be a finite-dimensional k -vector space, and let $D_a(V)$ denote the algebraic group $R \rightsquigarrow \text{Hom}_{k\text{-lin}}(V, R)$ (see I, 3.6). Then

$$\text{Lie}(D_a(V)) \simeq \text{Hom}_{k\text{-lin}}(V, k)$$

(as a k -vector space). Similarly,

$$\text{Lie}(V_a) \simeq V.$$

1.22 Let $\phi: V \times V \rightarrow k$ be a k -bilinear form, and let G be the subgroup of GL_V of α preserving the form, i.e., such that

$$G(R) = \{\alpha \in \text{GL}_V(R) \mid \phi(\alpha x, \alpha x') = \phi(x, x') \text{ for all } x, x' \in V(R)\}.$$

Then $\text{Lie}(G)$ consists of the endomorphisms $\text{id} + \varepsilon\alpha$ of $V(\varepsilon)$ such that

$$\phi((\text{id} + \varepsilon\alpha)(x + \varepsilon y), (\text{id} + \varepsilon\alpha)(x' + \varepsilon y')) = \phi(x + \varepsilon y, x' + \varepsilon y'), \quad \text{all } x, y, x', y' \in V.$$

The left hand side equals

$$\phi(x + \varepsilon y + \varepsilon \cdot \alpha x, x' + \varepsilon y' + \varepsilon \cdot \alpha x') = \phi(x + \varepsilon y, x' + \varepsilon y') + \varepsilon(\phi(\alpha x, x') + \phi(x, \alpha x')),$$

and so

$$\text{Lie}(G) \simeq \{\alpha \in \text{End}_{k\text{-lin}}(V) \mid \phi(\alpha x, x') + \phi(x, \alpha x') = 0 \text{ all } x, x' \in V\}.$$

1.23 Let G be the unitary group defined by a quadratic extension K of k (I, 3.11). The Lie algebra of G consists of the $A \in M_n(K)$ such that

$$(I + \varepsilon A)^*(I + \varepsilon A) = I$$

i.e., such that

$$A^* + A = 0.$$

Note that this is *not* a K -vector space, reflecting the fact that G is an algebraic group over k , not K .

1.24 Let $G = D(M)$ (see I, §14c), so that $G(R) = \text{Hom}(M, R^\times)$ (homomorphisms of abelian groups). On applying $\text{Hom}(M, -)$ to the split-exact sequence of commutative groups

$$0 \longrightarrow k \xrightarrow{a \mapsto 1+a\varepsilon} k[\varepsilon]^\times \xrightarrow{\varepsilon \mapsto 0} k^\times \longrightarrow 0,$$

we find that

$$\text{Lie}(G) \simeq \text{Hom}(M, k) \simeq \text{Hom}(M, \mathbb{Z}) \otimes_{\mathbb{Z}} k.$$

A split torus T is the diagonalizable group associated with $M = X(T)$. For such a group,

$$\text{Lie}(T) \simeq \text{Hom}(X(T), \mathbb{Z}) \otimes_{\mathbb{Z}} k$$

and

$$\text{Hom}_{k\text{-lin}}(\text{Lie}(T), k) \simeq k \otimes_{\mathbb{Z}} X(T).$$

1e Description of $\text{Lie}(G)$ in terms of derivations

DEFINITION 1.25 Let A be a k -algebra and M an A -module. A k -linear map $D: A \rightarrow M$ is a k -*derivation* of A into M if

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad (\text{Leibniz rule}).$$

For example, $D(1) = D(1 \times 1) = D(1) + D(1)$ and so $D(1) = 0$. By k -linearity, this implies that

$$D(c) = 0 \text{ for all } c \in k. \quad (132)$$

Conversely, every additive map $A \rightarrow M$ satisfying the Leibniz rule and zero on k is a k -derivation.

Let $\alpha: A \rightarrow k[\varepsilon]$ be a k -linear map, and write

$$\alpha(f) = \alpha_0(f) + \varepsilon\alpha_1(f).$$

Then

$$\alpha(fg) = \alpha(f)\alpha(g)$$

if and only if

$$\begin{aligned} \alpha_0(fg) &= \alpha_0(f)\alpha_0(g) \text{ and} \\ \alpha_1(fg) &= \alpha_0(f)\alpha_1(g) + \alpha_0(g)\alpha_1(f). \end{aligned}$$

The first condition says that α_0 is a homomorphism $A \rightarrow k$ and, when we use α_0 to make k into an A -module, the second condition says that α_1 is a k -derivation $A \rightarrow k$.

Recall that $\mathcal{O}(G)$ has a co-algebra structure (Δ, ϵ) . By definition, the elements of $\text{Lie}(G)$ are the k -algebra homomorphisms $\mathcal{O}(G) \rightarrow k[\varepsilon]$ such that the composite

$$\mathcal{O}(G) \xrightarrow{\alpha} k[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} k$$

is ϵ , i.e., such that $\alpha_0 = \epsilon$. Thus, we have proved the following statement.

PROPOSITION 1.26 *There is a natural one-to-one correspondence between the elements of $\text{Lie}(G)$ and the k -derivations $\mathcal{O}(G) \rightarrow k$ (where $\mathcal{O}(G)$ acts on k through ϵ), i.e.,*

$$\text{Lie}(G) \simeq \text{Der}_{k, \epsilon}(\mathcal{O}(G), k). \quad (133)$$

The correspondence is $\epsilon + \varepsilon D \leftrightarrow D$, and the Leibniz condition is

$$D(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f) \quad (134)$$

1f Extension of the base field

PROPOSITION 1.27 *For any field K containing k , $\text{Lie}(G_K) \simeq K \otimes_k \text{Lie}(G)$.*

PROOF. We use the description of the Lie algebra in terms of derivations (133). Let e_i be a basis for $\mathcal{O}(G)$ as a k -vector space, and let

$$e_i e_j = \sum a_{ijk} e_k, \quad a_{ijk} \in k.$$

In order to show that a k -linear map $D: A \rightarrow k$ is a k -derivation, it suffices to check the Leibniz condition on the elements of the basis. Therefore, D is a k -derivation if and only if the scalars $c_i = D(e_i)$ satisfy

$$\sum_k a_{ijk} c_k = \epsilon(e_i) c_j + \epsilon(e_j) c_i$$

for all i, j . This is a homogeneous system of linear equations in the c_i , and so a basis for the solutions in k is also a basis for the solutions in K (see the next lemma).

(Alternatively, use that

$$\text{Lie}(G) \simeq \text{Hom}_{k\text{-lin}}(I_G/I_G^2, k)$$

and that $I_{G_K} \simeq K \otimes_k I_G$.)

□

LEMMA 1.28 Let S be the space of solutions in k of a system of homogeneous linear equations with coefficients in k . Then the space of solutions in any k -algebra R of the system of equations is $R \otimes_k S$.

PROOF. The space S is the kernel of a linear map

$$0 \rightarrow S \rightarrow V \xrightarrow{\alpha} W.$$

Tensoring this sequence with R gives a sequence

$$0 \rightarrow R \otimes_k S \rightarrow R \otimes_k V \xrightarrow{\text{id}_R \otimes \alpha} R \otimes_k W,$$

which is exact because R is flat. Alternatively, for a finite system, we can put the matrix of the system of equations in row echelon form (over k), from which the statement is obvious. \square

REMARK 1.29 Let G be an algebraic group over k . For a k -algebra R , define

$$\mathfrak{g}(R) = \text{Ker}(G(R[\varepsilon]) \rightarrow G(R))$$

where $R[\varepsilon] = k[\varepsilon] \otimes_k R \simeq R[X]/(X^2)$. Then, as in (1.26), $\mathfrak{g}(R)$ can be identified with the space of k -derivations $A \rightarrow R$ (with R regarded as an A -module through ϵ), and the same proof shows that

$$\mathfrak{g}(R) \simeq R \otimes_k \mathfrak{g}(k) \quad (135)$$

where $\mathfrak{g}(k) = \text{Lie}(G)$. In other words, the functor $R \rightsquigarrow \mathfrak{g}(R)$ is canonically isomorphic to \mathfrak{g}_a .

1g The adjoint map $\text{Ad}: G \rightarrow \text{Aut}(\mathfrak{g})$

For any k -algebra R , we have homomorphisms

$$R \xrightarrow{i} R[\varepsilon] \xrightarrow{\pi} R, \quad i(a) = a + \varepsilon 0, \quad \pi(a + \varepsilon b) = a, \quad \pi \circ i = \text{id}_R.$$

For an algebraic group G over k , they give homomorphisms

$$G(R) \xrightarrow{i} G(R[\varepsilon]) \xrightarrow{\pi} G(R), \quad \pi \circ i = \text{id}_{G(R)}$$

where we have written i and π for $G(i)$ and $G(\pi)$. Let $\mathfrak{g}(R) = \text{Ker}(G(R[\varepsilon]) \xrightarrow{\pi} G(R))$, so that

$$\mathfrak{g}(R) \simeq R \otimes_k \mathfrak{g}(k)$$

(see 1.29). We define

$$\text{Ad}: G(R) \rightarrow \text{Aut}(\mathfrak{g}(R))$$

by

$$\text{Ad}(g)x = i(g) \cdot x \cdot i(g)^{-1}, \quad g \in G(R), \quad x \in \mathfrak{g}(R) \subset G(R[\varepsilon]).$$

The following formulas hold:

$$\begin{aligned} \text{Ad}(g)(x + x') &= \text{Ad}(g)x + \text{Ad}(g)x', \quad g \in G(R), \quad x, x' \in \mathfrak{g}(R) \\ \text{Ad}(g)(cx) &= c(\text{Ad}(g)x), \quad g \in G(R), \quad c \in R, \quad x \in \mathfrak{g}(R). \end{aligned}$$

The first is clear from the definition of Ad , and the second follows from the description of the action of c in (1.14). Therefore Ad maps into $\text{Aut}_{R\text{-lin}}(\mathfrak{g}(R))$. All the constructions are clearly natural in R , and so we get a natural transformation

$$\text{Ad}: G \rightarrow \underline{\text{Aut}}(\mathfrak{g}_a)$$

of group-valued functors on Alg_k .

Let $f: G \rightarrow H$ be a homomorphism of algebraic groups over k . Because f is a functor, the diagrams

$$\begin{array}{ccc} G(R[\varepsilon]) & \xrightarrow{\pi} & G(R) & & G(R[\varepsilon]) & \xleftarrow{i} & G(R) \\ \downarrow f(R[\varepsilon]) & & \downarrow f(R) & & \downarrow f(R[\varepsilon]) & & \downarrow f(R) \\ H(R[\varepsilon]) & \xrightarrow{\pi} & H(R) & & H(R[\varepsilon]) & \xleftarrow{i} & H(R) \end{array}$$

commute. Thus f defines a homomorphism of functors

$$\text{Lie}(f): \mathfrak{g}_a \rightarrow \mathfrak{h}_a,$$

and the diagrams

$$\begin{array}{ccccc} G(R) & \times & \mathfrak{g}(R) & \longrightarrow & \mathfrak{g}(R) \\ \downarrow f & & \downarrow \text{Lie}(f) & & \uparrow \text{Lie}(f) \\ H(R) & \times & \mathfrak{h}(R) & \longrightarrow & \mathfrak{g}(R) \end{array}$$

commute for all R , i.e.,

$$\text{Lie}(f)(\text{Ad}_G(g) \cdot x) = \text{Ad}_H(f(g)) \cdot x, \quad g \in G(R), \quad x \in \mathfrak{g}(R). \quad (136)$$

1h First definition of the bracket

The idea of the construction is the following. In order to define the bracket $[\cdot, \cdot]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$, it suffices to define the map $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$, $\text{ad}(x)(y) = [x, y]$. For this, it suffices to define a homomorphism of algebraic groups $\text{ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$, or, in other words, an action of G on \mathfrak{g} . But G acts on itself by inner automorphisms, and hence on its Lie algebra.

In more detail, in the last subsection, we defined a homomorphism of algebraic groups

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}.$$

Specifically,

$$\text{Ad}(g)x = i(g) \cdot x \cdot i(g)^{-1}, \quad g \in G(R), \quad x \in \mathfrak{g}(R) \subset G(R[\varepsilon]).$$

On applying the functor Lie to the homomorphism Ad , we obtain a homomorphism of k -vector spaces

$$\text{ad}: \text{Lie } G \rightarrow \text{Lie } \text{GL}_{\mathfrak{g}} \stackrel{(1.20)}{\simeq} \text{End}_{k\text{-lin}}(\mathfrak{g}).$$

DEFINITION 1.30 For $a, x \in \text{Lie}(G)$,

$$[a, x] = \text{ad}(a)(x).$$

LEMMA 1.31 For $G = \mathrm{GL}_n$, the construction gives $[A, X] = AX - XA$.

PROOF. An element $I + \varepsilon A \in \mathrm{Lie}(\mathrm{GL}_n)$ acts on $M_n(k[\varepsilon])$ as

$$X + \varepsilon Y \mapsto (I + \varepsilon A)(X + \varepsilon Y)(I - \varepsilon A) = X + \varepsilon Y + \varepsilon(AX - XA).$$

On comparing this with (1.20), we see that $\mathrm{ad}(A)$ acts as $\mathrm{id} + \varepsilon\alpha$ where $\alpha(X) = AX - XA$. \square

LEMMA 1.32 The construction is functorial in G , i.e., the map $\mathrm{Lie} G \rightarrow \mathrm{Lie} H$ defined by a homomorphism of algebraic groups $G \rightarrow H$ is compatible with the two brackets.

PROOF. This follows from (136). \square

Because the bracket $[A, X] = AX - XA$ on \mathfrak{gl}_n satisfies the conditions in (1.1) and every G can be embedded in GL_n (I, 8.31), the bracket on $\mathrm{Lie}(G)$ makes it into a Lie algebra. This completes the first proof of Theorem 1.12.

1i Second definition of the bracket

Let $A = \mathcal{O}(G)$, and consider the space $\mathrm{Der}_k(A, A)$ of k -derivations of A into A (with A regarded as an A -module in the obvious way). The bracket

$$[D, D'] \stackrel{\mathrm{def}}{=} D \circ D' - D' \circ D$$

of two derivations is again a derivation. In this way $\mathrm{Der}_k(A, A)$ becomes a Lie algebra.

Let G be an algebraic group. A derivation $D: \mathcal{O}(G) \rightarrow \mathcal{O}(G)$ is *left invariant* if

$$\Delta \circ D = (\mathrm{id} \otimes D) \circ \Delta. \quad (137)$$

If D and D' are left invariant, then

$$\begin{aligned} \Delta \circ [D, D'] &= \Delta \circ (D \circ D' - D' \circ D) \\ &= (\mathrm{id} \otimes (D \circ D') - \mathrm{id} \otimes (D' \circ D)) \\ &= (\mathrm{id} \otimes [D, D']) \circ \Delta \end{aligned}$$

and so $[D, D']$ is left invariant.

PROPOSITION 1.33 The map $D \mapsto \epsilon \circ D: \mathrm{Der}_k(\mathcal{O}(G), \mathcal{O}(G)) \rightarrow \mathrm{Der}_k(\mathcal{O}(G), k)$ defines an isomorphism from the subspace of left invariant derivations onto $\mathrm{Der}_k(\mathcal{O}(G), k)$.

PROOF. If D is a left invariant derivation $\mathcal{O}(G) \rightarrow \mathcal{O}(G)$, then

$$D \stackrel{\mathrm{I}, (30)}{=} (\mathrm{id} \otimes \epsilon) \circ \Delta \circ D \stackrel{(137)}{=} (\mathrm{id} \otimes \epsilon) \circ (\mathrm{id} \otimes D) \circ \Delta = (\mathrm{id} \otimes (\epsilon \circ D)) \circ \Delta$$

and so D is determined by $\epsilon \circ D$. Conversely, if $d: \mathcal{O}(G) \rightarrow k$ is a derivation, then $D = (\mathrm{id} \otimes d) \circ \Delta$ is a left invariant derivation $\mathcal{O}(G) \rightarrow \mathcal{O}(G)$. \square

Thus, $\mathrm{Lie}(G)$ is isomorphic (as a k -vector space) to the space of left invariant derivations $\mathcal{O}(G) \rightarrow \mathcal{O}(G)$, which is a Lie subalgebra of $\mathrm{Der}_k(\mathcal{O}(G), \mathcal{O}(G))$. In this way, $\mathrm{Lie}(G)$ acquires a Lie algebra structure, which is clearly natural in G .

It remains to check that, when $G = \mathrm{GL}_n$, this gives the bracket $[A, B] = AB - BA$ (left as an exercise for the present).

1j The functor Lie preserves fibred products

PROPOSITION 1.34 For any homomorphisms $G \rightarrow H \leftarrow G'$ of algebraic groups,

$$\text{Lie}(G \times_H G') \simeq \text{Lie}(G) \times_{\text{Lie}(H)} \text{Lie}(G'). \tag{138}$$

PROOF. By definition (I §4b),

$$(G \times_H G')(R) = G(R) \times_{H(R)} G'(R), \quad R \text{ a } k\text{-algebra.}$$

Therefore,

$$\begin{aligned} \text{Lie}(G \times_H G') &= \text{Ker}(G(k[\varepsilon]) \times_{H(k[\varepsilon])} G'(k[\varepsilon]) \rightarrow G(k) \times_{H(k)} G'(k)) \\ &= \{(g, g') \in G(k[\varepsilon]) \times G'(k[\varepsilon]) \mid g, g' \text{ have the same image in } H(k[\varepsilon]), G(k), \text{ and } G'(k)\} \\ &= \text{Ker}(G(k[\varepsilon]) \rightarrow G(k)) \times_{H(k[\varepsilon])} \text{Ker}(G'(k[\varepsilon]) \rightarrow G'(k)) \\ &= \text{Lie}(G) \times_{\text{Lie}(H)} \text{Lie}(G'). \end{aligned} \quad \square$$

EXAMPLE 1.35 Let k be a field of characteristic $p \neq 0$. There are fibred product diagrams:

$$\begin{array}{ccc} \mu_p & \longrightarrow & \mathbb{G}_m \\ \downarrow & & \downarrow y \mapsto (y^p, y) \\ \mathbb{G}_m & \xrightarrow{x \mapsto (1, x)} & \mathbb{G}_m \times \mathbb{G}_m \end{array} \quad \overset{\text{Lie}}{\rightsquigarrow} \quad \begin{array}{ccc} k & \xrightarrow{\text{id}} & k \\ \downarrow \text{id} & & \downarrow c \mapsto (0, c) \\ k & \xrightarrow{c \mapsto (0, c)} & k \times k. \end{array}$$

EXAMPLE 1.36 Recall (I, 7.15) that the kernel of a homomorphism $\alpha: G \rightarrow H$ of algebraic groups can be obtained as a fibred product:

$$\begin{array}{ccc} \text{Ker}(\alpha) & \longrightarrow & \{1_H\} \\ \downarrow & & \downarrow \\ G & \xrightarrow{\alpha} & H \end{array}$$

Therefore (138) shows that

$$\text{Lie}(\text{Ker}(\alpha)) = \text{Ker}(\text{Lie}(\alpha)).$$

In other words, an exact sequence of algebraic groups $1 \rightarrow N \rightarrow G \rightarrow H$ gives rise to an exact sequence of Lie algebras

$$0 \rightarrow \text{Lie } N \rightarrow \text{Lie } G \rightarrow \text{Lie } H.$$

For example, the exact sequence (cf. 1.35)

$$1 \rightarrow \mu_p \xrightarrow{x \mapsto (x, x)} \mathbb{G}_m \times \mathbb{G}_m \xrightarrow{(x, y) \mapsto (y^p, x/y)} \mathbb{G}_m \times \mathbb{G}_m$$

gives rise to an exact sequence

$$0 \rightarrow k \xrightarrow{x \mapsto (x, x)} k \oplus k \xrightarrow{(x, y) \mapsto (0, x-y)} k \oplus k.$$

EXAMPLE 1.37 Let H and H' be algebraic subgroups of an algebraic group G . The algebraic subgroup $H \cap H'$ with $(H \cap H')(R) = H(R) \cap H'(R)$ (inside $G(R)$) is the fibred product of the inclusion maps, and so

$$\text{Lie}(H \cap H') = \text{Lie}(H) \cap \text{Lie}(H') \quad (\text{inside } \text{Lie}(G)).$$

More generally,

$$\text{Lie}\left(\bigcap_{i \in I} H_i\right) = \bigcap_{i \in I} \text{Lie } H_i \quad (\text{inside } \text{Lie}(G)) \tag{139}$$

for any family of subgroups H_i of G .

For example, the homomorphisms in (1.35) realize \mathbb{G}_m in two ways as subgroups of $\mathbb{G}_m \times \mathbb{G}_m$, which intersect in μ_p , and so

$$\text{Lie}(\mu_p) = \text{Lie}(\mathbb{G}_m) \cap \text{Lie}(\mathbb{G}_m) \quad (\text{inside } \text{Lie}(\mathbb{G}_m \times \mathbb{G}_m)).$$

1.38 The examples 1.35–1.37 show that the functor Lie does *not* preserve fibred products, left exact sequences, or intersections in the category of *smooth* algebraic groups.

1.39 The sequence

$$1 \rightarrow \mu_p \xrightarrow{x \mapsto (x,x)} \mathbb{G}_m \times \mathbb{G}_m \xrightarrow{(x,y) \mapsto (y^p, x/y)} \mathbb{G}_m \times \mathbb{G}_m \rightarrow 1$$

is exact in the category of algebraic groups over k , but

$$0 \rightarrow k \xrightarrow{x \mapsto (x,x)} k \oplus k \xrightarrow{(x,y) \mapsto (0,x-y)} k \oplus k \rightarrow 0$$

is not exact, and so functor Lie is *not* right exact.

1k Abelian Lie algebras

A Lie algebra \mathfrak{g} is said to be *abelian* (or *commutative*) if $[x, y] = 0$ for all $x, y \in \mathfrak{g}$. Thus, to give an abelian Lie algebra amounts to giving a finite-dimensional vector space.

If G is commutative, then $\text{Lie}(G)$ is commutative. This can be seen directly from the first definition of the bracket because the inner automorphisms are trivial if G is commutative. Alternatively, observe that if G is a commutative subgroup of GL_n , then $\text{Lie}(G)$ is a commutative subalgebra of $\text{Lie}(\text{GL}_n)$. See also (2.24) below.

1l Normal subgroups and ideals

A normal algebraic subgroup N of an algebraic group G is the kernel of a quotient map $G \rightarrow Q$ (see I, 8.70); therefore, $\text{Lie}(N)$ is the kernel of a homomorphism of Lie algebras $\text{Lie } G \rightarrow \text{Lie } Q$ (see 1.36), and so is an ideal in $\text{Lie } G$. Of course, this can also be proved directly.

1m Algebraic Lie algebras

A Lie algebra is said to be *algebraic* if it is the Lie algebra of an algebraic group. A sum of algebraic Lie algebras is algebraic. Let $\mathfrak{g} = \text{Lie}(G)$, and let \mathfrak{h} be a Lie subalgebra of \mathfrak{g} . The intersection of the algebraic Lie subalgebras of \mathfrak{g} containing \mathfrak{h} is again algebraic (see (139)) — it is called the *algebraic envelope* or *hull* of \mathfrak{h} .

Let \mathfrak{h} be a Lie subalgebra of \mathfrak{gl}_V . A necessary condition for \mathfrak{h} to be algebraic is that the semisimple and nilpotent components of each element of \mathfrak{h} (as an endomorphism of \mathfrak{gl}_V) lie in \mathfrak{h} . However, this condition is not sufficient, even in characteristic zero.

Let \mathfrak{h} be a Lie subalgebra of \mathfrak{gl}_V over a field k of characteristic zero. We explain how to determine the algebraic hull of \mathfrak{h} . For any $X \in \mathfrak{h}$, let $\mathfrak{g}(X)$ be the algebraic hull of the Lie algebra spanned by X . Then the algebraic hull of \mathfrak{h} is the Lie subalgebra of \mathfrak{gl}_V generated by the $\mathfrak{g}(X)$, $X \in \mathfrak{h}$. In particular, \mathfrak{h} is algebraic if and only if each X is contained in an algebraic Lie subalgebra of \mathfrak{h} . Write X as the sum $S + N$ of its semisimple and nilpotent components. Then $\mathfrak{g}(N)$ is spanned by N , and so we may suppose that X is semisimple. For some finite extension L of k , there exists a basis of $L \otimes V$ for which the matrix of X is $\text{diag}(\alpha_1, \dots, \alpha_n)$. Let W be the subspace $M_n(L)$ consisting of the matrices $\text{diag}(a_1, \dots, a_n)$ such that

$$\sum_i c_i \alpha_i = 0, c_i \in L \implies \sum_i c_i a_i = 0,$$

i.e., such that the a_i satisfy every linear relation over L that the α_i do. Then the map

$$\mathfrak{gl}_V \rightarrow L \otimes \mathfrak{gl}_V \simeq M_n(L)$$

induces maps

$$\mathfrak{g}(X) \rightarrow L \otimes \mathfrak{g}(X) \simeq W.$$

See Chevalley 1951 (also Fieker and de Graaf 2007 where it is explained how to implement this as an algorithm).

1.40 The following rules define a five-dimensional solvable Lie algebra $\mathfrak{g} = \bigoplus_{1 \leq i \leq 5} kx_i$:

$$[x_1, x_2] = x_5, [x_1, x_3] = x_3, [x_2, x_4] = x_4, [x_1, x_4] = [x_2, x_3] = [x_3, x_4] = [x_5, \mathfrak{g}] = 0$$



(Bourbaki LIE, I, §5, Exercise 6). For every injective homomorphism $\mathfrak{g} \hookrightarrow \mathfrak{gl}_V$, there exists an element of \mathfrak{g} whose semisimple and nilpotent components (as an endomorphism of V) do not lie in \mathfrak{g} (ibid., VII, §5, Exercise 1). It follows that the image of \mathfrak{g} in \mathfrak{gl}_V is not the Lie algebra of an algebraic subgroup of GL_V (ibid., VII, §5, 1, Example).

NOTES Need to prove the statements in this subsection (not difficult). They are important in III, 3.

1n The exponential notation

Let S be an R -algebra, and let a be an element of S such that $a^2 = 0$. There is a unique R -algebra homomorphism $R[\varepsilon] \rightarrow S$ sending ε to a . Following DG, II §4, 3.7, p.209, we denote the image of $x \in \text{Lie}(G)(R)$ under the composite

$$\text{Lie}(G)(R) \hookrightarrow G(R[\varepsilon]) \rightarrow G(S)$$

by e^{ax} . For example, $x = e^{\varepsilon x}$ in $G(R[\varepsilon])$. For $x, y \in \text{Lie}(G)(R)$,

$$e^{a(x+y)} = e^{ax} e^{ay} \quad (\text{in } G(S)).$$

The action of $a \in R$ on $x \in \text{Lie}(G)(R)$ is described by

$$e^{(\varepsilon a)x} = e^{\varepsilon(ax)} \quad (\text{in } G(R[\varepsilon])).$$

If $f: G \rightarrow H$ is a homomorphism of algebraic groups and $x \in \text{Lie}(G)(R)$, then

$$f(e^{ax}) = e^{a(\text{Lie}(f)(x))}.$$

The adjoint map Ad is described by

$$g e^{\varepsilon x} g^{-1} = e^{\varepsilon(\text{Ad}(g)x)} \quad (\text{in } G(R[\varepsilon])),$$

($g \in G(R)$, $x \in \text{Lie}(G)(R)$). Moreover,

$$\text{Ad}(e^{\varepsilon x}) = \text{id} + \varepsilon \text{ad}(x) \quad (\text{in } \text{Aut}_{R\text{-lin}}(\text{Lie}(G)(R))).$$

Let $x, y \in \text{Lie}(G)(R)$ and let $a, b \in S$ be of square 0. Then

$$e^{ax} e^{by} e^{-ax} e^{-by} = e^{ab[x,y]} \quad (\text{in } G(S))$$

(ibid. 4.4).

1o Arbitrary base rings

Now let k be a commutative ring, and let $k[\varepsilon] = k[X]/(X^2)$. For any smooth affine group G over k , define $\mathfrak{g} = \text{Lie}(G)$ to be

$$\text{Lie}(G) = \text{Ker}(G(k[\varepsilon]) \xrightarrow{\varepsilon \mapsto 0} G(k)).$$

This is a finitely generated projective k -module, and for any k -algebra R ,

$$\text{Lie}(G_R) = R \otimes \mathfrak{g}.$$

Therefore, the functor $R \rightsquigarrow \text{Lie}(G_R)$ is equal to \mathfrak{g}_R . The action of G on itself by inner automorphisms defines an action of G on \mathfrak{g} , and, in fact, a homomorphism

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$$

of affine groups over k . On applying the functor Lie to this, we get the adjoint map

$$\text{ad}: \mathfrak{g} \rightarrow \text{Hom}_{k\text{-lin}}(\mathfrak{g}, \mathfrak{g}).$$

Now we can define a bracket operation on \mathfrak{g} by

$$[x, y] = \text{ad}(x)y.$$

Equipped with this bracket, \mathfrak{g} is a Lie algebra over k . Most of the material in this subsection extends to smooth affine groups over rings.

NOTES Perhaps should rewrite this subsection for smooth algebraic groups over rings.

2 Lie algebras and algebraic groups

In this subsection, we apply some algebraic geometry (actually, just commutative algebra CA) to study the relation between Lie algebras and algebraic groups. The strongest results require that k have characteristic zero.

2a The dimension of $\text{Lie}(G)$ versus the dimension of G

In Chapter I, we defined the dimension of an algebraic group G to be the dimension of the associated algebraic scheme $|G|$.

2.1 We list some alternative descriptions of $\dim G$.

- (a) According to the Noether normalization theorem (CA 5.11), there exists a finite set S of elements in $\mathcal{O}(G)$ such that $k[S]$ is a polynomial ring in the elements of S and $\mathcal{O}(G)$ is finitely generated as a $k[S]$ -module. The cardinality of S is $\dim G$.
- (b) Let G° be the identity component of G (see I, 13.12). The algebraic variety $|G^\circ|$ is irreducible, and so $\mathcal{O}(G^\circ)/\mathfrak{A}$ is an integral domain (I, 13.13). The transcendence degree of its field of fractions is $\dim G$.
- (c) Let \mathfrak{m} be a maximal ideal of $\mathcal{O}(G)$. The height of \mathfrak{m} is $\dim G$.

PROPOSITION 2.2 *For an algebraic group G , $\dim \text{Lie } G \geq \dim G$, with equality if and only if G is smooth.*

PROOF. Because $\text{Lie}(G_{k^{\text{al}}}) \simeq \text{Lie}(G) \otimes_k k^{\text{al}}$ (see 1.27), we may suppose $k = k^{\text{al}}$. According to (1.11),

$$\text{Lie}(G) \simeq \text{Hom}_{k\text{-lin}}(\mathfrak{m}/\mathfrak{m}^2, k)$$

where $\mathfrak{m} = \text{Ker}(\mathcal{O}(G) \xrightarrow{\epsilon} k)$. Therefore, $\dim \text{Lie}(G) \geq \dim G$, with equality if and only if the local ring $\mathcal{O}(G)_{\mathfrak{m}}$ is regular (I, 6.22), but $\mathcal{O}(G)_{\mathfrak{m}}$ is regular if and only if G is smooth (I, 6.25). \square

EXAMPLE 2.3 We have

$$\begin{aligned} \dim \text{Lie } \mathbb{G}_a &= 1 = \dim \mathbb{G}_a \\ \dim \text{Lie } \alpha_p &= 1 > 0 = \dim \alpha_p \\ \dim \text{Lie } \text{SL}_n &= n^2 - 1 = \dim \text{SL}_n. \end{aligned}$$

PROPOSITION 2.4 *If*

$$1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$$

is exact, then

$$\dim G = \dim N + \dim Q.$$

PROOF. See I, 7.60. \square

2b Applications

PROPOSITION 2.5 *Let H be a smooth algebraic subgroup of a connected algebraic group G . If $\text{Lie } H = \text{Lie } G$, then G is smooth and $H = G$.*

PROOF. We have

$$\dim H \stackrel{(2.2)}{=} \dim \text{Lie } H = \dim \text{Lie } G \stackrel{(2.2)}{\geq} \dim G.$$

Because H is a subgroup of G , $\dim H \leq \dim G$ (see I, 6.24). Therefore

$$\dim H = \dim \text{Lie}(G) = \dim G,$$

and so G is smooth (2.2) and $H = G$ (see I, 6.24). \square

COROLLARY 2.6 *Assume $\text{char}(k) = 0$ and that G is connected. A homomorphism $H \rightarrow G$ is a surjective if $\text{Lie } H \rightarrow \text{Lie } G$ is surjective.*

PROOF. We know (I, 8.70) that $H \rightarrow G$ factors into

$$H \rightarrow \bar{H} \rightarrow G$$

with $H \rightarrow \bar{H}$ surjective and $\bar{H} \rightarrow G$ injective. Correspondingly, we get a diagram of Lie algebras

$$\text{Lie } H \rightarrow \text{Lie } \bar{H} \rightarrow \text{Lie } G.$$

Because $\bar{H} \rightarrow G$ is injective, $\text{Lie } \bar{H} \rightarrow \text{Lie } G$ is injective (1.36). If $\text{Lie } H \rightarrow \text{Lie } G$ is surjective, then $\text{Lie } \bar{H} \rightarrow \text{Lie } G$ is an isomorphism. As we are in characteristic zero, \bar{H} is smooth (I, 6.31), and so (2.5) shows that $\bar{H} = G$. \square

COROLLARY 2.7 *Assume $\text{char}(k) = 0$. If*

$$1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$$

is exact, then

$$0 \rightarrow \text{Lie}(N) \rightarrow \text{Lie}(G) \rightarrow \text{Lie}(Q) \rightarrow 0$$

is exact.

PROOF. The sequence $0 \rightarrow \text{Lie}(N) \rightarrow \text{Lie}(G) \rightarrow \text{Lie}(Q)$ is exact (by 1.36), and the equality

$$\dim G \stackrel{(2.4)}{=} \dim N + \dim Q$$

implies a similar statement for the Lie algebras (by 2.2, as the groups are smooth). This implies (by linear algebra) that $\text{Lie}(G) \rightarrow \text{Lie}(Q)$ is surjective. \square

COROLLARY 2.8 *The Lie algebra of G is zero if and only if G is étale; in particular, a connected algebraic group with zero Lie algebra is trivial.*

PROOF. We have seen that the Lie algebra of an étale group is zero (1.18). Conversely, if $\text{Lie } G = 0$ then G has dimension 0, and so $\mathcal{O}(G)$ is a finite k -algebra; moreover, $I_G/I_G^2 = 0$, which implies that $\mathcal{O}(G)$ is étale. \square

COROLLARY 2.9 *In characteristic zero, a homomorphism $G \rightarrow H$ of connected algebraic groups is an isogeny if and only if $\text{Lie}(G) \rightarrow \text{Lie}(H)$ is an isomorphism.*

PROOF. Apply (2.6), (2.7), and 2.8). \square

2.10 The smoothness and connectedness assumptions are necessary in (2.5) because



$$\begin{aligned} \text{Lie}(\alpha_p) &= \text{Lie}(\mathbb{G}_a) \text{ but } \alpha_p \neq \mathbb{G}_a \text{ and} \\ \text{Lie}(\text{SO}_n) &= \text{Lie}(\text{O}_n) \text{ but } \text{SO}_n \neq \text{O}_n. \end{aligned}$$

The same examples show that the characteristic and connectedness assumptions are necessary in (2.6). The characteristic assumption is necessary in (2.7) because

$$0 \rightarrow \alpha_p \rightarrow \mathbb{G}_a \xrightarrow{x \mapsto x^p} \mathbb{G}_a \rightarrow 0$$

is exact, but the sequence

$$0 \rightarrow \text{Lie } \alpha_p \rightarrow \text{Lie } \mathbb{G}_a \rightarrow \text{Lie } \mathbb{G}_a \rightarrow 0$$

is

$$0 \rightarrow k \xrightarrow{\cong} k \xrightarrow{0} k \rightarrow 0,$$

which is not exact.

THEOREM 2.11 *Assume that $\text{char}(k) = 0$ and that G is connected. The map $H \mapsto \text{Lie } H$ from connected algebraic subgroups of G to Lie subalgebras of $\text{Lie } G$ is injective and inclusion preserving.*

PROOF. Let H and H' be connected algebraic subgroups of G . Then (see 1.37)

$$\text{Lie}(H \cap H') = \text{Lie}(H) \cap \text{Lie } H'.$$

If $\text{Lie}(H) = \text{Lie}(H')$, then

$$\text{Lie}(H) = \text{Lie}(H \cap H') = \text{Lie}(H'),$$

and so (2.5) shows that

$$H = H \cap H' = H'. \quad \square$$

EXAMPLE 2.12 Let k be a field of characteristic zero, and consider GL_n as an algebraic group over k . According to I, 8.31, every algebraic group over k can be realized as a subgroup of GL_n for some n , and, according to (2.11), the algebraic subgroups of GL_n are in one-to-one correspondence with the algebraic Lie subalgebras of \mathfrak{gl}_n . This suggests two questions: find an algorithm to decide whether a Lie subalgebra of \mathfrak{gl}_n is algebraic

(i.e., arises from an algebraic subgroup)²; given an algebraic Lie subalgebra of \mathfrak{gl}_n , find an algorithm to construct the group. For a recent discussion of these questions, see, de Graaf, Willem, A. Constructing algebraic groups from their Lie algebras. *J. Symbolic Comput.* 44 (2009), no. 9, 1223–1233.³

PROPOSITION 2.13 *Assume $\text{char}(k) = 0$. Let α, β be homomorphisms of algebraic groups $G \rightarrow H$. If $\text{Lie}(\alpha) = \text{Lie}(\beta)$ and G is connected, then $\alpha = \beta$.*

PROOF. Let Δ denote the diagonal in $G \times G$ — it is an algebraic subgroup of $G \times G$ isomorphic to G . The homomorphisms α and β agree on the algebraic group

$$G' \stackrel{\text{def}}{=} \Delta \cap G \times_H G.$$

The hypothesis implies $\text{Lie}(G') = \text{Lie}(\Delta)$, and so $G' = \Delta$. □

Thus, when $\text{char}(k) = 0$, the functor $G \rightsquigarrow \text{Lie}(G)$ from connected algebraic groups to Lie algebras is faithful and exact. It is not fully faithful, because

$$\text{End}(\mathbb{G}_m) = \mathbb{Z} \neq k = \text{End}(\text{Lie}(\mathbb{G}_m)).$$

Moreover, it is trivial on étale algebraic groups.

2.14 Even in characteristic zero, infinitely many nonisomorphic connected algebraic groups can have the same Lie algebra. For example, let \mathfrak{g} be the two-dimensional Lie algebra $\langle x, y \mid [x, y] = y \rangle$, and, for each nonzero $n \in \mathbb{N}$, let G_n be the semidirect product $\mathbb{G}_a \rtimes \mathbb{G}_m$ defined by the action $(t, a) \mapsto t^n a$ of \mathbb{G}_m on \mathbb{G}_a . Then $\text{Lie}(G_n) = \mathfrak{g}$ for all n , but no two groups G_n are isomorphic.

2c Representations; stabilizers; isotropy groups

A **representation** of a Lie algebra \mathfrak{g} on a k -vector space V is a homomorphism $\rho: \mathfrak{g} \rightarrow \mathfrak{gl}_V$. Thus ρ sends $x \in \mathfrak{g}$ to a k -linear endomorphism $\rho(x)$ of V , and

$$\rho([x, y]) = \rho(x)\rho(y) - \rho(y)\rho(x).$$

We often call V a **\mathfrak{g} -module** and write xv for $\rho(x)(v)$. With this notation

$$[x, y]v = x(yv) - y(xv). \tag{140}$$

A representation ρ is said to be **faithful** if it is injective. The representation $x \mapsto \text{ad } x: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$ is called the **adjoint representation** of \mathfrak{g} (see 1.4).

Let W be a subspace of V . The **stabilizer** of W in \mathfrak{g} is

$$\mathfrak{g}_W \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid xW \subset W\}.$$

²See §1m.

³de Graaf (ibid.) and his MR reviewer write: “A connected algebraic group in characteristic 0 is uniquely determined by its Lie algebra.” This is obviously false — for example, SL_2 and its quotient by $\{\pm I\}$ have the same Lie algebra. What they mean (but didn’t say) is that a connected algebraic subgroup of GL_n in characteristic zero is uniquely determined by its Lie algebra (as a subalgebra of \mathfrak{gl}_n).

It is clear from (140) that \mathfrak{g}_W is a Lie subalgebra of \mathfrak{g} .

Let $v \in V$. The *isotropy algebra* of v in \mathfrak{g} is

$$\mathfrak{g}_v \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid xv = 0\}.$$

It is a Lie subalgebra of \mathfrak{g} . The Lie algebra \mathfrak{g} is said to *fix* v if $\mathfrak{g} = \mathfrak{g}_v$, i.e., if $\mathfrak{g}v = 0$.

Let $r: G \rightarrow \text{GL}_V$ be a representation of G on a k -vector space V . Then $\text{Lie}(r)$ is a representation of $\text{Lie}(G)$ on V . Recall (I, 8.52) that, for any subspace W of V , the functor

$$R \rightsquigarrow G_W(R) \stackrel{\text{def}}{=} \{g \in G(R) \mid g(W \otimes R) = W \otimes R\}$$

is an algebraic subgroup of G , called the stabilizer of W in G .

PROPOSITION 2.15 For any representation $G \rightarrow \text{GL}_V$ and subspace $W \subset V$,

$$\text{Lie } G_W = (\text{Lie } G)_W.$$

PROOF. By definition, $\text{Lie } G_W$ consists of the elements $\text{id} + \varepsilon\alpha$ of $G(k[\varepsilon])$, $\alpha \in \text{End}(V)$, such that

$$(\text{id} + \varepsilon\alpha)(W + \varepsilon W) \subset W + \varepsilon W,$$

(cf. 1.20), i.e., such that $\alpha(W) \subset W$. □

COROLLARY 2.16 If W is stable under G , then it is stable under $\text{Lie}(G)$, and the converse is true when $\text{char}(k) = 0$ and G is connected.

PROOF. To say that W is stable under G means that $G = G_W$, but if $G = G_W$, then $\text{Lie } G = \text{Lie } G_W = (\text{Lie } G)_W$, which means that W is stable under $\text{Lie } G$. Conversely, to say that W is stable under $\text{Lie } G$, means that $\text{Lie } G = (\text{Lie } G)_W$. But if $\text{Lie } G = (\text{Lie } G)_W$, then $\text{Lie } G = \text{Lie } G_W$, which implies that $G_W = G$ when $\text{char}(k) = 0$ and G is connected (2.5). □

Let $r: G \rightarrow \text{GL}_V$ be a representation of G on a k -vector space V . Recall (I, 8.55) that, for any $v \in V$, the functor

$$R \rightsquigarrow G_v(R) \stackrel{\text{def}}{=} \{g \in G(R) \mid g(v \otimes 1) = v \otimes 1\}$$

is an algebraic subgroup of G , called the isotropy group of v in G .

PROPOSITION 2.17 For any representation $G \rightarrow \text{GL}_V$ and $v \in V$,

$$\text{Lie } G_v = (\text{Lie } G)_v.$$


PROOF. By definition, $\text{Lie } G_v$ consists of the elements $\text{id} + \varepsilon\alpha$ of $G(k[\varepsilon])$ such that

$$\text{id}(v) + \varepsilon\alpha(v) = v + 0\varepsilon,$$

i.e., such that $\alpha(v) = 0$. □

COROLLARY 2.18 *If v is fixed by G , then it is fixed by $\text{Lie}(G)$, and the converse holds when $\text{char}(k) = 0$ and G is connected. In other words, $V^G \subset V^{\mathfrak{g}}$, with equality when $\text{char}(k) = 0$ and G is connected.*

PROOF. The proof is the same as that of Corollary 2.16. □

2.19 Let V be a one-dimensional vector space over \mathbb{Q} , and let μ_3 act on V through the inclusion $\mu_3 \hookrightarrow \mathbb{G}_m = \text{GL}_V$; thus $\zeta \in \mu_3(\mathbb{C})$ acts on $V(\mathbb{C})$ as $v \mapsto \zeta v$. Then 

$$V^{\mu_3} = 0$$

but

$$V^{\mu_3(\mathbb{Q})} = V = V^{\text{Lie}(\mu_3)}.$$

For a representation $G \rightarrow \text{GL}(V)$ of G and subspace W of V , the functor

$$R \rightsquigarrow C_G(W)(R) \stackrel{\text{def}}{=} \{g \in G(R) \mid gw = w \text{ for all } w \in W\}$$

is an algebraic subgroup of G because

$$C_G(W) = \bigcap_{w \in S} G_w$$

for any set S spanning W . It is called the **centralizer** of W in G . When $C_G(W) = G$, the algebraic group G is said to **centralize** W .

Similarly, for a representation $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ of \mathfrak{g} and subspace W of V ,

$$c_{\mathfrak{g}}(W) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid xw = 0 \text{ for all } w \in W\}$$

is a Lie subalgebra of \mathfrak{g} , called the **centralizer** of W in \mathfrak{g} . When $c_{\mathfrak{g}}(W) = \mathfrak{g}$, the Lie algebra \mathfrak{g} is said to **centralize** W .

As Lie commutes with intersections (1.37), Proposition 2.17 implies the following statement.

COROLLARY 2.20 *For a representation $G \rightarrow \text{GL}(V)$ of G and subspace W of V ,*

$$\text{Lie}(C_G(W)) = c_{\mathfrak{g}}(W).$$

If G centralizes W , then \mathfrak{g} centralizes W , and the converse holds when $\text{char}(k) = 0$ and G is connected.

COROLLARY 2.21 *Let G be an algebraic group with Lie algebra \mathfrak{g} . If G is connected and k has characteristic zero, then the functor $\text{Rep}_k(G) \rightarrow \text{Rep}_k(\mathfrak{g})$ is fully faithful.*

PROOF. Let V and W be representations of G . Let α be a k -linear map $V \rightarrow W$, and let β be the element of $V^\vee \otimes W$ corresponding to α under the isomorphism $\text{Hom}_k(V, W) \simeq V^\vee \otimes W$. Then α is a homomorphism of representations of G if and only if β is fixed by G . Since a similar statement holds for \mathfrak{g} , the claim follows from (2.18). □

COROLLARY 2.22 *Let $r: G \rightarrow GL_V$ be a representation of an algebraic group G , and let $W' \subset W$ be subspace of V . There exists an algebraic subgroup $G_{W',W}$ of G such that $G_{W',W}(R)$ consists of the elements of $G(R)$ stabilizing each of $W'(R)$ and $W(R)$ and acting trivially on $W(R)/W'(R)$; its Lie algebra is*

$$\text{Lie}(G_{W',W}) = \mathfrak{g}_{W',W} \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid \text{Lie}(r)(x) \text{ maps } W \text{ into } W'\}.$$

PROOF. Apply (2.15) twice, and then (2.20). (See also DG II, §2, 1.3; §5, 5.7). \square

2d Normalizers and centralizers

Clearly $z(\mathfrak{g})$ is an ideal in \mathfrak{g} . For a subalgebra \mathfrak{h} of \mathfrak{g} , the **normalizer** and **centralizer** of \mathfrak{h} in \mathfrak{g} are

$$\begin{aligned} n_{\mathfrak{g}}(\mathfrak{h}) &= \{x \in \mathfrak{g} \mid [x, \mathfrak{h}] \subset \mathfrak{h}\} \\ c_{\mathfrak{g}}(\mathfrak{h}) &= \{x \in \mathfrak{g} \mid [x, \mathfrak{h}] = 0\}. \end{aligned}$$

Thus $n_{\mathfrak{g}}(\mathfrak{h})$ is the largest subalgebra of \mathfrak{g} containing \mathfrak{h} as an ideal. The centralizer is a subalgebra; when \mathfrak{h} is abelian, it is the largest subalgebra of \mathfrak{g} containing \mathfrak{h} in its centre.

PROPOSITION 2.23 *Let G be an algebraic group, and let H be a connected subgroup of G .*

(a) *Then*

$$\begin{aligned} \text{Lie}(N_G(H)) &\subset n_{\mathfrak{g}}(\mathfrak{h}) \\ \text{Lie}(C_G(H)) &\subset c_{\mathfrak{g}}(\mathfrak{h}) \end{aligned}$$

with equalities when $\text{char}(k) = 0$.

- (b) *If H is normal in G , then \mathfrak{h} is an ideal in $\text{Lie}(G)$, and the converse holds when $\text{char}(k) = 0$ and G is connected.*
- (c) *If H lies in the centre of G , then \mathfrak{h} lies in the centre of \mathfrak{g} , and the converse holds when $\text{char}(k) = 0$ and G is connected.*

PROOF. (a) We prove this below.

(b) If H is normal in G , then $N_G(H) = G$, and so $n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$ by (a); hence \mathfrak{h} is an ideal in \mathfrak{g} . Conversely, if $\text{char}(k) = 0$ and $n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$, then $\text{Lie}(N_G(H)) = \text{Lie}(G)$ by (a), which implies that $N_G(H) = G$ when G is connected (see 2.5).

(c) If H lies in the centre of G , then $C_G(H) = G$, and so $c_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$ by (a); hence \mathfrak{h} lies in the centre of \mathfrak{g} . Conversely, if $\text{char}(k) = 0$ and $c_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$, then $\text{Lie}(C_G(H)) = \text{Lie}(G)$, which implies that $C_G(H) = G$ when G is connected (see 2.5). \square

COROLLARY 2.24 *For any connected algebraic group G , $\text{Lie } Z(G) \subset z(\mathfrak{g})$, with equality when $\text{char}(k) = 0$. If an algebraic group G is commutative, then so also is its Lie algebra, and the converse holds when $\text{char}(k) = 0$ and G is connected.*

PROOF. Since $Z(G) = C_G(G)$ and $z(\mathfrak{g}) = c_{\mathfrak{g}}(\mathfrak{g})$, the first statement follows from (a) of the proposition, and the second follows from the first. \square

PROOF OF PROPOSITION 2.23(a)

Let $H: \text{Alg}_k \rightarrow \text{Grp}$ and $X: \text{Alg}_k \rightarrow \text{Set}$ be functors, and let $H \times X \rightarrow X$ be an action of H on X (cf. I, §6n) Let X^H be the subfunctor of X ,

$$R \rightsquigarrow X^H(R) = \{x \in X(R) \mid hx_S = x_S \text{ for all } h \in H(S) \text{ with } S \text{ an } R\text{-algebra}\}. \quad (141)$$

LEMMA 2.25 For all k -algebras R ,

$$X^H(R) = \{x \in X(R) \mid h_{R \otimes_k S} x_{R \otimes_k S} = x_{R \otimes_k S} \text{ for all } h \in H(S) \text{ with } S \text{ a } k\text{-algebra}\}.$$

PROOF. Let S be a R -algebra, and let S_0 denote S regarded as a k -algebra. The k -algebra maps $R \rightarrow S$ and $\text{id}: S_0 \rightarrow S$ define a homomorphism $R \otimes_k S_0 \rightarrow S$ of k -algebras:

$$\begin{array}{ccccc} R & \longrightarrow & R \otimes_k S_0 & \longrightarrow & S \\ \uparrow & & \uparrow & \nearrow \text{id} & \\ k & \longrightarrow & S_0 & & \end{array}$$

Let $h \in H(S) = H(S_0)$, and let $x \in X(R)$. If $h_{R \otimes_k S_0} x_{R \otimes_k S_0} = x_{R \otimes_k S_0}$ in $X(R \otimes_k S_0)$, then $hx_S = x_S$ in $X(S)$. □

Let $H \times G \rightarrow G$ be an action of an algebraic group H on an algebraic group G by group automorphisms. Let $\mathfrak{g} = \text{Lie}(G)$. Then H acts on the functor

$$R \rightsquigarrow \mathfrak{g}(R) \stackrel{\text{def}}{=} R \otimes \mathfrak{g}(k) \simeq \text{Ker}(G(R[\varepsilon]) \rightarrow G(R))$$

(see 1.29). By definition (141),

$$\mathfrak{g}^H(k) = \{x \in \mathfrak{g}(k) \mid hx_S = x_S \text{ (in } \mathfrak{g}(S)) \text{ for all } h \in H(S), S \text{ a } k\text{-algebra}\}. \quad (142)$$

On the other hand, Lemma 2.25 says that

$$G^H(k[\varepsilon]) = \{x \in G(k[\varepsilon]) \mid h_{S[\varepsilon]} x_{S[\varepsilon]} = x_{S[\varepsilon]} \text{ (in } G(S[\varepsilon])) \text{ for all } h \in H(S), S \text{ a } k\text{-algebra}\},$$

and so

$$\text{Lie}(G^H) = \{x \in \text{Lie}(G) \mid hx_S = x_S \text{ (in } \text{Lie}(G^H)(S)) \text{ for all } h \in H(S), S \text{ a } k\text{-algebra}\}. \quad (143)$$

Thus we have proved the following statement.

LEMMA 2.26 Let $H \times G \rightarrow G$ be an action of an algebraic group H on an algebraic group G by group automorphisms. Then

$$\text{Lie}(G^H) \simeq \text{Lie}(G)^H.$$

LEMMA 2.27 Let G be an algebraic group, and let H be a subgroup of G . Let H act on \mathfrak{g} via $H \rightarrow G \xrightarrow{\text{Ad}} \text{Aut}(\mathfrak{g})$. Then

$$\begin{aligned} \text{Lie}(C_G(H)) &= \text{Lie}(G)^H \\ \text{Lie}(N_G(H))/\text{Lie}(H) &\simeq (\text{Lie}(G)/\text{Lie}(H))^H. \end{aligned}$$

PROOF. Recall (I, 7f) that $C_G(H) = G^H$ (H acting on G by inner automorphisms), and so the assertion concerning $C_G(H)$ follows directly from Lemma 2.26.

Let $x \in \text{Lie}(G)$. According to Lemma 2.25, $x \in \text{Lie}(N_G(H))$ if and only if, for all k -algebras R and all $h \in H(R)$,⁴

$$\begin{aligned} (1 + \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}(1 - \varepsilon x_{R[\varepsilon]}) &\in H(R[\varepsilon]) \\ (1 - \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}(1 + \varepsilon x_{R[\varepsilon]}) &\in H(R[\varepsilon]), \end{aligned}$$

i.e., that

$$\begin{aligned} (1 + \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}(1 - \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}^{-1} &\in H(R[\varepsilon]) \\ (1 - \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}(1 + \varepsilon x_{R[\varepsilon]})h_{R[\varepsilon]}^{-1} &\in H(R[\varepsilon]). \end{aligned}$$

But this last condition can be written in the form

$$1 \pm \varepsilon(x_R - \text{Ad}(h)x_R) \in H(R[\varepsilon]),$$

i.e., in the form

$$x_R - \text{Ad}(h)x_R \in \text{Lie}(H)(R). \quad (144a)$$

We have shown that $x \in \text{Lie}(N_G(H))$ if and only if its image in $\text{Lie}(G)/\text{Lie}(H)$ is fixed by H . Therefore the subspace of $\text{Lie}(G)/\text{Lie}(H)$ fixed by H is $\text{Lie } N_G(H)/\text{Lie}(H)$. (Cf. DG II §5, 5.7). \square

We now prove Proposition 2.23(a). We know (2.27) that

$$\text{Lie } N_G(H)/\text{Lie } H = (\text{Lie } G/\text{Lie } H)^H;$$

moreover (2.18),

$$(\text{Lie } G/\text{Lie } H)^H \subset (\text{Lie } G/\text{Lie } H)^{\text{Lie } H}$$

with equality when $\text{char}(k) = 0$ and H is connected. Since

$$n_{\mathfrak{g}}(\mathfrak{h})/\mathfrak{h} = (\mathfrak{g}/\mathfrak{h})^{\mathfrak{h}},$$

this implies the first statement.

We know (2.27) that $\text{Lie}(C_G(H)) = \text{Lie}(G)^H$; moreover (2.18), $\text{Lie}(G)^H \subset \text{Lie}(G)^{\text{Lie}(H)}$ with equality when $\text{char}(k) = 0$ and G is connected. Since $\text{Lie}(G)^{\text{Lie}(H)} = c_{\mathfrak{g}}(\mathfrak{h})$, this proves the second statement. (Cf. DG II §6, 2.1.)

⁴In the notation of §1n, this reads:

$$\begin{aligned} (e^{\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]} \cdot (e^{-\varepsilon x})_{R[\varepsilon]} &\in H(R[\varepsilon]) \\ (e^{-\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]} \cdot (e^{\varepsilon x})_{R[\varepsilon]} &\in H(R[\varepsilon]), \end{aligned}$$

i.e., that

$$\begin{aligned} (e^{\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]} \cdot (e^{-\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]}^{-1} &\in H(R[\varepsilon]) \\ (e^{-\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]} \cdot (e^{\varepsilon x})_{R[\varepsilon]} \cdot h_{R[\varepsilon]}^{-1} &\in H(R[\varepsilon]). \end{aligned}$$

But this last condition can also be written

$$e^{\pm \varepsilon(x_R - \text{Ad}(h)x_R)} \in H(R[\varepsilon]),$$

i.e.,

$$x_R - \text{Ad}(h)x_R \in \text{Lie}(H)(R).$$

2e A nasty example



2.28 Let k be a field of characteristic $p \neq 0$. The following simple example (already encountered in I, 7.47) illustrates some of the things that can go wrong in this case. Define G to be the algebraic subgroup of GL_3 such that

$$G(R) = \left\{ \begin{pmatrix} u & 0 & 0 \\ 0 & u^p & a \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

In other words, G is algebraic subgroup defined by the equations $X_{22} = X_{11}^p$, $X_{33} = 1$, $X_{12} = X_{13} = X_{21} = X_{31} = X_{32} = 0$. Note that G is isomorphic to $\mathbb{G}_a \times \mathbb{G}_m$ but with the noncommutative group structure

$$(a, u)(b, v) = (a + bu^p, uv).$$

In other words, G is the semi-direct product $\mathbb{G}_a \rtimes \mathbb{G}_m$ with $u \in \mathbb{G}_m(R)$ acting on $\mathbb{G}_a(R)$ as multiplication by u^p . The Lie algebra of G is the semi-direct product $\mathrm{Lie}(\mathbb{G}_a) \rtimes \mathrm{Lie}(\mathbb{G}_m)$ with the *trivial* action of $\mathrm{Lie}(\mathbb{G}_m)$ on $\mathrm{Lie}(\mathbb{G}_a)$ and so is commutative. The centre of G is $\{(0, u) \mid u^p = 1\} \simeq \mu_p$, and the centre of $G(k^{\mathrm{al}})$ is trivial. Thus,

$$\mathrm{Lie}(Z(G)_{\mathrm{red}}) \subsetneq \mathrm{Lie}(Z(G)) \subsetneq Z(\mathrm{Lie}(G)).$$

On the other hand

$$(\mathrm{Ad}(a, u))(b\varepsilon, 1 + v\varepsilon) = (bu^p\varepsilon, 1 + \varepsilon v)$$

and so the subset of $\mathrm{Lie}(G)$ fixed by $\mathrm{Ad}(G)$ is

$$0 \times k = \mathrm{Lie}(Z(G)).$$

3 Nilpotent and solvable Lie algebras

We write $\langle a, b, \dots \rangle$ for $\mathrm{Span}(a, b, \dots)$, and we write $\langle a, b, \dots \mid R \rangle$ for the Lie algebra with basis a, b, \dots and the bracket given by the rules R .

3a Definitions

DEFINITION 3.1 A Lie algebra \mathfrak{g} is said to be *solvable* (resp. *nilpotent*) if it admits a filtration

$$\mathfrak{g} = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \dots \supset \mathfrak{a}_r = 0 \tag{145}$$

by ideals such that $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ is abelian (resp. contained in the centre of $\mathfrak{a}/\mathfrak{a}_{i+1}$). Such a filtration is called a *solvable series* (resp. *nilpotent series*).

In other words, a Lie algebra is solvable (resp. nilpotent) if it can be obtained from abelian Lie algebras by successive extensions (resp. successive central extensions).

For example,

$$\mathfrak{b}_3 = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\} \supset \{0\}$$

is solvable because $[b_3, b_3]$ is contained in

$$\mathfrak{n}_3 = \left\{ \begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix} \right\} \supset \left\{ \begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\} \supset \{0\},$$

which is nilpotent. More generally, for any maximal flag

$$F : V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

in a vector space V , the Lie algebras

$$\mathfrak{b}(F) \stackrel{\text{def}}{=} \{x \in \mathfrak{gl}_V \mid xV_i \subset V_i\}$$

$$\mathfrak{n}(F) \stackrel{\text{def}}{=} \{x \in \mathfrak{gl}_V \mid xV_i \subset V_{i+1}\}$$

are respectively solvable and nilpotent.

PROPOSITION 3.2 *A Lie algebra \mathfrak{g} is solvable if and only if its **derived series***

$$\mathfrak{g} \supset \mathfrak{g}' = [\mathfrak{g}, \mathfrak{g}] \supset \mathfrak{g}'' = [\mathfrak{g}', \mathfrak{g}'] \supset \cdots \supset \mathfrak{g}^{(i+1)} = [\mathfrak{g}^{(i)}, \mathfrak{g}^{(i)}] \supset \cdots$$

*terminates with zero, and it is nilpotent if and only if its **descending central series***

$$\mathfrak{g} \supset \mathfrak{g}^1 = [\mathfrak{g}, \mathfrak{g}] \supset \mathfrak{g}^2 = [\mathfrak{g}, \mathfrak{g}^1] \supset \cdots \supset \mathfrak{g}^{i+1} = [\mathfrak{g}, \mathfrak{g}^i] \supset \cdots$$

terminates with zero.

PROOF. If the derived (resp. descending central series) terminates with zero, then it is a solvable (resp. nilpotent) series. Conversely, if there exists a solvable (resp. nilpotent) series $\mathfrak{g} \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$, then $\mathfrak{g}^{(i)} \subset \mathfrak{a}_i$ (resp. $\mathfrak{g}^i \subset \mathfrak{a}_i$) and so the derived series (resp. descending central series) terminates with zero. \square

For example, the Lie algebra

$$\langle x, y \mid [x, y] = y \rangle$$

is solvable but not nilpotent, and the Lie algebra

$$\langle x, y, z \mid [x, y] = z, [x, z] = [y, z] = 0 \rangle$$

is nilpotent (hence also solvable).

PROPOSITION 3.3 (a) *Subalgebras and quotient algebras of solvable Lie algebras are solvable.*

(b) *A Lie algebra \mathfrak{g} is solvable if it contains an ideal \mathfrak{n} such that \mathfrak{n} and $\mathfrak{g}/\mathfrak{n}$ are solvable.*

(c) *Let \mathfrak{n} be an ideal in a Lie algebra \mathfrak{g} , and let \mathfrak{h} be a subalgebra of \mathfrak{g} . If \mathfrak{n} and \mathfrak{h} are solvable, then $\mathfrak{h} + \mathfrak{n}$ is solvable.*

PROOF. (a) Let $\mathfrak{g} \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ be solvable series for \mathfrak{g} . For any subalgebra \mathfrak{h} of \mathfrak{g} , $\mathfrak{h} \supset \mathfrak{h} \cap \mathfrak{a}_1 \supset \mathfrak{h} \cap \mathfrak{a}_2 \supset \cdots$ is a solvable series for \mathfrak{h} , and, for any quotient $\alpha: \mathfrak{g} \rightarrow \mathfrak{q}$ of \mathfrak{g} , $\mathfrak{q} \supset \alpha(\mathfrak{a}_1) \supset \alpha(\mathfrak{a}_2) \supset \cdots$ is solvable series for \mathfrak{q} .

(b) Because $\mathfrak{g}/\mathfrak{n}$ is solvable, $\mathfrak{g}^{(m)} \subset \mathfrak{n}$ for some m . Now $\mathfrak{g}^{(m+n)} \subset \mathfrak{n}^{(n)}$, which is zero for some n .

(c) This follows from (b) because $\mathfrak{h} + \mathfrak{n}/\mathfrak{n} \simeq \mathfrak{h}/\mathfrak{h} \cap \mathfrak{n}$, which is solvable by (a). \square

COROLLARY 3.4 *Every finite-dimensional Lie algebra contains a largest solvable ideal.*

PROOF. Let \mathfrak{n} be a maximal solvable ideal. If \mathfrak{h} is also a solvable subalgebra, then $\mathfrak{h} + \mathfrak{n}$ is solvable by (3.3c). Therefore, if \mathfrak{h} is a solvable ideal, then $\mathfrak{h} + \mathfrak{n}$ is a solvable ideal, and so $\mathfrak{h} \subset \mathfrak{n}$. \square

DEFINITION 3.5 The largest solvable ideal in \mathfrak{g} is called the **radical** of \mathfrak{g} .

PROPOSITION 3.6 (a) *Subalgebras and quotient algebras of nilpotent Lie algebras are nilpotent.*

(b) *A nonzero Lie algebra \mathfrak{g} is nilpotent if and only if $\mathfrak{g}/\mathfrak{a}$ is nilpotent for some ideal $\mathfrak{a} \subset z(\mathfrak{g})$.*

PROOF. Statement (a) follows directly from the definition. If \mathfrak{g} is nilpotent, then the last nonzero term \mathfrak{a} in a nilpotent series is contained in $z(\mathfrak{g})$ and $\mathfrak{g}/\mathfrak{a}$ is obviously nilpotent. Conversely, for any ideal $\mathfrak{a} \subset z(\mathfrak{g})$, the inverse image of a nilpotent series for $\mathfrak{g}/\mathfrak{a}$ becomes a nilpotent series for \mathfrak{g} when extended by 0. \square



3.7 An extension of nilpotent algebras is solvable, but not necessarily nilpotent. For example, \mathfrak{n}_n is nilpotent and $\mathfrak{b}_n/\mathfrak{n}_n$ is abelian, but \mathfrak{b}_n is not nilpotent when $n \geq 3$.

PROPOSITION 3.8 *Let k' be a field containing k . A Lie algebra \mathfrak{g} over k is solvable (resp. nilpotent) if and only if $\mathfrak{g}_{k'} \stackrel{\text{def}}{=} k' \otimes_k \mathfrak{g}$ is solvable (resp. nilpotent).*

PROOF. Obviously, for any subalgebras \mathfrak{h} and \mathfrak{h}' of \mathfrak{g} , $[\mathfrak{h}, \mathfrak{h}']_{k'} = [\mathfrak{h}_{k'}, \mathfrak{h}'_{k'}]$. \square

3b Nilpotent Lie algebras: Engel's theorems

If the $n + 1$ st term \mathfrak{g}^{n+1} of the descending central series of \mathfrak{g} is zero, then

$$[x_1, [x_2, \dots [x_n, y] \dots]] = 0$$

for all $x_1, \dots, x_n, y \in \mathfrak{g}$; in other words, $\text{ad}(x_1) \circ \dots \circ \text{ad}(x_n) = 0$; in particular, $\text{ad}(x)^n = 0$. There is a converse statement.

THEOREM 3.9 *A Lie algebra \mathfrak{g} is nilpotent if $\text{ad}(x): \mathfrak{g} \rightarrow \mathfrak{g}$ is nilpotent for every $x \in \mathfrak{g}$.*

The next two theorems are variants of (3.9).


THEOREM 3.10 *Let V be a finite-dimensional vector space, and let \mathfrak{g} be subalgebra of \mathfrak{gl}_V . If \mathfrak{g} consists of nilpotent endomorphisms, then there exists a basis of V for which \mathfrak{g} is contained in \mathfrak{n}_n , $n = \dim V$.*

In other words, there exists a basis e_1, \dots, e_n for V such that

$$\mathfrak{g}e_i \subset \langle e_1, \dots, e_{i-1} \rangle, \text{ all } i. \quad (146)$$

THEOREM 3.11 *Let $\alpha: \mathfrak{g} \rightarrow \mathfrak{gl}_V$ be a representation of a Lie algebra \mathfrak{g} on a nonzero finite-dimensional vector space V . If $\alpha(x)$ is nilpotent for all $x \in \mathfrak{g}$, then there exists a nonzero vector v in such that $\mathfrak{g}v = 0$.*

We note that, for a single $x \in \mathfrak{g}$ such that $\alpha(x)$ is nilpotent, there is no problem finding a nonzero v such that $xv = 0$: choose any nonzero vector v_0 in V , and let $v = x^m v_0$ with m the greatest element of \mathbb{N} such that $x^m v_0 \neq 0$.

3.12 Let \mathfrak{g} be a subalgebra of \mathfrak{gl}_V . If there exists a basis of V for which $\mathfrak{g} \subset \mathfrak{n}_{\dim V}$, then \mathfrak{g} is nilpotent, but the converse statement is false. For example, if V has dimension 1, then $\mathfrak{g} = \mathfrak{gl}_V$ is nilpotent (even abelian), but there is no basis for which the elements of \mathfrak{g} are represented by strictly upper triangular matrices. Note that Theorem 3.9 says only that, for an element x of a nilpotent algebra, $\text{ad}(x)$ is nilpotent; it doesn't say that x acts nilpotently on every \mathfrak{g} -module V . 

PROOF THAT (3.11) IMPLIES (3.9)

Assume that \mathfrak{g} satisfies the hypothesis of (3.9) and is nonzero. On applying (3.11) to the homomorphism $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$, we see there exists a nonzero $x \in \mathfrak{g}$ such that $[\mathfrak{g}, x] = 0$. Therefore $z(\mathfrak{g}) \neq 0$. The quotient algebra $\mathfrak{g}/z(\mathfrak{g})$ satisfies the hypothesis of (3.9) and has smaller dimension than \mathfrak{g} . Using induction on the dimension of \mathfrak{g} , we find that $\mathfrak{g}/z(\mathfrak{g})$ is nilpotent, which implies that \mathfrak{g} is nilpotent by (3.6b).

PROOF THAT (3.11) IMPLIES (3.10).

Let $\mathfrak{g} \subset \mathfrak{gl}_V$ satisfy the hypothesis of (3.10). If $V \neq 0$, then (3.11) applied to $\mathfrak{g} \rightarrow \mathfrak{gl}_V$, shows that there exists a vector $e_1 \neq 0$ such that $\mathfrak{g}e_1 = 0$; if $V \neq \langle e_1 \rangle$, then (3.11) applied to $\mathfrak{g} \rightarrow \mathfrak{gl}_{V/\langle e_1 \rangle}$ shows that there exists a vector $e_2 \notin \langle e_1 \rangle$ such that $\mathfrak{g}e_2 \subset \langle e_1 \rangle$. Continuing in this fashion, we obtain a basis e_1, \dots, e_n for V satisfying (146).

PROOF OF (3.11)

LEMMA 3.13 *Let V be a vector space, and let $x: V \rightarrow V$ be an endomorphism of V . If x is nilpotent, then so also is $\text{ad } x: \mathfrak{gl}_V \rightarrow \mathfrak{gl}_V$.*

PROOF. Let $y \in \mathfrak{gl}_V = \text{End}(V)$. Then

$$\begin{aligned} (\text{ad } x)(y) &= [x, y] = x \circ y - y \circ x \\ (\text{ad } x)^2(y) &= [x, [x, y]] = x^2 \circ y - 2x \circ y \circ x + y \circ x^2 \\ (\text{ad } x)^3(y) &= x^3 \circ y - 3x^2 \circ y \circ x + 3x \circ y \circ x^2 - y \circ x^3 \\ &\dots \end{aligned}$$

In general, $(\text{ad } x)^m(y)$ is a sum of terms $x^j \circ y \circ x^{m-j}$ with $0 \leq j \leq m$. Therefore, if $x^n = 0$, then $(\text{ad } x)^{2n} = 0$. \square

We now prove (3.11). By induction, we may assume that the statement holds for Lie algebras of dimension less than $\dim \mathfrak{g}$. Also, we may replace \mathfrak{g} with its image in \mathfrak{gl}_V , and so assume that $\mathfrak{g} \subset \mathfrak{gl}_V$.

Let \mathfrak{h} be a proper subalgebra of \mathfrak{g} . We claim that $n_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h}$.⁵ The lemma shows that $\text{ad } x: \mathfrak{gl}_V \rightarrow \mathfrak{gl}_V$ is nilpotent for all $x \in \mathfrak{g}$. For any $x \in \mathfrak{h}$, $\text{ad } x$ preserves both \mathfrak{g} and \mathfrak{h} , and it induces a nilpotent endomorphism on $\mathfrak{g}/\mathfrak{h}$. Therefore, by induction ($\dim \mathfrak{h} < \dim \mathfrak{g}$), there exists nonzero element $y + \mathfrak{h}$ of $\mathfrak{g}/\mathfrak{h}$ such that $[\mathfrak{h}, y + \mathfrak{h}] \subset \mathfrak{h}$. Such a $y \in n_{\mathfrak{g}}(\mathfrak{h}) \setminus \mathfrak{h}$.

This shows that, when \mathfrak{h} is a maximal proper subalgebra \mathfrak{h} of \mathfrak{g} , its normalizer $n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$, and so \mathfrak{h} is an ideal in \mathfrak{g} . Hence, for any $x \in \mathfrak{g} \setminus \mathfrak{h}$, the subspace $\mathfrak{h} + \langle x \rangle$ of \mathfrak{g} is a Lie subalgebra. Since it properly contains \mathfrak{h} , it equals \mathfrak{g} .

Let $W = \{v \in V \mid \mathfrak{h}v = 0\}$; then $W \neq 0$ by induction ($\dim \mathfrak{h} < \dim \mathfrak{g}$). Because x acts nilpotently on W , there exists a nonzero $v \in W$ such that $xv = 0$. Now $\mathfrak{g}v = (\mathfrak{h} + \langle x \rangle)v = 0$.

3c Solvable Lie algebras: Lie's theorem

THEOREM 3.14 *Let V be a finite-dimensional vector space over an algebraically closed field k of characteristic zero, and let \mathfrak{g} be a subalgebra of \mathfrak{gl}_V . If \mathfrak{g} is solvable, then there exists a basis of V for which \mathfrak{g} is contained in $\mathfrak{b}_{\dim V}$.*

In other words, there exists a basis e_1, \dots, e_n for V such that


$$\mathfrak{g}e_i \subset \langle e_1, \dots, e_i \rangle, \text{ all } i.$$


COROLLARY 3.15 *Assume k has characteristic zero. If \mathfrak{g} is solvable, then $[\mathfrak{g}, \mathfrak{g}]$ is nilpotent.*

PROOF. We may suppose that k is algebraically closed (3.8). It suffices to show that $\text{ad}(\mathfrak{g})$ is solvable, and so we may suppose that $\mathfrak{g} \subset \mathfrak{gl}_V$ for some finite-dimensional vector space V . According to Lie's theorem, there exists a basis of V for which \mathfrak{g} is contained in $\mathfrak{b}_{\dim V}$. Then $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{n}_{\dim V}$, which is nilpotent. \square

In order for the map $v \mapsto xv$ be trigonalizable, all of its eigenvalues must lie in k . This explains why k is required to be algebraically closed. The condition that k have characteristic zero is more surprising, but the following examples shows that it is necessary.

EXAMPLES IN NONZERO CHARACTERISTIC

 3.16 In characteristic 2, \mathfrak{sl}_2 is solvable but for no basis is it contained in \mathfrak{b}_2 .

 3.17 Let k have characteristic $p \neq 0$, and consider the matrices

$$x = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & p-2 & 0 \\ 0 & 0 & \cdots & 0 & p-1 \end{pmatrix}.$$

⁵Cf.: Let H be a proper subgroup of a finite nilpotent group G ; then $H \neq N_G(H)$ (GT 6.20).


Then

$$[x, y] = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p-1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p-2 \\ p-1 & 0 & 0 & \cdots & 0 \end{pmatrix} = x$$

(this uses that $p \neq 0$). Therefore, $\mathfrak{g} = \langle x, y \rangle$ is a solvable subalgebra of \mathfrak{gl}_p . The matrices x and y have the following eigenvectors:

$$x : \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}; \quad y : \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Therefore \mathfrak{g} has no simultaneous eigenvector, and so Lie's theorem fails.

3.18 Even the corollary fails in nonzero characteristic. Note that it implies that, for a solvable subalgebra \mathfrak{g} of \mathfrak{gl}_V , the derived algebra $[\mathfrak{g}, \mathfrak{g}]$ consists of nilpotent endomorphisms. Example (a), and example (b) in the case $\text{char}(k) = 2$, and show that this is false in characteristic 2. For more examples in all nonzero characteristics, see Humphreys 1972, §4, Exercise 4. 

PROOF OF LIE'S THEOREM

LEMMA 3.19 (INVARIANCE LEMMA) *Let V be a finite-dimensional vector space, and let \mathfrak{g} be a Lie subalgebra of \mathfrak{gl}_V . For any ideal \mathfrak{a} in \mathfrak{g} and linear map $\lambda: \mathfrak{a} \rightarrow k$, the eigenspace*

$$V_\lambda = \{v \in V \mid av = \lambda(a)v \text{ for all } a \in \mathfrak{a}\} \tag{147}$$

is invariant under \mathfrak{g} .

PROOF. Let $x \in \mathfrak{g}$ and let $v \in V_\lambda$. We have to show that $xv \in V_\lambda$, but for $a \in \mathfrak{a}$,

$$a(xv) = x(av) + [a, x](v) = \lambda(a)xv + \lambda([a, x])v.$$

Thus a nonzero V_λ is invariant under \mathfrak{g} if and only if $\lambda([\mathfrak{a}, \mathfrak{g}]) = 0$.

Fix an $x \in \mathfrak{g}$ and a nonzero $v \in V_\lambda$, and consider the subspaces

$$\langle v \rangle \subset \langle v, xv \rangle \subset \cdots \subset \langle v, xv, \dots, x^{i-1}v \rangle \subset \cdots$$

of V . Let m be the first integer such that $\langle v, \dots, x^{m-1}v \rangle = \langle v, \dots, x^m v \rangle$. Then

$$W \stackrel{\text{def}}{=} \langle v, xv, \dots, x^{m-1}v \rangle$$

has basis $v, xv, \dots, x^{m-1}v$ and contains $x^i v$ for all i .

We claim that an element a of \mathfrak{a} maps W into itself and has matrix

$$\begin{pmatrix} \lambda(a) & * & \cdots & * \\ 0 & \lambda(a) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda(a) \end{pmatrix}$$

with respect to the given basis. We check this column by column. The equality

$$av = \lambda(a)v$$

shows that the first column is as claimed. As $[a, x] \in \mathfrak{a}$,

$$\begin{aligned} a(xv) &= x(av) + [a, x]v \\ &= \lambda(a)xv + \lambda([a, x])v, \end{aligned}$$

and so that the second column is as claimed (with $*$ = $\lambda([a, x])$). Assume that the first i columns are as claimed, and consider

$$a(x^i v) = ax(x^{i-1}v) = (xa + [a, x])x^{i-1}v. \quad (148)$$

From knowing the i th column, we find that

$$a(x^{i-1}v) = \lambda(a)x^{i-1}v + u \quad (149)$$

$$[a, x](x^{i-1}v) = \lambda([a, x])x^{i-1}v + u' \quad (150)$$

with $u, u' \in \langle v, xv, \dots, x^{i-2}v \rangle$. On multiplying (149) with x we obtain the equality

$$xa(x^{i-1}v) = \lambda(a)x^i v + xu \quad (151)$$

with $xu \in \langle v, xv, \dots, x^{i-1}v \rangle$. Now (148), (150), and (151) show that the $(i + 1)$ st column is as claimed.

This completes the proof that the matrix of $a \in \mathfrak{a}$ acting on W has the form claimed, and shows that

$$\mathrm{Tr}_W(a) = m\lambda(a). \quad (152)$$

We now complete the proof of the lemma by showing that $\lambda([\mathfrak{a}, \mathfrak{g}]) = 0$. Let $a \in \mathfrak{a}$ and $x \in \mathfrak{g}$. On applying (152) to the element $[a, x]$ of \mathfrak{a} , we find that

$$m\lambda([a, x]) = \mathrm{Tr}_W([a, x]) = \mathrm{Tr}_W(ax - xa) = 0,$$

and so $\lambda([a, x]) = 0$ (because $m \neq 0$ in k). \square

LEMMA 3.20 *Under the hypotheses of Lie's theorem, assume that $V \neq 0$; then there exists a nonzero vector $v \in V$ such that $\mathfrak{g}v \subset \langle v \rangle$.*

PROOF. We use induction on the dimension of \mathfrak{g} . If $\dim \mathfrak{g} = 1$, then $\mathfrak{g} = k\alpha$ for some endomorphism α of V , and α has an eigenvector because k is algebraically closed. Because \mathfrak{g} is solvable, its derived algebra $\mathfrak{g}' \neq \mathfrak{g}$. The quotient $\mathfrak{g}/\mathfrak{g}'$ is abelian, and so is essentially just a vector space. Write $\mathfrak{g}/\mathfrak{g}'$ as the direct sum of a subspace of codimension 1 and a subspace of dimension 1. This decomposition corresponds to a decomposition $\mathfrak{g} = \mathfrak{a} + \langle x \rangle$ with \mathfrak{a} and $\langle x \rangle$ ideals in \mathfrak{g} . By induction, there exists a nonzero $w \in V$ such that $\mathfrak{a}w \subset \langle w \rangle$, i.e., such that $aw = \lambda(a)w$, all $a \in \mathfrak{a}$, for some $\lambda: \mathfrak{a} \rightarrow k$. Let V_λ be the corresponding eigenspace for \mathfrak{a} (147). According to the Invariance Lemma, V_λ is stable under \mathfrak{g} . As it is nonzero, it contains a nonzero eigenvector v for x . Now, for any element $g = a + cx \in \mathfrak{g}$,

$$gv = \lambda(a)v + c(xv) \in \langle v \rangle. \quad \square$$

Lie's theorem follows directly from Lemma 3.20 (cf. the proof of (3.11) \Rightarrow (3.10)).

ASIDE 3.21 The proof shows that Lie's theorem holds when k has characteristic p provided that $\dim V < p$. This is a general phenomenon: for any specific problem, there will be a p_0 such that the characteristic p case behaves as the characteristic 0 case provided $p \geq p_0$.

3d Jordan decompositions

PROPOSITION 3.22 Let V be a finite-dimensional vector space over a perfect field. For any endomorphism α of V , there exist unique endomorphisms α_s and α_n of V such that

- (a) $\alpha = \alpha_s + \alpha_n$,
- (b) $\alpha_s \circ \alpha_n = \alpha_n \circ \alpha_s$, and
- (c) α_s is semisimple and α_n is nilpotent.

Moreover, each of α_s and α_n is a polynomial in α .

PROOF. Assume first that α has all of its eigenvalues in k , so that V is a direct sum of the generalized eigenspaces of α , say, $V = \bigoplus_{a \in I} V_a$ where I is the set of distinct eigenvalues of α (see I, 10.11). Define α_s to be the endomorphism of V that acts as a on V_a for each $a \in I$. Then α_s is a semisimple endomorphism of V , and $\alpha_n \stackrel{\text{def}}{=} \alpha - \alpha_s$ commutes α_s (because it does on each V_a) and is nilpotent (because it is so on each V_a). Thus α_s and α_n satisfy the conditions (a,b,c).

Let n_a be the multiplicity of an eigenvalue a . Because the polynomials $(T-a)^{n_a}$, $a \in I$, are relatively prime, the Chinese remainder theorem shows that there exists a $Q(T) \in k[T]$ such that

$$Q(T) \equiv a \pmod{(T-a)^{n_a}}$$

for all $a \in I$. Then $Q(\alpha)$ acts as a on V_a for each i , and so $\alpha_s = Q(\alpha)$. Moreover, $\alpha_n = \alpha - Q(\alpha)$.

The rest of the proof is similar to that of (I, 10.12). □

REMARK 3.23 (a) If $0 \in I$, then $Q(T)$ has no constant term. Otherwise, we can choose it satisfy the additional congruence

$$Q(T) \equiv 0 \pmod{T}$$

in order to achieve the same result.

(b) Suppose $k = \mathbb{C}$, and let \bar{a} denote the complex conjugate of a . There exists a $Q(T) \in \mathbb{C}[T]$ such that

$$Q(T) \equiv \bar{a} \pmod{(T-a)^{n_a}}$$

for all $a \in I$. Then $Q(\alpha)$ is an endomorphism of V that acts on V_a as \bar{a} . Again, we can choose $Q(T)$ to have no constant term.

The endomorphisms α_s and α_n are called the *semisimple* and *nilpotent parts* of α , and

$$\alpha = \alpha_s + \alpha_n$$

is the (*additive*) *Jordan decomposition* of α .

PROPOSITION 3.24 Let α be an endomorphism of a finite-dimensional vector space V over a perfect field. The Jordan decomposition of $\text{ad}(\alpha)$ in $\text{End}(\text{End}(V))$ is $\text{ad}(\alpha) = \text{ad}(\alpha_s) + \text{ad}(\alpha_n)$.

PROOF. Suppose first that α is semisimple. After a field extension, there will exist a basis $(e_i)_{1 \leq i \leq \dim V}$ of V for which α has matrix $\text{diag}(a_1, a_2, \dots)$. If $(e_{ij})_{1 \leq i, j \leq \dim V}$ is the corresponding basis for $\text{End}(V)$, then $\text{ad}(\alpha)e_{ij} = (a_i - a_j)e_{ij}$ for all i, j . Therefore $\text{ad}(\alpha)$ is semisimple.

For a general α , the decomposition $\alpha = \alpha_s + \alpha_n$ gives a decomposition $\text{ad}\alpha = \text{ad}\alpha_s + \text{ad}\alpha_n$. We have just seen that $\text{ad}(\alpha_s)$ is semisimple, and Lemma 3.13 shows that $\text{ad}(\alpha_n)$ is nilpotent. The two commute because

$$[\text{ad}\alpha_s, \text{ad}\alpha_n] = \text{ad}[\alpha_s, \alpha_n] = 0.$$

Therefore the decomposition $\text{ad}\alpha = \text{ad}\alpha_s + \text{ad}\alpha_n$ satisfies the conditions (a,b,c) of (3.22). \square

3e Cartan's first criterion

THEOREM 3.25 (CARTAN'S CRITERION) *Let \mathfrak{g} be a subalgebra of \mathfrak{gl}_V , where V is a finite-dimensional vector space over a field k of characteristic zero. Then \mathfrak{g} is solvable if $\text{Tr}_V(x \circ y) = 0$ for all $x, y \in \mathfrak{g}$.*

PROOF. We first observe that, if k' is a field containing k , then the theorem is true for $\mathfrak{g} \subset \mathfrak{gl}_V$ if and only if it is true for $\mathfrak{g}_{k'} \subset \mathfrak{gl}_{V_{k'}}$ (because, for example, \mathfrak{g} is solvable if and only if $\mathfrak{g}_{k'}$ is solvable). Therefore, we may assume that k is finitely generated over \mathbb{Q} , hence embeddable in \mathbb{C} , and then that $k = \mathbb{C}$.

We shall show that the condition implies that each $x \in [\mathfrak{g}, \mathfrak{g}]$ defines a nilpotent endomorphism of V . Then Engel's theorem 3.10 will show that $[\mathfrak{g}, \mathfrak{g}]$ is nilpotent, and it will follow that \mathfrak{g} is solvable (3.3b).

Let $x \in [\mathfrak{g}, \mathfrak{g}]$, and fix a basis of V for which the matrix of x_s is diagonal, say, $\text{diag}(a_1, \dots, a_n)$, and the matrix of x_n is strictly upper triangular. We have to show that $x_s = 0$, and for this it suffices to show that

$$\bar{a}_1 a_1 + \dots + \bar{a}_n a_n = 0.$$

Note that

$$\text{Tr}_V(\bar{x}_s \circ x) = \bar{a}_1 a_1 + \dots + \bar{a}_n a_n,$$

where $\bar{x}_s = \text{diag}(\bar{a}_1, \dots, \bar{a}_n)$. By assumption, x is a sum of commutators $[y, z]$, and so it suffices to show that

$$\text{Tr}_V(\bar{x}_s \circ [y, z]) = 0, \quad \text{all } y, z \in \mathfrak{g}.$$

From the trivial identity (see 5.8 below)

$$\text{Tr}_V(a \circ [b, c]) = \text{Tr}_V([a, b] \circ c), \quad a, b, c \in \text{End}(V),$$

we see that it suffices to show that

$$\text{Tr}_V([\bar{x}_s, y] \circ z) = 0, \quad \text{all } y, z \in \mathfrak{g}. \quad (153)$$

This will follow from the hypothesis once we have shown that $[\bar{x}_s, y] \in \mathfrak{g}$. According to (3.23(b)),

$$\bar{x}_s = c_1 x + c_2 x^2 + \dots, \quad \text{for some } c_i \in k,$$

and so

$$[\bar{x}_s, \mathfrak{g}] \subset \mathfrak{g}$$

because $[x, \mathfrak{g}] \subset \mathfrak{g}$. \square

COROLLARY 3.26 *Let V be a finite-dimensional vector space over a field k of characteristic zero, and let \mathfrak{g} be a subalgebra of \mathfrak{gl}_V . If \mathfrak{g} is solvable, then $\mathrm{Tr}_V(x \circ y) = 0$ for all $x \in \mathfrak{g}$ and $y \in [\mathfrak{g}, \mathfrak{g}]$. Conversely, if $\mathrm{Tr}_V(x \circ y) = 0$ for all $x, y \in [\mathfrak{g}, \mathfrak{g}]$, then \mathfrak{g} is solvable.*

PROOF. Recall (3.8) that \mathfrak{g} is solvable if and only if $\mathfrak{g}_{k^{\mathrm{al}}}$ is solvable, and so we may suppose that k is algebraically closed. According to Lie's theorem 3.14, there exists a basis of V for which $\mathfrak{g} \subset \mathfrak{b}_n$, $n = \dim V$. Then $[\mathfrak{g}, \mathfrak{g}] \subset [\mathfrak{b}_n, \mathfrak{b}_n] = \mathfrak{n}_n$, from which the statement follows.

For the converse, note that the condition implies that $[\mathfrak{g}, \mathfrak{g}]$ is solvable by (3.25). But this implies that \mathfrak{g} is solvable (because $\mathfrak{g}^{(m)} = (\mathfrak{g}')^{(m-1)}$). \square

ASIDE 3.27 In the above proofs, it is possible to avoid passing to the case $k = \mathbb{C}$. Roughly speaking, instead of complex conjugation, one uses the elements of the dual of the subspace of k generated by the eigenvalues of x_s . See, for example, Humphreys 1972, 4.3.

4 Unipotent algebraic groups and nilpotent Lie algebras

In characteristic zero, the functor Lie is an equivalence from the category unipotent algebraic groups to that of nilpotent Lie algebras. The purpose of this section is to extract the proof of this from DG (see IV, §2, 4.5). It may be skipped by the reader, since it is not used later, and it exists only as a preliminary draft. (Cf. mo10730).

Throughout, k is a field of characteristic zero.

4a Preliminaries on Lie algebras

THE HAUSDORFF SERIES

For a nilpotent $n \times n$ matrix X ,

$$\exp(X) \stackrel{\mathrm{def}}{=} I + X + X^2/2! + X^3/3! + \dots$$

is a well defined element of $\mathrm{GL}_n(k)$. Moreover, when X and Y are nilpotent,

$$\exp(X) \cdot \exp(Y) = \exp(W)$$

for some nilpotent W , and we may ask for a formula expressing W in terms of X and Y . This is provided by the **Hausdorff series**⁶, which is a formal power series,

$$H(X, Y) = \sum_{n \geq 0} H^n(X, Y), \quad H^n(X, Y) \text{ homogeneous of degree } n,$$

with coefficients in \mathbb{Q} . The first few terms are

$$\begin{aligned} H^1(X, Y) &= X + Y \\ H^2(X, Y) &= \frac{1}{2}[X, Y]. \end{aligned}$$

⁶According to the Wikipedia, the formula was first noted in print by Campbell (1897); elaborated by Henri Poincaré (1899) and Baker (1902); and systematized geometrically, and linked to the Jacobi identity by Hausdorff (1906). I follow Bourbaki's terminology — others write Baker-Campbell-Hausdorff, or Campbell-Hausdorff, or ...

If \mathfrak{g} is a nilpotent Lie algebra over a field k of characteristic zero, then $H^n(x, y) = 0$ for $x, y \in \mathfrak{g}$ and n sufficiently large; we therefore have a morphism

$$\mathfrak{h}: \mathfrak{g}_\alpha \times \mathfrak{g}_\alpha \rightarrow \mathfrak{g}_\alpha$$

such that, for all k -algebras R , and $x, y \in \mathfrak{g}_R$,

$$\mathfrak{h}(x, y) = \sum_{n \geq 0} \mathfrak{h}^n(X, Y).$$

If x and y are nilpotent elements of $\mathrm{GL}_n(k)$, then

$$\exp(x) \cdot \exp(y) = \exp(\mathfrak{h}(x, y)),$$

and this determines the power series $H(X, Y)$ uniquely. See Bourbaki LIE, II.

ADO'S THEOREM

THEOREM 4.1 *Let \mathfrak{g} be a finite-dimensional Lie algebra over a field of characteristic zero, and let \mathfrak{n} be its largest nilpotent ideal. Then there exists a faithful representation (V, r) of \mathfrak{g} such that $r(\mathfrak{n})$ consists of nilpotent elements.*

PROOF. Bourbaki LIE, I, §7, 3. □

4b Preliminaries on unipotent groups

We need to use a little algebraic geometry, but only over an algebraically closed field; in fact, we only need the first ten chapters of AG.

NOTES The results in this subsection don't require k to be of characteristic zero, and should be moved to Chapter I.

LEMMA 4.2 *Let U be a unipotent subgroup of an algebraic group G . Then G/U is isomorphic to a subscheme of an affine scheme (DG IV 2 2.8, p. 489).*

PROOF. Let (V, r) be a representation of G such that U is the stabilizer of a line L in V . As U is unipotent, it acts trivially on L , and so $L^U = L$. For any nonzero $x \in L$, the map $g \mapsto gx$ is an injective regular map $G/U \rightarrow V_\alpha$. □

LEMMA 4.3 *For any connected algebraic group G , the quotient $\mathrm{Ker}(\mathrm{Ad}: G \rightarrow \mathrm{GL}_\mathfrak{g})/Z(G)$ is unipotent (DG IV 2 2.12, p. 490).*

PROOF. We may suppose that k is algebraically closed. Let $\mathcal{O}_e = \mathcal{O}(G)_e$ (the local ring at the identity element), and let \mathfrak{m}_e be its maximal ideal. Then G acts on k -vector space $\mathcal{O}_e/\mathfrak{m}_e^{r+1}$ by k -algebra homomorphisms. By definition, $\mathrm{Ker}(\mathrm{Ad})$ acts trivially on $\mathfrak{m}_e/\mathfrak{m}_e^2$, and so it acts trivially on each of the quotients $\mathfrak{m}_e^i/\mathfrak{m}_e^{i+1}$. Let C_r be the centralizer of $\mathcal{O}(G)_e/\mathfrak{m}^{r+1}$ in G (see Section 2). We have shown that $\mathrm{Ker}(\mathrm{Ad})/C_r$ is unipotent. It remains to show that $C_r = Z(G)$ for r sufficiently large. □

PROPOSITION 4.4 *Let G be a smooth connected algebraic group over an algebraically closed field k . If G contains no subgroup isomorphic to \mathbb{G}_m , then it is unipotent (DG IV 2 3.11, p. 496).*

PROOF. Let (V, r) be a faithful representation of G , and let F be the variety of maximal flags in V . Then G acts on V , and according to AG 10.6, there exists a closed orbit, say $Gd \simeq G/U$. Then U is solvable, and so, by the Lie-Kolchin theorem 16.31, $U_{\text{red}}^\circ \subset \mathbb{T}_n$ for some choice of basis. By hypothesis, $U_{\text{red}}^\circ \cap \mathbb{D}_n = 0$, and so U_{red}° is unipotent. Now G/U_{red}° is affine and connected, and so its image in F is a point. Hence $G = U_{\text{red}}^\circ$. \square

COROLLARY 4.5 *Let G be a smooth connected algebraic group. The following conditions are equivalent:*

- (a) G is unipotent;
- (b) The centre of G is unipotent and $\text{Lie}(G)$ is nilpotent;
- (c) For every representation (V, r) of G , $\text{Lie } r$ maps the elements of $\text{Lie}(G)$ to nilpotent endomorphisms of V ;
- (d) Condition (c) holds for one faithful representation (V, r) .

(DG IV 2 3.12, p. 496.)

PROOF. (a) \Rightarrow (c). There exists a basis for V such that G maps into \mathbb{U}_n (see I, 15.4).

(c) \Rightarrow (d). Trivial.

(a) \Rightarrow (b). Every subgroup of a unipotent group is unipotent (I, 15.7), and G has a filtration whose quotients are isomorphic to subgroups of \mathbb{G}_a (I, 15.14).

(d) \Rightarrow (a). We may assume that k is algebraically closed (I, 15.10). If G contains a subgroup H isomorphic to \mathbb{G}_m , then $V = \bigoplus_{n \in \mathbb{Z}} V_n$ where $h \in H(k)$ acts on V_n as h^n . Then $x \in \text{Lie}(H)$ acts on V_n as nx , which contradicts the hypothesis.

(b) \Rightarrow (a). The kernel of the adjoint representation is unipotent (in characteristic zero, it is $Z(G)$ — see 5.30 below; in general it is an extension of unipotent groups, and hence is unipotent by 15.7). Suppose that G contains a subgroup H isomorphic to \mathbb{G}_m . Then H acts faithfully on \mathfrak{g} , and its elements act semisimply, contradicting the nilpotence of \mathfrak{g} . \square

PROOF OF THE MAIN THEOREM

Let $H(X, Y) = \sum_{n>0} H^n(X, Y)$ denote the Hausdorff series. Recall (I, 3.6) that, for a finite-dimensional vector space V , $V_{\mathfrak{a}}$ denotes the algebraic group $R \rightsquigarrow R \otimes_k V$.

PROPOSITION 4.6 *Let G be a unipotent algebraic group. Then*

$$\exp(x) \cdot \exp(y) = \exp(\mathfrak{h}(x, y)) \quad (154)$$

for all $x, y \in \mathfrak{g}_R$ and k -algebras R .

PROOF. We may identify G with a subgroup of GL_V for some finite-dimensional vector space V . Then $\mathfrak{g} \subset \mathfrak{gl}_V$, and, because G is unipotent, \mathfrak{g} is nilpotent. Now (154) holds in G because it holds in GL_V . \square

THEOREM 4.7 Assume $\text{char}(k) = 0$.

(a) For any finite-dimensional nilpotent Lie algebra over k , the maps

$$(x, y) \mapsto \sum_{n>0} H^n(x, y): \mathfrak{g}(R) \times \mathfrak{g}(R) \rightarrow \mathfrak{g}(R)$$

(R a k -algebra) make \mathfrak{g}_α into a unipotent algebraic group over k .

(b) The functor $\mathfrak{g} \rightsquigarrow \mathfrak{g}_\alpha$ is an equivalence from the category of finite-dimensional nilpotent Lie algebras over k to the category of unipotent algebraic groups, with quasi-inverse $G \rightsquigarrow \text{Lie}(G)$.

PROOF. (a) Ado's theorem allows us to identify \mathfrak{g} with a Lie subalgebra of \mathfrak{gl}_V whose elements are nilpotent endomorphisms of V . Now (3.10) shows that there exists a basis of V for which \mathfrak{g} is contained in the Lie subalgebra \mathfrak{n} of \mathfrak{gl}_n consisting of strictly upper triangular matrices. Endow \mathfrak{n}_α with the multiplication

$$(x, y) \mapsto \sum_n H^n(x, y), \quad x, y \in R \otimes \mathfrak{n}_n, \quad R \text{ a } k\text{-algebra.}$$

According to the above discussion, we obtain in this way an algebraic group isomorphic to \mathbb{U}_n . It is clear that \mathfrak{g}_α is an affine subgroup of \mathfrak{n}_α . It remains to show that $\text{Lie}(\mathfrak{g}_\alpha) = \mathfrak{g}$ (as a Lie subalgebra of \mathfrak{gl}_n), but this follows from the definitions.

(b) We saw in the proof of (a) that $\text{Lie}(\mathfrak{g}_\alpha) \simeq \mathfrak{g}$, and it follows that $G \simeq (\text{Lie } G)_\alpha$. \square

COROLLARY 4.8 Every Lie subalgebra of \mathfrak{gl}_V formed of nilpotent endomorphisms is algebraic.

See also §1m.

REMARK 4.9 In the equivalence of categories in (b), commutative Lie algebras (i.e., finite-dimensional vector spaces) correspond to commutative unipotent algebraic groups. In other words, $U \rightsquigarrow \text{Lie}(U)$ is an equivalence from the category of commutative unipotent algebraic groups over a field of characteristic zero to the category of finite-dimensional vector spaces, with quasi-inverse $V \rightsquigarrow V_\alpha$.

NONZERO CHARACTERISTIC

ASIDE 4.10 Unipotent groups over fields of nonzero characteristic are very complicated. For example, if $p > 2$, then there exist many "fake Heisenberg groups" (connected noncommutative smooth unipotent algebraic groups of exponent p and dimension 2) over finite fields.

ASIDE 4.11 The nilpotent Lie algebras in low dimension have been classified:

Many articles on the classification of low-dimensional Lie algebras do contain mistakes. To the best of my knowledge, the full detailed proof is provided in the dissertation of Ming-Peng Gong, where he classifies all algebras up to dimension 7 over algebraically closed fields of any characteristics except 2, and also over \mathbb{R} . (mo21114, mathreader)

There is indeed a lot of work devoted to the classification of nilpotent Lie algebras of low dimension . . . , with numerous mistakes and omissions. Even worse, they use different nomenclature and invariants to classify the algebras, and it is a nontrivial task to compare different lists. Luckily, Willem de Graaf undertook the painstaking task to make order out of this somewhat messy situation in "Classification of 6-dimensional

nilpotent Lie algebras over fields of characteristic not 2”, J. Algebra 309 (2007), 640-653; arXiv:math/0511668 . Even better, he provides an algorithm for identifying any given nilpotent Lie algebra with one in his list, and the corresponding code is available as a part of GAP package. He builds on earlier work of Skjelbred-Sund and his own method of identification of Lie algebras by means of Groebner bases. (mo21114, Pasha Zusmanovich)

5 Semisimple Lie algebras and algebraic groups

Throughout this section, k has characteristic zero, and all Lie algebras are of finite dimension over k .

5a Semisimple Lie algebras

DEFINITION 5.1 A Lie algebra \mathfrak{g} is said to be *semisimple* if its only abelian ideal is $\{0\}$ (Bourbaki LIE I, §6, 1).

5.2 The algebra $\{0\}$ is semisimple, but no Lie algebra of dimension 1 or 2 is semisimple (because they are all abelian). There exist semisimple Lie algebras of dimension 3, for example, \mathfrak{sl}_2 (see 5.10 below).

5.3 A Lie algebra \mathfrak{g} is semisimple if and only its radical $r(\mathfrak{g}) = 0$. (Recall (3.5) that $r(\mathfrak{g})$ is the largest solvable ideal in \mathfrak{g} . If $r(\mathfrak{g}) \neq 0$, then the last nonzero term of its derived series is an abelian ideal in \mathfrak{g} ; if $r(\mathfrak{g}) = 0$, then every abelian ideal is zero because it is contained in $r(\mathfrak{g})$.)

5.4 For any Lie algebra \mathfrak{g} , the quotient $\mathfrak{g}/r(\mathfrak{g})$ is semisimple. (A nonzero abelian ideal in $\mathfrak{g}/r(\mathfrak{g})$ would correspond to a solvable ideal in \mathfrak{g} properly containing $r(\mathfrak{g})$.)

5.5 A product $\mathfrak{g} = \mathfrak{g}_1 \times \cdots \times \mathfrak{g}_n$ of semisimple Lie algebras is semisimple. (Let \mathfrak{a} be an abelian ideal in \mathfrak{g} ; the projection of \mathfrak{a} in \mathfrak{g}_i is zero for each i , and so \mathfrak{a} is zero.)

5.6 A Lie algebra \mathfrak{g} is said to be *reductive* if its radical equals its centre; a reductive Lie algebra \mathfrak{g} decomposes into a direct product of Lie algebras

$$\mathfrak{g} = \mathfrak{c} \times [\mathfrak{g}, \mathfrak{g}]$$

with \mathfrak{c} commutative and $[\mathfrak{g}, \mathfrak{g}]$ semisimple (Bourbaki LIE, I, §6, 4).

TRACE FORMS

Let \mathfrak{g} be a Lie algebra. A symmetric k -bilinear form $B: \mathfrak{g} \times \mathfrak{g} \rightarrow k$ on \mathfrak{g} is said to be *associative*⁷ if

$$B([x, y], z) = B(x, [y, z]) \quad \text{for all } x, y, z \in \mathfrak{g}.$$

LEMMA 5.7 Let B be an associative form on \mathfrak{g} , and let \mathfrak{a} be an ideal in \mathfrak{g} . The orthogonal complement \mathfrak{a}^\perp of \mathfrak{a} with respect to B is again an ideal. If B is nondegenerate, then $\mathfrak{a} \cap \mathfrak{a}^\perp$ is abelian.

⁷Bourbaki LIE, I, §3, 6, says “invariant” instead of “associative”.

PROOF. By definition

$$\mathfrak{a}^\perp = \{x \in \mathfrak{g} \mid B(\mathfrak{a}, x) = 0\}.$$

Let $a' \in \mathfrak{a}^\perp$ and $x \in \mathfrak{g}$. Then, for $a \in \mathfrak{a}$,

$$B(a, [x, a']) = -B(a, [a', x]) = -B([a, a'], x) = 0$$

and so $[x, a'] \in \mathfrak{a}^\perp$. This shows that \mathfrak{a}^\perp is an ideal.

Now assume that B is nondegenerate, and let \mathfrak{b} be an ideal in \mathfrak{g} such that $B|_{\mathfrak{b} \times \mathfrak{b}} = 0$. For $x, y \in \mathfrak{b}$ and $z \in \mathfrak{g}$, $B([x, y], z) = B(x, [y, z])$, which is zero because $[y, z] \in \mathfrak{b}$. Hence $[x, y] = 0$, and so \mathfrak{b} is abelian. \square

Let $\rho: \mathfrak{g} \rightarrow \mathfrak{gl}_V$ be a representation of \mathfrak{g} on a finite-dimensional vector space V . For $x \in \mathfrak{g}$, write x_V for $\rho(x)$. The **trace form** $\beta_V: \mathfrak{g} \times \mathfrak{g} \rightarrow k$ defined by V is

$$(x, y) \mapsto \text{Tr}_V(x_V \circ y_V), \quad x, y \in \mathfrak{g}.$$

LEMMA 5.8 *The trace form is a symmetric bilinear form on \mathfrak{g} , and it is associative:*

$$\beta_V([x, y], z) = \beta_V(x, [y, z]), \quad \text{all } x, y, z \in \mathfrak{g}.$$

PROOF. It is k -bilinear because ρ is linear, composition of maps is bilinear, and trace is linear. It is symmetric because for any $n \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$,

$$\text{Tr}(AB) = \sum_{i,j} a_{ij} b_{ji} = \text{Tr}(BA). \quad (155)$$

It is associative because for $x, y, z \in \mathfrak{g}$,

$$\begin{aligned} \beta_V([x, y], z) &= \text{Tr}([x, y] \circ z) = \text{Tr}(x \circ y \circ z) - \text{Tr}(y \circ x \circ z) \quad (\text{definitions}) \\ &= \text{Tr}(x \circ y \circ z) - \text{Tr}(x \circ z \circ y) \quad (\text{apply (155)}) \\ &= \text{Tr}(x \circ [y, z]) = \beta_V(x, [y, z]) \quad (\text{definitions}). \quad \square \end{aligned}$$

Therefore (see 5.7), the orthogonal complement \mathfrak{a}^\perp of an ideal \mathfrak{a} of \mathfrak{g} with respect to a trace form is again an ideal.

PROPOSITION 5.9 *If $\rho: \mathfrak{g} \rightarrow \mathfrak{gl}_V$ is faithful and \mathfrak{g} is semisimple, then β_V is nondegenerate.*

PROOF. We have to show that $\mathfrak{g}^\perp = 0$, but we know that it is an ideal (5.7), and Cartan's criterion (3.25) shows that it is solvable because

$$\text{Tr}_V(x_V \circ y_V) = \beta_V(x, y) = 0$$

for all $x, y \in \mathfrak{g}^\perp$. \square

THE CARTAN-KILLING CRITERION

The trace form for the adjoint representation $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$ is called the **Killing form**⁸ $\kappa_{\mathfrak{g}}$ on \mathfrak{g} . Thus,

$$\kappa_{\mathfrak{g}}(x, y) = \text{Tr}_{\mathfrak{g}}(\text{ad}(x) \circ \text{ad}(y)), \quad \text{all } x, y \in \mathfrak{g}.$$

In other words, $\kappa_{\mathfrak{g}}(x, y)$ is the trace of the k -linear map

$$z \mapsto [x, [y, z]]: \mathfrak{g} \rightarrow \mathfrak{g}.$$

EXAMPLE 5.10 The Lie algebra \mathfrak{sl}_2 consists of the 2×2 matrices with trace zero. It has as basis the elements⁹

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and

$$[h, x] = 2x, \quad [h, y] = -2y, \quad [x, y] = h.$$

Then

$$\text{ad } x = \begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{ad } h = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \text{ad } y = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

and so the top row $(\kappa(x, x), \kappa(x, h), \kappa(x, y))$ of the matrix of κ consists of the traces of

$$\begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In fact, κ has matrix $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 0 \end{pmatrix}$, which has determinant -128 .

Note that, for \mathfrak{sl}_n , the matrix of κ is $n^2 - 1 \times n^2 - 1$, and so this is not something one would like to compute.

LEMMA 5.11 *Let \mathfrak{a} be an ideal in \mathfrak{g} . The Killing form on \mathfrak{g} restricts to the Killing form on \mathfrak{a} , i.e.,*

$$\kappa_{\mathfrak{g}}(x, y) = \kappa_{\mathfrak{a}}(x, y) \quad \text{all } x, y \in \mathfrak{a}.$$

PROOF. Let α be an endomorphism of a vector space V such that $\alpha(V) \subset W$; then $\text{Tr}_V(\alpha) = \text{Tr}_W(\alpha|_W)$, because when we choose a basis for W and extend it to a basis for V , the matrix for α takes the form $\begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix}$ where A is the matrix of $\alpha|_W$. If $x, y \in \mathfrak{a}$, then $\text{ad } x \circ \text{ad } y$ is an endomorphism of \mathfrak{g} mapping \mathfrak{g} into \mathfrak{a} , and so its trace (on \mathfrak{g}), $\kappa_{\mathfrak{g}}(x, y)$, equals

$$\text{Tr}_{\mathfrak{a}}(\text{ad } x \circ \text{ad } y|_{\mathfrak{a}}) = \text{Tr}_{\mathfrak{a}}(\text{ad}_{\mathfrak{a}} x \circ \text{ad}_{\mathfrak{a}} y) = \kappa_{\mathfrak{a}}(x, y). \quad \square$$

⁸Also called the **Cartan-Killing form**. According to Bourbaki (Note Historique to I, II, III), E. Cartan introduced the ‘‘Killing form’’ in his thesis and proved the two fundamental criteria: a Lie algebra is solvable if its Killing form is trivial (5.12); a Lie algebra is semisimple if its Killing form is nondegenerate (5.13). According to Helgason 1990, Killing introduced the Killing form, but Cartan made much more use of it.

⁹Some authors write (h, e, f) for (h, x, y) ; Bourbaki LIE, I, §6, 7, writes (H, X, Y) ; in VIII, §1, 1, *Base canonique de \mathfrak{sl}_2* , he writes $(H, X_+, -X_-)$, i.e., he sets $X_- = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$.

PROPOSITION 5.12 *If $\kappa_{\mathfrak{g}}(\mathfrak{g}, [\mathfrak{g}, \mathfrak{g}]) = 0$, then \mathfrak{g} is solvable.*

PROOF. The map $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$ has kernel the centre $z(\mathfrak{g})$ of \mathfrak{g} , and the condition implies that the image is solvable (Cartan's criterion, 3.26). \square

THEOREM 5.13 (*Cartan-Killing criterion*). *A nonzero Lie algebra \mathfrak{g} is semisimple if and only if its Killing form is nondegenerate.*

PROOF. \Rightarrow : Because \mathfrak{g} is semisimple, the adjoint representation $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$ is faithful, and so this follows (5.9).

\Leftarrow : Let \mathfrak{a} be an abelian ideal of \mathfrak{g} — we have to show that $\mathfrak{a} = 0$. For any $a \in \mathfrak{a}$ and $g \in \mathfrak{g}$, we have that

$$\mathfrak{g} \xrightarrow{\text{ad } g} \mathfrak{g} \xrightarrow{\text{ad } a} \mathfrak{a} \xrightarrow{\text{ad } g} \mathfrak{a} \xrightarrow{\text{ad } a} 0,$$

and so $(\text{ad } a \circ \text{ad } g)^2 = 0$. But an endomorphism of a vector space whose square is zero has trace zero (because its minimum polynomial divides X^2 , and so its eigenvalues are zero). Therefore

$$\kappa_{\mathfrak{g}}(a, g) \stackrel{\text{def}}{=} \text{Tr}_{\mathfrak{g}}(\text{ad } a \circ \text{ad } g) = 0,$$

and $\mathfrak{a} \subset \mathfrak{g}^{\perp} = 0$. \square

COROLLARY 5.14 *Let \mathfrak{g} be a Lie algebra over a field k , and let k' be a field containing k .*

- (a) *The Lie algebra \mathfrak{g} is semisimple if and only if $\mathfrak{g}_{k'}$ is semisimple.*
- (b) *The radical $r(\mathfrak{g}_{k'}) \simeq k' \otimes_k r(\mathfrak{g})$.*

PROOF. (a) The Killing form of $\mathfrak{g}_{k'}$ is obtained from that of \mathfrak{g} by extension of scalars.

(b) The exact sequence

$$0 \rightarrow r(\mathfrak{g}) \rightarrow \mathfrak{g} \rightarrow \mathfrak{g}/r(\mathfrak{g}) \rightarrow 0$$

gives rise to an exact sequence

$$0 \rightarrow r(\mathfrak{g})_{k'} \rightarrow \mathfrak{g}_{k'} \rightarrow (\mathfrak{g}/r(\mathfrak{g}))_{k'} \rightarrow 0.$$

As $r(\mathfrak{g})_{k'}$ is solvable (3.8) and $(\mathfrak{g}/r(\mathfrak{g}))_{k'}$ is semisimple, the sequence shows that $r(\mathfrak{g})_{k'}$ is the largest solvable ideal in $\mathfrak{g}_{k'}$, i.e., that $r(\mathfrak{g})_{k'} = r(\mathfrak{g}_{k'})$. \square

THE DECOMPOSITION OF SEMISIMPLE LIE ALGEBRAS

DEFINITION 5.15 A Lie algebra \mathfrak{g} is **simple** if it is nonabelian and its only ideals are $\{0\}$ and \mathfrak{g} .

Clearly a simple Lie algebra is semisimple, and so a product of simple Lie algebras is semisimple (by 5.5).

Let \mathfrak{g} be a Lie algebra, and let $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ be ideals in \mathfrak{g} . If \mathfrak{g} is a direct sum of the \mathfrak{a}_i as k -subspaces,

$$\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r,$$

then $[\mathfrak{a}_i, \mathfrak{a}_j] \subset \mathfrak{a}_i \cap \mathfrak{a}_j = 0$ for $i \neq j$, and so \mathfrak{g} is a direct product of the \mathfrak{a}_i as Lie subalgebras,

$$\mathfrak{g} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r.$$

The minimal nonzero ideals in a Lie algebra are either abelian or simple. Therefore, the minimal nonzero ideals in a semisimple Lie algebra are exactly the ideals that are simple as Lie algebras.

THEOREM 5.16 *A semisimple Lie algebra \mathfrak{g} has only finitely many minimal nonzero ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r$, and*

$$\mathfrak{g} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r.$$

Every ideal in \mathfrak{a} is a direct product of the \mathfrak{a}_i that it contains.

In particular, a Lie algebra is semisimple if and only if it is isomorphic to a product of simple Lie algebras.

PROOF. Let \mathfrak{a} be an ideal in \mathfrak{g} . Then the orthogonal complement \mathfrak{a}^\perp of \mathfrak{a} is also an ideal (5.7), and so $\mathfrak{a} \cap \mathfrak{a}^\perp$ is an ideal. By Cartan's criterion (5.12), it is solvable, and hence zero. Therefore, $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^\perp$.

If \mathfrak{g} is not simple, then it has a nonzero proper ideal \mathfrak{a} . Write $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^\perp$. If one of \mathfrak{a} or \mathfrak{a}^\perp is not simple (as a Lie subalgebra), then we can decompose again. Eventually,

$$\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$$

with the \mathfrak{a}_i simple (hence minimal) ideals.

Let \mathfrak{a} be a minimal nonzero ideal in \mathfrak{g} . Then $[\mathfrak{g}, \mathfrak{a}]$ is an ideal contained in \mathfrak{a} , which is nonzero because $z(\mathfrak{g}) = 0$, and so $[\mathfrak{g}, \mathfrak{a}] = \mathfrak{a}$. On the other hand,

$$[\mathfrak{g}, \mathfrak{a}] = [\mathfrak{a}_1, \mathfrak{a}] \oplus \cdots \oplus [\mathfrak{a}_r, \mathfrak{a}],$$

and so $\mathfrak{a} = [\mathfrak{a}_i, \mathfrak{a}] \subset \mathfrak{a}_i$ for exactly one i ; then $\mathfrak{a} = \mathfrak{a}_i$ (simplicity of \mathfrak{a}_i). This shows that $\{\mathfrak{a}_1, \dots, \mathfrak{a}_r\}$ is a complete set of minimal nonzero ideals in \mathfrak{g} .

Let \mathfrak{a} be an ideal in \mathfrak{g} . A similar argument shows that \mathfrak{a} is a direct sum of the minimal nonzero ideals contained in \mathfrak{a} . □

COROLLARY 5.17 *All nonzero ideals and quotients of a semisimple Lie algebra are semisimple.*

PROOF. Any such Lie algebra is a product of simple Lie algebras, and so is semisimple. □

COROLLARY 5.18 *If \mathfrak{g} is semisimple, then $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$.*

PROOF. If \mathfrak{g} is simple, then certainly $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$, and so this is true also for direct sums of simple algebras. □

REMARK 5.19 The theorem is surprisingly strong: a finite-dimensional vector space is a sum of its minimal subspaces but is far from being a direct sum (and so the theorem fails for abelian Lie algebras). Similarly, it fails for commutative groups: for example, if C_9 denotes a cyclic group of order 9, then

$$C_9 \times C_9 = \{(x, x) \in C_9 \times C_9\} \times \{(x, -x) \in C_9 \times C_9\}.$$

If \mathfrak{a} is a simple Lie algebra, one might expect that \mathfrak{a} embedded diagonally would be another simple ideal in $\mathfrak{a} \oplus \mathfrak{a}$. It is a simple Lie subalgebra, but it is not an ideal.

DERIVATIONS OF A SEMISIMPLE LIE ALGEBRA

Recall that $\text{Der}_k(\mathfrak{g})$ is the space of k -linear endomorphisms of \mathfrak{g} satisfying the Leibniz condition

$$D([x, y]) = [D(x), y] + [x, D(y)].$$

The bracket

$$[D, D'] = D \circ D' - D' \circ D$$

makes it into a Lie algebra.

LEMMA 5.20 *For any Lie algebra \mathfrak{g} , the space $\{\text{ad}(x) \mid x \in \mathfrak{g}\}$ of inner derivations of \mathfrak{g} is an ideal in $\text{Der}_k(\mathfrak{g})$.*

PROOF. Let D be a derivation of \mathfrak{g} , and let $x \in \mathfrak{g}$ — we have to show that the derivation $[D, \text{ad } x]$ is inner. For any $y \in \mathfrak{g}$,

$$\begin{aligned} [D, \text{ad } x](y) &= (D \circ \text{ad } x - \text{ad } x \circ D)(y) \\ &= D([x, y]) - [x, D(y)] \\ &= [D(x), y] + [x, D(y)] - [x, D(y)] \\ &= [D(x), y]. \end{aligned}$$

Therefore

$$[D, \text{ad}(x)] = \text{ad } D(x), \tag{156}$$

which is inner. \square

THEOREM 5.21 *Every derivation of a semisimple Lie algebra \mathfrak{g} is inner; therefore $\text{ad}: \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$ is an isomorphism.*

PROOF. Let $\text{ad } \mathfrak{g}$ denote the (isomorphic) image of \mathfrak{g} in $\text{Der}(\mathfrak{g})$, and let $(\text{ad } \mathfrak{g})^\perp$ denote its orthogonal complement for the Killing form on $\text{Der}(\mathfrak{g})$. It suffices to show that $(\text{ad } \mathfrak{g})^\perp = 0$.

We have

$$[(\text{ad } \mathfrak{g})^\perp, \text{ad } \mathfrak{g}] \subset (\text{ad } \mathfrak{g})^\perp \cap \text{ad } \mathfrak{g} = 0$$

because $\text{ad } \mathfrak{g}$ and $(\text{ad } \mathfrak{g})^\perp$ are ideals in $\text{Der}(\mathfrak{g})$ (5.20, 5.7) and $\kappa_{\text{Der}(\mathfrak{g})}|_{\text{ad } \mathfrak{g}} = \kappa_{\text{ad } \mathfrak{g}}$ is nondegenerate (5.13). Therefore

$$\text{ad}(Dx) \stackrel{(156)}{=} [D, \text{ad}(x)] = 0$$

if $D \in (\text{ad } \mathfrak{g})^\perp$ and $x \in \mathfrak{g}$. As $\text{ad}: \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$ is injective,

$$\text{ad}(Dx) = 0 \quad \text{for all } x \implies Dx = 0 \quad \text{for all } x \implies D = 0. \quad \square$$

5b Semisimple algebraic groups and their Lie algebras

REVIEW

Recall that k has characteristic zero.

5.22 A connected algebraic group G contains a largest connected normal solvable subgroup (I, 17.2), called the **radical** RG of G . The formation of RG commutes with extension of the base field (I, 17.3). A connected algebraic group G is said to be **semisimple** if its radical is trivial (I, 17.6). A connected algebraic group is semisimple if and only if its only connected normal commutative subgroup is $\{1\}$ (I, 17.7).

THE LIE ALGEBRA OF A SEMISIMPLE ALGEBRAIC GROUP

THEOREM 5.23 *A connected algebraic group G is semisimple if and only if its Lie algebra is semisimple.*

PROOF. Suppose that $\text{Lie}(G)$ is semisimple, and let N be a connected normal abelian subgroup of G . Then $\text{Lie}(N)$ is an abelian ideal in $\text{Lie}(G)$ (2.23, 2.24), and so is zero. This implies that $N = 1$ (2.8).

Conversely, suppose that G is semisimple, and let \mathfrak{n} be an abelian ideal in \mathfrak{g} . When G acts on \mathfrak{g} through the adjoint representation, the Lie algebra of $H = C_G(\mathfrak{n})$ is (see 2.20)

$$\mathfrak{h} = \{x \in \mathfrak{g} \mid [x, \mathfrak{n}] = 0\},$$

which contains \mathfrak{n} . Because \mathfrak{n} is an ideal, so also is \mathfrak{h} : if $h \in \mathfrak{h}$, $x \in \mathfrak{g}$, and $n \in \mathfrak{n}$, then

$$[[h, x], n] = [h, [x, n]] - [x, [h, n]] = 0$$

and so $[h, x] \in \mathfrak{h}$. Therefore, H° is normal in G (2.23), which implies that its centre $Z(H^\circ)$ is normal in G . Because G is semisimple, $Z(H^\circ)$ is finite, and so $z(\mathfrak{h}) = 0$ (2.24). But $z(\mathfrak{h}) \supset \mathfrak{n}$, and so $\mathfrak{n} = 0$. \square

COROLLARY 5.24 *For any connected algebraic group G , $\text{Lie}(R(G)) = r(\mathfrak{g})$.*

PROOF. From the exact sequence

$$1 \rightarrow RG \rightarrow G \rightarrow G/RG \rightarrow 1$$

we get an exact sequence (1.36)

$$1 \rightarrow \text{Lie}(RG) \rightarrow \mathfrak{g} \rightarrow \text{Lie}(G/RG) \rightarrow 1$$

in which $\text{Lie}(RG)$ is solvable (apply 2.23, 2.24) and $\text{Lie}(G/RG)$ is semisimple (5.23). Therefore $\text{Lie } RG$ is the largest solvable ideal in \mathfrak{g} . \square

THE LIE ALGEBRA OF $\text{Aut}_k(C)$

Let C be a finite-dimensional k -vector space with a k -bilinear pairing $C \times C \rightarrow C$ (i.e., C is a k -algebra, not necessarily associative or commutative).

PROPOSITION 5.25 *The functor*

$$R \rightsquigarrow \text{Aut}_{k\text{-alg}}(R \otimes_k C): \text{Alg}_k \rightarrow \text{Grp}$$

is an algebraic subgroup of GL_C .

PROOF. Choose a basis for C . Then an element of $\text{Aut}_{k\text{-lin}}(R \otimes_k C)$ is represented by a matrix, and the condition that it preserve the algebra product is a polynomial condition on the matrix entries. \square

Denote this algebraic group by Aut_C , so that

$$\text{Aut}_C(R) = \text{Aut}_{k\text{-alg}}(R \otimes_k C), \text{ all } k\text{-algebras } R.$$

PROPOSITION 5.26 *The Lie algebra of Aut_C is $\mathfrak{gl}_C \cap \text{Der}_k(C)$.*

PROOF. Let $\text{id} + \varepsilon\alpha \in \text{Lie}(\text{GL}_C)$, and let $a + \varepsilon a'$ and $b + \varepsilon b'$ be elements of $k[\varepsilon] \otimes_k C \simeq C \oplus \varepsilon C$. When we first apply $\text{id} + \varepsilon\alpha$ to the two elements and then multiply them, we get

$$ab + \varepsilon(ab' + a'b + a\alpha(b) + \alpha(a)b);$$

when we first multiply them, and then apply $\text{id} + \varepsilon\alpha$ we get

$$ab + \varepsilon(ab' + a'b + \alpha(ab)).$$

These are equal if and only if α satisfies the Leibniz rule. □

THE MAP Ad

Let G be a connected algebraic group. Recall (§1g) that there is a homomorphism

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}.$$

Specifically, $g \in G(R)$ acts on $\mathfrak{g}(R) \subset G(R[\varepsilon])$ as $\text{inn}(g)$,

$$x \mapsto gxg^{-1}.$$

On applying the functor Lie , we get a homomorphism

$$\text{ad}: \text{Lie}(G) \rightarrow \text{Lie}(\text{GL}_{\mathfrak{g}}) \simeq \text{End}(\mathfrak{g}),$$

and we defined

$$[x, y] = \text{ad}(x)(y).$$

LEMMA 5.27 *For all $g \in G(R)$, the automorphism $\text{Ad}(g)$ of $\mathfrak{g}(R)$ preserves the bracket.*

PROOF. Because every algebraic group can be embedded in some GL_n (I, 8.31), it suffices to prove the statement for GL_n . But $A \in \text{GL}_n(R)$ acts on $\mathfrak{g}(R) = M_n(R)$ as

$$X \mapsto AXA^{-1}.$$

Now

$$\begin{aligned} A[X, Y]A^{-1} &= A(XY - YX)A^{-1} \\ &= AXA^{-1}AYA^{-1} - AYA^{-1}AXA^{-1} \\ &= [AXA^{-1}, AYA^{-1}]. \end{aligned} \quad \square$$

Therefore Ad maps into $\text{Aut}_{\mathfrak{g}}$ (in the sense of the preceding subsection),

$$\text{Ad}: G \rightarrow \text{Aut}_{\mathfrak{g}},$$

and so (5.26) ad maps into $\text{Lie}(\text{Aut}_{\mathfrak{g}}) = \mathfrak{gl}_{\mathfrak{g}} \cap \text{Der}_k(\mathfrak{g})$,

$$\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}} \cap \text{Der}_k(\mathfrak{g}).$$

LEMMA 5.28 Let $g \in G(k)$. The functor $C_G(g)$

$$R \rightsquigarrow \{g' \in G(R) \mid gg' = g'g\}: \text{Alg}_k \rightarrow \text{Grp}$$

is an algebraic subgroup of G with Lie algebra

$$c_{\mathfrak{g}}(g) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid \text{Ad}(g)(x) = x\}.$$

PROOF. Embed G in GL_n . If we can prove the statement for GL_n , then we obtain it for G , because $C_G(g) = C_{\text{GL}_n}(g) \cap G$ and $c_{\mathfrak{g}}(g) = c_{\mathfrak{gl}_n}(g) \cap \mathfrak{g}$.

Let $A \in \text{GL}_n(k)$. Then

$$C_{\text{GL}_n}(A)(R) = \{B \in \text{GL}_n(R) \mid AB = BA\}.$$

Clearly this is a polynomial (even linear) condition on the entries of B . Moreover,

$$\begin{aligned} \text{Lie}(C_{\text{GL}_n}(A)) &= \{I + \varepsilon B \in \text{Lie}(\text{GL}_n) \mid A(I + \varepsilon B) = (I + \varepsilon B)A\} \\ &\simeq \{B \in M_n \mid AB = BA\}. \end{aligned} \quad \square$$

PROPOSITION 5.29 For a connected algebraic group G , the kernel of Ad is the centre $Z(G)$ of G .

PROOF. Clearly $Z \subset N \stackrel{\text{def}}{=} \text{Ker}(\text{Ad})$. As the formation of kernels and centres commute with extension of the base field, it suffices to prove that $Z = N$ when k is algebraically closed. For $g \in N(k)$, $c_{\mathfrak{g}}(g) = \mathfrak{g}$, and so (by 5.28) $\text{Lie} C_G(g) = \mathfrak{g}$. Hence $C_G(g) = G$ (2.5), and so $g \in Z(k)$. We have shown that $Z(k) = N(k)$, and this implies that $Z = N$ (7.30). \square

THEOREM 5.30 For any semisimple algebraic group G , the sequence

$$1 \rightarrow Z(G) \rightarrow G \xrightarrow{\text{Ad}} \text{Aut}_{\mathfrak{g}}^{\circ} \rightarrow 1$$

is exact.

PROOF. On applying Lie to $\text{Ad}: G \rightarrow \text{Aut}_{\mathfrak{g}}$, we get the homomorphism

$$\text{ad}: \mathfrak{g} \rightarrow \text{Lie}(\text{Aut}_{\mathfrak{g}}) \subset \text{Der}(\mathfrak{g}).$$

But, according to (5.21), the map $\mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$ is surjective, which shows that $\text{ad}: \mathfrak{g} \rightarrow \text{Lie}(\text{Aut}_{\mathfrak{g}})$ is surjective, and implies that $\text{Ad}: G \rightarrow \text{Aut}_{\mathfrak{g}}^{\circ}$ is surjective (2.6). \square

Two semisimple algebraic groups G_1, G_2 are said to be isogenous if $G_1/Z(G_1) \approx G_2/Z(G_2)$; equivalently if there exists a semisimple algebraic group G and isogenies

$$G_1 \leftarrow G \rightarrow G_2.$$

The theorem gives an inclusion

$$\{\text{semisimple algebraic groups}\}/\text{isogeny} \hookrightarrow \{\text{semisimple Lie algebras}\}/\text{isomorphism}.$$

In III, Section 2 below, we classify the isomorphism classes of semisimple Lie algebras over an algebraically closed field of characteristic zero. Since all of them arise from algebraic groups, this gives a classification of the isogeny classes of semisimple algebraic groups over such fields. In III, Section 3, we follow a different approach which allows us to describe the *category* of semisimple algebraic groups in terms of semisimple Lie algebras and their representations.

THE DECOMPOSITION OF SEMISIMPLE ALGEBRAIC GROUPS

An algebraic group G is *simple* if it is connected, noncommutative, and its only proper normal subgroups is 1, and it is *almost-simple* if it is connected, noncommutative, and all its proper normal subgroups are finite. Thus, for $n > 1$, SL_n is almost-simple and $\mathrm{PSL}_n = \mathrm{SL}_n / \mu_n$ is simple. A subgroup N of an algebraic group G that is minimal among the nonfinite normal subgroups of G is either commutative or almost-simple; if G is semisimple, then it is almost-simple.

An algebraic group G is said to be the *almost-direct product* of its algebraic subgroups G_1, \dots, G_r if the map

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G$$

is a surjective homomorphism with finite kernel. In particular, this means that the G_i commute and each G_i is normal in G .

THEOREM 5.31 *A semisimple algebraic group G has only finitely many almost-simple normal subgroups G_1, \dots, G_r , and the map*

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G$$

is surjective with finite kernel. Each connected normal algebraic subgroup of G is a product of those G_i that it contains, and is centralized by the remaining ones.

In particular, an algebraic group is semisimple if and only if it is an almost-direct product of almost-simple algebraic groups.

PROOF. Because $\mathrm{Lie}(G)$ is semisimple, it is a direct sum of its simple ideals

$$\mathrm{Lie}(G) = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r.$$

Let G_1 be the identity component of $C_G(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r)$ (notation as in 2.20). Then $\mathrm{Lie}(G_1) \stackrel{(2.20)}{=} c_{\mathfrak{g}}(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r) = \mathfrak{g}_1$, and so it is normal in G (2.23). If G_1 had a proper normal connected algebraic subgroup of dimension > 0 , then \mathfrak{g}_1 would have an ideal other than \mathfrak{g}_1 and 0, contradicting its simplicity. Therefore G_1 is almost-simple. Construct G_2, \dots, G_r similarly. Then $[\mathfrak{g}_i, \mathfrak{g}_j] = 0$ implies that G_i and G_j commute (2.23). The subgroup $G_1 \cdots G_r$ of G has Lie algebra \mathfrak{g} , and so equals G (2.5). Finally,

$$\mathrm{Lie}(G_1 \cap \cdots \cap G_r) \stackrel{(1.37)}{=} \mathfrak{g}_1 \cap \cdots \cap \mathfrak{g}_r = 0$$

and so $G_1 \cap \cdots \cap G_r$ is étale (2.8).

Let H be a connected algebraic subgroup of G . If H is normal, then $\mathrm{Lie} H$ is an ideal, and so is a direct sum of those \mathfrak{g}_i it contains and centralizes the remainder. This implies that H is a product of those G_i it contains, and is centralized by the remaining ones. \square

COROLLARY 5.32 *All nontrivial connected normal subgroups and quotients of a semisimple algebraic group are semisimple.*

PROOF. Any such group is an almost-product of almost-simple algebraic groups. \square

COROLLARY 5.33 *If G is semisimple, then $\mathcal{D}G = G$, i.e., a semisimple group has no commutative quotients.*

PROOF. This is obvious for almost-simple algebraic groups, and hence for any almost-product of such algebraic groups. \square

6 Semisimplicity of representations

The main theorem in this section is that the finite-dimensional representations of an algebraic group in characteristic zero are semisimple if and only if the identity component of the group is connected. The starting point for the proof of this result is the theorem of Weyl saying that the finite-dimensional representations of a semisimple Lie algebra in characteristic zero are semisimple. Throughout this section (except the first subsection), k is a field of characteristic zero.

6a Generalities on semisimple modules

Let k be a field, and let A be a k -algebra (either associative or a Lie algebra). An A -module is *simple* if it does not contain a nonzero proper submodule.

PROPOSITION 6.1 *The following conditions on an A -module M of finite dimension¹⁰ over k are equivalent:*

- (a) M is a sum of simple modules;
- (b) M is a direct sum of simple modules;
- (c) for every submodule N of M , there exists a submodule N' such that $M = N \oplus N'$.

PROOF. Assume (a), and let N be a submodule of M . Let I be the set of simple modules of M . For $J \subset I$, let $N(J) = \sum_{S \in J} S$. Let J be maximal among the subsets of I for which

- (i) the sum $\sum_{S \in J} S$ is direct and
- (ii) $N(J) \cap N = 0$.

I claim that M is the direct sum of $N(J)$ and N . To prove this, it suffices to show that each $S \subset N + N(J)$. Because S is simple, $S \cap (N + N(J))$ equals S or 0 . In the first case, $S \subset N + N(J)$, and in the second $J \cup \{S\}$ has the properties (i) and (ii). Because J is maximal, the first case must hold. Thus (a) implies (b) and (c), and it is obvious that (b) and (c) each implies (a). \square

DEFINITION 6.2 An A -module is *semisimple* if it satisfies the equivalent conditions of the proposition.

LEMMA 6.3 (SCHUR'S LEMMA) *If V is a simple A -module and k is algebraically closed, then $\text{End}_A(V) = k$.*

¹⁰I assume this only to avoid using Zorn's lemma in the proof.

PROOF. Let $\alpha: V \rightarrow V$ be A -homomorphism of V . Because k is algebraically closed, α has an eigenvector, say, $\alpha(v) = cv$, $c \in k$. Now $\alpha - c: V \rightarrow V$ is an A -homomorphism with nonzero kernel. Because V is simple, the kernel must equal V . Hence $\alpha = c$. \square

NOTES Rewrite this section for a k -linear abelian category.

6b Reduction to the case of an algebraically closed field

Let \mathfrak{g} be a Lie algebra. We saw in (1.2) that any associative k -algebra A becomes a Lie algebra with the bracket $[a, b] = ab - ba$. Among pairs consisting of an associative k -algebra A and a Lie algebra homomorphism $\mathfrak{g} \rightarrow A$, there is one, $\mathfrak{g} \rightarrow U(\mathfrak{g})$, that is universal — $U(\mathfrak{g})$ is called the *universal enveloping algebra* of \mathfrak{g} . It can be constructed as the quotient of the tensor algebra $T(\mathfrak{g})$ by the relations

$$x \otimes y - y \otimes x = [x, y], \quad x, y \in \mathfrak{g}.$$

The map $\mathfrak{g} \rightarrow U(\mathfrak{g})$ is injective, and so we may regard \mathfrak{g} as a subset of $U(\mathfrak{g})$. Any homomorphism $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ of Lie algebras extends uniquely to a homomorphism $U(\mathfrak{g}) \rightarrow \text{End}_{k\text{-lin}}(V)$ of associative algebras. Therefore the functor sending a representation $\rho: U(\mathfrak{g}) \rightarrow \text{End}_{k\text{-lin}}(V)$ of $U(\mathfrak{g})$ to $\rho|_{\mathfrak{g}}$ is an isomorphism(!) of categories

$$\text{Rep}_k(U(\mathfrak{g})) \rightarrow \text{Rep}_k(\mathfrak{g}). \quad (157)$$

PROPOSITION 6.4 For a Lie algebra \mathfrak{g} over k , the category $\text{Rep}_k(\mathfrak{g})$ is semisimple if and only if $\text{Rep}_{k^{\text{al}}}(\mathfrak{g}_{k^{\text{al}}})$ is semisimple.

PROOF. Let $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ be a finite-dimensional representation of \mathfrak{g} . Then V is semisimple as a \mathfrak{g} -module if and only if it is semisimple as a $U(\mathfrak{g})$ -module (obviously), and it is semisimple as a $U(\mathfrak{g})$ -module if and only if $k^{\text{al}} \otimes_k V$ is semisimple as a $k^{\text{al}} \otimes_k U(\mathfrak{g})$ -module (Bourbaki A, VIII, §13, 4). As $k^{\text{al}} \otimes_k U(\mathfrak{g}) \simeq U(\mathfrak{g}_{k^{\text{al}}})$, this shows that

$$\text{Rep}_{k^{\text{al}}}(\mathfrak{g}_{k^{\text{al}}}) \text{ semisimple} \implies \text{Rep}_k(\mathfrak{g}) \text{ semisimple}.$$

For the converse, let \bar{V} be an object of $\text{Rep}_{k^{\text{al}}}(\mathfrak{g}_{k^{\text{al}}})$. There exists a finite extension k' of k and a representation V' of $\mathfrak{g}_{k'}$ over k' that gives \bar{V} by extension of scalars $k' \rightarrow k^{\text{al}}$. When we regard V' as a vector space over k , we obtain a representation V of \mathfrak{g} over k . By assumption, V is semisimple and, as was observed above, this implies that $k^{\text{al}} \otimes_k V$ is semisimple. But \bar{V} is a quotient of $k^{\text{al}} \otimes_k V$, and so it also is semisimple. \square

COROLLARY 6.5 For a connected algebraic group G over k , the category $\text{Rep}_k(G)$ is semisimple if and only if $\text{Rep}_{k^{\text{al}}}(G_{k^{\text{al}}})$ is semisimple.

PROOF. Let $\mathfrak{g} = \text{Lie}(G)$. For any finite-dimensional representation $r: G \rightarrow \text{GL}_V$, a subspace W of V is stable under G if and only if it is stable under \mathfrak{g} (see 2.16). It follows that,

$$\begin{aligned} (V, r) \text{ is semisimple as a representation of } G & \\ \iff (V, dr) \text{ is semisimple as a representation of } \mathfrak{g} & \\ \iff (V, dr)_{k^{\text{al}}} \text{ is semisimple as a representation of } \mathfrak{g}_{k^{\text{al}}} \text{ (by 6.4)} & \\ \iff (V, r)_{k^{\text{al}}} \text{ is semisimple as a representation of } G_{k^{\text{al}}}. & \quad \square \end{aligned}$$

ASIDE 6.6 Let G be a connected algebraic group. It is not true that $\text{Rep}(G)$ is semisimple if and only if $\text{Rep}(\text{Lie}(G))$ is semisimple. For example, when G is reductive but not semisimple, the first category is semisimple, but the second category is not, because there are nonsemisimple representations of $\text{Lie}(G)$ not arising from representations of G .

ASIDE 6.7 The following two statements give an alternative proof of (6.4) and (6.5).

Let A be a k -linear abelian category such that every object X has finite length and $\text{Hom}(X, Y)$ is finite-dimensional. Then A is semisimple if and only if $\text{End}(X)$ is a semisimple k -algebra for all X .

Let A be a finite-dimensional k -algebra; if A is semisimple, then so also is $k' \otimes A$ for every field $k' \supset k$; conversely, if $k' \otimes A$ is semisimple for some field $k' \supset k$, then A is semisimple (Bourbaki A, VIII; CFT IV, 2.15).

To apply these statements, note that for any representations V and W of a Lie algebra \mathfrak{g} , or of an algebraic group G ,

$$\begin{aligned} k' \otimes \text{Hom}_{\mathfrak{g}}(V, W) &\simeq \text{Hom}_{\mathfrak{g}_{k'}}(V_{k'}, W_{k'}) \\ k' \otimes \text{Hom}_G(V, W) &\simeq \text{Hom}_{G_{k'}}(V_{k'}, W_{k'}), \end{aligned}$$

because

$$k' \otimes \text{Hom}(V, W) \simeq \text{Hom}(V_{k'}, W_{k'})$$

and the condition that a linear map $V \rightarrow W$ be \mathfrak{g} or G equivariant is linear (for G , regard V and W as comodules over $\mathcal{O}(G)$).

6c Representations of Lie algebras.

CASIMIR OPERATOR

Let \mathfrak{g} be semisimple, and fix a faithful representation $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ of \mathfrak{g} . Because the pairing

$$\beta_V: \mathfrak{g} \times \mathfrak{g} \rightarrow k$$

is nondegenerate (5.9), for any basis e_1, \dots, e_n for \mathfrak{g} as a k -vector space, there exists a dual basis e'_1, \dots, e'_n for \mathfrak{g} such that $\beta_V(e_i, e'_j) = \delta_{ij}$. Let $x \in \mathfrak{g}$, and let

$$\begin{aligned} [e_i, x] &= \sum_{j=1}^n a_{ij} e_j \\ [x, e'_i] &= \sum_{j=1}^n b_{ij} e'_j. \end{aligned}$$

Then

$$\begin{aligned} \beta_V([e_i, x], e'_{i'}) &= \sum_{j=1}^n a_{ij} \beta_V(e_j, e'_{i'}) = a_{ii'} \\ \beta_V(e_i, [x, e'_{i'}]) &= \sum_{j=1}^n b_{i'j} \beta_V(e_i, e'_j) = b_{ii'} \end{aligned}$$

and so $a_{ii'} = b_{ii'}$ (because β_V is associative). In other words, for $x \in \mathfrak{g}$,

$$[e_i, x] = \sum_{j=1}^n a_{ij} e_j \iff [x, e'_i] = \sum_{j=1}^n a_{ij} e'_j.$$

The *Casimir operator* attached to the representation $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ is

$$c_V = \sum_{i=1}^n e_{iV} \circ e'_{iV}.$$

PROPOSITION 6.8 (a) *The element c_V is independent of the choice of the basis e_1, \dots, e_n .*
 (b) *The map $c_V: V \rightarrow V$ is a \mathfrak{g} -module homomorphism.*
 (c) *We have $\text{Tr}_V(c_V) = n$ ($\dim \mathfrak{g}$).*

PROOF. (a) In fact, the element $\delta(1) \stackrel{\text{def}}{=} \sum_{i=1}^n e_i \otimes e'_i$ of $\mathfrak{g} \otimes \mathfrak{g}$ is the image of $\text{id}_{\mathfrak{g}}$ under the isomorphisms

$$\text{End}_{k\text{-lin}}(\mathfrak{g}) \simeq \mathfrak{g} \otimes \mathfrak{g}^{\vee} \simeq \mathfrak{g} \otimes \mathfrak{g}.$$

(b) This can be proved by a direct calculation (e.g., Erdmann and Wildon 2006, 17.3).

(c) We have

$$\begin{aligned} \text{Tr}_V(c_V) &= \sum_{i=1}^n \text{Tr}_V(e_i \circ e'_i) \\ &= \sum_{i=1}^n \beta_V(e_i, e'_i) \\ &= \sum_{i=1}^n \delta_{ii} \\ &= n. \end{aligned} \quad \square$$

ASIDE 6.9 For any basis e_1, \dots, e_n of \mathfrak{g} , let

$$c = \sum_{i=1}^n e_i \cdot e'_i \in U(\mathfrak{g}).$$

Then c maps to c_V under every representation of \mathfrak{g} , and is the unique element of $U(\mathfrak{g})$ with this property (the finite-dimensional representations of $U(\mathfrak{g})$ form a faithful family). In particular, it is independent of the choice of the basis. Statement 6.8b is equivalent to the statement that c lies in the centre of $U(\mathfrak{g})$.

WEYL'S THEOREM

Let $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ a representation of a Lie algebra \mathfrak{g} . If \mathfrak{g} is semisimple, then $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$, and so

$$\text{Tr}_V(g_V) = \text{Tr}_V([\mathfrak{g}_1, \mathfrak{g}_2]_V) = \text{Tr}_V(g_{1V} \circ g_{2V} - g_{2V} \circ g_{1V}) = 0, \quad \text{all } g \in \mathfrak{g}.$$

When V is one-dimensional, this implies that \mathfrak{g} acts trivially on V (i.e., $xv = 0$ for all $x \in \mathfrak{g}$ and $v \in V$).

THEOREM 6.10 (WEYL) *A Lie algebra \mathfrak{g} is semisimple if and only if every finite-dimensional representation \mathfrak{g} is semisimple.*

PROOF. \Leftarrow : For the adjoint representation $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$, the \mathfrak{g} -submodules of \mathfrak{g} are exactly the ideals in \mathfrak{g} . Therefore, if the adjoint representation is semisimple, then every ideal in \mathfrak{g} admits a complementary ideal, and so is a quotient of \mathfrak{g} . Hence, if \mathfrak{g} is not semisimple, then it admits a nonzero abelian quotient, and therefore a quotient of dimension 1. But the Lie algebra k of dimension 1 has nonsemisimple representations, for example, $c \mapsto \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$.

\Rightarrow : Let \mathfrak{g} be a semisimple Lie algebra, which we may suppose to be nonzero, and let $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ be a finite-dimensional representation of \mathfrak{g} . We have to show that every \mathfrak{g} -submodule W of V admits a \mathfrak{g} -complement. This we do by induction on $\dim W$. After (6.4), we may suppose that k is algebraically closed.

Assume first that $\dim V/W = 1$ and that W is simple. The first condition implies that \mathfrak{g} acts trivially on V/W (see the above remark). We may replace \mathfrak{g} with its image in \mathfrak{gl}_V , and so suppose that $\mathfrak{g} \subset \mathfrak{gl}_V$. Let $c_V: V \rightarrow V$ be the Casimir operator. As \mathfrak{g} acts trivially

on V/W , so also does c_V . On the other hand, c_V acts on W as a scalar a (Schur's lemma). This scalar is nonzero, because otherwise $\text{Tr}_V c_V = 0$, contradicting (6.8). Therefore, the kernel of c_V is a one-dimensional \mathfrak{g} -submodule of V which intersects W trivially, and so is a \mathfrak{g} -complement for W .

Next assume only that $\dim V/W = 1$. If W is simple, we have already proved that it has a \mathfrak{g} -complement, and so we may suppose that there is a proper nonzero \mathfrak{g} -submodule W' of W . Now W/W' is a \mathfrak{g} -submodule of V/W' of codimension 1, and so, by induction,

$$V/W' = W/W' \oplus V'/W'$$

for some \mathfrak{g} -submodule V' of V containing W' . Now W' is a \mathfrak{g} -submodule of V' of codimension 1 and so, by induction, $V' = W' \oplus L$ for some line L . Now L is a \mathfrak{g} -submodule of V , which intersects W trivially and has complementary dimension, and so is a \mathfrak{g} -complement for W .

Finally, we consider the general case, $W \subset V$. The space $\text{Hom}_{k\text{-lin}}(V, W)$ of k -linear maps has a natural \mathfrak{g} -module structure:

$$(xf)(v) = x \cdot f(v) - f(x \cdot v).$$

Let

$$\begin{aligned} V_1 &= \{f \in \text{Hom}_{k\text{-lin}}(V, W) \mid f|_W = a \text{id}_W \text{ for some } a \in k\} \\ W_1 &= \{f \in \text{Hom}_{k\text{-lin}}(V, W) \mid f|_W = 0\}. \end{aligned}$$

One checks easily that W_1 and V_1 are \mathfrak{g} -submodules of $\text{Hom}_{k\text{-lin}}(V, W)$. As V_1/W_1 has dimension 1, the first part of the proof shows that

$$V_1 = W_1 \oplus L$$

for some one-dimensional \mathfrak{g} -submodule L of V_1 . Let $L = \langle f \rangle$. Because \mathfrak{g} acts trivially on L ,

$$0 = (xf)(v) \stackrel{\text{def}}{=} x \cdot f(v) - f(x \cdot v), \quad \text{all } x \in \mathfrak{g}, \quad v \in V,$$

which says that f is a \mathfrak{g} -homomorphism $V \rightarrow W$. As $f|_W = a \text{id}_W$ with $a \neq 0$, the kernel of f is a \mathfrak{g} -complement to W . \square

ASIDE 6.11 An infinite-dimensional representation of a semisimple Lie algebra, even of \mathfrak{sl}_2 , need not be semisimple (see later, maybe).

ASIDE 6.12 Let V_n be the standard V_{n+1} -dimensional representation of SL_n over \mathbb{F}_p . Then V_n is simple for $0 \leq n \leq p-1$, but $V_n \otimes V_{n'}$ is not semisimple when $n+n' > p$ (mo57997).

ASIDE 6.13 In his original proof, Weyl showed that finite-dimensional representations of compact groups are semisimple (because they are unitary), and deduced the similar statement for semisimple Lie algebras over \mathbb{C} by showing that such algebras all arise from the Lie algebras of compact real Lie groups. The proof presented here follows that in Serre 1965.

6d Representations of reductive groups

Let G be an algebraic group. The discussion in §6a carries over to G -modules.

THEOREM 6.14 *The following conditions on a connected algebraic group G are equivalent:*

- (a) G is reductive;
- (b) every finite-dimensional representation of G is semisimple;
- (c) some faithful finite-dimensional representation of G is semisimple.

We first prove two lemmas.

LEMMA 6.15 *Let G be an algebraic group. The restriction to a normal subgroup N of a semisimple representation of G is again semisimple.*

PROOF. After (6.5), we may assume that k is algebraically closed. Let $G \rightarrow \mathrm{GL}_V$ be a representation of G , which we may suppose to be simple. Let S be a simple N -submodule of V . For any $g \in G(k)$, gS is a simple N -submodule, and V is a sum of the gS (because the sum is a nonzero G -submodule of V); hence it is semisimple (cf. 6.1). \square

LEMMA 6.16 *All finite-dimensional representations of a semisimple algebraic group are semisimple.*

PROOF. If G is a semisimple algebraic group, then $\mathrm{Lie}(G)$ is a semisimple Lie algebra (5.23). Hence the finite-dimensional representations of $\mathrm{Lie}(G)$ are semisimple by Weyl's theorem (6.10), which implies the same statement for G (2.16). \square

PROOF OF THEOREM 6.14.

We may assume that k is algebraically closed.

(b) \implies (c): Every algebraic group has a faithful finite-dimensional representation (I, 8.31).

(c) \implies (a): Let $G \rightarrow \mathrm{GL}_V$ be a faithful finite-dimensional representation of G . Let N be a normal unipotent subgroup of G . Because N is normal, V is semisimple as a representation of N , say, $V = \bigoplus V_i$ with V_i simple (6.15). Because N is unipotent, each V_i contains a fixed vector (I, 15.6), which implies that it has dimension one and that N acts trivially on it. Therefore, N acts trivially on V , but we chose V to be faithful, and so $N = 0$.

(a) \implies (b): If G is reductive, then $G = Z^\circ \cdot G'$ where Z° is the connected centre of G (a torus) and G' is the derived group of G (a semisimple group) — see (I, 17.20). Let $G \rightarrow \mathrm{GL}_V$ be a representation of G . Then $V = \bigoplus_i V_i$ where V_i is the subspace of V on which Z° acts through a character χ_i (I, 14.15). Because Z° and G' commute, each space V_i is stable under G' , and because G' is semisimple, $V_i = \bigoplus_j V_{ij}$ with each V_{ij} simple as a G' -module (6.16). Now $V = \bigoplus_{i,j} V_{ij}$ is a decomposition of V into a direct sum of simple G -modules.

NONCONNECTED GROUPS

THEOREM 6.17 *All finite-dimensional representations of an algebraic group G are semisimple if and only if the identity component G° of G is reductive.*

This follows from Theorem 6.14 and the next lemma.

LEMMA 6.18 *All finite-dimensional representations of G are semisimple if and only if all finite-dimensional representations of G° are semisimple*

PROOF. We may assume that k is algebraically closed.

\implies : Since G° is a normal algebraic subgroup of G (I, 13.17), this follows from Lemma 6.15.

\impliedby : Let V be a G -module, and let W be a subspace stable under G . Then W is also stable under G° , and so there exists a G° -equivariant linear map $p: V \rightarrow W$ such that $p|_W = \text{id}_W$. Define

$$q: V \rightarrow W, \quad q = \frac{1}{n} \sum_g g p g^{-1},$$

where $n = (G(k):G^\circ(k))$ and g runs over a set of coset representatives for $G^\circ(k)$ in $G(k)$. Then q is independent of the choice of the coset representatives, and is a G -equivariant linear map $V \rightarrow W$ such that $q|_W = \text{id}_W$ (cf. the second proof of GT 7.4). Hence $\text{Ker}(q)$ is a G -stable complement for W . \square

REMARK 6.19 The lemma implies that the representations of a finite group are semisimple. This would fail if we allowed the characteristic to be a prime dividing the order of the finite group.

6e A criterion to be reductive

There is an isomorphism of algebraic groups $\text{GL}_n \rightarrow \text{GL}_n$ sending an invertible matrix A to the transpose $(A^{-1})^t$ of its inverse. The image of an algebraic subgroup H of GL_n under this map is the algebraic subgroup H^t of GL_n such that $H^t(R) = \{A^t \mid A \in H(R)\}$ for all k -algebras R .

Now consider GL_V . The choice of a basis for V determines an isomorphism $\text{GL}_V \approx \text{GL}_n$ and hence a transpose map on GL_V , which depends on the choice of the basis.

PROPOSITION 6.20 *Every connected algebraic subgroup G of GL_V such that $G = G^t$ for all choices of a basis for V is reductive.*

PROOF. We have to show that $RG = 0$ is a group of multiplicative type. It suffices to check this after an extension of scalars to the algebraic closure of k (because $RG_{k^{\text{al}}} = (RG)_{k^{\text{al}}}$ when k is perfect). Recall that the radical of G is the largest connected normal solvable subgroup of G . It follows from (17.1c) that RG is contained in every maximal connected solvable subgroup of G . Let B be such a subgroup. According to the Lie-Kolchin theorem 16.31, there exists a basis of V for which $B \subset \mathbb{T}_n$ (upper triangular matrices). Then B^t is also a maximal connected solvable subgroup of G , and so

$$RG \subset B \cap B^t = \mathbb{D}_n.$$

This proves that RG is diagonalizable. \square

EXAMPLE 6.21 The group GL_V itself is reductive.

EXAMPLE 6.22 Since the transpose of a matrix of determinant 1 has determinant 1, SL_V is reductive.

ASIDE 6.23 Prove (or disprove): a connected algebraic subgroup of GL_V that is preserved by conjugate transpose with respect to *one basis* is necessarily reductive.

The Structure of Semisimple Lie Algebras and Algebraic Groups in Characteristic Zero

To a semisimple Lie algebra, we attach some combinatorial data called a root system, from which we can read off the structure of the Lie algebra and its representations. As every root system arises from a semisimple Lie algebra and determines it up to isomorphism, the root systems classify the semisimple Lie algebras. In the first section, we review the theory of root systems and how they are classified in turn by Dynkin diagrams, and in the second section we explain their application to the theory of semisimple Lie algebras.

The category of representations of a Lie algebra is a neutral tannakian category, and so there exists an affine group $G(\mathfrak{g})$ such that $\text{Rep}(G(\mathfrak{g})) = \text{Rep}(\mathfrak{g})$. We show that, when \mathfrak{g} is semisimple and the base field has characteristic zero, $G(\mathfrak{g})$ is a connected algebraic group with Lie algebra \mathfrak{g} that finitely covers every other connected algebraic group with Lie algebra \mathfrak{g} . In other words, $G(\mathfrak{g})$ is the (unique) simply connected semisimple algebraic group with Lie algebra \mathfrak{g} . Once we have determined the centre of $G(\mathfrak{g})$ in terms of \mathfrak{g} and its root system, we are able to read off the structure and classification of the semisimple algebraic groups and of their representations from the similar results for Lie algebras.

In the first three sections, we work over an arbitrary field of characteristic zero, but only with semisimple Lie algebras and algebraic groups that are split over the field. In Section 4, we explain how the theory extends to arbitrary semisimple Lie algebras and algebraic groups over \mathbb{R} .

Finally, in Section 5 we explain how the theory extends to reductive groups.

NOTES Sections 1 and 2 omit some (standard) proofs, Section 3 needs to be extended, and Sections 4 and 5 are not yet available.

1	Root systems and their classification	296
2	Structure of semisimple Lie algebras and their representations	305
3	Structure of semisimple algebraic groups and their representations	317
4	Real Lie algebras and real algebraic groups	325
5	Reductive groups	326

1 Root systems and their classification

At present, this section omits some proofs. For more detailed accounts, see: Bourbaki LIE, Chapter VI; Erdmann and Wildon 2006, 11,13; Humphreys 1972, III; Serre 1966, Chapter V; or Casselman's notes roots.pdf on his website.

Throughout, F is a field of characteristic zero and V is a finite-dimensional vector space over F . An **inner product** on a real vector space is a positive definite symmetric bilinear form.

1a Reflections

A **reflection** of a vector space V is an endomorphism of V that fixes the vectors in a hyperplane and acts as -1 on a complementary line. Let α be a nonzero element of V . A **reflection with vector** α is an endomorphism s of V such that $s(\alpha) = -\alpha$ and the set of vectors fixed by s is a hyperplane H . Then $V = H \oplus \langle \alpha \rangle$ with s acting as $1 \oplus -1$, and so $s^2 = 1$. Let V^\vee be the dual vector space to V , and write $\langle \cdot, \cdot \rangle$ for the tautological pairing $V \times V^\vee \rightarrow k$. If α^\vee is an element of V^\vee such that $\langle \alpha, \alpha^\vee \rangle = 2$, then

$$s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha \quad (158)$$

is a reflection with vector α , and every reflection with vector α is of this form (for a unique α^\vee)¹.

LEMMA 1.1 *Let R be a finite spanning set for V . For any nonzero vector α in V , there exists at most one reflection s with vector α such that $s(R) \subset R$.*

PROOF. Let s and s' be such reflections, and let $t = ss'$. Then t acts as the identity map on both $F\alpha$ and $V/F\alpha$, and so

$$(t - 1)^2 V \subset (t - 1)F\alpha = 0.$$

Thus the minimum polynomial of t divides $(T - 1)^2$. On the other hand, because R is finite, there exists an integer $m \geq 1$ such that $t^m(x) = x$ for all $x \in R$, and hence for all $x \in V$. Therefore the minimum polynomial of t divides $T^m - 1$. As $(T - 1)^2$ and $T^m - 1$ have greatest common divisor $T - 1$, this shows that $t = 1$. \square

LEMMA 1.2 *Let (\cdot, \cdot) be an inner product on a real vector space V . Then, for any nonzero vector α in V , there exists a unique symmetry s with vector α that is orthogonal for (\cdot, \cdot) , i.e., such that $(sx, sy) = (x, y)$ for all $x, y \in V$, namely*

$$s(x) = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha. \quad (159)$$

PROOF. Certainly, (159) does define an orthogonal symmetry with vector α . Suppose s' is a second such symmetry, and let $H = \langle \alpha \rangle^\perp$. Then H is stable under s' , and maps isomorphically on $V/\langle \alpha \rangle$. Therefore s' acts as 1 on H . As $V = H \oplus \langle \alpha \rangle$ and s' acts as -1 on $\langle \alpha \rangle$, it must coincide with s . \square

¹The composite of the quotient map $V \rightarrow V/H$ with the linear map $V/H \rightarrow F$ sending $\alpha + H$ to 2 is the unique element α^\vee of V^\vee such that $\alpha(H) = 0$ and $\langle \alpha, \alpha^\vee \rangle = 2$.

1b Root systems

DEFINITION 1.3 A subset R of V over F is a **root system** in V if

RS1 R is finite, spans V , and does not contain 0;

RS2 for each $\alpha \in R$, there exists a (unique) reflection s_α with vector α such that $s_\alpha(R) \subset R$;

RS3 for all $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is an integer multiple of α .

In other words, R is a root system if it satisfies RS1 and, for each $\alpha \in R$, there exists a (unique) vector $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \in \mathbb{Z}$, and the reflection $s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ maps R in R .

We sometimes refer to the pair (V, R) as a root system over F . The elements of R are called the **roots** of the root system. If α is a root, then $s_\alpha(\alpha) = -\alpha$ is also a root. The dimension of V is called the **rank** of the root system.

EXAMPLE 1.4 Let V be the hyperplane in F^{n+1} of $n + 1$ -tuples $(x_i)_{1 \leq i \leq n+1}$ such that $\sum x_i = 0$, and let

$$R = \{\alpha_{ij} \stackrel{\text{def}}{=} e_i - e_j \mid i \neq j, \quad 1 \leq i, j \leq n + 1\}$$

where $(e_i)_{1 \leq i \leq n+1}$ is the standard basis for F^{n+1} . For each $i \neq j$, let $s_{\alpha_{ij}}$ be the linear map $V \rightarrow V$ that switches the i th and j th entries of an $n + 1$ -tuple in V . Then $s_{\alpha_{ij}}$ is a reflection with vector α_{ij} such that $s_{\alpha_{ij}}(R) \subset R$ and $s_{\alpha_{ij}}(\beta) - \beta \in \mathbb{Z}\alpha_{ij}$ for all $\beta \in R$. As R obviously spans V , this shows that R is a root system in V .

For other examples of root systems, see §2h below.

PROPOSITION 1.5 Let (V, R) be a root system over F , and let V_0 be the \mathbb{Q} -vector space generated by R . Then $c \otimes v \mapsto cv: F \otimes_{\mathbb{Q}} V_0 \rightarrow V$ is an isomorphism, and R is a root system in V_0 (Bourbaki LIE, VI, 1.1, Pptn 1; Serre 1987, V, 17, Thm 5, p. 41).

Thus, to give a root system over F is the same as giving a root system over \mathbb{Q} (or \mathbb{R} or \mathbb{C}). In the following, we assume that $F \subset \mathbb{R}$ (and sometimes that $F = \mathbb{R}$).

PROPOSITION 1.6 If $(V_i, R_i)_{i \in I}$ is a finite family of root systems, then

$$\bigoplus_{i \in I} (V_i, R_i) \stackrel{\text{def}}{=} (\bigoplus_{i \in I} V_i, \bigsqcup R_i)$$

is a root system (called the **direct sum** of the (V_i, R_i)).

A root system is **indecomposable** (or **irreducible**) if it can not be written as a direct sum of nonempty root systems.

PROPOSITION 1.7 Let (V, R) be a root system. There exists a unique partition $R = \bigsqcup_{i \in I} R_i$ of R such that

$$(V, R) = \bigoplus_{i \in I} (V_i, R_i), \quad V_i = \text{span of } R_i,$$

and each (V_i, R_i) is an indecomposable root system (Bourbaki LIE, VI, 1.2).

Suppose that roots α and β are multiples of each other, say,

$$\beta = c\alpha, \quad c \in F, \quad 0 < c < 1.$$

Then $\langle c\alpha, \alpha^\vee \rangle = 2c \in \mathbb{Z}$ and so $c = \frac{1}{2}$. For each root α , the set of roots that are multiples of α is either $\{-\alpha, \alpha\}$ or $\{-\alpha, -\alpha/2, \alpha/2, \alpha\}$. When only the first case occurs, the root system is said to be **reduced**.

From now on “root system” will mean “reduced root system”.

1c The Weyl group

Let (V, R) be a root system. The **Weyl group** $W = W(R)$ of (V, R) is the subgroup of $GL(V)$ generated by the reflections s_α for $\alpha \in R$. Because R spans V , the group W acts faithfully on R , and so is finite.

For $\alpha \in R$, we let H_α denote the hyperplane of vectors fixed by s_α . A **Weyl chamber** is a connected component of $V \setminus \bigcup_{\alpha \in R} H_\alpha$.

PROPOSITION 1.8 *The group $W(R)$ acts simply transitively on the set of Weyl chambers (Bourbaki LIE, VI, §1, 5).*

1d Existence of an inner product

PROPOSITION 1.9 *For any root system (V, R) , there exists an inner product $(,)$ on V such the $w \in R$, act as orthogonal transformations, i.e., such that*

$$(wx, wy) = (x, y) \text{ for all } w \in W, x, y \in V.$$

PROOF. Let $(,)'$ be any inner product $V \times V \rightarrow \mathbb{R}$, and define

$$(x, y) = \sum_{w \in W} (wx, wy)'$$

Then $(,)$ is again symmetric and bilinear, and

$$(x, x) = \sum_{w \in W} (wx, wx)' > 0$$

if $x \neq 0$, and so $(,)$ is positive-definite. On the other hand, for $w_0 \in W$,

$$\begin{aligned} (w_0x, w_0y) &= \sum_{w \in W} (ww_0x, ww_0y)' \\ &= (x, y) \end{aligned}$$

because as w runs through W , so also does ww_0 . □

In fact, there is a canonical inner product on V .

When we equip V with an inner product $(,)$ as in (1.9),

$$s_\alpha(x) = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha \text{ for all } x \in V.$$

Therefore the hyperplane of vectors fixed by α is orthogonal to α , and the ratio $(x, \alpha)/(\alpha, \alpha)$ is independent of the choice of the inner product:

$$2 \frac{(x, \alpha)}{(\alpha, \alpha)} = \langle x, \alpha^\vee \rangle.$$

1e Bases

Let (V, R) be a root system. A subset S of R is a **base** for R if it is a basis for V and if each root can be written $\beta = \sum_{\alpha \in S} m_\alpha \alpha$ with the m_α integers of the same sign (i.e., either all $m_\alpha \geq 0$ or all $m_\alpha \leq 0$). The elements of a (fixed) base are called the **simple roots** (for the base).

PROPOSITION 1.10 *There exists a base S for R (Bourbaki LIE, VI, §1, 5).*

More precisely, let t lie in a Weyl chamber, so t is an element of V such that $\langle t, \alpha^\vee \rangle \neq 0$ if $\alpha \in R$, and let $R^+ = \{\alpha \in R \mid \langle \alpha, t \rangle > 0\}$. Say that $\alpha \in R^+$ is **indecomposable** if it can not be written as a sum of two elements of R^+ . The indecomposable elements form a base, which depends only on the Weyl chamber of t . Every base arises in this way from a unique Weyl chamber, and so (1.8) shows that W acts simply transitively on the set of bases for R .

PROPOSITION 1.11 *Let S be a base for R . Then W is generated by the $\{s_\alpha \mid \alpha \in S\}$, and $W \cdot S = R$ (Serre 1987, V, 10, p. 33).*

PROPOSITION 1.12 *Let S be a base for R . If S is indecomposable, there exists a root $\tilde{\alpha} = \sum_{\alpha \in S} n_\alpha \alpha$ such that, for any other root $\sum_{\alpha \in S} m_\alpha \alpha$, we have that $n_\alpha \geq m_\alpha$ for all α (Bourbaki LIE, VI, §1, 8).*

Obviously $\tilde{\alpha}$ is uniquely determined by the base S . It is called the **highest root** (for the base). The simple roots α with $n_\alpha = 1$ are said to be **special**.

EXAMPLE 1.13 Let (V, R) be the root system in (1.4), and endow V with the usual inner product (assume $F \subset \mathbb{R}$). When we choose

$$t = ne_1 + \cdots + e_n - \frac{n}{2}(e_1 + \cdots + e_{n+1}),$$

then

$$R^+ \stackrel{\text{def}}{=} \{\alpha \mid \langle \alpha, t \rangle > 0\} = \{e_i - e_j \mid i > j\}.$$

For $i > j + 1$,

$$e_i - e_j = (e_i - e_{i+1}) + \cdots + (e_{j+1} - e_j),$$

and so $e_i - e_j$ is decomposable. The indecomposable elements are $e_1 - e_2, \dots, e_n - e_{n+1}$. Obviously, they *do* form a base S for R . The Weyl group has a natural identification with S_{n+1} , and it certainly is generated by the elements $s_{\alpha_1}, \dots, s_{\alpha_n}$ where $\alpha_i = e_i - e_{i+1}$; moreover, $W \cdot S = R$. The highest root is

$$\tilde{\alpha} = e_1 - e_{n+1} = \alpha_1 + \cdots + \alpha_n.$$

1f Reduced root systems of rank 2

The root systems of rank 1 are the subsets $\{\alpha, -\alpha\}$, $\alpha \neq 0$, of a vector space V of dimension 1, and so the first interesting case is rank 2. Assume $F = \mathbb{R}$, and choose an invariant inner product. For roots α, β , we let

$$n(\beta, \alpha) = 2 \frac{(\beta, \alpha)}{(\alpha, \alpha)} = \langle \beta, \alpha^\vee \rangle \in \mathbb{Z}.$$

Write

$$n(\beta, \alpha) = 2 \frac{|\beta|}{|\alpha|} \cos \phi$$

where $|\cdot|$ denotes the length of a vector and ϕ is the angle between α and β . Then

$$n(\beta, \alpha) \cdot n(\alpha, \beta) = 4 \cos^2 \phi \in \mathbb{Z}.$$

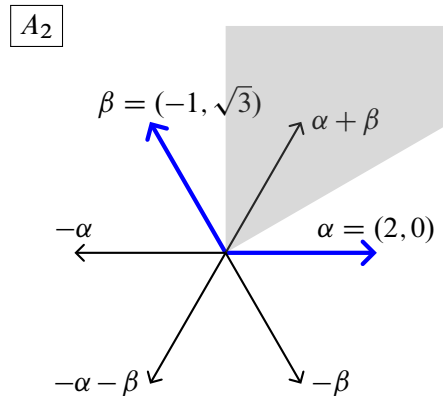
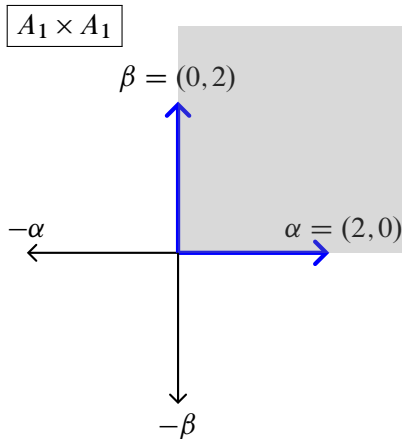
When we exclude the possibility that β is a multiple of α , there are only the following possibilities (in the table, we have chosen β to be the longer root):

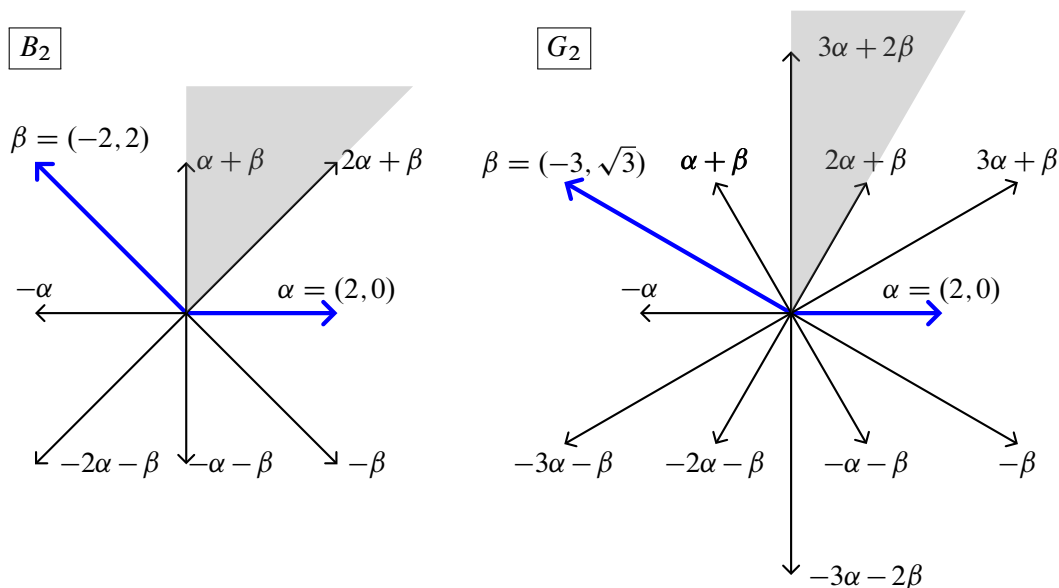
$n(\beta, \alpha) \cdot n(\alpha, \beta)$	$n(\alpha, \beta)$	$n(\beta, \alpha)$	ϕ	$ \beta / \alpha $
0	0	0	$\pi/2$	
1	1	1	$\pi/3$	1
2	1	2	$\pi/4$	$\sqrt{2}$
3	1	3	$\pi/6$	$\sqrt{3}$
	-1	-3	$5\pi/6$	

If α and β are simple roots and $n(\alpha, \beta)$ and $n(\beta, \alpha)$ are strictly positive (i.e., the angle between α and β is acute), then (from the table) one, say, $n(\beta, \alpha)$, equals 1. Then

$$s_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha = \beta - \alpha,$$

and so $\pm(\alpha - \beta)$ are roots, and one, say $\alpha - \beta$, will be in R^+ . But then $\alpha = (\alpha - \beta) + \beta$, contradicting the simplicity of α . We conclude that $n(\alpha, \beta)$ and $n(\beta, \alpha)$ are both negative. From this it follows that there are exactly the four nonisomorphic root systems of rank 2 displayed below. The set $\{\alpha, \beta\}$ is the base determined by the shaded Weyl chamber.





Note that each set of vectors does satisfy (RS1–3). The root system $A_1 \times A_1$ is decomposable and the remainder are indecomposable.

We have

	$A_1 \times A_1$	A_2	B_2	G_2
$s_\alpha(\beta) - \beta$	0α	1α	2α	3α
ϕ	$\pi/2$	$2\pi/3$	$3\pi/4$	$5\pi/6$
$W(R)$	D_2	D_3	D_4	D_6
$(\text{Aut}(R): W(R))$	2	2	1	1

where D_n denotes the dihedral group of order $2n$.

1g Cartan matrices

Let (V, R) be a root system. As before, for $\alpha, \beta \in R$, we let

$$n(\alpha, \beta) = \langle \alpha, \beta^\vee \rangle \in \mathbb{Z},$$

so that

$$n(\alpha, \beta) = 2 \frac{(\alpha, \beta)}{(\beta, \beta)}$$

for any inner form satisfying (1.9). From the second expression, we see that $n(w\alpha, w\beta) = n(\alpha, \beta)$ for all $w \in W$.

Let S be a base for R . The **Cartan matrix** of R (relative to S) is the matrix $(n(\alpha, \beta))_{\alpha, \beta \in S}$. Its diagonal entries $n(\alpha, \alpha)$ equal 2, and the remaining entries are negative or zero.

For example, the Cartan matrices of the root systems of rank 2 are,

$$\begin{matrix}
 \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -2 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \\
 A_1 \times A_1 & A_2 & B_2 & G_2
 \end{matrix}$$

and the Cartan matrix for the root system in (1.4) is

$$\begin{pmatrix} 2 & -1 & 0 & & 0 & 0 \\ -1 & 2 & -1 & & 0 & 0 \\ 0 & -1 & 2 & & 0 & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & & 2 & -1 \\ 0 & 0 & 0 & & -1 & 2 \end{pmatrix}$$

because

$$2 \frac{(e_i - e_{i+1}, e_{i+1} - e_{i+2})}{(e_i - e_{i+1}, e_i - e_{i+1})} = -1, \text{ etc.}$$

PROPOSITION 1.14 *The Cartan matrix of (V, R) is independent of S , and determines (V, R) up to isomorphism.*

In fact, if S' is a second base for R , then we know that $S' = wS$ for a *unique* $w \in W$ and that $n(w\alpha, w\beta) = n(\alpha, \beta)$. Thus S and S' give the same Cartan matrices up to re-indexing the columns and rows. Let (V', R') be a second root system with the same Cartan matrix. This means that there exists a base S' for R' and a bijection $\alpha \mapsto \alpha': S \rightarrow S'$ such that

$$n(\alpha, \beta) = n(\alpha', \beta') \text{ for all } \alpha, \beta \in S. \quad (160)$$

The bijection extends uniquely to an isomorphism of vector spaces $V \rightarrow V'$, which sends s_α to $s_{\alpha'}$ for all $\alpha \in S$ because of (160). But the s_α generate the Weyl groups (1.11), and so the isomorphism maps W onto W' , and hence it maps $R = W \cdot S$ onto $R' = W' \cdot S'$ (see 1.11). We have shown that the bijection $S \rightarrow S'$ extends uniquely to an isomorphism $(V, R) \rightarrow (V', R')$ of root systems.

1h Classification of root systems by Dynkin diagrams

Let (V, R) be a root system, and let S be a base for R .

PROPOSITION 1.15 *Let α and β be distinct simple roots. Up to interchanging α and β , the only possibilities for $n(\alpha, \beta)$ are*

$n(\alpha, \beta)$	$n(\beta, \alpha)$	$n(\alpha, \beta)n(\beta, \alpha)$
0	0	0
-1	-1	1
-2	-1	2
-3	-1	3

If W is the subspace of V spanned by α and β , then $W \cap R$ is a root system of rank 2 in W , and so (1.15) can be read off from the Cartan matrices of the rank 2 systems.

Choose a base S for R . Then the **Coxeter graph** of (V, R) is the graph whose nodes are indexed by the elements of S ; two distinct nodes are joined by $n(\alpha, \beta) \cdot n(\beta, \alpha)$ edges. Up to the indexing of the nodes, it is independent of the choice of S .

PROPOSITION 1.16 *The Coxeter graph is connected if and only if the root system is indecomposable.*

In other words, the decomposition of the Coxeter graph of (V, R) into its connected components corresponds to the decomposition of (V, R) into a direct sum of its indecomposable summands.

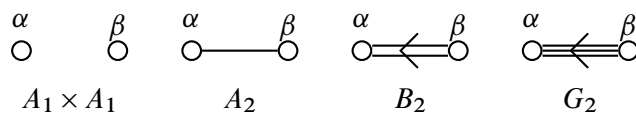
PROOF. A root system is decomposable if and only if R can be written as a disjoint union $R = R_1 \sqcup R_2$ with each root in R_1 orthogonal to each root in R_2 . Since roots α, β are orthogonal if and only if $n(\alpha, \beta) \cdot n(\beta, \alpha) = 4 \cos^2 \phi = 0$, this is equivalent to the Coxeter graph being disconnected. □

The Coxeter graph doesn't determine the Cartan matrix because it only gives the number $n(\alpha, \beta) \cdot n(\beta, \alpha)$. However, for each value of $n(\alpha, \beta) \cdot n(\beta, \alpha)$ there is only one possibility for the unordered pair

$$\{n(\alpha, \beta), n(\beta, \alpha)\} = \left\{ 2 \frac{|\alpha|}{|\beta|} \cos \phi, 2 \frac{|\beta|}{|\alpha|} \cos \phi \right\}.$$

Thus, if we know in addition which is the longer root, then we know the *ordered* pair. To remedy this, we put an arrowhead on the lines joining the nodes indexed by α and β pointing towards the shorter root. The resulting diagram is called the **Dynkin diagram** of the root system. It determines the Cartan matrix and hence the root system.

For example, the Dynkin diagrams of the root systems of rank 2 are:



THEOREM 1.17 *The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_6 , E_7 , E_8 , F_4 , G_2 listed at the end of the section — we have used the conventional (Bourbaki) numbering for the simple roots.*

PROOF. See, for example, Humphreys 1972, 11.4. □

For example, the Dynkin diagram of the root system in (1.4, 1.13) is A_n . Note that Coxeter graphs do not distinguish B_n from C_n .

1i The root and weight lattices

1.18 Let X be a lattice in a vector space V over F . The **dual lattice** to X is

$$Y = \{y \in V^\vee \mid \langle X, y \rangle \subset \mathbb{Z}\}.$$

If e_1, \dots, e_m is a basis of V that generates X as a \mathbb{Z} -module, then Y is generated by the dual basis f_1, \dots, f_m (defined by $\langle e_i, f_j \rangle = \delta_{ij}$).

1.19 Let (V, R) be a root system in V . Recall that, for each $\alpha \in R$, there is a unique $\alpha^\vee \in V$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \in \mathbb{Z}$, and the reflection $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ sends R into R . The set $R^\vee \stackrel{\text{def}}{=} \{\alpha^\vee \mid \alpha \in R\}$ is a root system in V^\vee (called the *inverse root system*).

1.20 (Bourbaki LIE, VI, §1, 9.) Let (V, R) be a root system. The *root lattice* $Q = Q(R)$ is the \mathbb{Z} -submodule of V generated by the roots:

$$Q(R) = \mathbb{Z}R = \left\{ \sum_{\alpha \in R} m_\alpha \alpha \mid m_\alpha \in \mathbb{Z} \right\}.$$

Every base for R forms a basis for Q . The *weight lattice* $P = P(R)$ is the lattice dual to $Q(R^\vee)$:

$$P = \{x \in V \mid \langle x, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}.$$

The elements of P are called the *weights* of the root system. We have $P(R) \supset Q(R)$ (because $\langle R, \alpha^\vee \rangle \subset \mathbb{Z}$ for all $\alpha \in R$), and the quotient $P(R)/Q(R)$ is finite (because the lattices generate the same \mathbb{Q} -vector space).

1.21 (Bourbaki LIE, VI, §1, 10.) Let S be a base for R . Then $S^\vee \stackrel{\text{def}}{=} \{\alpha^\vee \mid \alpha \in S\}$ is a base for R^\vee . For each simple root α , define $\varpi_\alpha \in P(R)$ by the condition

$$\langle \varpi_\alpha, \beta^\vee \rangle = \delta_{\alpha, \beta}, \quad \text{all } \beta \in S.$$

Then $\{\varpi_\alpha \mid \alpha \in S\}$ is a basis for the weight lattice $P(R)$, dual to the basis S^\vee . Its elements are called the *fundamental weights*.

1.22 (Bourbaki LIE, VIII, §7.) Let S be a base for R , so that

$$R = R_+ \sqcup R_- \text{ with } \begin{cases} R_+ &= \{ \sum m_\alpha \alpha \mid m_\alpha \in \mathbb{N} \} \cap R \\ R_- &= \{ \sum m_\alpha \alpha_i \mid -m_\alpha \in \mathbb{N} \} \cap R \end{cases}$$

We let $P_+ = P_+(R)$ denote the set of weights that are positive for the partial ordering on V defined by S ; thus

$$P_+(R) = \left\{ \sum_{\alpha \in S} c_\alpha \alpha \mid c_\alpha \geq 0, \quad c_\alpha \in \mathbb{Q} \right\} \cap P(R).$$

A weight λ is *dominant* if $\langle \lambda, \alpha^\vee \rangle \in \mathbb{N}$ for all $\alpha \in S$, and we let $P_{++} = P_{++}(R)$ denote the set of dominant weights of R ; thus

$$P_{++}(R) = \{x \in V \mid \langle x, \alpha^\vee \rangle \in \mathbb{N} \text{ all } \alpha \in S\} \subset P_+(R).$$

Since the ϖ_α are dominant, they are sometimes called the *fundamental dominant weights*.

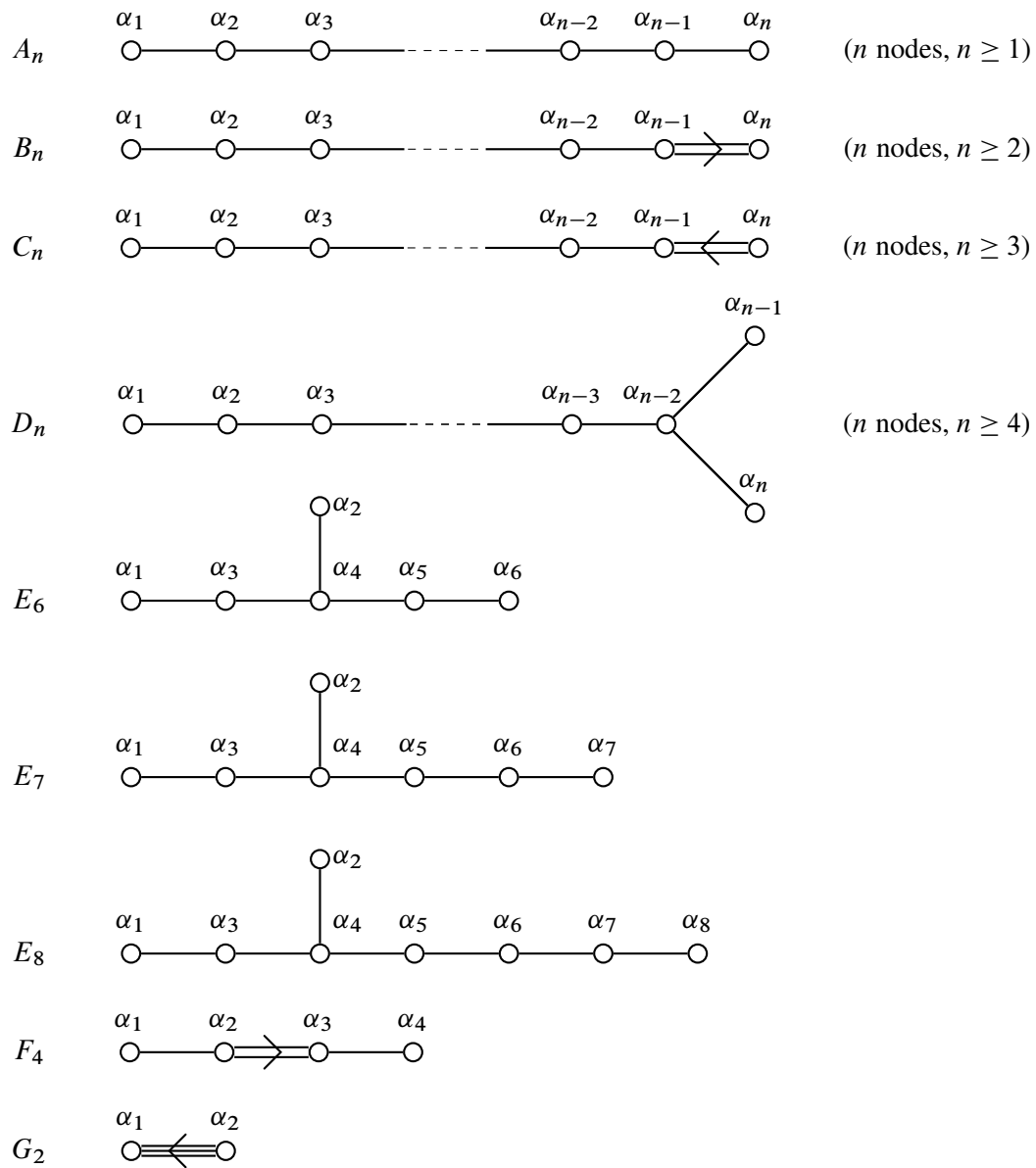
1.23 When we write $S = \{\alpha_1, \dots, \alpha_n\}$, the fundamental weights are $\varpi_1, \dots, \varpi_n$, where

$$\langle \varpi_i, \alpha_j^\vee \rangle = \delta_{ij}.$$

Moreover

$$\begin{aligned} R &= R_+ \sqcup R_- \text{ with } \begin{cases} R_+ &= \{ \sum m_i \alpha_i \mid m_i \in \mathbb{N} \} \cap R \\ R_- &= \{ \sum m_i \alpha_i \mid -m_i \in \mathbb{N} \} \cap R \end{cases}; \\ Q(R) &= \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n \subset V = \mathbb{R}\alpha_1 \oplus \dots \oplus \mathbb{R}\alpha_n; \\ P(R) &= \mathbb{Z}\varpi_1 \oplus \dots \oplus \mathbb{Z}\varpi_n \subset V = \mathbb{R}\varpi_1 \oplus \dots \oplus \mathbb{R}\varpi_n; \\ P_{++}(S) &= \left\{ \sum m_i \varpi_i \mid m_i \in \mathbb{N} \right\}. \end{aligned}$$

1j List of indecomposable Dynkin diagrams



2 Structure of semisimple Lie algebras and their representations

This section is an introductory survey, based on Bourbaki LIE, where the reader can find omitted details. Most can also be found in Jacobson 1962 and, when the ground field k is algebraically closed field, in Humphreys 1972 and Serre 1966.

Throughout this section, k is a field of characteristic zero, and all representations of Lie algebras are finite dimensional.

2a Elementary automorphisms of a Lie algebra

2.1 If u is a nilpotent endomorphism of a k -vector space V , then the sum $e^u = \sum_{n \geq 0} u^n/n!$ has only finitely many terms (it is a polynomial in u), and so it is also an endomorphism of V . If v is another nilpotent endomorphism of V that commutes with u , then

$$\begin{aligned} e^u e^v &= \left(\sum_{m \geq 0} \frac{u^m}{m!} \right) \left(\sum_{n \geq 0} \frac{v^n}{n!} \right) \\ &= \sum_{m, n \geq 0} \frac{u^m v^n}{m! n!} \\ &= \sum_{r \geq 0} \frac{1}{r!} \left(\sum_{m+n=r} \binom{r}{m} u^m v^n \right) \\ &= \sum_{r \geq 0} \frac{1}{r!} (u+v)^r \\ &= e^{u+v}. \end{aligned}$$

In particular, $e^u e^{-u} = e^0 = 1$, and so e^u an automorphism of V .

2.2 Now suppose that V is equipped with a k -bilinear pairing $V \times V$ (i.e., it is a k -algebra) and that u is a nilpotent *derivation* of V . Recall that this means that

$$u(xy) = x \cdot u(y) + u(x) \cdot y \quad (x, y \in V).$$

On iterating this, we find that

$$u^r(x, y) = \sum_{m+n=r} \binom{r}{m} u^m(x) \cdot u^n(y) \quad (\text{Leibniz's formula}).$$

Hence

$$\begin{aligned} e^u(xy) &= \sum_{r \geq 0} \frac{1}{r!} u^r(xy) \quad (\text{definition of } e^u) \\ &= \sum_{r \geq 0} \frac{1}{r!} \sum_{m+n=r} \binom{r}{m} u^m(x) \cdot u^n(y) \quad (\text{Leibniz's formula}) \\ &= \sum_{m, n \geq 0} \frac{u^m(x)}{m!} \cdot \frac{u^n(y)}{n!} \\ &= e^u(x) \cdot e^u(y). \end{aligned}$$

Therefore e^u is an automorphism of the k -algebra V . In particular, a nilpotent derivation u of a Lie algebra defines an automorphism of the Lie algebra.

2.3 The **nilpotent radical** of a Lie algebra \mathfrak{g} is the intersection of the kernels of the *simple* representations of \mathfrak{g} . For any x in the nilpotent radical of \mathfrak{g} , $\text{ad}_{\mathfrak{g}} x$ is a nilpotent derivation of \mathfrak{g} , and so $e^{\text{ad}_{\mathfrak{g}}(x)}$ is an automorphism of \mathfrak{g} . Such an automorphism is said to be **special**. (Bourbaki LIE, I, §6, 8.)

2.4 More generally, any element x of \mathfrak{g} such that $\text{ad}_{\mathfrak{g}}(x)$ is nilpotent defines an automorphism of \mathfrak{g} . A finite products of such automorphisms is said to be **elementary**. The elementary automorphisms of \mathfrak{g} form a subgroup $\text{Aut}_e(\mathfrak{g})$ of $\text{Aut}(\mathfrak{g})$. As $u e^{\text{ad}(x)} u^{-1} = e^{\text{ad}(ux)}$ for any automorphism u of \mathfrak{g} , $\text{Aut}_e(\mathfrak{g})$ is a normal subgroup of $\text{Aut}(\mathfrak{g})$. (Bourbaki Lie, VII, §3, 1).

2.5 Let \mathfrak{g} be a Lie algebra. According to Theorem 11.14, there exists an affine group G such that

$$\text{Rep}(G) = \text{Rep}(\mathfrak{g}).$$

Let x be an element of \mathfrak{g} such that $\rho(x)$ is nilpotent for all representation (V, ρ) of \mathfrak{g} over k , and let $(e^x)_V = e^{\rho(x)}$. Then

- ◇ $(e^x)_{V \otimes W} = (e^x)_V \otimes (e^x)_W$ for all representations (V, ρ_V) and (W, ρ_W) of \mathfrak{g} ;
- ◇ $(e^x)_V = \text{id}_V$ if \mathfrak{g} acts trivially on V ;
- ◇ $(e^x)_W \circ \alpha_R = \alpha_R \circ (e^x)_V$ for all homomorphisms $\alpha: (V, \rho_V) \rightarrow (W, \rho_W)$ of representations of \mathfrak{g} over k .

Therefore (Theorem 10.2), there exists a unique element e^x in $G(k)$ such that e^x acts on V as $e^{\rho(x)}$ for all representations (V, ρ) of \mathfrak{g} .

ASIDE 2.6 Let $\text{Aut}_0(\mathfrak{g})$ denote the (normal) subgroup of $\text{Aut}(\mathfrak{g})$ consisting of automorphisms that become elementary over k^{al} . If \mathfrak{g} is semisimple, then $\text{Aut}_e(\mathfrak{g})$ is equal to its own derived group, and when \mathfrak{g} is split, it is equal to the derived group of $\text{Aut}_0(\mathfrak{g})$ (Bourbaki LIE, VIII, §5, 2; §11, 2, Pptn 3).

2b Jordan decompositions in semisimple Lie algebras

Recall that every endomorphism of a vector space has a unique (additive Jordan) decomposition into the sum of a semisimple endomorphism and a commuting nilpotent endomorphism (II, 3.22). For a Lie subalgebra \mathfrak{g} of \mathfrak{gl}_V , the semisimple and nilpotent components of an element of \mathfrak{g} need not lie in \mathfrak{g} (II, 1.40).

DEFINITION 2.7 An element x of a semisimple Lie algebra is *semisimple* (resp. *nilpotent*) if, for every \mathfrak{g} -module V , x_V is semisimple (resp. nilpotent).

THEOREM 2.8 *Every element of a semisimple Lie has a unique (Jordan) decomposition into the sum of a semisimple element and a commuting nilpotent element.*

PROOF. Omitted for the present (Bourbaki LIE, I, §6, 3, Thm 3) — the proof uses Weyl's theorem (II, 6.10). □

Let x be an element of a semisimple Lie algebra \mathfrak{g} , and let $x = x_s + x_n$ be its decomposition. For any \mathfrak{g} -module V , $x_V = (x_s)_V + (x_n)_V$ is the Jordan decomposition of x_V .

COROLLARY 2.9 *In order to show that an element of a semisimple Lie algebra is semisimple (resp. nilpotent), it suffices to check that it acts semisimply (resp. nilpotently) on one faithful module.*

PROOF. If $(x_n)_V = 0$ for one faithful \mathfrak{g} -module V , then $x_n = 0$, and so $x_W = (x_s)_W$ for every \mathfrak{g} -module W . □

ASIDE 2.10 As noted earlier (§1m), Theorem 2.8 holds for every algebraic Lie algebra. The theorem may be regarded as the first step in the proof that all semisimple Lie algebras are algebraic.

2c Split semisimple Lie algebras

DEFINITION 2.11 A Lie algebra \mathfrak{h} is **toral** if $\text{ad}_{\mathfrak{h}} x$ is semisimple for every element x of \mathfrak{h} .

PROPOSITION 2.12 *Every toral Lie algebra is abelian.*

PROOF. Let x be an element of such an algebra. We have to show that $\text{ad } x = 0$. If not, then, after possibly passing to a larger base field, $\text{ad } x$ will have an eigenvector with nonzero eigenvalue, say $\text{ad}(x)(y) = cy$, $c \neq 0$, $y \neq 0$. Now $\text{ad}(y)(x) = -\text{ad}(x)(y) = -cy \neq 0$ but $\text{ad}(y)^2(x) = \text{ad}(y)(-cy) = 0$. Thus, $\text{ad}(y)$ doesn't act semisimply on the subspace of \mathfrak{h} spanned by x and y , which contradicts its semisimplicity on \mathfrak{h} . \square

DEFINITION 2.13 A **Cartan subalgebra** of a semisimple Lie algebra is a maximal toral subalgebra.²

Because the adjoint representation of a semisimple Lie algebra is faithful, (2.9) shows that the elements of toral subalgebra of a semisimple Lie algebra are semisimple (in the sense of 2.7).

EXAMPLE 2.14 For any maximal torus T in a semisimple algebraic group G , $\text{Lie}(T)$ is a Cartan subalgebra of $\text{Lie}(G)$.

PROPOSITION 2.15 *A toral subalgebra of a semisimple Lie algebra is a Cartan subalgebra if and only if it is equal to its own centralizer.*

PROOF. If $\mathfrak{h} = c_{\mathfrak{g}}(\mathfrak{h})$ then obviously \mathfrak{h} is maximal. For the converse, see Humphreys 1972, 8.2. \square

DEFINITION 2.16 A Cartan subalgebra \mathfrak{h} of a semisimple Lie algebra \mathfrak{g} is said to be **splitting** if the eigenvalues of the linear maps $\text{ad}(h): \mathfrak{g} \rightarrow \mathfrak{g}$ lie in k for all $h \in \mathfrak{h}$. A **split semisimple Lie algebra** is a pair $(\mathfrak{g}, \mathfrak{h})$ consisting of a semisimple Lie algebra \mathfrak{g} and a splitting Cartan subalgebra \mathfrak{h} (Bourbaki LIE, VIII, §2, 1, Déf. 1).

More loosely, we say that a semisimple Lie algebra is **split** if it contains a splitting Cartan subalgebra (Bourbaki says splittable).

EXAMPLE 2.17 (a) For any split maximal torus T in a semisimple algebraic group G , $\text{Lie}(T)$ is a splitting Cartan subalgebra of $\text{Lie}(G)$ (see 3.15).

(b) The subalgebra of diagonal elements is a splitting Cartan subalgebra of \mathfrak{sl}_n (see §2h).

The semisimple Lie algebra \mathfrak{g} determines the pair $(\mathfrak{g}, \mathfrak{h})$ up to isomorphism. More precisely, there is the following important result.

THEOREM 2.18 *Let \mathfrak{h} and \mathfrak{h}' be splitting Cartan subalgebras of a semisimple Lie algebra \mathfrak{g} . Then there exists an elementary automorphism e of \mathfrak{g} such that $e(\mathfrak{h}) = \mathfrak{h}'$.*

²This is not the usual definition, but is equivalent to it when the algebra is semisimple (Bourbaki LIE, VII, §2, 4, Th. 2).

PROOF. Bourbaki LIE, VIII, §3, 3, Cor. to Prop. 10. \square

DEFINITION 2.19 The common dimension of the splitting Cartan subalgebras of a split semisimple Lie algebra is called the *rank* of the Lie algebra.

2d The roots of a split semisimple Lie algebra

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra. For each $h \in \mathfrak{h}$, the action of $\text{ad}_{\mathfrak{g}} h$ is semisimple with eigenvalues in k , and so \mathfrak{g} has a basis of eigenvectors for $\text{ad}_{\mathfrak{g}} h$. Because \mathfrak{h} is abelian, the $\text{ad}_{\mathfrak{g}} h$ form a commuting family of diagonalizable endomorphisms of \mathfrak{g} , and so there exists a basis of simultaneous eigenvectors. In other words, \mathfrak{g} is a direct sum of the subspaces³

$$\mathfrak{g}^{\alpha} \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid [h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}\}, \quad \alpha \in \mathfrak{h}^{\vee} \stackrel{\text{def}}{=} \text{Hom}_{k\text{-linear}}(\mathfrak{h}, k).$$

The *roots* of $(\mathfrak{g}, \mathfrak{h})$ are the nonzero α such that $\mathfrak{g}^{\alpha} \neq 0$. Write R for the set of roots of $(\mathfrak{g}, \mathfrak{h})$. Then the Lie algebra \mathfrak{g} decomposes into a direct sum

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^{\alpha}.$$

Clearly the set R is finite, and (by definition) doesn't contain 0. We shall see that R is a reduced root system in \mathfrak{h}^{\vee} , but first we look at the basic example of \mathfrak{sl}_2 .

2e The Lie algebra \mathfrak{sl}_2

2.20 This is the Lie algebra of 2×2 matrices with trace 0. Let

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Then

$$[x, y] = h, \quad [h, x] = 2x, \quad [h, y] = -2y.$$

Therefore $\{x, h, y\}$ is a basis of eigenvectors for $\text{ad} h$ with integer eigenvalues 2, 0, -2, and

$$\begin{aligned} \mathfrak{sl}_2 &= \mathfrak{g}^{\alpha} \oplus \mathfrak{h} \oplus \mathfrak{g}^{-\alpha} \\ &= \langle x \rangle \oplus \langle h \rangle \oplus \langle y \rangle \end{aligned}$$

where $\mathfrak{h} = \langle h \rangle$ and α is the linear map $\mathfrak{h} \rightarrow k$ such that $\alpha(h) = 2$. The decomposition shows that \mathfrak{h} is equal to its centralizer, and so it is a splitting Cartan subalgebra for \mathfrak{g} . Hence, \mathfrak{sl}_2 is a split simple Lie algebra of rank one; in fact, up to isomorphism, it is the only such Lie algebra. Let $R = \{\alpha\} \subset \mathfrak{h}^{\vee}$. Then R is a root system in \mathfrak{h}^{\vee} : it is finite, spans \mathfrak{h}^{\vee} , and doesn't contain 0; if we let α^{\vee} denote h regarded as an element of $(\mathfrak{h}^{\vee})^{\vee}$, then $\langle \alpha, \alpha^{\vee} \rangle = 2$, the reflection $x \mapsto x - \langle x, \alpha^{\vee} \rangle \alpha$ maps R to R , and $\langle \alpha, \alpha^{\vee} \rangle \in \mathbb{Z}$. The root lattice $Q = \mathbb{Z}\alpha$ and the weight lattice $P = \mathbb{Z}\frac{\alpha}{2}$.

³Elsewhere we write V_{α} rather than V^{α} . Which should it be?

2f The root system attached to a split semisimple Lie algebra

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra, and let $R \subset \mathfrak{h}^\vee$ be the set of roots of $(\mathfrak{g}, \mathfrak{h})$, so that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha.$$

LEMMA 2.21 For $\alpha, \beta \in \mathfrak{h}^\vee$, $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] \subset \mathfrak{g}^{\alpha+\beta}$.

PROOF. Let $x \in \mathfrak{g}^\alpha$ and $y \in \mathfrak{g}^\beta$. Then, for $h \in \mathfrak{h}$, we have

$$\begin{aligned} \text{ad}(h)[x, y] &= [\text{ad}(h)x, y] + [x, \text{ad}(h)y] \\ &= [\alpha(h)x, y] + [x, \beta(h)y] \\ &= (\alpha(h) + \beta(h))[x, y]. \end{aligned} \quad \square$$

THEOREM 2.22 Let α be a root of $(\mathfrak{g}, \mathfrak{h})$.

- (a) The spaces \mathfrak{g}^α and $\mathfrak{h}_\alpha \stackrel{\text{def}}{=} [\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}]$ are one-dimensional.
- (b) There is a unique element $h_\alpha \in \mathfrak{h}_\alpha$ such that $\alpha(h_\alpha) = 2$.
- (c) For each nonzero element $x_\alpha \in \mathfrak{g}^\alpha$, there is a unique $y_\alpha \in \mathfrak{g}^{-\alpha}$ such that

$$[x_\alpha, y_\alpha] = h_\alpha, \quad [h_\alpha, x_\alpha] = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -2y_\alpha.$$

Hence $\mathfrak{s}_\alpha \stackrel{\text{def}}{=} \mathfrak{g}^{-\alpha} \oplus \mathfrak{h}_\alpha \oplus \mathfrak{g}^\alpha$ is a subalgebra isomorphic to \mathfrak{sl}_2 .

PROOF. Bourbaki LIE, VIII, §2, 2, Pptn 1, Thm 1. □

In particular, for each root α of $(\mathfrak{g}, \mathfrak{h})$, there is a unique one-dimensional k -subspace \mathfrak{g}^α of \mathfrak{g} such that

$$[h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}, x \in \mathfrak{g}^\alpha.$$

The subalgebra \mathfrak{s}_α is the centralizer of $\text{Ker}(\alpha)$.

An \mathfrak{sl}_2 -triple in a Lie algebra \mathfrak{g} is a triple $(x, h, y) \neq (0, 0, 0)$ of elements such that

$$[x, y] = h, \quad [h, x] = 2x, \quad [h, y] = -2y.$$

There is a canonical one-to-one correspondence between \mathfrak{sl}_2 -triples in \mathfrak{g} and injective homomorphisms $\mathfrak{sl}_2 \rightarrow \mathfrak{g}$. The theorem says that, for each root α of \mathfrak{g} and choice of $x \in \mathfrak{g}^\alpha$, there is a unique \mathfrak{sl}_2 -triple (x, h, y) such that $\alpha(h) = 2$. Replacing x with cx replaces (x, h, y) with $(cx, h, c^{-1}y)$.⁴

THEOREM 2.23 For each $\alpha \in R$, let α^\vee denote h_α regarded as an element of $(\mathfrak{h}^\vee)^\vee$. Then R is a reduced root system in \mathfrak{h}^\vee ; moreover, α^\vee is the unique element of $(\mathfrak{h}^\vee)^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and the reflection $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ preserves R .

PROOF. Bourbaki LIE, VIII, §2, 2, Thm 2. □

⁴Cf. Bourbaki LIE, §11, 1, where it is required that $[x, y] = -h$. In other words, Bourbaki replaces everyone else's y with $-y$.

Note that, once we choose a base for R , the dominant weights (i.e., the elements of P_{++}) are exactly the elements α of \mathfrak{h}^\vee such that $\alpha(h_\beta) \in \mathbb{N}$ for all $\beta \in R_+$.

ASIDE 2.24 Let x be an element of a semisimple Lie algebra \mathfrak{g} (not necessarily split). If x belongs to an \mathfrak{sl}_2 -triple (x, h, y) , then x is nilpotent (apply 2.9). Conversely, the Jacobson-Morozov theorem says that every nonzero nilpotent element x in a semisimple Lie algebra extends to an \mathfrak{sl}_2 -triple (x, h, y) (Bourbaki LIE, VIII, §11, 2).

2g Criteria for simplicity and semisimplicity

PROPOSITION 2.25 Let \mathfrak{g} be a Lie algebra, and let \mathfrak{h} be an abelian Lie subalgebra. For each $\alpha \in \mathfrak{h}^\vee$, let

$$\mathfrak{g}^\alpha = \{x \in \mathfrak{g} \mid hx = \alpha(h)x \text{ all } h \in \mathfrak{h}\},$$

and let R be the set of nonzero $\alpha \in \mathfrak{h}^\vee$ such that $\mathfrak{g}^\alpha \neq 0$. Suppose that:

- (a) $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha$;
- (b) for each $\alpha \in R$, the space \mathfrak{g}^α has dimension 1;
- (c) for each nonzero $h \in \mathfrak{h}$, there exists an $\alpha \in R$ such that $\alpha(h) \neq 0$; and
- (d) if $\alpha \in R$, then $-\alpha \in R$ and $[[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha] \neq 0$.

Then \mathfrak{g} is semisimple and \mathfrak{h} is a splitting Cartan subalgebra of \mathfrak{g} .

PROOF. Let \mathfrak{a} be an abelian ideal in \mathfrak{g} ; we have to show that $\mathfrak{a} = 0$. As $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$, (a) gives us a decomposition

$$\mathfrak{a} = \mathfrak{a} \cap \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{a} \cap \mathfrak{g}^\alpha.$$

If $\mathfrak{a} \cap \mathfrak{g}^\alpha \neq 0$ for some $\alpha \in R$, then $\mathfrak{a} \supset \mathfrak{g}^\alpha$ (by (b)). As \mathfrak{a} is an ideal, this implies that $\mathfrak{a} \supset [\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}]$, and as $[\mathfrak{a}, \mathfrak{a}] = 0$, this implies that $[[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha] = 0$, contradicting (d).

Suppose $\mathfrak{a} \cap \mathfrak{h} \neq 0$, and let h be a nonzero element of $\mathfrak{a} \cap \mathfrak{h}$. According to (c), there exists an $\alpha \in R$ such that $\alpha(h) \neq 0$. Let x be a nonzero element of \mathfrak{g}^α . Then $[h, x] = \alpha(h)x$, which is a nonzero element of \mathfrak{g}^α . As $[h, x] \in \mathfrak{a}$, this contradicts the last paragraph.

Condition (a) implies that the elements of \mathfrak{h} act semisimply on \mathfrak{g} and that their eigenvalues lie in k and that \mathfrak{h} is its own centralizer. Therefore \mathfrak{h} is a splitting Cartan subalgebra of \mathfrak{g} . \square

PROPOSITION 2.26 Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple algebra. A decomposition $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ of semisimple Lie algebras defines a decomposition $(\mathfrak{g}, \mathfrak{h}) = (\mathfrak{g}_1, \mathfrak{h}_1) \oplus (\mathfrak{g}_2, \mathfrak{h}_2)$, and hence a decomposition of the root system of $(\mathfrak{g}, \mathfrak{h})$.

PROOF. Let

$$\begin{aligned} \mathfrak{g} &= \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha \\ \mathfrak{g}_1 &= \mathfrak{h}_1 \oplus \bigoplus_{\alpha \in R_1} \mathfrak{g}_1^\alpha \\ \mathfrak{g}_2 &= \mathfrak{h}_2 \oplus \bigoplus_{\alpha \in R_2} \mathfrak{g}_2^\alpha \end{aligned}$$

be the eigenspace decompositions of \mathfrak{g} , \mathfrak{g}_1 , and \mathfrak{g}_2 respectively defined by the action of \mathfrak{h} . Then $\mathfrak{h} = \mathfrak{h}_1 \oplus \mathfrak{h}_2$ and $R = R_1 \sqcup R_2$. \square

COROLLARY 2.27 *If the root system of $(\mathfrak{g}, \mathfrak{h})$ is indecomposable (equivalently, its Dynkin diagram is connected), then \mathfrak{g} is simple.*

ASIDE 2.28 The converses of (2.26) and (2.27) are also true: a decomposition of its root system defines a decomposition of $(\mathfrak{g}, \mathfrak{h})$, and if \mathfrak{g} is simple then the root system of $(\mathfrak{g}, \mathfrak{h})$ is indecomposable (2.32 below).

2h Examples

We first look at $\hat{\mathfrak{g}} = \mathfrak{gl}_{n+1}$, even though this is not (quite) a semisimple algebra (its centre is the subalgebra of scalar matrices). Let $\hat{\mathfrak{h}}$ be the Lie subalgebra of diagonal elements in $\hat{\mathfrak{g}}$. Let E_{ij} be the matrix in $\hat{\mathfrak{g}}$ with 1 in the (i, j) th position and zeros elsewhere. Then $(E_{ij})_{1 \leq i, j \leq n+1}$ is a basis for $\hat{\mathfrak{g}}$ and $(E_{ii})_{1 \leq i \leq n+1}$ is a basis for $\hat{\mathfrak{h}}$. Let $(\varepsilon_i)_{1 \leq i \leq n+1}$ be the dual basis for $\hat{\mathfrak{h}}^\vee$; thus

$$\varepsilon_i(\text{diag}(a_1, \dots, a_{n+1})) = a_i.$$

An elementary calculation shows that, for $h \in \hat{\mathfrak{h}}$,

$$[h, E_{ij}] = (\varepsilon_i(h) - \varepsilon_j(h))E_{ij}.$$

Thus,

$$\hat{\mathfrak{g}} = \hat{\mathfrak{h}} \oplus \bigoplus_{\alpha \in R} \hat{\mathfrak{g}}^\alpha$$

where $R = \{\varepsilon_i - \varepsilon_j \mid i \neq j, 1 \leq i, j \leq n+1\}$ and $\hat{\mathfrak{g}}^{\varepsilon_i - \varepsilon_j} = kE_{ij}$.

EXAMPLE (A_n): \mathfrak{sl}_{n+1}

Let $\mathfrak{g} = \mathfrak{sl}(W)$ where W is a vector space of dimension $n+1$. Choose a basis $(e_i)_{1 \leq i \leq n+1}$ for W , and use it to identify \mathfrak{g} with \mathfrak{sl}_{n+1} , and let \mathfrak{h} be the Lie subalgebra of diagonal matrices in \mathfrak{g} . The matrices

$$E_{i,i} - E_{i+1,i+1} \quad (1 \leq i \leq n)$$

form a basis for \mathfrak{h} , and, together with the matrices

$$E_{ij} \quad (1 \leq i, j \leq n, i \neq j),$$

they form a basis for \mathfrak{g} .

Let V be the hyperplane in $\hat{\mathfrak{h}}^\vee$ consisting of the elements $\alpha = \sum_{i=1}^{n+1} a_i \varepsilon_i$ such that $\sum_{i=1}^{n+1} a_i = 0$. The restriction map $\lambda \mapsto \lambda|_{\mathfrak{h}}$ defines an isomorphism of V onto \mathfrak{h}^\vee , which we use to identify the two spaces.⁵ Now

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha$$

where $R = \{\varepsilon_i - \varepsilon_j \mid i \neq j\} \subset V$ and $\mathfrak{g}^{\varepsilon_i - \varepsilon_j} = kE_{ij}$. We check the conditions of Proposition 2.25. We already know that (a) and (b) hold. For (c), let

$$h = \text{diag}(c_1, \dots, c_{n+1}), \quad \sum c_i = 0,$$

⁵In more detail: $\hat{\mathfrak{h}}$ is a vector space with basis $E_{11}, \dots, E_{n+1, n+1}$, and \mathfrak{h} its subspace $\{\sum a_i E_{ii} \mid \sum a_i = 0\}$. The dual of $\hat{\mathfrak{h}}$ is a vector space with basis $\varepsilon_1, \dots, \varepsilon_{n+1}$ where $\varepsilon_i(E_j) = \delta_{ij}$, and the dual of \mathfrak{h} is the quotient of $(\hat{\mathfrak{h}})^\vee$ by the line $\langle \varepsilon_1 + \dots + \varepsilon_{n+1} \rangle$. However, it is more convenient to identify dual of \mathfrak{h} with the orthogonal complement of this line, namely, with the hyperplane V in $(\hat{\mathfrak{h}})^\vee$.

be an element of \mathfrak{h} . If $h \neq 0$, then $c_i \neq c_j$ for some i, j , and so $(\varepsilon_i - \varepsilon_j)(h) = c_i - c_j \neq 0$. For (d), let $\alpha = \varepsilon_i - \varepsilon_j$. Then $-\alpha$, is also a root and

$$\begin{aligned} [[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha] &\ni [[E_{ij}, E_{ji}], kE_{ij}] \\ &= [E_{ii} - E_{jj}, E_{ij}] \\ &= 2. \end{aligned}$$

Therefore $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra.

The family $(\alpha_i)_{1 \leq i \leq n}$, $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, is a base for R . Relative to the inner product

$$(\sum a_i \varepsilon_i, \sum b_i \varepsilon_i) = \sum a_i b_i,$$

we find that

$$n(\alpha_i, \alpha_j) = 2 \frac{(\alpha_i, \alpha_j)}{(\alpha_j, \alpha_j)} = (\alpha_i, \alpha_j) = \begin{cases} 2 & \text{if } j = i \\ -1 & \text{if } j = i \pm 1 \\ 0 & \text{otherwise} \end{cases}$$

and so

$$n(\alpha_i, \alpha_j) \cdot n(\alpha_j, \alpha_i) = \begin{cases} 1 & \text{if } j = i \pm 1 \\ 0 & \text{if } j \neq i, i \pm 1. \end{cases}$$

Thus, the Dynkin diagram of $(\mathfrak{g}, \mathfrak{h})$ is indecomposable of type A_n . Therefore \mathfrak{g} is simple.

EXAMPLE (B_n): \mathfrak{o}_{2n+1}

EXAMPLE (C_n): \mathfrak{sp}_{2n}

EXAMPLE (A_n): \mathfrak{o}_{2n}

See Bourbaki LIE, VIII, §13 (for the present). In fact, the calculations are almost the same as those in V, §2n.

2i Subalgebras of split semisimple Lie algebras

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra with root system $R \subset \mathfrak{h}^\vee$. We wish to determine the subalgebras \mathfrak{a} of \mathfrak{g} normalized by \mathfrak{h} , i.e., such that $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$.

For a subset P of R , we let

$$\mathfrak{g}^P = \sum_{\alpha \in P} \mathfrak{g}^\alpha \text{ and } \mathfrak{h}_P = \sum_{\alpha \in P} \mathfrak{h}_\alpha.$$

DEFINITION 2.29 A subset P of R is said to be *closed*⁶ if

$$\alpha, \beta \in P, \quad \alpha + \beta \in R \implies \alpha + \beta \in P.$$

As $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] \subset \mathfrak{g}^{\alpha+\beta}$ (see 2.21), in order for $\mathfrak{h}_P + \mathfrak{g}^P$ to be a Lie subalgebra of \mathfrak{g} , we should expect to have to require P to be closed.

⁶This is Bourbaki's terminology, LIE VI, §1, 7.

PROPOSITION 2.30 For every closed subset P of R and subspace \mathfrak{h}' of \mathfrak{h} containing $\mathfrak{h}_{P \cap -P}$, the subspace $\mathfrak{a} = \mathfrak{h}' + \mathfrak{g}^P$ of \mathfrak{g} is a Lie subalgebra normalized by \mathfrak{h} , and every Lie subalgebra of \mathfrak{g} normalized by \mathfrak{h} is of this form for some \mathfrak{h}' and P . Moreover,

- (a) \mathfrak{a} is semisimple if and only if $P = -P$ and $\mathfrak{h}' = \mathfrak{h}_P$;
 (b) \mathfrak{a} is solvable if and only if

$$P \cap (-P) = \emptyset. \quad (161)$$

PROOF. See Bourbaki LIE, VIII, §3, 1, Pptn 1, Pptn 2. \square

EXAMPLE 2.31 For any root α , $P = \{\alpha, -\alpha\}$ is a closed subset of R , and $[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] + \mathfrak{g}^P$ is the Lie subalgebra \mathfrak{s}_α of (2.22).

PROPOSITION 2.32 The root system R is indecomposable if and only if \mathfrak{g} is simple.

PROOF. Ibid., VIII, §3, 2, Pptn 6. \square

In more detail, let R_1, \dots, R_m be the indecomposable components of R . Then $\mathfrak{h}_{R_1} + \mathfrak{g}_{R_1}, \dots, \mathfrak{h}_{R_m} + \mathfrak{g}_{R_m}$ are the minimal ideals of \mathfrak{g} .

For base S of R , the set R_+ of positive roots is a maximal closed subset of R satisfying (161), and every maximal such set arises in this way from a base (Bourbaki LIE, VI, §1, 7, Pptn 22). Therefore, the maximal solvable subalgebras of \mathfrak{g} containing \mathfrak{h} are exactly subalgebras of the form

$$\mathfrak{b}(S) \stackrel{\text{def}}{=} \mathfrak{h} \oplus \bigoplus_{\alpha > 0} \mathfrak{g}^\alpha, \quad S \text{ a base of } R.$$

The subalgebra $\mathfrak{b}(S)$ determines R_+ , and hence the base S (as the set of indecomposable elements of R_+).

DEFINITION 2.33 Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra; a **Borel subalgebra** of $(\mathfrak{g}, \mathfrak{h})$ is a maximal solvable subalgebra of \mathfrak{g} containing \mathfrak{h} . Let \mathfrak{g} be a semisimple Lie algebra; a **Borel subalgebra** of \mathfrak{g} is a Lie subalgebra of \mathfrak{g} that is a Borel subalgebra of $(\mathfrak{g}, \mathfrak{h})$ for some splitting Cartan subalgebra \mathfrak{h} of \mathfrak{g} .

EXAMPLE 2.34 Let $\mathfrak{g} = \mathfrak{sl}_{n+1}$ and let \mathfrak{h} be the subalgebra of diagonal matrices. For the base $S = (\alpha_i)_{1 \leq i \leq n}$, $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, as in §2h, the positive roots are those of the form $\varepsilon_i - \varepsilon_j$ with $i < j$, and the Borel subalgebra $\mathfrak{b}(S)$ consists of upper triangular matrices of trace 0. More generally, let $\mathfrak{g} = \mathfrak{sl}(W)$ with W a vector space of dimension $n + 1$. For any maximal flag δ in W , the set \mathfrak{b}_δ of elements of \mathfrak{g} leaving stable all the elements of δ is a Borel subalgebra of \mathfrak{g} , and the map $\delta \mapsto \mathfrak{b}_\delta$ is a bijection from the set of maximal flags onto the set of Borel subgroups of \mathfrak{g} (Bourbaki LIE, VIII, §13).

2j Classification of split semisimple Lie algebras

THEOREM 2.35 Every root system over k arises from a split semisimple Lie algebra over k .

For an indecomposable root system of type $A_n - D_n$ this follows from examining the standard examples (see §2h). In the general case, it is possible to define \mathfrak{g} by generators $(x_\alpha, h_\alpha, y_\alpha)_{\alpha \in S}$ and explicit relations (Bourbaki LIE, VIII, §4, 3, Thm 1).

THEOREM 2.36 *The root system of a split semisimple Lie algebra determines it up to isomorphism.*

In more detail, let $(\mathfrak{g}, \mathfrak{h})$ and $(\mathfrak{g}', \mathfrak{h}')$ be split semisimple Lie algebras, and let S and S' be bases for their corresponding root systems. For each $\alpha \in S$, choose a nonzero $x_\alpha \in \mathfrak{g}^\alpha$, and similarly for \mathfrak{g}' . For any bijection $\alpha \mapsto \alpha': S \rightarrow S'$ such that $\langle \alpha, \beta^\vee \rangle = \langle \alpha', \beta'^\vee \rangle$ for all $\alpha, \beta \in S$, there exists a unique isomorphism $\mathfrak{g} \rightarrow \mathfrak{g}'$ such that $x_\alpha \mapsto x_{\alpha'}$ and $h_\alpha \mapsto h_{\alpha'}$ for all $\alpha \in S$; in particular, \mathfrak{h} maps into \mathfrak{h}' (Bourbaki LIE, VIII, §4, 4, Thm 2).

2k Representations of split semisimple Lie algebras

Throughout this subsection, $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra with root system $R \subset \mathfrak{h}^\vee$, and \mathfrak{b} is the Borel subalgebra of $(\mathfrak{g}, \mathfrak{h})$ attached to a base S for R . According to Weyl's theorem (II, 6.10), \mathfrak{g} -modules, and so to classify them it suffices to classify the simple representations.

Proofs of the next three theorems can be found in Bourbaki LIE, VIII, §7 (and elsewhere).

THEOREM 2.37 *Let V be a simple \mathfrak{g} -module.*

- (a) *There exists a unique one-dimensional subspace L of V stabilized by \mathfrak{b} .*
- (b) *The L in (a) is a weight space for \mathfrak{h} , i.e., $L = V_{\varpi_V}$ for some $\varpi_V \in \mathfrak{h}^\vee$.*
- (c) *The ϖ_V in (b) is dominant, i.e., $\varpi_V \in P_{++}$;*
- (d) *If ϖ is also a weight for \mathfrak{h} in V , then $\varpi = \varpi_V - \sum_{\alpha \in S} m_\alpha \alpha$ with $m_\alpha \in \mathbb{N}$.*

Lie's theorem (II, 3.14) shows that there does exist a one-dimensional eigenspace for \mathfrak{b} — the content of (a) is that when V is a simple \mathfrak{g} -module, the space is unique. Since L is mapped into itself by \mathfrak{b} , it is also mapped into itself by \mathfrak{h} , and so lies in a weight space. The content of (b) is that it is the whole weight space.

Because of (d), ϖ_V is called the **highest weight** of the simple \mathfrak{g} -module V .

THEOREM 2.38 *Every dominant weight occurs as the highest weight of a simple \mathfrak{g} -module.*

THEOREM 2.39 *Two simple \mathfrak{g} -modules are isomorphic if and only if their highest weights are equal.*

Thus $V \mapsto \varpi_V$ defines a bijection from the set of isomorphism classes of simple \mathfrak{g} -modules onto the set of dominant weights P_{++} .

COROLLARY 2.40 *If V is a simple \mathfrak{g} -module, then $\text{End}(V, r) \simeq k$.*

Let $V = V_\varpi$ with ϖ dominant. Every isomorphism $V_\varpi \rightarrow V_\varpi$ maps the highest weight line L into itself, and is determined by its restriction to L because L generates V_ϖ as a \mathfrak{g} -module.

EXAMPLE 2.41 Let $\mathfrak{g} = \mathfrak{sl}(W)$, and choose a basis $(e_i)_{1 \leq i \leq n+1}$ for W as in §2h. Recall that

$$S = \{\alpha_1, \dots, \alpha_n\}, \quad \alpha_i = \varepsilon_i - \varepsilon_{i+1}, \quad \varepsilon_i(\text{diag}(a_1, \dots, a_n)) = a_i$$

is a base for the root system of $(\mathfrak{g}, \mathfrak{h})$; moreover $h_{\alpha_i} = E_{i,i} - E_{i+1,i+1}$. Let

$$\varpi'_i = \varepsilon_1 + \dots + \varepsilon_i.$$

Then

$$\varpi_i(h_{\alpha_j}) = \delta_{ij}, \quad 1 \leq i, j \leq n,$$

and so $\varpi'_i|_{\mathfrak{h}}$ is the fundamental weight corresponding to α_i . This is represented by the element

$$\varpi_i = \varepsilon_1 + \dots + \varepsilon_i - \frac{i}{n+1}(\varepsilon_1 + \dots + \varepsilon_{n+1})$$

of V . Thus the fundamental weights corresponding to the base S are $\varpi_1, \dots, \varpi_n$. We have

$$Q(R) = \{m_1\varepsilon_1 + \dots + m_{n+1}\varepsilon_{n+1} \mid m_i \in \mathbb{Z}, \quad m_1 + \dots + m_{n+1} = 0\}$$

$$P(R) = Q(R) + \mathbb{Z} \cdot \varpi_1$$

$$P(R)/Q(R) \simeq \mathbb{Z}/(n+1)\mathbb{Z}.$$

The action of \mathfrak{g} on W defines an action of \mathfrak{g} on $\bigwedge^r W$. The elements

$$e_{i_1} \wedge \dots \wedge e_{i_r}, \quad i_1 < \dots < i_r,$$

form a basis for $\bigwedge^r W$, and $h \in \mathfrak{h}$ acts by

$$h \cdot (e_{i_1} \wedge \dots \wedge e_{i_r}) = (\varepsilon_{i_1}(h) + \dots + \varepsilon_{i_r}(h))(e_{i_1} \wedge \dots \wedge e_{i_r}).$$

Therefore the weights of \mathfrak{h} in $\bigwedge^r W$ are the elements

$$\varepsilon_{i_1} + \dots + \varepsilon_{i_r}, \quad i_1 < \dots < i_r,$$

and each has multiplicity 1. As the Weyl group acts transitively on the weights, $\bigwedge^r W$ is a simple \mathfrak{g} -module, and its highest weight is ϖ_r .

2.42 The category $\text{Rep}(\mathfrak{g})$ is a semisimple k -linear tensor category to which we can apply (I, 21.20). Statements (2.38, 2.39) allow us to identify the set of isomorphism classes of $\text{Rep}(\mathfrak{g})$ with P_{++} . Let $M(P_{++})$ be the free abelian group with generators the elements of P_{++} and relations

$$\varpi = \varpi_1 + \varpi_2 \text{ if } V_{\varpi} \subset V_{\varpi_1} \otimes V_{\varpi_2}.$$

Then $P_{++} \rightarrow M(P_{++})$ is surjective, and two elements ϖ and ϖ' of P_{++} have the same image in $M(P_{++})$ if and only if there exist $\varpi_1, \dots, \varpi_m \in P_{++}$ such that W_{ϖ} and $W_{\varpi'}$ are subrepresentations of $W_{\varpi_1} \otimes \dots \otimes W_{\varpi_m}$ (I, 21.22). Later we shall prove that this condition is equivalent to $\varpi - \varpi' \in Q$, and so $M(P_{++}) \simeq P/Q$. In other words, $\text{Rep}(\mathfrak{g})$ has a gradation by $P_{++}/Q \cap P_{++} \simeq P/Q$ but not by any larger quotient.

For example, let $\mathfrak{g} = \mathfrak{sl}_2$, so that $Q = \mathbb{Z}\alpha$ and $P = \mathbb{Z}\frac{\alpha}{2}$. For $n \in \mathbb{N}$, let $V(n)$ be a simple representation of \mathfrak{g} with highest weight $\frac{n}{2}\alpha$. From the Clebsch-Gordon formula (Bourbaki LIE, VIII, §9), namely,

$$V(m) \otimes V(n) \approx V(m+n) \oplus V(m+n-2) \oplus \dots \oplus V(m-n), \quad n \leq m,$$

we see that $\text{Rep}(\mathfrak{g})$ has a natural P/Q -gradation (but not a gradation by any larger quotient of P).

ASIDE 2.43 The above theorems are important, but are far from being the whole story. For example, we need an explicit construction of the simple representation with a given highest weight, and we need to know its properties, e.g., its character. Moreover, in order to determine $\text{Rep}(\mathfrak{g})$ as a tensor category, it is necessary to describe how the tensor product of two simple \mathfrak{g} -modules decomposes as a direct sum of \mathfrak{g} -modules.

ASIDE 2.44 Is it possible to prove that the kernel of $P_{++} \rightarrow M(P_{++})$ is $\mathcal{Q} \cap P_{++}$ by using only the formulas for the characters and multiplicities of the tensor products of simple representations (cf. Humphreys 1972, §24, especially Exercise 12)?

3 Structure of semisimple algebraic groups and their representations

In this section, we classify the split semisimple algebraic groups and their representations over a field of characteristic zero. Throughout, the ground field k has characteristic zero.

3a Basic theory

Recall (II, 2.7, 2.13) that the functor $G \rightsquigarrow \text{Lie}(G)$ is exact and faithful on connected algebraic groups. However, it is not full, and infinitely many nonisomorphic connected algebraic groups may have the same Lie algebra (II, 2.14).

For any connected algebraic group G , the map $H \mapsto \text{Lie}(H)$ is a bijection from the set of connected algebraic subgroups of G onto the set of algebraic Lie subalgebras of $\text{Lie}(G)$ (II, 2.11). As commutative subgroups (resp. normal subgroups) correspond to commutative subalgebras (resp. ideals), we see G is semisimple if $\text{Lie}(G)$ is semisimple; the converse statement is also true (II, 5.23).

Let G be a semisimple algebraic group, and let \mathfrak{g} be its Lie algebra. Then

$$\mathfrak{g} = \mathfrak{g}_1 \times \cdots \times \mathfrak{g}_n$$

where $\mathfrak{g}_1, \dots, \mathfrak{g}_n$ are the minimal nonzero ideals in \mathfrak{g} ; each \mathfrak{g}_i is a simple Lie algebra. Correspondingly, there is an isogeny

$$(g_1, \dots, g_n) \mapsto g_1 \cdots g_n: G_1 \times \cdots \times G_n \rightarrow G$$

where G_i is the connected algebraic subgroup of G with Lie algebra \mathfrak{g}_i ; each G_i is almost-simple.

3b Rings of representations of Lie algebras

Let \mathfrak{g} be a Lie algebra over k . A *ring of representations* of \mathfrak{g} is a collection of representations of \mathfrak{g} that is closed under the formation of direct sums, subquotients, tensor products, and duals. An *endomorphism* of such a ring \mathcal{R} is a family

$$\alpha = (\alpha_V)_{V \in \mathcal{R}}, \quad \alpha_V \in \text{End}_{k\text{-linear}}(V),$$

such that

- ◇ $\alpha_{V \otimes W} = \alpha_V \otimes \text{id}_W + \text{id}_V \otimes \alpha_W$ for all $V, W \in \mathcal{R}$,
- ◇ $\alpha_V = 0$ if \mathfrak{g} acts trivially on V , and

◇ for any homomorphism $\beta: V \rightarrow W$ of representations in \mathcal{R} ,

$$\alpha_W \circ \beta = \alpha_V \circ \beta.$$

The set $\mathfrak{g}_{\mathcal{R}}$ of all endomorphisms of \mathcal{R} becomes a Lie algebra over k (possibly infinite dimensional) with the bracket

$$[\alpha, \beta]_V = [\alpha_V, \beta_V].$$

EXAMPLE 3.1 (IWAHORI 1954) Let k be an algebraically closed field, and let \mathfrak{g} be k regarded as a one-dimensional Lie algebra. To give a representation of \mathfrak{g} on a vector space V is the same as to give an endomorphism α of V , and so the category of representations of \mathfrak{g} is equivalent to the category of pairs (k^n, A) , $n \in \mathbb{N}$, with A an $n \times n$ matrix. It follows that to give an endomorphism of the ring \mathcal{R} of all representations of \mathfrak{g} is the same as to give a map $A \mapsto \lambda(A)$ sending a square matrix A to a matrix of the same size and satisfying certain conditions. A pair (g, c) consisting of an additive homomorphism $g: k \rightarrow k$ and an element c of k defines a λ as follows:

- ◇ $\lambda(S) = U \operatorname{diag}(ga_1, \dots, ga_n) U^{-1}$ if λ is the semisimple matrix $U \operatorname{diag}(a_1, \dots, a_n) U^{-1}$;
- ◇ $\lambda(N) = cN$ if N is nilpotent;
- ◇ $\lambda(A) = \lambda(S) + \lambda(N)$ if $A = S + N$ is the decomposition of A into its commuting semisimple and nilpotent parts.

Moreover, every λ arises from a unique pair (g, c) . Note that $\mathfrak{g}_{\mathcal{R}}$ has infinite dimension.

Let \mathcal{R} be a ring of representations of a Lie algebra \mathfrak{g} . For any $x \in \mathfrak{g}$, $(r_V(x))_{V \in \mathcal{R}}$ is an endomorphism of \mathcal{R} , and $x \mapsto (r_V(x))$ is a homomorphism of Lie algebras $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$.

LEMMA 3.2 *If \mathcal{R} contains a faithful representation of \mathfrak{g} , then the homomorphism $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is injective.*

PROOF. For any representation (V, r_V) of \mathfrak{g} , the composite

$$\mathfrak{g} \xrightarrow{x \mapsto (r_V(x))} \mathfrak{g}_{\mathcal{R}} \xrightarrow{\lambda \mapsto \lambda_V} \mathfrak{gl}(V).$$

is r_V . Therefore, $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is injective if r_V is injective. □

PROPOSITION 3.3 *Let G be an affine group over k , and let \mathcal{R} be the ring of representations of $\operatorname{Lie}(G)$ arising from a representation of G . Then $\mathfrak{g}_{\mathcal{R}} \simeq \operatorname{Lie}(G)$; in particular, $\mathfrak{g}_{\mathcal{R}}$ depends only of G° .*

PROOF. By definition, $\operatorname{Lie}(G)$ is the kernel of $G(k[\varepsilon]) \rightarrow G(k)$. Therefore, to give an element of $\operatorname{Lie}(G)$ is the same as to give a family of $k[\varepsilon]$ -linear maps

$$\operatorname{id}_V + \alpha_V \varepsilon: V[\varepsilon] \rightarrow V[\varepsilon]$$

indexed by $V \in \mathcal{R}$ satisfying the three conditions of (I, 10.2). The first of these conditions says that

$$\operatorname{id}_{V \otimes W} + \alpha_{V \otimes W} \varepsilon = (\operatorname{id}_V + \alpha_V \varepsilon) \otimes (\operatorname{id}_W + \alpha_W \varepsilon),$$

i.e., that

$$\alpha_{V \otimes W} = \operatorname{id}_V \otimes \alpha_W + \alpha_V \otimes \operatorname{id}_W.$$

The second condition says that

$$\alpha_{\mathbb{1}} = 0,$$

and the third says that the α_V commute with all G -morphisms (= \mathfrak{g} -morphisms by 2.21). Therefore, to give such a family is the same as to give an element $(\alpha_V)_{V \in \mathcal{R}}$ of $\mathfrak{g}_{\mathcal{R}}$. \square

PROPOSITION 3.4 *Let \mathfrak{g} be a Lie algebra, and let \mathcal{R} be a ring of representations of \mathfrak{g} . The canonical map $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is an isomorphism if and only if \mathfrak{g} is the Lie algebra of an affine group G whose identity component is algebraic and \mathcal{R} is the ring of representations of G arising from a representation of G .*

PROOF. On applying I, 11.14, to the full subcategory of $\text{Rep}(\mathfrak{g})$ whose objects are those in \mathcal{R} and the forgetful functor, we obtain an affine group such that $\text{Lie}(G) \simeq \mathfrak{g}_{\mathcal{R}}$ (by (3.3) and \mathcal{R} is the ring of representation of $\mathfrak{g}_{\mathcal{R}}$ arising from a representation of G). If $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is an isomorphism, then G° is algebraic because its Lie algebra is finite-dimensional. This proves the necessity, and the sufficiency follows immediately from (3.3). \square

COROLLARY 3.5 *Let $\mathfrak{g} \rightarrow \mathfrak{gl}(V)$ be a faithful representation of \mathfrak{g} , and let $\mathcal{R}(V)$ be the ring of representations of \mathfrak{g} generated by V . Then $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism if and only if \mathfrak{g} is algebraic, i.e., the Lie algebra of an algebraic subgroup of GL_V .*

PROOF. Immediate consequence of the proposition. \square

3.6 Let \mathcal{R} be the ring of all representations of \mathfrak{g} . When $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is an isomorphism we says that **Tannaka duality holds for \mathfrak{g}** . It follows from (II, 2.22) that Tannaka duality holds for \mathfrak{g} if $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$. On the other hand, Example 3.1 shows that Tannaka duality fails when $[\mathfrak{g}, \mathfrak{g}] \neq \mathfrak{g}$, and even that $\mathfrak{g}_{\mathcal{R}}$ has infinite dimension in this case.

EXAMPLE 3.7 Let \mathfrak{g} be a one-dimensional Lie algebra over an algebraically closed field k . The affine group attached to $\text{Rep}(\mathfrak{g})$ is $D(M) \times \mathbb{G}_a$ where M is k regarded as an additive abelian group (cf. I, §14c). In other words, $D(M)$ represents the functor $R \rightsquigarrow \text{Hom}(M, R^\times)$ (homomorphisms of abelian groups). This follows from Iwahori's result (3.1). Note that M is not finitely generated as an abelian group, and so $D(M)$ is not an algebraic group.

NOTES Let $\mathfrak{g} \rightarrow \mathfrak{gl}(V)$ be a faithful representation of \mathfrak{g} , and let $\mathcal{R}(V)$ be the ring of representations of \mathfrak{g} generated by V . When is $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}(V)}$ an isomorphism? It follows easily from (II, 2.22) that it is, for example, when $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$. In particular, $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism when \mathfrak{g} is semisimple. For an abelian Lie group \mathfrak{g} , $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism if and only if $\mathfrak{g} \rightarrow \mathfrak{gl}(V)$ is a semisimple representation and there exists a lattice in \mathfrak{g} on which the characters of \mathfrak{g} in V take integer values. For the Lie algebra in (II, 1.40), $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}(V)}$ is *never* an isomorphism.

3c An adjoint to the functor Lie

Let \mathfrak{g} be a Lie algebra, and let \mathcal{R} be the ring of all representations of \mathfrak{g} . We define $G(\mathfrak{g})$ to be the Tannaka dual of the neutral tannakian category $(\text{Rep}(\mathfrak{g}), \text{forget})$. Recall (I, 11.14) that this means that $G(\mathfrak{g})$ is the affine group whose R -points for any k -algebra R are the families

$$\lambda = (\lambda_V)_{V \in \mathcal{R}}, \quad \lambda_V \in \text{End}_{R\text{-linear}}(V(R)),$$

such that

- ◇ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ for all $V \in \mathcal{R}$;
- ◇ if V is the trivial representation of \mathfrak{g} (i.e., $x_V = 0$ for all $x \in \mathfrak{g}$), then $\lambda_V = \text{id}_V$;
- ◇ for every \mathfrak{g} -homomorphism $\beta: V \rightarrow W$,

$$\lambda_W \circ \beta = \beta \circ \lambda_V.$$

For each $V \in \mathcal{R}$, there is a representation r_V of $G(\mathfrak{g})$ on V defined by

$$r_V(\lambda)v = \lambda_V v, \quad \lambda \in G(\mathfrak{g})(R), \quad v \in V(R), \quad R \text{ a } k\text{-algebra},$$

and $V \rightsquigarrow (V, r_V)$ is an equivalence of categories

$$\text{Rep}(\mathfrak{g}) \xrightarrow{\sim} \text{Rep}(G(\mathfrak{g})). \quad (162)$$

LEMMA 3.8 *The homomorphism $\eta: \mathfrak{g} \rightarrow \text{Lie}(G(\mathfrak{g}))$ is injective, and the composite of the functors*

$$\text{Rep}(G(\mathfrak{g})) \xrightarrow{(V, r) \rightsquigarrow (V, \text{Lie}(r))} \text{Rep}(\text{Lie}(G(\mathfrak{g}))) \xrightarrow{\eta^\vee} \text{Rep}(\mathfrak{g}) \quad (163)$$

is an equivalence of categories.

PROOF. According to (3.3), $\text{Lie}(G(\mathfrak{g})) \simeq \mathfrak{g}_{\mathcal{R}}$, and so the first assertion follows from (3.2) and Ado's theorem. The composite of the functors in (163) is a quasi-inverse to the functor in (162). \square

LEMMA 3.9 *The affine group $G(\mathfrak{g})$ is connected.*

PROOF. When \mathfrak{g} is one-dimensional, we computed $G(\mathfrak{g})$ in (3.7) and found it to be connected.

For a general \mathfrak{g} , we have to show that only a trivial representation of \mathfrak{g} has the property that the category of subquotients of direct sums of copies of the representation is stable under tensor products (see I, 13.30). When \mathfrak{g} is semisimple, this follows from (2.37).

Let V be a representation of \mathfrak{g} with the property. It follows from the one-dimensional case that the radical of \mathfrak{g} acts trivially on V , and then it follows from the semisimple case that \mathfrak{g} itself acts trivially. \square

PROPOSITION 3.10 *The pair $(G(\mathfrak{g}), \eta)$ is universal: for any algebraic group H and k -algebra homomorphism $a: \mathfrak{g} \rightarrow \text{Lie}(H)$, there is a unique homomorphism $b: G(\mathfrak{g}) \rightarrow H$ such that $a = \text{Lie}(b) \circ \eta$:*

$$\begin{array}{ccc}
 G(\mathfrak{g}) & & \mathfrak{g} \xrightarrow{\eta} \text{Lie}(G(\mathfrak{g})) \\
 \downarrow \exists! b & \xrightarrow{\text{Lie}} & \downarrow \text{Lie}(b) \\
 H & & \text{Lie}(H)
 \end{array}$$

(Note: In the original image, a wavy arrow labeled 'Lie' points from $G(\mathfrak{g})$ to \mathfrak{g} , and a solid arrow labeled 'a' points from \mathfrak{g} to $\text{Lie}(H)$.)

In other words, the map sending a homomorphism $b: G(\mathfrak{g}) \rightarrow H$ to the homomorphism $\text{Lie}(b) \circ \eta: \mathfrak{g} \rightarrow \text{Lie}(H)$ is a bijection

$$\text{Hom}_{\text{affine groups}}(G(\mathfrak{g}), H) \rightarrow \text{Hom}_{\text{Lie algebras}}(\mathfrak{g}, \text{Lie}(H)). \quad (164)$$

If a is surjective and $\text{Rep}(G(\mathfrak{g}))$ is semisimple, then b is surjective.

PROOF. From a homomorphism $b:G(\mathfrak{g}) \rightarrow H$, we get a commutative diagram

$$\begin{array}{ccc} \text{Rep}(H) & \xrightarrow{b^\vee} & \text{Rep}(G(\mathfrak{g})) \\ \text{fully faithful} \downarrow (2.21) & & \simeq \downarrow (3.8) \quad a \stackrel{\text{def}}{=} \text{Lie}(b) \circ \eta. \\ \text{Rep}(\text{Lie}(H)) & \xrightarrow{a^\vee} & \text{Rep}(\mathfrak{g}) \end{array}$$

If $a = 0$, then a^\vee sends all objects to trivial objects, and so the functor b^\vee does the same, which implies that the image of b is 1. Hence (164) is injective.

From a homomorphism $a:\mathfrak{g} \rightarrow \text{Lie}(H)$, we get a tensor functor

$$\text{Rep}(H) \rightarrow \text{Rep}(\text{Lie}(H)) \xrightarrow{a^\vee} \text{Rep}(\mathfrak{g}) \simeq \text{Rep}(G(\mathfrak{g}))$$

and hence a homomorphism $G(\mathfrak{g}) \rightarrow H$, which acts as a on the Lie algebras. Hence (164) is surjective.

If a is surjective, then a^\vee is fully faithful, and so $\text{Rep}(H) \rightarrow \text{Rep}(G(\mathfrak{g}))$ is fully faithful, which implies that $G(\mathfrak{g}) \rightarrow G$ is surjective by (I, 10.21a). □

PROPOSITION 3.11 *For any finite extension $k' \supset k$ of fields, $G(\mathfrak{g}_{k'}) \simeq G(\mathfrak{g})_{k'}$.*

PROOF. More precisely, we prove that the pair $(G(\mathfrak{g})_{k'}, \eta_{k'})$ obtained from $(G(\mathfrak{g}), \eta)$ by extension of the base field has the universal property characterizing $(G(\mathfrak{g}_{k'}), \eta)$. Let H be an algebraic group over k' , and let H_* be the group over k obtained from H by restriction of the base field. Then

$$\begin{aligned} \text{Hom}_{k'}(\mathcal{G}(\mathfrak{g})_{k'}, H) &\simeq \text{Hom}_k(\mathcal{G}(\mathfrak{g}), H_*) \quad (\text{universal property of } H_*) \\ &\simeq \text{Hom}_k(\mathfrak{g}, \text{Lie}(H_*)) \quad (3.10) \\ &\simeq \text{Hom}_{k'}(\mathfrak{g}_{k'}, \text{Lie}(H)). \end{aligned}$$

For the last isomorphism, note that

$$\text{Lie}(H_*) \stackrel{\text{def}}{=} \text{Ker}(H_*(k[\varepsilon]) \rightarrow H_*(k)) \simeq \text{Ker}(H(k'[\varepsilon]) \rightarrow H(k')) \stackrel{\text{def}}{=} \text{Lie}(H).$$

In other words, $\text{Lie}(H_*)$ is $\text{Lie}(H)$ regarded as a Lie algebra over k (instead of k'), and the isomorphism is simply the canonical isomorphism in linear algebra,

$$\text{Hom}_{k\text{-linear}}(V, W) \simeq \text{Hom}_{k'\text{-linear}}(V \otimes_k k', W)$$

(V, W vector spaces over k and k' respectively). □

The next theorem shows that, when \mathfrak{g} is semisimple, $G(\mathfrak{g})$ is a semisimple algebraic group with Lie algebra \mathfrak{g} , and any other semisimple group with Lie algebra \mathfrak{g} is a quotient of $G(\mathfrak{g})$; moreover, the centre of $G(\mathfrak{g})$ has character group P/Q .

THEOREM 3.12 *Let \mathfrak{g} be a semisimple Lie algebra.*

- (a) *The homomorphism $\eta:\mathfrak{g} \rightarrow \text{Lie}(G(\mathfrak{g}))$ is an isomorphism.*
- (b) *The affine group $G(\mathfrak{g})$ is a semisimple algebraic group.*

- (c) For any algebraic group H and isomorphism $a: \mathfrak{g} \rightarrow \text{Lie}(H)$, there exists a unique isogeny $b: G(\mathfrak{g}) \rightarrow H^\circ$ such that $a = \text{Lie}(b) \circ \eta$:

$$\begin{array}{ccc}
 T(\mathfrak{g}) & & \mathfrak{g} \xrightarrow{\eta} \text{Lie}(T(\mathfrak{g})) \\
 \vdots \exists! b \downarrow & & \searrow a \quad \downarrow \text{Lie}(b) \\
 H & & \text{Lie}(H).
 \end{array}$$

- (d) Let Z be the centre of $G(\mathfrak{g})$; then $X^*(Z) \simeq P/Q$.

PROOF. (a) Because $\text{Rep}(G(\mathfrak{g}))$ is semisimple, $G(\mathfrak{g})$ is reductive (II, 6.14). Therefore $\text{Lie}(G(\mathfrak{g}))$ is reductive, and so $\text{Lie}(G(\mathfrak{g})) = \mathfrak{a} \times \mathfrak{c}$ with \mathfrak{a} semisimple and \mathfrak{c} commutative (II, 5.6; II, 5.16). If \mathfrak{a} or \mathfrak{c} is nonzero, then there exists a nontrivial representation r of $G(\mathfrak{g})$ such that $\text{Lie}(r)$ is trivial on \mathfrak{g} . But this is impossible because η defines an equivalence $\text{Rep}(G(\mathfrak{g})) \rightarrow \text{Rep}(\mathfrak{g})$.

(b) Now $G(\mathfrak{g})$ is semisimple because its Lie algebra is semisimple (see II, 5.23).

(c) Proposition 3.10 shows that there exists a unique homomorphism b such that $a = \text{Lie}(b) \circ \eta$, which is an isogeny because $\text{Lie}(b)$ is an isomorphism (see II, 2.9).

(d) In the next subsection, we show that if \mathfrak{g} is split, then $X^*(Z) \simeq P/Q$ (as abelian groups). As \mathfrak{g} splits over a finite Galois extension, this implies (d). \square

REMARK 3.13 The isomorphism $X^*(Z) \simeq P/Q$ in (d) commutes with the natural actions of $\text{Gal}(k^{\text{al}}/k)$.

3d Split semisimple algebraic groups

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra, and let P and Q be the corresponding weight and root lattices. The action of \mathfrak{h} on a \mathfrak{g} -module V decomposes it into a direct sum $V = \bigoplus_{\omega \in P} V_\omega$ of weight spaces. Let $D(P)$ be the diagonalizable group attached to P (I, §14c). Thus $D(P)$ is a split torus such that $\text{Rep}(D(P))$ has a natural identification with the category of P -graded vector spaces. The functor $(V, r_V) \mapsto (V, (V_\omega)_{\omega \in P})$ is an exact tensor functor $\text{Rep}(\mathfrak{g}) \rightarrow \text{Rep}(D(P))$ compatible with the forgetful functors, and hence defines a homomorphism $D(P) \rightarrow G(\mathfrak{g})$. Let $T(\mathfrak{h})$ be the image of this homomorphism.

THEOREM 3.14 With the above notations:

- (a) The group $T(\mathfrak{h})$ is a split maximal torus in $G(\mathfrak{g})$, and η restricts to an isomorphism $\mathfrak{h} \rightarrow \text{Lie}(T(\mathfrak{h}))$.
- (b) The map $D(P) \rightarrow T(\mathfrak{h})$ is an isomorphism; therefore, $X^*(T(\mathfrak{h})) \simeq P$.
- (c) The centre of $G(\mathfrak{g})$ is contained in $T(\mathfrak{h})$ and equals

$$\bigcap_{\alpha \in R} \text{Ker}(\alpha: T(\mathfrak{h}) \rightarrow \mathbb{G}_m)$$

(and so has character group P/Q).

PROOF. (a) The torus $T(\mathfrak{h})$ is split because it is the quotient of a split torus. Certainly, η restricts to an injective homomorphism $\mathfrak{h} \rightarrow \text{Lie}(T(\mathfrak{h}))$. It must be surjective because

otherwise \mathfrak{h} wouldn't be a Cartan subalgebra of \mathfrak{g} . The torus $T(\mathfrak{h})$ must be maximal because otherwise \mathfrak{h} wouldn't be equal to its normalizer.

(b) Let V be the representation $\bigoplus V_{\varpi}$ of \mathfrak{g} where ϖ runs through a set of fundamental weights. Then $G(\mathfrak{g})$ acts on V , and the map $D(P) \rightarrow \mathrm{GL}(V)$ is injective. Therefore, $D(P) \rightarrow T(\mathfrak{h})$ is injective.

(c) A gradation on $\mathrm{Rep}(\mathfrak{g})$ is defined by a homomorphism $P \rightarrow M(P_{++})$ (see 2.42), and hence by a homomorphism $D(M(P_{++})) \rightarrow T(\mathfrak{h})$. This shows that the centre of $G(\mathfrak{g})$ is contained in $T(\mathfrak{h})$. The kernel of the adjoint map $\mathrm{Ad}: G(\mathfrak{g}) \rightarrow \mathrm{GL}_{\mathfrak{g}}$ is the centre $Z(G(\mathfrak{g}))$ of $G(\mathfrak{g})$ (see 5.29), and so the kernel of $\mathrm{Ad}|T(\mathfrak{h})$ is $Z(G(\mathfrak{g})) \cap T(\mathfrak{h}) = Z(G(\mathfrak{g}))$. But

$$\mathrm{Ker}(\mathrm{Ad}|T(\mathfrak{h})) = \bigcap_{\alpha \in R} \mathrm{Ker}(\alpha),$$

so $Z(G(\mathfrak{g}))$ is as described. □

LEMMA 3.15 *The following conditions on a subtorus T of a semisimple algebraic group G are equivalent;*

- (a) T is a maximal torus in G ;
- (b) $T_{k^{\mathrm{al}}}$ is a maximal torus in $G_{k^{\mathrm{al}}}$;
- (c) $T = C_G(T)^{\circ}$;
- (d) \mathfrak{t} is a Cartan subalgebra of \mathfrak{g} .

PROOF. (c) \Rightarrow (a). Obvious.

(a) \Rightarrow (d). Let T be a torus in G , and let $G \rightarrow \mathrm{GL}_V$ be a faithful representation of G . After we have extended k , V will decompose into a direct sum $\bigoplus_{\chi \in X^*(T)} V_{\chi}$, and $\mathrm{Lie}(T)$ acts (semisimply) on each factor V_{χ} through the character $\mathrm{Lie}(\chi)$. As $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ is faithful, this shows that \mathfrak{t} consists of semisimple elements (2.9). Hence \mathfrak{t} is toral. Any toral subalgebra of \mathfrak{g} containing \mathfrak{t} arises from a subtorus of G , and so \mathfrak{t} is maximal.

(d) \Rightarrow (c). Because \mathfrak{t} is a Cartan subalgebra, $\mathfrak{t} = \mathfrak{c}_{\mathfrak{g}}(\mathfrak{t})$ (see 2.15). As $\mathrm{Lie}(C_G(T)) = \mathfrak{c}_{\mathfrak{g}}(\mathfrak{t})$ (see II, 2.23), we see that T and $C_G(T)$ have the same Lie algebra, and so $T = C_G(T)^{\circ}$ (see 2.11).

(b) \Leftrightarrow (a). This follows from the equivalence of (a) and (d) and the fact that \mathfrak{t} is a Cartan subalgebra of \mathfrak{g} if and only if $\mathfrak{t}_{k^{\mathrm{al}}}$ is a Cartan subalgebra of $\mathfrak{g}_{k^{\mathrm{al}}}$. □

DEFINITION 3.16 A **split semisimple algebraic group** is a pair (G, T) consisting of a semisimple algebraic group G and a split maximal torus T .

More loosely, we say that a semisimple algebraic group is **split** if it contains a split maximal torus.⁷

THEOREM 3.17 *Let T and T' be split maximal tori in a semisimple algebraic group G . Then $T' = gTg^{-1}$ for some $g \in G(k)$.*

⁷Caution: a semisimple algebraic group always contains a maximal split torus, but that torus may not be maximal among all subtori, and hence not a split maximal torus.

PROOF. We may set $G = G(\mathfrak{g})$ with \mathfrak{g} the semisimple Lie algebra $\text{Lie}(G)$. Let x be a nilpotent element of \mathfrak{g} . For any representation (V, r_V) of \mathfrak{g} , $e^{r_V(x)} \in G(\mathfrak{g})(k)$. According to (2.16), there exist nilpotent elements x_1, \dots, x_m in \mathfrak{g} such that

$$e^{\text{ad}(x_1)} \dots e^{\text{ad}(x_m)} \text{Lie}(T) = \text{Lie}(T').$$

Let $g = e^{\text{ad}(x_1)} \dots e^{\text{ad}(x_m)}$; then $gTg^{-1} = T'$ because they have the same Lie algebra. \square

3e Classification

We can now read off the classification theorems for split semisimple algebraic groups from the similar theorems for split semisimple Lie algebras.

Let (G, T) be a split semisimple algebraic group. Because T is diagonalizable, the k -vector space \mathfrak{g} decomposes into eigenspaces under its action:

$$\mathfrak{g} = \bigoplus_{\alpha \in X^*(T)} \mathfrak{g}^\alpha.$$

The roots of (G, T) are the nonzero α such that $\mathfrak{g}^\alpha \neq 0$. Let R be the set of roots of (G, T) .

PROPOSITION 3.18 *The set of roots of (G, T) is a reduced root system R in $V \stackrel{\text{def}}{=} X^*(T) \otimes \mathbb{Q}$; moreover,*

$$Q(R) \subset X^*(T) \subset P(R). \quad (165)$$

PROOF. Let $\mathfrak{g} = \text{Lie } G$ and $\mathfrak{h} = \text{Lie } T$. Then $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra, and, when we identify V with a \mathbb{Q} -subspace of $\mathfrak{h}^\vee \simeq X^*(T) \otimes k$, the roots of (G, T) coincide with the roots of $(\mathfrak{g}, \mathfrak{h})$ and so (165) holds. \square

By a **diagram** (V, R, X) , we mean a reduced root system (V, R) over \mathbb{Q} and a lattice X in V that is contained between $Q(R)$ and $P(R)$.

THEOREM 3.19 (EXISTENCE) *Every diagram arises from a split semisimple algebraic group over k .*

More precisely, we have the following result.

THEOREM 3.20 *Let (V, R, X) be a diagram, and let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra over k with root system $(V \otimes k, R)$ (see 2.35). Let $\text{Rep}(\mathfrak{g})^X$ be the full subcategory of $\text{Rep}(\mathfrak{g})$ whose objects are those whose simple components have highest weight in X . Then $\text{Rep}(\mathfrak{g})^X$ is a tannakian subcategory of $\text{Rep}(\mathfrak{g})$, and there is a natural tensor functor $\text{Rep}(\mathfrak{g})^X \rightarrow \text{Rep}(D(X))$ compatible with the forgetful functors. The Tannaka dual (G, T) of this functor is a split semisimple algebraic group with diagram (V, R, X) .*

In more detail: the pair $(\text{Rep}(\mathfrak{g})^X, \text{forget})$ is a neutral tannakian category, with Tannaka dual G say; the pair $(\text{Rep}(D(X)), \text{forget})$ is a neutral tannakian category, with Tannaka dual $D(X)$; the tensor functor

$$(\text{Rep}(\mathfrak{g})^X, \text{forget}) \rightarrow (\text{Rep}(D(X)), \text{forget})$$

defines an injective homomorphism

$$D(X) \rightarrow G,$$

whose image we denote T . Then (G, T) is split semisimple group with diagram (V, R, X) .

PROOF. When $X = Q$, $(G, T) = (G(\mathfrak{g}), T(\mathfrak{h}))$, and the statement follows from Theorem 3.14. For an arbitrary X , let

$$N = \bigcap_{\chi \in X/Q} \text{Ker}(\chi: Z(G(\mathfrak{g})) \rightarrow \mathbb{G}_m).$$

Then $\text{Rep}(\mathfrak{g})^X$ is the subcategory of $\text{Rep}(\mathfrak{g})$ on which N acts trivially, and so it is a tannakian category with Tannaka dual $G(\mathfrak{g})/N$ (see I, 8.63). Now it is clear that $(G(\mathfrak{g})/N, T(\mathfrak{h})/N)$ is the Tannaka dual of $\text{Rep}(\mathfrak{g})^X \rightarrow \text{Rep}(D(X))$, and that it has diagram (V, R, X) . \square

THEOREM 3.21 (ISOGENY) *Let (G, T) and (G', T') be split semisimple algebraic groups over k , and let (V, R, X) and (V', R', X') be their associated diagrams. Any isomorphism $V \rightarrow V'$ sending R onto R' and X into X' arises from an isogeny $G \rightarrow G'$ mapping T onto T' .*

PROOF. Let $(\mathfrak{g}, \mathfrak{h})$ and $(\mathfrak{g}', \mathfrak{h}')$ be the split semisimple Lie algebras of (G, T) and (G', T') . An isomorphism $V \rightarrow V'$ sending R onto R' and X into X' arises from an isomorphism $(\mathfrak{g}, \mathfrak{h}) \xrightarrow{\beta} (\mathfrak{g}', \mathfrak{h}')$ (see 2.36). Now β defines an exact tensor functor $\text{Rep}(\mathfrak{g}')^{X'} \rightarrow \text{Rep}(\mathfrak{g})^X$, and hence a homomorphism $\alpha: G \rightarrow G'$, which has the required properties. \square

PROPOSITION 3.22 *Let (G, T) be a split semisimple algebraic group. For each root α of (G, T) and choice of a nonzero element of \mathfrak{g}^α , there is a unique homomorphism*

$$\varphi: \text{SL}_2 \rightarrow G$$

such that $\text{Lie}(\varphi)$ is the inclusion $\mathfrak{s}_\alpha \rightarrow \mathfrak{g}$ of (2.22).

PROOF. From the inclusion $\mathfrak{s}_\alpha \rightarrow \mathfrak{g}$ we get a tensor functor $\text{Rep}(\mathfrak{g}) \rightarrow \text{Rep}(\mathfrak{s}_\alpha)$, and hence a tensor functor $\text{Rep}(G) \rightarrow \text{Rep}(\text{SL}_2)$; this arises from a homomorphism $\text{SL}_2 \rightarrow G$. \square

The image U_α of \mathbb{U}_2 under φ is called the **root group** of α . It is uniquely determined by having the following properties: it is isomorphic to \mathbb{G}_a , and for any isomorphism $u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$,

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \quad a \in k, \quad t \in T(k).$$

NOTES To be continued — there is much more to be said. In particular, we need to determine the algebraic subalgebras of \mathfrak{g} , so that we can read off everything about the algebraic subgroups of G in terms of the subalgebras of \mathfrak{g} (and hence in terms of the root system of (G, T)).

4 Real Lie algebras and real algebraic groups

The statement (3.12),

the affine group attached to the category of representations of a semisimple Lie algebra \mathfrak{g} is the simply connected semisimple algebraic group with Lie algebra \mathfrak{g}

holds over any field of characteristic zero, in particular, over \mathbb{R} . Thus, we can read off the whole theory of algebraic groups over \mathbb{R} and their representations (including the theory of Cartan involutions) from the similar theory for Lie algebras.

In this section, I'll develop the theory of real Lie algebras, and then read off the similar theory for algebraic groups.

5 Reductive groups

Explain how everything extends to reductive algebraic groups (or perhaps rewrite the chapter for reductive groups).

5a Filtrations of $\text{Rep}_k(G)$

Let V be a vector space. A homomorphism $\mu: \mathbb{G}_m \rightarrow \text{GL}(V)$ defines a filtration

$$\dots \supset F^p V \supset F^{p+1} V \supset \dots, \quad F^p V = \bigoplus_{i \geq p} V^i,$$

of V , where $V = \bigoplus_i V^i$ is the grading defined by μ .

Let G be an algebraic group over a field k of characteristic zero. A homomorphism $\mu: \mathbb{G}_m \rightarrow G$ defines a filtration F^\bullet on V for each representation (V, r) of G , namely, that corresponding to $r \circ \mu$. These filtrations are compatible with the formation of tensor products and duals, and they are exact in the sense that $V \mapsto \text{Gr}_F^\bullet(V)$ is exact. Conversely, any functor $(V, r) \mapsto (V, F^\bullet)$ from representations of G to filtered vector spaces compatible with tensor products and duals which is exact in this sense arises from a (nonunique) homomorphism $\mu: \mathbb{G}_m \rightarrow G$. We call such a functor a *filtration* F^\bullet of $\text{Rep}_k(G)$, and a homomorphism $\mu: \mathbb{G}_m \rightarrow G$ defining F^\bullet is said to *split* F^\bullet . We write $\text{Filt}(\mu)$ for the filtration defined by μ .

For each p , we define $F^p G$ to be the subgroup of G of elements acting as the identity map on $\bigoplus_i F^i V / F^{i+p} V$ for all representations V of G . Clearly $F^p G$ is unipotent for $p \geq 1$, and $F^0 G$ is the semi-direct product of $F^1 G$ with the centralizer $Z(\mu)$ of any μ splitting F^\bullet .

PROPOSITION 5.1 *Let G be a reductive group over a field k of characteristic zero, and let F^\bullet be a filtration of $\text{Rep}_k(G)$. From the adjoint action of G on \mathfrak{g} , we acquire a filtration of \mathfrak{g} .*

(a) $F^0 G$ is the subgroup of G respecting the filtration on each representation of G ; it is a parabolic subgroup of G with Lie algebra $F^0 \mathfrak{g}$.

(b) $F^1 G$ is the subgroup of $F^0 G$ acting trivially on the graded module $\bigoplus_p F^p V / F^{p+1} V$ associated with each representation of G ; it is the unipotent radical of $F^0 G$, and $\text{Lie}(F^1 G) = F^1 \mathfrak{g}$.

(c) The centralizer $Z(\mu)$ of any μ splitting F^\bullet is a Levi subgroup of $F^0 G$; therefore, $Z(\mu) \simeq F^0 G / F^1 G$, and the composite $\bar{\mu}$ of μ with $F^0 G \rightarrow F^0 G / F^1 G$ is central.

(d) Two cocharacters μ and μ' of G define the same filtration of G if and only if they define the same group $F^0 G$ and $\bar{\mu} = \bar{\mu}'$; μ and μ' are then conjugate under $F^1 G$.

PROOF. Omitted for the present (Saavedra Rivano 1972, especially IV 2.2.5). □

REMARK 5.2 It is sometimes more convenient to work with ascending filtrations. To turn a descending filtration F^\bullet into an ascending filtration W_\bullet , set $W_i = F^{-i}$; if μ splits F^\bullet then $z \mapsto \mu(z)^{-1}$ splits W . With this terminology, we have $W_0 G = W_{-1} G \rtimes Z(\mu)$.

Lie groups

The theory of algebraic groups can be described as that part of the theory of Lie groups that can be developed using only polynomials (not convergent power series), and hence works over any field. Alternatively, it is the elementary part that doesn't require analysis. As we'll see, it does in fact capture an important part of the theory of Lie groups.

Throughout this chapter, $k = \mathbb{R}$ or \mathbb{C} . The identity component of a topological group G is denoted by G^+ . All vector spaces and representations are finite-dimensional. In this chapter, reductive algebraic groups are not required to be connected.

NOTES Only a partial summary of this chapter exists. Eventually it will include an explanation of the exact relation between algebraic groups and Lie groups; an explanation of how to derive the theory of reductive Lie groups and their representations from the corresponding theory for real and complex algebraic groups; and enough of the basic material to provide a complete introduction to the theory of Lie groups. It is intended as introduction to Lie groups for algebraists (not analysts, who prefer to start at the other end).

1	Lie groups	327
2	Lie groups and algebraic groups	328
3	Compact topological groups	331

1 Lie groups

In this section, we define Lie groups, and develop their basic properties.

DEFINITION 1.1 (a) A **real Lie group** is a smooth manifold G together with a group structure such that both the multiplication map $G \times G \rightarrow G$ and the inverse map $G \rightarrow G$ are smooth.

(b) A **complex Lie group** is a complex manifold G together with a group structure such that both the multiplication map $G \times G \rightarrow G$ and the inverse map $G \rightarrow G$ are holomorphic.

Here "smooth" means infinitely differentiable.

A real (resp. complex) Lie group is said to be **linear** if it admits a faithful real (resp. complex) representation. A real (resp. complex) linear Lie group is said to be **reductive** if every real (resp. complex) representation is semisimple.

2 Lie groups and algebraic groups

In this section, we discuss the relation between Lie groups and algebraic groups (especially those that are reductive).

2a The Lie group attached to an algebraic group

THEOREM 2.1 *There is a canonical functor L from the category of real (resp. complex) algebraic groups to real (resp. complex) Lie groups, which respects Lie algebras and takes GL_n to $GL_n(\mathbb{R})$ (resp. $GL_n(\mathbb{C})$) with its natural structure as a Lie group. It is faithful on connected algebraic groups (all algebraic groups in the complex case).*

According to taste, the functor can be constructed in two ways.

- (a) Choose an embedding $G \hookrightarrow GL_n$. Then $G(k)$ is a closed subgroup of $GL_n(\mathbb{C})$, and it is known that every such subgroup has a unique structure of a Lie group (it is real or complex according to whether its tangent space at the neutral element is a real or complex Lie algebra). See Hall 2003, 2.33.
- (b) For $k = \mathbb{R}$ (or \mathbb{C}), there is a canonical functor from the category of nonsingular real (or complex) algebraic varieties to the category of smooth (resp. complex) manifolds (Shafarevich 1994, II, 2.3, and VII, 1), which clearly takes algebraic groups to Lie groups.

To prove that the functor is faithful in the real case, use (II, 2.13). In the complex case, use that $G(\mathbb{C})$ is dense in G (I, §7e).

We often write $G(\mathbb{R})$ or $G(\mathbb{C})$ for $L(G)$, i.e., we regard the group $G(\mathbb{R})$ (resp. $G(\mathbb{C})$) as a real Lie group (resp. complex Lie group) endowed with the structure given by the theorem.

2b Negative results

2.2 *In the real case, the functor is not faithful on nonconnected algebraic groups.*

Let $G = H = \mu_3$. The real Lie group attached to μ_3 is $\mu_3(\mathbb{R}) = \{1\}$, and so $\text{Hom}(L(G), L(H)) = 1$, but $\text{Hom}(\mu_3, \mu_3)$ is cyclic of order 3.

2.3 *The functor is not full.*

For example, $z \mapsto e^z: \mathbb{C} \rightarrow \mathbb{C}^\times$ is a homomorphism of Lie groups not arising from a homomorphism of algebraic groups $\mathbb{G}_a \rightarrow \mathbb{G}_m$.

For another example, consider the quotient map of algebraic groups $SL_3 \rightarrow PSL_3$. It is not an isomorphism of algebraic groups because its kernel is μ_3 , but it does give an isomorphism $SL_3(\mathbb{R}) \rightarrow PSL_3(\mathbb{R})$ of Lie groups. The inverse of this isomorphism is not algebraic.

2.4 *A Lie group can have nonclosed Lie subgroups (for which quotients don't exist).*

This is a problem with definitions, not mathematics. Some authors allow a Lie subgroup of a Lie group G to be any subgroup H endowed with a Lie group structure for which the

inclusion map is a homomorphism of Lie groups. If instead one requires that a Lie subgroup be a submanifold in a strong sense (for example, locally isomorphic to a coordinate inclusion $\mathbb{R}^m \rightarrow \mathbb{R}^n$), these problems don't arise, and the theory of Lie groups quite closely parallels that of algebraic groups.

2.5 Not all Lie groups have a faithful representation.

For example, $\pi_1(\mathrm{SL}_2(\mathbb{R})) \approx \mathbb{Z}$, and its universal covering space \mathcal{G} has a natural structure of a Lie group. Every representation of \mathcal{G} factors through its quotient $\mathrm{SL}_2(\mathbb{R})$. Another (standard) example is the Lie group $\mathbb{R}^1 \times \mathbb{R}^1 \times S^1$ with the group structure

$$(x_1, y_1, u_1) \cdot (x_2, y_2, u_2) = (x_1 + x_2, y_1 + y_2, e^{ix_1 y_2} u_1 u_2).$$

This homomorphism

$$\begin{pmatrix} 1 & x & a \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto (x, y, e^{ia}),$$

realizes this group as a quotient of $\mathbb{U}_3(\mathbb{R})$, but it can not itself be realized as a matrix group (see Hall 2003, C.3).

A related problem is that there is no very obvious way of attaching a complex Lie group to a real Lie group (as there is for algebraic groups).

2.6 Even when a Lie group has a faithful representation, it need not be of the form $L(G)$ for any algebraic group G .

Consider, for example, $\mathrm{GL}_2(\mathbb{R})^+$.

2.7 Let G be an algebraic group over \mathbb{C} . Then the Lie group $G(\mathbb{C})$ may have many more representations than G .

Consider \mathbb{G}_a ; the homomorphisms $z \mapsto e^{cz}: \mathbb{C} \rightarrow \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$ and $z \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}: \mathbb{C} \rightarrow \mathrm{GL}_2(\mathbb{C})$ are representations of the Lie group \mathbb{C} , but only the second is algebraic.

2c Complex groups

A complex Lie group G is **algebraic** if it is the Lie group defined by an algebraic group over \mathbb{C} .

For any complex Lie group G , the category $\mathrm{Rep}_{\mathbb{C}}(G)$ is obviously tannakian.

PROPOSITION 2.8 *All representations of a complex Lie group G are semisimple (i.e., G is reductive) if and only if G contains a compact subgroup K such that $\mathbb{C} \cdot \mathrm{Lie}(K) = \mathrm{Lie}(G)$ and $G = K \cdot G^+$.*

PROOF. Lee 2002, Proposition 4.22. □

For a complex Lie group G , the **representation radical** $N(G)$ is the intersection of the kernels of all simple representations of G . It is the largest closed normal subgroup of G whose action on every representation of G is unipotent. When G is linear, $N(G)$ is the radical of the derived group of G (Lee 2002, 4.39).

THEOREM 2.9 *For a complex linear Lie group G , the following conditions are equivalent:*

- (a) *the tannakian category $\text{Rep}_{\mathbb{C}}(G)$ is algebraic (i.e., admits a tensor generator I, 21.13);*
- (b) *there exists an algebraic group $T(G)$ over \mathbb{C} and a homomorphism $G \rightarrow T(G)(\mathbb{C})$ inducing an equivalence of categories $\text{Rep}_{\mathbb{C}}(T(G)) \rightarrow \text{Rep}_{\mathbb{C}}(G)$.*
- (c) *G is the semidirect product of a reductive subgroup and $N(G)$.*

Moreover, when these conditions hold, the homomorphism $G \rightarrow T(G)(\mathbb{C})$ is an isomorphism.

PROOF. The equivalence of (a) and (b) follows from (I, 21.10) and (I, 21.13). For the remaining statements, see Lee 2002, Theorem 5.20. \square

COROLLARY 2.10 *Let V be a complex vector space, and let G be a complex Lie subgroup of $\text{GL}(V)$. If $\text{Rep}_{\mathbb{C}}(G)$ is algebraic, then G is an algebraic subgroup of GL_V , and every complex analytic representation of G is algebraic.*

PROOF. Lee 2002, 5.22. \square

REMARK 2.11 The theorem shows, in particular, that every reductive Lie group G is algebraic: more precisely, there exists a reductive algebraic group $T(G)$ and an isomorphism $G \rightarrow T(G)(\mathbb{C})$ of Lie groups inducing an isomorphism $\text{Rep}_{\mathbb{C}}(T(G)) \rightarrow \text{Rep}_{\mathbb{C}}(G)$. Note that $T(G)$ is reductive (6.14). Conversely, if G is a reductive algebraic group, then $\text{Rep}_{\mathbb{C}}(G) \simeq \text{Rep}_{\mathbb{C}}(G(\mathbb{C}))$ (see Lee 1999, 2.8); therefore $G(\mathbb{C})$ is a reductive Lie group, and $T(G(\mathbb{C})) \simeq G$. We have shown that the functors T and L are quasi-inverse equivalences between the categories of complex reductive Lie groups and complex reductive algebraic groups.

EXAMPLE 2.12 The Lie group \mathbb{C} is algebraic, but nevertheless the conditions in (2.9) fail for it — see (2.7).

2d Real groups

We say that a real Lie group G is **algebraic** if $G^+ = H(\mathbb{R})^+$ for some algebraic group H (here $^+$ denotes the identity component for the real topology).

THEOREM 2.13 *For every real reductive Lie group G , there exists an algebraic group $T(G)$ and a homomorphism $G \rightarrow T(G)(\mathbb{R})$ inducing an equivalence of categories $\text{Rep}_{\mathbb{R}}(G) \rightarrow \text{Rep}_{\mathbb{R}}(T(G))$. The Lie group $T(G)(\mathbb{R})$ is the largest algebraic quotient of G , and equals G if and only if G admits a faithful representation.*

PROOF. The first statement follows from the fact that $\text{Rep}_{\mathbb{R}}(G)$ is tannakian. For the second statement, we have to show that $T(G)(\mathbb{R}) = G$ if G admits a faithful representation, but this follows from Lee 1999, 3.4, and (2.9). \square

THEOREM 2.14 *For every compact connected real Lie group K , there exists a semisimple algebraic group $T(K)$ and an isomorphism $K \rightarrow T(K)(\mathbb{R})$ which induces an equivalence of categories $\text{Rep}_{\mathbb{R}}(K) \rightarrow \text{Rep}_{\mathbb{R}}(T(K))$. Moreover, for any reductive algebraic group G' over \mathbb{C} ,*

$$\text{Hom}_{\mathbb{C}}(T(K)_{\mathbb{C}}, G') \simeq \text{Hom}_{\mathbb{R}}(K, G'(\mathbb{C}))$$

PROOF. See Chevalley 1957, Chapter 6, §§8–12, and Serre 1993. □

3 Compact topological groups

Let K be a *topological group*. The category $\text{Rep}_{\mathbb{R}}(K)$ of continuous representations of K on finite-dimensional real vector spaces is, in a natural way, a neutral tannakian category over \mathbb{R} with the forgetful functor as fibre functor. There is therefore (I, 21.10) a real affine algebraic group G called the **real algebraic envelope** of K and a continuous homomorphism $K \rightarrow G(\mathbb{R})$ inducing an equivalence of tensor categories $\text{Rep}_{\mathbb{R}}(K) \rightarrow \text{Rep}_{\mathbb{R}}(G)$. The **complex algebraic envelope** of K is defined similarly.

LEMMA 3.1 *Let K be a compact group, and let G be the real envelope of K . Each $f \in \mathcal{O}(G)$ defines a real-valued function on K , and in this way A becomes identified with the set of all real-valued functions f on K such that*

- (a) *the left translates of f form a finite-dimensional vector space;*
- (b) *f is continuous.*

PROOF. Serre 1993, 4.3, Ex. b), p. 67. □

Similarly, if G' is the complex envelope of K , then the elements of $\mathcal{O}(G')$ can be identified with the continuous complex valued functions on K whose left translates form a finite-dimensional vector space.

PROPOSITION 3.2 *If G and G' are the real and complex envelopes of a compact group K , then $G' = G_{\mathbb{C}}$.*

PROOF. Let A and A' be the bialgebras of G and G' . Then it is clear from Lemma 3.1 that $A' = \mathbb{C} \otimes_{\mathbb{R}} A$. □

DEFINITION 3.3 An affine algebraic group G over \mathbb{R} is said to be **anisotropic** (or **compact**) if it satisfies the following conditions:

- (a) $G(\mathbb{R})$ is compact, and
- (b) $G(\mathbb{R})$ is dense in G for the Zariski topology.

As $G(\mathbb{R})$ contains a neighbourhood of 1 in G , condition (b) is equivalent to the following:

- (b'). Every connected component (for the Zariski topology) of G contains a real point.

In particular, (b) holds if G is connected.

PROPOSITION 3.4 *Let G be an algebraic group over \mathbb{R} , and let K be a compact subgroup of $G(\mathbb{R})$ that is dense in G for the Zariski topology. Then G is anisotropic, $K = G(\mathbb{R})$, and G is the algebraic envelope of K .*

PROOF. Serre 1993, 5.3, Pptn 5, p. 71. □

If K is a compact Lie group, then $\text{Rep}_{\mathbb{R}}(K)$ is semisimple, and so its real algebraic envelope G is reductive. Hence $G_{\mathbb{C}}$ is a complex reductive group. Conversely:

THEOREM 3.5 *Let G be a reductive algebraic group over \mathbb{C} , and let K be a maximal compact subgroup of $G(\mathbb{C})$. Then the complex algebraic envelope of K is G , and so the real algebraic envelope of K is a compact real form of G .*

PROOF. Serre 1993, 5.3, Thm 4, p. 74. □

COROLLARY 3.6 *There is a one-to-one correspondence between the maximal compact subgroups of $G(\mathbb{C})$ and the anisotropic real forms of G .*

PROOF. Obvious from the theorem (see Serre 1993, 5.3, Rem., p. 75). □

THEOREM 3.7 *Let K be a compact Lie group, and let G be its real algebraic envelope. The map*

$$H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), K) \rightarrow H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), G(\mathbb{C}))$$

defined by the inclusion $K \hookrightarrow G(\mathbb{C})$ is an isomorphism.

PROOF. Serre 1964, III, Thm 6. □

Since $\text{Gal}(\mathbb{C}/\mathbb{R})$ acts trivially on K , $H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), K)$ is the set of conjugacy classes in K consisting of elements of order 2.

ASIDE 3.8 A subgroup of an anisotropic group is anisotropic. Maximal compact subgroups of complex algebraic groups are conjugate.

The Structure of Reductive Groups: the split case

This chapter gives an exposition of the theory of split reductive groups and their representations over arbitrary fields (potentially, over \mathbb{Z}), including a proof of the classification (isomorphism, existence, and isogeny theorems) along the lines of Steinberg 1998, 1999. It assumes a knowledge of elementary algebraic geometry (varieties over algebraically closed fields, as in my notes AG), and the basic theory of algebraic groups (Chapter I and II, of these notes). Except for §1 of Chapter III (Root systems and their classification), it is largely independent of Chapters III and IV.

Throughout this section, k is a field (not necessarily of characteristic zero, or even perfect). Also, “semisimple group” and “reductive group” mean “semisimple affine algebraic group” and “reductive affine algebraic group”.

NOTES At present, only the first 4 sections are more-or-less complete (but need even they need revision).

1	Split reductive groups: the program	333
2	The root datum of a split reductive group	338
3	Borel fixed point theorem and applications	351
4	Parabolic subgroups and roots	363
5	Root data and their classification	366
6	Construction of split reductive groups: the existence theorem	374
7	Construction of isogenies of split reductive groups: the isogeny theorem . . .	377
8	Representations of split reductive groups	378

1 Split reductive groups: the program

1a Brief review of reductive groups

1.1 The unipotent radical $R_u G$ of smooth algebraic group G is the largest smooth connected normal unipotent subgroup of G . The geometric unipotent radical of G is the unipotent radical of $G_{k^{\text{al}}}$. (I, 17.2.)

1.2 A reductive group is a smooth connected algebraic group whose geometric unipotent radical is trivial. If G is reductive, then $R_u G = 0$, and the converse is true when k is perfect¹. (I, 17.5, 17.6.)

1.3 Let G be a smooth connected algebraic group. If G is reductive, then every smooth connected normal commutative subgroup is a torus; the converse is true if k is perfect. (I, 17.7.)

1.4 If G is reductive, then the derived group G^{der} of G is semisimple, the connected centre $Z(G)^\circ$ of G is a torus equal to the radical RG of G , and $Z(G) \cap G^{\text{der}}$ is the (finite) centre of G^{der} ; moreover,

$$Z(G)^\circ \cdot G^{\text{der}} = G$$

(I, 17.20).

1.5 Let G' be a semisimple group, let Z be a torus, and let $\varphi: Z(G') \rightarrow Z$ be a homomorphism; the algebraic group G defined by the exact sequence

$$1 \rightarrow Z(G') \xrightarrow{z \mapsto (\varphi(z)^{-1}, z)} Z \times G' \rightarrow G \rightarrow 1 \quad (166)$$

is reductive, and every reductive group arises in this fashion (take Z to be the connected centre of G). (I, 17.21.)

1.6 Let G be an algebraic group over a field of characteristic zero. All representations of G are semisimple if and only if G° is reductive. (II, 6.17.)

1b Split tori

Recall that a split torus is a connected diagonalizable group. Equivalently, it is an algebraic group isomorphic to a product of copies of \mathbb{G}_m (I, 14.16). A torus over k is a connected algebraic group that becomes diagonalizable over k^{al} . A torus in GL_V is split if and only if it is contained in \mathbb{D}_n for some basis of V .

Consider for example

$$T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 \neq 0 \right\}.$$

The characteristic polynomial of such a matrix is

$$X^2 - 2aX + a^2 + b^2 = (X - a)^2 + b^2$$

and so its eigenvalues are

$$\lambda = a \pm b\sqrt{-1}.$$

It is easy to see that T is split (i.e., diagonalizable over k) if and only if -1 is a square in k .

¹But not when k is nonperfect, otherwise Conrad, Gabber, and Prasad wouldn't have had to write their book.

Recall (I, §14) that $\text{End}(\mathbb{G}_m) \simeq \mathbb{Z}$: the only group-like elements in $k[\mathbb{G}_m] = k[X, X^{-1}]$ are the powers of X , and the only homomorphisms $\mathbb{G}_m \rightarrow \mathbb{G}_m$ are the maps $t \mapsto t^n$ for $n \in \mathbb{Z}$. For a split torus T , we set

$$\begin{aligned} X^*(T) &= \text{Hom}(T, \mathbb{G}_m) = \text{group of characters of } T, \\ X_*(T) &= \text{Hom}(\mathbb{G}_m, T) = \text{group of cocharacters of } T. \end{aligned}$$

There is a pairing

$$\langle \cdot, \cdot \rangle: X^*(T) \times X_*(T) \rightarrow \text{End}(\mathbb{G}_m) \simeq \mathbb{Z}, \quad \langle \chi, \lambda \rangle = \chi \circ \lambda. \quad (167)$$

Thus

$$\chi(\lambda(t)) = t^{\langle \chi, \lambda \rangle} \quad \text{for } t \in \mathbb{G}_m(R) = R^\times.$$

Both $X^*(T)$ and $X_*(T)$ are free abelian groups of rank equal to the dimension of T , and the pairing $\langle \cdot, \cdot \rangle$ realizes each as the dual of the other.

For example, let

$$T = \mathbb{D}_n = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \right\}.$$

Then $X^*(T)$ has basis χ_1, \dots, χ_n , where

$$\chi_i(\text{diag}(a_1, \dots, a_n)) = a_i,$$

and $X_*(T)$ has basis $\lambda_1, \dots, \lambda_n$, where

$$\lambda_i(t) = \text{diag}(1, \dots, t, \dots, 1).$$

Note that

$$\langle \chi_j, \lambda_i \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases},$$

i.e.,

$$\chi_j(\lambda_i(t)) = \begin{cases} t = t^1 & \text{if } i = j \\ 1 = t^0 & \text{if } i \neq j \end{cases}.$$

Some confusion is caused by the fact that we write $X^*(T)$ and $X_*(T)$ as additive groups. For example, if $a = \text{diag}(a_1, a_2, a_3)$, then

$$(5\chi_2 + 7\chi_3)a = \chi_2(a)^5 \chi_3(a)^7 = a_2^5 a_3^7.$$

For this reason, some authors use an exponential notation $\chi(a) = a^\chi$. With this notation, the preceding equation becomes

$$a^{5\chi_2 + 7\chi_3} = a^{5\chi_2} a^{7\chi_3} = a_2^5 a_3^7.$$

1c Split reductive groups

Let G be an algebraic group over a field k . When $k = k^{\text{al}}$, a torus $T \subset G$ is *maximal* if it is not properly contained in any other torus. In general, $T \subset G$ is said to be *maximal* if $T_{k^{\text{sep}}}$ is maximal in $G_{k^{\text{sep}}}$. If a torus T in G is its own centralizer, then this remains true over k^{sep} (I, 7.44 et seq.), and so T is maximal. For example, \mathbb{D}_n is a maximal torus in GL_n because it is equal to own centralizer. A reductive group is *split* if it contains a split maximal torus.

A reductive group over a separably closed field is automatically split, as all tori over such field are split (by definition I, 14.24). As we discuss below, for any reductive group G over a separably closed field k and subfield k_0 of k , there exists a split reductive group G_0 over k_0 , unique up to isomorphism, that becomes isomorphic to G over k .

EXAMPLE 1.7 The group GL_n is a split reductive group (over any field) with split maximal torus \mathbb{D}_n . On the other hand, let \mathbb{H} be the quaternion algebra over \mathbb{R} . As an \mathbb{R} -vector space, \mathbb{H} has basis $1, i, j, ij$, and the multiplication is determined by

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji.$$

It is a division algebra with centre \mathbb{R} . There is an algebraic group G over \mathbb{R} such that

$$G(R) = (R \otimes_{\mathbb{R}} \mathbb{H})^{\times}$$

for all \mathbb{R} -algebras R (I, 2.19). In particular, $G(\mathbb{R}) = \mathbb{H}^{\times}$. As $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \approx M_2(\mathbb{C})$, G becomes isomorphic to GL_2 over \mathbb{C} , but as an algebraic group over \mathbb{R} it is not split, because its derived group G' is the subgroup of elements of norm 1, and as $G'(\mathbb{R})$ is compact, it can't contain a split torus.

EXAMPLE 1.8 The group SL_n is a split semisimple group, with split maximal torus the diagonal matrices of determinant 1.

EXAMPLE 1.9 Let (V, q) be a nondegenerate quadratic space (see I, §18b). Recall that this means that V is a finite-dimensional vector space and q is a nondegenerate quadratic form on V with associated symmetric form ϕ . Recall (I, 18.7) that the Witt index of (V, q) is the maximum dimension of an isotropic subspace of V . If the Witt index is r , then V is an orthogonal sum

$$V = H_1 \perp \dots \perp H_r \perp V_1 \quad (\text{Witt decomposition})$$

where each H_i is a hyperbolic plane and V_1 is anisotropic (I, 18.9). The associated algebraic group $\text{SO}(q)$ is split if and only if its Witt index is as large as possible.

(a) Case $\dim V = n$ is even, say, $n = 2r$. When the Witt index is as large as possible there is a basis for which the matrix² of the form is $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$, and so

$$q(x_1, \dots, x_n) = x_1 x_{r+1} + \dots + x_r x_{2r}.$$

²Recall that $\text{SO}(q)$ consists of the automorphs of this matrix with determinant 1, i.e., $\text{SO}(q)(R)$ consists of the $n \times n$ matrices A with entries in R and determinant 1 such that $A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

Note that the subspace of vectors

$$(*, \dots, *, 0, \dots, 0)$$

is totally isotropic. The algebraic subgroup consisting of the diagonal matrices of the form

$$\text{diag}(a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in $\text{SO}(q)$.

(b) Case $\dim V = n$ is odd, say, $n = 2r + 1$. When the Witt index is as large as possible

there is a basis for which the matrix of the form is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix}$, and so

$$q(x_0, x_1, \dots, x_n) = x_0^2 + x_1 x_{r+1} + \dots + x_r x_{2r}.$$

The algebraic subgroup consisting of the diagonal matrices of the form

$$\text{diag}(1, a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in $\text{SO}(q)$.

Notice that any two nondegenerate quadratic spaces with largest Witt index and the same dimension are isomorphic. In the rest of the notes, I'll refer to these groups as the split SO_n 's.

EXAMPLE 1.10 Let $V = k^{2n}$, and let ψ be the skew-symmetric form with matrix $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, so

$$\psi(\vec{x}, \vec{y}) = x_1 y_{n+1} + \dots + x_n y_{2n} - x_{n+1} y_1 - \dots - x_{2n} y_n.$$

The corresponding symplectic group Sp_n is split, and the algebraic subgroup consisting of the diagonal matrices of the form

$$\text{diag}(a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in Sp_n .

1d The program

1.11 A reductive group G over k is split if it contains a split maximal torus³ T , i.e., a split torus $T \subset G$ such $T_{k^{\text{sep}}}$ is maximal in $G_{k^{\text{sep}}}$. A **split reductive group** is a pair (G, T) consisting of a reductive group G and a split maximal torus T .

1.12 Any two split maximal tori in G are conjugate by an element of $G(k)$ (see 3.22); in particular, the isomorphism class of (G, T) depends only on G .

1.13 To each split reductive group (G, T) we attach a more elementary object, namely, its root datum $\Psi(G, T)$ (see §2). The root datum $\Psi(G, T)$ determines (G, T) up to isomorphism, and every root datum arises from a pair (G, T) .

³Not to be confused with a maximal split torus in G , which is a torus that is maximal among the split tori in G . A split maximal torus is a maximal split torus, but the converse need not be true.

1.14 We study, and classify, the root data.

1.15 Since knowing the root datum of (G, T) is equivalent to knowing (G, T) , we should be able to read off information about the structure of G and its representations from the root datum. This is true.

1.16 The root data have nothing to do with the field! In particular, we see that for each reductive group G over k^{al} , there is (up to isomorphism) exactly one split reductive group over k that becomes isomorphic to G over k^{al} . However, there will in general be many nonsplit groups, and so we are left with the problem of understanding them (Chapter VI).

In linear algebra and the theory of algebraic groups, one often needs the ground field to be algebraically closed in order to have enough eigenvalues (and eigenvectors). By requiring that the group contains a split maximal torus, we ensure that there are enough eigenvalues without having to make an assumption on the ground field.

2 The root datum of a split reductive group

2a Roots

Let (G, T) be a split reductive group. Then G acts on $\mathfrak{g} = \text{Lie}(G)$ via the adjoint representation

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$$

(II, §1g). In particular, T acts on \mathfrak{g} , and so it decomposes as

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\chi} \mathfrak{g}_{\chi}$$

where \mathfrak{g}_0 is the subspace on which T acts trivially, and \mathfrak{g}_{χ} is the subspace on which T acts through the nontrivial character χ (I, 14.15). The nonzero χ occurring in this decomposition are called the *roots* of (G, T) . They form a finite subset R of $X^*(T)$.

NOTES There is probably some inconsistency in my notations for root data: $R(G, T)$, $\Phi(G, T)$, and $\Psi(G, T)$ all seem to be used. Conrad et al. 2010 write $R = \Phi(G, T)$ in 3.2.2, p. 94, and $R(G, T) = (X(T), \Phi(G, T), X_*(T), \Phi(G, T)^{\vee})$ in 3.2.5, p. 96.

2b Example: GL_2

Here

$$\mathfrak{g} = \mathfrak{gl}_2 = M_2(k) \text{ with } [A, B] = AB - BA,$$

and

$$T = \left\{ \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \mid x_1 x_2 \neq 0 \right\}.$$

Therefore,

$$X^*(T) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2, \text{ where } \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \xrightarrow{a\chi_1 + b\chi_2} x_1^a x_2^b.$$

The torus T acts on \mathfrak{g} by conjugation,

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1^{-1} & 0 \\ 0 & x_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{x_1}{x_2}b \\ \frac{x_2}{x_1}c & d \end{pmatrix}.$$

Write E_{ij} for the matrix with a 1 in the ij th-position, and zeros elsewhere. Then T acts trivially on $\mathfrak{g}_0 = \langle E_{11}, E_{22} \rangle$, through the character $\alpha = \chi_1 - \chi_2$ on $\mathfrak{g}_\alpha = \langle E_{12} \rangle$, and through the character $-\alpha = \chi_2 - \chi_1$ on $\mathfrak{g}_{-\alpha} = \langle E_{21} \rangle$.

Thus, $R = \{\alpha, -\alpha\}$ where $\alpha = \chi_1 - \chi_2$. When we use χ_1 and χ_2 to identify $X^*(T)$ with $\mathbb{Z} \oplus \mathbb{Z}$, R becomes identified with $\{\pm(e_1 - e_2)\}$.

2c Example: SL_2

Here

$$\mathfrak{g} = \mathfrak{sl}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \mid a + d = 0 \right\},$$

and

$$T = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \right\}.$$

Therefore,

$$X^*(T) = \mathbb{Z}\chi \text{ where } \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mapsto x.$$

Again T acts on \mathfrak{g} by conjugation,

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} a & x^2b \\ x^{-2}c & -a \end{pmatrix}$$

Therefore, the roots are $\alpha = 2\chi$ and $-\alpha = -2\chi$. When we use χ to identify $X^*(T)$ with \mathbb{Z} , R becomes identified with $\{2, -2\}$.

2d Example: PGL_2

Recall that this is the quotient of GL_2 by its centre: $PGL_2 = GL_2 / \mathbb{G}_m$. For all fields $R \supset k$, $PGL_2(R) = GL_2(R) / R^\times$. In this case,

$$\mathfrak{g} = \mathfrak{pgl}_2 = \mathfrak{gl}_2 / \{\text{scalar matrices}\},$$

and

$$T = \left\{ \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \mid x_1 x_2 \neq 0 \right\} / \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \mid x \neq 0 \right\}.$$

Therefore,

$$X^*(T) = \mathbb{Z}\chi \text{ where } \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \mapsto \frac{x_1}{x_2},$$

and T acts on \mathfrak{g} by conjugation:

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1^{-1} & 0 \\ 0 & x_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{x_1}{x_2}b \\ \frac{x_2}{x_1}c & d \end{pmatrix}.$$

Therefore, the roots are $\alpha = \chi$ and $-\alpha = -\chi$. When we use χ to identify $X^*(T)$ with \mathbb{Z} , R becomes identified with $\{1, -1\}$.

2e Example: GL_n

Here

$$\mathfrak{g} = \mathfrak{gl}_n = M_n(k) \text{ with } [A, B] = AB - BA,$$

and

$$T = \left\{ \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \mid x_1 \cdots x_n \neq 0 \right\}.$$

Therefore,

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \mapsto x_i.$$

The torus T acts on \mathfrak{g} by conjugation:

$$\begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1^{-1} & & 0 \\ & \ddots & \\ 0 & & x_n^{-1} \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & \frac{x_1}{x_n} a_{1n} \\ \vdots & \frac{x_i}{x_j} a_{ij} & \vdots \\ \vdots & \vdots & \vdots \\ \frac{x_n}{x_1} a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Write E_{ij} for the matrix with a 1 in the ij th-position, and zeros elsewhere. Then T acts trivially on $\mathfrak{g}_0 = \langle E_{11}, \dots, E_{nn} \rangle$ and through the character $\alpha_{ij} = \chi_i - \chi_j$ on $\mathfrak{g}_{\alpha_{ij}} = \langle E_{ij} \rangle$. Therefore

$$R = \{\alpha_{ij} \mid 1 \leq i, j \leq n, \quad i \neq j\}.$$

When we use the χ_i to identify $X^*(T)$ with \mathbb{Z}^n , then R becomes identified with

$$\{e_i - e_j \mid 1 \leq i, j \leq n, \quad i \neq j\}$$

where e_1, \dots, e_n is the standard basis for \mathbb{Z}^n .

2f Definition of a root datum

DEFINITION 2.1 A *root datum* is a quadruple $\Psi = (X, R, X^\vee, R^\vee)$ where⁴

- ◇ X, X^\vee are free \mathbb{Z} -modules of finite rank in duality by a pairing $\langle \cdot, \cdot \rangle: X \times X^\vee \rightarrow \mathbb{Z}$,
- ◇ R, R^\vee are finite subsets of X and X^\vee in bijection by a map $\alpha \leftrightarrow \alpha^\vee$,

satisfying the following conditions

(rd1) $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in R$;

(rd2) $s_\alpha(R) \subset R$ for all $\alpha \in R$, where s_α is the homomorphism $X \rightarrow X$ defined by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad x \in X, \alpha \in R,$$

(rd3) the group of automorphisms $W(\Psi)$ of X generated by the s_α for $\alpha \in R$ is finite.

⁴More accurately, it is an ordered sextuple,

$$(X, X^\vee, \langle \cdot, \cdot \rangle, \Phi, \Phi^\vee, \Phi \rightarrow \Phi^\vee),$$

but everyone says quadruple.

Note that (rd1) implies that

$$s_\alpha(\alpha) = -\alpha,$$

and that the converse holds if $\alpha \neq 0$. Moreover, because $s_\alpha(\alpha) = -\alpha$,

$$s_\alpha(s_\alpha(x)) = s_\alpha(x - \langle x, \alpha^\vee \rangle \alpha) = (x - \langle x, \alpha^\vee \rangle \alpha) - \langle x, \alpha^\vee \rangle s_\alpha(\alpha) = x,$$

i.e.,

$$s_\alpha^2 = 1.$$

Clearly, also $s_\alpha(x) = x$ if $\langle x, \alpha^\vee \rangle = 0$. Thus, s_α should be considered an “abstract reflection in the hyperplane orthogonal to α^\vee ”.

The elements of R and R^\vee are called the **roots** and **coroots** of the root datum (and α^\vee is the **coroot** of α). The group $W = W(\Psi)$ of automorphisms of X generated by the s_α for $\alpha \in R$ is called the **Weyl group** of the root datum.

We want to attach to each pair (G, T) consisting of a split reductive group G and split maximal torus T , a root datum $\Psi(G, T)$ with

$$\begin{aligned} X &= X^*(T), \\ R &= \text{roots}, \\ X^\vee &= X_*(T) \text{ with the pairing } X^*(T) \times X_*(T) \rightarrow \mathbb{Z} \text{ in (167), p. 335} \\ R^\vee &= \text{coroots (to be defined)}. \end{aligned}$$

2g First examples of root data

EXAMPLE 2.2 Let $G = \text{SL}_2$. Here

$$\begin{aligned} X &= X^*(T) = \mathbb{Z}\chi, & \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} &\xrightarrow{X} x \\ X^\vee &= X_*(T) = \mathbb{Z}\lambda, & t &\xrightarrow{\lambda} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \\ R &= \{\alpha, -\alpha\}, & \alpha &= 2\chi \\ R^\vee &= \{\alpha^\vee, -\alpha^\vee\}, & \alpha^\vee &= \lambda. \end{aligned}$$

Note that

$$t \xrightarrow{\lambda} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \xrightarrow{2\chi} t^2$$

and so

$$\langle \alpha, \alpha^\vee \rangle = 2;$$

in fact, we had only one choice for α^\vee . As always,

$$s_\alpha(\alpha) = -\alpha, \quad s_\alpha(-\alpha) = \alpha$$

etc., and so $s_{\pm\alpha}(R) \subset R$. Finally, s_α has order 2, and so $W(\Psi) = \{1, s_\alpha\}$ is finite. Hence $\Psi(\text{SL}_2, T)$ is a root system, isomorphic to

$$(\mathbb{Z}, \{2, -2\}, \mathbb{Z}, \{1, -1\})$$

with the canonical pairing $\langle x, y \rangle = xy$ and the bijection $2 \leftrightarrow 1, -2 \leftrightarrow -1$.

EXAMPLE 2.3 Let $G = \mathrm{PGL}_2$. Here

$$R^\vee = \{\alpha^\vee, -\alpha^\vee\}, \quad \alpha^\vee = 2\lambda.$$

In this case $\Psi(\mathrm{PGL}_2, T)$ is a root system, isomorphic to

$$(\mathbb{Z}, \{1, -1\}, \mathbb{Z}, \{2, -2\}).$$

REMARK 2.4 If α is a root, then so also is $-\alpha$, and there exists an α^\vee such that $\langle \alpha, \alpha^\vee \rangle = 2$. It follows immediately, that the above are the only two root data with $X = \mathbb{Z}$ and R nonempty. There is also the root datum

$$(\mathbb{Z}, \emptyset, \mathbb{Z}, \emptyset),$$

which is the root datum of the reductive group \mathbb{G}_m .

EXAMPLE 2.5 Let $G = \mathrm{GL}_n$. Here

$$\begin{aligned} X &= X^*(\mathbb{D}_n) = \bigoplus_i \mathbb{Z}\chi_i, & \mathrm{diag}(x_1, \dots, x_n) &\xrightarrow{\chi_i} x_i \\ X^\vee &= X_*(\mathbb{D}_n) = \bigoplus_i \mathbb{Z}\lambda_i, & t &\xrightarrow{\lambda_i} \mathrm{diag}(1, \dots, 1, t, 1, \dots, 1) \\ R &= \{\alpha_{ij} \mid i \neq j\}, & \alpha_{ij} &= \chi_i - \chi_j \\ R^\vee &= \{\alpha_{ij}^\vee \mid i \neq j\}, & \alpha_{ij}^\vee &= \lambda_i - \lambda_j. \end{aligned}$$

Note that

$$t \xrightarrow{\lambda_i - \lambda_j} \mathrm{diag}(1, \dots, t^i, \dots, t^{-j}, \dots) \xrightarrow{\chi_i - \chi_j} t^2$$

and so

$$\langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = 2.$$

Moreover, $s_\alpha(R) \subset R$ for all $\alpha \in R$. We have, for example,

$$\begin{aligned} s_{\alpha_{ij}}(\alpha_{ij}) &= -\alpha_{ij} \\ s_{\alpha_{ij}}(\alpha_{ik}) &= \alpha_{ik} - \langle \alpha_{ik}, \alpha_{ij}^\vee \rangle \alpha_{ij} \\ &= \alpha_{ik} - \langle \chi_i, \lambda_i \rangle \alpha_{ij} \quad (\text{if } k \neq i, j) \\ &= \chi_i - \chi_k - (\chi_i - \chi_j) \\ &= \alpha_{jk} \\ s_{\alpha_{ij}}(\alpha_{kl}) &= \alpha_{kl} \quad (\text{if } k \neq i, j, l \neq i, j). \end{aligned}$$

Finally, let $E(ij)$ be the permutation matrix in which the i th and j th rows have been swapped. The action

$$A \mapsto E(ij) \cdot A \cdot E(ij)^{-1}$$

of E_{ij} on GL_n by inner automorphisms stabilizes T and swaps x_i and x_j . Therefore, it acts on $X = X^*(T)$ as $s_{\alpha_{ij}}$. This shows that the group generated by the $s_{\alpha_{ij}}$ is isomorphic to the subgroup of GL_n generated by the $E(ij)$, which is isomorphic to S_n . In particular, W is finite.

Therefore, $\Psi(\mathrm{GL}_n, \mathbb{D}_n)$ is a root datum, isomorphic to

$$(\mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}, \mathbb{Z}^n, \{e_i - e_j \mid i \neq j\})$$

equipped with the pairing $\langle e_i, e_j \rangle = \delta_{ij}$ and the bijection $(e_i - e_j)^\vee = e_i - e_j$. Here, as usual, e_1, \dots, e_n is the standard basis for \mathbb{Z}^n .

In the above examples we wrote down the coroots without giving any idea of how to find (or even define) them. Before defining them, we need to state some general results on reductive groups.

2h Semisimple groups of rank 0 or 1

The *rank* of a reductive group is the dimension of a maximal torus, i.e., it is the largest r such that $G_{k^{\text{al}}}$ contains a subgroup isomorphic to \mathbb{G}_m^r . Since all maximal tori in $G_{k^{\text{al}}}$ are conjugate (see 3.22 below), the rank is well-defined.

THEOREM 2.6 (a) *Every semisimple group of rank 0 is trivial.*

(b) *Every semisimple group of rank 1 over an algebraically closed field is isomorphic to SL_2 or PGL_2 .*

PROOF. (a) Let G be a semisimple group of rank 0. We may assume that k is algebraically closed. If all the elements of $G(k)$ are unipotent, then G is solvable (I, 15.2), and hence trivial (being semisimple). Otherwise, $G(k)$ contains a semisimple element (I, 10.18). The smallest algebraic subgroup H of G such that $H(k)$ contains the element is commutative, and therefore decomposes into $H_s \times H_u$ (I, 16.12). If all semisimple elements of $G(k)$ are of finite order, then G is finite, and hence trivial (being connected). If $G(k)$ contains a semisimple element of infinite order, then H_s° is a nontrivial torus, and so G is not of rank 0.

(b) One shows that G contains a solvable subgroup B such that $G/B \approx \mathbb{P}^1$. From this one gets a nontrivial homomorphism $G \rightarrow \text{Aut}(\mathbb{P}^1) \simeq \text{PGL}_2$. See Theorem 3.40 below or Springer 1998, 7.3.2. \square

2i Centralizers and normalizers

Let H be a subgroup of an algebraic group G . Recall (I, §7f) that normalizer of H in G is the algebraic subgroup $N = N_G(H)$ of G such that, for any k -algebra R ,

$$N(R) = \{g \in G(R) \mid g \cdot H(R') \cdot g^{-1} = H(R') \text{ for all } R\text{-algebras } R'\},$$

and that the centralizer of H in G is the algebraic subgroup $C = C_G(H)$ of G such that, for any k -algebra R ,

$$C(R) = \{g \in G(R) \mid gh = hg \text{ for all } h \in H(R') \text{ and all } R\text{-algebras } R'\}.$$

If $H(k')$ is dense H for some field $k' \supset k$, then

$$\begin{aligned} N(k) &= G(k) \cap N_{G(k')}(H(k')) \\ C(k) &= G(k) \cap C_{G(k')}(H(k')). \end{aligned}$$

This last applies when H is smooth, for example a torus, and $k' = k^{\text{sep}}$.

THEOREM 2.7 *Let T be a torus in a reductive group G .*

- (a) *The centralizer $C_G(T)$ of T in G is a reductive group; in particular, it is smooth and connected.*
- (b) *The identity component of the normalizer $N_G(T)$ of T in G is $C_G(T)$; therefore, $N_G(T)/C_G(T)$ is a finite étale group.*

(c) The torus T is maximal if and only if $T = C_G(T)$.

PROOF. (a) We defer the proof to the next section (and the next version of the notes; cf. 3.44).

(b) Certainly $N_G(T)^\circ \supset C_G(T)^\circ = C_G(T)$. But $N_G(T)^\circ/C_G(T)$ acts faithfully on T , and so is trivial by rigidity (I, 14.32). For any algebraic group H , the quotient H/H° is a finite étale group (almost by definition; see I, 13.17).

(c) Certainly, if $C_G(T) = T$, then T is maximal because any torus containing T is contained in $C_G(T)$. Conversely, $C_G(T)$ is a reductive group containing T as a maximal torus, and so $Z(C_G(T))^\circ$ is a torus (1.4) containing T and therefore equal to it. Hence $C_G(T)/T$ is a semisimple group (1.4) of rank 0, and so is trivial (2.6). Thus $C_G(T) = Z(C_G(T))^\circ = T$. \square

The quotient $W(G, T) = N_G(T)/C_G(T)$ is called the **Weyl group** of (G, T) . It is a constant étale algebraic group⁵ when T is split, and so may be regarded simply as a finite group.

2j Definition of the coroots

LEMMA 2.8 *Let (G, T) be a split reductive group. The action of $W(G, T)$ on $X^*(T)$ stabilizes R .*

PROOF. Take $k = k^{\text{al}}$. Let s normalize T (and so represent an element of W). Then s acts on $X^*(T)$ (on the left) by

$$(s\chi)(t) = \chi(s^{-1}ts).$$

Let α be a root. Then, for $x \in \mathfrak{g}_\alpha$ and $t \in T(k)$,

$$t(sx) = s(s^{-1}ts)x = s(\alpha(s^{-1}ts)x) = \alpha(s^{-1}ts)sx,$$

and so T acts on $s\mathfrak{g}_\alpha$ through the character $s\alpha$, which must therefore be a root. [This is at least the third proof of this.] \square

PROPOSITION 2.9 *Let (G, T) be a split reductive group, and let $R \subset X \stackrel{\text{def}}{=} X^*(T)$ be its root system.*

(a) *For each $\alpha \in R$, there exists a unique subgroup U_α of G isomorphic to \mathbb{G}_a such that, for any isomorphism $u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$,*

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \text{ all } t \in T(k^{\text{al}}), a \in G(k^{\text{al}}).$$

(b) *For a root α of (G, T) , let $T_\alpha = \text{Ker}(\alpha)^\circ$, and let G_α be centralizer of T_α . Then $W(G_\alpha, T)$ contains exactly one nontrivial element s_α , and there is a unique $\alpha^\vee \in X_*(T)$ such that*

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad \text{for all } x \in X^*(T). \quad (168)$$

Moreover, $\langle \alpha, \alpha^\vee \rangle = 2$.

⁵That is, $W(R)$ is the same finite group for all integral domains R . Roughly speaking, the reason for this is that $W(k)$ equals the Weyl group of the root datum, which doesn't depend on the base field (or base ring).

- (c) For each root α of (G, T) , G_α is the affine subgroup of G generated by T , U_α , and $U_{-\alpha}$.

We prove this after giving an application and some examples. The group U_α in (a) is called the **root group** of α .

THEOREM 2.10 For any split reductive group (G, T) , the system

$$(X^*(T), R, X_*(T), R^\vee)$$

with $R^\vee = \{\alpha^\vee \mid \alpha \in R\}$ and the map $\alpha \mapsto \alpha^\vee: R \rightarrow R^\vee$ determined by (168) is a root datum.

PROOF. We noted in (2.9b) that (rd1) holds. The s_α attached to α lies in $W(G_\alpha, T) \subset W(G, T)$, and so stabilizes R by the lemma. Finally, all s_α lie in the Weyl group $W(G, T)$, and so they generate a finite group (in fact, they generate exactly $W(G, T)$; see 3.43). \square

EXAMPLE 2.11 Let $G = \text{SL}_2$, and let α be the root 2χ . Then $T_\alpha = 1$ and $G_\alpha = G$. The unique $s \neq 1$ in $W(G, T)$ is represented by

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and the unique α^\vee for which (168) holds is λ .

EXAMPLE 2.12 Let $G = \text{GL}_n$, and let $\alpha = \alpha_{12} = \chi_1 - \chi_2$. Then

$$T_\alpha = \{\text{diag}(x, x, x_3, \dots, x_n) \mid xx x_3 \dots x_n \neq 1\}$$

and G_α consists of the invertible matrices of the form

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

Clearly

$$n_\alpha = \begin{pmatrix} 0 & 1 & 0 & & 0 \\ 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

represents the unique nontrivial element s_α of $W(G_\alpha, T)$. It acts on T by

$$\text{diag}(x_1, x_2, x_3, \dots, x_n) \mapsto \text{diag}(x_2, x_1, x_3, \dots, x_n).$$

For $x = m_1\chi_1 + \dots + m_n\chi_n$,

$$\begin{aligned} s_\alpha x &= m_2\chi_1 + m_1\chi_2 + m_3\chi_3 + \dots + m_n\chi_n \\ &= x - \langle x, \lambda_1 - \lambda_2 \rangle (\chi_1 - \chi_2). \end{aligned}$$

Thus (168), p. 344, holds if and only if α^\vee is taken to be $\lambda_1 - \lambda_2$.

SKETCH OF THE PROOF OF PROPOSITION 2.9.

The key point is that the derived group of G_α is a semisimple group of rank one and T is a maximal torus of G_α . Thus, we are essentially in the case of SL_2 or PGL_2 , where everything is obvious (see above). Note that the uniqueness of α^\vee follows from that of s_α .

For GL_n , the coroot α_{ij}^\vee of α_{ij} is

$$t \mapsto \text{diag}(1, \dots, 1, t^i, 1, \dots, 1, t^{-j}, 1, \dots, 1).$$

Clearly $\langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = \alpha_{ij} \circ \alpha_{ij}^\vee = 2$.

LEMMA 2.13 *Let G_α be the subgroup of G of semisimple rank 1 generated by T, U_α , and $U_{-\alpha}$, and let $w_\alpha \in G_\alpha$ represent the nontrivial element of the Weyl group of (G_α, T) . Then there is a unique $\alpha^\vee \in X^\vee$ such that*

$$w_\alpha \chi = \chi - \langle \chi, \alpha^\vee \rangle \alpha \text{ all } \chi \in X. \tag{169}$$

PROOF. Let $\chi \in X = X^*(T)$. We first show that there exists a G_α -module V such that $V_\chi \neq 0$. To see this, regard χ as an element of $\mathcal{O}(T)$, and let f be an element of $\mathcal{O}(G_\alpha)$ that restricts to it. Let V be any finite-dimensional subspace of $\mathcal{O}(G_\alpha)$ containing f and stable under G_α (I, §8i). For $v \in V$,

$$u_\alpha(a)v = \sum_{i \geq 0} a^i v_i, \quad \text{some } v_i \in V, \tag{170}$$

because $u_\alpha(a)$ is a polynomial in a . If $v \in V_\psi$ for some $\psi \in X$, then $v_i \in V_{\psi+i\alpha}$. This is a simple calculation using (170) and the definition of U_α . We have that $V_\chi \neq 0$ and that $\sum_{i \in \mathbb{Z}} V_{\chi+i\alpha}$ is invariant under T, U_α , and $U_{-\alpha}$, and hence also under G_α and w_α . Thus $w_\alpha \chi = \chi + i\alpha$ for some $i \in \mathbb{Z}$, and the map $\chi \mapsto -i$ defines an $\alpha^\vee \in X^\vee$ for which (169) holds; and clearly α^\vee is unique. □

It follows that $\langle \alpha, \alpha^\vee \rangle = 2$, either because $w_\alpha \alpha = -\alpha$ or because $w_\alpha^2 = 1$, both of which hold because the semisimple rank of G_α is 1. If we extend scalars $\mathbb{Z} \rightarrow \mathbb{R}$ and X^\vee is identified with X via any w_α -invariant positive definite bilinear form, then α^\vee takes on the familiar form $(2/(\alpha, \alpha))\alpha$ so that the lemma implies that important fact that $2(\beta, \alpha)/(\alpha, \alpha) \in \mathbb{Z}$ for any two roots α, β .

2k Computing the centre

PROPOSITION 2.14 (a) *Every maximal torus T in a reductive algebraic group G contains the centre $Z = Z(G)$ of G .*

(b) *The kernel of $\text{Ad}: T \rightarrow \text{GL}_{\mathfrak{g}}$ is $Z(G)$.*

PROOF. (a) Clearly $Z \subset C_G(T)$, but (see 2.7), $C_G(T) = T$.

(b) In characteristic zero, the kernel of $\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$ is $Z(G)$ (II, 5.29), and so the kernel of $\text{Ad}|_T$ is $Z(G) \cap T = Z(G)$. In general, $\text{Ker}(\text{Ad})/Z(G)$ is a unipotent group (II, 4.3). Therefore, the image of $\text{Ker}(\text{Ad}|_T)$ in $\text{Ker}(\text{Ad})/Z(G)$ is trivial, which implies that $\text{Ker}(\text{Ad}|_T) \subset Z(G)$. The reverse inclusion follows from (a). □

From the proposition,

$$Z(G) = \text{Ker}(\text{Ad}|T) = \bigcap_{\alpha \in R} \text{Ker}(\alpha).$$

We can use this to compute the centres of groups. For example,

$$\begin{aligned} Z(\text{GL}_n) &= \bigcap_{i \neq j} \text{Ker}(\chi_i - \chi_j) = \left\{ \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \mid x_1 = x_2 = \dots = x_n \neq 0 \right\}, \\ Z(\text{SL}_2) &= \text{Ker}(2\chi) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x^2 = 1 \right\} = \mu_2, \\ Z(\text{PGL}_2) &= \text{Ker}(\chi) = 1. \end{aligned}$$

On applying X^* to the exact sequence

$$0 \rightarrow Z(G) \rightarrow T \xrightarrow{t \mapsto (\dots, \alpha(t), \dots)} \prod_{\alpha \in R} \mathbb{G}_m \quad (171)$$

we get (I, 14.20) an exact sequence

$$\bigoplus_{\alpha \in R} \mathbb{Z} \xrightarrow{(\dots, m_\alpha, \dots) \mapsto \sum m_\alpha \alpha} X^*(T) \rightarrow X^*(Z(G)) \rightarrow 0,$$

and so

$$X^*(Z(G)) = X^*(T) / \{\text{subgroup generated by } R\}. \quad (172)$$

For example,

$$\begin{aligned} X^*(Z(\text{GL}_n)) &\simeq \mathbb{Z}^n / \langle e_i - e_j \mid i \neq j \rangle \xrightarrow[(\simeq)]{(a_1, \dots, a_n) \mapsto \sum a_i} \mathbb{Z}, \\ X^*(Z(\text{SL}_2)) &\simeq \mathbb{Z}/(2), \\ X^*(Z(\text{PGL}_2)) &\simeq \mathbb{Z}/\mathbb{Z} = 0. \end{aligned}$$

21 Semisimple and toral root data

DEFINITION 2.15 A root datum is *semisimple* if R generates a subgroup of finite index in X .

PROPOSITION 2.16 A split reductive group is semisimple if and only if its root datum is semisimple.

PROOF. A reductive group is semisimple if and only if its centre is finite, and so this follows from (172), p. 347. \square

DEFINITION 2.17 A root datum is *toral* if R is empty.

PROPOSITION 2.18 A split reductive group is a torus if and only if its root datum is toral.

PROOF. If the root datum is toral, then (172), p. 347, shows that $Z(G) = T$. Hence $\mathcal{D}G$ has rank 0, and so is trivial. It follows that $G = T$. Conversely, if G is a torus, the adjoint representation is trivial and so $\mathfrak{g} = \mathfrak{g}_0$. \square

2m The main theorems

Let (G, T) be a split reductive group, with root datum $\Psi(G, T)$.

THEOREM 2.19 *Let T' be a split maximal torus in G . Then T' is conjugate to T by an element of $G(k)$.*

PROOF. See 3.22, 3.23 below. (When k has characteristic zero and G is semisimple, this was proved in III, 3.17.) □

EXAMPLE 2.20 Let $G = \mathrm{GL}_V$, and let T be a split torus. A split torus is (by definition) diagonalizable, i.e., there exists a basis for V such that $T \subset \mathbb{D}_n$. Since T is maximal, it equals \mathbb{D}_n . This proves the theorem for GL_V since any two bases are conjugate by an element of $\mathrm{GL}_V(k)$.

It follows that the root datum attached to (G, T) depends only on G (up to isomorphism).

THEOREM 2.21 (EXISTENCE) *Every reduced root datum arises from a split reductive group (G, T) .*

PROOF. See Section 6 below (or Springer 1998, 16.5). □

A root datum is **reduced** if the only multiples of a root α that can also be a root are α and $-\alpha$.

THEOREM 2.22 (ISOMORPHISM) *Every isomorphism $\Psi(G, T) \rightarrow \Psi(G', T')$ of root data arises from an isomorphism $(G, T) \rightarrow (G', T')$.*

PROOF. See Section 7 below Springer 1998, 16.3.2. □

In fact, with the appropriate definitions, every isogeny of root data (or even epimorphism of root data) arises from and isogeny (or epimorphism) of split reductive groups $(G, T) \rightarrow (G', T')$.

Later we shall define the notion of a base for a root datum. If bases are fixed for (G, T) and (G', T') , then φ can be chosen to send one base onto the other, and it is then unique up to composition with a homomorphism $\mathrm{inn}(t)$ such that $t \in T(k^{\mathrm{al}})$ and $\alpha(t) \in k$ for all α .

2n Examples

We now work out the root datum attached to each of the classical split semisimple groups. In each case the strategy is the same. We work with a convenient form of the group G in GL_n . We first compute the weights of the split maximal torus of G on \mathfrak{gl}_n , and then check that each nonzero weight occurs in \mathfrak{g} (in fact, with multiplicity 1). Then for each α we find a natural copy of SL_2 (or PGL_2) centralizing T_α , and use it to find the coroot α^\vee .

EXAMPLE (A_n): SL_{n+1} .

Let G be SL_{n+1} and let T be the algebraic subgroup of diagonal matrices:

$$\{\text{diag}(t_1, \dots, t_{n+1}) \mid t_1 \cdots t_{n+1} = 1\}.$$

Then

$$X^*(T) = \bigoplus \mathbb{Z}\chi_i / \mathbb{Z}\chi, \quad \left\{ \begin{array}{l} \text{diag}(t_1, \dots, t_{n+1}) \xrightarrow{\chi_i} t_i \\ \chi = \sum \chi_i \end{array} \right.$$

$$X_*(T) = \{\sum a_i \lambda_i \mid \sum a_i = 0\}, \quad t \xrightarrow{\sum a_i \lambda_i} \text{diag}(t^{a_1}, \dots, t^{a_n}), \quad a_i \in \mathbb{Z},$$

with the obvious pairing $\langle \cdot, \cdot \rangle$. Write $\bar{\chi}_i$ for the class of χ_i in $X^*(T)$. Then all the characters $\bar{\chi}_i - \bar{\chi}_j, i \neq j$, occur as roots, and their coroots are respectively $\lambda_i - \lambda_j, i \neq j$. This follows easily from the calculation of the root datum of GL_n .

EXAMPLE (B_n): SO_{2n+1} .

Consider the symmetric bilinear form ϕ on k^{2n+1} ,

$$\phi(\vec{x}, \vec{y}) = 2x_0y_0 + x_1y_{n+1} + x_{n+1}y_1 + \cdots + x_ny_{2n} + x_{2n}y_n$$

Then $SO_{2n+1} \stackrel{\text{def}}{=} SO(\phi)$ consists of the $2n + 1 \times 2n + 1$ matrices A of determinant 1 such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix}.$$

The Lie algebra of SO_{2n+1} consists of the $2n + 1 \times 2n + 1$ matrices A of trace 0 such that

$$\phi(A\vec{x}, \vec{y}) = -\phi(\vec{x}, A\vec{y}),$$

(II, 1.22), i.e., such that

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} = - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A.$$

Take T to be the maximal torus of diagonal matrices

$$\text{diag}(1, t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1})$$

Then

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \text{diag}(1, t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \xrightarrow{\chi_i} t_i$$

$$X_*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\lambda_i, \quad t \xrightarrow{\lambda_i} \text{diag}(1, \dots, t^{i+1}, \dots, 1)$$

with the obvious pairing $\langle \cdot, \cdot \rangle$. All the characters

$$\pm \chi_i, \quad \pm \chi_i \pm \chi_j, \quad i \neq j$$

occur as roots, and their coroots are, respectively,

$$\pm 2\lambda_i, \quad \pm \lambda_i \pm \lambda_j, \quad i \neq j.$$

EXAMPLE (C_n): Sp_{2n} .

Consider the skew symmetric bilinear form $k^{2n} \times k^{2n} \rightarrow k$,

$$\phi(\vec{x}, \vec{y}) = x_1 y_{n+1} - x_{n+1} y_1 + \cdots + x_n y_{2n} - x_{2n} y_n.$$

Then Sp_{2n} consists of the $2n \times 2n$ matrices A such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The Lie algebra of Sp_n consists of the $2n \times 2n$ matrices A such that

$$\phi(A\vec{x}, \vec{y}) = -\phi(\vec{x}, A\vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} = - \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A.$$

Take T to be the maximal torus of diagonal matrices

$$\mathrm{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}).$$

Then

$$\begin{aligned} X^*(T) &= \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, & \mathrm{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) &\xrightarrow{\chi_i} t_i \\ X_*(T) &= \bigoplus_{1 \leq i \leq n} \mathbb{Z}\lambda_i, & t &\xrightarrow{\lambda_i} \mathrm{diag}(1, \dots, t, \dots, 1) \end{aligned}$$

with the obvious pairing $\langle \cdot, \cdot \rangle$. All the characters

$$\pm 2\chi_i, \quad \pm\chi_i \pm \chi_j, \quad i \neq j$$

occur as roots, and their coroots are, respectively,

$$\pm\lambda_i, \quad \pm\lambda_i \pm \lambda_j, \quad i \neq j.$$

EXAMPLE (D_n): SO_{2n} .

Consider the symmetric bilinear form $k^{2n} \times k^{2n} \rightarrow k$,

$$\phi(\vec{x}, \vec{y}) = x_1 y_{n+1} + x_{n+1} y_1 + \cdots + x_n y_{2n} + x_{2n} y_n.$$

Then $\mathrm{SO}_n = \mathrm{SO}(\phi)$ consists of the $n \times n$ matrices A of determinant 1 such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

The Lie algebra of SO_n consists of the $n \times n$ matrices A of trace 0 such that

$$\phi(A\vec{x}, \vec{y}) = -\phi(\vec{x}, A\vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = - \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A.$$

When we write the matrix as $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, then this last condition becomes

$$A + D^t = 0, \quad C + C^t = 0, \quad B + B^t = 0.$$

Take T to be the maximal torus of matrices

$$\mathrm{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1})$$

and let χ_i , $1 \leq i \leq r$, be the character

$$\mathrm{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \mapsto t_i.$$

All the characters

$$\pm \chi_i \pm \chi_j, \quad i \neq j$$

occur, and their coroots are, respectively,

$$\pm \lambda_i \pm \lambda_j, \quad i \neq j.$$

REMARK 2.23 The subscript on A_n , B_n , C_n , D_n denotes the rank of the group, i.e., the dimension of a maximal torus.

3 Borel fixed point theorem and applications

3a Brief review of algebraic geometry

We need the notion of an algebraic variety (not necessarily affine). To keep things simple, I assume that k is algebraically closed, and I use the conventions of my notes AG. Thus, an algebraic variety over k is topological space X together with a sheaf \mathcal{O}_X such that $\mathcal{O}_X(U)$ is a k -algebra of functions $U \rightarrow k$; it is required that X admits a finite open covering $X = \bigcup U_i$ such that, for each i , $(U_i, \mathcal{O}_X|_{U_i})$ is isomorphic to $\mathrm{Spm} A_i$ for some finitely generated reduced k -algebra A_i ; finally, X is required to be separated.

3.1 A projective variety is a variety that can be realized as a closed subvariety of some projective space \mathbb{P}^n . In particular, any closed subvariety of a projective variety is projective.

3.2 Let V be a vector space of dimension n over k .

(a) The set $\mathbb{P}(V)$ of one-dimensional subspaces of V is in a natural way a projective variety: in fact the choice of a basis for V defines a bijection $\mathbb{P}(V) \leftrightarrow \mathbb{P}^{n-1}$.

(b) Let $G_d(V)$ be the set of d -dimensional subspaces of V . When we fix a basis for V , the choice of a basis for S determines a $d \times n$ matrix $A(S)$ whose rows are the coordinates of the basis elements. Changing the basis for S multiplies $A(S)$ on the left by an invertible $d \times$

d matrix. Thus, the family of $d \times d$ minors of $A(S)$ is determined by S up to multiplication by a nonzero constant, and so defines a point $P(S)$ of $\mathbb{P}^{\binom{n}{d}-1}$. One shows that $S \mapsto P(S)$ is a bijection of $G_d(V)$ onto a closed subset of $\mathbb{P}^{\binom{n}{d}-1}$ (called a **Grassmann variety**; AG 6.26). For a d -dimensional subspace S of V , the tangent space

$$T_S(G_d(V)) \simeq \text{Hom}(S, V/S)$$

(ibid. 6.29).

(c) For any sequence of integers $n > d_r > d_{r-1} > \cdots > d_1 > 0$ the set of flags

$$V_r \supset \cdots \supset V_1$$

with V_i a subspace of V of dimension d_i has a natural structure of a projective algebraic variety (called a **flag variety**; AG p. 131).

3.3 An algebraic variety X is said to be **complete** if, for all algebraic varieties T , the projection map $X \times T \rightarrow T$ is closed (AG 7.1). Every projective variety is complete (AG 7.7). If X is complete, then its image under any regular map $X \rightarrow Y$ is closed and complete (AG 7.3). An affine variety is complete if and only if it has dimension zero, and so is a finite set of points (AG 7.5).

3.4 A regular map $f: X \rightarrow S$ is **proper** if, for all regular maps $T \rightarrow S$, the map $X \times_S T \rightarrow T$ is closed. If $f: X \rightarrow S$ is proper, then, for any complete subvariety Z of X , the image fZ of Z in S is complete (AG 8.26); moreover, X is complete if S is complete (AG 8.24). Finite maps are proper because they are closed (AG 8.7) and the base change of a finite map is finite.

3.5 A regular map $\varphi: Y \rightarrow X$ is said to be **dominant** if its image is dense in X . If φ is dominant, then the map $f \mapsto \varphi \circ f: \mathcal{O}_X(X) \rightarrow \mathcal{O}_Y(Y)$ is injective, and so, when X and Y are irreducible, φ defines a homomorphism $k(X) \rightarrow k(Y)$ of the fields of rational functions. A dominant map $Y \rightarrow X$ of irreducible varieties is said to be **separable** when $k(Y)$ is separably generated over $k(X)$, i.e., it is a finite separable extension of a purely transcendental extension of $k(X)$. A regular map $\varphi: Y \rightarrow X$ of irreducible varieties is dominant and separable if and only if there exists a nonsingular point $y \in Y$ such $x = \varphi(y)$ is nonsingular and the map $d\varphi: T_y(Y) \rightarrow T_x(X)$ is surjective (in which case, the set of such points y is open).

3.6 A bijective regular map of algebraic varieties need not be an isomorphism. For example, $x \mapsto x^p: \mathbb{A}^1 \rightarrow \mathbb{A}^1$ in characteristic p corresponds to the map of k -algebras $T \mapsto T^p: k[T] \rightarrow k[T]$, which is not an isomorphism, and

$$t \mapsto (t^2, t^3): \mathbb{A}^1 \rightarrow \{y^2 = x^3\} \subset \mathbb{A}^2$$

corresponds to the map $k[t^2, t^3] \hookrightarrow k[t]$, which is not an isomorphism. In the first example, the map is not separable, and in the second the curve $y^2 = x^3$ is not normal. Every separable bijective map $\varphi: Y \rightarrow X$ with X normal is an isomorphism (AG 10.12 shows that φ is birational, and AG 8.19 then shows that it is an isomorphism).

3.7 The set of nonsingular points of a variety is dense and open (AG 5.18). Therefore, an algebraic variety on which an algebraic group acts transitively by regular maps is nonsingular (cf. AG 5.20). As a nonsingular point is normal (i.e., $\mathcal{O}_{X,x}$ is integrally closed; see CA 17.5), the same statements hold with “nonsingular” replaced by “normal”.⁶

3b Quotients

In Chapter I, we defined the quotient of an algebraic group G by a *normal* algebraic subgroup N . Now we need to consider the quotient of G by an arbitrary algebraic subgroup H .

We continue with the conventions of the last subsection: k is algebraically closed, and we consider only reduced (hence smooth) algebraic groups.

3.8 Let G be a smooth algebraic group. An *action* of G on a variety X is a regular map $G \times X \rightarrow X$ such that the underlying map of sets is an action of the abstract group G on the set X . Every orbit for the action is open in its closure, and every orbit of minimum dimension is closed. In particular, each orbit is a subvariety of X and there exist closed orbits. The *isotropy group* G_o at a point o of X is the pre-image of o under the regular map $g \mapsto go: G \rightarrow X$, and so is an affine algebraic subgroup of G . (AG 10.6.)

3.9 Let H be a smooth subgroup of the smooth algebraic group G . A *quotient* of G by H is an algebraic variety X together with a transitive action $G \times X \rightarrow X$ of G and a point o fixed by H having the following universal property: for any variety X' with action of G and point o' of X' fixed by H , the regular map

$$(g, o') \mapsto go': G \times X \rightarrow X'$$

factors through X (as a regular map). Clearly, a quotient is unique (up to a unique isomorphism) if it exists.

3.10 Let H be a smooth subgroup of a connected smooth algebraic group G , and consider a transitive action $G \times X \rightarrow X$ of G on a variety X . Suppose that there exists a point o in X such that the isotropy group G_o at o is H . The pair (X, o) is a quotient of G by H if and only if the map

$$g \mapsto g \cdot o: G \xrightarrow{\varphi} X$$

is separable. The fibres of the map φ are the conjugates of H . In particular, they all have dimension $\dim H$, and so

$$\dim X = \dim G - \dim H$$

(AG 10.9). The map

$$(d\varphi)_e: T_e G \rightarrow T_e X$$

contains $T_e H$ in its kernel. As $\dim T_e G = \dim G$ and $\dim T_e H = \dim H$ (because G and H are smooth), we see that $(d\varphi)_e$ is surjective if and only if its kernel is exactly $T_e H$. Therefore (X, o) is a quotient of G by H if $\text{Ker}((d\varphi)_e) = \text{Lie}(H)$ (by (3.5) and (3.10)).

⁶The proof that nonsingular points are normal is quite difficult. It is possible to avoid it by showing directly that the set of normal points in an algebraic variety is open and dense (Springer 1998, 5.2.11).

PROPOSITION 3.11 *A quotient exists for every smooth subgroup H of a smooth algebraic group G . It is a quasi-projective algebraic variety, and the isotropy group of the distinguished point is H .*

PROOF. As in the case of a normal subgroup, a key tool in the proof is Chevalley's theorem (I, 8.57): there exists a representation $G \rightarrow \mathrm{GL}_V$ and a one-dimensional subspace L in V such that H is the stabilizer of L . The action of G on V defines an action

$$G \times \mathbb{P}(V) \rightarrow \mathbb{P}(V)$$

of the algebraic group G on the algebraic variety $\mathbb{P}(V)$. Let X be the orbit of L in $\mathbb{P}(V)$, i.e., $X = G \cdot L$. Then X is a subvariety of $\mathbb{P}(V)$, and so it is quasi-projective (because $\mathbb{P}(V)$ is projective). Let φ be the map $g \mapsto gL: G \rightarrow X$. It follows from II, 2.15, that the kernel of $(d\varphi)_e$ is \mathfrak{h} , and so the map is separable. This implies that X is a quotient of G by H . \square

We let G/H denote the quotient of G by H . Because H is the isotropy group at the distinguished point,

$$(G/H)(k) = G(k)/H(k).$$

3.12 In the proof of the proposition, we showed that, for any representation (V, r) of G and line L such that H is the stabilizer of L , the orbit of L in $\mathbb{P}(V)$ is a quotient of G by H .

3.13 Let $G = \mathrm{GL}_2$ and $H = \mathbb{T}_2 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$. Then G acts on k^2 , and H is the subgroup fixing the line $L = \left\{ \begin{pmatrix} * \\ 0 \end{pmatrix} \right\}$. The proof of the proposition shows that G/H is isomorphic to the orbit of L , but G acts transitively on the set of lines, and so $G/H \simeq \mathbb{P}^1$.

3.14 When H is normal in G , this construction of G/H agrees with that in (I 7.63). In particular, when H is normal, G/H is affine.

3.15 Let $G \times X \rightarrow X$ be a transitive action of a smooth algebraic G on a variety X , and let o be a point of X . Let H be the isotropy group at o . The universal property of the quotient shows that the map $g \mapsto go$ factors through G/H . The resulting map $G/H \rightarrow X$ is finite and purely inseparable.

ASIDE 3.16 Quotients exist under much more general hypotheses. Let G be an affine algebraic group scheme over an arbitrary field k , and let H be an affine subgroup scheme. Then the associated sheaf of the presheaf $R \rightsquigarrow G(R)/H(R)$ is represented by an algebraic scheme G/H over k . See DG, III, §3, 5.4, p. 341.

For any homomorphism of k -algebras $R \rightarrow R'$, the map $G(R)/H(R) \rightarrow G(R')/H(R')$ is injective. Therefore, the statement means that there exists a scheme G/H of finite type over k and a morphism $\pi: G \rightarrow G/H$ such that,

- ◇ for all k -algebras R , the nonempty fibres of the map $\pi(R): G(R) \rightarrow (G/H)(R)$ are cosets of $H(R)$;
- ◇ for all k -algebras R and $x \in (G/H)(R)$, there exists a finitely generated faithfully flat R -algebra R' and a $y \in G(R')$ lifting the image of x in $(G/H)(R')$.

3c The Borel fixed point theorem

THEOREM 3.17 *When a smooth connected solvable algebraic group acts on an algebraic variety, no orbit contains a complete subvariety of dimension > 0 .*

PROOF. Let G be a connected solvable smooth algebraic group. If the statement fails for G acting on X , then it fails for $G_{k^{\text{al}}}$ acting on $X_{k^{\text{al}}}$, and so we may suppose that k is algebraically closed. We use induction on the dimension of G .

It suffices to prove the statement for G acting on G/H where H is a smooth connected subgroup of G (because any orbit of G acting on a variety has a finite covering by such a variety G/H (3.15), and the inverse image of a complete subvariety under a finite map is complete (3.4)).

Fix a smooth connected subgroup H of G with $H \neq G$. Either H maps onto $G/\mathcal{D}G$ or it doesn't. In the first case, $\mathcal{D}G$ acts transitively on G/H , and the statement follows by induction (using I, 16.21). In the second case, we let N be the subgroup of G containing H corresponding to the image of H in $G/\mathcal{D}G$ (see I, 9.14); then N is normal in G and $G/N \simeq \text{Im}(H)/\mathcal{D}G$.⁷ Consider the quotient map $\pi: G/H \rightarrow G/N$. Let Z be a complete subvariety of G/H , which we may assume to be connected. Because N is normal, G/N is affine (see 3.14), and so the image of Z in G/N is a point (see 3.3). Therefore Z is contained in one of the fibres of the map π , but these are all isomorphic to N/H , and so we can conclude by induction again. \square

THEOREM 3.18 (BOREL FIXED POINT THEOREM) *Any smooth connected solvable algebraic group acting on a complete variety over an algebraically closed field has a fixed point.*

PROOF. According to (3.8), the action has a closed orbit, which is complete, and hence is a finite set of points (Theorem 3.17). As the group is connected, so is the orbit. \square

REMARK 3.19 It is possible to recover the Lie-Kolchin theorem (I, 16.31) from the Borel fixed point theorem. Let G be a smooth connected solvable subgroup of GL_V , and let X be the collection of maximal flags in V (i.e., the flags corresponding to the sequence $\dim V = n > n-1 > \dots > 1 > 0$). As noted in (3.2), this has a natural structure of a projective variety, and G acts on it by a regular map

$$g, F \mapsto gF: G \times X \rightarrow X$$

where

$$g(V_n \supset V_{n-1} \supset \dots) = gV_n \supset gV_{n-1} \supset \dots.$$

According to the theorem, there is a fixed point, i.e., a maximal flag such that $gF = F$ for all $g \in G(k)$. Relative to a basis e_1, \dots, e_n adapted to the flag,⁸ $G \subset \mathbb{T}_n$.

NOTES The improvement, Theorem 3.17 of Borel's fixed point theorem, is from Allcock 2009.

⁷The group N is connected by I, 13.21, and smooth by I, 17.1.

⁸That is, such that e_1, \dots, e_i is a basis of V_i .

3d Borel subgroups

Throughout this subsection, G is a reductive group.

DEFINITION 3.20 A **Borel subgroup** of G is a smooth subgroup B such that $B_{k^{\text{al}}}$ is a maximal smooth connected solvable subgroup of $G_{k^{\text{al}}}$.

For example, $\mathbb{T}_2 \stackrel{\text{def}}{=}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ is a Borel subgroup of GL_2 (it is certainly connected and solvable, and the only connected subgroup properly containing it is GL_2 , which isn't solvable).

THEOREM 3.21 *Let G be a reductive group over k .*

- ◇ *If B is a Borel subgroup of G , then G/B is projective.*
- ◇ *Any two Borel subgroups of G are conjugate by an element of k^{al} .*

PROOF. We may assume $k = k^{\text{al}}$.

We first prove that G/B is projective when B is a Borel subgroup of largest possible dimension. Apply the theorem of Chevalley (I, 8.57) to obtain a representation $G \rightarrow \text{GL}_V$ and a one-dimensional subspace L such that B is the subgroup fixing L . Then B acts on V/L , and the Lie-Kolchin theorem gives us a maximal flag in V/L stabilized by B . On pulling this back to V , we get a maximal flag,

$$F: V = V_n \supset V_{n-1} \supset \cdots \supset V_1 = L \supset 0$$

in V . Not only does B stabilize F , but (because of our choice of V_1), B is the isotropy group at F , and so the map $G/B \rightarrow B \cdot F$ is finite (see 3.15). This shows that, when we let G act on the variety of maximal flags, $G \cdot F$ is the orbit of smallest dimension, because for any other maximal flag F' , the stabilizer H of F' is a solvable algebraic subgroup of dimension at most that of B , and so

$$\dim G \cdot F' = \dim G - \dim H \geq \dim G - \dim B = \dim G \cdot F.$$

Therefore $G \cdot F$ is closed (3.8), and hence projective variety of maximal flags in V , $G \cdot F$ is projective. The map $G/B \rightarrow G \cdot F$ is finite, and so G/B is complete (see 3.4). As it is quasi-projective, this implies that it is projective.

To complete the proof of the theorems, it remains to show that for any Borel subgroups B and B' with B of largest possible dimension, $B' \subset gBg^{-1}$ for some $g \in G(k)$ (because the maximality of B' will then imply that $B' = gBg^{-1}$). Let B' act on G/B by $b', gB \mapsto b'gB$. The Borel fixed point theorem shows that there is a fixed point, i.e., for some $g \in G(k)$, $B'gB \subset gB$. Then $B'g \subset gB$, and so $B' \subset gBg^{-1}$ as required. \square

THEOREM 3.22 *Let G be a smooth connected algebraic group. All maximal tori in G are conjugate by an element of $G(k^{\text{al}})$.*

PROOF. Let T and T' be maximal tori. Being smooth, connected, and solvable, they are contained in Borel subgroups, say $T \subset B$, $T' \subset B'$. For some $g \in G$, $gB'g^{-1} = B$, and so $gT'g^{-1} \subset B$. Now T and $gT'g^{-1}$ are maximal tori in the B , and we know that the theorem holds for connected solvable groups (I, 16.35). \square

REMARK 3.23 We mention two stronger results.

- (a) (Grothendieck): Let G be a smooth affine group over a separably closed field k . Then any two maximal tori in G are conjugate by an element of $G(k)$. In Conrad et al. 2010, Appendix A, 2.10, p. 401, it is explained how to deduce this from the similar statement with k algebraically closed.
- (b) (Borel-Tits): Let G be a smooth affine group over a field k . Then any two maximal split tori in G are conjugate by an element of $G(k)$. In Conrad et al. 2010, Appendix C, 2.3, p. 506, it is explained how to deduce this from the statement that maximal tori in solvable groups are $G(k)$ -conjugate.

THEOREM 3.24 For any Borel subgroup B of G , $G = \bigcup_{g \in G(k^{\text{al}})} gBg^{-1}$.

SKETCH OF PROOF. Show that every element x of G is contained in a connected solvable subgroup of G (sometimes the identity component of the closure of the group generated by x is such a group), and hence in a Borel subgroup, which is conjugate to B (3.21). \square

THEOREM 3.25 For any torus T in G , $C_G(T)$ is connected.

PROOF. We may assume that k is algebraically closed. Let $x \in C_G(T)(k)$, and let B be a Borel subgroup of G . Then x is contained in a connected solvable subgroup of G (see 3.24), and so the Borel fixed point theorem shows that the subset X of G/B of cosets gB such that $xgB = gB$ is nonempty. It is also closed, being the subset where the regular maps $gB \mapsto xgB$ and $gB \mapsto gB$ agree. As T commutes with x , it stabilizes X , and another application of the Borel fixed point theorem shows that it has a fixed point in X . In other words, there exists a $g \in G$ such that

$$\begin{aligned} xgB &= gB \\ TgB &= gB. \end{aligned}$$

Thus, both x and T lie in gBg^{-1} and we know that the theorem holds for connected solvable groups (I, 16.36). Therefore $x \in C_G(T)^\circ$. \square

3e Parabolic subgroups

In this subsection, assume that k is algebraically closed.

DEFINITION 3.26 An algebraic subgroup P of G is *parabolic* if G/P is projective.

THEOREM 3.27 Let G be a connected algebraic group. An algebraic subgroup P of G is parabolic if and only if it contains a Borel subgroup.

PROOF. \implies : Let B be a Borel subgroup of G . According to the Borel fixed point theorem, the action of B on G/P has a fixed point, i.e., there exists a $g \in G$ such that $BgP = gP$. Then $Bg \subset gP$ and $g^{-1}Bg \subset P$.

\impliedby : Suppose P contains the Borel subgroup B . Then there is quotient map $G/B \rightarrow G/P$. Recall that G/P is quasi-projective, i.e., can be realized as a locally closed subvariety of \mathbb{P}^N for some N . Because G/B is projective, the composite $G/B \rightarrow G/P \rightarrow \mathbb{P}^N$ has closed image (see 3.4), but this image is G/P , which is therefore projective. \square

COROLLARY 3.28 *Any connected solvable parabolic algebraic subgroup of a connected algebraic group is a Borel subgroup.*

PROOF. Because it is parabolic it contains a Borel subgroup, which, being maximal among connected solvable groups, must equal it. \square

3f Examples of Borel and parabolic subgroups

EXAMPLE: GL_V

Let $G = GL_V$ with V of dimension n . Let F be a maximal flag

$$F: V_{n-1} \supset \cdots \supset V_1$$

and let $G(F)$ be the stabilizer of F , so

$$G(F)(R) = \{g \in GL(V \otimes R) \mid g(V_i \otimes R) \subset V_i \otimes R \text{ for all } i\}.$$

Then $G(F)$ is connected and solvable (because the choice of a basis adapted to F defines an isomorphism $G(F) \rightarrow \mathbb{T}_n$), and $GL_V / G(F)$ is projective (because $GL(V)$ acts transitively on the space of all maximal flags in V). Therefore, $G(F)$ is a Borel subgroup (3.28). For $g \in GL(V)$,

$$G(gF) = g \cdot G(F) \cdot g^{-1}.$$

Since all Borel subgroups are conjugate, we see that the Borel subgroups of GL_V are precisely the groups of the form $G(F)$ with F a maximal flag.

Now consider $G(F)$ with F a (not necessarily maximal) flag. Clearly F can be refined to a maximal flag F' , and $G(F)$ contains the Borel subgroup $G(F')$. Therefore it is parabolic. Later we'll see that all parabolic subgroups of GL_V are of this form.

EXAMPLE: SO_{2n}

Let V be a vector space of dimension $2n$, and let ϕ be a nondegenerate symmetric bilinear form on V with Witt index n . By a **totally isotropic flag** we mean a flag $\cdots \supset V_i \supset V_{i-1} \supset \cdots$ such that each V_i is totally isotropic. We say that such a flag is **maximal** if it has the maximum length n .

Let

$$F: V_n \supset V_{n-1} \supset \cdots \supset V_1$$

be such a flag, and choose a basis e_1, \dots, e_n for V_n such that $V_i = \langle e_1, \dots, e_i \rangle$. Then $\langle e_2, \dots, e_n \rangle^\perp$ contains V_n and has dimension⁹ $n+1$, and so it contains an x such that $\langle e_1, x \rangle \neq 0$. Scale x so that $\langle e_1, x \rangle = 1$, and define $e_{n+1} = x - \frac{1}{2}\phi(x, x)e_1$. Then $\phi(e_{n+1}, e_{n+1}) = 0$ and $\phi(e_1, e_{n+1}) = 1$. Continuing in this fashion, we obtain a basis $e_1, \dots, e_n, e_{n+1}, \dots, e_{2n}$

for which the matrix of ϕ is $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

⁹Recall that in a nondegenerate quadratic space (V, ϕ) ,

$$\dim W + \dim W^\perp = \dim V.$$

Now let F' be a second such flag, and choose a similar basis e'_1, \dots, e'_n for it. Then the linear map $e_i \mapsto e'_i$ is orthogonal, and maps F onto F' . Thus $O(\phi)$ acts transitively on the set X of maximal totally isotropic flags of V . One shows that X is closed (for the Zariski topology) in the flag variety consisting of all maximal flags $V_n \supset \dots \supset V_1$, and is therefore a projective variety. It may fall into two connected components which are the orbits of $SO(\phi)$.¹⁰

Let $G = SO(\phi)$. The stabilizer $G(F)$ of any totally isotropic flag is a parabolic subgroup, and one shows as in the preceding case that the Borel subgroups are exactly the stabilizers of maximal totally isotropic flags.

EXAMPLE: Sp_{2n}

Again the stabilizers of totally isotropic flags are parabolic subgroups, and the Borel subgroups are exactly the stabilizers of maximal totally isotropic flags.

EXAMPLE: SO_{2n+1}

Same as the last two cases.

EXERCISE 3-1 Write out a proof that the Borel subgroups of SO_{2n} , Sp_{2n} , and SO_{2n+1} are those indicated above.

3g Algebraic groups of rank one

Throughout this section, we assume that k is algebraically closed (for the present).

PRELIMINARIES

Let G be a reductive algebraic group, and let B be a Borel subgroup of G . The following are consequences of the completeness of the flag variety G/B .

3.29 All Borel subgroups, and all maximal tori, are conjugate (see 3.21; in fact, for any maximal torus T , $N_G(T)$ acts transitively on the Borel subgroups containing T).

3.30 The group G is solvable if one of its Borel subgroups is commutative.

3.31 The connected centralizer $C_G(T)^\circ$ of any maximal torus T lies in every Borel subgroup containing T .

3.32 The normalizer $N_G(B)$ of a Borel subgroup B contains B as a subgroup of finite index (and therefore is equal to its own normalizer).

3.33 The centralizer of a torus T in G has dimension equal $\dim \mathfrak{g}^T$.

¹⁰Let (V, ϕ) be a hyperbolic plane with its standard basis e_1, e_2 . Then the flags

$$\begin{aligned} F_1 &: \langle e_1 \rangle \\ F_2 &: \langle e_2 \rangle \end{aligned}$$

fall into different $SO(\phi)$ orbits.

According to (II, 2.26),

$$\mathrm{Lie}(C_G(T)) = \mathrm{Lie}(G)^T.$$

As $C_G(T)$ is smooth (see 2.7),

$$\dim C_G(T) = \dim(\mathrm{Lie}(C_G(T)))$$

(see II, 2.2).

PROPOSITION 3.34 *Let (V, r) be a representation of a torus T . In any closed subvariety of dimension d in $\mathbb{P}(V)$ stable under T , there are at least $d + 1$ points fixed by T .*

PROOF. (Borel 1991, IV, 13.5). Let Y be a closed subvariety of $\mathbb{P}(V)$ of dimension d . As T is connected, it leaves stable each irreducible component of Y , and so we may suppose that Y is irreducible. We use induction on the dimension of Y . If $\dim Y = 0$, the statement is obvious.

Let χ_1, \dots, χ_n be the distinct characters of T on V . There exists a $\lambda \in X_*(T)$ such that the integers $\langle \chi_i, \lambda \rangle$ are distinct. Now $\lambda(\mathbb{G}_m)$ and T have the same eigenvectors in V , and hence the same fixed points, and so we may suppose that $T = \mathbb{G}_m$.

If $\dim Y^T > 0$, then Y^T is infinite, so we may assume that this not so. The intersection of the hyperplanes containing Y (i.e., the smallest affine space containing Y) is stable under T , and so we may suppose that no hyperplane in $\mathbb{P}(V)$ contains Y .

Choose a basis $\{e_1, \dots, e_n\}$ of eigenvectors for \mathbb{G}_m , so $\lambda(t)e_i = t^{m_i}e_i$ for some $m_i \in \mathbb{Z}$ and $t \in \mathbb{G}_m(k)$. We may suppose that $m_1 \leq \dots \leq m_n$. Since Y is not contained in a hyperplane, there exists a $v \in V$ such that $\langle v \rangle \in Y$ and

$$v = a_1e_1 + \dots + a_n e_n, \quad a_i \in k,$$

with $a_1 \neq 0$. The map $t \mapsto \lambda(t)v: \mathbb{G}_m \rightarrow \mathbb{P}(V)$ extends to \mathbb{A}^1 — let $\lambda(0)v$ denote the image of 0. Then $\langle \lambda(0)v \rangle$ lies in Y and is fixed by \mathbb{G}_m . Moreover, it doesn't lie in the intersection of Y with the hyperplane in $\mathbb{P}(V)$ defined by the condition $a_1 = 0$. This intersection has dimension at most $d - 1$ (AG 9.18) and is stable under \mathbb{G}_m and so, by induction, it has at least d fixed points. Together with $\langle \lambda(0)v \rangle$, this gives \mathbb{G}_m at least $d + 1$ fixed points in Y . \square

COROLLARY 3.35 *Let P be a parabolic subgroup of a smooth connected algebraic group G , and let T be a torus in G . Then T fixes at least $1 + \dim G/P$ points of G/P .*

PROOF. There exists a representation (V, r) of G and an $o \in \mathbb{P}(V)$ such $g \mapsto go: G \rightarrow \mathbb{P}(V)$ defines an isomorphism of G/P onto the orbit $G \cdot o$ (see 3.12). We can apply the proposition with $Y = G \cdot o \simeq G/P$. \square

PRELIMINARIES ON SOLVABLE GROUPS

Let G be a smooth connected algebraic group. Let $\lambda: \mathbb{G}_m \rightarrow G$ be a cocharacter of G , and for $g \in G(k)$, consider the regular map

$$t \mapsto \lambda(t) \cdot g \cdot \lambda(t)^{-1}: \mathbb{G}_m \rightarrow G.$$

We let $P(\lambda)$ denote subgroup of $G(k)$ consisting of those g for which the map extends to $\mathbb{A}^1 = \mathbb{G}_m \cup \{0\}$. For $g \in P(\lambda)$, $\lim_{t \rightarrow 0} \lambda(t) \cdot g \cdot \lambda(t)^{-1}$ denote the value of the extended map at $t = 0$. We let

$$U(\lambda) = \{g \in P(\lambda) \mid \lim_{t \rightarrow 0} \lambda(t) \cdot g \cdot \lambda(t)^{-1} = 1\}.$$

Both $P(\lambda)$ and $U(\lambda)$ are closed subgroups of $G(k)$, and so may be regarded as smooth algebraic subgroups of G (cf. Springer 1998, 13.4).

PROPOSITION 3.36 *The subgroup G_+ is unipotent, and every weight of \mathbb{G}_m on $\text{Lie}(U(\lambda))$ is a strictly positive integer. If G is smooth, connected, and solvable, then $\text{Lie}(U(\lambda))$ contains all the strictly positive weight spaces for \mathbb{G}_m on $\text{Lie}(G)$.*

PROOF. Choose a faithful representation (V, r) of G . There exists a basis for V such that $r(\lambda(\mathbb{G}_m)) \subset \mathbb{D}_n$, say $\lambda \circ r(t) = \text{diag}(t^{m_1}, \dots, t^{m_n})$, $m_1 \geq m_2 \geq \dots \geq m_n$. Then $U(\lambda) \subset \mathbb{U}_n$, and the first statement is obvious.

Now assume that G is smooth, connected, and solvable. Then there is a unique connected normal unipotent subgroup G_u of G such that G/G_u is a torus (I, 16.33). We use induction on $\dim G_u$. When $\dim G_u = 0$, G is a torus, and there are no nonzero weight spaces.

Thus, we may assume that $\dim G_u > 0$. Then there exists a surjective homomorphism $\pi: G_u \rightarrow \mathbb{G}_a$, and

$$\pi(\lambda(t) \cdot g \cdot \lambda(t)^{-1}) = t^n \cdot \pi(g), \quad g \in G_u(k), \quad t \in \mathbb{G}_m(k),$$

for some $n \in \mathbb{Z}$.

If $n \leq 0$, then $t \mapsto \pi(\lambda(t) \cdot g \cdot \lambda(t)^{-1}): \mathbb{G}_m \rightarrow \mathbb{G}_a$ doesn't extend to \mathbb{A}^1 unless $\pi(g) = 0$. Hence $U(\lambda) \subset \text{Ker}(\pi)$, and we can apply induction.

If $n > 0$, then one shows that $\pi(U(\lambda)) = \mathbb{G}_a$, and we can again apply induction to $\text{Ker}(\pi)$. See Allcock 2009, Pptn 1. □

COROLLARY 3.37 *If G is connected, smooth, and solvable, then G is generated its subgroups $U(\lambda)$, $C_G(\lambda(\mathbb{G}_m))^\circ$, and $U(-\lambda)$.*

PROOF. Their Lie algebras span \mathfrak{g} . □

ALGEBRAIC GROUPS OF RANK ONE

Let G be smooth connected algebraic group of rank 1, and assume that G is not solvable. Let T be a maximal torus in G , and fix an isomorphism $\lambda: \mathbb{G}_m \rightarrow T$. Call a Borel subgroup positive if it contains $U(\lambda)$ and negative if it contains $U(-\lambda)$.

LEMMA 3.38 *With the above assumptions:*

- (a) T lies in at least two Borel subgroups, one positive and one negative.
- (b) If B (resp. B') is a positive (resp. negative) Borel subgroup containing T , then every Borel subgroup containing T lies in the subgroup generated by B and B' .
- (c) No Borel subgroup containing T is both positive and negative.
- (d) The normalizer of T in G contains an element acting on T as $t \mapsto t^{-1}$.

PROOF. (a) The subgroup $U(\lambda)$ is connected, unipotent, and normalized by T . Therefore $TU(\lambda)$ lies in a Borel subgroup, which is positive (by definition). A similar argument applies to $U(-\lambda)$.

(b) Apply Corollary 3.37.

(c) Otherwise (b) would imply that every Borel subgroup is contained in a single Borel subgroup, which contradicts (a).

(d) The normalizer $N_G(T)$ acts transitively on the Borel subgroups containing T (see 3.29). Any element taking a negative Borel subgroup to a positive Borel subgroup acts as $t \mapsto t^{-1}$ on T . \square

LEMMA 3.39 *Each maximal torus of G lies in exactly two Borel subgroups, one positive and one negative.*

PROOF. Let T be a maximal torus, and choose an identification of it with \mathbb{G}_m . We use induction on the dimension of a Borel subgroup B . If $\dim B = 1$, then it is commutative, and so G is solvable (3.30), contradicting the hypothesis.

We next consider the case $\dim B = 2$. We already know that T lies in a positive and in a negative Borel subgroup, and we have to show that any two positive Borel subgroups coincide. If not, their unipotent radicals would be distinct subgroups of $U(\lambda)$, and hence would generate a unipotent subgroup of dimension > 1 , contradicting $\dim B_u = 1$.

Now suppose that $\dim B \geq 3$. We may suppose that $B \supset T$ and is positive. Consider the action of B on G/N where $N = N_G(B)$. Because the only Borel subgroup that B normalizes is itself, B has a unique fixed point in G/N . Let O be an orbit of B in G/N of minimal dimension > 0 . The closure of O in G/N is a union of orbits of lower dimension, and so O is either a projective variety or a projective variety with one point omitted. This forces O to be a curve, because otherwise it would contain a complete curve, in contradiction to Theorem 3.17. Therefore, there exists a Borel subgroup B' such that $B \cap N_G(B')$ has codimension 1 in B .

Thus $H \stackrel{\text{def}}{=} (B \cap B')^\circ$ has codimension 1 in each of B and B' . Either $H = B_u = B'_u$ or it contains a torus. In the first case, $\langle B, B' \rangle$ normalizes H , and a Borel subgroup in $\langle B, B' \rangle/H$ has no unipotent part, and so $\langle B, B' \rangle$ is solvable, which is impossible.

Therefore H contains a torus. Conclude that B and B' are the only Borel subgroups of $\langle B, B' \rangle$ containing T , and one is positive and one negative. Then Lemma 3.38(d) shows that B and B' are interchanged by an element of $N_{\langle B, B' \rangle}(T)$ that acts as $t \mapsto t^{-1}$ on T . This implies that B' is negative as a Borel subgroup of G . Finally Lemma 3.38(b) implies that every Borel subgroup of G containing T lies in $\langle B, B' \rangle$, hence equals B or B' \square

THEOREM 3.40 *Let G be a connected smooth algebraic group of rank 1. Either G is solvable or there exists an isogeny $G/R_u G \rightarrow \text{PGL}_2$.*

PROOF. Let T be a maximal torus, let B be a Borel subgroup of G , and let $N = N_G(B)$. Since N is its own normalizer (3.32), it fixes only one point in B/N , and so the stabilizers of distinct points of G/N are the normalizers of distinct Borel subgroups. The fixed points of T in G/N correspond to the Borel subgroups that T normalizes, and hence contain T . Lemma 3.39 shows that T has exactly 2 fixed points in G/N . As G is nonsolvable, G/B (hence also G/N) has dimension ≥ 1 . In fact, G/N has dimension 1, because otherwise Corollary 3.33b would show that T has more than 2 fixed points. Therefore G/N is a

projective curve. Standard arguments show that it must be isomorphic to \mathbb{P}^1 (tba; see Borel 1991, 10.7; Humphreys 1975, p. 155). Choose an isomorphism $G/N \simeq \mathbb{P}^1$. This gives nontrivial homomorphism $G \rightarrow \text{Aut}(\mathbb{P}^1)$, and $\text{Aut}(\mathbb{P}^1) \simeq \text{PGL}_2(k)$ (AG 6.22). \square

3h Applications

Let G be a connected algebraic group, and let T be maximal torus in G . Let W be the subgroup of $N_G(T)/C_G(T)$ generated by reflections.

THEOREM 3.41 (Bruhat decomposition). *For any Borel subgroup B of G , $B = BWB$.*

PROOF. Springer 1998, 8.3.8. \square

THEOREM 3.42 (Normalizer theorem). *For any Borel subgroup B of G , $N_G(B) = B$.*

PROOF. This follows from the Bruhat decomposition and the simple transitivity of W on the Weyl chambers. \square

COROLLARY 3.43 $W = N_G(T)/C_G(T)$.

THEOREM 3.44 (Connectedness of torus centralizers). *For any torus T in G , $C_G(T)$ is connected.*

PROOF. This can be deduced from the Bruhat decomposition and a standard fact about reflection groups: the pointwise stabilizer of a linear subspace is generated by the reflections that fix it pointwise. \square

ASIDE 3.45 Our proof of Theorem 3.40 follows Allcock 2009. Unlike the standard proofs (e.g., Humphreys 1975, §25), it avoids using the normalizer theorem (every Borel subgroup of a connected group is its own normalizer).

4 Parabolic subgroups and roots

Throughout this section, k is algebraically closed of characteristic zero.

NOTES This needs to be rewritten for split reductive groups over arbitrary fields.

Recall (I, 14.15) that for a representation $T \rightarrow \text{GL}_V$ of a (split) torus T ,

$$V = \bigoplus_{\chi \in X^*(T)} V_\chi$$

where V_χ is the subspace on which T acts through the character χ . The χ for which $V_\chi \neq 0$ are called the **weights** of T in V , and the corresponding V_χ are called the **weight spaces**. Clearly

$$\text{Ker}(T \rightarrow \text{GL}_V) = \bigcap_{\chi \text{ a weight}} \text{Ker}(\chi).$$

Therefore T acts faithfully on V if and only if the weights generate $X^*(T)$ (by I, 14.12).

We wish to understand the Borel and parabolic subgroups in terms of root systems. We first state a weak result.

THEOREM 4.1 *Let G be a connected reductive group, T a maximal torus in G , and (V, R) the corresponding root system (so $V = \mathbb{R} \otimes_{\mathbb{Q}} Q$ where Q is the \mathbb{Z} -module generated by R).*

(a) *The Borel subgroups of G containing T are in one-to-one correspondence with the bases of R .*

(b) *Let B be the Borel subgroup of G corresponding to a base S for R . The number of parabolic subgroups of G containing B is $2^{|S|}$.*

We examine this statement for $G = \text{GL}_V$. Let $n = \dim V$.

4.2 *The maximal tori of G are in natural one-to-one correspondence with the decompositions of V into a direct sum $V = \bigoplus_{j \in J} V_j$ of one-dimensional subspaces.*

Let T be a maximal torus of GL_V . As the weights of T in V generate $X^*(T)$, there are n of them, and so each weight space has dimension one. Conversely, given a decomposition $V = \bigoplus_{j \in J} V_j$ of V into one-dimensional subspaces, we take T to be the subgroup of g such that $gV_j \subset V_j$ for all j .

Now fix a maximal torus T in G , and let $V = \bigoplus_{j \in J} V_j$ be the corresponding weight decomposition of V .

4.3 *The Borel subgroups of G containing T are in natural one-to-one correspondence with the orderings of J .*

The Borel subgroups of V are the stabilizers of maximal flags

$$F: V = W_n \supset W_{n-1} \supset \dots$$

If T stabilizes F , then each W_r is a direct sum of eigenspaces for T , but the V_j are the only eigenspaces, and so W_r is a direct sum of r of the V_j 's. Therefore, from F we obtain a unique ordering $j_n > \dots > j_1$ of J such that $W_r = \bigoplus_{i \leq r} V_{j_i}$. Conversely, given an ordering of J we can use this formula to define a maximal flag.

4.4 *The bases for R are in natural one-to-one correspondence with the orderings of J .*

The vector space V has basis $(\chi_j)_{j \in J}$, and $R = \{\chi_i - \chi_j \mid i \neq j\}$. Recall that to define a base, we choose a $t \in V^\vee$ that is not orthogonal to any root, and let S be the set of indecomposable elements in $R^+ = \{\chi_i - \chi_j \mid \langle \chi_i - \chi_j, t \rangle > 0\}$. Clearly, specifying R^+ in this way amounts to choosing an ordering on J .¹¹

4.5 *Fix a Borel subgroup B of G containing T , and hence a base S for R . The parabolic subgroups containing B are in one-to-one correspondence with the subsets of S .*

Having fixed a Borel subgroup, we have an ordering of J , and so we may as well write $J = \{1, 2, \dots, n\}$. From a sequence a_1, \dots, a_r of positive integers with sum n , we get a parabolic subgroup, namely, the stabilizer of the flag

$$V \supset V_r \supset \dots \supset V_1 \supset 0$$

with $V_j = \bigoplus_{i \leq a_1 + \dots + a_j} V_i$. Since the number of such sequences¹² is 2^{n-1} , the theorem implies that this is a complete list of parabolic subgroups.

¹¹Let $(f_i)_{i \in I}$ be the dual basis to $(\chi_i)_{i \in I}$. We can take t to be any vector $\sum a_i f_i$ with the a_i distinct. Then R^+ depends only on ordering of the a_i (relative to the natural order on \mathbb{R}), and it determines this ordering.

¹²Such sequences correspond to functions $\mu: \{1, \dots, n\} \rightarrow \{0, 1\}$ with $\mu(0) = 1$ — the a_i are the lengths of the strings of zeros or ones.

4a Lie algebras

Recall that \mathfrak{sl}_2 consists of the 2×2 matrices with trace zero, and that for the basis

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

and

$$[x, y] = h, \quad [h, x] = 2x, \quad [h, y] = -2y.$$

A Lie algebra \mathfrak{g} is said to be **reductive** if it is the direct sum of a commutative Lie algebra and a semisimple Lie algebra. Let \mathfrak{h} be a maximal subalgebra consisting of elements x such that $\text{ad } x$ is semisimple. Then

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$$

where \mathfrak{g}_0 is the subspace of \mathfrak{g} on which \mathfrak{h} acts trivially, and \mathfrak{g}_α is the subspace on which \mathfrak{h} acts through the nonzero linear form α . The α occurring in the decomposition are called the **roots** of \mathfrak{g} (relative to \mathfrak{h}).

THEOREM 4.6 For each $\alpha \in R$, the spaces \mathfrak{g}_α and $\mathfrak{h}_\alpha \stackrel{\text{def}}{=} [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}]$ are one-dimensional. There is a unique element $h_\alpha \in \mathfrak{h}_\alpha$ such that $\alpha(h_\alpha) = 2$. For each nonzero element $x_\alpha \in X_\alpha$, there exists a unique y_α such that

$$[x_\alpha, y_\alpha] = h_\alpha, \quad [h_\alpha, x_\alpha] = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -2y_\alpha.$$

Hence $\mathfrak{g}_\alpha = \mathfrak{g}_{-\alpha} \oplus \mathfrak{h}_\alpha \oplus \mathfrak{g}_\alpha$ is isomorphic to \mathfrak{sl}_2 .

PROOF. See Serre 1987, Chapter VI. □

4b Algebraic groups

Let G be a reductive group containing a split maximal torus T . Let $\text{Lie}(G, T) = (\mathfrak{g}, \mathfrak{h})$. Then

$$\text{Hom}_{k\text{-lin}}(\mathfrak{h}, k) \simeq k \otimes_{\mathbb{Z}} X^*(T)$$

(II, 1.24), and so each $\alpha \in R$ defines a linear form α' on \mathfrak{h} . It can be shown that these are the roots of \mathfrak{g} . Every vector space W defines an algebraic group $R \mapsto R \otimes_k W$ (considered as a group under addition).

THEOREM 4.7 For each $\alpha \in R$ there is a unique homomorphism $\exp_\alpha: \mathfrak{g}_\alpha \rightarrow G$ of algebraic groups such that

$$t \exp_\alpha(x) t^{-1} = \exp(\alpha(t)x) \\ \text{Lie}(\exp_\alpha) = (\mathfrak{g}_\alpha \hookrightarrow \mathfrak{g}).$$

PROOF. Omitted. □

EXAMPLE 4.8 Let $G = \text{GL}_n$, and let $\alpha = \alpha_{ij}$. Then

$$\exp_\alpha(x) = \sum (xE_{ij})^n / n! \\ = I + xE_{ij}$$

where E_{ij} is the matrix with 1 in the (i, j) -position, and zeros elsewhere.

Let U_α denote the image of \exp_α .

THEOREM 4.9 *For any base S for R , the subgroup of G generated by T and the U_α for $\alpha \in R^+$ is a Borel subgroup of G , and all Borel subgroups of G containing T arise in this way from a unique base. The base corresponding to B is that for which*

$$R^+ = \{\alpha \in R \mid U_\alpha \in B\}$$

is the set of positive roots (so S is the set of indecomposable elements in R^+).

PROOF. Omitted. □

THEOREM 4.10 *Let S be a base for R and let B be the corresponding Borel subgroup. For each subset I of R , there is a unique parabolic subgroup P containing B such that*

$$U_{-\alpha} \subset P \iff \alpha \in I.$$

PROOF. Omitted. □

For example, the parabolic subgroup corresponding to the subset

$$\{\chi_1 - \chi_2, \chi_2 - \chi_3, \chi_4 - \chi_5\}$$

of the simple roots of GL_5 is

$$\left\{ \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \end{pmatrix} \right\}.$$

5 Root data and their classification

NOTES No algebraic groups in this section — only combinatorics. Need to rewrite this section to remove overlap with III, §1. Then, include complete proofs assuming the results from that section.

5a Generalities

The following is the standard definition.

DEFINITION 5.1 A root datum is an ordered quadruple $\Psi = (X, R, X^\vee, R^\vee)$ where

- ◇ X, X^\vee are free \mathbb{Z} -modules of finite rank in duality by a pairing $\langle \cdot, \cdot \rangle: X \times X^\vee \rightarrow \mathbb{Z}$,
- ◇ R, R^\vee are finite subsets of X and X^\vee in bijection by a correspondence $\alpha \leftrightarrow \alpha^\vee$,

satisfying the following conditions

RD1 $\langle \alpha, \alpha^\vee \rangle = 2,$

RD2 $s_\alpha(R) \subset R, s_\alpha^\vee(R^\vee) \subset R^\vee$, where

$$\begin{aligned} s_\alpha(x) &= x - \langle x, \alpha^\vee \rangle \alpha, & \text{for } x \in X, \alpha \in R, \\ s_\alpha^\vee(y) &= y - \langle \alpha, y \rangle \alpha^\vee, & \text{for } y \in X^\vee, \alpha \in R. \end{aligned}$$

Recall that RD1 implies that $s_\alpha(\alpha) = -\alpha$ and $s_\alpha^2 = 1$.

Set¹³

$$\begin{aligned} Q &= \mathbb{Z}R \subset X & Q^\vee &= \mathbb{Z}R^\vee \subset X^\vee \\ V &= \mathbb{Q} \otimes_{\mathbb{Z}} Q & V^\vee &= \mathbb{Q} \otimes_{\mathbb{Z}} Q^\vee. \\ X_0 &= \{x \in X \mid \langle x, R^\vee \rangle = 0\} \end{aligned}$$

By $\mathbb{Z}R$ we mean the \mathbb{Z} -submodule of X generated by the $\alpha \in R$.

LEMMA 5.2 For $\alpha \in R, x \in X$, and $y \in X^\vee$,

$$\langle s_\alpha(x), y \rangle = \langle x, s_\alpha^\vee(y) \rangle, \quad (173)$$

and so

$$\langle s_\alpha(x), s_\alpha^\vee(y) \rangle = \langle x, y \rangle. \quad (174)$$

PROOF. We have

$$\begin{aligned} \langle s_\alpha(x), y \rangle &= \langle x - \langle x, \alpha^\vee \rangle \alpha, y \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle \\ \langle x, s_\alpha^\vee(y) \rangle &= \langle x, y - \langle \alpha, y \rangle \alpha^\vee \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle, \end{aligned}$$

which gives the first formula, and the second is obtained from the first by replacing y with $s_\alpha^\vee(y)$. \square

In other words, as the notation suggests, s_α^\vee (which is sometimes denoted s_{α^\vee}) is the transpose of s_α .

LEMMA 5.3 The following hold for the mapping

$$p: X \rightarrow X^\vee, \quad p(x) = \sum_{\alpha \in R} \langle x, \alpha^\vee \rangle \alpha^\vee.$$

(a) For all $x \in X$,

$$\langle x, p(x) \rangle = \sum_{\alpha \in R} \langle x, \alpha^\vee \rangle^2 \geq 0, \quad (175)$$

with strict inequality holding if $x \in R$.

(b) For all $x \in X$ and $w \in W$,

$$\langle wx, p(wx) \rangle = \langle x, p(x) \rangle. \quad (176)$$

(c) For all $\alpha \in R$,

$$\langle \alpha, p(\alpha) \rangle \alpha^\vee = 2p(\alpha), \quad \text{all } \alpha \in R. \quad (177)$$

¹³The notation Q^\vee is a bit confusing, because Q^\vee is not in fact the dual of Q .

PROOF. (a) This is obvious.

(b) It suffices to check this for $w = s_\alpha$, but

$$\langle s_\alpha x, \alpha^\vee \rangle = \langle x, \alpha^\vee \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, \alpha^\vee \rangle = -\langle x, \alpha^\vee \rangle$$

and so each term on the right of (175) is unchanged if x with replaced with $s_\alpha x$.

(c) Recall that, for $y \in X^\vee$,

$$s_\alpha^\vee(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

On multiplying this by $\langle \alpha, y \rangle$ and re-arranging, we find that

$$\langle \alpha, y \rangle^2 \alpha^\vee = \langle \alpha, y \rangle y - \langle \alpha, y \rangle s_\alpha^\vee(y).$$

But

$$\begin{aligned} -\langle \alpha, y \rangle &= \langle s_\alpha(\alpha), y \rangle \\ &\stackrel{(173)}{=} \langle \alpha, s_\alpha^\vee(y) \rangle \end{aligned}$$

and so

$$\langle \alpha, y \rangle^2 \alpha^\vee = \langle \alpha, y \rangle y + \langle \alpha, s_\alpha^\vee(y) \rangle s_\alpha^\vee(y).$$

As y runs through the elements of R^\vee , so also does $s_\alpha^\vee(y)$, and so when we sum over $y \in R^\vee$, we obtain (177). \square

REMARK 5.4 Suppose $m\alpha$ is also a root. On replacing α with $m\alpha$ in (177) and using that p is a homomorphism of \mathbb{Z} -modules, we find that

$$m\langle \alpha, p(\alpha) \rangle (m\alpha)^\vee = 2p(\alpha), \quad \text{all } \alpha \in R.$$

Therefore,

$$(m\alpha)^\vee = m^{-1}\alpha^\vee. \quad (178)$$

In particular,

$$(-\alpha)^\vee = -(\alpha^\vee). \quad (179)$$

LEMMA 5.5 *The map $p: X \rightarrow X^\vee$ defines an isomorphism*

$$1 \otimes p: V \rightarrow V^\vee.$$

In particular, $\dim V = \dim V^\vee$.

PROOF. As $\langle \alpha, p(\alpha) \rangle \neq 0$, (177) shows that $p(Q)$ has finite index in Q^\vee . Therefore, when we tensor $p: Q \rightarrow Q^\vee$ with \mathbb{Q} , we get a surjective map $1 \otimes p: V \rightarrow V^\vee$; in particular, $\dim V \geq \dim V^\vee$. The definition of a root datum is symmetric between (X, R) and (X^\vee, R^\vee) , and so the symmetric argument shows that $\dim V^\vee \leq \dim V$. Hence

$$\dim V = \dim V^\vee,$$

and $1 \otimes p: V \rightarrow V^\vee$ is an isomorphism. \square

LEMMA 5.6 *The kernel of $p: X \rightarrow X^\vee$ is X_0 .*

PROOF. Clearly, $X_0 \subset \text{Ker}(p)$, but (175) proves the reverse inclusion. \square

PROPOSITION 5.7 *We have*

$$\begin{aligned} Q \cap X_0 &= 0 \\ Q + X_0 &\text{ is of finite index in } X. \end{aligned}$$

Thus, there is an exact sequence

$$0 \rightarrow Q \oplus X_0 \xrightarrow{(q,x) \mapsto q+x} X \rightarrow \text{finite group} \rightarrow 0.$$

PROOF. The map

$$1 \otimes p: \mathbb{Q} \otimes X \rightarrow V^\vee$$

has kernel $\mathbb{Q} \otimes X_0$ (see 5.6) and maps the subspace V of $\mathbb{Q} \otimes X$ isomorphically onto V^\vee (see 5.5). This implies that

$$(\mathbb{Q} \otimes_{\mathbb{Z}} X_0) \oplus V \simeq \mathbb{Q} \otimes X,$$

from which the proposition follows. \square

LEMMA 5.8 *The bilinear form $\langle \cdot, \cdot \rangle$ defines a nondegenerate pairing $V \times V^\vee \rightarrow \mathbb{Q}$.*

PROOF. Let $x \in X$. If $\langle x, \alpha^\vee \rangle = 0$ for all $\alpha^\vee \in R^\vee$, then $x \in \text{Ker}(p) = X_0$. \square

LEMMA 5.9 *For any $x \in X$ and $w \in W$, $w(x) - x \in Q$.*

PROOF. From (RD2),

$$s_\alpha(x) - x = -\langle x, \alpha^\vee \rangle \alpha \in Q.$$

Now

$$(s_{\alpha_1} \circ s_{\alpha_2})(x) - x = s_{\alpha_1}(s_{\alpha_2}(x) - x) + s_{\alpha_1}(x) - x \in Q,$$

and so on. \square

Recall that the Weyl group $W = W(\Psi)$ of Ψ is the subgroup of $\text{Aut}(X)$ generated by the s_α , $\alpha \in R$. We let $w \in W$ act on X^\vee as $(w^\vee)^{-1}$, i.e., so that

$$\langle wx, wy \rangle = \langle x, y \rangle, \quad \text{all } w \in W, x \in X, y \in X^\vee.$$

Note that this makes s_α act on X^\vee as $(s_\alpha^\vee)^{-1} = s_\alpha^\vee$ (see 173).

PROPOSITION 5.10 *The Weyl group W acts faithfully on R (and so is finite).*

PROOF. By symmetry, it is equivalent to show that W acts faithfully on R^\vee . Let w be an element of W such that $w(\alpha) = \alpha$ for all $\alpha \in R^\vee$. For any $x \in X$,

$$\begin{aligned} \langle w(x) - x, \alpha^\vee \rangle &= \langle w(x), \alpha^\vee \rangle - \langle x, \alpha^\vee \rangle \\ &= \langle x, w^{-1}(\alpha^\vee) \rangle - \langle x, \alpha^\vee \rangle \\ &= 0. \end{aligned}$$

Thus $w(x) - x$ is orthogonal to R^\vee . As it lies in Q (see 5.9), this implies that it is zero (5.8), and so $w = 1$. \square

Thus, a root datum in the sense of (5.1) is a root datum in the sense of (2.1), and the next proposition proves the converse.

PROPOSITION 5.11 *Let $\Psi = (X, R, X^\vee, R^\vee)$ be a system satisfying the conditions (rd1), (rd2), (rd3) of (2.1). Then Ψ is a root datum.*

PROOF. We have to show that

$$s_\alpha^\vee(R^\vee) \subset R^\vee \text{ where } s_\alpha^\vee(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

As in Lemma 5.2, $\langle s_\alpha(x), s_\alpha^\vee(y) \rangle = \langle x, y \rangle$.

Let $\alpha, \beta \in R$, and let $t = s_{s_\alpha(\beta)} s_\alpha s_\beta s_\alpha$. An easy calculation¹⁴ shows that

$$t(x) = x + (\langle x, s_\alpha^\vee(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle) s_\alpha(\beta), \quad \text{all } x \in X.$$

Since

$$\langle s_\alpha(\beta), s_\alpha^\vee(\beta^\vee) \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = \langle \beta, \beta^\vee \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = 2 - 2 = 0,$$

we see that $t(s_\alpha(\beta)) = s_\alpha(\beta)$. Thus,

$$(t - 1)^2 = 0,$$

and so the minimum polynomial of t acting on $\mathbb{Q} \otimes_{\mathbb{Z}} X$ divides $(T - 1)^2$. On the other hand, since t lies in a finite group, it has finite order, say $t^m = 1$. Thus, the minimum polynomial also divides $T^m - 1$, and so it divides

$$\gcd(T^m - 1, (T - 1)^2) = T - 1.$$

This shows that $t = 1$, and so

$$\langle x, s_\alpha^\vee(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle = 0 \text{ for all } x \in X.$$

Hence

$$s_\alpha^\vee(\beta^\vee) = s_\alpha(\beta)^\vee \in R^\vee. \quad \square$$

REMARK 5.12 To give a root datum amounts to giving a triple (X, R, f) where

- ◇ X is a free abelian group of finite rank,
- ◇ R is a finite subset of X , and
- ◇ f is an injective map $\alpha \mapsto \alpha^\vee$ from R into the dual X^\vee of X

satisfying the conditions (rd1), (rd2), (rd3) of (2.1).

¹⁴Or so it is stated in Springer 1979, 1.4.

5b Classification of semisimple root data

Throughout this section, F is a field of characteristic zero, for example $F = \mathbb{Q}, \mathbb{R},$ or \mathbb{C} . An *inner product* on a real vector space is a positive-definite symmetric bilinear form.

GENERALITIES ON SYMMETRIES

See III, §1a, p. 296.

GENERALITIES ON LATTICES

In this subsection V is a finite-dimensional vector space over F .

DEFINITION 5.13 A subgroup of V is a *lattice* in V if it can be generated (as a \mathbb{Z} -module) by a basis for V . Equivalently, a subgroup X is a lattice if the natural map $F \otimes_{\mathbb{Z}} X \rightarrow V$ is an isomorphism.

REMARK 5.14 (a) When $F = \mathbb{Q}$, every finitely generated subgroup of V that spans V is a lattice, but this is not true for $F = \mathbb{R}$ or \mathbb{C} . For example, $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ is not a lattice in \mathbb{R} .

(b) When $F = \mathbb{R}$, the discrete subgroups of V are the *partial lattices*, i.e., \mathbb{Z} -modules generated by an \mathbb{R} -linearly independent set of vectors for V (see my notes on algebraic number theory 4.13).

DEFINITION 5.15 A *perfect pairing* of free \mathbb{Z} -modules of finite rank is one that realizes each as the dual of the other. Equivalently, it is a pairing into \mathbb{Z} with discriminant ± 1 .

PROPOSITION 5.16 Let

$$\langle , \rangle : V \times V^\vee \rightarrow k$$

be a nondegenerate bilinear pairing, and let X be a lattice in V . Then

$$Y = \{y \in V^\vee \mid \langle X, y \rangle \subset \mathbb{Z}\}$$

is the unique lattice in V^\vee such that \langle , \rangle restricts to a perfect pairing

$$X \times Y \rightarrow \mathbb{Z}.$$

PROOF. Let e_1, \dots, e_n be a basis for V generating X , and let e'_1, \dots, e'_n be the dual basis. Then

$$Y = \mathbb{Z}e'_1 + \dots + \mathbb{Z}e'_n,$$

and so it is a lattice, and it is clear that \langle , \rangle restricts to a perfect pairing $X \times Y \rightarrow \mathbb{Z}$.

Let Y' be a second lattice in V^\vee such that $\langle x, y \rangle \in \mathbb{Z}$ for all $x \in X, y \in Y'$. Then $Y' \subset Y$, and an easy argument shows that the discriminant of the pairing $X \times Y' \rightarrow \mathbb{Z}$ is $\pm(Y:Y')$, and so the pairing on $X \times Y'$ is perfect if and only if $Y' = Y$. \square

ROOT SYSTEMS

See III, §1b, 297.

ROOT SYSTEMS AND SEMISIMPLE ROOT DATA

Compare (III, 1.3 and 5.12):

Semisimple root datum	Root system (over \mathbb{Q})
$X, R, \alpha \mapsto \alpha^\vee: R \hookrightarrow X^\vee$	V, R
R is finite	R is finite
$(X: \mathbb{Z}R)$ finite	R spans V
	$0 \notin R$
$\langle \alpha, \alpha^\vee \rangle = 2, s_\alpha(R) \subset R$	$\exists s_\alpha$ such that $s_\alpha(R) \subset R$
	$\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}, \text{ all } \alpha, \beta \in R$
Weyl group finite	

For a root system (V, R) , let $Q = \mathbb{Z}R$ be the \mathbb{Z} -submodule of V generated by R and let Q^\vee be the \mathbb{Z} -submodule of V^\vee generated by the $\alpha^\vee, \alpha \in R$. Then, Q and Q^\vee are lattices¹⁵ in V and V^\vee , and we let

$$P = \{x \in V \mid \langle x, Q^\vee \rangle \subset \mathbb{Z}\}.$$

Then P is a lattice in V (see 5.16), and because of (RS3),

$$Q \subset P. \tag{180}$$

PROPOSITION 5.17 *If $(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum, then $(\mathbb{Q} \otimes_{\mathbb{Z}} X, R)$ is a root system over \mathbb{Q} . Conversely, if (V, R) is root system over \mathbb{Q} , then for any choice X of a lattice in V such that*

$$Q \subset X \subset P \tag{181}$$

$(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum.

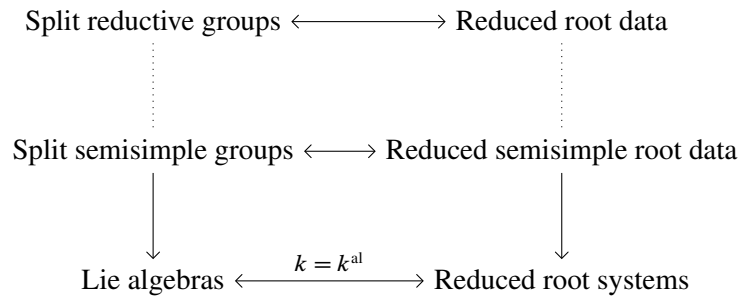
PROOF. If $(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum, then $0 \notin R$ because $\langle \alpha, \alpha^\vee \rangle = 2$, and $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$ because $\alpha^\vee \in X^\vee$. Therefore $(\mathbb{Q} \otimes_{\mathbb{Z}} X, R)$ is a root system.

Conversely, let (V, R) be a root system. Let X satisfy (181), and let X^\vee denote the lattice in V^\vee in duality with X (see 5.16). For each $\alpha \in R$, there exists an $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and $s_\alpha(R) \subset R$ (because (V, R) is a root datum); moreover, α^\vee is unique (see III, §1a). Therefore, we have a function $\alpha \mapsto \alpha^\vee: R \rightarrow V^\vee$ which takes its values in X^\vee (because $X \subset P$ implies $X^\vee \supset R^\vee$), and is injective. The Weyl group of $(X, R, \alpha \mapsto \alpha^\vee)$ is the Weyl group of (V, R) , which, as we noted above, is finite. Therefore $(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum. \square

THE BIG PICTURE

Recall that the base field k (for G) has characteristic zero.

¹⁵They are finitely generated, and Φ^\vee spans V^\vee by Serre 1987, p28.



5.18 As we discussed in §2, the reduced root data classify the split reductive groups over k .

5.19 As we discussed in (1.4), from a reductive group G , we get semisimple groups $\mathcal{D}G$ and $G/Z(G)$ together with an isogeny $\mathcal{D}G \rightarrow G/Z(G)$. Conversely, every reductive group G can be built up from a semisimple group and a torus (1.5).

5.20 As we discuss in the next section, the relation between reduced root data and reduced semisimple root data is the same as that between split reductive groups and split semisimple groups. It follows that to show that the reduced root data classify split reductive groups, it suffices to show that reduced semisimple root data classify split semisimple groups.

5.21 From a semisimple group G we get a semisimple Lie algebra $\text{Lie}(G)$ (see II, 5.23), and from $\text{Lie}(G)$ we can recover $G/Z(G)$ (see II, 5.30). Passing from G to $\text{Lie}(G)$ amounts to forgetting the centre of G .¹⁶

5.22 From a semisimple root datum $(X, R, \alpha \mapsto \alpha^\vee)$, we get a root system $(V = \mathbb{Q} \otimes_{\mathbb{Z}} X, R)$. Passing from the semisimple root datum to the root system amounts to forgetting the lattice X in V .

5.23 Take $k = k^{\text{al}}$, and let \mathfrak{g} be a semisimple Lie algebra over k . A *Cartan subalgebra* \mathfrak{h} of \mathfrak{g} is a commutative subalgebra that is equal to its own centralizer. For example, the algebra of diagonal matrices of trace zero in \mathfrak{sl}_n is a Cartan subalgebra. Then \mathfrak{h} acts on \mathfrak{g} via the adjoint map $\text{ad}: \mathfrak{h} \rightarrow \text{End}(\mathfrak{g})$, i.e., for $h \in \mathfrak{h}$, $x \in \mathfrak{g}$, $\text{ad}(h)(x) = [h, x]$. One shows that \mathfrak{g} decomposes as a sum

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \mathfrak{h}^\vee} \mathfrak{g}_\alpha$$

where \mathfrak{g}_0 is the subspace on which \mathfrak{h} acts trivially, and hence equals \mathfrak{h} , and \mathfrak{g}_α is the subspace on which \mathfrak{h} acts through the linear form $\alpha: \mathfrak{h} \rightarrow k$, i.e., for $h \in \mathfrak{h}$, $x \in \mathfrak{g}_\alpha$, $[h, x] = \alpha(h)x$. The nonzero α occurring in the above decomposition form a reduced root system R in \mathfrak{h}^\vee (and hence in the \mathbb{Q} -subspace of \mathfrak{h}^\vee spanned by R). In this way, the semisimple Lie algebras over k are classified by the reduced root systems (see III, §8).

¹⁶Perhaps this was accurate when first written, but, as we show in Chapter II??, it is possible to recover the centre also from $\text{Lie}(G)$ by looking at its representations.

CLASSIFICATION OF THE REDUCED ROOT SYSTEM

See Chapter III, Section 1.

6 Construction of split reductive groups: the existence theorem

We show that, for any field k , every root datum arises from a split reductive group over k .

NOTES Show first that it suffices to prove the result for root systems and semisimple groups. Discuss three proofs.

- (a) Construct a split almost simple group for each diagram, as in Chapter I. Only the exceptional case still requires work (from me).
- (b) In characteristic zero, construct the Lie algebra; get the semisimple group as in Chapter III. Then discuss Chevalley bases and explain how to get the groups over \mathbb{Z} , and hence over each prime field. Also take a look at the Tannakian point of view; perhaps look at the Tannakian category over \mathbb{Z} .
- (c) Directly — see Springer (Chapter 10, 10 pages) in the case that k is algebraically closed, and the notes at the end of his chapter. Better: do this directly of \mathbb{Z} .

6a Preliminaries on root data/systems

Recall (5.17) that semisimple root data (hence semisimple algebraic groups) correspond to reduced root systems (V, R) together with a choice of a lattice X ,

$$Q \subset X \subset P$$

where $Q = \mathbb{Z}R$ and P is the lattice in duality with $\mathbb{Z}R^\vee$. Thus

$$P = \{x \in V \mid \langle x, \alpha^\vee \rangle \in \mathbb{Z}, \quad \text{all } \alpha \in R\}.$$

When we take V to be a real vector space and choose an inner product as in (III, 1.9), this becomes

$$P = \left\{ x \in V \mid 2 \frac{\langle x, \alpha \rangle}{\langle \alpha, \alpha \rangle} \in \mathbb{Z}, \quad \text{all } \alpha \in R \right\}.$$

Choose a base $S = \{\alpha_1, \dots, \alpha_n\}$ for R (see III, 1.10). Then

$$Q = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n,$$

and we want to find a basis for P . Let $\{\lambda_1, \dots, \lambda_n\}$ be the basis of V dual to the basis

$$\left\{ \frac{2}{\langle \alpha_1, \alpha_1 \rangle} \alpha_1, \dots, \frac{2}{\langle \alpha_i, \alpha_i \rangle} \alpha_i, \dots, \frac{2}{\langle \alpha_n, \alpha_n \rangle} \alpha_n \right\},$$

i.e., $(\lambda_i)_{1 \leq i \leq n}$ is characterized by

$$2 \frac{\langle \lambda_i, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} = \delta_{ij} \quad (\text{Kronecker delta}).$$

PROPOSITION 6.1 *The set $\{\lambda_1, \dots, \lambda_n\}$ is a basis for P , i.e.,*

$$P = \mathbb{Z}\lambda_1 \oplus \dots \oplus \mathbb{Z}\lambda_n.$$

PROOF. Let $\lambda \in V$, and let

$$m_i = 2 \frac{(\lambda, \alpha_i)}{(\alpha_i, \alpha_i)}, i = 1, \dots, n.$$

Then

$$(\lambda - \sum m_i \lambda_i, \alpha) = 0$$

if $\alpha \in S$. Since S is a basis for V , this implies that $\lambda - \sum m_i \lambda_i = 0$ and

$$\lambda = \sum m_i \lambda_i = \sum 2 \frac{(\lambda, \alpha_i)}{(\alpha_i, \alpha_i)} \lambda_i.$$

Hence,

$$\lambda \in \bigoplus \mathbb{Z} \lambda_i \iff 2 \frac{(\lambda, \alpha_i)}{(\alpha_i, \alpha_i)} \in \mathbb{Z} \text{ for } i = 1, \dots, n,$$

and so $P \subset \bigoplus \mathbb{Z} \lambda_i$. The reverse inclusion follows from the next lemma. □

LEMMA 6.2 *Let R be a reduced root system, and let R' be the root system consisting of the vectors $\alpha' = \frac{2}{(\alpha, \alpha)} \alpha$ for $\alpha \in R$. For any base S for R , the set $S' = \{\alpha' \mid \alpha \in S\}$ is a base for R' .*

PROOF. See Serre 1987, V 9, Proposition 7. □

PROPOSITION 6.3 *For each j ,*

$$\alpha_j = \sum_{1 \leq i \leq n} 2 \frac{(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)} \lambda_i.$$

PROOF. This follows from the calculation in the above proof. □

Thus, we have

$$P = \bigoplus_i \mathbb{Z} \lambda_i \supset Q = \bigoplus_i \mathbb{Z} \alpha_i$$

and when we express the α_i in terms of the λ_i , the coefficients are the entries of the Cartan matrix. Replacing the λ_i 's and α_i 's with different bases amounts to multiplying the transition (Cartan) matrix on the left and right by invertible matrices. A standard algorithm allows us to obtain new bases for which the transition matrix is diagonal, and hence expresses P/Q as a direct sum of cyclic groups. When one does this, one obtains the following table:

A_n	B_n	C_n	D_n (n odd)	D_n (n even)	E_6	E_7	E_8	F_4	G_2
C_{n+1}	C_2	C_2	C_4	$C_2 \times C_2$	C_3	C_2	C_1	C_1	C_1

In the second row, C_m denotes a cyclic group of order m .

Also, by inverting the Cartan matrix one obtains an expression for the λ_i 's in terms of the α_i 's. Cf. Humphreys 1972, p. 69.

6b Brief review of diagonalizable groups

Recall from I, §14 that we have a (contravariant) equivalence $M \mapsto D(M)$ from the category of finitely generated abelian groups to the category of diagonalizable algebraic groups. For example, $D(\mathbb{Z}/m\mathbb{Z}) = \mu_m$ and $D(\mathbb{Z}) = \mathbb{G}_m$. A quasi-inverse is provided by

$$D \mapsto X(D) \stackrel{\text{def}}{=} \text{Hom}(D, \mathbb{G}_m).$$

Moreover, these functors are exact. For example, an exact sequence

$$0 \rightarrow D' \rightarrow D \xrightarrow{\pi} D'' \rightarrow 0$$

of diagonalizable groups corresponds to an exact sequence

$$0 \rightarrow X(D'') \rightarrow X(D) \rightarrow X(D') \rightarrow 0$$

of abelian groups. Under this correspondence,

$$D' = \text{Ker}(D \rightarrow D'') \xrightarrow{\chi} \prod_{\chi \in X(D'')} \mathbb{G}_m$$

i.e.,

$$D' = \bigcap_{\chi \in X(D'')} \text{Ker}(D \xrightarrow{\pi \circ \chi} \mathbb{G}_m). \tag{182}$$

6c Construction of all almost-simple split semisimple groups

Recall that the indecomposable reduced root systems are classified by the Dynkin diagrams, and that from the Dynkin diagram we can read off the Cartan matrix, and hence the group P/Q .

THEOREM 6.4 *For each indecomposable reduced Dynkin diagram, there exists an algebraic group G , unique up to isomorphism, with the given diagram as its Dynkin diagram and equipped with an isomorphism $X(ZG) \simeq P/Q$.*

For each diagram, one can simply write down the corresponding group. For example, for A_n it is SL_{n+1} and for C_n it Sp_{2n} . For B_n and D_n one tries SO_{2n+1} and SO_{2n} (as defined in 1.9), but their centres are too small. In fact the centre of O_m is $\pm I$, and so SO_{2n+1} has trivial centre and O_{2n} has centre of order 2. The group one needs is the corresponding spin group (see I, §18). The exceptional groups can be found, for example, in Springer 1998.

The difficult part in the above theorem is the uniqueness. Also, one needs to know that the remaining groups with the same Dynkin diagram are quotients of the one given by the theorem (which has the largest centre, and is said to be *simply connected*).

Here is how to obtain the group $G(X)$ corresponding to a lattice X ,

$$P \supset X \supset Q.$$

As noted earlier ((172), p. 347), the centre of $G(X)$ has character group X/Q , so, for example, the group corresponding to P is the simply connected group G . The quotient of G by

$$N = \bigcap_{\chi \in X/Q} \text{Ker}(\chi: Z(G) \rightarrow \mathbb{G}_m)$$

has centre with character group X/Q (cf. (182), p. 376), and is $G(X)$.

It should be noted that, because of the existence of outer automorphisms, it may happen that $G(X)$ is isomorphic to $G(X')$ with $X \neq X'$.

6d Split semisimple groups.

These are all obtained by taking a finite product of split simply connected semisimple groups and dividing out by a subgroup of the centre (which is the product of the centres of the factor groups).

6e Split reductive groups

Let G' be a split semisimple group, D a diagonalizable group, and $Z(G') \rightarrow D$ a homomorphism from $Z(G')$ to D . Define G to be the quotient

$$Z(G') \rightarrow G' \times D \rightarrow G \rightarrow 1.$$

All split reductive groups arise in this fashion (1.4).

ASIDE 6.5 With only minor changes, the above description works over fields of nonzero characteristic.

6f Exercise

EXERCISE 6-1 Assuming Theorem 6.4, show that the split reductive groups correspond exactly to the reduced root data.

7 Construction of isogenies of split reductive groups: the isogeny theorem

In this section we (shall) rewrite Steinberg 1999 for split reductive groups over arbitrary fields.

Let (G, T) be a split reductive group, and let $R \subset X(T)$ be the root system of (G, T) . For each $\alpha \in R$, let U_α be the corresponding root group. Recall that this means that $U_\alpha \approx \mathbb{G}_a$ and, for any isomorphism $u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$,

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \quad t \in T(k), a \in k.$$

DEFINITION 7.1 An *isogeny* of root data is a homomorphism $\varphi: X' \rightarrow X$ such that

- (a) both φ and φ^\vee are injective (equivalently, φ is injective with finite cokernel);
- (b) there exists a bijection $\alpha \mapsto \alpha'$ from R to R' and positive integers $q(\alpha)$, each an integral power of the characteristic exponent p of k , such that $\varphi(\alpha') = q(\alpha)\alpha$ and $\varphi^\vee(\alpha^\vee) = q(\alpha)(\alpha')^\vee$ for all $\alpha \in R$.

Let $f: (G, T) \rightarrow (G', T')$ be an isogeny of split reductive groups. This defines a homomorphism $\varphi: X' \rightarrow X$ of character groups:

$$\varphi(\chi') = \chi' \circ f|_T \text{ for all } \chi' \in X'.$$

Moreover, for each $\alpha \in R$, $f(U_\alpha) = U_{\alpha'}$ for some $\alpha' \in R'$.

PROPOSITION 7.2 Let $f: (G, T) \rightarrow (G', T')$ be an isogeny. Then the associated map $\varphi: X' \rightarrow X$ is an isogeny. Moreover, for each $\alpha \in R$,

$$f(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q(\alpha)})$$

for some $q(\alpha)$ as in (b), some $c_\alpha \in k^\times$, and all $a \in k$.

Thus, an isogeny $(G, T) \rightarrow (G', T')$ defines an isogeny of root data. The isogeny of root data does not determine f , because an inner automorphism of (G, T) defined by an element of $T(k)$ induces the identity map on the root datum of (G, T) . However, as the next lemma shows, this is the only indeterminacy.

LEMMA 7.3 *If two isogenies $(G, T) \rightarrow (G', T')$ induce the same map on the root data, then they differ by an inner automorphism by an element of $(T/Z)(k)$.*

PROOF. Let f and g be such isogenies. Then they agree on T obviously. Let S be a base for R . For each $\alpha \in S$, it follows from $\varphi(\alpha') = q(\alpha)\alpha$ that $f(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q(\alpha)})$, and similarly for g with c_α replaced by d_α . As S is linearly independent, there exists a $t \in T$ such $a(t)^{q(\alpha)} = d_\alpha c_\alpha^{-1}$ for all $\alpha \in S$. Let $h = f \circ i_t$ where i_t is the inner automorphism of G defined by t . Then g and h agree on every U_α , $\alpha \in S$, as well as on T , and hence also on the Borel subgroup B that these groups generate. It follows that they agree on G because the map $xB \mapsto h(x)g(x)^{-1}: G/B \rightarrow G'$ must be constant (the variety G/B is complete and G' is affine). As $h(e)g(e)^{-1} = 1$, we see that $h(x) = g(x)$ for all x . \square

THEOREM 7.4 (Isogeny theorem). *Let (G, T) and (G', T') be split reductive algebraic groups over a field k , and let $\varphi: X(T') \rightarrow X(T)$ be an isogeny of their root data. Then there exists an isogeny $f: (G, T) \rightarrow (G', T')$ inducing φ .*

THEOREM 7.5 *Let (G, T) and (G', T') be split reductive algebraic groups over a field k , and let $f_T: T \rightarrow T'$ be an isogeny. Then f_T extends to an isogeny $f: G \rightarrow G'$ if and only if $X(f_T)$ is an isogeny of root data.*

THEOREM 7.6 (Isomorphism theorem). *Let (G, T) and (G', T') be split reductive algebraic groups over a field k . An isomorphism $f: (G, T) \rightarrow (G', T')$ defines an isomorphism of root data, and every isomorphism of root data arises from an isomorphism f , which is uniquely determined up to an inner automorphism by an element of $T(k)$.*

Immediate consequence of the isogeny theorem. The key point is that an isogeny $f: G \rightarrow G'$ that induces the identity map on root data is an isomorphism. The first step is that it is an isomorphism $T \rightarrow T'$.

To be continued.

8 Representations of split reductive groups

Throughout this section, k is algebraically closed of characteristic zero (get rid of that).

NOTES This needs to be rewritten for split reductive groups over arbitrary fields.

8a The dominant weights of a root datum

Let (X, R, X^\vee, R^\vee) be a root datum. We make the following definitions:

- ◇ $Q = \mathbb{Z}R$ (**root lattice**) is the \mathbb{Z} -submodule of X generated by the roots;
- ◇ $X_0 = \{x \in X \mid \langle x, \alpha^\vee \rangle = 0 \text{ for all } \alpha \in R\}$;
- ◇ $V = \mathbb{R} \otimes_{\mathbb{Z}} Q \subset \mathbb{R} \otimes_{\mathbb{Z}} X$;

- ◇ $P = \{\lambda \in V \mid \langle \lambda, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}$ (*weight lattice*).

Now choose a base $S = \{\alpha_1, \dots, \alpha_n\}$ for R , so that:

- ◇ $R = R^+ \sqcup R^-$ where $R^+ = \{\sum m_i \alpha_i \mid m_i \geq 0\}$ and $R^- = \{\sum m_i \alpha_i \mid m_i \leq 0\}$;
- ◇ $Q = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n \subset V = \mathbb{R}\alpha_1 \oplus \dots \oplus \mathbb{R}\alpha_n$,
- ◇ $P = \mathbb{Z}\lambda_1 \oplus \dots \oplus \mathbb{Z}\lambda_n$ where λ_i is defined by $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{ij}$.

The λ_i are called the *fundamental (dominant) weights*. Define

- ◇ $P^+ = \{\lambda \in P \mid \langle \lambda, \alpha^\vee \rangle \geq 0 \text{ all } \alpha \in R^\vee\}$.

An element λ of X is *dominant* if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in R^+$. Such a λ can be written uniquely

$$\lambda = \sum_{1 \leq i \leq n} m_i \lambda_i + \lambda_0 \quad (183)$$

with $m_i \in \mathbb{N}$, $\sum m_i \lambda_i \in X$, and $\lambda_0 \in X_0$.

8b The dominant weights of a semisimple root datum

Recall (5.17) that to give a semisimple root datum amounts to giving a root system (V, R) and a lattice X ,

$$P \supset X \supset Q.$$

Choose an inner product $(,)$ on V for which the s_α act as orthogonal transformations (I, 1.9). Then, for $\lambda \in V$

$$\langle \lambda, \alpha^\vee \rangle = 2 \frac{(\lambda, \alpha)}{(\alpha, \alpha)}.$$

Since in this case $X_0 = 0$, the above definitions become:

- ◇ $Q = \mathbb{Z}R = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$,
- ◇ $P = \{\lambda \in V \mid 2 \frac{(\lambda, \alpha)}{(\alpha, \alpha)} \in \mathbb{Z} \text{ all } \alpha \in R\} = \mathbb{Z}\lambda_1 \oplus \dots \oplus \mathbb{Z}\lambda_n$ where λ_i is defined by

$$2 \frac{(\lambda_i, \alpha)}{(\alpha, \alpha)} = \delta_{ij}.$$

- ◇ $P^+ = \{\lambda = \sum_i m_i \lambda_i \mid m_i \geq 0\} = \{\text{dominant weights}\}$.

8c The classification of representations

Let G be a reductive group. We choose a maximal torus T and a Borel subgroup B containing T (hence, we get a root datum (X, R, X^\vee, R^\vee) and a base S for R). As every representation of G is (uniquely) a sum of simple representations (II, 6.14), we only need to classify them.

THEOREM 8.1 *Let $r: G \rightarrow \text{GL}_W$ be a simple representation of G .*

- (a) *There exists a unique one-dimensional subspace L of W stabilized by B .*
- (b) *The L in (a) is a weight space for T , say, $L = W_{\lambda_r}$.*
- (c) *The λ_r in (b) is dominant.*
- (d) *If λ is also a weight for T in W , then $\lambda = \lambda_r - \sum m_i \alpha_i$ with $m_i \in \mathbb{N}$.*

PROOF. Omitted. □

Note that the Lie-Kolchin theorem (I, 16.31) implies that there does exist a one-dimensional eigenspace for B — the content of (a) is that when W is simple (as a representation of G), the space is unique. Since L is mapped into itself by B , it is also mapped into itself by T , and so lies in a weight space. The content of (b) is that it is the whole weight space. Because of (d), λ_r is called the **highest weight** of the simple representation r .

THEOREM 8.2 *The map $(W, r) \mapsto \lambda_r$ defines a bijection from the set of isomorphism classes of simple representations of G onto the set of dominant weights in $X = X^*(T)$.*

PROOF. Omitted. □

8d Example:

Here the root datum is isomorphic to $\{\mathbb{Z}, \{\pm 2\}, \mathbb{Z}, \{\pm 1\}\}$. Hence $Q = 2\mathbb{Z}$, $P = \mathbb{Z}$, and $P^+ = \mathbb{N}$. Therefore, there is (up to isomorphism) exactly one simple representation for each $m \geq 0$. There is a natural action of $\mathrm{SL}_2(k)$ on the ring $k[X, Y]$, namely, let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} aX + bY \\ cX + dY \end{pmatrix}.$$

In other words,

$$f^A(X, Y) = f(aX + bY, cX + dY).$$

This is a right action, i.e., $(f^A)^B = f^{AB}$. We turn it into a left action by setting $Af = f^{A^{-1}}$. Then one can show that the representation of SL_2 on the homogeneous polynomials of degree m is simple, and every simple representation is isomorphic to exactly one of these.

8e Example: GL_n

As usual, let T be \mathbb{D}_n , and let B be the standard Borel subgroup. The characters of T are χ_1, \dots, χ_n . Note that GL_n has representations

$$\mathrm{GL}_n \xrightarrow{\det} \mathbb{G}_m \xrightarrow{t \mapsto t^m} \mathrm{GL}_1 = \mathbb{G}_m$$

for each m , and that any representation can be tensored with this one. Thus, given any simple representation of GL_n we can shift its weights by any integer multiple of $\chi_1 + \dots + \chi_n$.

In this case, the simple roots are $\chi_1 - \chi_2, \dots, \chi_{n-1} - \chi_n$, and the root datum is isomorphic to

$$(\mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}, \mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}).$$

In this notation the simple roots are $e_1 - e_2, \dots, e_{n-1} - e_n$, and the fundamental dominant weights are $\lambda_1, \dots, \lambda_{n-1}$ with

$$\lambda_i = e_1 + \dots + e_i - n^{-1}i(e_1 + \dots + e_n).$$

The dominant weights are the expressions

$$a_1\lambda_1 + \dots + a_{n-1}\lambda_{n-1} + m(e_1 + \dots + e_n), \quad a_i \in \mathbb{N}, \quad m \in \mathbb{Z}.$$

These are the expressions

$$m_1e_1 + \dots + m_n e_n$$

where the m_i are integers with $m_1 \geq \dots \geq m_n$. The simple representation with highest weight e_1 is the representation of GL_n on k^n (obviously), and the simple representation with highest weight $e_1 + \dots + e_i$ is the representation on $\bigwedge^i(k^n)$ (Springer 1998, 4.6.2).

8f Example: SL_n

Let T_1 be the diagonal in SL_n . Then $X^*(T_1) = X^*(T)/\mathbb{Z}(\chi_1 + \cdots + \chi_n)$ with $T = \mathbb{D}_n$. The root datum for SL_n is isomorphic to $(\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n), \{\varepsilon_i - \varepsilon_j \mid i \neq j\}, \dots)$ where ε_i is the image of e_i in $\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n)$. It follows from the GL_n case that the fundamental dominant weights are $\lambda_1, \dots, \lambda_{n-1}$ with

$$\lambda_i = \varepsilon_1 + \cdots + \varepsilon_i.$$

Again, the simple representation with highest weight ε_1 is the representation of SL_n on k^n , and the simple representation with highest weight $\varepsilon_1 + \cdots + \varepsilon_i$ is the representation SL_n on $\bigwedge^i(k^n)$ (ibid.).

ASIDE 8.3 Including pinnings (épinglages) — cf. mo17594.

The Structure of Reductive Groups: general case

In this chapter, we study algebraic groups, especially nonsplit reductive groups, over arbitrary fields.

The algebraic groups over a field k that become isomorphic to a fixed algebraic group over k^{al} are classified by a certain cohomology group. In the first section, we explain this, and discuss what is known about the cohomology groups.

Over an algebraically closed field, the classical semisimple groups are exactly those described by central simple algebras equipped with an involution. In the second section, we show that this remains true over an arbitrary field, roughly speaking, because the two are classified by the same cohomology groups [this has been moved to Chapter I]

Root data are also important in the nonsplit case. For a reductive group G , one chooses a torus that is maximal among those that are split, and defines the root datum much as before — in this case it is not necessarily reduced. This is an important approach to describing arbitrary algebraic groups, but clearly it yields no information about anisotropic groups (those with no split torus). We explain this approach in the third section.

In this version of the chapter, we usually assume that k has characteristic zero. Let A be a set with an equivalence relation \sim , and let B be a second set. When there exists a canonical surjection $A \rightarrow B$ whose fibres are the equivalence classes, I say that B *classifies* the \sim -classes of elements of A .

NOTES This chapter is in disarray, since I moved part of it to Chapter I. Probably it should be split into two parts, one on the cohomology of algebraic groups and one on the Tits-Selbach classification of reductive groups and their representations over arbitrary fields.

1	The cohomology of algebraic groups; applications	384
2	Classical groups and algebras with involution	394
3	Relative root systems and the anisotropic kernel.	395

EXAMPLE: THE FORMS OF GL_2 .

What are the groups G over a field k such that $G_{k^{\text{al}}} \approx GL_2$? For any $a, b \in k^\times$, define $\mathbb{H}(a, b)$ to be the algebra over k with basis $1, i, j, ij$ as a k -vector space, and with the

multiplication given by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

This is a k -algebra with centre k , and it is either a division algebra or is isomorphic to $M_2(k)$. For example, $\mathbb{H}(1, 1) \approx M_2(k)$ and $\mathbb{H}(-1, -1)$ is the usual quaternion algebra when $k = \mathbb{R}$.

Each algebra $\mathbb{H}(a, b)$ defines an algebraic group $G = G(a, b)$ with $G(R) = (R \otimes \mathbb{H}(a, b))^\times$. These are exactly the algebraic groups over k becoming isomorphic to GL_2 over k^{al} , and

$$G(a, b) \approx G(a', b') \iff \mathbb{H}(a, b) \approx \mathbb{H}(a', b').$$

Over \mathbb{R} , every \mathbb{H} is isomorphic to $\mathbb{H}(-1, -1)$ or $M_2(\mathbb{R})$, and so there are exactly two forms of GL_2 over \mathbb{R} .

Over \mathbb{Q} , the isomorphism classes of \mathbb{H} 's are classified by the subsets of

$$\{2, 3, 5, 7, 11, 13, \dots, \infty\}$$

having a finite even number of elements. The proof of this uses the quadratic reciprocity law in number theory. In particular, there are infinitely many forms of GL_2 over \mathbb{Q} , exactly one of which, GL_2 , is split.

1 The cohomology of algebraic groups; applications

Throughout this section, vector spaces and modules are finitely generated. In the early part of the section, there is no need to assume k to be of characteristic zero.

1a Non-commutative cohomology.

Let Γ be a group. A Γ -set is a set A with an action

$$(\sigma, a) \mapsto \sigma a: \Gamma \times A \rightarrow A$$

of Γ on A (so $(\sigma\tau)a = \sigma(\tau a)$ and $1a = a$). If, in addition, A has the structure of a group and the action of Γ respects this structure (i.e., $\sigma(aa') = \sigma a \cdot \sigma a'$), then we say A is a Γ -group.

DEFINITION OF $H^0(\Gamma, A)$

For a Γ -set A , $H^0(\Gamma, A)$ is defined to be the set A^Γ of elements left fixed by the operation of Γ on A , i.e.,

$$H^0(\Gamma, A) = A^\Gamma = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in \Gamma\}.$$

If A is a Γ -group, then $H^0(\Gamma, A)$ is a group.

DEFINITION OF $H^1(\Gamma, A)$

Let A be a Γ -group. A mapping $\sigma \mapsto a_\sigma$ of Γ into A is said to be a 1-cocycle of Γ in A if the relation $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ holds for all $\sigma, \tau \in \Gamma$. Two 1-cocycles (a_σ) and (b_σ) are said to be *equivalent* if there exists a $c \in A$ such that

$$b_\sigma = c^{-1} \cdot a_\sigma \cdot \sigma c \quad \text{for all } \sigma \in \Gamma.$$

This is an equivalence relation on the set of 1-cocycles of Γ in A , and $H^1(\Gamma, A)$ is defined to be the set of equivalence classes of 1-cocycles.

In general $H^1(\Gamma, A)$ is not a group unless A is commutative, but it has a distinguished element, namely, the class of 1-cocycles of the form $\sigma \mapsto b^{-1} \cdot \sigma b$, $b \in A$ (the *principal 1-cocycles*).

COMPATIBLE HOMOMORPHISMS

Let Δ be a second group. Let A be Γ -group and B an Δ -group. Two homomorphisms $f: A \rightarrow B$ and $g: \Delta \rightarrow \Gamma$ are said to be *compatible* if

$$f(g(\sigma)a) = \sigma(f(a)) \text{ for all } \sigma \in \Delta, a \in A.$$

If (a_σ) is a 1-cocycle for A , then

$$b_\sigma = f(a_{g(\sigma)})$$

is a 1-cocycle of Δ in B , and this defines a mapping $H^1(\Gamma, A) \rightarrow H^1(\Delta, B)$, which is a homomorphism if A and B are commutative.

When $\Delta = \Gamma$, a homomorphism $f: A \rightarrow B$ compatible with the identity map, i.e., such that

$$f(\sigma a) = \sigma(f(a)) \text{ for all } \sigma \in \Gamma, a \in A,$$

f is said to be a Γ -*homomorphism* (or be Γ -*equivariant*).

EXACT SEQUENCES

PROPOSITION 1.1 *An exact sequence*

$$1 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 1$$

of Γ -groups gives rise to an exact sequence of cohomology sets

$$1 \rightarrow H^0(\Gamma, A') \rightarrow H^0(\Gamma, A) \rightarrow H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A') \rightarrow H^1(\Gamma, A) \rightarrow H^1(\Gamma, A'')$$

Exactness at $H^0(\Gamma, A'')$ means that the fibres of the map $H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A')$ are the orbits of the group $H^0(\Gamma, A)$ acting on $H^0(\Gamma, A'')$. Exactness at $H^1(\Gamma, A')$ means that fibre of $H^1(\Gamma, A') \rightarrow H^1(\Gamma, A)$ over the distinguished element is the image of $H^0(\Gamma, A'')$.

We now define the boundary map $H^0(\Gamma, A'') \rightarrow H^1(\Gamma, A')$. For simplicity, regard A' as a subgroup of A with quotient A'' . Let a'' be an element of A'' fixed by Γ , and choose an a in A mapping to it. Because a'' is fixed by Γ , $a^{-1} \cdot \sigma a$ is an element of A' , which we denote a_σ . The map $\sigma \mapsto a_\sigma$ is a 1-cocycle whose class in $H^1(\Gamma, A')$ is independent of the choice of a . To define the remaining maps and check the exactness is now very easy.

PROFINITE GROUPS

For simplicity, we now assume k to be perfect. Let $\Gamma = \text{Gal}(k^{\text{al}}/k)$ where k^{al} is the algebraic closure of k . For any subfield K of k^{al} finite over k , we let

$$\Gamma_K = \{\sigma \in \Gamma \mid \sigma x = x \text{ for all } x \in K\}.$$

We consider only Γ -groups A for which

$$A = \bigcup A^{\Gamma_K} \tag{184}$$

and we define $H^1(\Gamma, A)$ to be the set of equivalence classes of 1-cocycles that factor through $\text{Gal}(K/k)$ for some subfield K of k^{al} finite and Galois over k . With these definitions,¹

$$H^1(\Gamma, A) = \varinjlim H^1(\text{Gal}(K/k), A^{\Gamma_K}) \tag{185}$$

where K runs through the subfields K of k^{al} finite and Galois over k .

THE GALOIS COHOMOLOGY OF ALGEBRAIC GROUPS

When G is an algebraic group over k ,

$$G(k^{\text{al}}) = \bigcup G(K), \quad G(K) = G(k^{\text{al}})^{\Gamma_K},$$

and so $G(k^{\text{al}})$ satisfies (119). We write $H^i(k, G)$ for $H^i(\text{Gal}(k^{\text{al}}/k), G(k^{\text{al}}))$.

An exact sequence

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

of algebraic groups over k gives rise to an exact sequence

$$1 \rightarrow G'(k^{\text{al}}) \rightarrow G(k^{\text{al}}) \rightarrow G''(k^{\text{al}}) \rightarrow 1$$

(I, §7)², and hence (see (120), p. 219) to an exact sequence

$$1 \rightarrow G'(k) \rightarrow G(k) \rightarrow G''(k) \rightarrow H^1(k, G') \rightarrow H^1(k, G) \rightarrow H^1(k, G'').$$

1b Classifying bilinear forms

Let K be a finite Galois extension of k with Galois group Γ . Let V be a finite-dimensional K -vector space. A *semi-linear action* of Γ on V is a homomorphism $\Gamma \rightarrow \text{Aut}_{k\text{-lin}}(V)$ such that

$$\sigma(cv) = \sigma c \cdot \sigma v \quad \text{all } \sigma \in \Gamma, c \in K, v \in V.$$

If $V = K \otimes_k V_0$, then there is a unique semi-linear action of Γ on V for which $V^\Gamma = 1 \otimes V_0$, namely,

$$\sigma(c \otimes v) = \sigma c \otimes v \quad \sigma \in \Gamma, c \in K, v \in V.$$

PROPOSITION 1.2 *The functor $V \mapsto K \otimes_k V$ from k -vector spaces to K -vector spaces endowed with a semi-linear action of Γ is an equivalence of categories with quasi-inverse $V \mapsto V^\Gamma$.*

LEMMA 1.3 *Let S be the standard $M_n(k)$ -module, namely, k^n with $M_n(k)$ acting by left multiplication. The functor $V \mapsto S \otimes_k V$ is an equivalence from the category of k -vector spaces to that of left $M_n(k)$ -modules.*

¹Equivalently, we consider only Γ -groups A for which the pairing $\Gamma \times A \rightarrow A$ is continuous relative to the Krull topology on Γ and the discrete topology on A , and we require that the 1-cocycles be continuous for the same topologies.

²In fact,

$$1 \rightarrow G'(R) \rightarrow G(R) \rightarrow G''(R)$$

is exact for all k -algebras; only the surjectivity $G(R) \rightarrow G''(R)$ requires that R be an algebraically closed field (I, 7.54).

PROOF. Note that S is a simple $M_n(k)$ -module. Since

$$\text{End}_{k\text{-lin}}(k) = k = \text{End}_{M_n(k)}(k^n)$$

and every k -vector space is isomorphic to a direct sum of copies of k , the functor is obviously fully faithful (i.e., gives isomorphisms on Homs). It remains to show that every left $M_n(k)$ -module is a direct sum of copies of S . This is certainly true of $M_n(k)$ itself:

$$M_n(k) = \bigoplus_{1 \leq i \leq n} L(i) \quad (\text{as a left } M_n(k)\text{-module})$$

where $L(i)$ is the set of matrices whose entries are zero except for those in the i th column. Since every left $M_n(k)$ -module M is a quotient of a direct sum of copies of $M_n(k)$, this shows that such an M is a sum of copies of S . Let I be the set of submodules of M isomorphic to S , and let J be a subset that is maximal among those for which $\sum_{N \in J} N$ is direct. Then $M = \bigoplus_{N \in J} N$ (see II, 6.1). \square

LEMMA 1.4 *For any k -vector space W , the functor $V \mapsto W \otimes_k V$ is an equivalence from the category of k -vector spaces to that of left $\text{End}_k(W)$ -modules.*

PROOF. When we choose a basis for W , this becomes the previous lemma. \square

PROOF OF PROPOSITION 1.2

Let $K[\Gamma]$ be the K -vector space with basis the elements of Γ , made into a k -algebra by the rule

$$(a\sigma) \cdot (b\tau) = a \cdot \sigma b \cdot \sigma\tau, \quad a, b \in K, \quad \sigma, \tau \in \Gamma.$$

Then $K[\Gamma]$ acts k -linearly on K by

$$(\sum a_\sigma \sigma)c = \sum a_\sigma \sigma c,$$

and the resulting homomorphism

$$K[\Gamma] \rightarrow \text{End}_k(K)$$

is injective by Dedekind's theorem on the independence of characters (FT 5.14). Since $K[\Gamma]$ and $\text{End}_k(K)$ have the same dimension as k -vector spaces, the map is an isomorphism. Therefore, the corollary shows that

$$V \mapsto K \otimes_k V$$

is an equivalence from the category of k -vector spaces to that of left modules over $\text{End}_k(K) \simeq K[\Gamma]$. This is the statement of the proposition.

BILINEAR FORMS AND COHOMOLOGY SETS

Let V_0 be a k -vector space equipped with a bilinear form $\phi_0: V \times V \rightarrow k$, and write $(V_0, \phi_0)_K$ for the pair over K obtained from (V_0, ϕ_0) by extension of scalars. Let $\mathcal{A}(K)$ denote the set of automorphisms of $(V_0, \phi_0)_K$.³

³In more detail: $(V_0, \phi_0)_K = (V_{0K}, \phi_{0K})$ where $V_{0K} = K \otimes_k V_0$ and ϕ_{0K} is the unique K -bilinear map $V_{0K} \times V_{0K} \rightarrow K$ extending ϕ_0 ; an element of $\mathcal{A}(K)$ is a K -linear isomorphism $\alpha: V_{0K} \rightarrow V_{0K}$ such that $\phi_{0K}(\alpha x, \alpha y) = \phi_{0K}(x, y)$ for all $x, y \in V_{0K}$.

THEOREM 1.5 *The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K .*

PROOF. Suppose $(V, \phi)_K \approx (V_0, \phi_0)_K$, and choose an isomorphism

$$f: (V_0, \phi_0)_K \rightarrow (V, \phi)_K.$$

Let

$$a_\sigma = f^{-1} \circ \sigma f.$$

Then

$$\begin{aligned} a_\sigma \cdot \sigma a_\tau &= (f^{-1} \circ \sigma f) \circ (\sigma f^{-1} \circ \sigma \tau f) \\ &= a_{\sigma\tau}, \end{aligned}$$

and so $a_\sigma(f)$ is a 1-cocycle. Moreover, any other isomorphism $f': (V_0, \phi_0)_K \rightarrow (V, \phi)_K$ differs from f by a $g \in \mathcal{A}(K)$, and

$$a_\sigma(f \circ g) = g^{-1} \cdot a_\sigma(f) \cdot \sigma g.$$

Therefore, the cohomology class of $a_\sigma(f)$ depends only on (V, ϕ) . It is easy to see that, in fact, it depends only on the isomorphism class of (V, ϕ) , and that two pairs (V, ϕ) and (V', ϕ') giving rise to the same class are isomorphic. It remains to show that every cohomology class arises from a pair (V, ϕ) . Let $(a_\sigma)_{\sigma \in \Gamma}$ be a 1-cocycle, and use it to define a new action of Γ on $V_K \stackrel{\text{def}}{=} K \otimes_k V$:

$${}^\sigma x = a_\sigma \cdot \sigma x, \quad \sigma \in \Gamma, \quad x \in V_K.$$

Then

$${}^\sigma (cv) = \sigma c \cdot {}^\sigma v, \text{ for } \sigma \in \Gamma, c \in K, v \in V,$$

and

$${}^\sigma ({}^\tau v) = {}^\sigma (a_\tau \tau v) = a_\sigma \cdot \sigma a_\tau \cdot \sigma \tau v = {}^{\sigma\tau} v,$$

and so this is a semilinear action. Therefore,

$$V_1 \stackrel{\text{def}}{=} \{x \in V_K \mid {}^\sigma x = x\}$$

is a subspace of V_K such that $K \otimes_k V_1 \simeq V_K$ (by 1.2). Because ϕ_{0K} arises from a pairing over k ,

$$\phi_{0K}(\sigma x, \sigma y) = \sigma \phi(x, y), \quad \text{all } x, y \in V_K.$$

Therefore (because $a_\sigma \in \mathcal{A}(K)$),

$$\phi_{0K}({}^\sigma x, {}^\sigma y) = \phi_{0K}(\sigma x, \sigma y) = \sigma \phi_{0K}(x, y).$$

If $x, y \in V_1$, then $\phi_{0K}({}^\sigma x, {}^\sigma y) = \phi_{0K}(x, y)$, and so $\phi_{0K}(x, y) = \sigma \phi_{0K}(x, y)$. By Galois theory, this implies that $\phi_{0K}(x, y) \in k$, and so ϕ_{0K} induces a k -bilinear pairing on V_1 . \square

APPLICATIONS

Again let K be a finite Galois extension of k with Galois group Γ .

PROPOSITION 1.6 For all n , $H^1(\Gamma, \mathrm{GL}_n(K)) = 1$.

PROOF. Apply Theorem 1.5 with $V_0 = k^n$ and ϕ_0 the zero form. It shows that $H^1(\Gamma, \mathrm{GL}_n(K))$ classifies the isomorphism classes of k -vector spaces V such that $K \otimes_k V \approx K^n$. But such k -vector spaces have dimension n , and therefore are isomorphic. \square

PROPOSITION 1.7 For all n , $H^1(\Gamma, \mathrm{SL}_n(K)) = 1$

PROOF. Because the determinant map $\det: \mathrm{GL}_n(K) \rightarrow K^\times$ is surjective,

$$1 \rightarrow \mathrm{SL}_n(K) \rightarrow \mathrm{GL}_n(K) \xrightarrow{\det} K^\times \rightarrow 1$$

is an exact sequence of Γ -groups. It gives rise to an exact sequence

$$\mathrm{GL}_n(k) \xrightarrow{\det} k^\times \rightarrow H^1(\Gamma, \mathrm{SL}_n) \rightarrow H^1(\Gamma, \mathrm{GL}_n)$$

from which the statement follows. \square

PROPOSITION 1.8 Let ϕ_0 be a nondegenerate alternating bilinear form on V_0 , and let Sp be the associated symplectic group⁴. Then $H^1(\Gamma, \mathrm{Sp}(K)) = 1$.

PROOF. According to Theorem 1.5, $H^1(\Gamma, \mathrm{Sp}(K))$ classifies isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K . But this condition implies that ϕ is a nondegenerate alternating form and that $\dim V = \dim V_0$. All such pairs (V, ϕ) are isomorphic. \square

REMARK 1.9 Let ϕ_0 be a nondegenerate bilinear symmetric form on V_0 , and let O be the associated orthogonal group. Then $H^1(\Gamma, \mathrm{O}(K))$ classifies the isomorphism classes of quadratic spaces over k that become isomorphic to (V, ϕ) over K . This can be a very large set.

1c Classifying the forms of an algebraic group

Again let K be a finite Galois extension of k with Galois group Γ . Let G_0 be an algebraic group over k , and let $\mathcal{A}(K)$ be the group of automorphisms $\alpha: G_K \rightarrow G_K$. Then Γ acts on $\mathcal{A}(K)$ in a natural way:

$$\sigma \alpha = \sigma \circ \alpha \circ \sigma^{-1}.$$

THEOREM 1.10 The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of algebraic groups G over k that become isomorphic to G_0 over K .

⁴So $\mathrm{Sp}(R) = \{a \in \mathrm{End}_{R\text{-lin}}(R \otimes_k V) \mid \phi(ax, ay) = \phi(x, y)\}$

PROOF. Let G be such an algebraic group over k , choose an isomorphism

$$f: G_{0K} \rightarrow G_K,$$

and write

$$a_\sigma = f^{-1} \circ \sigma f.$$

As in the proof of Theorem 1.5, $(a_\sigma)_{\sigma \in \Gamma}$ is a 1-cocycle, and the map

$$G \mapsto \text{class of } (a_\sigma)_{\sigma \in \Gamma} \text{ in } H^1(\Gamma, A(K))$$

is well-defined and its fibres are the isomorphism classes.

In proving that the map is surjective, it is useful to identify $\mathcal{A}(K)$ with the automorphism group of the Hopf algebra $\mathcal{O}(G_{0K}) = K \otimes_k \mathcal{O}(G_0)$. Let $A_0 = \mathcal{O}(G_0)$ and $A = K \otimes_k A_0$. As in the proof of Theorem 1.5, we use a 1-cocycle $(a_\sigma)_{\sigma \in \Gamma}$ to twist the action of Γ on A ; specifically, we define

$${}^\sigma a = a_\sigma \circ \sigma a, \quad \sigma \in \Gamma, \quad a \in A.$$

Proposition 1.2 in fact holds for infinite dimensional vector spaces V with the same⁵ proof, and so the k -subspace

$$B = \{a \in A \mid {}^\sigma a = a\}$$

of A has the property that

$$K \otimes_k B \simeq A.$$

It remains to show that the Hopf algebra structure on A induces a Hopf algebra structure on B . Consider for example the comultiplication. The k -linear map

$$\Delta_0: A_0 \rightarrow A_0 \otimes_k A_0$$

has a unique extension to a K -linear map

$$\Delta: A \rightarrow A \otimes_K A.$$

This map commutes with the action of Γ :

$$\Delta(\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Because a_σ is a Hopf algebra homomorphism,

$$\Delta(a_\sigma a) = a_\sigma \Delta(a), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Therefore,

$$\Delta({}^\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

In particular, we see that Δ maps B into $(A \otimes_K A)^\Gamma$, which equals $B \otimes_k B$ because the functor in (1.2) preserves tensor products. Similarly, all the maps defining the Hopf algebra structure on A preserve B , and therefore define a Hopf algebra structure on B . Finally, one checks that the 1-cocycle attached to B and the given isomorphism $K \otimes_k B \rightarrow A$ is (a_σ) . \square

⁵Except that the last step of the proof of (1.3) requires Zorn's lemma.

EXAMPLES

1.11 For all n , $H^1(k, \text{GL}_n) = 1$.

This follows from (1.6) and (120).

1.12 For all n , $H^1(k, \text{SL}_n) = 1$.

1.13 For all n , $H^1(k, \text{Sp}_n) = 1$.

1.14 Let (V, ϕ) be a nondegenerate quadratic space over k . Then $H^1(k, O(\phi))$ classifies the isomorphism classes of quadratic spaces over k with the same dimension as V .

PROOF. Over k^{al} , all nondegenerate quadratic spaces of the same dimension are isomorphic. □

1.15 Let G be an algebraic group of k . The isomorphism classes of algebraic groups over k that become isomorphic to $G_{k^{\text{al}}}$ over k^{al} are classified by $H^1(\Gamma, \mathcal{A}(k^{\text{al}}))$. Here $\Gamma = \text{Gal}(k^{\text{al}}/k)$ and $\mathcal{A}(k^{\text{al}})$ is the automorphism group of $G_{k^{\text{al}}}$.

(WEIL) RESTRICTION OF THE BASE FIELD

Let K be a finite extension of k , and let G be an algebraic group over K . Recall (I, §4d) that the functor

$$R \rightsquigarrow G_*(R) = G(K \otimes_k R)$$

from k -algebras to groups is an algebraic group over k .

PROPOSITION 1.16 There is a canonical isomorphism

$$G_{*k^{\text{al}}} \simeq \prod_{\rho: K \rightarrow k^{\text{al}}} \rho G. \tag{186}$$

PROOF. The product is over the k -homomorphisms $K \rightarrow k^{\text{al}}$, and by ρG , we mean the algebraic group over k^{al} such that, for a k^{al} -algebra R ,

$$(\rho G)(R) = G(R)$$

— on the right, R is regarded as a k -algebra via ρ . For a k^{al} -algebra R ,

$$\begin{aligned} K \otimes_k R &\simeq K \otimes_k (k^{\text{al}} \otimes_{k^{\text{al}}} R) \\ &\simeq (K \otimes_k k^{\text{al}}) \otimes_{k^{\text{al}}} R \\ &\simeq \left(\prod_{\rho: K \rightarrow k^{\text{al}}} k^{\text{al}} \right) \otimes_{k^{\text{al}}} R. \end{aligned}$$

Thus, $G_{*k^{\text{al}}} \simeq \prod_{\rho: K \rightarrow k^{\text{al}}} \rho G$ as functors, and therefore as algebraic groups. □

COROLLARY 1.17 We have

$$H^i(k, G_*) \simeq H^i(K, G) \text{ for } i = 0, 1 \text{ (and for all } i \geq 0 \text{ when } G \text{ is commutative).}$$

PROOF. Combine (186) with Shapiro's lemma (CFT II, 1.11 for the commutative case; need to add for the noncommutative case). □

From now on, we assume that k has characteristic zero.

1d Reductive algebraic groups

According to (I, 17.21), to give a reductive algebraic group G over a field k amounts to giving a simply connected semisimple group G over k , an algebraic group Z of multiplicative type over k , and homomorphism $Z(G) \rightarrow Z$. Because k has characteristic zero, $Z(G)$ is of multiplicative type (even étale), and according to I, Theorem 14.20, the functor sending an algebraic group of multiplicative type to its character group is an equivalence to the category finitely generated \mathbb{Z} -modules with a continuous action of Γ . If we suppose this last category to be known, then describing the reductive algebraic groups amounts to describing the simply connected semisimple groups together with their centres.

TORI

A torus T over a field k is said to be *quasi-trivial* if it is a product of tori of the form $(\mathbb{G}_m)_{k'/k}$ with k' a finite field extension of k . If $T = \prod_i (\mathbb{G}_m)_{k_i/k}$, then

$$H^1(k, T) \stackrel{(1.17)}{\simeq} \prod_i H^1(k_i, \mathbb{G}_m) \stackrel{(1.6)}{=} 0.$$

If T is quasi-trivial over k , then $T_{k'}$ is quasi-trivial over k' for any field $k' \supset k$, and so $H^1(k', T_{k'}) = 0$. There is a converse to this.

THEOREM 1.18 *A torus T over k has the property that $H^1(k', T_{k'}) = 0$ for all fields k' containing k if and only if T is a direct factor of a quasi-trivial torus.*

PROOF. Omitted for the present. □

SIMPLY CONNECTED SEMISIMPLE GROUPS

Let G be a simply connected semisimple group over k . Then, according to II, Theorem 5.31, $G_{k^{\text{al}}}$ decomposes into a product

$$G_{k^{\text{al}}} = G_1 \times \cdots \times G_r \tag{187}$$

of its almost-simple subgroups G_i . The set $\{G_1, \dots, G_r\}$ contains all the almost-simple subgroups of G . When we apply $\sigma \in \Gamma$ to (187), it becomes

$$G_{k^{\text{al}}} = \sigma G_{k^{\text{al}}} = \sigma G_1 \times \cdots \times \sigma G_r$$

with $\{\sigma G_1, \dots, \sigma G_r\}$ a permutation of $\{G_1, \dots, G_r\}$. Let H_1, \dots, H_s denote the products of G_i in the different orbits of Γ . Then $\sigma H_i = H_i$, and so H_i is defined over k (I, 4.13), and

$$G = H_1 \times \cdots \times H_s$$

is a decomposition of G into a product of its almost-simple subgroups.

Now suppose that G itself is almost-simple, so that Γ acts transitively on the G_i in (187). Let

$$\Delta = \{\sigma \in \Gamma \mid \sigma G_1 = G_1\}.$$

Then G_1 is defined over the subfield $K = k^{\text{al}\Delta}$ of k^{al} (I, 4.13).

PROPOSITION 1.19 *We have $G \simeq G_{1*}$ (and so $H^1(k, G) \simeq H^1(K, G_1)$).*

PROOF. We can rewrite (187) as

$$G_{k^{\text{al}}} = \prod \sigma G_{1k^{\text{al}}}$$

where σ runs over a set of cosets for Δ in Γ . On comparing this with (186), we see that there is a canonical isomorphism

$$G_{k^{\text{al}}} \simeq (G_{1*})_{k^{\text{al}}}.$$

In particular, it commutes with the action of Γ , and so is defined over k (I, 4.13). □

The group G_1 over K is **geometrically almost-simple**, i.e., it is almost-simple and remains almost-simple over k^{al} . The discussion in this section shows that it suffices to consider such groups.

ABSOLUTELY ALMOST-SIMPLE SIMPLY-CONNECTED SEMISIMPLE GROUPS

For an algebraic group G , let $G^{\text{ad}} = G/Z(G)$.

PROPOSITION 1.20 *For any simply connected semisimple group G , there is an exact sequence*

$$1 \rightarrow G^{\text{ad}}(k^{\text{al}}) \rightarrow \mathcal{A}(k^{\text{al}}) \rightarrow \text{Sym}(D) \rightarrow 1.$$

When G is split, Γ acts trivially on $\text{Sym}(D)$, and the sequence is split, i.e., there is a subgroup of $\mathcal{A}(k^{\text{al}})$ on which Γ acts trivially and which maps isomorphically onto $\text{Sym}(D)$.

PROOF. An element of $G^{\text{ad}}(k^{\text{al}}) = G(k^{\text{al}})/Z(k^{\text{al}})$ acts on $G_{k^{\text{al}}}$ by an inner automorphism. Here D is the Dynkin diagram of G , and $\text{Sym}(D)$ is the group of symmetries of it. This description of the outer automorphisms of G , at least in the split case, is part of the full statement of the isomorphism theorem (V, 2.22). □

The indecomposable Dynkin diagrams don't have many symmetries: for D_4 the symmetry group is S_3 (symmetric group on 3 letters), for A_n , D_n , and E_6 it has order 2, and otherwise it is trivial.

THEOREM 1.21 *For each indecomposable Dynkin diagram D , there is a split, geometrically almost-simple, simply connected algebraic group G over k such that $G_{k^{\text{al}}}$ has the type of the Dynkin diagram; moreover G is unique up to isomorphism. The isomorphism classes of algebraic groups over k becoming isomorphic to G over k^{al} are classified by $H^1(k, \mathcal{A}(k^{\text{al}}))$ where $\mathcal{A}(k^{\text{al}})$ is the automorphism group of $G_{k^{\text{al}}}$. For the split group G , $X^*(Z(G)) = P(D)/Q(D)$ with Γ acting trivially. For the form G' of G defined by a 1-cocycle (a_σ) , $Z(G') = Z(G)$ but with Γ acting through a_σ .*

For example, for A_n , the split group is SL_n . This has centre μ_n , which is the group of multiplicative type corresponding to $\mathbb{Z}/n\mathbb{Z}$ with the trivial action of Γ . Let G_0 and G be groups over k , and let $f: G_0 \rightarrow G$ be an isomorphism over k^{al} . Write $a_\sigma = f^{-1} \circ \sigma f$. Then f defines an isomorphism

$$f: Z_0(k^{\text{al}}) \rightarrow Z(k^{\text{al}})$$

on the points of their centres, and

$$f(a_\sigma \sigma x) = \sigma(f(x)).$$

When we use f to identify $Z_0(k^{\text{al}})$ with $Z(k^{\text{al}})$, this says that Γ acts on $Z(k^{\text{al}})$ by the twisted action ${}^\sigma x = a_\sigma \sigma x$.

REMARK 1.22 Let G_0 be the split simply connected group of type X_y , and let G be a form of G_0 . Let c be its cohomology class. If $c \in H^1(k, G^{\text{ad}})$, then G is called an *inner form* of G . In general, c will map to a nontrivial element of

$$H^1(k, \text{Sym}(D)) = \text{Hom}_{\text{continuous}}(\Gamma, \text{Sym}(D)).$$

Let Δ be the kernel of this homomorphism, and let L be the corresponding extension field of k . Let $z = (\Gamma: \Delta)$. Then we say G is of type ${}^z X_y$.

1e The main theorems on the cohomology of groups

To complete the classification of algebraic groups, it remains to compute the cohomology groups. This, of course, is an important problem. All I can do here is list some of the main theorems.

1.23 Let k be finite. If G is connected, then $H^1(k, G) = 1$.

1.24 Let k be a finite extension of the field of p -adic numbers \mathbb{Q}_p . If G is simply connected and semisimple, then $H^1(k, G) = 1$.

1.25 Let $k = \mathbb{Q}$, and let G be a semisimple group over \mathbb{Q} .

(a) If G is simply connected, then

$$H^1(\mathbb{Q}, G) \simeq H^1(\mathbb{R}, G).$$

(b) If G is an adjoint group (i.e., has trivial centre), or equals $O(\phi)$ for some nondegenerate quadratic space (V, ϕ) , then

$$H^1(\mathbb{Q}, G) \rightarrow \prod_{p=2,3,5,\dots,\infty} H^1(\mathbb{Q}_p, G)$$

is injective.

Note that the last result implies that two quadratic spaces over \mathbb{Q} are isomorphic if and only if they become isomorphic over \mathbb{Q}_p for all p (including $p = \infty$, for which we set $\mathbb{Q}_p = \mathbb{R}$). This is a very important, and deep result, in number theory.

Statement 1.25 extends in an obvious way to finite extensions of \mathbb{Q} .

NOTES For more on the cohomology of algebraic groups, see Kneser 1969 or Platonov and Rapinchuk 1994.

2 Classical groups and algebras with involution

Moved to Chapter I.

3 Relative root systems and the anisotropic kernel.

The aim of this section is to explain Tits's strategy for classifying nonsplit groups and their representations. Here is a brief overview.

The isomorphism classes of split semisimple algebraic groups are classified over any field. Given a semisimple algebraic group G over a field k , one knows that G splits over the separable algebraic closure K of k , and so the problem is to determine the isomorphism classes of semisimple algebraic groups over k corresponding to a given isomorphism class over K . Tits (1966) sketches a program for doing this. Let T_0 be a maximal split subtorus of G , and let T be a maximal torus containing T_0 . The derived group of the centralizer of T_0 is called the *anisotropic kernel* of G — it is a semisimple algebraic group over k whose split subtori are trivial. Let S be a simple set of roots for (G_K, T_K) , and let S_0 be the subset vanishing on T_0 . The Galois group of K/k acts on S , and the triple consisting of S , S_0 , and this action is called the *index* of G . Tits sketches a proof (corrected in the MR review of the article) that the isomorphism class of G is determined by the isomorphism class of G_K , its anisotropic kernel, and its index. It remains therefore to determine for each isomorphism class of semisimple algebraic groups over k (a) the possible indices, and (b) for each possible index, the possible anisotropic kernels. Tits (ibid.) announces some partial results on (a) and (b).

Problem (b) is related to the problem of determining the central division algebras over a field, and so it is only plausible to expect a solution to it for fields k for which the Brauer group is known.

Tits's work was continued by his student Selbach. To quote the MR review of Selbach 1976 (slightly edited):

This booklet treats the classification of quasisimple algebraic groups over arbitrary fields along the lines of Tits 1966. Tits had shown that each such group is described by three data: the index, the anisotropic kernel and the connectedness type. For his general results Tits had given or sketched proofs, but not for the enumeration of possible indices, whereas the classification of possible anisotropic kernels was not dealt with at all. The booklet under review starts with an exposition with complete proofs of the necessary general theory. Some proofs are simplified using results on representation theory over arbitrary fields from another paper by Tits (Crelle 1971), and a different proof is given for the main result, viz., that a simply connected group is determined by its index and anisotropic kernel, because Tits's original proof contained a mistake, as was indicated in the review of that paper. Then it presents the detailed classifications with proofs of all possible indices, and of the anisotropic kernels of exceptional type. Questions of existence over special fields (finite, reals, p -adic, number) are dealt with only in cases which fit easily in the context (Veldkamp).

It is interesting to note that, while Tits's article has been cited 123 times, Selbach's has been cited on twice (MR April 2010).

Here is the MR review of Tits 1971 (my translation).

The author proposes to study the linear irreducible k -representations of a reductive algebraic group G over k , where k is any field. When k is algebraically closed, Chevalley showed that the irreducible representations of G are characterized, as in the classical case, by the weights of G (characters of a maximal torus of G), every weight "dominant relative to a Borel subgroup" being the

dominant weight of an irreducible representation. The author first shows that this correspondence continues when G is split over k . In the general case, it is necessary to start with a maximal k -torus T in G and a Borel subgroup B of G containing T in order to define the weights (forming a group Λ) and the set Λ_+ of dominant weights with respect to B ; let Λ_0 denote the subgroup of Λ generated by the roots and by the weights zero on the intersection $T \cap D(G)$; the quotient $C^* = \Lambda/\Lambda_0$ is the dual of the centre of G . The Galois group Γ of the separable closure k^{sep} of k over k acts canonically on Λ , Λ_0 , and Λ_+ ; the central result attaches to each dominant weight $\lambda \in \Lambda_+$ invariant under Γ an absolutely irreducible representation of G in a linear group $\text{GL}(m, D)$, well determined up to equivalence, D being a skew field with centre k , well determined up to isomorphism; moreover, if $\lambda \in \Lambda_0$ or if G is quasi-split (in which case the Borel group B is defined over k), then $D = k$. One attaches in this way to any weight λ of Λ_+ invariant by Γ an element $[D] = \alpha_{G,k}(\lambda)$ of the Brauer group $\text{Br}(k)$, and one shows that $\alpha_{G,k}$ extends to a homomorphism of the group Λ^Γ of weights invariant under Γ into $\text{Br}(k)$; moreover, the kernel of $\alpha_{G,k}$ contains Λ_0 , and so there is a fundamental homomorphism $\beta_{G,k}: C^{*\Gamma} \rightarrow \text{Br}(k)$ (where $C^{*\Gamma}$ is the subgroup of C^* formed of the elements invariant under Γ). The author shows that this homomorphism can be defined cohomologically, in relation with the “Brauer-Witt invariant” of the group G . A good part of the memoir is concerned with the study of the homomorphism β , notably the relations between $\beta_{G,k}$ and $\beta_{G_1,k}$, where G_1 is a reductive subgroup of G , as well as with majorizing the degree of $\beta(c)$ in $\text{Br}(k)$ when G is an almost-simple group and c is the class of the minuscule dominant weight. He examines also a certain number of examples, notably the groups of type E_6 and E_7 . Finally, he shows how starting from a knowledge of α , one obtains all the irreducible k -representations of G : start with a dominant weight $\lambda \in \Lambda_+$, and denote by k_λ the field of invariants of the stabilizer of λ in Γ ; then if $\alpha_{G,k_\lambda}(\lambda) = [D_\lambda]$, one obtains a k_λ -representation $G \rightarrow \text{GL}(m, D_\lambda)$, whence one deduces canonically a k -representation ${}^k\rho_\lambda$, which is irreducible; every irreducible k -representation is equivalent to a ${}^k\rho_\lambda$, and ${}^k\rho_\lambda$ and ${}^k\rho_{\lambda'}$ are k -equivalent if and only if λ and λ' are transformed into one another by an element of Γ (Dieudonné).

Arithmetic Subgroups

We study discrete subgroups of real Lie groups that are large in the sense that the quotient has finite volume. For example, if the Lie group equals $G(\mathbb{R})^+$ for some algebraic group G over \mathbb{Q} , then $G(\mathbb{Z})$ is such a subgroup of $G(\mathbb{R})^+$. The discrete subgroups of a real Lie group \mathcal{G} arising in (roughly) this way from algebraic groups over \mathbb{Q} are called the arithmetic subgroups of \mathcal{G} (see 15.1 for a precise definition). Except when \mathcal{G} is $SL_2(\mathbb{R})$ or a similarly special group, no one was able to construct a discrete subgroup of finite covolume in a semisimple Lie group except by this method. Eventually, Selberg conjectured that there *are* no others, and this was proved by Margulis.

NOTES At present this chapter is only an introductory survey. My intention is to expand it by adding, for example, a more detailed discussion of Margulis’s theorem and its applications, and by adding more proofs (but not, of course, all proofs).

1	Commensurable groups	397
2	Definitions and examples	398
3	Questions	399
4	Independence of ρ and L	399
5	Behaviour with respect to homomorphisms	400
6	Adèlic description of congruence subgroups	401
7	Applications to manifolds	402
8	Torsion-free arithmetic groups	402
9	A fundamental domain for SL_2	403
10	Application to quadratic forms	404
11	“Large” discrete subgroups	405
12	Reduction theory	406
13	Presentations	408
14	The congruence subgroup problem	409
15	The theorem of Margulis	410
16	Shimura varieties	411

1 Commensurable groups

Subgroups H_1 and H_2 of a group are said to be *commensurable* if $H_1 \cap H_2$ is of finite index in both H_1 and H_2 .

The subgroups $a\mathbb{Z}$ and $b\mathbb{Z}$ of \mathbb{R} are commensurable if and only if $a/b \in \mathbb{Q}$. For example, $6\mathbb{Z}$ and $4\mathbb{Z}$ are commensurable because they intersect in $12\mathbb{Z}$, but $1\mathbb{Z}$ and $\sqrt{2}\mathbb{Z}$ are *not* commensurable because they intersect in $\{0\}$. More generally, lattices L and L' in a real vector space V are commensurable if and only if they generate the same \mathbb{Q} -subspace of V .

Commensurability is an equivalence relation: obviously, it is reflexive and symmetric, and if H_1, H_2 and H_2, H_3 are commensurable, one shows easily that $H_1 \cap H_2 \cap H_3$ is of finite index in H_1, H_2 , and H_3 .

2 Definitions and examples

Let G be an algebraic group over \mathbb{Q} . Let $\rho: G \rightarrow \mathrm{GL}_V$ be a faithful representation of G on a finite-dimensional vector space V , and let L be a lattice in V . Define

$$G(\mathbb{Q})_L = \{g \in G(\mathbb{Q}) \mid \rho(g)L = L\}.$$

An *arithmetic subgroup* of $G(\mathbb{Q})$ is any subgroup commensurable with $G(\mathbb{Q})_L$. For an integer $N > 1$, the *principal congruence subgroup of level N* is

$$\Gamma(N)_L = \{g \in G(\mathbb{Q})_L \mid g \text{ acts as } 1 \text{ on } L/NL\}.$$

In other words, $\Gamma(N)_L$ is the kernel of

$$G(\mathbb{Q})_L \rightarrow \mathrm{Aut}(L/NL).$$

In particular, it is normal and of finite index in $G(\mathbb{Q})_L$. A *congruence subgroup* of $G(\mathbb{Q})$ is any subgroup containing some $\Gamma(N)$ as a subgroup of finite index, so congruence subgroups are arithmetic subgroups.

EXAMPLE 2.1 Let $G = \mathrm{GL}_n$ with its standard representation on \mathbb{Q}^n and its standard lattice $L = \mathbb{Z}^n$. Then $G(\mathbb{Q})_L$ consists of the $A \in \mathrm{GL}_n(\mathbb{Q})$ such that

$$A\mathbb{Z}^n = \mathbb{Z}^n.$$

On applying A to e_1, \dots, e_n , we see that this implies that A has entries in \mathbb{Z} . Since $A^{-1}\mathbb{Z}^n = \mathbb{Z}^n$, the same is true of A^{-1} . Therefore, $G(\mathbb{Q})_L$ is

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}.$$

The arithmetic subgroups of $\mathrm{GL}_n(\mathbb{Q})$ are those commensurable with $\mathrm{GL}_n(\mathbb{Z})$.

By definition,

$$\begin{aligned} \Gamma(N) &= \{A \in \mathrm{GL}_n(\mathbb{Z}) \mid A \equiv I \pmod{N}\} \\ &= \{(a_{ij}) \in \mathrm{GL}_n(\mathbb{Z}) \mid N \text{ divides } (a_{ij} - \delta_{ij})\}, \end{aligned}$$

which is the kernel of

$$\mathrm{GL}_n(\mathbb{Z}) \rightarrow \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z}).$$

EXAMPLE 2.2 Consider a triple (G, ρ, L) as in the definition of arithmetic subgroups. The choice of a basis for L identifies G with a subgroup of GL_n and L with \mathbb{Z}^n . Then

$$G(\mathbb{Q})_L = G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$$

and $\Gamma_L(N)$ for G is

$$G(\mathbb{Q}) \cap \Gamma(N).$$

For a subgroup G of GL_n , one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. By abuse of notation, given a triple (G, ρ, L) , one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q})_L$.

EXAMPLE 2.3 The group

$$\mathrm{Sp}_{2n}(\mathbb{Z}) = \left\{ A \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \right\}$$

is an arithmetic subgroup of $\mathrm{Sp}_{2n}(\mathbb{Q})$, and all arithmetic subgroups are commensurable with it.

EXAMPLE 2.4 Let (V, Φ) be a root system and X a lattice $P \supset X \supset Q$. Chevalley showed that (V, Φ, X) defines an “algebraic group G over \mathbb{Z} ” which over \mathbb{Q} becomes the split semisimple algebraic group associated with (V, Φ, X) , and $G(\mathbb{Z})$ is a canonical arithmetic group in $G(\mathbb{Q})$.

EXAMPLE 2.5 Arithmetic groups may be finite. For example $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$, and the arithmetic subgroups of $G(\mathbb{Q})$ will be finite if $G(\mathbb{R})$ is compact (because arithmetic subgroups are discrete in $G(\mathbb{R})$ — see later).

EXAMPLE 2.6 (for number theorists). Let K be a finite extension of \mathbb{Q} , and let U be the group of units in K . For the torus $T = (\mathbb{G}_m)_{K/k}$ over \mathbb{Q} , $T(\mathbb{Z}) = U$.

3 Questions

The definitions suggest a number of questions and problems.

- ◇ Show the sets of arithmetic and congruence subgroups of $G(\mathbb{Q})$ do not depend on the choice of ρ and L .
- ◇ Examine the properties of arithmetic subgroups, both intrinsically and as subgroups of $G(\mathbb{R})$.
- ◇ Give applications of arithmetic subgroups.
- ◇ When are all arithmetic subgroups congruence?
- ◇ Are there other characterizations of arithmetic subgroups?

4 Independence of ρ and L .

LEMMA 4.1 *Let G be a subgroup of GL_n . For any representation $\rho: G \rightarrow \mathrm{GL}_V$ and lattice $L \subset V$, there exists a congruence subgroup of $G(\mathbb{Q})$ leaving L stable (i.e., for some $m \geq 1$, $\rho(g)L = L$ for all $g \in \Gamma(m)$).*

PROOF. When we choose a basis for L , ρ becomes a homomorphism of algebraic groups $G \rightarrow \mathrm{GL}_{n'}$. The entries of the matrix $\rho(g)$ are polynomials in the entries of the matrix $g = (g_{ij})$, i.e., there exist polynomials $P_{\alpha,\beta} \in \mathbb{Q}[\dots, X_{ij}, \dots]$ such that

$$\rho(g)_{\alpha\beta} = P_{\alpha,\beta}(\dots, g_{ij}, \dots).$$

After a minor change of variables, this equation becomes

$$\rho(g)_{\alpha\beta} - \delta_{\alpha,\beta} = Q_{\alpha,\beta}(\dots, g_{ij} - \delta_{ij}, \dots)$$

with $Q_{\alpha,\beta} \in \mathbb{Q}[\dots, X_{ij}, \dots]$ and δ the Kronecker delta. Because $\rho(I) = I$, the $Q_{\alpha,\beta}$ have zero constant term. Let m be a common denominator for the coefficients of the $Q_{\alpha,\beta}$, so that

$$mQ_{\alpha,\beta} \in \mathbb{Z}[\dots, X_{ij}, \dots].$$

If $g \equiv I \pmod{m}$, then

$$Q_{\alpha,\beta}(\dots, g_{ij} - \delta_{ij}, \dots) \in \mathbb{Z}.$$

Therefore, $\rho(g)\mathbb{Z}^{n'} \subset \mathbb{Z}^{n'}$, and, as g^{-1} also lies in $\Gamma(m)$, $\rho(g)\mathbb{Z}^{n'} = \mathbb{Z}^{n'}$. \square

PROPOSITION 4.2 *For any faithful representations $G \rightarrow \mathrm{GL}_V$ and $G \rightarrow \mathrm{GL}_{V'}$ of G and lattices L and L' in V and V' , $G(\mathbb{Q})_L$ and $G(\mathbb{Q})_{L'}$ are commensurable.*

PROOF. According to the lemma, there exists a subgroup Γ of finite index in $G(\mathbb{Q})_L$ such that $\Gamma \subset G(\mathbb{Q})_{L'}$. Therefore,

$$(G(\mathbb{Q})_L : G(\mathbb{Q})_L \cap G(\mathbb{Q})_{L'}) \leq (G(\mathbb{Q})_L : \Gamma) < \infty.$$

Similarly,

$$(G(\mathbb{Q})_{L'} : G(\mathbb{Q})_L \cap G(\mathbb{Q})_{L'}) < \infty. \quad \square$$

Thus, the notion of arithmetic subgroup is independent of the choice of a faithful representation and a lattice. The same is true for congruence subgroups, because the proof of (4.1) shows that, for any N , there exists an m such that $\Gamma(Nm) \subset \Gamma_L(N)$.

5 Behaviour with respect to homomorphisms

PROPOSITION 5.1 *Let Γ be an arithmetic subgroup of $G(\mathbb{Q})$, and let $\rho: G \rightarrow \mathrm{GL}_V$ be a representation of G . Every lattice L of V is contained in a lattice stable under Γ .*

PROOF. According to (4.1), there exists a subgroup Γ' leaving L stable. Let

$$L' = \sum \rho(g)L$$

where g runs over a set of coset representatives for Γ' in Γ . The sum is finite, and so L' is again a lattice in V , and it is obviously stable under Γ . \square

PROPOSITION 5.2 *Let $\varphi: G \rightarrow G'$ be a homomorphism of algebraic groups over \mathbb{Q} . For any arithmetic subgroup Γ of $G(\mathbb{Q})$, $\varphi(\Gamma)$ is contained in an arithmetic subgroup of $G'(\mathbb{Q})$.*

PROOF. Let $\rho: G' \rightarrow \mathrm{GL}_V$ be a faithful representation of G' , and let L be a lattice in V . According to (5.1), there exists a lattice $L' \supset L$ stable under $(\rho \circ \varphi)(\Gamma)$, and so $G'(\mathbb{Q})_L \supset \varphi(\Gamma)$. \square

REMARK 5.3 If $\varphi: G \rightarrow G'$ is a quotient map and Γ is an arithmetic subgroup of $G(\mathbb{Q})$, then one can show that $\varphi(\Gamma)$ is of finite index in an arithmetic subgroup of $G'(\mathbb{Q})$ (Borel 1969a, 8.9, 8.11). Therefore, arithmetic subgroups of $G(\mathbb{Q})$ map to arithmetic subgroups of $G'(\mathbb{Q})$. (Because $\varphi(G(\mathbb{Q}))$ typically has infinite index in $G'(\mathbb{Q})$, this is far from obvious.)

6 Adèlic description of congruence subgroups

In this subsection, which can be skipped, I assume the reader is familiar with adèles. The *ring of finite adèles* is the restricted topological product

$$\mathbb{A}_f = \prod (\mathbb{Q}_\ell : \mathbb{Z}_\ell)$$

where ℓ runs over the finite primes of \mathbb{Q} . Thus, \mathbb{A}_f is the subring of $\prod \mathbb{Q}_\ell$ consisting of the (a_ℓ) such that $a_\ell \in \mathbb{Z}_\ell$ for almost all ℓ , and it is endowed with the topology for which $\prod \mathbb{Z}_\ell$ is open and has the product topology.

Let $V = \text{Spm } A$ be an affine variety over \mathbb{Q} . The set of points of V with coordinates in a \mathbb{Q} -algebra R is

$$V(R) = \text{Hom}_{\mathbb{Q}}(A, R).$$

When we write

$$A = \mathbb{Q}[X_1, \dots, X_m] / \mathfrak{a} = \mathbb{Q}[x_1, \dots, x_m],$$

the map $P \mapsto (P(x_1), \dots, P(x_m))$ identifies $V(R)$ with

$$\{(a_1, \dots, a_m) \in R^m \mid f(a_1, \dots, a_m) = 0, \quad \forall f \in \mathfrak{a}\}.$$

Let $\mathbb{Z}[x_1, \dots, x_m]$ be the \mathbb{Z} -subalgebra of A generated by the x_i , and let

$$V(\mathbb{Z}_\ell) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_m], \mathbb{Z}_\ell) = V(\mathbb{Q}_\ell) \cap \mathbb{Z}_\ell^m \quad (\text{inside } \mathbb{Q}_\ell^m).$$

This set depends on the choice of the generators x_i for A , but if $A = \mathbb{Q}[y_1, \dots, y_n]$, then the y_i 's can be expressed as polynomials in the x_i with coefficients in \mathbb{Q} , and vice versa. For some $d \in \mathbb{Z}$, the coefficients of these polynomials lie in $\mathbb{Z}[\frac{1}{d}]$, and so

$$\mathbb{Z}[\frac{1}{d}][x_1, \dots, x_m] = \mathbb{Z}[\frac{1}{d}][y_1, \dots, y_n] \quad (\text{inside } A).$$

It follows that for $\ell \nmid d$, the y_i 's give the same set $V(\mathbb{Z}_\ell)$ as the x_i 's. Therefore,

$$V(\mathbb{A}_f) = \prod (V(\mathbb{Q}_\ell) : V(\mathbb{Z}_\ell))$$

is independent of the choice of generators for A .

For an algebraic group G over \mathbb{Q} , we define

$$G(\mathbb{A}_f) = \prod (G(\mathbb{Q}_\ell) : G(\mathbb{Z}_\ell))$$

similarly. Now it is a topological group.¹ For example,

$$\mathbb{G}_m(\mathbb{A}_f) = \prod (\mathbb{Q}_\ell^\times : \mathbb{Z}_\ell^\times) = \mathbb{A}_f^\times.$$

PROPOSITION 6.1 *For any compact open subgroup K of $G(\mathbb{A}_f)$, $K \cap G(\mathbb{Q})$ is a congruence subgroup of $G(\mathbb{Q})$, and every congruence subgroup arises in this way.²*

¹The choice of generators determines a group structure on $G(\mathbb{Z}_\ell)$ for almost all ℓ , etc..

²To define a basic compact open subgroup K of $G(\mathbb{A}_f)$, one has to impose a congruence condition at each of a finite set of primes. Then $\Gamma = G(\mathbb{Q}) \cap K$ is obtained from $G(\mathbb{Z})$ by imposing the same congruence conditions. One can think of Γ as being the congruence subgroup defined by the "congruence condition" K .

PROOF. Fix an embedding $G \hookrightarrow \mathrm{GL}_n$. From this we get a surjection $\mathbb{Q}[\mathrm{GL}_n] \rightarrow \mathbb{Q}[G]$ (of \mathbb{Q} -algebras of regular functions), i.e., a surjection

$$\mathbb{Q}[X_{11}, \dots, X_{nn}, T]/(\det(X_{ij})T - 1) \rightarrow \mathbb{Q}[G],$$

and hence $\mathbb{Q}[G] = \mathbb{Q}[x_{11}, \dots, x_{nn}, t]$. For this presentation of $\mathbb{Q}[G]$,

$$G(\mathbb{Z}_\ell) = G(\mathbb{Q}_\ell) \cap \mathrm{GL}_n(\mathbb{Z}_\ell) \quad (\text{inside } \mathrm{GL}_n(\mathbb{Q}_\ell)).$$

For an integer $N > 0$, let

$$K(N) = \prod_\ell K_\ell, \quad \text{where } K_\ell = \begin{cases} G(\mathbb{Z}_\ell) & \text{if } \ell \nmid N \\ \{g \in G(\mathbb{Z}_\ell) \mid g \equiv I_n \pmod{\ell^{r_\ell}}\} & \text{if } r_\ell = \mathrm{ord}_\ell(N). \end{cases}$$

Then $K(N)$ is a compact open subgroup of $G(\mathbb{A}_f)$, and

$$K(N) \cap G(\mathbb{Q}) = \Gamma(N).$$

It follows that the compact open subgroups of $G(\mathbb{A}_f)$ containing $K(N)$ intersect $G(\mathbb{Q})$ exactly in the congruence subgroups of $G(\mathbb{Q})$ containing $\Gamma(N)$. Since every compact open subgroup of $G(\mathbb{A}_f)$ contains $K(N)$ for some N , this completes the proof. \square

7 Applications to manifolds

Clearly \mathbb{Z}^{n^2} is a discrete subset of \mathbb{R}^{n^2} , i.e., every point of \mathbb{Z}^{n^2} has an open neighbourhood (for the real topology) containing no other point of \mathbb{Z}^{n^2} . Therefore, $\mathrm{GL}_n(\mathbb{Z})$ is discrete in $\mathrm{GL}_n(\mathbb{R})$, and it follows that every arithmetic subgroup Γ of a group G is discrete in $G(\mathbb{R})$.

Let G be an algebraic group over \mathbb{Q} . Then $G(\mathbb{R})$ is a Lie group, and for every compact subgroup K of $G(\mathbb{R})$, $M = G(\mathbb{R})/K$ is a smooth manifold (Lee 2003, 9.22).

THEOREM 7.1 *For any discrete torsion-free subgroup Γ of $G(\mathbb{R})$, Γ acts freely on M , and $\Gamma \backslash M$ is a smooth manifold.*

PROOF. Standard; see for example Lee 2003, Chapter 9, or Milne 2005, 3.1. \square

Arithmetic subgroups are an important source of discrete groups acting freely on manifolds. To see this, we need to know that there exist many *torsion-free* arithmetic groups.

8 Torsion-free arithmetic groups

Note that $\mathrm{SL}_2(\mathbb{Z})$ is not torsion-free. For example, the following elements have finite order:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3.$$

THEOREM 8.1 *Every arithmetic group contains a torsion-free subgroup of finite index.*

For this, it suffices to prove the following statement.

LEMMA 8.2 For any prime $p \geq 3$, the subgroup $\Gamma(p)$ of $GL_n(\mathbb{Z})$ is torsion-free.

PROOF. If not, it will contain an element of order a prime ℓ , and so we will have an equation

$$(I + p^m A)^\ell = I$$

with $m \geq 1$ and A a matrix in $M_n(\mathbb{Z})$ not divisible by p (i.e., not of the form pB with B in $M_n(\mathbb{Z})$). Since I and A commute, we can expand this using the binomial theorem, and obtain an equation

$$\ell p^m A = - \sum_{i=2}^{\ell} \binom{\ell}{i} p^{mi} A^i.$$

In the case that $\ell \neq p$, the exact power of p dividing the left hand side is p^m , but p^{2m} divides the right hand side, and so we have a contradiction.

In the case that $\ell = p$, the exact power of p dividing the left hand side is p^{m+1} , but, for $2 \leq i < p$, $p^{2m+1} \mid \binom{p}{i} p^{mi}$ because $p \mid \binom{p}{i}$, and $p^{2m+1} \mid p^{mp}$ because $p \geq 3$. Again we have a contradiction. \square

9 A fundamental domain for SL_2

Let \mathcal{H} be the complex upper half plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$,

$$\Im\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\Im(z)}{|cz+d|^2}. \quad (188)$$

Therefore, $SL_2(\mathbb{R})$ acts on \mathcal{H} by holomorphic maps

$$SL_2(\mathbb{R}) \times \mathcal{H} \rightarrow \mathcal{H}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

The action is transitive, because

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} i = a^2 i + ab,$$

and the subgroup fixing i is

$$O = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 = 1 \right\}$$

(compact circle group). Thus

$$\mathcal{H} \simeq (SL_2(\mathbb{R})/O) \cdot i$$

as a smooth manifold.

PROPOSITION 9.1 *Let D be the subset*

$$\{z \in \mathbb{C} \mid -1/2 \leq \Re(z) \leq 1/2, \quad |z| \geq 1\}$$

of \mathcal{H} . Then

$$\mathcal{H} = \mathrm{SL}_2(\mathbb{Z}) \cdot D,$$

and if two points of D lie in the same orbit then neither is in the interior of D .

PROOF. Let $z_0 \in \mathcal{H}$. One checks that, for any constant A , there are only finitely many $c, d \in \mathbb{Z}$ such that $|cz_0 + d| \leq A$, and so (see (188)) we can choose a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\Im(\gamma(z_0))$ is maximal. As $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acts on \mathcal{H} as $z \mapsto z + 1$, there exists an m such that

$$-1/2 \leq \Re(T^m \gamma(z_0)) \leq 1/2.$$

I claim that $T^m \gamma(z_0) \in D$. To see this, note that $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ acts by $S(z) = -1/z$, and so

$$\Im(S(z)) = \frac{\Im(z)}{|z|^2}.$$

If $T^m \gamma(z_0) \notin D$, then $|T^m \gamma(z_0)| < 1$, and $\Im(S(T^m \gamma(z_0))) > \Im(T^m \gamma(z_0))$, contradicting the definition of γ .

The proof of the second part of the statement is omitted. \square

10 Application to quadratic forms

Consider a binary quadratic form:

$$q(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{R}.$$

Assume q is positive definite, so that its discriminant $\Delta = b^2 - 4ac < 0$.

There are many questions one can ask about such forms. For example, for which integers N is there a solution to $q(x, y) = N$ with $x, y \in \mathbb{Z}$? For this, and other questions, the answer depends only on the equivalence class of q , where two forms are said to be equivalent if each can be obtained from the other by an integer change of variables. More precisely, q and q' are **equivalent** if there is a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ taking q into q' by the change of variables,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}.$$

In other words, the forms

$$q(x, y) = (x, y) \cdot Q \cdot \begin{pmatrix} x \\ y \end{pmatrix}, \quad q'(x, y) = (x, y) \cdot Q' \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

are equivalent if $Q = A^t \cdot Q' \cdot A$ for $A \in \mathrm{SL}_2(\mathbb{Z})$.

Every positive-definite binary quadratic form can be written uniquely

$$q(x, y) = a(x - \omega y)(x - \bar{\omega} y), \quad a \in \mathbb{R}_{>0}, \quad \omega \in \mathcal{H}.$$

If we let \mathcal{Q} denote the set of such forms, there are commuting actions of $\mathbb{R}_{>0}$ and $\mathrm{SL}_2(\mathbb{Z})$ on it, and

$$\mathcal{Q}/\mathbb{R}_{>0} \simeq \mathcal{H}$$

as $\mathrm{SL}_2(\mathbb{Z})$ -sets. We say that q is **reduced** if

$$|\omega| > 1 \text{ and } -\frac{1}{2} \leq \Re(\omega) < \frac{1}{2}, \text{ or}$$

$$|\omega| = 1 \text{ and } -\frac{1}{2} \leq \Re(\omega) \leq 0.$$

More explicitly, $q(x, y) = ax^2 + bxy + cy^2$ is reduced if and only if either

$$-a < b \leq a < c \text{ or}$$

$$0 \leq b \leq a = c.$$

Theorem 9.1 implies:

Every positive-definite binary quadratic form is equivalent to a reduced form;
two reduced forms are equivalent if and only if they are equal.

We say that a quadratic form is **integral** if it has integral coefficients, or, equivalently, if $x, y \in \mathbb{Z} \implies q(x, y) \in \mathbb{Z}$.

There are only finitely many equivalence classes of integral definite binary quadratic forms with a given discriminant.

Each equivalence class contains exactly one reduced form $ax^2 + bxy + cy^2$. Since

$$4a^2 \leq 4ac = b^2 - \Delta \leq a^2 - \Delta$$

we see that there are only finitely many values of a for a fixed Δ . Since $|b| \leq a$, the same is true of b , and for each pair (a, b) there is at most one integer c such that $b^2 - 4ac = \Delta$.

This is a variant of the statement that the class number of a quadratic imaginary field is finite, and goes back to Gauss (cf. my notes on Algebraic Number Theory, 4.28, or, in more detail, Borevich and Shafarevich 1966, especially Chapter 3, §6).

11 “Large” discrete subgroups

Let Γ be a subgroup of a locally compact group G . A discrete subgroup Γ of a locally compact group G is said to be **cocompact** (or **uniform**) if G/Γ is compact. This is a way of saying that Γ is “large” relative to G . There is another weaker notion of this. On each locally compact group G , there exists a left-invariant Borel measure, unique up to a constant, called the **left-invariant Haar measure**³, which induces a measure μ on $\Gamma \backslash G$. If $\mu(\Gamma \backslash G) < \infty$, then one says that Γ has **finite covolume**, or that Γ is a **lattice** in G . If K is a compact subgroup of G , the measure on G defines a left-invariant measure on G/K , and $\mu(\Gamma \backslash G) < \infty$ if and only if the measure $\mu(\Gamma \backslash G/K) < \infty$.

EXAMPLE 11.1 Let $G = \mathbb{R}^n$, and let $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_i$. Then $\Gamma \backslash G(\mathbb{R})$ is compact if and only if $i = n$. If $i < n$, Γ does not have finite covolume. (The left-invariant measure on \mathbb{R}^n is just the usual Lebesgue measure.)

³For real Lie groups, the proof of the existence is much more elementary than in the general case (cf. Boothby 1975, VI 3.5).

EXAMPLE 11.2 Consider, $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$. The left-invariant measure on $\mathrm{SL}_2(\mathbb{R})/O \simeq \mathcal{H}$ is $\frac{dx dy}{y^2}$, and

$$\int_{\Gamma \backslash \mathcal{H}} \frac{dx dy}{y^2} = \iint_D \frac{dx dy}{y^2} \leq \int_{\sqrt{3}/2}^{\infty} \int_{-1/2}^{1/2} \frac{dx dy}{y^2} = \int_{\sqrt{3}/2}^{\infty} \frac{dy}{y^2} < \infty.$$

Therefore, $\mathrm{SL}_2(\mathbb{Z})$ has finite covolume in $\mathrm{SL}_2(\mathbb{R})$ (but it is not cocompact — $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{H}$ is not compact).

EXAMPLE 11.3 Consider $G = \mathbb{G}_m$. The left-invariant measure⁴ on \mathbb{R}^\times is $\frac{dx}{x}$, and

$$\int_{\mathbb{R}^\times / \{\pm 1\}} \frac{dx}{x} = \int_0^{\infty} \frac{dx}{x} = \infty.$$

Therefore, $G(\mathbb{Z})$ is not of finite covolume in $G(\mathbb{R})$.

EXERCISE

EXERCISE 11-1 Show that, if a subgroup Γ of a locally compact group is discrete (resp. is cocompact, resp. has finite covolume), then so also is every subgroup commensurable with Γ .

12 Reduction theory

In this section, I can only summarize the main definitions and results from Borel 1969a.

Any positive-definite real quadratic form in n variables can be written uniquely as

$$\begin{aligned} q(\vec{x}) &= t_1(x_1 + u_{12}x_2 + \cdots + u_{1n}x_n)^2 + \cdots + t_{n-1}(x_{n-1} + u_{n-1n}x_n)^2 + t_n x_n^2 \\ &= \vec{y}^t \cdot \vec{y} \end{aligned}$$

where

$$\vec{y} = \begin{pmatrix} \sqrt{t_1} & 0 & & 0 \\ 0 & \sqrt{t_2} & & 0 \\ & & \ddots & \\ 0 & 0 & & \sqrt{t_n} \end{pmatrix} \begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ 0 & 1 & \cdots & u_{2n} \\ & & \ddots & \vdots \\ 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \quad (189)$$

Let \mathcal{Q}_n be the space of positive-definite quadratic forms in n variables,

$$\mathcal{Q}_n = \{Q \in M_n(\mathbb{R}) \mid Q^t = Q, \quad \vec{x}^t Q \vec{x} > 0\}.$$

Then $\mathrm{GL}_n(\mathbb{R})$ acts on \mathcal{Q}_n by

$$B, Q \mapsto B^t Q B: \mathrm{GL}_n(\mathbb{R}) \times \mathcal{Q}_n \rightarrow \mathcal{Q}_n.$$

⁴Because $\frac{dax}{ax} = \frac{dx}{x}$; alternatively,

$$\int_{t_1}^{t_2} \frac{dx}{x} = \log(t_2) - \log(t_1) = \int_{at_1}^{at_2} \frac{dx}{x}.$$

The action is transitive, and the subgroup fixing the form I is⁵ $O_n(\mathbb{R}) = \{A \mid A^t A = I\}$, and so we can read off from (189) a set of representatives for the cosets of $O_n(\mathbb{R})$ in $GL_n(\mathbb{R})$. We find that

$$GL_n(\mathbb{R}) \simeq A \cdot N \cdot K$$

where

- ◇ K is the compact group $O_n(\mathbb{R})$,
- ◇ $A = T(\mathbb{R})^+$ for T the split maximal torus in GL_n of diagonal matrices,⁶ and
- ◇ N is the group $U_n(\mathbb{R})$.

Since A normalizes N , we can rewrite this as

$$GL_n(\mathbb{R}) \simeq N \cdot A \cdot K.$$

For any compact neighbourhood ω of 1 in N and real number $t > 0$, let

$$\mathfrak{S}_{t,\omega} = \omega \cdot A_t \cdot K$$

where

$$A_t = \{a \in A \mid a_{i,i} \leq t a_{i+1,i+1}, \quad 1 \leq i \leq n-1\}. \quad (190)$$

Any set of this form is called a **Siegel set**.

THEOREM 12.1 *Let Γ be an arithmetic subgroup in $G(\mathbb{Q}) = GL_n(\mathbb{Q})$. Then*

- (a) *for some Siegel set \mathfrak{S} , there exists a finite subset C of $G(\mathbb{Q})$ such that*

$$G(\mathbb{R}) = \Gamma \cdot C \cdot \mathfrak{S};$$

- (b) *for any $g \in G(\mathbb{Q})$ and Siegel set \mathfrak{S} , the set of $\gamma \in \Gamma$ such that*

$$g\mathfrak{S} \cap \gamma\mathfrak{S} \neq \emptyset$$

is finite.

Thus, the Siegel sets are approximate fundamental domains for Γ acting on $G(\mathbb{R})$.

Now consider an arbitrary reductive group G over \mathbb{Q} . Since we are not assuming G to be split, it may not have a split maximal torus, but, nevertheless, we can choose a torus T that is maximal among those that are split. From (G, T) , we get a root system as before (not necessarily reduced). Choose a base S for the root system. Then there is a decomposition (depending on the choice of T and S)

$$G(\mathbb{R}) = N \cdot A \cdot K$$

where K is again a maximal compact subgroup and $A = T(\mathbb{R})^+$ (Borel 1969a, 11.4, 11.9). The definition of the **Siegel sets** is the same except now⁷

$$A_t = \{a \in A \mid \alpha(a) \leq t \text{ for all } \alpha \in S\}. \quad (191)$$

Then Theorem 12.1 continues to hold in this more general situation (Borel 1969a, 13.1, 15.4).

⁵So we are reverting to using O_n for the orthogonal group of the form $x_1^2 + \cdots + x_n^2$.

⁶The $+$ denotes the identity component of $T(\mathbb{R})$ for the real topology. Thus, for example,

$$(\mathbb{G}_m(\mathbb{R})^r)^+ = (\mathbb{R}^r)^+ = (\mathbb{R}_{>0})^r.$$

⁷Recall that, with the standard choices, $\chi_1 - \chi_2, \dots, \chi_{n-1} - \chi_n$ is a base for the roots of T in GL_n , so this definition agrees with that in (190).

EXAMPLE 12.2 The images of the Siegel sets for SL_2 in \mathcal{H} are the sets

$$\mathfrak{S}_{t,u} = \{z \in \mathcal{H} \mid \Im(z) \geq t, \quad |\Re(z)| \leq u\}.$$

THEOREM 12.3 *If $\mathrm{Hom}_k(G, \mathbb{G}_m) = 0$, then every Siegel set has finite measure.*

PROOF. Borel 1969a, 12.5. □

THEOREM 12.4 *Let G be a reductive group over \mathbb{Q} , and let Γ be an arithmetic subgroup of $G(\mathbb{Q})$.*

(a) *The volume of $\Gamma \backslash G(\mathbb{R})$ is finite if and only if G has no nontrivial character over \mathbb{Q} (for example, if G is semisimple).*

(b) *The quotient $\Gamma \backslash G(\mathbb{R})$ is compact if and only if it G has no nontrivial character over \mathbb{Q} and $G(\mathbb{Q})$ has no unipotent element $\neq 1$.*

PROOF. (a) The necessity of the conditions follows from (11.3). The sufficiency follows from (12.2) and (12.3).

(b) See Borel 1969a, 8.4. □

EXAMPLE 12.5 Let B be a quaternion algebra, and let G be the associated group of elements of B of norm 1 (we recall the definitions in 15.2 below).

(a) If $B \approx M_2(\mathbb{R})$, then $G = \mathrm{SL}_2(\mathbb{R})$, and $G(\mathbb{Z}) \backslash G(\mathbb{R})$ has finite volume, but is not compact ($\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is a unipotent in $G(\mathbb{Q})$).

(b) If B is a division algebra, but $\mathbb{R} \otimes_{\mathbb{Q}} B \approx M_2(\mathbb{R})$, then $G(\mathbb{Z}) \backslash G(\mathbb{R})$ is compact (if $g \in G(\mathbb{Q})$ is unipotent, then $g - 1 \in B$ is nilpotent, and hence zero because B is a division algebra).

(c) If $\mathbb{R} \otimes_{\mathbb{Q}} B$ is a division algebra, then $G(\mathbb{R})$ is compact (and $G(\mathbb{Z})$ is finite).

EXAMPLE 12.6 Let $G = \mathrm{SO}(q)$ for some nondegenerate quadratic form q over \mathbb{Q} . Then $G(\mathbb{Z}) \backslash G(\mathbb{R})$ is compact if and only if q doesn't represent zero in \mathbb{Q} , i.e., $q(\vec{x}) = 0$ does not have a nontrivial solution in \mathbb{Q}^n (Borel 1969a, 8.6).

13 Presentations

In this section, I assume some familiarity with free groups and presentations (see, for example, GT, Chapter 2).

PROPOSITION 13.1 *The group $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

PROOF. Let Γ' be the subgroup of $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ generated by S and T . The argument in the proof of (9.1) shows that $\Gamma' \cdot D = \mathcal{H}$.

Let z_0 lie in the interior of D , and let $\gamma \in \Gamma$. Then there exist $\gamma' \in \Gamma'$ and $z \in D$ such that $\gamma z_0 = \gamma' z$. Now $\gamma'^{-1} \gamma z_0$ lies in D and z_0 lies in the interior of D , and so $\gamma'^{-1} \gamma = \pm I$ (see 9.1). □

In fact $SL_2(\mathbb{Z})/\{\pm I\}$ has a presentation $\langle S, T \mid S^2, (ST)^3 \rangle$. It is known that every torsion-free subgroup Γ of $SL_2(\mathbb{Z})$ is free on $1 + \frac{(SL_2(\mathbb{Z}) : \Gamma)}{12}$ generators (thus the subgroup may be free on a larger number of generators than the group itself). For example, the commutator subgroup of $SL_2(\mathbb{Z})$ has index 12, and is the free group on the generators $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

For a general algebraic group G over \mathbb{Q} , choose \mathfrak{S} and C as in (12.1a), and let

$$D = \bigcup_{g \in C} g\mathfrak{S}/K.$$

Then D is a closed subset of $G(\mathbb{R})/K$ such that $\Gamma \cdot D = G(\mathbb{R})/K$ and

$$\{\gamma \in \Gamma \mid \gamma D \cap D \neq \emptyset\}$$

is finite. One shows, using the topological properties of D , that this last set generates Γ , and that, moreover, Γ has a finite presentation.

14 The congruence subgroup problem

Consider an algebraic subgroup G of GL_n . Is every arithmetic subgroup congruence? That is, does every subgroup commensurable with $G(\mathbb{Z})$ contain

$$\Gamma(N) \stackrel{\text{def}}{=} \text{Ker}(G(\mathbb{Z}) \rightarrow G(\mathbb{Z}/N\mathbb{Z}))$$

for some N .

That $SL_2(\mathbb{Z})$ has noncongruence arithmetic subgroups was noted by Klein as early as 1880. For a proof that $SL_2(\mathbb{Z})$ has infinitely many subgroups of finite index that are not congruence subgroups see Sury 2003, 3-4.1. The proof proceeds by showing that the groups occurring as quotients of $SL_2(\mathbb{Z})$ by principal congruence subgroups are of a rather special type, and then exploits the known structure of $SL_2(\mathbb{Z})$ as an abstract group (see above) to construct many finite quotients not of his type. It is known that, in fact, congruence subgroups are sparse among arithmetic groups: if $N(m)$ denotes the number of congruence subgroups of $SL_2(\mathbb{Z})$ of index $\leq m$ and $N'(m)$ the number of arithmetic subgroups, then $N(m)/N'(m) \rightarrow 0$ as $m \rightarrow \infty$.

However, SL_2 is unusual. For split simply connected almost-simple groups other than SL_2 , for example, for SL_n ($n \geq 3$), Sp_{2n} ($n \geq 2$), all arithmetic subgroups are congruence.

In contrast to arithmetic subgroups, the image of a congruence subgroup under an isogeny of algebraic groups need not be a congruence subgroup.

Let G be a semisimple group over \mathbb{Q} . The arithmetic and congruence subgroups of $G(\mathbb{Q})$ define topologies on it, namely, the topologies for which the subgroups form a neighbourhood base for 1. We denote the corresponding completions by \hat{G} and \bar{G} . Because every congruence group is arithmetic, the identity map on $G(\mathbb{Q})$ gives a surjective homomorphism $\hat{G} \rightarrow \bar{G}$, whose kernel $C(G)$ is called the **congruence kernel**. This kernel is trivial if and only if all arithmetic subgroups are congruence. The modern congruence subgroup problem is to compute $C(G)$. For example, the group $C(SL_2)$ is infinite. There is a precise conjecture predicting exactly when $C(G)$ is finite, and what its structure is when it is finite.

Now let G be simply connected, and let $G' = G/N$ where N is a nontrivial subgroup of $Z(G)$. Consider the diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C(G) & \longrightarrow & \hat{G} & \longrightarrow & \bar{G} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \hat{\pi} & & \downarrow \bar{\pi} & & \\ 1 & \longrightarrow & C(G') & \longrightarrow & \hat{G}' & \longrightarrow & \bar{G}' & \longrightarrow & 1. \end{array}$$

It is known that $\bar{G} = G(\mathbb{A}_f)$, and that the kernel of $\hat{\pi}$ is $N(\mathbb{Q})$, which is finite. On the other hand, the kernel of $\bar{\pi}$ is $N(\mathbb{A}_f)$, which is infinite. Because $\text{Ker}(\bar{\pi}) \neq N(\mathbb{Q})$, $\pi: G(\mathbb{Q}) \rightarrow G'(\mathbb{Q})$ doesn't map congruence subgroups to congruence subgroups, and because $C(G')$ contains a subgroup isomorphic to $N(\mathbb{A}_f)/N(\mathbb{Q})$, $G'(\mathbb{Q})$ contains a noncongruence arithmetic subgroup.

It is known that $C(G)$ is finite if and only if it is contained in the centre of $\widehat{G(\mathbb{Q})}$. For an geometrically almost-simple simply connected algebraic group G over \mathbb{Q} , the modern congruence subgroup problem has largely been solved when $C(G)$ is known to be central, because then $C(G)$ is the dual of the so-called metaplectic kernel which is known to be a subgroup of the predicted group (except possibly for certain outer forms of SL_n) and equal to it many cases (work of Gopal Prasad, Raghunathan, Rapinchuk, and others).

15 The theorem of Margulis

Already Poincaré wondered about the possibility of describing all discrete subgroups of finite covolume in a Lie group G . The profusion of such subgroups in $G = \text{PSL}_2(\mathbb{R})$ makes one at first doubt of any such possibility. However, $\text{PSL}_2(\mathbb{R})$ was for a long time the only simple Lie group which was known to contain non-arithmetic discrete subgroups of finite covolume, and further examples discovered in 1965 by Makarov and Vinberg involved only few other Lie groups, thus adding credit to conjectures of Selberg and Pyatetski-Shapiro to the effect that “for most semisimple Lie groups” discrete subgroups of finite covolume are necessarily arithmetic. Margulis's most spectacular achievement has been the complete solution of that problem and, in particular, the proof of the conjecture in question.

Tits 1980

DEFINITION 15.1 Let H be a semisimple algebraic group over \mathbb{R} . A subgroup Γ of $H(\mathbb{R})$ is *arithmetic* if there exists an algebraic group G over \mathbb{Q} , a surjective map $G_{\mathbb{R}} \rightarrow H$ such that the kernel of $\varphi(\mathbb{R}): G(\mathbb{R}) \rightarrow H(\mathbb{R})$ is compact, and an arithmetic subgroup Γ' of $G(\mathbb{R})$ such that $\varphi(\Gamma')$ is commensurable with Γ .

EXAMPLE 15.2 Let B be a quaternion algebra over a finite extension F of \mathbb{Q} ,

$$\begin{aligned} B &= F + Fi + Fj + Fk \\ i^2 &= a, \quad j^2 = b, \quad ij = k = -ji. \end{aligned}$$

The norm of an element $w + xi + yj + zk$ of $R \otimes_{\mathbb{Q}} B$ is

$$(w + xi + yj + zk)(w - xi - yj - zk) = w^2 - ax^2 - by^2 + abz^2.$$

Then B defines an almost-simple semisimple group G over \mathbb{Q} such that, for any \mathbb{Q} -algebra R ,

$$G(R) = \{b \in R \otimes_{\mathbb{Q}} B \mid \text{Nm}(b) = 1\}.$$

Assume that F is totally real, i.e.,

$$F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R} \times \cdots \times \mathbb{R},$$

and that correspondingly,

$$B \otimes_{\mathbb{Q}} \mathbb{R} \approx M_2(\mathbb{R}) \times \mathbb{H} \times \cdots \times \mathbb{H}$$

where \mathbb{H} is the usual quaternion algebra over \mathbb{R} (corresponding to $(a, b) = (-1, -1)$). Then

$$G(\mathbb{R}) \approx \text{SL}_2(\mathbb{R}) \times \mathbb{H}^1 \times \cdots \times \mathbb{H}^1$$

$$\mathbb{H}^1 = \{w + xi + yj + zk \in \mathbb{H} \mid w^2 + x^2 + y^2 + z^2 = 1\}.$$

Nonisomorphic B 's define different commensurability classes of arithmetic subgroups of $\text{SL}_2(\mathbb{R})$, and all such classes arise in this way.

Not every discrete subgroup in $\text{SL}_2(\mathbb{R})$ (or $\text{SL}_2(\mathbb{R})/\{\pm I\}$) of finite covolume is arithmetic. According to the Riemann mapping theorem, every compact Riemann surface of genus $g \geq 2$ is the quotient of \mathcal{H} by a discrete subgroup of $\text{Aut}(\mathcal{H}) = \text{SL}_2(\mathbb{R})/\{\pm I\}$ acting freely on \mathcal{H} . Since there are continuous families of such Riemann surfaces, this shows that there are uncountably many discrete cocompact subgroups in $\text{SL}_2(\mathbb{R})/\{\pm I\}$ (therefore also in $\text{SL}_2(\mathbb{R})$), but there only countably many arithmetic subgroups.

The following amazing theorem of Margulis shows that SL_2 is exceptional in this regard:

THEOREM 15.3 *Let Γ be a discrete subgroup of finite covolume in a noncompact almost-simple real algebraic group H ; then Γ is arithmetic unless H is isogenous to $\text{SO}(1, n)$ or $\text{SU}(1, n)$.*

PROOF. For the proof, see Margulis 1991 or Zimmer 1984, Chapter 6. For a discussion of the theorem, see Witte Morris 2008, §5B. □

Here

$$\text{SO}(1, n) \text{ correspond to } x_1^2 + \cdots + x_n^2 - x_{n+1}^2$$

$$\text{SU}(1, n) \text{ corresponds to } z_1 \bar{z}_1 + \cdots + z_n \bar{z}_n - z_{n+1} \bar{z}_{n+1}.$$

Note that, because $\text{SL}_2(\mathbb{R})$ is isogenous to $\text{SO}(1, 2)$, the theorem doesn't apply to it.

16 Shimura varieties

Let $U_1 = \{z \in \mathbb{C} \mid z\bar{z} = 1\}$. Recall that for a group G , $G^{\text{ad}} = G/Z(G)$ and that G is said to be adjoint if $G = G^{\text{ad}}$ (i.e., if $Z(G) = 1$).

THEOREM 16.1 *Let G be a semisimple adjoint group over \mathbb{R} , and let $u: U_1 \rightarrow G(\mathbb{R})$ be a homomorphism such that*

- (a) *only the characters $z^{-1}, 1, z$ occur in the representation of U_1 on $\text{Lie}(G)_{\mathbb{C}}$;*

(b) *the subgroup*

$$K_{\mathbb{C}} = \{g \in G(\mathbb{C}) \mid g = \text{inn}(u(-1))(\bar{g})\}$$

of $G(\mathbb{C})$ is compact; and

(c) *$u(-1)$ does not project to 1 in any simple factor of G .*

Then,

$$K = K_{\mathbb{C}} \cap G(\mathbb{R})^+$$

is a maximal compact subgroup of $G(\mathbb{R})^+$, and there is a unique structure of a complex manifold on $X = G(\mathbb{R})^+ / K$ such that $G(\mathbb{R})^+$ acts by holomorphic maps and $u(z)$ acts on the tangent space at $p = 1K$ as multiplication by z . (Here $G(\mathbb{R})^+$ denotes the identity for the real topology.)

PROOF. See Helgason 1978, VIII; see also Milne 2005, 1.21. □

The complex manifolds arising in this way are the **hermitian symmetric domains**. They are not the complex points of any algebraic variety, but certain quotients are.

THEOREM 16.2 *Let G be a simply connected semisimple algebraic group over \mathbb{Q} having no simple factor H with $H(\mathbb{R})$ compact. Let $u: U_1 \rightarrow G^{\text{ad}}(\mathbb{R})$ be a homomorphism satisfying (a) and (b) of (16.1), and let $X = G^{\text{ad}}(\mathbb{R})^+ / K$ with its structure as a complex manifold. For each torsion-free arithmetic subgroup Γ of $G(\mathbb{Q})$, $\Gamma \backslash X$ has a unique structure of an algebraic variety compatible with its complex structure.*

PROOF. This is the theorem of Baily and Borel, strengthened by a theorem of Borel. See Milne 2005, 3.12, for a discussion of the theorem. □

EXAMPLE 16.3 Let $G = \text{SL}_2$. For $z \in \mathbb{C}$, choose a square root $a + ib$, and map z to $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ in $\text{SL}_2(\mathbb{R}) / \{\pm I\}$. For example, $u(-1) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and

$$K_{\mathbb{C}} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \text{SL}_2(\mathbb{C}) \mid |a|^2 + |b|^2 = 1 \right\},$$

which is compact. Moreover,

$$K \stackrel{\text{def}}{=} K_{\mathbb{C}} \cap \text{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \text{SL}_2(\mathbb{R}) \mid a^2 + b^2 = 1 \right\}.$$

Therefore $G(\mathbb{R}) / K \approx \mathcal{H}$.

THEOREM 16.4 *Let G , u , and X be as in (16.2). If Γ is a congruence subgroup, then $\Gamma \backslash X$ has a canonical model over a specific finite extension \mathbb{Q}_{Γ} of \mathbb{Q} .*

PROOF. For a discussion of the theorem, see Milne 2005, §§12–14. □

The varieties arising in this way are called **connected Shimura varieties**. They are very interesting. For example, let $\Gamma_0(N)$ be the congruence subgroup of $\text{SL}_2(\mathbb{Q})$ consisting of matrices the $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\text{SL}_2(\mathbb{Z})$ with c divisible by N . Then $\mathbb{Q}_{\Gamma_0(N)} = \mathbb{Q}$, and so the algebraic curve $\Gamma_0(N) \backslash \mathcal{H}$ has a canonical model $Y_0(N)$ over \mathbb{Q} . It is known that, for every elliptic curve E over \mathbb{Q} , there exists a nonconstant map $Y_0(N) \rightarrow E$ for some N , and that from this Fermat's last theorem follows.

Bibliography

- ABE, E. 1980. Hopf algebras, volume 74 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge. Translated from the Japanese by Hisae Kinoshita and Hiroko Tanaka.
- ALLCOCK, D. 2009. A new approach to rank one linear algebraic groups. *J. Algebra* 321:2540–2544.
- ANDRÉ, Y. 1992. Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part. *Compositio Math.* 82:1–24.
- ARTIN, E. 1957. Geometric algebra. Interscience Publishers, Inc., New York-London.
- ARTIN, M. 1991. Algebra. Prentice Hall Inc., Englewood Cliffs, NJ.
- BARSOZZI, I. 1955a. Structure theorems for group-varieties. *Ann. Mat. Pura Appl. (4)* 38:77–119.
- BARSOZZI, I. 1955b. Un teorema di struttura per le varietà grupicali. *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (8)* 18:43–50.
- BOOTHBY, W. M. 1975. An introduction to differentiable manifolds and Riemannian geometry. Academic Press, New York-London.
- BOREL, A. 1969a. Introduction aux groupes arithmétiques. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris.
- BOREL, A. 1969b. Linear algebraic groups. Notes taken by Hyman Bass. W. A. Benjamin, Inc., New York-Amsterdam.
- BOREL, A. 1975. Linear representations of semi-simple algebraic groups, pp. 421–440. *In* Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974). Amer. Math. Soc., Providence, R.I.
- BOREL, A. 1991. Linear algebraic groups. Springer-Verlag, New York.
- BOREL, A. 2001. Essays in the history of Lie groups and algebraic groups, volume 21 of *History of Mathematics*. American Mathematical Society, Providence, RI.
- BOREVIČH, A. I. AND SHAFAREVICH, I. R. 1966. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York.

- BOURBAKI, N. A. Algèbre. Éléments de mathématique. Hermann; Masson, Paris.
- BOURBAKI, N. LIE. Groupes et Algèbres de Lie. Éléments de mathématique. Hermann; Masson, Paris. Chap. I, Hermann 1960; Chap. II,III, Hermann 1972; Chap. IV,V,VI, Masson 1981; Chap. VII,VIII, Masson 1975; Chap. IX, Masson 1982 (English translation available from Springer).
- CARTIER, P. 1956. Dualité de Tannaka des groupes et des algèbres de Lie. *C. R. Acad. Sci. Paris* 242:322–325.
- CARTIER, P. 1962. Groupes algébriques et groupes formels, pp. 87–111. *In* Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962). Librairie Universitaire, Louvain.
- CARTIER, P. 2007. A primer of Hopf algebras, pp. 537–615. *In* Frontiers in number theory, physics, and geometry. II. Springer, Berlin. Preprint available at IHES.
- CHEVALLEY, C. 1960. Une démonstration d’un théorème sur les groupes algébriques. *J. Math. Pures Appl.* (9) 39:307–317.
- CHEVALLEY, C. C. 1946 1957. Theory of Lie groups. I. Princeton University Press, Princeton, N. J.
- CHEVALLEY, C. C. 1951. Théorie des groupes de Lie. Tome II. Groupes algébriques. Actualités Sci. Ind. no. 1152. Hermann & Cie., Paris.
- CONRAD, B. 2002. A modern proof of Chevalley’s theorem [sic] on algebraic groups. *J. Ramanujan Math. Soc.* 17:1–18.
- CONRAD, B., GABBER, O., AND PRASAD, G. 2010. Pseudo-reductive groups, volume 17 of *New Mathematical Monographs*. Cambridge University Press, Cambridge.
- DĂSCĂLESCU, S., NĂSTĂSESCU, C., AND RAIANU, Ș. 2001. Hopf algebras: an introduction, volume 235 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York.
- DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics 900. Springer-Verlag, Berlin.
- DEMAZURE, M. 1972. Lectures on p -divisible groups. Springer-Verlag, Berlin.
- DEMAZURE, M. AND GABRIEL, P. 1970. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeur, Paris.
- ERDMANN, K. AND WILDON, M. J. 2006. Introduction to Lie algebras. Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London.
- FIEKER, C. AND DE GRAAF, W. A. 2007. Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras. *LMS J. Comput. Math.* 10:271–287.
- FIORISI, R. AND GAVARINI, F. 2008. Chevalley supergroups. arXiv:0808.07851.
- GREENBERG, M. J. 1961. Schemata over local rings. *Ann. of Math.* (2) 73:624–648.

- GREENBERG, M. J. 1963. Schemata over local rings. II. *Ann. of Math. (2)* 78:256–266.
- HALL, B. C. 2003. Lie groups, Lie algebras, and representations, volume 222 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.
- HARTSHORNE, R. 1977. Algebraic geometry. Springer-Verlag, New York.
- HAWKINS, T. 2000. Emergence of the theory of Lie groups. Sources and Studies in the History of Mathematics and Physical Sciences. Springer-Verlag, New York. An essay in the history of mathematics 1869–1926.
- HELGASON, S. 1978. Differential geometry, Lie groups, and symmetric spaces, volume 80 of *Pure and Applied Mathematics*. Academic Press Inc., New York.
- HELGASON, S. 1990. A centennial: Wilhelm Killing and the exceptional groups. *Math. Intelligencer* 12:54–57.
- HELGASON, S. 1994. Sophus Lie, the mathematician, pp. 3–21. In *The Sophus Lie Memorial Conference (Oslo, 1992)*. Scand. Univ. Press, Oslo.
- HUMPHREYS, J. E. 1972. Introduction to Lie algebras and representation theory. Springer-Verlag, New York.
- HUMPHREYS, J. E. 1975. Linear algebraic groups. Springer-Verlag, New York.
- IWAHORI, N. 1954. On some matrix operators. *J. Math. Soc. Japan* 6:76–105.
- JACOBSON, N. 1962. Lie algebras. Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers, New York-London. Reprinted by Dover 1979.
- KNESER, M. 1969. Lectures on Galois cohomology of classical groups. Tata Institute of Fundamental Research, Bombay.
- KOLCHIN, E. R. 1948. On certain concepts in the theory of algebraic matrix groups. *Ann. of Math. (2)* 49:774–789.
- LEE, D. H. 1999. Algebraic subgroups of Lie groups. *J. Lie Theory* 9:271–284.
- LEE, D. H. 2002. The structure of complex Lie groups, volume 429 of *Chapman & Hall/CRC Research Notes in Mathematics*. Chapman & Hall/CRC, Boca Raton, FL.
- LEE, J. M. 2003. Introduction to smooth manifolds, volume 218 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.
- MACLANE, S. 1971. Categories for the working mathematician. Springer-Verlag, New York. Graduate Texts in Mathematics, Vol. 5.
- MARGULIS, G. A. 1991. Discrete subgroups of semisimple Lie groups, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin.
- MILNE, J. S. 1980. Etale cohomology, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J.

- MILNE, J. S. 2005. Introduction to Shimura varieties, pp. 265–378. In J. Arthur and R. Kottwitz (eds.), Harmonic analysis, the trace formula, and Shimura varieties, volume 4 of *Clay Math. Proc.* Amer. Math. Soc., Providence, RI. Also available at www.claymath.org/library/.
- MUMFORD, D. 1966. Introduction to algebraic geometry. Harvard Notes. (Reprinted, with the introduction of errors, by Springer as *The Red Book of Varieties and Schemes*, 1999).
- NOETHER, E. 1927. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Mathematische Annalen* 96:26–61.
- OESTERLÉ, J. 1984. Nombres de Tamagawa et groupes unipotents en caractéristique p . *Invent. Math.* 78:13–88.
- OORT, F. 1966. Algebraic group schemes in characteristic zero are reduced. *Invent. Math.* 2:79–80.
- PERRIN, D. 1976. Approximation des schémas en groupes, quasi compacts sur un corps. *Bull. Soc. Math. France* 104:323–335.
- PINK, R. 2005. Finite group schemes. Available at the author's website www.math.ethz.ch/~pink/.
- PLATONOV, V. AND RAPINCHUK, A. 1994. Algebraic groups and number theory, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA.
- ROSENBLICHT, M. 1956. Some basic theorems on algebraic groups. *Amer. J. Math.* 78:401–443.
- RUSSELL, P. 1970. Forms of the affine line and its additive group. *Pacific J. Math.* 32:527–539.
- SAAVEDRA RIVANO, N. 1972. Catégories Tannakiennes. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin.
- SCHARLAU, W. 1985. Quadratic and Hermitian forms, volume 270 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin.
- SELBACH, M. 1976. Klassifikationstheorie halbeinfacher algebraischer Gruppen. Mathematisches Institut der Universität Bonn, Bonn. Diplomarbeit, Univ. Bonn, Bonn, 1973, Bonner Mathematische Schriften, Nr. 83.
- SERRE, J.-P. 1965. Lie algebras and Lie groups, volume 1964 of *Lectures given at Harvard University*. W. A. Benjamin, Inc., New York-Amsterdam.
- SERRE, J.-P. 1966. Algèbres de Lie semi-simples complexes. W. A. Benjamin, inc., New York-Amsterdam. English translation published by Springer Verlag 1987.
- SERRE, J.-P. 1987. Complex semisimple Lie algebras. Springer-Verlag, New York.
- SERRE, J.-P. 1993. Gèbres. *Enseign. Math.* (2) 39:33–85.
- SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 1,2. Springer-Verlag, Berlin.

- SPRINGER, T. A. 1979. Reductive groups, pp. 3–27. *In Automorphic forms, representations and L -functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I.*
- SPRINGER, T. A. 1989. Linear algebraic groups, pp. 5–136, 310–314, 315. *In Algebraic geometry, 4 (Russian), Itogi Nauki i Tekhniki. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow. Translated from the English. An English translation of the volume was published by Springer in 1996.*
- SPRINGER, T. A. 1998. Linear algebraic groups, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA.
- STEINBERG, R. 1998. The isomorphism and isogeny theorems for reductive algebraic groups, pp. 233–240. *In Algebraic groups and their representations (Cambridge, 1997), volume 517 of NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. Kluwer Acad. Publ., Dordrecht.*
- STEINBERG, R. 1999. The isomorphism and isogeny theorems for reductive algebraic groups. *J. Algebra* 216:366–383.
- SURY, B. 2003. The congruence subgroup problem, volume 24 of *Texts and Readings in Mathematics*. Hindustan Book Agency, New Delhi.
- SWEEDLER, M. E. 1969. Hopf algebras. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York.
- TAKEUCHI, M. 1972. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.* 7:251–270.
- TATE, J. 1997. Finite flat group schemes, pp. 121–154. *In Modular forms and Fermat’s last theorem (Boston, MA, 1995). Springer, New York.*
- TITS, J. 1966. Classification of algebraic semisimple groups, pp. 33–62. *In Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965). Amer. Math. Soc., Providence, R.I., 1966.*
- TITS, J. 1967. Lectures on Algebraic Groups, fall term 1966–1967, Yale University.
- TITS, J. 1971. Représentations linéaires irréductibles d’un groupe réductif sur un corps quelconque. *J. Reine Angew. Math.* 247:196–220.
- TITS, J. 1980. The work of Gregori Aleksandrovitch Margulis. *In Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 57–63, Helsinki. Acad. Sci. Fennica.*
- VARADARAJAN, V. S. 2004. Supersymmetry for mathematicians: an introduction, volume 11 of *Courant Lecture Notes in Mathematics*. New York University Courant Institute of Mathematical Sciences, New York.
- WATERHOUSE, W. C. 1975. Basically bounded functors and flat sheaves. *Pacific J. Math.* 57:597–610.

- WATERHOUSE, W. C. 1979. Introduction to affine group schemes, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.
- WEIL, A. 1960. Adeles and algebraic groups. Mimeographed Notes of a Seminar at IAS, 1959–1960. Reprinted by Birkhäuser Boston, 1982.
- WEIL, A. 1962. Foundations of algebraic geometry. American Mathematical Society, Providence, R.I.
- WITTE MORRIS, D. 2008. Introduction to Arithmetic Groups, v0.5. arXiv:math.DG/0106063.
- ZIMMER, R. J. 1984. Ergodic theory and semisimple groups, volume 81 of *Monographs in Mathematics*. Birkhäuser Verlag, Basel.

Index

- action, 67, 353
 - continuous, 170
 - of a monoid, 67
 - semi-linear, 219, 386
- acts through a character, 116, 168
- affine group
 - étale, 147
 - étale, 149
 - finite flat, 144
- algebra
 - affine, 56
 - central, 225
 - Clifford, 209
 - division, 225
 - étale, 145, 148
 - graded, 208
 - Hopf, 45
 - Lie, 239
 - opposite, 213
 - simple, 225
 - tensor, 209
- algebraic envelope
 - complex, 331
 - real, 331
- algebraic group
 - absolutely almost-simple, 223
 - almost-simple, 198, 286
 - anisotropic, 331
 - connected, 62
 - constant finite, 14, 29
 - diagonalizable, 166
 - finite, 50
 - flat, 50
 - general linear, 31
 - general linear GL_n , 14
 - geometrically almost-simple, 200, 223
 - multiplicative type, 169
 - of monomial matrices, 33
 - orthogonal, 32, 207
 - pseudoreductive, 195
 - reduced, 61
 - reduced attached to, 61
 - reductive, 16, 195
 - semisimple, 15, 195
 - simple, 198, 286
 - simply connected, 199, 376
 - smooth, 62
 - solvable, 16, 189
 - split, 193
 - special linear, 31
 - special linear SL_n , 14
 - special orthogonal, 207
 - split semisimple, 323
 - symplectic, 32
 - unipotent, 16
 - split, 181
 - wound, 183
- algebraic matrix group, 81
- algebraic space
 - regular, 62
 - smooth, 62
- algebraic variety
 - affine, 57
- almost-simple, 15, 127
- almost-simple factor, 198
- α_p , 30
- anisotropic kernel, 395
- antipode, 44
- automorphism
 - elementary, 306
 - special, 306
- automorphs, 207
- base
 - for a root system, 299
- basis
 - orthogonal, 204
- $\mathfrak{b}(F)$, 265
- bi-algebra, 43
 - commutative, 44
 - finitely generated, 44
 - finitely presented, 44
- bi-ideal, 52
- bilinear form
 - associative, 277
- bracket, 239
- Cartan subalgebra, 373
- category
 - linear, 137, 233
 - neutral tannakian, 235
 - rigid tensor, 234
 - tensor, 233
- centralize, 85
- centralizer, 261
- centre, 241
 - of an affine group, 84
- character, 116
- classifies, 383
- co-algebra
 - co-commutative, 49
- coaction, 97
- coalgebra, 41
 - coétale, 172
 - in a category, 140
- cocompact, 405
- coconnected, 177
- cocycle, 217, 384
- cocycles
 - equivalent, 217, 384
 - principal, 218, 385
- coideal, 52
- comodule
 - contragredient, 100
 - dual, 100
 - finite-dimensional, 97
 - free, 98
 - in a category, 140
 - over a bialgebra, 101

- right, 97
- components
 - irreducible, 55
- congruence kernel, 409
- connected
 - algebraic group, 14
 - strongly, 127
- contragredient
 - of a representation, 105
- coroots, 341
- correspondence
 - Tannaka, 236
- $D_{\alpha}(V)$, 30
- decomposition
 - Jordan, 134, 136
- degree
 - of an algebra, 217
- dense, 79
- derivation, 246
- diagram, 324
- dimension
 - Krull, 58
 - of an algebraic group, 59
 - of an algebraic space, 58
- \mathbb{D}_n , 16
- dominant, 379
- dual
 - Cartier, 50
 - of a representation, 105
 - Tannaka, 236
- eigenspace
 - generalized, 132
 - with character, 117
- element
 - group-like, 116, 163
 - semisimple, 186
 - unipotent, 186
- embedding, 73
- endomorphism
 - diagonalizable, 132
 - has all its eigenvalues, 132
 - locally finite, 135
 - nilpotent, 132
 - semisimple, 132
 - unipotent, 132
- equivalent, 404
- exact sequence, 88
- connected étale, 158
- finite covolume, 405
- fixed
 - vector, 104
- flag, 190
 - maximal, 358
 - totally isotropic, 358
- form
 - inner, 224, 394
 - quadratic, 203
- function
 - representative, 51
- functor
 - fibre, 235
 - fibred product, 34
 - representable, 21
 - tensor, 234
- \mathbb{G}_a , 29
 - geometrically almost-simple, 393
- GL_n , 31
- \mathbb{G}_m , 29
 - gradation, 236
 - graded, 208
- group
 - additive, 22, 29
 - algebraic matrix, 81
 - Clifford, 215
 - constant algebraic, 49
 - derived, 183, 187
 - fundamental, 148
 - Γ -, 217, 384
 - isotropy, 113, 353
 - multiplicative, 29
 - of monomial matrices, 17
 - root, 345
 - solvable, 183
 - stability, 113
 - Tannaka, 236
 - trivial algebraic, 29
- group algebra, 164
- group object, 47
- group scheme, 55
 - affine, 55
 - affine algebraic, 58
- group variety, 58
- Haar measure, 405
- height, 58
- hermitian, 231
 - skew, 231
- hermitian symmetric domain, 412
- homomorphism
 - crossed, 217
 - Γ -, 218, 385
 - injective, 73
 - of bialgebras, 43
 - of co-algebras, 42
 - of comodules, 97
 - of Hopf algebras, 45
 - of Lie algebras, 240
 - of monoids, 26
 - of superalgebras, 208
 - surjective, 85
- homomorphisms
 - compatible, 218, 385
 - of representations, 96
- Hopf algebra
 - coconnected, 177
- ideal
 - augmentation, 76
 - Hopf, 52
- idempotent, 152
 - trivial, 152
- idempotents
 - complete set of orthogonal, 152
 - orthogonal, 152
- index, 395
 - Witt, 207
- inner product, 296, 371
- inversion, 44
- involution, 213, 227
 - of the first kind, 227
 - of the second kind, 227
- irreducible, 55
- isogenous, 15
- isogeny, 15
 - of root data, 377
- isometry, 204
- Jacobi identity, 240
- kernel
 - of a homomorphism, 76
- Killing form, 279
- lattice, 371, 405
 - dual, 303
 - partial, 371
 - root, 304, 378
 - weight, 379

- Lie algebra
 - algebraic, 253
 - reductive, 277, 365
 - semisimple
 - split, 308
 - split semisimple, 308
 - toral, 308
- Lie group
 - algebraic, 329, 330
 - complex, 327
 - linear, 327
 - real, 327
 - reductive, 327
- map
 - lives in, 142
 - quotient, 85
 - tensor, 237
 - transposition, 42
- module
 - Dieudonné, 150
- monoid, 26
 - affine, 26
- monoid object, 47
 - morphism of, 47
- monoid scheme
 - affine algebraic, 58
- monoid variety, 58
- μ_n , 29
- $\mathfrak{n}(F)$, 265
- noetherian, 55
- norm
 - reduced, 226
- normalize, 85
- normalizer, 261
- object
 - dual, 234
 - monogenic, 138
 - trivial, 234
- O_n , 32
- p -group, 144
- part
 - semisimple, 134, 136
 - unipotent, 134, 136
- perfect pairing, 371
- plane
 - hyperbolic, 207
- point
 - regular, 62
- product
 - almost direct, 15, 198, 286
- semidirect, 89
 - semidirect defined by
 - a map, 90
- quadratic form
 - integral, 405
 - reduced, 405
- quadratic space
 - anisotropic, 204
 - isotropic, 204
 - nondegenerate, 204
 - regular, 204
 - singular, 204
 - totally isotropic, 204
- quotient
 - by N , 87
 - of an algebraic group, 85
 - of G by H , 353
- quotient object, 138
- radical, 194
 - geometric, 195
 - geometric unipotent, 195
 - nilpotent, 306
 - of a Lie algebra, 266
 - unipotent, 194
- rank
 - of a reductive group, 343
 - of a root system, 297
 - of semisimple Lie algebra, 309
- reduced, 57, 61
 - geometrically, 57
- reductive group
 - split, 336, 337
- reflection, 204, 296
 - with vector α , 296
- regular, 62
- represent, 21
- representation
 - diagonalizable, 167
 - faithful, 95
 - finite-dimensional, 95
 - linear, 95
 - of a Lie algebra, 258
 - regular, 95, 96
- ring
 - coordinate, 54
 - of dual numbers, 242
 - of finite adeles, 401
 - regular, 62
- root
 - highest, 299
 - indecomposable, 299
 - special, 299
- root datum, 340
 - reduced, 348
 - semisimple, 347
 - toral, 347
- root group, 325
- root system, 297
 - indecomposable, 297
 - reduced, 298
- roots, 309, 338, 341, 365
 - of a root system, 297
 - simple, 299
- scheme, 55
 - affine over k , 54
 - affine, 54
 - over k , 55
- series
 - composition, 127
 - derived, 189
 - subnormal, 126
- set
 - Γ -, 217, 384
- sheaf
 - for the fpqc topology, 91
- Shimura variety, 412
- Siegel set, 407
- simple, 15
- \mathfrak{sl}_2 -triple, 310
- SL_n , 31
- SO_n
 - split, 337
- space
 - quadratic, 203
- spectrum
 - prime, 53
- splitting, 308
- Sp_n , 32
- stabilizer, 112, 258
- subalgebra
 - Borel, 314
 - Cartan, 308
 - Hopf, 45
 - Lie, 240
- subcategory
 - replete, 115
- subcoalgebra, 42
- subcomodule, 99
- subfunctor
 - closed, 67

- subgroup
 - affine, 74
 - arithmetic, 398, 410
 - Borel, 356
 - characteristic, 75
 - congruence, 398
 - dense, 79
 - parabolic, 357
 - principal congruence, 398
- subgroups
 - commensurable, 397
- subobject, 138
 - generated by, 138
- subrepresentation, 95
- superalgebra, 27, 208
 - commutative, 27
- supergroup
 - affine algebraic, 27
- tannakian category
 - algebraic, 235
- tba, 90, 182, 198
- tba
- tensor product
 - super, 208
- theorem
 - description, 137
 - reconstruction, 131
- \mathbb{T}_n , 16
- topology
 - Zariski, 53
- torus, 16, 171
 - anisotropic, 171
 - maximal, 336
 - quasi-trivial, 392
 - split, 169
- trace form, 278
- transporter, 67
- \mathbb{U}_n , 16
- uniform, 405
- V_a , 30
- variety
 - flag, 352
 - Grassman, 352
- vector
 - anisotropic, 203
 - isotropic, 203
- weight
 - dominant, 304
 - fundamental, 304, 379
 - fundamental dominant, 304
 - highest, 315, 380
- weight spaces, 363
- weights, 304, 363
- Weyl group, 341, 344