# Algebraic Groups and Arithmetic Groups

J.S. Milne

Version 1.01
June 4, 2006

These notes provide an introductory overview of the theory of algebraic groups, Lie algebras, Lie groups, and arithmetic groups. They are a revision of those posted during the teaching of a course at CMS, Zhejiang University, Hangzhou in Spring, 2005.

**v0.00** (February 28 – May 7, 2005). As posted during the course.
**v1.00** May 22, 2005. Minor corrections and revisions; added table of contents and index.
**v1.01** June 4, 2006. Fixed problem with the diagrams.

Please send comments and corrections to me at math@jmilne.org

Available at `http://www.jmilne.org/math/`

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

# Contents

# Introduction

*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 of matrices determined by polynomial conditions. For example, the group of matrices of determinant 1 and the orthogonal group of a symmetric bilinear form are both algebraic groups. The elucidation of the structure of algebraic groups and the classification of them 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 an important source of discrete groups acting on manifolds, and recently they have appeared as the symmetry groups of several string theories in physics.

These are the notes for a 40 hour course that I gave at CMS, Zhejiang University, Hangzhou, in the spring of 2005. My goal was to give an introductory overview of algebraic groups, Lie algebras, Lie groups, and arithmetic groups. However, to adequately cover this topic would take twice as long and twice as many pages (but not more!). Thus, the treatment is very sketchy in places, and some important topics (for example, the crucial real case) are barely mentioned. Nevertheless, I hope that the notes may be useful for someone looking for a rapid introduction to the subject. Sometime I plan to produce an expanded version.

**The approach to algebraic groups taken in these notes** In most of the expository literature, the theory of algebraic groups is based (in spirit if not in fact) on the algebraic geometry of Weil's Foundations.[1] Thus coordinate rings are not allowed to have nonzero nilpotents, which means, for example, that the centre of $\mathrm{SL}_p$ in characteristic $p$ is visible only through its Lie algebra. Moreover, the isomorphism theorem in group theory, $HN/N \simeq H/N \cap H$, fails, and so the intuition provided by group theory is unavailable. It is true that in characteristic zero, all algebraic groups are reduced, but this is a theorem *that can only be stated when nilpotents are allowed.* Another problem is that an algebraic group over a field $k$ is defined to be an algebraic group over some large algebraically closed field together with a $k$-structure. This leads to a confusing terminology in conflict with that of today's algebraic geometry and prevents, for example, the theory of split reductive groups to be developed intrinsically over the base field.

Of course, the theory of algebraic groups should be based on Grothendieck's theory of schemes. However, the language of schemes is not entirely appropriate either, since the nonclosed points are an unnecessary complication when working over a field and they prevent the underlying space of an algebraic group from being a group. In these notes, we usually regard algebraic groups as functors (or bi-algebras), except that, in order to be able to apply algebraic geometry, we sometimes interpret them as algebraic varieties or algebraic spaces (in the sense of AG §11).

[1] Weil, André. Foundations of algebraic geometry. AMS, 1962

The expert need only note that by "algebraic group over a field" we mean "affine algebraic group scheme over a field", and that our ringed spaces have only closed points (thus, we are using $\mathrm{Spm}$ rather than $\mathrm{Spec}$).

## Notations

We use the standard (Bourbaki) notations: $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z}$ = ring of integers, $\mathbb{R}$ = field of real numbers, $\mathbb{C}$ = field of complex numbers, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ = field of $p$ elements, $p$ a prime number. Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. A family of elements of a set $A$ indexed by a second set $I$, denoted $(a_i)_{i\in I}$, is a function $i \mapsto a_i : I \to A$.

Throughout, $k$ is a field and $\overline{k}$ is an algebraic closure of $k$.

Rings will be commutative with 1 unless stated otherwise, and homomorphisms of rings are required to map 1 to 1. A $k$-algebra is a ring $A$ together with a homomorphism $k \to A$. For a ring $A$, $A^\times$ is the group of units in $A$:

$$A^\times = \{a \in A \mid \text{there exists a } b \in A \text{ such that } ab = 1\}.$$

We use Gothic (fraktur) letters for ideals:

| $\mathfrak{a}$ | $\mathfrak{b}$ | $\mathfrak{c}$ | $\mathfrak{m}$ | $\mathfrak{n}$ | $\mathfrak{p}$ | $\mathfrak{q}$ | $\mathfrak{A}$ | $\mathfrak{B}$ | $\mathfrak{C}$ | $\mathfrak{M}$ | $\mathfrak{N}$ | $\mathfrak{P}$ | $\mathfrak{Q}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | $b$ | $c$ | $m$ | $n$ | $p$ | $q$ | $A$ | $B$ | $C$ | $M$ | $N$ | $P$ | $Q$ |

| | |
|---|---|
| $X \stackrel{\text{df}}{=} Y$ | $X$ is defined to be $Y$, or equals $Y$ by definition; |
| $X \subset Y$ | $X$ is a subset of $Y$ (not necessarily proper, i.e., $X$ may equal $Y$); |
| $X \approx Y$ | $X$ and $Y$ are isomorphic; |
| $X \simeq Y$ | $X$ and $Y$ are canonically isomorphic (or there is a given or unique isomorphism). |

## Prerequisites

- ◇ A standard course on algebra, for example, a good knowledge of the Artin 1991.
- ◇ Some knowledge of the language of algebraic geometry, for example, the first few sections of AG.

## Acknowledgements

I thank the Scientific Committee and Faculty of CMS (Yau Shing-Tung, Liu Kefeng, Ji Lizhen, ...) for the invitation to lecture at CMS; Xu Hongwei and Dang Ying for helping to make my stay in Hangzhou an enjoyable one; 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.

## References


BASIC ALGEBRA

**Artin 1991:** Algebra, Prentice-Hall.

**FT:** Milne, J., Fields and Galois theory, available at www.jmilne.org/math/.

**GT:** Milne, J., Group theory, available at www.jmilne.org/math/.

COMMUTATIVE ALGEBRA

**Atiyah and Macdonald 1969:** Commutative algebra, Addison-Wesley.

ALGEBRAIC GEOMETRY

**AG:** Milne, J., Algebraic geometry, available at www.jmilne.org/math/.

GROUP VARIETIES

**Borel 1991:** Linear algebraic groups, Springer.

**Humphreys 1975:** Linear algebraic groups, Springer.

**Springer 1998:** Linear algebraic groups, Birkhäuser.

GROUP SCHEMES

**Demazure and Gabriel, 1970:** Groupes algébriques. Masson, Paris.

**SGA3:** Schémas en Groupes, Seminar organized by Demazure and Grothendieck (1963–64), available at www.grothendieck-circle.org.

**Waterhouse 1979:** Introduction to affine group schemes, Springer.

LIE ALGEBRAS

**Humphreys 1972:** Introduction to Lie algebras and representation theory, Springer.

**Serre 1987:** Complex semisimple Lie algebras, Springer.

LIE GROUPS

**Hall 2003:** Lie groups, Lie algebras and representation theory, Springer.

ARITHMETIC OF ALGEBRAIC GROUPS

**Platonov and Rapinchuk 1994:** Algebraic groups and number theory, Academic.

ARITHMETIC GROUPS

**Borel 1969:** Introduction aux groupes arithmétiques, Hermann.

HISTORY

**Borel 2001:** Essays in the history of Lie groups and algebraic groups, AMS.

# 1 Overview and examples

Loosely speaking, an algebraic group is a group defined by polynomials. Following Mike Artin's dictum (Artin 1991, p xiv), I give the main examples before the precise abstract definition.

The determinant of an $n \times n$ matrix $A = (a_{ij})$ is a polynomial in the entries of $A$, specifically,

$$\det(A) = \sum_{\sigma \in S_n} (\operatorname{sgn}(\sigma)) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

where $S_n$ is the symmetric group on $n$ letters, and $\operatorname{sgn}(\sigma)$ is the sign of $\sigma$. Moreover, the entries of the product of two matrices are polynomials in the entries of the two matrices. Therefore, for any field $k$, the group $\mathrm{SL}_n(k)$ of $n \times n$ matrices with determinant 1 is an algebraic group (called the ***special linear group***).

The group $\mathrm{GL}_n(k)$ of $n \times n$ matrices with nonzero determinant is also an algebraic group (called the ***general linear group***) because its elements can be identified with the $n^2 + 1$-tuples $((a_{ij})_{1 \le i,j \le n}, t)$ such that

$$\det(a_{ij})t = 1.$$

More generally, for a finite-dimensional vector space $V$, we define $\mathrm{GL}(V)$ (resp. $\mathrm{SL}(V)$) to be the groups automorphisms of $V$ (resp. automorphisms with determinant 1). These are again algebraic groups.

On the other hand, the subgroup

$$\{(x, e^x) \mid x \in \mathbb{R}\}$$

of $\mathbb{R} \times \mathbb{R}^\times$ is not an algebraic subgroup because any polynomial $f(X, Y) \in \mathbb{R}[X, Y]$ zero on it is identically zero.

An algebraic group is ***connected*** if it has no quotient algebraic group $Q$ such that $Q(\overline{k})$ is finite and $\neq 1$.

## The building blocks

### Unipotent groups

Recall that an endomorphism $\alpha$ of a vector space $V$ is ***nilpotent*** if $\alpha^n = 0$ for some $n > 0$ and that it is ***unipotent*** if $1 - \alpha$ is nilpotent. For example, a matrix $A$ of the form $\left(\begin{smallmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{smallmatrix}\right)$ is nilpotent ($A^3 = 0$) and so a matrix of the form $1 - A = \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right)$ is unipotent.

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

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

which we denote it $\mathbb{U}_n$. Thus, the elements of a unipotent group are unipotent.

### Algebraic tori

An endomorphism $\alpha$ of a vector space $V$ is ***diagonalizable*** if $V$ has a basis of eigenvectors for $\alpha$, and it is ***semisimple*** if it becomes diagonalizable after an extension of the field $k$. For example, the linear map $x \mapsto Ax: k^n \to k^n$ defined by an $n \times n$ matrix $A$ is diagonalizable if and only if there exists an invertible matrix $P$ with entries in $k$ 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 $k$.

Let $\overline{k}$ be an algebraic closure of $k$. A connected algebraic subgroup $T$ of $\mathrm{GL}(V)$ is an ***algebraic torus*** if, over $\overline{k}$, there exists a basis of $V$ relative to which $T$ is contained in the group of all diagonal matrices

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

which we denote $\mathbb{D}_n$. Thus, the elements of $T$ are semisimple.

### Semisimple groups

Let $G_1, \dots, G_r$ be algebraic subgroups of an algebraic group $G$. If

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

is a surjective homomorphism with finite kernel, then we say that $G$ is the ***almost direct product*** of the $G_i$. In particular, this means that each $G_i$ is normal and that the $G_i$ commute with each other. For example,

$$G = \mathrm{SL}_2 \times \mathrm{SL}_2 / N, \quad N = \{(I, I), (-I, -I)\} \tag{2}$$

is the almost direct product of $\mathrm{SL}_2$ and $\mathrm{SL}_2$, but it can't be written as a direct product.

A connected algebraic group $G$ is ***simple*** if it is non-commutative and has no normal algebraic subgroups, and it is ***almost simple***[2] if its centre $Z$ is finite and $G/Z$ is simple. For example, $\mathrm{SL}_n$ is almost-simple because its centre

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

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

A connected algebraic group is ***semisimple*** if it is an almost direct product of almost-simple subgroups. For example, the group $G$ in (2) is semisimple.

A ***central isogeny*** of connected algebraic groups is a surjective homomorphism $G \to H$ whose kernel is finite and contained in the centre of $G$ (in characteristic zero, a finite subgroup of a *connected* algebraic group is automatically central, and so "central" can be omitted from these definitions). We say that two algebraic groups $H_1$ and $H_2$ are ***centrally isogenous*** if there exist central isogenies

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

[2] Also called "quasi-simple" or, often, just "simple".

Thus, two algebraic groups are centrally isogenous if they differ only by finite central subgroup. This is an equivalence relation.

If $k$ is algebraically closed, then every almost-simple algebraic group is centrally isogenous to exactly one on the following list:

$A_n$ $(n \geq 1)$, the special linear group $\mathrm{SL}_{n+1}$ consisting of all $n+1 \times n+1$ matrices $A$ with $\det(A) = 1$;

$B_n$ $(n \geq 2)$, the special orthogonal group $\mathrm{SO}_{2n+1}$ consisting of all $2n+1 \times 2n+1$ matrices $A$ such that $A^tA = I$ and $\det(A) = 1$;

$C_n$ $(n \geq 3)$, the symplectic group $\mathrm{Sp}_{2n}$ consisting of all invertible $2n \times 2n$ matrices $A$ such that $A^tJA = J$ where $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$;

$D_n$ $(n \geq 4)$, the special orthogonal group $\mathrm{SO}_{2n}$;

$E_6, E_7, E_8, F_4, G_2$ the five exceptional types.

### Abelian varieties

Abelian varieties are algebraic groups that are complete (which implies that they are projective and commutative[3]). An abelian variety of dimension 1 is an elliptic curve, which can be given by a homogeneous equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In these lectures, we shall not be concerned with abelian varieties, and so I'll say nothing more about them.

### Finite groups

Every finite group can be regarded as an algebraic group. For example, let $\sigma$ be a permutation of $\{1, \dots, n\}$ and let $I(\sigma)$ be the matrix obtained from the identity matrix by using $\sigma$ to permute the rows. Then, for any $n \times n$ matrix $A$, $I(\sigma)A$ is obtained from $A$ by permuting the rows according to $\sigma$. In particular, if $\sigma$ and $\sigma'$ are two permutations, then $I(\sigma)I(\sigma') = I(\sigma\sigma')$. Thus, the matrices $I(\sigma)$ realize $S_n$ as a subgroup of $\mathrm{GL}_n$. Since every finite group is a subgroup of some $S_n$, this shows that every finite group can be realized as a subgroup of $\mathrm{GL}_n$, which is automatically algebraic.[4]

## Extensions

For the remainder of this section, **assume that $k$ is perfect.**

### Solvable groups

An algebraic group $G$ is ***solvable*** if it there exists a sequence of connected algebraic subgroups

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

[3] See for example my Storrs lectures (available on my website under preprints/reprints 1986b).

[4] Any finite subset of $k^n$ is algebraic. For example, $\{(a_1, \dots, a_n)\}$ is the zero-set of the polynomials $X_i - a_i$, $1 \leq i \leq n$, and $\{(a_1, \dots, a_n), (b_1, \dots, b_n)\}$ is the zero-set of the polynomials $(X_i - a_i)(X - b_j)$, $1 \leq i, j \leq n$, and so on.

such that $G_{i+1}$ is normal in $G_i$ and $G_i/G_{i+1}$ is commutative. According to the table below, they are extensions of tori by unipotent groups. For example, the group of upper triangular matrices $\mathbb{T}_n$ is solvable:

$$1 \to \mathbb{U}_n \to \mathbb{T}_n \to \mathbb{D}_n \to 1.$$

The Lie-Kolchin theorem says that, when $k = \overline{k}$, for any connected solvable subgroup $G$ of $\mathrm{GL}(V)$, there exists a basis for $V$ such that $G \subset \mathbb{T}_n$.

### Reductive groups

An algebraic group is ***reductive*** if it has no nontrivial connected unipotent subgroups. According to the table, they are extensions of semisimple groups by tori. For example, $\mathrm{GL}_n$ is reductive:

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

### Nonconnected groups

**The orthogonal group.** There is an exact sequence

$$1 \to \mathrm{SO}(n) \to O(n) \xrightarrow{\det} \{\pm 1\} \to 1$$

which shows that $O(n)$ is not connected.

**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. Then $M$ contains both $\mathbb{D}_n$ and the group $S_n$ of permutation matrices. Moreover, for any diagonal matrix $\mathrm{diag}(a_1, \dots, a_n)$,

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

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

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

where $\theta\colon S_n \to \mathrm{Aut}(\mathbb{D}_n)$ sends $\sigma$ to $\mathrm{Inn}(I(\sigma))$.

## Summary

When $k$ is perfect, every smooth 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 (all algebraic groups are smooth):

- ◇ An algebraic group $G$ contains a unique normal connected subgroup $G^\circ$ such that $G/G^\circ$ is finite and smooth (see 8.13).
- ◇ A connected algebraic group $G$ contains a unique normal affine algebraic subgroup $H$ such that $G/H$ is an abelian variety (Barsotti-Chevalley theorem).[5]

[5] B. Conrad, A modern proof of Chevalley's theorem on algebraic groups, available at www.math.lsa.umich.edu/∼bdconrad/papers/chev.pdf.

- ◇ A connected affine group $G$ contains a largest[6] normal solvable subgroup (called the ***radical*** $RG$ of $G$) that contains all other normal solvable subgroups (see p94). The quotient $G/RG$ is semisimple.
- ◇ A connected affine group $G$ contains a largest normal unipotent subgroup (called the ***unipotent radical*** $R_uG$ of $G$) (see p94). The quotient $G/R_uG$ is reductive, and is a torus if $G$ is solvable. (When $k = \overline{k}$, $G$ contains reductive groups $H$, called ***Levi subgroups***, such that $G = R_uG \rtimes H$.)
- ◇ The derived group $\mathcal{D}G$ of a reductive group $G$ is a semisimple algebraic group and the connected centre $Z(G)^\circ$ of $G$ is a torus; $G$ is an extension of a semisimple algebraic group by a torus (see 15.1).

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

| General algebraic group | | | Affine algebraic group | | | Reductive | | |
|---|---|---|---|---|---|---|---|---|
| general | • | | affine | $G$ | | | | |
| | \| | finite | | \| | finite | | |
| connected | • | | connected | $G^\circ$ | | reductive | • | |
| | \| | abelian variety | | \| | semisimple | \| | semisimple |
| connected affine | • | | solvable | $RG$ | | torus | • | |
| | \| | semisimple | | \| | torus | \| | torus |
| solvable | • | | unipotent | $R_uG$ | | $\{1\}$ | • | |
| | \| | torus | | \| | unipotent | | |
| unipotent | • | | | $\{1\}$ | | | | |
| | \| | unipotent | | | | | | |
| $\{1\}$ | • | | | | | | | |

ASIDE 1.1 We have seen that the theory of algebraic groups includes the theory of finite groups and the theory of abelian varieties. In listing the finite simple groups, one uses the listing of the almost-simple algebraic groups given above. The theory of abelian varieties doesn't use the theory of algebraic groups until one begins to look at families of abelian varieties when one needs both the theory of algebraic groups and the theory of arithmetic groups.

## Exercises

1-1 Show that a polynomial $f(X, Y) \in \mathbb{R}[X, Y]$ such that $f(x, e^x) = 0$ for all $x \in \mathbb{R}$ is zero (as an element of $\mathbb{R}[X, Y]$). Hence $\{(x, e^x) \mid x \in \mathbb{R}\}$ is not an algebraic subset of $\mathbb{R}^2$ (i.e., it is not the zero set of a collection of polynomials).

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

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

[6] This means that $RG$ is a normal solvable subgroup of $G$ and that it contains all other normal solvable subgroups of $G$.

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

# 2 Definition of an affine algebraic group

In this section, I assume known some of the language of categories and functors (see, for example, AG §1).

### Principle of permanence of identities

Let $f(X_1,\dots,X_m)$ and $g(X_1,\dots,X_m)$ be two polynomials with coefficients in $\mathbb{Z}$ such that

$$f(a_1,\dots,a_m) = g(a_1,\dots,a_m) \tag{4}$$

for all real numbers $a_i$. Then $f(X_1,\dots,X_m) = g(X_1,\dots,X_m)$ as polynomials with coefficients in $\mathbb{R}$ — see Artin 1991, Chapter 12, 3.8, or (4.1) below — and hence as polynomials with coefficients in $\mathbb{Z}$. Therefore, (4) is true with the $a_i$ in any ring $R$.
*Application.* When we define the ***determinant*** of an $n\times n$ matrix $M=(m_{ij})$ by

$$\det(M) = \sum_{\sigma\in S_n} (\operatorname{sgn}(\sigma)) m_{1\sigma(1)}\cdots m_{n\sigma(n)},$$

then

$$\det(MN) = \det(M)\cdot\det(N) \tag{5}$$

and

$$\operatorname{adj}(M)\cdot M = \det(M) I = M\cdot\operatorname{adj}(M) \qquad \text{(Cramer's rule).} \tag{6}$$

Here $I$ is the identity matrix, and $\operatorname{adj}(M)$ is the $n\times n$ matrix whose $(i,j)^{\text{th}}$ entry is $(-1)^{i+j}\det M_{ji}$ with $M_{ij}$ the matrix obtained from $M$ by deleting the $i^{\text{th}}$ row and the $j^{\text{th}}$ column.

For matrices with entries in the field of real numbers, this is proved, for example, in Artin 1991, Chapter I, §5, but we shall need the result for matrices with entries in any commutative ring $R$. There are two ways of proving this: observe that Artin's proof applies in general, or by using the above principle of permanence of identities. Briefly, when we consider a matrix $M$ whose entries are symbols $X_{ij}$, (5) becomes an equality of polynomials in $\mathbb{Z}[X_{11},\dots,X_{nn}]$. Because it becomes true when we replace the $X_{ij}$ with real numbers, it is true when we replace the $X_{ij}$ with elements of any ring $R$. A similar argument applies to (6) (regard it as a system of $n^2$ equalities).

### Affine algebraic groups

In §1, I said that an algebraic group over $k$ is a group defined by polynomial equations with coefficients in $k$. Given such an object, we should be able to look at the solutions of the equations in any $k$-algebra, and so obtain a group for every $k$-algebra. We make this into a definition.

Thus, let $G$ be a functor from $k$-algebras to groups. Recall that this means that for each $k$-algebra $R$ we have a group $G(R)$ and for each homomorphism of $k$-algebras $\alpha\colon R\to S$ we have a homomorphism $G(\alpha)\colon G(R)\to G(S)$; moreover,

$$\begin{aligned} G(\mathrm{id}_R) &= \mathrm{id}_{G(R)} \text{ all } R\\ G(\beta\circ\alpha) &= G(\beta)\circ G(\alpha) \text{ all composable } \alpha,\beta. \end{aligned}$$

We say that $G$ is an ***affine algebraic group***[7] if there exists a finitely generated $k$-algebra $A$ such that

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

functorially in $R$. Since we shall be considering only affine algebraic groups in these lectures (no abelian varieties), I'll omit the "affine".

In the following examples, we make repeated use of the following observation. Let $A = k[X_1, \dots, X_m]$; then a $k$-algebra homomorphism $A \to R$ is determined by the images $a_i$ of the $X_i$, and these are arbitrary. Thus, to give such a homomorphism amounts to giving an $m$-tuple $(a_i)_{1\le i\le m}$ in $R$. Let $A = k[X_1, \dots, X_m]/\mathfrak{a}$ where $\mathfrak{a}$ is the ideal generated by some polynomials $f_j(X_1, \dots, X_m)$. The homomorphism $X_i \mapsto a_i : k[X_1, \dots, X_m] \to R$ factors through $A$ if and only if the $a_i$ satisfy the equations $f_j(a_1, \dots, a_m) = 0$. Therefore, to give a $k$-algebra homomorphism $A \to R$ amounts to giving an $m$-tuple $a_1, \dots, a_m$ such that $f_j(a_1, \dots, a_m) = 0$ for all $j$.

EXAMPLE 2.1 Let $\mathbb{G}_a$ be the functor sending a $k$-algebra $R$ to $R$ considered as an additive group, i.e., $\mathbb{G}_a(R) = (R, +)$. Then

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

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

EXAMPLE 2.2 Let $\mathbb{G}_m(R) = (R^\times, \times)$. Let $k(X)$ be the field of fractions of $k[X]$, and let $k[X, X^{-1}]$ be the subring of $k(X)$ of polynomials in $X$ and $X^{-1}$. Then

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

and so $\mathbb{G}_m$ is an algebraic group, called the ***multiplicative group***.

EXAMPLE 2.3 From (5) and the fact that $\det(I) = 1$, we see that if $M$ is an invertible matrix in $M_n(R)$, then $\det(M) \in R^\times$. Conversely, Cramer's rule (6) shows that if $\det(M) \in R^\times$, then $M$ in invertible (and it gives an explicit polynomial formula for the inverse). Therefore, the $n \times n$ matrices of determinant 1 with entries in a $k$-algebra $R$ form a group $\mathrm{SL}_n(R)$, and $R \mapsto \mathrm{SL}_n(R)$ is a functor. Moreover,

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

and so $\mathrm{SL}_n$ is an algebraic group, called the ***special linear group***. Here $\det(X_{ij})$ is the polynomial $\sum \mathrm{sgn}(\sigma) X_{1\sigma(1)} X_{2\sigma(2)} \cdots$.

EXAMPLE 2.4 The arguments in the last example show that the $n \times n$ matrices with entries in a $k$-algebra $R$ and determinant a unit in $R$ form a group $\mathrm{GL}_n(R)$, and $R \mapsto \mathrm{GL}_n(R)$ is a functor. Moreover,[8]

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

and so $\mathrm{GL}_n$ is an algebraic group, called the ***general linear group***.

[7] When $k$ has characteristic zero, this definition agrees with that in Borel 1991, Humphreys 1975, and Springer 1998; when $k$ has nonzero characteristic, it differs (but is better) — see below.

[8] To give an element on the right is to given an $n \times n$ matrix $M$ with entries in $R$ and an element $c \in R$ such that $\det(M)c = 1$. Thus, $c$ is determined by $M$ (it must be $\det(M)^{-1}$), and $M$ can be any matrix such that $\det(M) \in R^\times$.

EXAMPLE 2.5 For a $k$-algebra $R$, let $G(R)$ be 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

$$A_\sigma = k[\mathrm{GL}_n]/(X_{ij} \mid j \neq \sigma(i))$$

and let $k[G] = \prod_{\sigma \in S_n} A_\sigma$. The $k[G]$ represents $G$, and so $G$ is an algebraic group, called the ***group of monomial matrices***.

EXAMPLE 2.6 Let $C$ be a symmetric matrix with entries in $R$. An ***automorph***[9] of $C$ is an invertible matrix $T$ such that $T^t \cdot C \cdot T = C$, in other words, such that

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

Let $G$ be the functor sending $R$ to the group of automorphs of $C$ with entries in $R$. Then $G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$ with $A$ the quotient of $k[X_{11}, \dots, X_{nn}, Y]$ by the ideal generated by the polynomials

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

EXAMPLE 2.7 Let $G$ be the functor such that $G(R) = \{1\}$ for all $k$-algebras $R$. Then $G(R) \simeq \mathrm{Hom}_{k\text{-algebra}}(k, R)$, and so $G$ is an algebraic group, called the ***trivial algebraic group***.

EXAMPLE 2.8 Let $\mu_n$ be the functor $\mu_n(R) = \{r \in R \mid r^n = 1\}$. Then

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

and so $\mu_n$ is an algebraic group with $k[\mu_n] = k[X]/(X^n - 1)$.

EXAMPLE 2.9 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 a group, and $R \mapsto \alpha_p(R)$ is a functor. Moreover, $\alpha_p(R) = \mathrm{Hom}_{k\text{-alg}}(k[T]/(T^p), R)$, and so $\alpha_p$ is an algebraic group.

EXAMPLE 2.10 There are abstract versions of the above groups. Let $V$ be a finite-dimensional vector space over $k$, and let $\phi$ be a symmetric bilinear $V \times V \to k$. Then there are algebraic groups with

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

[9] If we let $\phi(x, y) = x^t C y$, $x, y \in k^n$, then the automorphs of $C$ are the linear isomorphisms $T: k^n \to k^n$ such that $\phi(Tx, Ty) = \phi(x, y)$.

### Homomorphisms of algebraic groups

A homomorphism of algebraic groups over $k$ is a natural homomorphism[10] $G \to H$, i.e., a family of homomorphisms $\alpha(R)\colon G(R) \to H(R)$ such that, for every homomorphism of $k$-algebras $R \to S$, the diagram

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

commutes. For example, the determinant defines a homomorphism

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

and the homomorphisms

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

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

### The Yoneda lemma

Any $k$-algebra $A$ defines a functor $h_A$ from $k$-algebras to sets, namely,

$$R \mapsto h_A(R) \stackrel{\text{df}}{=} \mathrm{Hom}_{k\text{-alg}}(A, R).$$

A homomorphism $\alpha\colon A \to B$ defines a morphism of functors $h_B \to h_A$, namely,

$$\beta \mapsto \beta \circ \alpha\colon h_B(R) \to h_A(R).$$

Conversely, a morphism of functors $h_B \to h_A$ defines a homomorphism $\alpha\colon A \to B$, namely, the image of $\mathrm{id}_B$ under $h_B(B) \to h_A(B)$.

It is easy to check that these two maps are inverse (exercise!), and so

$$\mathrm{Hom}_{k\text{-alg}}(A, B) \simeq \mathrm{Hom}(h_B, h_A). \tag{7}$$

This remarkably simple, but useful result, is known as the ***Yoneda lemma***.

A functor $F$ from $k$-algebras to sets is ***representable*** if it is isomorphic to $h_A$ for some $k$-algebra $A$ (we then say that $A$ ***represents*** $F$). With this definition, an algebraic group is a functor from $k$-algebras to groups that is representable (as a functor to sets) by a finitely generated $k$-algebra.

Let $\mathbb{A}^1$ be the functor sending a $k$-algebra $R$ to $R$ (as a set); then $k[X]$ represents $\mathbb{A}^1$:

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

Note that

$$\mathrm{Hom}_{\text{functors}}(h_A, \mathbb{A}^1) \stackrel{\text{Yoneda}}{\simeq} \mathrm{Hom}_{k\text{-alg}}(k[X], A) \simeq A. \tag{8}$$

[10] Also called a natural transformation or a morphism of functors.

## The coordinate ring of an algebraic group

A ***coordinate ring*** of an algebraic group $G$ is a finitely generated $k$-algebra $A$ together with an isomorphism of functors $h_A \to G$. If $h_{A_1} \to G$ and $h_{A_2} \to G$ are coordinate rings, then we get an isomorphism

$$h_{A_2} \to G \to h_{A_1}$$

by inverting the first isomorphism. Hence, by the Yoneda lemma, we get an isomorphism

$$A_1 \to A_2,$$

and so the coordinate ring of an algebraic group is uniquely determined up to a unique isomorphism. We sometimes write it $k[G]$.

Let $(A, h_A \xrightarrow{\simeq} G)$ be a coordinate ring for $G$. Then

$$A \overset{(8)}{\simeq} \operatorname{Hom}(h_A, \mathbb{A}^1) \simeq \operatorname{Hom}(G, \mathbb{A}^1).$$

Thus, an $f \in A$ defines a natural map[11] $G(R) \to R$, and each such natural map arises from a unique $f$.

For example,[12]

$$k[\mathrm{GL}_n] = \frac{k[\ldots, X_{ij}, \ldots]}{(Y \det(X_{ij}) - 1)} = k[\ldots, x_{ij}, \ldots, y],$$

and $x_{ij}$ sends a matrix in $\mathrm{GL}_n(R)$ to its $(i, j)^{\text{th}}$-entry and $y$ to the inverse of its determinant.

## Very brief review of tensor products.

Let $A$ and $B$ be $k$-algebras. A $k$-algebra $C$ together with homomorphisms $i: A \to C$ and $j: B \to C$ is called the ***tensor product*** of $A$ and $B$ if it has the following universal property: for every pair of homomorphisms (of $k$-algebras) $\alpha: A \to R$ and $\beta: B \to R$, there is a unique homomorphism $\gamma: C \to R$ such that $\gamma \circ i = \alpha$ and $\gamma \circ j = \beta$:

$$\begin{array}{ccccc} A & \xrightarrow{i} & C & \xleftarrow{j} & B \\ & \searrow^{\alpha} & \vdots\ \exists!\ \gamma & \swarrow_{\beta} & \\ & & R & & \end{array} \tag{9}$$

If it exists, the tensor product, is uniquely determined up to a unique isomorphism by this property. We write it $A \otimes_k B$.is an isomorphism. For its construction, see AG §1.

EXAMPLE 2.11 For a set $X$ and a $k$-algebra $R$, let $A$ be the set of maps $X \to R$. Then $A$ becomes a $k$-algebra with the structure

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

Let $Y$ be a second set and let $B$ be the $k$-algebra of maps $Y \to R$. Then the elements of $A \otimes_k B$ define maps $X \times Y \to R$ by

$$(f \otimes g)(x, y) = f(x)g(y).$$

[11] That is, a natural transformation of functors from $k$-algebras to sets.

[12] Here, and elsewhere, I use $x_{ij}$ to denote the image of $X_{ij}$ in the quotient ring.

The maps $X \times Y \to R$ arising from elements of $A \otimes_k B$ are exactly those that can be expressed as

$$(x, y) \mapsto \sum f_i(x)g_i(y)$$

for some maps $f_i: X \to R$ and $g_i: Y \to R$.

EXAMPLE 2.12 Let $A$ be a $k$-algebra and let $k'$ be a field containing $k$. The homomorphism $i: k' \to k' \otimes_k A$ makes $k' \otimes_k A$ into a $k'$-algebra. If $R$ is a second $k'$-algebra, a $k'$-algebra homomorphism $\gamma: k' \otimes_k A \to R$ is simply a $k$-algebra homomorphism such that $k' \xrightarrow{i} k' \otimes_k A \xrightarrow{\gamma} R$ is the given homomorphism. Therefore, in this case, (9) becomes

$$\mathrm{Hom}_{k'\text{-alg}}(k' \otimes_k A, R) \simeq \mathrm{Hom}_{k\text{-alg}}(A, R). \tag{10}$$

## Products of algebraic groups

Let $G$ and $H$ be algebraic groups, and let $G \times H$ be the functor

$$(G \times H)(R) = G(R) \times H(R).$$

Then,

$$(G \times H)(R) \overset{(9)}{\simeq} \mathrm{Hom}_{k\text{-alg}}(k[G] \otimes_k k[H], R),$$

and so $G \times H$ is an algebraic group with coordinate ring

$$k[G \times H] = k[G] \otimes_k k[H]. \tag{11}$$

## Fibred products of algebraic groups

Let $G_1 \to H \leftarrow G_2$ be homomorphisms of algebraic groups, and let $G_1 \times_H G_2$ be the functor sending a $k$-algebra $R$ to the set $(G_1 \times_H G_2)(R)$ of pairs $(g_1, g_2) \in G_1(R) \times G_2(R)$ having the same image in $H(R)$. Then $G_1 \times_H G_2$ is an algebraic group with coordinate ring

$$k[G_1 \times_H G_2] = k[G_1] \otimes_{k[H]} k[G_2]. \tag{12}$$

This follows from a standard property of tensor products, namely, that $A_1 \otimes_B A_2$ is the largest quotient of $A_1 \otimes_k A_2$ such that

$$\begin{array}{ccc} B & \longrightarrow & A_2 \\ \downarrow & & \downarrow \\ A_1 & \longrightarrow & A_1 \otimes_B A_2 \end{array}$$

commutes.

## Extension of the base field (extension of scalars)

Let $G$ be an algebraic group over $k$, and let $k'$ be a field containing $k$. Then each $k'$-algebra $R$ can be regarded as a $k$-algebra through $k \to k' \to R$, and so $G(R)$ is defined; moreover

$$G(R) \simeq \mathrm{Hom}_{k\text{-alg}}(k[G], R) \overset{(10)}{\simeq} \mathrm{Hom}_{k'\text{-alg}}(k' \otimes_k k[G], R).$$

Therefore, by restricting the functor $G$ to $k'$-algebras, we get an algebraic group $G_{k'}$ over $k'$ with coordinate ring $k[G_{k'}] = k' \otimes_k k[G]$.

## Algebraic groups and bi-algebras

Let $G$ be an algebraic group over $k$ with $A = k[G]$. The functor $G \times G$ is represented by $A \otimes_k A$, and the functor $R \mapsto \{1\}$ is represented by $k$. Therefore, by the Yoneda lemma, the maps of functors

$$\text{(m)ultiplication: } G \times G \to G, \quad \text{(i)dentity: } \{1\} \to G, \quad \text{(inv)erse: } G \to G$$

define homomorphisms of $k$-algebras

$$\Delta\colon A \to A \otimes_k A, \quad \epsilon\colon A \to k, \quad S\colon A \to A.$$

Let[13] $f \in A$. Then $\Delta(f)$ is the (unique) element of $A \otimes_k A$ such that, for any $k$-algebra $R$ and elements $x, y \in G(R)$,

$$(\Delta f)(x, y) = f(xy). \tag{13}$$

Similarly,

$$(\epsilon f)(1) = f(1) \tag{14}$$

and

$$(Sf)(x) = f(x^{-1}), \quad x \in G(R). \tag{15}$$

For example,

| | points | ring | $\Delta$ | $\epsilon$ | $S$ |
|---|---|---|---|---|---|
| $\mathbb{G}_a$ | $(R, +)$ | $k[X]$ | $\Delta(X) = X \otimes 1 + 1 \otimes X$ | $\epsilon(X) = 0$ | $X \mapsto -X$ |
| $\mathbb{G}_m$ | $(R^\times, \times)$ | $k[X, X^{-1}]$ | $\Delta(X) = X \otimes X$ | $\epsilon(X) \mapsto 1$ | $X \mapsto X^{-1}$ |
| $\mathrm{GL}_n$ | $\mathrm{GL}_n(R)$ | $\frac{k[X_{11},\dots,X_{nn},Y]}{(Y \det(X_{ij})-1)}$ | $\begin{cases} \Delta(x_{ik}) = \sum_{j=1,\dots,n} x_{ij} \otimes x_{jk} \\ \Delta(y) = y \otimes y \end{cases}$ | $\begin{cases} x_{ii} \mapsto 1 \\ x_{ij} \mapsto 0, i \neq j \\ y \mapsto 1 \end{cases}$ | Cramer's rule. |

In more detail: $k[X] \otimes_k k[X]$ is a polynomial ring in the symbols $X \otimes 1$ and $1 \otimes X$, and we mean (for $\mathbb{G}_a$) that $\Delta$ is the unique homomorphism of $k$-algebras $k[X] \to k[X \otimes 1, 1 \otimes X]$ sending $X$ to $X \otimes 1 + 1 \otimes X$; thus, a polynomial $f(X)$ in $X$ maps to $f(X \otimes 1 + 1 \otimes X)$.

For $G = \mathrm{GL}_n$, $S$ maps $x_{kl}$ to the $(k, l)^{\text{th}}$-entry of $y(-1)^{k+l} \det M_{lk}$ where $M_{kl}$ is the matrix obtained from the matrix $(x_{ij})$ by omitting the $k^{\text{th}}$-row and $l^{\text{th}}$-column (see Cramer's rule).

We should check that these maps of $k$-algebras have the properties (13,14,15), at least for $\mathrm{GL}_n$. For equation (13),

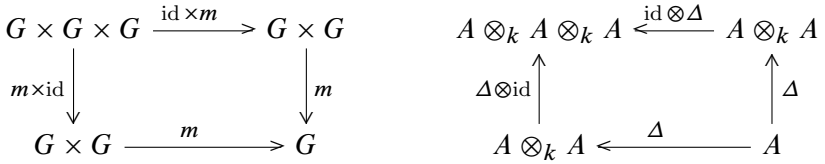
$$\begin{aligned} (\Delta x_{ik})((a_{ij}), (b_{ij})) &= (\sum_{j=1,\dots,n} x_{ij} \otimes x_{jk})((a_{ij}), (b_{ij})) && \text{(definition of } \Delta) \\ &= \sum_j a_{ij} b_{jk} && \text{(recall that } x_{kl}((a_{ij})) = a_{kl}) \\ &= x_{ik}((a_{ij})(b_{ij})). \end{aligned}$$

Also, we defined $\epsilon$ so that $\epsilon(x_{ij})$ is the $(i, j)^{\text{th}}$-entry of $I$, and we defined $S$ so that $(Sx_{ij})(M) = (i, j)^{\text{th}}$ entry of $M^{-1}$.

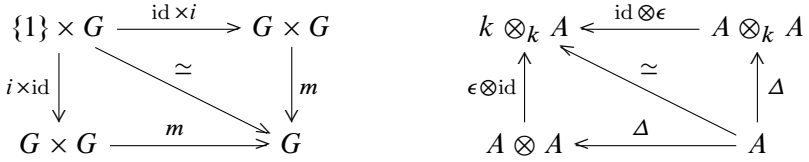
[13] The picture to think of:

$$\begin{array}{ccccc} G(R) \times G(R) & \xrightarrow{\text{m}} & G(R) & \quad \{1\} \xrightarrow{i} G(R) & \quad G(R) \xrightarrow{\text{inv}} G(R) \\ A \otimes A & \xleftarrow{\Delta} & A & \quad k \xleftarrow{\epsilon} A & \quad A \xleftarrow{S} A \end{array}$$

The diagrams below on the left commute by definition, and those on the right commute because the maps all come from those on the left via the Yoneda lemma:




associativity coassociativity




identity coidentity


inverse coinverse

We define a ***bi-algebra*** (or ***bialgebra***) over $k$ to be a finitely generated $k$-algebra $A$ together with maps $\Delta$, $\epsilon$, and $S$ such that the three diagrams commute, i.e., such that

$$(\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta \quad \text{(co-associativity)} \tag{16}$$

$$\text{if } \Delta(a) = \sum a_i \otimes b_i, \text{ then } \begin{cases} a = \sum \epsilon(a_i) b_i & \text{(co-identity)} \\ \epsilon(a) = \sum S(a_i) b_i & \text{(co-inverse)} \end{cases} \tag{17}$$

(Terminology varies — sometimes this is called a Hopf algebra, or a Hopf algebra with identity, or bi-algebra with antipode, or ....)

PROPOSITION 2.13 *The functor $G \mapsto k[G]$ is a contravariant equivalence from the category of algebraic groups over $k$ to the category of bi-algebras over $k$.*

PROOF. We have seen that an algebraic group defines a bi-algebra, and conversely the structure of a bi-algebra on $A$ makes $h_A$ a functor to groups (rather than sets). For example,

$$\begin{aligned} G(R) \times G(R) &= \mathrm{Hom}_{k\text{-alg}}(A, R) \times \mathrm{Hom}_{k\text{-alg}}(A, R) \\ &\simeq \mathrm{Hom}_{k\text{-alg}}(A \otimes_k A, R) \qquad \text{(see (9))} \end{aligned}$$

and $\Delta$ defines a map from $\mathrm{Hom}_{k\text{-alg}}(A \otimes_k A, R)$ to $\mathrm{Hom}_{k\text{-alg}}(A, R)$. Thus, $\Delta$ defines a law of composition on $G$ which the existence of $\epsilon$ and $S$ and the axioms show to be a group law. The rest of the verification is completely straightforward. □

EXAMPLE 2.14 Let $F$ be a finite group, and let $A$ be the set of maps $F \to k$ with its natural $k$-algebra structure. Then $A$ is a product of copies of $k$ indexed by the elements of

$F$. More precisely, let $e_\sigma$ be the function that is 1 on $\sigma$ and 0 on the remaining elements of $F$. Then the $e_\sigma$'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

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

define a bi-algebra structure on $A$. Let $\underline{F}$ be the associated algebraic group, so that

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

If $R$ has no idempotents other than 0 or 1, then a $k$-algebra homomorphism $A \to R$ must send one $e_\sigma$ to 1 and the remainder to 0. Therefore, $\underline{F}(R) \simeq \Gamma$, and one checks that the group structure provided by the maps $\Delta, \epsilon, S$ is the given one. For this reason, $\underline{F}$ is called the ***constant algebraic group defined*** by $\underline{F}$ and often denoted by $\underline{F}$ (even though for $k$-algebras $R$ with more idempotents than 0 and 1, $\underline{F}(R)$ will be bigger than $F$).

## Homogeneity

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

PROPOSITION 2.15 *For each $a \in G(k)$, the natural map*

$$T_a\colon G(R) \to G(R), \quad g \mapsto a_R g,$$

*is an isomorphism of set-valued functors. Moreover,*

$$T_e = \mathrm{id}_G$$
$$T_a \circ T_b = T_{ab}, \quad \text{all } a, b \in G(k).$$

PROOF. It is obvious that $T_a$ is a natural map (i.e., a morphism of set-valued functors) and that $T_e = \mathrm{id}_G$ and $T_a \circ T_b = T_{ab}$. From this it follows that $T_a \circ T_{a^{-1}} = \mathrm{id}_G$, and so $T_a$ is an isomorphism. □

For $a \in G(k)$, we let $\mathfrak{m}_a$ denote the kernel of $a\colon k[G] \to k$. Then $k[G]/\mathfrak{m}_a \simeq k$, and so $\mathfrak{m}_a$ is a maximal ideal in $k[G]$. Let $k[G]_{\mathfrak{m}_a}$ denote the ring of fractions obtained by inverting the elements of

$$S = \{f \in k[G] \mid f \notin \mathfrak{m}_a\} = \{f \in k[G] \mid f(a) \neq 0\}.$$

Then $k[G]_{\mathfrak{m}_a}$ is a local ring with maximal ideal $\mathfrak{m}_a k[G]_{\mathfrak{m}_a}$ (AG 1.28).

PROPOSITION 2.16 *For each $a \in G(k)$, $k[G]_{\mathfrak{m}_a} \simeq k[G]_{\mathfrak{m}_e}$.*

PROOF. The homomorphism $t\colon k[G] \to k[G]$ corresponding (by the Yoneda lemma) to $T_a$ is defined by $t(f)(g) = f(ag)$, all $g \in G(R)$. Therefore, $t^{-1}\mathfrak{m}_e = \mathfrak{m}_a$, and so $t$ extends to an isomorphism $k[G]_{\mathfrak{m}_a} \to k[G]_{\mathfrak{m}_e}$. □

REMARK 2.17 The map $T_a$ corresponds to the map

$$k[G] \xrightarrow{\Delta} k[G] \otimes_k k[G] \xrightarrow{a\otimes \mathrm{id}_{k[G]}} k \otimes_k k[G] \simeq k[G]$$

of $k$-algebras.

**Warning:** For an algebraic group $G$ over a nonalgebraically closed field $k$, it is **not true** that the local rings of $k[G]$ are all isomorphic. For example, if $G = \mu_3$ over $\mathbb{Q}$, then $k[G] = \mathbb{Q} \times \mathbb{Q}[\sqrt{-3}]$.

## Reduced algebras and their tensor products

Recall that a ring is ***reduced*** if it has no nonzero nilpotents, i.e., no elements $a \neq 0$ such that $a^n = 0$ for $n > 1$. For example, $A = k[X]/(X^n)$ is not reduced if $n \geq 2$.

PROPOSITION 2.18 *A finitely generated $k$-algebra $A$ is reduced if and only if*

$$\bigcap\{\mathfrak{m} \mid \mathfrak{m} \text{ maximal ideal in } A\} = 0.$$

PROOF. $\Longleftarrow$ : When $\mathfrak{m}$ is maximal, $A/\mathfrak{m}$ is reduced, and so every nilpotent element of $A$ lies in $\mathfrak{m}$. Therefore, every nilpotent element of $A$ lies in $\bigcap \mathfrak{m} = 0$.

$\Longrightarrow$ : Let $a$ be a nonnilpotent element of $A$. The map $A \to \overline{k} \otimes_k A$ is injective, and so $a$ is not nilpotent in $\overline{k} \otimes_k A$. It follows from the strong Nullstellensatz (AG 2.11), that there exists a $k$-algebra homomorphism $f: \overline{k} \otimes_k A \to \overline{k}$ such that $f(a) \neq 0$.[14] Then $f(A)$ is a field, and so its kernel is a maximal ideal not containing $a$. □

For a nonperfect field $k$ of characteristic $p \neq 0$, there exists an element $a$ of $k$ that is not a $p$th power. Then $X^p - a$ is irreducible in $k[X]$, but $X^p - a = (X - \alpha)^p$ in $\overline{k}[X]$. Therefore, $A = k[X]/(X^p - a)$ is a field, but $\overline{k} \otimes A = \overline{k}[X]/(X - \alpha)^p$ is not reduced. We now show that such things do not happen when $k$ is perfect.

PROPOSITION 2.19 *Let $A$ be a finitely generated $k$-algebra over a perfect field $k$. If $A$ is reduced, then so also is $K \otimes_k A$ for all fields $K \supset k$.*

PROOF. Let $(e_i)$ be a basis for $K$ as a $k$-vector space, and suppose $\alpha = \sum e_i \otimes a_i$ is a nonzero nilpotent in $K \otimes_k A$. Because $A$ is reduced, the intersection of the maximal ideals in it is zero. Let $\mathfrak{m}$ be a maximal ideal in $A$ that does not contain all of the $a_i$. The image $\overline{\alpha}$ of $\alpha$ in $K \otimes_k (A/\mathfrak{m})$ is a nonzero nilpotent, but $A/\mathfrak{m}$ is a finite separable field extension of $k$, and so this is impossible.[15] □

PROPOSITION 2.20 *Let $A$ and $B$ be finitely generated $k$ algebras. If $A$ and $B$ are reduced, then so also is $A \otimes_k B$.*

PROOF. Let $(e_i)$ be a basis for $B$ as a $k$-vector space, and suppose $\alpha = \sum a_i \otimes e_i$ is a nonzero nilpotent element of $A \otimes_k B$. Choose a maximal ideal $\mathfrak{m}$ in $A$ not containing all of the $a_i$. Then the image $\overline{\alpha}$ of $\alpha$ in $(A/\mathfrak{m}) \otimes_k B$ is a nonzero nilpotent. But $A/\mathfrak{m}$ is a field, and so this is impossible by (2.19). □

[14] Write $\overline{k} \otimes_k A = \overline{k}[X_1, \dots, X_n]/\mathfrak{a}$, and take $f$ to be evaluation at a point not in the zero-set of $(a)$ in $V(\mathfrak{a})$.

[15] Every separable field extension of $k$ is of the form $k[X]/(f(X))$ with $f(X)$ separable and therefore without repeated factors in any extension field of $k$ (see FT, especially 5.1).

## Reduced algebraic groups and smooth algebraic groups

DEFINITION 2.21 An algebraic group $G$ over $k$ is ***reduced*** if $k[G]$ is reduced, and it is ***smooth*** if $G_{\overline{k}}$ is reduced. (Thus, the notions coincide when $k = \overline{k}$.)

PROPOSITION 2.22 *If $G$ is smooth, then it is reduced; the converse is true when $k$ is perfect.*

PROOF. Since $k[G] \to \overline{k} \otimes_k k[G] \simeq \overline{k}[G_{\overline{k}}]$ is injective, the first part of the statement is obvious, and the second part follows (2.19). □

REMARK 2.23 Let $k$ be perfect. Let $G$ be an algebraic group over $k$ with coordinate ring $A$, and let $\overline{A}$ be the quotient of $A$ by its nilradical $\mathfrak{N}$ (ideal of nilpotent elements). Because $\overline{A} \otimes_k \overline{A}$ is reduced (2.20), the map $\Delta\colon A \to \overline{A} \otimes_k \overline{A}$ factors through $\overline{A}$. Similarly, $S$ and $\epsilon$ are defined on $\overline{A}$, and it follows easily that there exists a unique structure of a $k$-bi-algebra on $\overline{A}$ such that $A \to \overline{A}$ is a homomorphism. Let $\overline{G} \to G$ be the corresponding homomorphism of algebraic groups over $k$. Then $\overline{G}$ is smooth, and any homomorphism $H \to G$ with $H$ smooth factors through $\overline{G} \to G$. We denote $\overline{G}$ by $G_{\text{red}}$, and called it the ***reduced algebraic group attached to*** $G$.

## Smooth algebraic groups and group varieties

In this subsection, $k$ is algebraically closed.

In this subsection and the next, I assume the reader is familiar with §§1,2,3,5 of my notes AG. In particular, I make use of the isomorphisms

$$A/\mathfrak{m}^n \simeq A_{\mathfrak{m}}/\mathfrak{n}^n, \quad \mathfrak{m}^r/\mathfrak{m}^n \simeq \mathfrak{n}^r/\mathfrak{n}^n \tag{18}$$

which hold when $\mathfrak{m}$ is a maximal ideal of a noetherian ring $A$ and $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$ (AG 1.31). To avoid confusion, I shall refer to an algebraic variety $G$ over $k$ equipped with regular maps

$$m\colon G \times G \to G, \quad \text{inv}\colon G \to G, \quad i\colon \mathbb{A}^0 \to G$$

making $G$ into a group in the usual sense as a ***group variety*** (see AG 4.23). For any reduced $k$-bi-algebra $A$, the maps $\Delta, S, \epsilon$ define on $\operatorname{Spm} A$ the structure of a group variety.

PROPOSITION 2.24 *The functor $G \mapsto \operatorname{Spm} k[G]$ defines an equivalence from the category of smooth algebraic groups to the category of affine group varieties ($k$ algebraically closed).*

PROOF. The functors sending a smooth algebraic group or an affine group variety to its coordinate ring are both contravariant equivalences to the category of reduced $k$-bi-algebras.□

Recall that the ***(Krull) dimension*** of a local noetherian ring $A$ is the greatest length of a chain of prime ideals

$$\mathfrak{m} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0$$

with strict inclusions. For a local noetherian ring $A$ with maximal ideal $\mathfrak{m}$, the ***associated graded ring*** is $gr(A) = \bigoplus_{n \geq 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ with the multiplication defined as follows: for $a \in \mathfrak{m}^n$ and $a' \in \mathfrak{m}^{n'}$,

$$(a + \mathfrak{m}^{n+1}) \cdot (a' + \mathfrak{m}^{n'+1}) = aa' + \mathfrak{m}^{n+n'+1}.$$

PROPOSITION 2.25 *For a noetherian local ring $A$ of dimension $d$ and residue field $k_0 = A/\mathfrak{m}$, the following conditions are equivalent:*

(a) *$gr(A)$ is a polynomial ring over $k_0$ in $d$ symbols;*
(b) *$\dim_{k_0}(\mathfrak{m}/\mathfrak{m}^2) = d$;*
(c) *$\mathfrak{m}$ can be generated by $d$ elements.*

*Moreover, any ring satisfying these conditions is an integral domain.*

PROOF. Atiyah and MacDonald 1969, 11.22, 11.23. □

A noetherian local ring satisfying the equivalent conditions of the proposition is said to be ***regular***.

PROPOSITION 2.26 *An algebraic group $G$ over $k$ (algebraically closed) is smooth if and only if $k[G]_{\mathfrak{m}_a}$ is regular for all $a \in G(k)$.*

PROOF. As $k$ is algebraically closed, the ideals $\mathfrak{m}_a$, $a \in G(k)$, are exactly the maximal ideals of $k[G]$ (AG 2.14). If each $k[G]_{\mathfrak{m}_a}$ is regular, then it is reduced, which implies that $k[G]$ is reduced (Atiyah and MacDonald 1969, 3.8). Conversely, if $G$ is smooth, then $k[G] = k[G']$ for $G'$ a group variety, but it is known that the local rings of a group variety are regular (AG 5.20, 5.25). □

For the next section, we need the following criterion.

PROPOSITION 2.27 *An algebraic group $G$ over $k$ (algebraically closed) is smooth if every nilpotent element of $k[G]$ is contained in $\mathfrak{m}_e^2$.*

PROOF. Let $\overline{G}$ be the associated reduced algebraic group (2.23), and let $\overline{e}$ be the neutral element of $\overline{G}(k)$. Then $k[\overline{G}] = k[G]/\mathfrak{N}$, and so $k[\overline{G}]_{\mathfrak{m}_{\overline{e}}}$ and $k[G]_{\mathfrak{m}_e}$ have the same Krull dimension. The hypothesis implies that

$$\mathfrak{m}_e/\mathfrak{m}_e^2 \to \mathfrak{m}_{\overline{e}}/\mathfrak{m}_{\overline{e}}^2$$

is an isomorphism of $k$-vector spaces, and so $k[G]_{\mathfrak{m}_e}$ is regular. Now (2.16) shows that $k[G]_{\mathfrak{m}}$ is regular for all maximal ideals $\mathfrak{m}$ in $k[G]$, and we can apply (2.26). □

ASIDE 2.28 Now allow $k$ to be an arbitrary field.

(a) In AG, §11, I define an affine algebraic space to be the max spectrum of a finitely generated $k$-algebra $A$. Define an ***affine group space*** to be an affine algebraic space equipped with regular maps

$$m\colon G \times G \to G, \quad \text{inv}\colon G \to G, \quad i\colon \mathbb{A}^0 \to G$$

making $G(R)$ into a group for all $k$-algebras $R$. Then $G \mapsto \operatorname{Spm} G$ is an equivalence from the category of algebraic groups over $k$ to the category of affine group spaces over $k$ (and each is contravariantly equivalent with the category of $k$-bi-algebras).

(b) The functor $G \mapsto \operatorname{Spec} G$ defines an equivalence from the category of algebraic groups over $k$ to the category of affine group schemes of finite type over $k$.

## Algebraic groups in characteristic zero are smooth

LEMMA 2.29 *Let $(A, \Delta, S, \epsilon)$ be a $k$-bi-algebra, and let $\mathfrak{m} = \mathrm{Ker}(\epsilon)$.*
(a) *As a $k$-vector space, $A = k \oplus \mathfrak{m}$.*
(b) *For any $a \in \mathfrak{m}$,*

$$\Delta(a) = a \otimes 1 + 1 \otimes a \quad \text{mod } \mathfrak{m} \otimes \mathfrak{m}.$$

PROOF. (a) The maps $k \longrightarrow A \xrightarrow{\epsilon} k$ are $k$-linear, and compose to the identity.

(b) Choose a basis $(f_i)$ for $\mathfrak{m}$ as a $k$-vector space, and extend it to a basis for $A$ by taking $f_0 = 1$. Write

$$\Delta a = \sum\nolimits_{i \geq 0} d_i \otimes f_i, \quad d_i \in A.$$

From the identities

$$(\mathrm{id}_A, \epsilon) \circ \Delta = \mathrm{id}_A = (\epsilon, \mathrm{id}_A) \circ \Delta$$

we find that

$$d_0 f_0 = a = \sum\nolimits_{i \geq 1} \epsilon(d_i) f_i.$$

Therefore,

$$\Delta(a) - a \otimes 1 - 1 \otimes a = \sum\nolimits_{i \geq 1} (d_i - \epsilon(d_i)) \otimes f_i \in \mathfrak{m} \otimes \mathfrak{m}.$$

□

LEMMA 2.30 *Let $V$ and $V'$ be vector spaces, and let $W$ be a subspace of $V$ such that $V/W$ is finite-dimensional.*[16] *For $x \in V$, $y \in V'$,*

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

PROOF. Because $V/W$ is finite dimensional, there exists a finite set $S$ in $V$ whose image in $V/W$ is a basis. The subspace $W'$ of $V$ spanned by $S$ is a complement to $W$ in $V$, i.e., $V = W \oplus W'$, and so $x$ decomposes uniquely as $x = x_W + x_{W'}$ with $x_W \in W$ and $x_{W'} \in W'$. As

$$V \otimes V' = (W \otimes V') \oplus (W' \otimes V'),$$

we see that $x \otimes y \in W \otimes V'$ if and only if $x_{W'} \otimes y = 0$, which holds if and only if $x_{W'}$ or $y$ is zero. □

THEOREM 2.31 (CARTIER) *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 $A = k[G]$. Let $\mathfrak{m} = \mathfrak{m}_e$. According to (2.27), it suffices to show that every nilpotent element $a$ of $A$ lies in $\mathfrak{m}^2$.

If $a$ maps to zero in $A_{\mathfrak{m}}$, then then it maps to zero in $A/\mathfrak{m}^2 \overset{(18)}{\simeq} A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2$, and there is nothing to prove. Thus, we may suppose 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 may suppose 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 2.29)

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

[16] We assume this only to avoid using Zorn's lemma.

Because $\Delta$ is a homomorphism of $k$-algebras,

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

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

$$(a \otimes 1)^h (1 \otimes a)^i y^j, \quad h + i + j = n.$$

Those with $i + j \geq 2$ lie in $A \otimes_k \mathfrak{m}^2$, and so

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

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

$$na^{n-1} \otimes \overline{a} \in a^{n-1}\mathfrak{m} \otimes_k A/\mathfrak{m}^2 \quad \text{(inside } A \otimes_k A/\mathfrak{m}^2\text{)}. \tag{19}$$

As $k$ has characteristic zero, $n$ is a nonzero element of $k$, and hence it is a unit in $A$. On the other hand, $a^{n-1} \notin a^{n-1}\mathfrak{m}$, because if $a^{n-1} = a^{n-1}m$ with $m \in \mathfrak{m}$, then $(1-m)a^{n-1} = 0$; as $1 - m$ is a unit in $A_{\mathfrak{m}}$, this would imply $a^{n-1} = 0$ in $A_{\mathfrak{m}}$.

Hence $na^{n-1} \notin a^{n-1}\mathfrak{m}$, and so (see 2.30), $a \in \mathfrak{m}^2$. This completes the proof. □

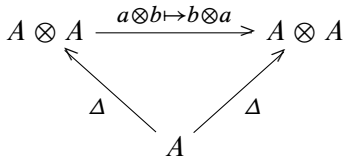
## Cartier duality

To give a $k$-bi-algebra is to give a multiplication map $A \otimes_k A \to A$, a homomorphism $i: k \to A$, and maps $\Delta, \epsilon, S$ satisfying certain conditions which can all be expressed by the commutativity of certain diagrams.

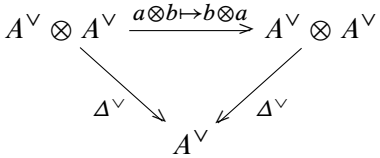
Now suppose that $A$ is finite-dimensional as a $k$-vector space. Then we can form its dual $A^\vee = \mathrm{Hom}_{k\text{-lin}}(A, k)$ and tensor products and Homs behave as you would hope with respect to duals. Thus, from the $k$-linear maps at left, we get the $k$-linear maps at right.

| | |
|---|---|
| $m: A \otimes_k A \to A$ | $m^\vee: A^\vee \to A^\vee \otimes_k A^\vee$ |
| $i: k \to A$ | $i^\vee: A^\vee \to k$ |
| $S: A \to A$ | $S^\vee: A^\vee \to A^\vee$ |
| $\epsilon: A \to k$ | $\epsilon^\vee: k \to A^\vee$ |
| $\Delta: A \to A \otimes_k A$ | $\Delta^\vee: A^\vee \otimes A^\vee \to A^\vee.$ |

This raises the natural question: does $A^\vee$ become a $k$-bi-algebra with these structures? The answer is "no", because the multiplication $m$ is commutative but there is no commutativity condition on $\Delta$. In turns out that this is the only problem. Call a $k$-bialgebra $A$ ***cocommutative*** if the diagram




commutes. Then



commutes, and so $A^\vee$ is a commutative $k$-algebra. Now one can show that $A \mapsto A^\vee$ sends cocommutative finite $k$-bi-algebras to cocommutative finite $k$-bi-algebras (and $A^{\vee\vee} \simeq A$) (Waterhouse 1979, 2.4).

Obviously, the algebraic group $G$ corresponding to the $k$-bi-algebra $A$ is commutative if and only $A$ is cocommutative. We say that an algebraic group $G$ is ***finite*** if $A$ is finite-dimensional as a $k$-vector space. Thus commutative finite algebraic groups correspond to finite-dimensional cocommutative $k$-bialgebras, and so the functor $A \mapsto A^\vee$ defines a functor $G \mapsto G^\vee$ such that $G^{\vee\vee} \simeq G$. The group $G^\vee$ is called the ***Cartier dual*** of $G$. For example, if $G$ is the constant algebraic group defined by a finite commutative group $\Gamma$, then $G^\vee$ is the constant algebraic group defined by the dual group $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$ provided the order of $\Gamma$ is not divisible by the characteristic. If $k$ has characteristic $p$, then $\alpha_p^\vee = \alpha_p$ and $(\mathbb{Z}/p\mathbb{Z})^\vee = \mu_p$, where $\mu_p$ is the algebraic group $R \mapsto \{r \in R^\times \mid r^p = 1\}$.

## Exercises

2-1 Show that there is no algebraic group $G$ over $k$ such that $G(R)$ has two elements for every $k$-algebra $R$.

2-2 Verify directly that $k[\mathbb{G}_a]$ and $k[\mathbb{G}_m]$ (as described in the table) satisfy the axioms to be a bi-algebra.

2-3 Verify all the statements in 2.14.

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 definition of "algebraic group" is equivalent to "affine group scheme algebraic over a field". The approach through functors can be found in Demazure and Gabriel 1970 and Waterhouse 1979. The important Theorem 2.31 was announced in a footnote to Cartier 1962[17]. The proof given here is from Oort 1966.[18]

[17]Cartier, P. Groupes algébriques et groupes formels. 1962 Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962) pp. 87–111, GauthierVillars, Paris.

[18]Oort, F. Algebraic group schemes in characteristic zero are reduced. Invent. Math. 2 1966 79–80.

# 3 Linear representations

The main result in this section is that all affine algebraic groups can be realized as subgroups of $\mathrm{GL}_n$ for some $n$. At first sight, this is a surprising result. For example, it says that all possible multiplications in algebraic groups are just matrix multiplication in disguise.

Before looking at the case of algebraic groups, we should review how to realize a finite group as a matrix group. Let $G$ be a finite group. A representation of $G$ on a $k$-vector space $V$ is a homomorphism of groups $G \to \mathrm{Aut}_{k\text{-lin}}(V)$, i.e., an action $G \times V \to V$ in which each $\gamma \in G$ acts as a $k$-linear map. Let $X \times G \to X$ be a (right) action of $G$ on a finite set $X$. Define $V$ to be the $k$-vector space of maps $X \to k$, and let $G$ act on $V$ by the rule:

$$(\gamma f)(x) = f(x\gamma) \quad \gamma \in G,\ f \in V,\ x \in X.$$

This defines a representation of $G$ on $V$, which is injective if $G$ acts effectively on $X$. The vector space $V$ has a natural basis consisting of the maps that send one element of $X$ to 1 and the remaining elements to 0, and so this gives a homomorphism $G \to \mathrm{GL}_n(k)$ where $n = \#X$.

For example, for $S_n$ acting on $\{1, 2, \dots, n\}$, this gives the map $\sigma \mapsto I(\sigma)\colon S_n \to \mathrm{GL}_n(k)$ in §1. When we take $X = G$, the representation we get is called the ***regular representation***, and the map $G \to \mathrm{Aut}_{k\text{-linear}}(V)$ is injective.

## Linear representations and comodules

Let $G$ be an algebraic group over $k$, and let $V$ be a vector space over $k$ (not necessarily finite dimensional). A ***linear representation*** of $G$ on $V$ is a natural homomorphism[19]

$$\Phi\colon G(R) \to \mathrm{Aut}_{R\text{-lin}}(V \otimes_k R).$$

In other words, for each $k$-algebra $R$, we have an action

$$G(R) \times (V \otimes_k R) \to V \otimes_k R$$

of $G(R)$ on $V \otimes_k R$ in which each $g \in G(R)$ acts $R$-linearly, and for each homomorphism of $k$-algebras $R \to S$, the following diagram

$$\begin{array}{ccccc} G(R) & \times & V \otimes_k R & \to & V \otimes_k R \\ \downarrow & & \downarrow & & \downarrow \\ G(S) & \times & V \otimes_k S & \to & V \otimes_k S. \end{array}$$

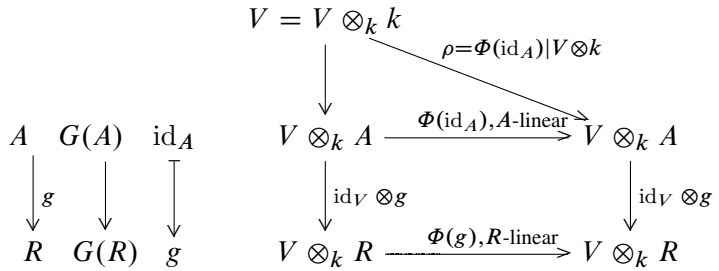
commutes. We often drop the "linear".

Let $\Phi$ be a linear representation of $G$ on $V$. Given a homomorphism $\alpha\colon R \to S$ and an element $g \in G(R)$ mapping to $h$ in $G(S)$, we get a diagram:

$$\begin{array}{ccc} R & G(R) & g \\ \downarrow{\scriptstyle \alpha} & \downarrow & \downarrow \\ S & G(S) & h \end{array} \qquad \begin{array}{ccc} V \otimes_k R & \xrightarrow{\Phi(g)} & V \otimes_k R \\ \downarrow{\scriptstyle \mathrm{id}_V \otimes \alpha} & & \downarrow{\scriptstyle \mathrm{id}_V \otimes \alpha} \\ V \otimes_k S & \xrightarrow{\Phi(h)} & V \otimes_k S \end{array}$$

[19] The reader should attach no importance to the fact that I sometimes write $R \otimes_k V$ and sometimes $V \otimes_k R$.

Now let $g \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$. Then $g\colon A \to R$ sends the "universal" element $\mathrm{id}_A \in G(A) = \mathrm{Hom}_{k\text{-alg}}(A, A)$ to $g$, and so the picture becomes the bottom part of




In particular, we see that $\Phi$ defines a $k$-linear map $\rho =_{\mathrm{df}} \Phi(\mathrm{id}_A)|V\colon V \to V \otimes_k A$. Moreover, it is clear from the diagram that $\rho$ determines $\Phi$, because $\Phi(\mathrm{id}_A)$ is the unique[20] $A$-linear extension of $\rho$ to $V \otimes_k A$, and $\Phi(g)$ is the unique $R$-linear extension of $\Phi(\mathrm{id}_A)$ to $V \otimes_k R$.

Conversely, suppose we have a $k$-linear map $\rho\colon V \to V \otimes_k A$. Then the diagram shows that we get a natural *map*

$$\Phi\colon G(R) \to \mathrm{Aut}_{R\text{-lin}}(V \otimes_k R),$$

namely, given $g\colon A \to R$, $\Phi(g)$ is the unique $R$-linear map making

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V \otimes_k A \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}_V \otimes g} \\ V \otimes_k R & \xrightarrow{\Phi(g)} & V \otimes_k R \end{array}$$

commute. These maps will be *homomorphisms* if and only if the following diagrams commute:

$$\begin{array}{ccccc} V & \xrightarrow{\rho} & V \otimes_k A & \qquad & V \xrightarrow{\rho} V \otimes_k A \\ & \searrow^{=} & \downarrow{\scriptstyle \mathrm{id}_V \otimes \epsilon} & & \rho\downarrow \qquad\qquad \downarrow{\scriptstyle \mathrm{id}_V \otimes \Delta} \\ & & V \otimes_k k & & V \otimes_k A \xrightarrow{\rho \otimes \mathrm{id}_A} V \otimes_k A \otimes_k A \end{array} \tag{20}$$

For example, we must have $\Phi(1_{G(R)}) = \mathrm{id}_{V \otimes_k R}$. By definition, $1_{G(R)} = (A \xrightarrow{\epsilon} k \to R)$ as an element of $\mathrm{Hom}_{k\text{-alg}}(A, R)$, and so the following diagram must commute

$$\begin{array}{ccc} V & \xrightarrow[k\text{-linear}]{\rho} & V \otimes_k A \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}_V \otimes \epsilon} \\ V \otimes k & \longrightarrow & V \otimes_k k \\ \downarrow & & \downarrow \\ V \otimes_k R & \xrightarrow{\mathrm{id}_{V \otimes_k R}} & V \otimes_k R. \end{array}$$

[20] Let $R \to S$ be a homomorphism of rings, and let $M$ be an $R$-module. Then $m \mapsto 1 \otimes m\colon M \to S \otimes_R M$ is $R$-linear and universal: any other $R$-linear map $M \to N$ from $M$ to an $S$-module factors uniquely through it:

$$\mathrm{Hom}_{R\text{-lin}}(M, N) \xrightarrow{\simeq} \mathrm{Hom}_{S\text{-lin}}(M \otimes_R S, N).$$

This means that the upper part of the diagram must commute with the map $V \otimes_k k \to V \otimes_k k$ being the identity map, which is the first of the diagrams in (20). Similarly, the second diagram in (20) commutes if and only if the formula

$$\Phi(gh) = \Phi(g)\Phi(h)$$

holds.[21]

DEFINITION 3.1 A ***comodule*** over a $k$-bialgebra $A$ is a $k$-linear map $V \to V \otimes_k A$ such that the diagrams (20) commute.

The above discussion has proved the following proposition:

PROPOSITION 3.2 *Let $G$ be an algebraic group over $k$ with corresponding bialgebra $A$, and let $V$ be a $k$-vector space. To give a linear representation of $G$ on $V$ is the same as to give an $A$-comodule structure on $V$.*

An element $g$ of $G(R) = \mathrm{Hom}_{k\text{-alg}}(k[G], R)$ acts on $v \in V \otimes_k R$ according to the rule:

$$g\,v = ((\mathrm{id}_V, g) \circ \rho)(v). \tag{23}$$

EXAMPLE 3.3 For any $k$-bialgebra $A$, the map $\Delta\colon A \to A \otimes_k A$ is a comodule structure on $A$. The corresponding representation of $A$ is called the ***regular representation***.

A $k$-subspace $W$ of an $A$-comodule $V$ is a ***subcomodule*** if $\rho(W) \subset W \otimes_k A$. Then $W$ itself is an $A$-comodule, and the linear representation of $G$ on $W$ defined by this comodule structure is the restriction of that on $V$.

PROPOSITION 3.4 *Let $(V, \rho)$ be a comodule over a $k$-bialgebra $A$. Every finite subset of $V$ is contained in a sub-comodule of $V$ having finite dimension over $k$.*

PROOF. Since a finite sum of (finite-dimensional) subcomodules is again a (finite-dimensional) subcomodule, it suffices to show that each element $v$ of $V$ is contained in finite-dimensional subcomodule. Let $\{a_i\}$ be a basis (possibly infinite) for $A$ as a $k$-vector space, and let

$$\rho(v) = \sum_i v_i \otimes a_i, \quad v_i \in V,$$

[21] Here (from Waterhouse 1979, p23) is the argument that the commutativity of the second diagram in (20) means that $\Phi(gh) = \Phi(g)\Phi(h)$ for $g, h \in G(R)$. By definition, $gh$ is the composite

$$A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{(g,h)} R$$

and so $\Phi(gh)$ is the extension of

$$V \xrightarrow{\rho} V \otimes_k A \xrightarrow{\mathrm{id}_V \otimes \Delta} V \otimes_k A \otimes_k A \xrightarrow{\mathrm{id}_V \otimes (g,h)} V \otimes_k R \tag{21}$$

to $V \otimes_k R$. On the other hand, $\Phi(g) \circ \Phi(h)$ is given by

$$V \xrightarrow{\rho} V \otimes_k A \xrightarrow{\mathrm{id}_V \otimes h} V \otimes_k R \xrightarrow{\rho \otimes \mathrm{id}_R} V \otimes_k A \otimes_k R \xrightarrow{\mathrm{id} \otimes (g, \mathrm{id})} V \otimes R,$$

which equals

$$V \xrightarrow{\rho} V \otimes_k A \xrightarrow{\rho \otimes \mathrm{id}_A} V \otimes_k A \otimes_k A \xrightarrow{\mathrm{id} \otimes (g,h)} V \otimes R. \tag{22}$$

Now (21) and (22) agree for all $g, h$ if and only if the second diagram in (20) commutes.

(finite sum, i.e., only finitely many $v_i$ are nonzero). Write

$$\Delta(a_i) = \sum_{j,k} r_{ijk}(a_j \otimes a_k), \quad r_{ijk} \in k.$$

We shall show that

$$\rho(v_k) = \sum_{i,j} v_i \otimes r_{ijk}a_j \tag{24}$$

from which it follows that the $k$-subspace of $V$ spanned by $v$ and the $v_i$ is a subcomodule containing $v$. Recall from (20) that

$$(\rho \otimes \mathrm{id}_A) \circ \rho = (\mathrm{id}_V \otimes \Delta) \circ \rho.$$

On applying the left hand side to $v$, we get

$$(\rho \otimes \mathrm{id}_A)(\rho(v)) = \sum_i \rho(v_i) \otimes a_i \quad \text{(inside } V \otimes_k A \otimes_k A).$$

On applying the right hand side to $v$, we get

$$(\mathrm{id}_V \otimes \Delta)(\rho(v)) = \sum_{i,j,k} v_i \otimes r_{ijk}a_j \otimes a_k.$$

On comparing the coefficients of $1 \otimes 1 \otimes a_k$, we obtain (24)[22]. □

Let $\Phi$ be a linear representation of $G$ on finite-dimensional vector space $V$. On choosing a basis $(e_i)_{1 \le i \le n}$ for $V$, we get a homomorphism $G \to \mathrm{GL}_n$, and hence a homomorphism of $k$-algebras

$$k[\mathrm{GL}_n] = k[\ldots, X_{ij}, \ldots, \det(X_{ij})^{-1}] \to A.$$

Let

$$\rho(e_j) = \sum_i e_i \otimes a_{ij}, \quad a_{ij} \in A.$$

LEMMA 3.5 *The image of $X_{ij}$ in $A$ is $a_{ij}$.*

PROOF. Routine. □

DEFINITION 3.6 A homomorphism $G \to H$ of algebraic groups is an ***embedding*** if the corresponding map of algebras $k[H] \to k[G]$ is surjective. We then call $G$ an ***algebraic subgroup*** of $H$.

PROPOSITION 3.7 *If $G \to H$ is an embedding, then the homomorphisms $G(R) \to H(R)$ are all injective.*

[22]The choice of a basis $(a_i)_{i \in I}$ for $A$ as a $k$-vector space determines an isomorphism

$$A \simeq k^{(I)}$$

(direct sum of copies of $k$ indexed by $I$). When tensored, this becomes

$$V \otimes_k A \otimes_k A \simeq (V \otimes_k A)^{(I)}.$$

We are equating the components in the above decomposition corresponding to the index $k$.

PROOF. When $k[H] \to k[G]$ is surjective, two homomorphisms $k[G] \to R$ that become equal when composed with it must already be equal. □

THEOREM 3.8 *Let $G$ be an algebraic group. For some $n$, there exists an embedding $G \to \mathrm{GL}_n$.*

PROOF. Let $A = k[G]$, and let $V$ be a finite-dimensional subcomodule of $A$ containing a set of generators for $A$ as a $k$-algebra. Let $(e_i)_{1\le i\le n}$ be a basis for $V$, and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. According to (3.5), the image of $k[\mathrm{GL}_V] \to A$ contains the $a_{ij}$. But

$$e_j \overset{(20)}{=} (\epsilon \otimes \mathrm{id}_A)\Delta(e_j) = \sum_i \epsilon(e_i)a_{ij}, \quad \epsilon(e_i) \in k,$$

and so the image contains $V$; it therefore equals $A$. □

In other words, every algebraic group can be realized as an algebraic subgroup of a $\mathrm{GL}_n$ for some $n$. The theorem is analogous to the theorem that every finite-dimensional vector space is isomorphic to $k^n$ for some $n$. Just as that theorem does *not* mean that we should consider only the vector spaces $k^n$, Theorem 3.8 does *not* mean that we should consider only subgroups of $\mathrm{GL}_n$ because realizing an algebraic group in this way involves many choices.

PROPOSITION 3.9 *Let $G \to \mathrm{GL}_V$ be a faithful representation of $G$. Then every other representation of $G$ can be obtained from $V$ by forming tensor products, direct sums, duals, and subquotients.*

PROOF. Omitted for the present (see Waterhouse 1979, 3.5). □

EXAMPLE 3.10 Let $G$ be the functor sending a $k$-algebra $R$ to $R \times R \times R$ with

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

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

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

is an embedding of $G$ into $\mathrm{GL}_3$. Note that the functor $R \to R \times R \times R$ also has an obvious commutative group structure (componentwise addition), and so the $k$-algebra $k[X, Y, Z]$ has more than one bialgebra structure.

REMARK 3.11 In the notes, we make frequent use of the fact that, when $k$ is a field, $V \mapsto V \otimes_k W$ is an exact functor (not merely right exact). To prove it, note that any subspace $V'$ of $V$ has a complement, $V = V' \oplus V''$, and $- \otimes_k W$ preserves direct sums (see also 6.5).

## Stabilizers of subspaces

PROPOSITION 3.12 *Let $G \to \mathrm{GL}_V$ be a representation of $G$, and let $W$ subspace of $V$. For a $k$-algebra $R$, define*

$$G_W(R) = \{g \in G(R) \mid g(W \otimes_k R) = W \otimes_k R\}.$$

*Then the functor $G_W$ is an algebraic subgroup of $G$.*

PROOF. Let $e_1, \dots, e_m$ be a basis for $W$, and extend it to a basis $e_1, \dots, e_n$ for $V$. Write

$$\rho(e_j) = \sum e_i \otimes a_{ij}.$$

Let $g \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$. Then

$$ge_j = \sum e_i \otimes g(a_{ij}).$$

Thus, $g(W \otimes_k R) \subset W \otimes_k R$ if and only if $g(a_{ij}) = 0$ for $j \le m, i > m$. Hence $G_W$ is represented by the quotient of $A$ by the ideal generated by $\{a_{ij} \mid j \le m, i > m\}$. □

The algebraic group $G_W$ is called the ***stabilizer*** of $W$ in $G$.

THEOREM 3.13 (CHEVALLEY) *Every algebraic subgroup of an algebraic group $G$ arises as the stabilizer of a subspace in some finite-dimensional linear representation of $G$; the subspace can even be taken to be one-dimensional.*

PROOF. Waterhouse 1979, 16.1. □

**Summary of formulas**

$k$ is a field. A functor $G$ such that $G \approx h_A$ for some $k$-algebra $A$ is said to be representable (by $A$).

| Algebra | Functor |
|---|---|
| $k$-algebra $A$ | Functor $h_A$: $k$-algebras$\to$Sets<br>$h_A(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$<br>$h_A(R \xrightarrow{\alpha} S) = (g \mapsto \alpha \circ g)$ |
| $\Delta: A \to A \otimes_k A$ | Law of composition<br>$G(R) \times G(R) \to G(R)$<br>$h_A(R) \times h_A(R) \simeq h_{A\otimes_k A}(R) \xrightarrow{-\circ\Delta} h_A(R)$ |
| $\epsilon: A \to k$ | Natural map $\{1\} \to G(R)$<br>$h_k(R) \xrightarrow{-\circ\epsilon} h_A(R)$ |
| $S: A \to A$ | Natural map $G(R) \to G(R)$<br>$h_A(R) \xrightarrow{-\circ S} h_A(R)$ |
| $\begin{array}{ccc} A\otimes_k A\otimes_k A & \xleftarrow{\mathrm{id}_A\otimes\Delta} & A\otimes_k A \\ \uparrow{\scriptstyle \Delta\otimes\mathrm{id}_A} & & \uparrow{\scriptstyle \Delta} \\ A\otimes_k A & \xleftarrow{\Delta} & A \end{array}$ | The law of composition<br>is associative. |
| $\begin{array}{ccc} A & \xleftarrow{\epsilon\otimes\mathrm{id}_A} & A\otimes_k A \\ \uparrow{\scriptstyle \mathrm{id}_A\otimes\epsilon} & \nwarrow^{\mathrm{id}_A} & \uparrow{\scriptstyle \Delta} \\ A\otimes_k A & \xleftarrow{\Delta} & A \end{array}$ | The element $1 \in G(R)$<br>given by $\epsilon$ is neutral. |
| $\begin{array}{ccc} A & \underset{(\mathrm{id}_A,S)}{\overset{(S,\mathrm{id}_A)}{\leftarrow}} & A\otimes_k A \\ \uparrow & & \uparrow{\scriptstyle \Delta} \\ k & \xleftarrow{\epsilon} & A \end{array}$ | For $g \in G(R)$, $g \circ S$<br>is an inverse. |
| $k$-bialgebra | algebraic group if $A$ f.g. |
| $k$-vector space $V$ | |
| $\rho: V \to V \otimes_k A$ | Natural map<br>$\Phi: G(R) \to \mathrm{End}_{R\text{-linear}}(V \otimes_k R)$<br>$\begin{array}{ccc} V & \xrightarrow[k\text{-linear}]{\rho} & V\otimes_k A \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}_V\otimes g} \\ V\otimes_R R & \xrightarrow[R\text{-linear}]{\Phi(g)\text{ unique}} & V\otimes_k R \end{array}$ |
| $\begin{array}{ccc} V & \xrightarrow{\rho} & V\otimes_k A \\ & \searrow^{\simeq} & \downarrow{\scriptstyle \mathrm{id}_V\otimes\epsilon} \\ & & V\otimes_k k \end{array}$ | $\Phi(1_{G(R)}) = \mathrm{id}_{V\otimes_k R}$ |
| $\begin{array}{ccc} V & \xrightarrow{\rho} & V\otimes_k A \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \mathrm{id}_V\otimes\Delta} \\ V\otimes_k A & \xrightarrow{\rho\otimes\mathrm{id}_A} & V\otimes_k A\otimes_k A \end{array}$ | $\Phi(g \cdot g') = \Phi(g) \circ \Phi(g')$. |
| $A$-comodule | linear representation of $G$ on $V$ |

# 4 Matrix Groups

In this section, $k$ is an *infinite* field.

An algebraic subgroup $G$ of $\mathrm{GL}_n$ defines a subgroup $G(k)$ of $\mathrm{GL}_n(k)$. In this section, we determine the subgroups $\Gamma$ of $\mathrm{GL}_n(k)$ that arise in this way from algebraic subgroups of $\mathrm{GL}_n$, and we shall see that this gives an elementary way of defining many algebraic groups.

## An elementary result

PROPOSITION 4.1 *Let $f \in k[X_1, \dots, X_n]$. If $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots a_n) \in k^n$, then $f$ is the zero polynomial (i.e., all its coefficients are zero).*

PROOF. We use induction on $n$. For $n = 1$, it becomes the statement that a nonzero polynomial in one variable has only finitely many roots (which follows from unique factorization, for example). Now suppose $n > 1$ and write $f = \sum g_i X_n^i$ with each $g_i \in k[X_1, \dots, X_{n-1}]$. For every $(a_1, \dots, a_{n-1}) \in k^{n-1}$, $f(a_1, \dots, a_{n-1}, X_n)$ is a polynomial of degree 1 with infinitely many zeros, and so each of its coefficients $g_i(a_1, \dots, a_{n-1}) = 0$. By induction, this implies that each $g_i$ is the zero polynomial. □

COROLLARY 4.2 *Let $f, g \in k[X_1, \dots, X_n]$ with $g$ not the zero polynomial. If $f$ is zero at every $(a_1, \dots, a_n)$ with $g(a_1, \dots, a_n) \neq 0$, then $f$ is the zero polynomial.*

PROOF. The polynomial $fg$ is zero on all of $k^n$. □

The proposition shows that we can identify $k[X_1, \dots, X_n]$ with a ring of functions on $k^n$ (the ring of ***polynomial functions***).

## How to get bialgebras from groups

For a set $X$, let $R(X)$ be the ring of maps $X \to k$. For sets $X$ and $Y$, let $R(X) \otimes_k R(Y)$ act on $X \times Y$ by $(f \otimes g)(x, y) = f(x)g(y)$.

LEMMA 4.3 *The map $R(X) \otimes_k R(Y) \to R(X \times Y)$ just defined is injective.*

PROOF. Let $(g_i)_{i \in I}$ be a basis for $R(Y)$ as a $k$-vector space, and let $h = \sum f_i \otimes g_i$ be a nonzero element of $R(X) \otimes_k R(Y)$. Some $f_i$, say $f_{i_0}$, is not the zero function. Let $x \in X$ be such that $f_{i_0}(x) \neq 0$. Then $\sum f_i(x)g_i$ is a linear combination of the $g_i$ with at least one coefficient nonzero, and so is nonzero. Thus, there exists a $y$ such that $\sum f_i(x)g_i(y) \neq 0$; hence $h(x, y) \neq 0$. □

Let $\Gamma$ be a group. From the group structure on $\Gamma$, we get the following maps:

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

PROPOSITION 4.4 *If $\Delta$ maps $R(\Gamma)$ into the subring $R(\Gamma) \otimes_k R(\Gamma)$ of $R(\Gamma \times \Gamma)$, then $(R(\Gamma), \epsilon, S, \Delta)$ is a $k$-bialgebra.*

PROOF. We have to check (see p17) that, for example,

$$((\mathrm{id}\otimes\Delta)\circ\Delta)(f) = ((\Delta\otimes\mathrm{id})\circ\Delta)(f)$$

for all $f \in R(\Gamma)$, but, because of the lemma it suffices to prove that the two sides are equal as functions on $\Gamma\times\Gamma\times\Gamma$. Let $\Delta(f) = \sum f_i\otimes g_i$, so that $\sum f_i(x)g_i(y) = f(xy)$ for all $x, y \in \Gamma$. Then

$$\begin{aligned}((\mathrm{id}\otimes\Delta)\circ\Delta)(f))(x,y,z) &= (\sum f_i\otimes\Delta(g_i))(x,y,z)\\ &= \sum f_i(x)g_i(yz)\\ &= f(x(yz)).\end{aligned}$$

Similarly,

$$((\Delta\otimes\mathrm{id})\circ\Delta)(f) = f((xy)z).$$

□

## A little algebraic geometry

A subset $V$ of $k^n$ is[23] ***closed*** if it is the set of common zeros of some set $S$ of polynomials

$$V = \{(a_1,\dots,a_n)\in k^n \mid f(a_1,\dots,a_n) = 0 \text{ all } f(X_1,\dots,X_n)\in S\}.$$

We write $V(S)$ for the zero-set (set of common zeros) of $S$.

The ideal $\mathfrak{a}$ generated by $S$ consists of all finite sums $\sum f_i g_i$ with $f_i \in k[X_1,\dots,X_n]$ and $g_i \in S$. Clearly, $V(\mathfrak{a}) = V(S)$, and so the algebraic subsets can also be described as the zero-sets of ideals in $k[X_1,\dots,X_n]$. According to the Hilbert basis theorem (AG, 2.2), every ideal in $k[X_1,\dots,X_n]$ is finitely generated, and so every algebraic set is the zero-set of a *finite* set of polynomials.

If the sets $V_i$ are closed, then so also is $\bigcap V_i$. Moreover, if $W$ is the zero-set of some polynomials $f_i$ and $V$ is the zero-set of the polynomials $g_j$, then $V\cup W$ is the zero-set[24] of the polynomials $f_i g_j$. As $\emptyset = V(1)$ and $k^n = V(0)$ are both closed, this shows that the closed sets are the closed sets for a topology on $k^n$, called the ***Zariski topology***.

Note that

$$D(h) = \{P\in k^n \mid h(P)\neq 0\}$$

is an open subset of $k^n$, being the complement of $V(h)$. Moreover, $D(h_1)\cup\ldots\cup D(h_n)$ is the complement of $V(h_1,\dots,h_n)$, and so every open subset of $k^n$ is a finite union of $D(h)$'s; in particular, the $D(h)$'s form a base for the topology on $k^n$.

Let $V$ be a closed set, and let $I(V)$ be the set of polynomials zero on $V$. Then

$$k[V] \stackrel{\text{df}}{=} k[X_1,\dots,X_n]/I(V)$$

can be identified with the ring of functions $V\to k$ defined by polynomials.

We shall need two easy facts.

[23] Or algebraic, but that would cause confusion for us.

[24] Certainly, the $f_i g_j$ are zero on $V\cup W$; conversely, if $f_i(P)g_j(P) = 0$ for all $i, j$ and $g_j(P)\neq 0$ for some $j$, then $f_i(P) = 0$ for all $i$, and so $P\in V$.

4.5 Let $W$ be a closed subset of $k^m$ and let $V$ be a closed subset of $k^n$. Let $\varphi: k^m \to k^n$ be the map defined by polynomials $f_i(X_1, \dots, X_m)$, $1 \le i \le n$. Then $\varphi(W) \subset V$ if and only if the map $X_i \mapsto f_i: k[X_1, \dots, X_n] \to k[X_1, \dots, X_m]$ sends $I(V)$ into $I(W)$, and so gives rise to a commutative diagram

$$\begin{array}{ccc} k^m & \xrightarrow{\varphi} & k^n \\ \cup & & \cup \\ W & \longrightarrow & V \end{array} \qquad \begin{array}{ccc} k[X_1, \dots, X_m] & \xleftarrow{\varphi^*} & k[X_1, \dots, X_n] \\ \downarrow & & \downarrow \\ k[W] & \longleftarrow & k[V]. \end{array}$$

4.6 Let $W \subset k^m$ and $V \subset k^n$ be closed sets. Then $W \times V \subset k^m \times k^n$ is a closed subset of $k^{m+n}$, and the canonical map

$$k[W] \otimes_k k[V] \to k[W \times V]$$

is an isomorphism. In more detail, let $\mathfrak{a} = I(W) \subset k[X_1, \dots, X_m]$ and $\mathfrak{b} = I(V) \subset k[Y_1, \dots, Y_n]$; then

$$k[W] \otimes_k k[V] \simeq k[X_1, \dots, X_m, Y_1, \dots, Y_n]/(\mathfrak{a}, \mathfrak{b})$$

where $(\mathfrak{a}, \mathfrak{b})$ is the ideal generated by $\mathfrak{a}$ and $\mathfrak{b}$ (see AG 4.14). Certainly $(\mathfrak{a}, \mathfrak{b}) \subset I(W \times V)$, but because of (4.3) it equals $I(W \times V)$. Moreover, we have a commutative diagram

$$\begin{array}{ccc} k[X_1, \dots, X_m] \otimes_k k[X_1, \dots, X_n] & \xrightarrow[1 \otimes X_i \mapsto X_{m+i}]{X_i \otimes 1 \mapsto X_i} & k[X_1, \dots, X_{m+n}] \\ \downarrow & & \downarrow \\ k[W] \otimes_k k[V] & \longrightarrow & k[W \times V] \end{array}$$

The ***radical*** of an ideal $\mathfrak{a}$, $\operatorname{rad}(\mathfrak{a})$, is $\{f \mid f^n \in \mathfrak{a} \text{ for some } n \ge 1\}$. Clearly, it is again an ideal. An ideal $\mathfrak{a}$ is ***radical*** if $\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$, i.e., if $k[X_1, \dots, X_n]/\mathfrak{a}$ is reduced.

For a subset $S$ of $k^n$, let $I(S)$ be the set of $f \in k[X_1, \dots, X_n]$ such that $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in S$.

THEOREM 4.7 (STRONG NULLSTELLENSATZ) *For any ideal $\mathfrak{a}$, $IV(\mathfrak{a}) \supset \operatorname{rad}(\mathfrak{a})$, and equality holds if $k$ is algebraically closed.*

PROOF. If $f^n \in \mathfrak{a}$, then clearly $f$ is zero on $V(\mathfrak{a})$, and so the inclusion is obvious. For a proof of the second part, see AG 2.11. □

When $k$ is not algebraically closed, then in general $IV(\mathfrak{a}) \ne \mathfrak{a}$. For example, let $k = \mathbb{R}$ and let $\mathfrak{a} = (X^2 + Y^2 + 1)$. Then $V(\mathfrak{a})$ is empty, and so $IV(\mathfrak{a}) = k[X_1, \dots, X_n]$.

## Variant

Let $k(X_1, \dots, X_n)$ be the field of fractions of $k[X_1, \dots, X_n]$. Then, for any nonzero polynomial $h$, the subring $k[X_1, \dots, X_n, \frac{1}{h}]$ of $k(X_1, \dots, X_n)$ is the ring obtained from $k[X_1, \dots, X_n]$ by inverting $h$ (AG 1.27). Because of (4.2), it can be identified with a ring of functions on $D(h)$. The closed subsets of $D(h)$ (as a subspace of $k^n$), are just the zero-sets of collections of functions in $k[X_1, \dots, X_n, \frac{1}{h}]$. Now the above discussion holds with $k^n$ and $k[X_1, \dots, X_n]$ replaced by $D(h)$ and $k[X_1, \dots, X_n, \frac{1}{h}]$. This can be proved directly, or by identifying $D(h)$ with the closed subset $V(hX_{n+1} - 1)$ of $k^{n+1}$ via $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_n, h(x_1, \dots, x_n)^{-1})$.

## Closed subgroups of $\mathrm{GL}_n$ and algebraic subgroups

We now identify $k[\mathrm{GL}_n]$ with the subring $k[X_{11},\dots,X_{nn},\frac{1}{\det(X_{ij})}]$ of $k(\dots,X_{ij},\dots)$, and apply the last paragraph. Because $k[\mathrm{GL}_n]$ is obtained from $k[X_{11},\dots,X_{nn}]$ by inverting $\det(X_{ij})$, a $k$-algebra homomorphism $k[\dots,X_{ij},\dots,\frac{1}{\det(X_{ij})}]\to R$ is determined by the images of the $X_{ij}$, and these can be any values $r_{ij}$ such that $\det(r_{ij})$ is a unit.

Let $G\to\mathrm{GL}_n$ be an algebraic subgroup of $\mathrm{GL}_n$. By definition, the embedding $G\hookrightarrow\mathrm{GL}_n$ is defined by a surjective homomorphism $\alpha\colon k[\mathrm{GL}_n]\to k[G]$. Let $\mathfrak{a}$ be the kernel of $\alpha$. Then

$$\begin{aligned}G(k)&=\mathrm{Hom}_{k\text{-alg}}(A,k)\\&=\{\varphi\colon k[\mathrm{GL}_n]\to k\mid \mathrm{Ker}(\varphi)\supset\mathrm{Ker}(\alpha)\}\\&\simeq V(\mathfrak{a}).\end{aligned}$$

Thus, $G(k)$ is a closed subgroup of $\mathrm{GL}_n(k)$.

Conversely, let $\Gamma$ be a closed subgroup $\mathrm{GL}_n(k)$ and let $k[\Gamma]$ be the ring of polynomial functions on $\Gamma$ (i.e., functions defined by elements of $k[\mathrm{GL}_n]$). The map $S$ sends polynomial functions on $\Gamma$ to polynomial functions on $\Gamma$ because it is defined by a polynomial (Cramer's rule). Similarly, $\Delta$ sends polynomial functions on $\Gamma$ to polynomial functions on $\Gamma\times\Gamma$, i.e., to elements of $k[\Gamma\times\Gamma]\simeq k[\Gamma]\otimes_k k[\Gamma]$. Now one sees as in the proof of (4.4) that $(k[\Gamma],\epsilon,S,\Delta)$ is a $k$-bialgebra. Moreover, it is clear that the algebraic subgroup $G$ of $\mathrm{GL}_n$ corresponding to it has $G(k)=\Gamma$.

From an algebraic subgroup $G$ of $\mathrm{GL}_n$, we get

$$G\rightsquigarrow\Gamma=G(k)\rightsquigarrow G'. \tag{25}$$

If $k[G]$ is the quotient of $k[\mathrm{GL}_n]$ by the ideal $\mathfrak{a}$, then $k[G']$ is the quotient of $k[\mathrm{GL}_n]$ by the ideal $IV(\mathfrak{a})$. Therefore, when $k=\overline{k}$ the strong Nullstellensatz shows that $G=G'$ if and only if $G$ is smooth (i.e., $k[G]$ is reduced).

In summary:

THEOREM 4.8 *Let $\Gamma$ be a subgroup of $\mathrm{GL}_n(k)$. There exists an algebraic subgroup $G$ of $\mathrm{GL}_n$ such that $G(k)=\Gamma$ if and only if $\Gamma$ is closed, in which case there exists a well-defined reduced $G$ with this property (that for which $k[G]$ is the ring of polynomial functions on $\Gamma$). When $k$ is algebraically closed, the algebraic subgroups of $\mathrm{GL}_n$ arising in this way are exactly the smooth algebraic groups.*

The algebraic group $G$ corresponding to $\Gamma$ can be described as follows: let $\mathfrak{a}\subset k[\mathrm{GL}_n]$ be the ideal of polynomials zero on $\Gamma$; then $G(R)$ is the zero-set of $\mathfrak{a}$ in $\mathrm{GL}_n(R)$.

ASIDE 4.9 When $k$ is not algebraically closed, then not every reduced algebraic subgroup of $\mathrm{GL}_n$ arises from an closed subgroup of $\mathrm{GL}_n(k)$. For example, consider $\mu_3$ regarded as a subgroup of $\mathbb{G}_m=\mathrm{GL}_1$ over $\mathbb{R}$. Then $\mu_3(\mathbb{R})=1$, and the algebraic group associated with 1 is 1. Assume, for simplicity, that $k$ has characteristic zero, and let $G$ be an algebraic subgroup of $\mathrm{GL}_n$. Then, with the notation of (25), $G=G'$ if and only if $G(k)$ is dense in $G(\overline{k})$ for the Zariski topology. It is known that this is always true when $G(\overline{k})$ is connected for the Zariski topology, but unfortunately, the proof uses the structure theory of algebraic groups (Borel 1991, 18.3, p220).

# 5 Example: the spin group

Let $\phi$ be a nondegenerate bilinear form on a $k$-vector space $V$. The special orthogonal group $\mathrm{SO}(\phi)$ is connected and almost-simple, and it has a 2-fold covering $\mathrm{Spin}(\phi)$ which we now define.

Throughout this section, $k$ is a field not of characteristic 2 and "$k$-algebra" means "associative (not necessarily commutative) $k$-algebra containing $k$ 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 $cI_n$.

## 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

$$q\colon V \to k$$

such that $q(x) = \phi_q(x,x)$ for some symmetric bilinear form $\phi_q\colon V \times V \to k$. Note that

$$q(x+y) = q(x) + q(y) + 2\phi_q(x,y), \tag{26}$$

and so $\phi_q$ 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 $\phi$ (rather than $\phi_q$) for the associated symmetric bilinear form and denote $(V,q)$ by $(V,\phi_q)$ or $(V,\phi)$. A nonzero vector $x$ in $V$ is ***isotropic*** if $q(x) = 0$ and ***anisotropic*** if $q(x) \neq 0$.

Let $(V_1,q_1)$ and $(V_2,q_2)$ be quadratic spaces. An injective $k$-linear map $\sigma\colon V_1 \to V_2$ is an ***isometry*** if $q_2(\sigma x) = q_1(x)$ 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

$$V = V_1 \oplus V_2$$
$$q(x_1 + x_2) = q(x_1) + q(x_2).$$

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 5.1 *Every quadratic space has an orthogonal basis (and so is an orthogonal sum of quadratic spaces of dimension* 1*).*

PROOF. If $q(V) = 0$, every basis is orthogonal. Otherwise, there exist $x, y \in V$ such that $\phi(x,y) \neq 0$. From (26) we see that at least one of the vectors $x, y, x+y$ is anisotropic. Thus, 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

$$e, e_2 - \frac{\phi(e,e_2)}{q(e)}, \dots, e_n - \frac{\phi(e,e_n)}{q(e)}$$

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 $W$. □

An orthogonal basis defines an isometry $(V,q) \approx (k^n, q')$, where

$$q'(x_1,\dots,x_n) = c_1x_1^2 + \cdots + c_nx_n^2, \quad c_i = q(e_i) \in k.$$

If every element of $k$ is a square, for example, if $k = \overline{k}$, we can even scale the $e_i$ so that each $c_i$ is 0 or 1.

**Theorems of Witt and Cartan-Dieudonné**

A quadratic space $(V,q)$ is said to be ***regular***[25] (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
- ◇ ***anistropic*** 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 $a \in V$,

$$\langle a\rangle^{\perp} \stackrel{\text{df}}{=} \{x \in V \mid \phi(a,x) = 0\}$$

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 $W = \langle a\rangle^{\perp}$. Moreover,

$$q(R_a(x)) = q(x) - 4\frac{2\phi(a,x)}{q(a)}\phi(a,x) + \frac{4\phi(a,x)^2}{q(a)^2}q(a) = q(x),$$

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 $\operatorname{diag}(-1,1,\dots,1)$, and so $\det(R_a) = -1$.

THEOREM 5.2 *Let $(V,q)$ be a regular quadratic space, and let $\sigma$ be an isometry from a subspace $W$ of $V$ into $V$. Then there exists a composite of reflections $V \to V$ extending $\sigma$.*

PROOF. Suppose first that $W = \langle x\rangle$ with $x$ anisotropic, and let $\sigma x = y$. Geometry in the plane suggests we should reflect in the line $x + y$, which is the line orthogonal to $x - y$. In fact, if $x - y$ is anistropic,

$$R_{x-y}(x) = y$$

as required. To see this, note that

$$\phi(x-y,x) = -\phi(x-y,y)$$

because $q(x) = q(y)$, and so

$$\phi(x-y,x-y) = 2\phi(x-y,x),$$

which shows that

$$R_{x-y}(x) = x - \frac{2\phi(x-y,x)}{\phi(x-y,x-y)}(x-y) = x - (x-y) = y.$$

If $x - y$ is isotropic, then

$$4q(x) = q(x+y) + q(x-y) = q(x+y)$$

and so $x + y$ is anistropic. In this case,

$$R_{x+y} \circ R_x(x) = R_{x-(-y)}(-x) = y.$$

[25] With the notations of the last paragraph, $(V,q)$ is regular if $c_1 \dots c_n \neq 0$.

We now proceed[26] by induction on

$$m(W) = \dim W + 2\dim(W \cap W^\perp).$$

CASE $W$ NOT TOTALLY ISOTROPIC: As in the proof of (5.1), 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 $\Sigma'$ of reflections such that $\Sigma'|W' = \sigma|W'$. From the definition of $W'$, $x \in W'^\perp$; moreover, for any $w' \in W'$,

$$\phi(\Sigma'^{-1}\sigma x, w') = \phi(x, \sigma^{-1}\Sigma' w') = \phi(x, w') = 0,$$

and so $y \overset{\text{df}}{=} \Sigma'^{-1}\sigma x \in W'^\perp$. By the argument in the first paragraph, there exists reflections (one or two) of the form $R_z$, $z \in W'^\perp$, whose composite $\Sigma''$ maps $x$ to $y$. Because $\Sigma''$ 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 $V^\vee = \mathrm{Hom}_{k\text{-lin}}(V, k)$ be the dual vector space, and consider the surjective map

$$\alpha\colon V \xrightarrow{x \mapsto \phi(x,-)} V^\vee \xrightarrow{f \mapsto f|W} W^\vee$$

(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

$$x + x' \mapsto (x, \alpha(x'))\colon W + W' \to W \oplus W^\vee \tag{27}$$

is an isometry.

The same argument applied to $\sigma W$ gives a subspace $W''$ and an isometry

$$x + x'' \mapsto (x, \ldots)\colon \sigma W + W'' \to \sigma W \oplus (\sigma W)^\vee. \tag{28}$$

Now the map

$$W + W' \xrightarrow{(27)} W \oplus W^\vee \xrightarrow{\sigma \oplus \sigma^{\vee -1}} \sigma W \oplus (\sigma W)^\vee \xrightarrow{(28)} \sigma W + W'' \subset V$$

is an isometry extending $\sigma$. As

$$m(W \oplus W') = 2\dim W < 3\dim W = m(W)$$

we can apply induction to complete the proof. □

[26] Following W. Scharlau, Quadratic and Hermitian Forms, 1985, Chapter 1, 5.5.

COROLLARY 5.3 *Every isometry of $(V,q)$ is a composite of reflections.*

PROOF. This is the special case of the theorem in which $W = V$. □

COROLLARY 5.4 (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 $V_1 \to V_1' \subset V$ to an isometry of $V$. It will map $V_2 = V_1^{\perp}$ isometrically onto $V_2' = V_1'^{\perp}$. □

COROLLARY 5.5 *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 $\dim W_1 \le \dim W_2$. Then there exists an injective linear map $\sigma\colon W_1 \to W_2 \subset V$, which is automatically an isometry. Therefore, by Theorem 5.2 it extends to an isometry $\sigma\colon V \to V$. 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 $\dim W_1 = \dim \sigma^{-1}W_2 = \dim W_2$. □

REMARK 5.6 In the situation of Theorem 5.2, Witt's theorem says simply that there exists an isometry extending $\sigma$ 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 5.2 shows this, but the general case is considerably more difficult — see E Artin, Geometric Algebra, 1957.

DEFINITION 5.7 The ***(Witt) index*** of a regular quadratic space $(V,q)$ is the maximum dimension of a totally isotropic subspace of $V$.

DEFINITION 5.8 A ***hyperbolic plane*** is a regular isotropic quadratic space $(V,q)$ of dimension 2.

Equivalent conditions: for some basis, the matrix of the form is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; the discriminant of $(V,q)$ is $-1$ (modulo squares).

THEOREM 5.9 (WITT DECOMPOSITION) *A regular quadratic space $(V,q)$ with Witt index $m$ has an orthogonal decomposition*

$$V = H_1 \oplus \cdots \oplus H_m \oplus V_a \tag{29}$$

*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 $\phi(e_i,e_{m+j}) = \delta_{i,j}$ (Kronecker delta) and $q(e_{m+i}) = 0$ for $i \le m$. Then $V$ decomposes as (29) with[27] $H_i = \langle e_i, e_{m+i}\rangle$ and $V_a = \langle e_1,\dots,e_{2m}\rangle^{\perp}$. The uniqueness of $V_a$ follows from Witt cancellation (5.4). □

[27] We often write $\langle S\rangle$ for the $k$-space spanned by a subset $S$ of a vector space $V$.

## 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 $\mathrm{GL}_V$ (see 2.6), called the ***orthogonal group*** of $q$ (it is also called the orthogonal group of $\phi$, 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 $\mathrm{SL}_V$, called the ***special orthogonal group*** $\mathrm{SO}(q)$.

## Super algebras

A ***super*** (or ***graded***) $k$-***algebra*** is $k$-algebra $C$ together with a decomposition $C = C_0 \oplus C_1$ of $C$ as a $k$-vector space such that

$$k \subset C_0, \quad C_0C_0 \subset C_0, \quad C_0C_1 \subset C_1, \quad C_1C_0 \subset C_1, \quad C_1C_1 \subset C_0.$$

Note that $C_0$ is a $k$-subalgebra of $C$. A ***homomorphism*** of super $k$-algebras is a homomorphism $\varphi: C \to D$ of algebras such that $\varphi(C_i) \subset D_i$ for $i = 0, 1$.

EXAMPLE 5.10 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

$$e_i^2 = c_i, \quad e_j e_i = -e_i e_j \ (i \neq j).$$

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 $2^n$. With $C_0$ and $C_1$ equal to the subspaces

$$C_0 = \langle e_1^{i_1} \dots e_n^{i_n} \mid i_1 + \cdots + i_n \text{ even} \rangle$$
$$C_1 = \langle e_1^{i_1} \dots e_n^{i_n} \mid i_1 + \cdots + i_n \text{ odd} \rangle,$$

$C(c_1, \dots, c_n)$ 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 $D$, $C \widehat{\otimes} D$, is $C \otimes_k D$ as a vector space, but

$$\left(C \widehat{\otimes} D\right)_0 = (C_0 \otimes D_0) \oplus (C_1 \otimes D_1)$$
$$\left(C \widehat{\otimes} D\right)_1 = (C_0 \otimes D_1) \oplus (C_1 \otimes D_0)$$
$$(c_i \otimes d_j)(c'_k \otimes d'_l) = (-1)^{jk}(c_i c'_k \otimes d_j d'_l) \quad c_i \in C_i, d_j \in D_j \text{ etc..}$$

The maps

$$i_C: C \to C \widehat{\otimes} D, \quad c \mapsto c \otimes 1$$
$$i_D: D \to C \widehat{\otimes} D, \quad d \mapsto 1 \otimes d$$

have the following universal property: for any homomorphisms of $k$-superalgebras

$$f: C \to T, \quad g: D \to T$$

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 homomorphism $h: C\widehat{\otimes}D \to T$ such that $f = h \circ i_C$, $g = h \circ i_D$.

EXAMPLE 5.11 As a $k$-vector space, $C(c_1)\widehat{\otimes}C(c_2)$ has basis $1 \otimes 1$ $(= 1_{C(c_1)\widehat{\otimes}C(c_2)})$, $e \otimes 1$, $1 \otimes e$, $e \otimes e$, and

$$(e \otimes 1)^2 = e^2 \otimes 1 = c_1$$
$$(1 \otimes e)^2 = 1 \otimes e^2 = c_2$$
$$(e \otimes 1)(1 \otimes e) = e \otimes e = -(1 \otimes e)(e \otimes 1).$$

Therefore,

$$C(c_1)\widehat{\otimes}C(c_2) \simeq C(c_1, c_2)$$
$$e \otimes 1 \leftrightarrow e_1$$
$$1 \otimes e \leftrightarrow e_2.$$

Similarly,

$$C(c_1, \dots, c_{i-1})\widehat{\otimes}C(c_i) \simeq C(c_1, \dots, c_i),$$

and so, by induction,

$$C(c_1)\widehat{\otimes}\cdots\widehat{\otimes}C(c_n) \simeq C(c_1, \dots, c_n).$$

EXAMPLE 5.12 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 $A \otimes_k B = A\widehat{\otimes}_k B$.

EXAMPLE 5.13 Let $X$ be a manifold. Then $H(X) =_{\text{df}} \bigoplus_i H^i(X, \mathbb{R})$ 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

$$H(X \times Y) = H(X)\widehat{\otimes}H(Y)$$

(super tensor product).

## Brief review of the tensor algebra

Let $V$ be a $k$-vector space. The ***tensor algebra*** of $V$ is $TV = \bigoplus_{n\geq 0} V^{\otimes n}$, where

$$V^{\otimes 0} = k,$$
$$V^{\otimes 1} = V,$$
$$V^{\otimes n} = V \otimes_k \cdots \otimes_k V \ (n \text{ copies of } V)$$

with the algebra structure defined by juxtaposition, i.e.,

$$(v_1 \otimes \cdots \otimes v_m) \cdot (v_{m+1} \otimes \cdots \otimes v_{m+n}) = v_1 \otimes \cdots \otimes v_{m+n}.$$

It is a $k$-algebra.

If $V$ has a basis $e_1, \dots, e_m$, then $TV$ is the $k$-algebra of noncommuting polynomials in $e_1, \dots, e_m$.

There is a $k$-linear map $V \to TV$, 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 $TV \to R$.

## The Clifford algebra

Let $(V,q)$ be a quadratic space, and let $\phi$ be the corresponding bilinear form on $V$.

DEFINITION 5.14 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 $\rho\colon V\to C(V,q)$ be the composite of the canonical map $V\to T(V)$ and the quotient map $T(V)\to C(V,q)$. Then $\rho$ is $k$-linear, and[28]

$$\rho(x)^2 = q(x), \text{ all } x\in V. \tag{30}$$

Note that if $x$ is anisotropic in $V$ then $\rho(x)$ is invertible in $C(V,q)$, because (30) shows that

$$\rho(x)\cdot\frac{\rho(x)}{q(x)} = 1.$$

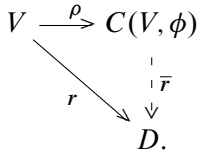
EXAMPLE 5.15 If $V$ is one-dimensional with basis $e$ and $q(e) = c$, then $T(V)$ is a polynomial algebra in one symbol $e$, $T(V) = k[e]$, and $I(q) = (e^2 - c)$. Therefore, $C(V,q)\approx C(c)$.

EXAMPLE 5.16 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 5.17 *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 $\overline{r}\colon C(V,q)\to D$ such that $\overline{r}\circ\rho = r$:*




PROOF. By the universal property of the tensor algebra, $r$ extends uniquely to a homomorphism of $k$-algebras $r'\colon T(V)\to D$, 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.

[28] More careful authors define a $k$-algebra to be a ring $R$ together with a homomorphism $k\to R$ (instead of containing $k$), and so write (30) as

$$\rho(x)^2 = q(x)\cdot 1_{C(V,q)}.$$

**The map $C(c_1,\dots,c_n) \to C(V,q)$**

Because $\rho$ 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

$$\rho(x+y)^2 \overset{(30)}{=} q(x+y) = q(x) + q(y) + 2\phi(x,y),$$

we find that

$$\rho(x)\rho(y) + \rho(y)\rho(x) = 2\phi(x,y). \tag{31}$$

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

$$e_i \mapsto \rho(f_i)\colon C(c_1,\dots,c_n) \to C(V,\phi). \tag{32}$$

**The grading (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

$$\begin{array}{ccccc} V & = & V_1 \oplus V_2 & \xrightarrow{r} & C(V_1,q_1)\widehat{\otimes}C(V_2,q_2) \\ x & = & (x_1,x_2) & \mapsto & \rho_1(x_1)\otimes 1 + 1 \otimes \rho_2(x_2). \end{array}$$

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

$$(\rho(x_1) \otimes 1)(1 \otimes \rho(x_2)) = \rho(x_1) \otimes \rho(x_2) = -(1 \otimes \rho(x_2))(\rho(x_1) \otimes 1)).$$

Therefore, it factors uniquely through $C(V, q)$:

$$C(V, q) \to C(V_1, q_1) \widehat{\otimes} C(V_2, q_2). \tag{33}$$

**Explicit description of the Clifford algebra**

THEOREM 5.18 *Let $(V, q)$ a quadratic space of dimension $n$.*

(a) *For every orthogonal basis for $(V, q)$, the homomorphism (32)*

$$C(c_1, \dots, c_n) \to C(V, q)$$

*is an isomorphism.*

(b) *For every orthogonal decomposition $(V, q) = (V_1, q_1) \oplus (V_2, q_2)$, the homomorphism (33)*

$$C(V, q) \to C(V_1, q_1) \widehat{\otimes} C(V_2, q_2)$$

*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 (5.15). 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 (33) is surjective because its image contains $\rho_1(V_1) \otimes 1$ and $1 \otimes \rho_2(V_2)$, which generate $C(V_1, q_1) \widehat{\otimes} C(V_2, q_2)$, 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 (33). Therefore,

$$\dim(C(V, q)) \leq 2^n.$$

It follows that $\dim(C(V, q)) = 2^n$. By comparing dimensions, we deduce that the homomorphism (32) and (33) are isomorphisms. □

COROLLARY 5.19 *The map $\rho\colon V \to C(V, q)$ is injective.*

From now on, we shall regard $V$ as a subset of $C(V, q)$ (i.e., we shall omit $\rho$).

REMARK 5.20 Let $L$ be a field containing $k$. Then $\phi$ extends uniquely to an $L$-bilinear form

$$\phi'\colon V' \times V' \to L, \quad V' = L \otimes_k V,$$

and

$$C(V', \phi') \simeq L \otimes_k C(V, \phi).$$

### 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

$$\Delta = (-1)^{\frac{n(n-1)}{2}} c_1\cdots c_n = (-1)^{\frac{n(n-1)}{2}} \det(\phi).$$

We saw in (5.18) 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 5.21 *(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, $C_0 \cap \mathrm{Centre}(C(q)) = k$.*

*(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 $e_ie_j$). □

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 $\Delta$, and, if $\Delta$ 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 $*\colon D\to D$ such that $(ab)^* = b^*a^*$ and $a^{**} = 1$. For example, $M \mapsto M^t$ (transpose) is an involution of $M_n(k)$.

Let $C(V,q)^{\mathrm{opp}}$ be the ***opposite*** $k$-algebra to $C(V,q)$, i.e., $C(V,q)^{\mathrm{opp}} = C(V,q)$ as a $k$-vector space but

$$ab \text{ in } C(V,q)^{\mathrm{opp}} = ba \text{ in } C(V,q).$$

The map $\rho\colon V\to C(V,q)^{\mathrm{opp}}$ is $k$-linear and has the property that $\rho(x)^2 = q(x)$. Thus, there exists an isomorphism $*\colon C(V,q)\to C(V,q)^{\mathrm{opp}}$ 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 $x\in V$, $x^*x = q(x)$.

## The Spin group

Initially we define the spin group as an abstract group.

DEFINITION 5.22 The group $\mathrm{Spin}(q)$ consists of the elements $t$ of $C_0(V,q)$ such that
(a) $t^*t = 1$,
(b) $tVt^{-1} = V$,
(c) the map $x \mapsto txt^{-1}: V \to V$ has determinant 1.

REMARK 5.23 (a) The condition (a) implies that $t$ is invertible in $C_0(V,q)$, and so (b) makes sense.

(b) We shall see in (5.27) below that the condition (c) is implied by (a) and (b).

### The map $\mathrm{Spin}(q) \to \mathrm{SO}(q)$

Let $t$ be an invertible element of $C(V,q)$ such that $tVt^{-1} = V$. Then the mapping $x \mapsto txt^{-1}: V \to V$ is an isometry, because

$$q(txt^{-1}) = (txt^{-1})^2 = tx^2t^{-1} = tq(x)t^{-1} = q(x).$$

Therefore, an element $t \in \mathrm{Spin}(q)$ defines an element $x \mapsto txt^{-1}$ of $\mathrm{SO}(q)$.

THEOREM 5.24 *The homomorphism*

$$\mathrm{Spin}(q) \to \mathrm{SO}(q)$$

*just defined has kernel of order* 2, *and it is surjective if* $k$ *is algebraically closed.*

PROOF. The kernel consists of those $t \in \mathrm{Spin}(\phi)$ such that $txt^{-1} = x$ for all $x \in V$. As $V$ generates $C$, such a $t$ must lie in the centre of $C$. 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 5.2, each element $\sigma$ of $\mathrm{SO}(q)$ 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 $\mathrm{SO}(q)$ is generated by elements $R_aR_b$ 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

$$\begin{aligned} axa^{-1} &= (-xa + 2\phi(a,x))\,a^{-1} && \text{as } (ax + xa = 2\phi(a,x), \text{ see (31)}) \\ &= -\left(x - \frac{2\phi(a,x)}{q(a)}a\right) && \text{as } a^2 = q(a) \\ &= -R_a(x). \end{aligned}$$

Moreover,

$$(ab)^*ab = baab = q(a)q(b).$$

Therefore, if $q(a)q(b) = 1$, then $R_aR_b$ is in the image of $\mathrm{Spin}(q) \to \mathrm{SO}(q)$. As we noted above, such elements generate SO when $k$ is algebraically closed. □

In general, the homomorphism is not surjective. For example, if $k = \mathbb{R}$, then $\mathrm{Spin}(q)$ is connected but $\mathrm{SO}(q)$ will have two connected components when $\phi$ is indefinite. In this case, the image is the identity component of $\mathrm{SO}(q)$.

## The Clifford group

Write $\gamma$ 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 5.25 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 $x \mapsto \gamma(t)xt^{-1}: V \to V$.

PROPOSITION 5.26 *For all $t \in \Gamma(q)$, $\alpha(t)$ is an isometry of $V$, and the sequence*

$$1 \to k^\times \to \Gamma(q) \xrightarrow{\alpha} O(q) \to 1$$

*is exact (no condition on $k$).*

PROOF. Let $t \in \Gamma(q)$. On applying $\gamma$ and $*$ to $\gamma(t)V = Vt$, we find that $\gamma(t^*)V = Vt^*$, and so $t^* \in \Gamma(q)$. Now, because $*$ and $\gamma$ 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

$$\gamma(t^*)\gamma(t)x = xt^*t. \tag{34}$$

We use this to prove that $\alpha(t)$ is an isometry:

$$q(\alpha(t)(x)) = (\alpha(t)(x))^*\cdot(\alpha(t)(x)) = t^{*-1}x\gamma(t)^*\cdot\gamma(t)xt^{-1} \overset{(34)}{=} t^{*-1}xxt^*tt^{-1} = q(x).$$

As $k$ is in the centre of $\Gamma(q)$, $k^\times$ is in the kernel of $\alpha$. 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 $k$ (5.21a), and that $t_1$ centralizes $C_0$, and hence is zero (5.21b). We have shown that

$$\mathrm{Ker}(\alpha) = k^\times.$$

It remains to show that $\alpha$ is surjective. For $t \in V$, $\alpha(t)(y) = -tyt^{-1}$ and so (see the proof of (5.24)), $\alpha(t) = R_t$. Therefore the surjectivity follows from Theorem 5.2. □

COROLLARY 5.27 *For an invertible element $t$ of $C_0(V,q)$ such that $tVt^{-1} = V$, the determinant of $x \mapsto txt^{-1}: V \to V$ 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 $\det(t) = 1$. □

Hence, the condition (c) in the definition of $\mathrm{Spin}(q)$ is superfluous.

### Action of $O(q)$ on $\mathrm{Spin}(q)$

5.28 An element $\sigma$ of $O(q)$ defines an automorphism of $C(V,q)$ as follows. Consider $\rho\circ\sigma: V \to C(\phi)$. 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 $\tilde{\sigma}: C \to C$ rendering

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\tilde{\sigma}} \\ V & \xrightarrow{\rho} & C \end{array}$$

commutative. Clearly $\widetilde{\sigma_1\circ\sigma_2} = \widetilde{\sigma_1}\circ\widetilde{\sigma_2}$ and $\widetilde{\mathrm{id}} = \mathrm{id}$, 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 $C(\phi)$ by an invertible element of $C^+(\phi)$.

### 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 (5.20), $C(q_K) = K\otimes_k C(q)$.

THEOREM 5.29 *There exists a naturally defined algebraic group $\underline{\mathrm{Spin}}(q)$ over $k$ such that*

$$\underline{\mathrm{Spin}}(q)(K) \simeq \mathrm{Spin}(q_K)$$

*for all fields $K$ containing $k$. Moreover, there is a homomorphism of algebraic groups*

$$\underline{\mathrm{Spin}}(q) \to \mathrm{SO}(q)$$

*giving the homomorphism in (5.24) for each field $K$ containing $k$. Finally, the action of $O(q)$ on $C(V,q)$ described in (5.24) defines an action of $O(q)$ on $\underline{\mathrm{Spin}}(q)$.*

PROOF. Omitted for the present (it is not difficult). □

In future, we shall write $\mathrm{Spin}(q)$ for the algebraic group $\underline{\mathrm{Spin}}(q)$.

NOTES 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 adoped 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.

# 6 Group Theory

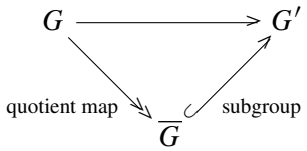
## Review of group theory

For a group $G$, we have the notions of
- ◇ a subgroup $H$,
- ◇ a normal subgroup $N$,
- ◇ a quotient map $G \to Q$ (surjective homomorphism).

There are the following basic results (see for example my course notes Group Theory §1,3).

6.1 (Existence of quotients). The kernel of a quotient map $G \to Q$ is a normal subgroup of $G$, and every normal subgroup arises as the kernel of a quotient map.

6.2 (Factorization theorem). Every homomorphism $G \to G'$ factors into




6.3 (Isomorphism theorem). Let $H$ be a subgroup of $G$ and $N$ a normal subgroup of $G$; then $HN$ is a subgroup of $G$, $H \cap N$ is a normal subgroup of $H$, and the map

$$h(H \cap N) \mapsto hN\colon H/H \cap N \to HN/H$$

is an isomorphism.

In this section, we shall see that, appropriately interpreted, all these statements hold for algebraic groups. The proofs involve only basic commutative algebra.

## Review of flatness

Let $R \to S$ be a homomorphism of rings. If the sequence of $R$-modules

$$0 \to M' \to M \to M'' \to 0 \tag{35}$$

is exact, then the sequence of $S$-modules

$$S \otimes_R M' \to S \otimes_R M \to S \otimes_R M'' \to 0$$

is exact, but $S \otimes_R M' \to S \otimes_R M$ need not be injective. For example, when we tensor the exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

with $\mathbb{Z}/2\mathbb{Z}$, we get the sequence

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{2=0} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Moreover, if the $R$-module $M$ is nonzero, then the $S$-module $N$ need not be nonzero. For example,

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$$

because it is killed by both 2 and 3.

DEFINITION 6.4 A homomorphism of rings $R \to S$ is ***flat*** (and $S$ is a ***flat*** $R$-algebra) if

$$M \to N \text{ injective } \implies S \otimes_R M \to S \otimes_R N \text{ is injective.}$$

It is ***faithfully flat*** if, in addition,

$$S \otimes_R M = 0 \implies M = 0.$$

Thus, if $R \to S$ is flat if and only if $S \otimes_R -$ is an exact functor, i.e.,

$$0 \to S \otimes_R M' \to S \otimes_R M \to S \otimes_R M'' \to 0 \tag{36}$$

is exact whenever (35) is exact.

PROPOSITION 6.5 *A homomorphism $k \to R$ with $k$ a field is always flat, and it is faithfully flat if and only if $R$ is nonzero.*

PROOF. For an injective map $M \to N$ of $k$-vector spaces, there exists a $k$-linear map $N \to M$ such that the composite $M \to N \to M$ is $\mathrm{id}_M$. On tensoring with $R$, we get $R$-linear maps $R \otimes_k M \to R \otimes_k N \to R \otimes_k M$ whose composite is $\mathrm{id}_{R\otimes_k M}$, which shows that the first map is injective. Similarly, if $R \neq 0$, then there exists a $k$-linear map $R \to k$ such that composite $k \to R \to k$ is $\mathrm{id}_k$. On tensoring with $M \neq 0$ we get $R$-linear maps $M \to R \otimes_k M \to M$ whose composite is $\mathrm{id}_M$, which shows that $R \otimes_k M \neq 0$. □

PROPOSITION 6.6 *Let $i: R \to S$ be faithfully flat.*

*(a) A sequence (35) is exact if and only if (36) is exact.*

*(b) Let $M$ be an $R$-module. The map $m \mapsto 1 \otimes m: M \to S \otimes_R M$ is injective, and its image consists of the elements of $S \otimes_R M$ on which the two maps $S \otimes_R M \to S \otimes_R S \otimes_R M$*

$$s \otimes m \mapsto 1 \otimes s \otimes m$$
$$s \otimes m \mapsto s \otimes 1 \otimes m$$

*coincide.*

PROOF. (a) We have to show that (35) is exact if (36) is exact. Let $N$ be the kernel of $M' \to M$. Then, because $R \to S$ is flat, $S \otimes_R N$ is the kernel of $S \otimes_R M' \to S \otimes_R M$, which is zero by assumption. Because $R \to S$ is *faithfully* flat, this implies that $N = 0$. This proves the exactness at $M'$, and the proof of exactness elsewhere is similar.

(b) We have to show that the sequence

$$0 \to M \xrightarrow{d_0} S \otimes_R M \xrightarrow{d_1} S \otimes_R S \otimes_R M \qquad (*)$$
$$d_0(m) = 1 \otimes m,$$
$$d_1(s \otimes m) = 1 \otimes s \otimes m - s \otimes 1 \otimes m$$

is exact.

Assume first that there exists an $R$-linear section to $R \to S$, i.e., a $R$-linear map $f: S \to R$ such that $f \circ i = \mathrm{id}_R$, and define

$$k_0: S \otimes_R M \to M, \qquad k_0(s \otimes m) = f(s)m$$
$$k_1: S \otimes_R S \otimes_R M \to S \otimes_R M, \qquad k_1(s \otimes s' \otimes m) = f(s)s' \otimes m.$$

Then $k_0 d_0 = \mathrm{id}_M$, which shows that $d_0$ is injective. Moreover,

$$k_1 \circ d_1 + d_0 \circ k_0 = \mathrm{id}_{S \otimes_R M}$$

which shows that if $d_1(x) = 0$ then $x = d_0(k_0(x))$, as required.

We now consider the general case. Because $R \to S$ is faithfully flat, it suffices to prove that (*) becomes exact after tensoring in $S$. But the sequence obtained from (*) by tensoring with $S$ can be shown to be isomorphic to the sequence (*) for the homomorphism of rings $s \mapsto 1 \otimes s \colon S \to S \otimes_R S$ and the $S$-module $S \otimes_R M$. Now $S \to S \otimes_R S$ has an $S$-linear section, namely, $f(s \otimes s') = ss'$, and so we can apply the first part. □

COROLLARY 6.7 *If $R \to S$ is faithfully flat, then it is injective with image the set of elements on which the maps $S \to S \otimes_R S$*

$$s \mapsto 1 \otimes s, \quad s \mapsto s \otimes 1$$

*coincide.*

PROOF. This is the special case $M = R$ of the Proposition. □

PROPOSITION 6.8 *Let $R \to R'$ be a homomorphism of rings. If $R \to S$ is flat (or faithfully flat), so also is $R' \to S \otimes_R R'$.*

PROOF. For any $R'$-module,

$$S \otimes_R R' \otimes_{R'} M \simeq S \otimes_R M,$$

from which the statement follows. □

## The faithful flatness of bialgebras

THEOREM 6.9 *Let $A \subset B$ be $k$-bialgebras for some field $k$ (inclusion respecting the bialgebra structure). Then $B$ is faithfully flat over $A$.*

PROOF. See Waterhouse 1979, Chapter 14. [Let $A \subset B$ be finitely generated $k$-algebras with $A$ an integral domain. Then "generic faithful flatness" says that for some nonzero elements $a$ of $A$ and $b$ of $B$, the map $A_a \to B_b$ is faithfully flat (ibid. 13.4). Here $A_a$ and $B_b$ denote the rings of fractions in which $a$ and $b$ have been inverted. Geometrically $A \subset B$ corresponds to a homomorphism $G \to H$, and geometrically "generic faithful flatness" says that when we replace $G$ and $H$ with open subsets, the map on the coordinate rings is faithfully flat. Now we can translate these open sets by elements of $G$ in order to get that the coordinate ring of the whole of $G$ is faithfully flat over $H$ (cf. da11b).] □

## Definitions; factorization theorem

DEFINITION 6.10 Let $H \to G$ be a homomorphism of algebraic groups with corresponding map of coordinate rings $k[G] \to k[H]$.

(a) If $k[G] \to k[H]$ is surjective, we call $H \to G$ an ***embedding*** (and we call $H$ and ***algebraic subgroup***[29] of $G$).

[29] In Waterhouse 1979, p13, these are called a *closed* embedding and a *closed* subgroup respectively.

(b) If $k[G] \to k[H]$ is injective, we call $H \to G$ a ***quotient map***.

THEOREM 6.11 *Every homomorphism of algebraic groups is the composite of a quotient map and an embedding.*

PROOF. The image $\alpha(A)$ of any homomorphism $\alpha: A \to B$ of $k$-bialgebras is a sub-bialgebra. Corresponding to the factorization $A \twoheadrightarrow \alpha(A) \hookrightarrow B$ of $\alpha$ into homomorphisms of bialgebras, we get a factorization into homomorphisms of algebraic groups. □

## Embeddings; subgroups.

Recall (3.7) that if $H \to G$ is an embedding, then $H(R) \to G(R)$ is injective for all $R$.

THEOREM 6.12 *A homomorphism $H \to G$ of algebraic groups is an embedding if and only if $H(R) \to G(R)$ is injective for all $k$-algebras $R$.*

PROOF. Assume $H(R) \to G(R)$ is injective for all $k$-algebras $R$. According to Theorem 6.11, $H \to G$ factors into $H \to \overline{H} \to G$ where $H \to \overline{H}$ is a quotient map and $\overline{H} \to G$ is an embedding. We have to show that $H \to \overline{H}$ is an isomorphism. This is the next lemma.□

LEMMA 6.13 *A quotient map $H \to G$ such that $H(R) \to G(R)$ is injective for all $R$ is an isomorphism.*

PROOF. The homomorphism $H \to G$ corresponds to an injective homomorphism $k[G] \to k[H]$ of bialgebras. The homomorphisms

$$x \mapsto x \otimes 1, 1 \otimes x: k[H] \to k[H] \otimes_{k[G]} k[H]$$

agree on $k[G]$, and so define elements of $H(k[H] \otimes_{k[G]} k[H])$ which map to the same element in $G(k[H] \otimes_{k[G]} k[H])$. Therefore they are equal. Because $k[H]$ is a faithfully flat $k[G]$-algebra (6.9), the subset of $k[H]$ on which the two maps agree is $k[G]$ (6.7). Therefore $k[G] = k[H]$, as required. □

## Kernels

Let $\alpha: H \to G$ be a homorphism of algebraic groups with corresponding map $k[G] \to k[H]$ of coordinate rings. The kernel of $\alpha$ is the functor $R \mapsto N(R)$ with

$$N(R) = \operatorname{Ker}(H(R) \xrightarrow{\alpha(R)} G(R))$$

for all $R$. Recall that the identity element in $G(R)$ is the map $\epsilon: k[G] \to k$. Therefore, $h: k[H] \to R$ lies in $N(R)$ if and only if its composite with $k[G] \to k[H]$ factors through $\epsilon$

$$\begin{array}{ccc} k[H] & \longleftarrow & k[G] \\ \downarrow & & \downarrow \epsilon \\ R & \longleftarrow\!\cdots & k \end{array}$$

Let $I_G$ be the kernel of $\epsilon: k[G] \to k$ (this is often called the ***augmentation ideal***), and let $I_G k[H]$ denote the ideal generated by its image in $k[H]$. Then the elements of $N(R)$ correspond to the homomorphisms $k[H]$ zero on $I_G k[H]$, i.e.,

$$N(R) = \operatorname{Hom}_{k\text{-alg}}(k[H]/I_G k[H], R).$$

We have proved:

PROPOSITION 6.14 *For any homomorphism $H \to G$ of algebraic group, there is an algebraic group $N$ (called the **kernel** of the homomorphism) such that*

$$N(R) = \operatorname{Ker}(H(R) \to G(R))$$

*for all $R$. It is represented by the $k$-bialgebra $k[H]/I_G k[H]$.*

Alternatively, note that the kernel of $\alpha$ is the fibred product of $H \to G \leftarrow \{1_G\}$, and so is an algebraic group with coordinate ring $k[H] \otimes_{k[G]} (k[G]/I_G) \simeq k[H]/I_G k[H]$ — see p15.

For example, consider the map $g \mapsto g^n: \mathbb{G}_m \to \mathbb{G}_m$. This corresponds to the map on bialgebras[30] $Y \mapsto X^n: k[Y, Y^{-1}] \to k[X, X^{-1}]$. The map $\epsilon: k[Y, Y^{-1}] \to k$ sends $f(Y)$ to $f(1)$, and so $I_{\mathbb{G}_m} = (Y - 1)$. Thus, the kernel is represented by the bialgebra $k[X, X^{-1}]/(X^n - 1)$. In this quotient, $k[x, x^{-1}]$, $x^n = 1$, and so $x^{-1} = x^{n-1}$. Thus, $k[x, x^{-1}] = k[x] \simeq k[X]/(X^n - 1)$.[31]

For example, consider the map $(a_{ij}) \mapsto \det(a_{ij}): \mathrm{GL}_n \to \mathbb{G}_m$. The map on $k$-algebras is[32]

$$X \mapsto \det(X_{ij}): k[X, X^{-1}] \to k[\dots, X_{ij}, \dots, \det(X_{ij})^{-1}].$$

The augmentation ideal $I_{\mathbb{G}_m} = (X - 1)$, so

$$k[\mathrm{SL}_n] = \frac{k[\dots, X_{ij}, \dots, \det(X_{ij})^{-1}]}{(\det(X_{ij}) - 1)} \simeq \frac{k[\dots, X_{ij}, \dots]}{(\det(X_{ij}) - 1)}.$$

PROPOSITION 6.15 *If $k$ has characteristic zero, a homomorphism $G \to H$ is an embedding if and only if $G(\bar{k}) \to H(\bar{k})$ is injective.*

PROOF. We have to show that the condition implies that $N = 1$. According to Theorem 2.31, the kernel $N$ of the homomorphism of a *smooth* algebraic group. This means that $\bar{k}[N] =_{\mathrm{df}} k[N] \otimes_k \bar{k}$ is a reduced $\bar{k}$-algebra, and so the next lemma shows that $\bar{k}[N] = \bar{k}$. □

LEMMA 6.16 *Let $k$ be an algebraically closed field, and let $A$ be a reduced finitely generated $k$-algebra. If there exists only one homomorphism of $k$-algebras $A \to k$, then $A = k$.*

PROOF. Write $A = k[X_1, \dots, X_n]/\mathfrak{a}$. Because $A$ is reduced, $\mathfrak{a} = \operatorname{rad}(\mathfrak{a}) = IV(\mathfrak{a})$ (in the terminology of §4). A point $(a_1, \dots, a_n)$ of $V(\mathfrak{a})$ defines a homomorphism $A \to k$, namely, $f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$. Since there is only one homomorphism, $V(\mathfrak{a})$ consists of a single point $(a_1, \dots, a_n)$ and $IV(\mathfrak{a}) = (X - a_1, \dots, X - a_n)$. Therefore $A = k[X_1, \dots, X_n]/(X - a_1, \dots, X - a_n) \simeq k$. □

EXAMPLE 6.17 Let $k$ be a field of characteristic $p \neq 0$, and consider the homomorphism $x \mapsto x^p: \mathbb{G}_a \to \mathbb{G}_a$. For any field $K$, $x \mapsto x^p: K \to K$ is injective, but $\mathbb{G}_a \to \mathbb{G}_a$ is not an embedding (it corresponds to the homomorphism of rings $X \mapsto X^p: k[X] \to k[X]$, which is not surjective).

[30] Check: let $r \in \mathbb{G}_m(R)$; then $Y(r^n) = r^n = X^n(r)$.

[31] More precisely, the map $k[X] \to k[X, X^{-1}]/(X^n - 1)$ defines a isomorphism $k[X]/(X^n - 1) \simeq k[X, X^{-1}]/(X^n - 1)$.

[32] Check: for $(a_{ij}) \in \mathrm{GL}_n(R)$, $X(\det(a_{ij})) = \det(a_{ij}) = \det(X_{ij})(a_{ij})$.

## Quotient maps

What should a quotient map be? One might first guess that it is a homomorphism $H \to G$ such that $H(R) \to G(R)$ is surjective for all $R$, but this is too stringent. For example, it would say that $x \mapsto x^n: \mathbb{G}_m \to \mathbb{G}_m$ is not a quotient map. But the cokernel functor, $R \mapsto R^\times/R^{\times n}$ is **not** representable because it fails the following obvious test: if $F$ is representable and $R \to R'$ is injective, then $F(R) \to F(R')$ is injective. In fact, any homomorphism of algebraic groups $\mathbb{G}_m \to G$ zero on the image of $x \mapsto x^n$ has zero image. This suggests that $x \mapsto x^n: \mathbb{G}_m \to \mathbb{G}_m$ should be a quotient map, and, according to our definition 6.10, it is: the map $X \mapsto X^n: k[X, X^{-1}] \to k[X, X^{-1}]$ is injective.

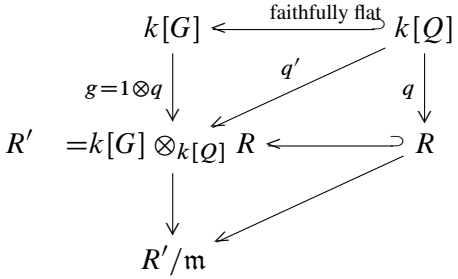
The next two theorems indicate that our definition of a quotient map is the correct one.

THEOREM 6.18 *(a) A homomorphism $G \to Q$ of algebraic groups is a quotient map if and only if, for every $k$-algebra $R$ and $q \in Q(R)$, there exists a finitely generated faithfully flat $R$-algebra $R'$ and a $g \in G(R')$ mapping to $q$ in $Q(R')$:*

$$\begin{array}{ccc} G(R') & \longrightarrow & Q(R') \\ \uparrow & & \uparrow \\ G(R) & \longrightarrow & Q(R) \end{array} \qquad \begin{array}{ccc} g & \longmapsto & * \\ & & \uparrow \\ & & q. \end{array}$$

*(b) If $G \to Q$ is a quotient map, then $G(\bar{k}) \to Q(\bar{k})$ is surjective; the converse is true if $Q$ is smooth.*

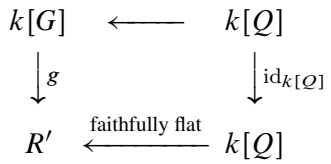
PROOF. $\Longrightarrow$ : Suppose $G \to Q$ is a quotient map, so that $k[Q] \to k[G]$ is injective (and hence faithfully flat (6.9)). Let $q \in Q(R) = \mathrm{Hom}_{k\text{-alg}}(k[Q], R)$, and form the tensor product $R' = k[G] \otimes_{k[Q]} R$:




The map $R \to R'$ is faithfully flat (6.8), and $R'$ is a finitely generated $R$-algebra because $k[G]$ is a finitely generated $k$-algebra. Because the upper square commutes, $g \in G(R')$ maps to the image $q'$ of $q$ in $Q(R')$.

Now suppose $R = k$. Let $\mathfrak{m}$ be a maximal ideal in $R'$. Then $R'/\mathfrak{m}$ is a field that is finitely generated as a $k$-algebra, and hence is a finite extension of $k$ (Zariski's Lemma AG 2.7). In particular, if $k$ is algebraically closed, then $k = R'/\mathfrak{m}$. The element of $G(k)$ given by the homomorphism $k[G] \to R'/\mathfrak{m} = k$ in the diagram maps to $q \in Q(k)$.

$\Longleftarrow$ : Let $q = \mathrm{id}_{k[Q]} \in Q(k[Q])$.Then, there exists a $g \in G(R')$ for some $R'$ faithfully flat over $k[Q]$ such that $g$ and $q$ map to the same element of $Q(R')$, i.e., such that



commutes. The map $k[Q] \to R'$, being faithfully flat, is injective (6.7), which shows that $k[Q] \to k[G]$ is injective (and $G \to Q$ is a quotient map).

Now suppose that $k$ is algebraically closed and $Q$ is smooth. In this case, we saw (4.8) that the homomorphism $k[Q] \to \mathrm{Map}(Q(k), k)$ is injective. If $G(k) \to Q(k)$ is surjective, then $\mathrm{Map}(Q(k), k) \to \mathrm{Map}(G(k), k)$ is injective, and so $k[Q] \to k[G]$ is injective. □

EXAMPLE 6.19 Let $k$ be a field of characteristic $p \neq 0$, and consider the homomorphism $1 \to \alpha_p$, where $\alpha_p$ is the algebraic group such that $\alpha_p(R) = \{r \in R \mid r^p = 0\}$. This homomorphism is not a quotient map — the map on coordinate rings is $k[X]/(X^p) \to k$ which is not injective — even though the map $1(\overline{k}) \to \alpha_p(\overline{k})$ is surjective.

THEOREM 6.20 *Let $G \to Q$ be a quotient map with kernel $N$. Then any homomorphism $G \to Q'$ sending $N$ to 1 factors uniquely through $Q$.*

PROOF. Note that, if $g, g'$ are elements in $G$ with the same image in $Q$, then $g^{-1}g' \in N$ and so maps to 1 in $Q(R)$. Therefore $g, g'$ have the same image in $G'$.

This shows that the composites of the homomorphisms

$$G \times_Q G \rightrightarrows G \to Q'$$

are equal. Therefore, the composites of the homomorphisms

$$k[G] \otimes_{k[Q]} k[G] \leftleftarrows k[G] \leftarrow k[Q']$$

are equal. Since the pair of maps coincides on $k[Q]$ (see 6.7), the map $k[Q'] \to k[G]$ factors through $k[Q] \hookrightarrow k[G]$; therefore $G \to Q'$ factors through $G \to Q$. □

COROLLARY 6.21 *If $\theta\colon H \to Q$ and $\theta'\colon H \to Q'$ are quotient maps with the same kernel, then there is a unique homomorphism $\alpha\colon Q \to Q'$ such that $\alpha \circ \theta = \theta'$, and $\alpha$ is an isomorphism.*

PROOF. Immediate consequence of the theorem. □

## Existence of quotients

An algebraic subgroup $N$ of $G$ is ***normal*** if $N(R)$ is a normal subgroup of $G(R)$ for all $k$-algebras $R$. Clearly, the kernel of any homomorphism is normal.

THEOREM 6.22 *Let $N$ be a normal subgroup of $G$. Then there exists a quotient map $G \to Q$ with kernel $N$.*

PROOF. Waterhouse 1979, Chapter 16. [The idea of the proof is to find, starting from Chevalley's theorem (3.13), a representation $G \to \mathrm{GL}(V)$ of $G$ and a subspace $W$ of $V$, stable under $G$, such that $N$, and only $N$, acts trivially on $W$. Then the homomorphism $G \to \mathrm{GL}_W$ has kernel $N$, and (according to 6.10) it factors into

$$G \twoheadrightarrow Q \hookrightarrow \mathrm{GL}_W .]$$

□

**Warning:** Let $G \to Q$ be the quotient map with kernel $N$. By definition

$$1 \to N(R) \to G(R) \to Q(R)$$

is exact for all $R$, but the map $G(R) \to Q(R)$ need not be surjective — all you can say is what is said by Theorem 6.18. In particular,

$$1 \to N(\overline{k}) \to G(\overline{k}) \to Q(\overline{k}) \to 1$$

*is* exact.

EXAMPLE 6.23 Let $\mathrm{PGL}_n$ be the quotient of $\mathrm{GL}_n$ by its centre, and let $\mathrm{PSL}_n$ be the quotient of $\mathrm{SL}_n$ by its centre:

$$\mathrm{PGL}_n = \mathrm{GL}_n/\mathbb{G}_m, \quad \mathrm{PSL}_n = \mathrm{SL}_n/\mu_n.$$

The homomorphism $\mathrm{SL}_n \to \mathrm{GL}_n \to \mathrm{PGL}_n$ defines a homomorphism

$$\mathrm{PSL}_n \to \mathrm{PGL}_n \tag{37}$$

(apply 6.20). Is this an isomorphism? Note that

$$\mathrm{SL}_n(k)/\mu_n(k) \to \mathrm{GL}_n(k)/\mathbb{G}_m(k) \tag{38}$$

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 (for example, such a matrix has determinant in $k^{\times n}$). Nevertheless, I claim that (37) is an isomorphism of algebraic groups. In characteristic zero, this follows from the fact that (38) is an isomorphism when $k = \overline{k}$ (apply 6.15 and 6.18b). In the general case, we have to apply (6.12) and (6.18a).

Let $q \neq 1 \in \mathrm{PSL}_n(R)$. For some faithfully flat $R$-algebra $R'$, there exists a $g \in \mathrm{SL}_n(R')$ mapping to $q$ in $\mathrm{PSL}_n(R')$. The image of $g$ in $\mathrm{GL}_n(R')$ is not in $\mathbb{G}_m(R')$ (because $q \neq 1$); therefore, the image of $g$ in $\mathrm{PGL}_n(R')$ is $\neq 1$, which implies that the image of $q$ in $\mathrm{PGL}(R)$ is $\neq 1$:

$$\begin{array}{ccc} \mathrm{PSL}_n(R') & \longrightarrow & \mathrm{PGL}_n(R') \\ \uparrow & & \uparrow \\ \mathrm{PSL}_n(R) & \longrightarrow & \mathrm{PGL}_n(R). \end{array}$$

We have shown that (37) is an embedding.

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 $q$. Let $a = \det(g)$, and let $R'' = R'[T]/(T^n - a)$. In $R''$, $a$ is an $n^{\text{th}}$ power $a = t^n$, and so $g = g_0 t$ with $\det(g_0) = 1$. Thus, 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 $\mathrm{PSL}_n(R'')$. As an $R'$-module, $R''$ is free of finite rank; hence it is a faithfully flat $R$-algebra, and we have shown that (37) is a quotient map.

## The isomorphism theorem

THEOREM 6.24 *Let $H$ be an algebraic subgroup of an algebraic group $G$, and let $N$ be a normal algebraic subgroup of $G$. Then:*

(a) *there exists an algebraic subgroup $HN$ of $G$ such that, 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 $R'$ (and $(HN)(\overline{k}) = H(\overline{k})N(\overline{k})$);*

(b) *there exists a normal algebraic subgroup $H \cap N$ of $H$ such that $(H \cap N)(R) = H(R) \cap N(R)$ for all $k$-algebras $R$;*

(c) *the natural map*

$$H/H \cap N \to HN/N \tag{39}$$

*is an isomorphism.*

PROOF. Omitted (for the present). (For (a), cf. Waterhouse 1979, Chapter 15, Exercise 6.) □

EXAMPLE 6.25 Let $G = \mathrm{GL}_n$, $H = \mathrm{SL}_n$, and $N = \mathbb{G}_m$ (scalar matrices in $G$). Then $N \cap H = \mu_n$ (obviously), $HN = \mathrm{GL}_n$ (by the arguments in 6.23), and (39) becomes the isomorphism

$$\mathrm{SL}_n /\mu_n \to \mathrm{GL}_n /\mathbb{G}_m.$$

REMARK 6.26 The category of commutative algebraic groups over a field is an abelian category (SGA3, $\mathrm{VI}_A$, 5.4).

NOTES As noted earlier, in much of the expository literature (e.g., Humphreys 1975, Borel 1991, Springer 1998), "algebraic group" means "smooth algebraic group". With this terminology, almost all the results in this section become false.[33] Fortunately, because of Theorem 2.31, this is only a problem in nonzero characteristic. The importance of allowing nilpotents was pointed out by Cartier[34] more than forty years ago, but, except for Gabriel and Demazure 1970 and Waterhouse 1979, this point-of-view has not been adopted in the expository literature.

[33]The situation is even worse, because these books use a terminology based on Weil's Foundations, which sometimes makes it difficult to understand their statements. For example, in Humphreys 1975, p218, one finds the following statement: "for a homomorphism $\varphi: G \to G'$ of $k$-groups, the kernel of $\varphi$ need not be defined over $k$." By this, he means the following: form the kernel $N$ of $\varphi_{\overline{k}}: G_{\overline{k}} \to G'_{\overline{k}}$ (in our sense); then $N_{\mathrm{red}}$ need not arise from a smooth algebraic group over $k$.

[34]Cartier P, Groupes algébriques et groupes formels, In *Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962)*, pp. 87–111, Librairie Universitaire Louvain.

# 7 Finite (étale) algebraic groups

All rings and $k$-algebras are commutative.

## Separable $k$-algebras

Let $A$ be a finite $k$-algebra (i.e., a $k$-algebra that is of finite dimension $[A:k]$ as a $k$-vector space). There are two reasons why $A \otimes_k \overline{k}$ may not be reduced (i.e., have nilpotents).

- $\diamond$ $A$ itself may not be reduced. For example, if $A = k[X]/(X^n)$, $n > 2$, then $A \otimes_k \overline{k} = \overline{k}[X]/(X^n)$ contains a nonzero element $x$, namely, the class of $X$, such that $x^n = 0$.
- $\diamond$ $A$ may be an inseparable field extension of $k$. For example, if $k$ has characteristic $p \neq 0$ and $a \in k$ is not a $p^{\text{th}}$ power, then $X^p - a$ is irreducible in $k[X]$ and $A = k[X]/(X^p - a) = k[x]$ is a field. However, $\overline{k}$ contains a (unique) element $\alpha$ such that $\alpha^p = a$, and

$$A \otimes_k \overline{k} = \overline{k}[X]/(X^p - a) = \overline{k}[X]/((X - \alpha)^p),$$

which contains a nonzero element $x - \alpha$ such that $(x - \alpha)^p = 0$.

On the other hand, if $A$ is a separable field extension of $k$, then $A \otimes_k \overline{k}$ is reduced. From the primitive element theorem (FT 5.1), $A = k[\alpha]$ for some $\alpha$ whose minimum polynomial $f(X)$ is separable, which means that

$$f(X) = \prod (X - \alpha_i), \quad \alpha_i \neq \alpha_j,$$

in $\overline{k}[X]$. By the Chinese remainder theorem (AG 1.1)

$$A \otimes_k \overline{k} \approx \overline{k}[X]/(f) \simeq \prod\nolimits_i \overline{k}[X]/(X - \alpha_i) \simeq \overline{k} \times \cdots \times \overline{k}.$$

Moreover, the maps $\alpha \mapsto \alpha_i$ are $[A:k]$ distinct $k$-algebra homomorphisms $K \to \overline{k}$.

PROPOSITION 7.1 *The following conditions on a finite $k$-algebra $A$ are equivalent:*

(a) *$A$ is a product of separable field extensions of $k$;*
(b) *$A \otimes_k \overline{k}$ is a product of copies of $\overline{k}$;*
(c) *there are $[A:k]$ distinct $k$-algebra homomorphisms $A \to \overline{k}$;*
(d) *$A \otimes_k \overline{k}$ is reduced.*

PROOF. We have seen that (a) implies the remaining statements. That each of (b) and (c) implies (a) is similarly straightforward. That (d) implies (a) requires a little more (see Waterhouse 1979, 6.2) [but we may not need it].

It remains to show that (d) implies (b). For this, we may assume that $k = \overline{k}$. For any finite set $S$ of maximal ideals in $A$, the Chinese remainder theorem (AG 1.1) says that the map $A \to \prod_{\mathfrak{m} \in S} A/\mathfrak{m}$ is surjective with kernel $\bigcap_{\mathfrak{m} \in S} \mathfrak{m}$. In particular, $\#S \leq [A:k]$, and so $A$ has only finitely many maximal ideals. For $S$ equal to the set of all maximal ideals in $A$, $\bigcap_{\mathfrak{m} \in S} \mathfrak{m} = 0$ by (2.18), and so $A \simeq \prod A/\mathfrak{m} \simeq \prod k$. □

DEFINITION 7.2 A finite $k$-algebra satisfying the equivalent conditions of the proposition is said to be ***separable***.

PROPOSITION 7.3 *Finite products, tensor products, and quotients of separable $k$-algebras are separable.*

PROOF. This is obvious from the condition (b). □

COROLLARY 7.4 *The composite of any finite set of separable subalgebras of a $k$-algebra is separable.*

PROOF. Let $A_i$ be separable subalgebras of $B$. Then $A_1 \cdots A_n$ is the image of the map

$$a_1 \otimes \cdots \otimes a_n \mapsto a_1 \cdots a_n \colon A_1 \otimes_k \cdots \otimes_k A_n \to B,$$

and so is separable. □

PROPOSITION 7.5 *Let $K$ be a field extension of $k$. If $A$ is separable over $k$, then $A \otimes_k K$ is separable over $K$.*

PROOF. Let $\overline{K}$ be an algebraic closure of $K$, and let $\overline{k}$ be the algebraic closure of $k$ in $\overline{K}$. Then

$$\begin{array}{ccc} K & \longrightarrow & \overline{K} \\ \uparrow & & \uparrow \\ k & \longrightarrow & \overline{k} \end{array}$$

is commutative, and so

$$(A \otimes_k K) \otimes_K \overline{K} \simeq \left(A \otimes_k \overline{k}\right) \otimes_{\overline{k}} \overline{K} \simeq (\overline{k} \times \cdots \times \overline{k}) \otimes_{\overline{k}} \overline{K} \simeq \overline{K} \times \cdots \times \overline{K}.$$ □

## Classification of separable $k$-algebras

Let $k^{\mathrm{sep}}$ be the composite of the separable subfields of $\overline{k}$. If $k$ is perfect, for example, of characteristic zero, then $k^{\mathrm{sep}} = \overline{k}$. Let $\Gamma$ be the group of $k$-automorphisms of $k^{\mathrm{sep}}$. For any subfield $K$ of $k^{\mathrm{sep}}$, finite and Galois of $k$, an easy Zorn's lemma argument shows that

$$\sigma \mapsto \sigma|K \colon \Gamma \to \mathrm{Gal}(K/k)$$

is surjective. Let $X$ be a finite set with an action[35] of $\Gamma$,

$$\Gamma \times X \to X.$$

We say that the action is[36] continuous if it factors through $\Gamma \to \mathrm{Gal}(K/k)$ for some subfield $K$ of $k^{\mathrm{sep}}$ finite and Galois over $k$.

For a separable $k$-algebra $A$, let

$$F(A) = \mathrm{Hom}_{k\text{-alg}}(A, \overline{k}) = \mathrm{Hom}_{k\text{-alg}}(A, k^{\mathrm{sep}}).$$

Then $\Gamma$ acts on $F(A)$ through its action on $k^{\mathrm{sep}}$:

$$(\sigma f)(a) = \sigma(f(a)), \quad \sigma \in \Gamma,\ f \in F(A), a \in A.$$

The images of all homomorphisms $A \to k^{\mathrm{sep}}$ will lie in some finite Galois extension of $k$, and so the action of $\Gamma$ on $F(A)$ is continuous.

[35]This means $1_\Gamma x = x$ and $(\sigma\tau)x = \sigma(\tau x)$ for all $\sigma, \tau \in \Gamma$ and $x \in X$, i.e., that $\Gamma \to \mathrm{Aut}(X)$ is a homomorphism.

[36]Equivalently, the action is continuous relative to the discrete topology on $X$ and the Krull topology on $\Gamma$ (FT §7).

THEOREM 7.6 *The map $A \mapsto F(A)$ is a contravariant equivalence from the category separable $k$-algebras to the category of finite sets with a continuous action of $\Gamma$.*

PROOF. This is mainly a restatement of the fundamental theorem of Galois theory (FT §3), and is left as an exercise (or see Waterhouse 1979, 6.3). □

Let $A = k[X]/(f(X)) = k[x]$. Then $A$ is separable if and only if $f(X)$ is separable, i.e., has distinct roots in $\overline{k}$. Assume this, and (for simplicity) that $f(X)$ is monic. A $k$-algebra homomorphism $A \to k^{\text{sep}}$ is determined by the image of $x$, which can be any root of $f$ in $k^{\text{sep}}$. Therefore, $F(A)$ can be identified with the set of roots of $f$. Suppose $F(A)$ decomposes into $r$ orbits under the action of $\Gamma$, and let $f_1, \dots, f_r$ be the monic polynomials whose roots are the orbits. Then each $f_i$ is stable under $\Gamma$, 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 $A = \prod_{1 \le i \le r} k[X]/(f_i(X))$ is the decomposition of $A$ into a product of fields.

## Etale algebraic groups

Recall that an algebraic group $G$ is said to be finite if $k[G]$ is finite-dimensional as a $k$-vector space. We say $G$ is ***étale*** if in addition $k[G]$ is separable.

REMARK 7.7 (a) When $k$ has characteristic zero, Theorem 2.31 says that *every* finite algebraic group is étale.

(b) Algebraic geometers will recognize that an algebraic group $G$ is étale if and only if the morphism of schemes $G \to \operatorname{Spec} k$ is étale.

According to Theorem 7.6, to give a separable $k$-algebra is to give a finite set with a continuous action of $\Gamma$. To give a bialgebra structure on a separable $k$-algebra is equivalent to giving a group structure on the set for which $\Gamma$ acts by group homomorphisms (cf. 4.4). As

$$\operatorname{Hom}_{k\text{-alg}}(k[G], k^{\text{sep}}) = G(k^{\text{sep}}),$$

we have the following theorem.

THEOREM 7.8 *The functor $G \mapsto G(k^{\text{sep}})$ is an equivalence from the category of étale algebraic groups over $k$ to the category of finite groups endowed with a continuous action of $\Gamma$.*

Let $K$ be a subfield of $k^{\text{sep}}$ containing $k$, and let $\Gamma'$ be the subgroup of $\Gamma$ consisting of the $\sigma$ fixing the elements of $K$. Then $K$ is the subfield of $k^{\text{sep}}$ of elements fixed by $\Gamma'$ (see FT 7.10), and it follows that $G(K)$ is the subgroup $G(k^{\text{sep}})$ of elements fixed by $\Gamma'$.

## Examples

The ***order*** of a finite algebraic group $G$ is defined to be $[k[G]:k]$. For an étale algebraic group $G$, it is the order of $G(\overline{k})$.

Since $\operatorname{Aut}(X) = 1$ when $X$ is a group of order 1 or 2, we see that over any field $k$, there is exactly one étale algebraic group of order 1 and one of order 2 (up to isomorphism).

Let $X$ be a group of order 3. Such a group is cyclic and $\operatorname{Aut}(X) = \mathbb{Z}/2\mathbb{Z}$. Therefore the étale algebraic groups of order 3 over $k$ correspond to homomorphisms $\Gamma \to \mathbb{Z}/2\mathbb{Z}$

factoring through $\mathrm{Gal}(K/k)$ for some finite Galois extension $K$ of $k$. A separable quadratic extension $K$ of $k$ defines such a homomorphism, namely,

$$\sigma \mapsto \sigma|K\colon \Gamma \to \mathrm{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$$

and all nontrivial such homomorphisms arise in this way (see FT §7). Thus, up to isomorphism, there is exactly one étale algebraic group $G^K$ of order 3 over $k$ for each separable quadratic extension $K$ of $k$, plus the constant group $G_0$. For $G_0$, $G_0(k)$ has order 3. For $G^K$, $G^K(k)$ has order 1 but $G^K(K)$ has order 3. There are infinitely many distinct quadratic extensions of $\mathbb{Q}$, for example, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, …, $\mathbb{Q}[\sqrt{p}]$, …. Since $\mu_3(\mathbb{Q}) = 1$ but $\mu_3(\mathbb{Q}[\sqrt[3]{1}]) = 3$, $\mu_3$ must be the group corresponding to $\mathbb{Q}[\sqrt[3]{1}]$.

**Exercise**

7-1 How many finite algebraic groups of orders $1, 2, 3, 4$ are there over $\mathbb{R}$ (up to isomorphism)?

# 8 The connected components of an algebraic group

Recall that a topological space $X$ is disconnected if it is a disjoint union of two nonempty open subsets; equivalently, if it contains a nonempty proper closed-open subset. Otherwise, it is connected. The maximal connected subspaces of $X$ are called the connected components of $X$, and $X$ is a disjoint union of them. Write $\pi_0(X)$ for the set of connected components of $X$ (for good spaces it is finite).

For a topological group $G$, $\pi_0(G)$ is again a group, and the kernel of $G \to \pi_0(G)$ is a normal connected subgroup $G^\circ$ of $G$, called the identity (connected) component of $G$. For example, $\mathrm{GL}_2(\mathbb{R})$ has two connected components, namely, the identity component consisting of the matrices with determinant $> 0$ and another component consisting of the matrices with determinant $< 0$.

## Some algebraic geometry

The ***max spectrum*** of a commutative ring $A$, $\operatorname{spm} A$, is the set of maximal ideals $\mathfrak{m}$ in $A$. For an ideal $\mathfrak{a}$ in $A$, let

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

Then $V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ and $V(\sum \mathfrak{a}_i) = \bigcap V(\mathfrak{a}_i)$, and so there is a topology on $\operatorname{spm} A$ (called the ***Zariski topology***) whose closed sets are exactly the $V(\mathfrak{a})$. For each $f \in A$, the set $D(f) = \{\mathfrak{m} \mid f \notin \mathfrak{m}\}$ is open, and these sets form a base for the topology.

EXAMPLE 8.1 Let $k = \overline{k}$, and let $A = k[X_1, \dots, X_n]/\mathfrak{c}$. For each point $\mathbf{a} = (a_1, \dots, a_n)$ in the zero-set of $\mathfrak{c}$, we get a homomorphism $A \to k$, $f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$, whose kernel is the maximal ideal

$$\mathfrak{m}_\mathbf{a} = (x_1 - a_1, \dots, x_n - a_n).$$

The Nullstellensatz implies that every maximal ideal $\mathfrak{m}$ of $A$ has a zero in the zero-set of $\mathfrak{c}$, and therefore is of this form. Thus, we have a one-to-one correspondence

$$\mathbf{a} \leftrightarrow \mathfrak{m}_\mathbf{a}$$

between the zero-set of $\mathfrak{c}$ and $\operatorname{spm} A$. Under this correspondence, the topologies correspond (cf. AG §3).

For the remainder of this subsection, $A$ is a finitely generated $k$-algebra.

PROPOSITION 8.2 *The space* $\operatorname{spm} A$ *is noetherian (i.e., has the ascending chain condition on open subsets; equivalently, has the descending chain condition on closed subsets).*

PROOF. A descending chain of closed subsets gives rise to an ascending chain of ideals in $A$, which terminates because $A$ is noetherian (Hilbert basis theorem; AG 2.2). □

PROPOSITION 8.3 *For any ideal* $\mathfrak{a}$ *in* $A$,

$$\bigcap \{\mathfrak{m} \mid \mathfrak{m} \text{ maximal}, \mathfrak{m} \supset \mathfrak{a}\} = \operatorname{rad}(\mathfrak{a}).$$

PROOF. When $\mathfrak{m}$ is maximal, $A/\mathfrak{m}$ is reduced, and so

$$\mathfrak{m} \supset \mathfrak{a} \implies \mathfrak{m} \supset \operatorname{rad}(\mathfrak{a}).$$

This shows that the left hand side contains the right, and the reverse inclusion follows from Proposition 2.18 applied to $A/\operatorname{rad}(\mathfrak{a})$. □

COROLLARY 8.4 *The intersection of all maximal ideals in $A$ is the nilradical $\mathfrak{N}$ of $A$ (ideal consisting of the nilpotent elements).*

PROOF. The nilradical is the radical of the ideal (0). □

Because all maximal ideals contain $\mathfrak{N}$,

$$\operatorname{spm} A \simeq \operatorname{spm} A/\mathfrak{N}. \tag{40}$$

Recall that a nonempty topological space is ***irreducible*** if it is not the union of two proper closed subsets.

PROPOSITION 8.5 *Let $A$ be reduced. Then $\operatorname{spm} A$ is irreducible if and only if $A$ is an integral domain.*

PROOF. $\implies$ : Suppose $fg = 0$ in $A$. For each maximal ideal $\mathfrak{m}$, either $f$ or $g$ is in $\mathfrak{m}$. Therefore, $\operatorname{spm} A = V(f) \cup V(g)$. Because $\operatorname{spm} A$ is irreducible, this means $\operatorname{spm} A$ equals $V(f)$ or $V(g)$. But if $\operatorname{spm} A = V(f)$, then $f = 0$ by (8.4).

$\impliedby$ : Suppose $\operatorname{spm} A = V(\mathfrak{a}) \cup V(\mathfrak{b})$. If $V(\mathfrak{a})$ and $V(\mathfrak{b})$ are proper sets, then there exist nonzero $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$. Then $fg \in \mathfrak{a} \cap \mathfrak{b} \subset \bigcap \mathfrak{m} = 0$, which is a contradiction. □

COROLLARY 8.6 *The space $\operatorname{spm} A$ is irreducible if and only if $A/\mathfrak{N}$ is an integral domain.*

PROOF. Apply (40). □

PROPOSITION 8.7 *Let $e_1, \dots, e_n$ be elements of $A$ such that*

$$e_i^2 = e_i \text{ all } i, \quad e_i e_j = 0 \text{ all } i \neq j, \quad e_1 + \cdots + e_n = 1. \tag{41}$$

*Then*

$$\operatorname{spm} A = D(e_1) \sqcup \ldots \sqcup D(e_n)$$

*is a decomposition of $\operatorname{spm} A$ into a disjoint union of open subsets. Conversely, every such decomposition arises from a family of idempotents satisfying (41).*

PROOF. Let $e_1, \dots, e_n$ satisfy (41). For a maximal ideal $\mathfrak{m}$, the map $A \to A/\mathfrak{m}$ must send exactly one of the $e_i$ to a nonzero element (cf. 2.14). This shows that $\operatorname{spm} A$ is a disjoint union of the $D(e_i)$, each of which is open.

For the converse, we take $n = 2$ to simplify the notation. Each of thhe open sets is also closed, and so $\operatorname{spm} A = V(\mathfrak{a}) \sqcup V(\mathfrak{b})$ for some ideals $\mathfrak{a}$ and $\mathfrak{b}$. Because the union is disjoint, no maximal 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 maximal ideals contain $ab$, which is therefore nilpotent, say $(ab)^m = 0$. Any maximal ideal containing $a^m$ contains $a$; similarly, any maximal ideal containing $b^m$ contains $b$; thus no maximal ideal contains both $a^m$ and $b^m$,

which shows that the ideal they generate is $A$. Therefore, we can write $1 = ra^m + sb^m$ for some $r, s \in A$. Now

$$(ra^m)(sb^m) = 0, \quad (ra^m)^2 = (ra^m)(1 - sb^m) = ra^m, ra^m + sb^m = 1.$$

Finally, $V(\mathfrak{a}) \subset V(ra^m)$ and $V(\mathfrak{b}) \subset V(sb^m)$. As $V(ra^m) \cap V(sb^m) = \emptyset$, we see that

$$\operatorname{spm} A = V(ra^m) \sqcup V(sb^m) = D(sb^m) \sqcup D(ra^m).$$

For $n > 2$, the above argument doesn't work directly. Either do it two at a time, or use a different argument to show that taking products of rings corresponds to taking disjoint unions of spm's. □

COROLLARY 8.8 *The space* $\operatorname{spm} A$ *is disconnected if and only if* $A$ *contains an idempotent* $e \neq 0, 1$.

PROOF. $\Longleftarrow$ : If $e$ is an idempotent, then the pair $e, f = 1 - e$ satisfies (41), and so $\operatorname{spm}(A) = V(e) \sqcup V(f)$. If $V(e) = \operatorname{spm}(A)$, then $e$ is nilpotent by (8.4) and hence 0; if $V(e) = \emptyset$, then $f = 0$ and $e = 1$.

$\Longrightarrow$ : Immediate from the proposition. □

ASIDE 8.9 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, Basic Algebraic Geometry, 1994, VII 2.

## Separable subalgebras

Recall that a $k$-algebra $B$ is finite if it has finite dimension as a $k$-vector space, in which case we write $[B\colon k]$ for this dimension (and call it the ***degree*** of $B$ over $k$).

LEMMA 8.10 *Let* $A$ *be a finitely generated* $k$*-algebra. The degrees of the separable subalgebras of* $A$ *are bounded.*

PROOF. A separable subalgebra of $A$ will give a separable subalgebra of the same degree of $A \otimes_k \overline{k}$, and so we can assume $k = \overline{k}$. Then a separable subalgebra is of the form $\overline{k} \times \cdots \times \overline{k}$. For such a subalgebra, the elements $e_1 = (1, 0, \ldots), \ldots, e_r = (0, \ldots, 0, 1)$ satisfy (41). Therefore $D(e_1), \ldots, D(e_r)$ are disjoint open subsets of $\operatorname{spm} A$. Because $\operatorname{spm} A$ is noetherian, it is a finite union of its irreducible components (AG 2.21). Each connected component of $\operatorname{spm} A$ is a finite union of irreducible components, and so there are only finitely many of them. Hence $r \leq \#\pi_0(\operatorname{spm} A) < \infty$. □

Let $A$ be a finitely generated $k$-algebra. The composite of two separable subalgebras of $A$ is separable (7.4), and so, because of the lemma, there is a largest separable subalgebra $\pi_0(A)$ of $A$ containing all other.

Let $K$ be a field containing $k$. Then $\pi_0(A) \otimes_k K$ is a separable subalgebra of $A \otimes_k K$ (see 7.5). We shall need to know that it contains all other such subalgebras.

PROPOSITION 8.11 *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. Waterhouse 1979, 6.5. □

Let $A$ and $A'$ be finitely generated $k$-algebras. Then $\pi_0(A) \otimes_k \pi_0(A')$ is a separable subalgebra of $A \otimes_k A'$ (see 7.3). We shall need to know that it contains all other such subalgebras.

PROPOSITION 8.12 *Let $A$ and $A'$ be finitely generated $k$-algebras. Then*

$$\pi_0(A \otimes_k A') = \pi_0(A) \otimes_k \pi_0(A').$$

PROOF. Waterhouse 1979, 6.5. □

## The group of connected components of an algebraic group

Let $G$ be an algebraic group with coordinate ring $A = k[G]$. The map $\Delta: A \to A \otimes_k A$ is a $k$-algebra homomorphism, and so sends $\pi_0(A)$ into $\pi_0(A \otimes_k A) \overset{8.12}{=} \pi_0(A) \otimes_k \pi_0(A)$. Similarly, $S: A \to A$ sends $\pi_0(A)$ into $\pi_0(A)$, and we can define $\epsilon$ on $\pi_0(A)$ to be the restriction of $\epsilon$ on $A$. With these maps $\pi_0(A)$ becomes a sub-bialgebra of $A$.

THEOREM 8.13 *Let $G \to \pi_0(G)$ be the quotient map corresponding to the inclusion of bialgebras $\pi_0(A) \to A$.*

(a) *Every quotient map from $G$ to an étale algebraic group factors uniquely through $G \to \pi_0(G)$.*

(b) *Let $G^\circ = \operatorname{Ker}(G \to \pi_0(G))$. Then $G^\circ$ is the unique normal algebraic subgroup of $G$ such that*

i) $\pi_0(G^\circ) = 1$,

ii) *$G/G^\circ$ is étale.*

PROOF. (a) A quotient map $G \to H$ corresponds to an injective homomorphism $k[H] \to k[G]$ of $k$-bialgebras. If $H$ is étale, then $k[H]$ is separable, and so the image of the homomorphism is contained in $\pi_0(k[G]) = k[\pi_0(G)]$. This proves (a).

(b) The $k$-algebra homomorphism $\epsilon: \pi_0(k[G]) \to k$ decomposes $\pi_0(k[G])$ into a direct product

$$\pi_0(k[G]) = k \times B.$$

Let $e = (1, 0)$. Then the augmentation ideal of $\pi_0(k[G])$ is $(1 - e)$, and

$$k[G] = ek[G] \times (1 - e)k[G]$$

with $ek[G] \simeq k[G]/(1 - e)k[G] = k[G^\circ]$ (see 6.14). Clearly, $k = \pi_0(ek[G]) \simeq \pi_0(k[G^\circ])$. This shows that $G^\circ$ has the properties (i) and (ii).

Suppose $H$ is a second normal algebraic subgroup of $G$ satisfying (i) and (ii). Because $G/H$ is étale, the homomorphism $G \to G/H$ factors through $\pi_0(G)$, and so we get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G^\circ & \longrightarrow & G & \longrightarrow & \pi_0(G) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 1 \end{array}$$

with exact rows. The similar diagram with each $*$ replaced with $*(R)$ gives, for each $k$-algebra $R$, an exact sequence

$$1 \to G^\circ(R) \to H(R) \to \pi_0(G)(R). \tag{42}$$

Since this functorial in $R$, it gives a sequence of algebraic groups

$$1 \to G^\circ \to H \to \pi_0(G).$$

The exactness of (42) shows that $G^\circ$ is the kernel of $H \to \pi_0(G)$. Because $\pi_0(H) = 1$, the kernel is $H$, and so $G^\circ \simeq H$. □

DEFINITION 8.14 The subgroup $G^\circ$ is called ***identity component*** of $G$.

Recall (p13) that from an algebraic group $G$ over $k$ and a field extension $K \supset k$ we get an algebraic group $G_K$ over $K$: for any $K$-algebra $R$, $G_K(R) = G(R)$, and $K[G_K] = K \otimes_k k[G]$.

THEOREM 8.15 *For any field extension $K \supset k$, $\pi_0(G_K) \simeq \pi_0(G)_K$ and $(G_K)^\circ \simeq (G^\circ)_K$.*

PROOF. Apply (8.11). □

THEOREM 8.16 *For any algebraic groups $G$ and $G'$, $\pi_0(G \times G') \simeq \pi_0(G) \times \pi_0(G')$.*

PROOF. Apply (8.12). □

## Connected algebraic groups

DEFINITION 8.17 An algebraic group $G$ is ***connected*** if $\pi_0(G) = 1$ (i.e., $\pi_0(k[G]) = k$).

Then Theorem 8.13 says that, for any algebraic group $G$, there is a unique exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

with $G^\circ$ connected and $\pi_0(G)$ étale.

REMARK 8.18 (a) Let $K$ be a field containing $k$. Then Theorem 8.15 implies that $G$ is connected if and only if $G_K$ is connected.

(b) Let $G$ and $G'$ be algebraic groups over $k$. Then Theorem 8.16 shows that $G \times G'$ is connected if and only if both $G$ and $G'$ are connected.

THEOREM 8.19 *The following conditions on an algebraic group $G$ are equivalent:*

(a) *$G$ is connected;*
(b) *the topological space* $\operatorname{spm}(k[G])$ *is connected;*
(c) *the topological space* $\operatorname{spm}(k[G])$ *is irreducible;*
(d) *the ring $k[G]/\mathfrak{N}$ is an integral domain.*

PROOF. (a) $\Longrightarrow$ (b). If $e \in k[G]$ is idempotent, then $k[e]$ is a separable subalgebra of $k[G]$, and so equals $k$. Therefore, $e = 0$ or 1, and Corollary 8.8 implies that $\operatorname{spm}(k[G])$ is connected.

(b) $\Longrightarrow$ (a). If $k[G]$ contains no idempotents other than $0, 1$, then $\pi_0(k[G])$ is a field $K$ containing $k$. The existence of the $k$-algebra homomorphism $\epsilon\colon k[G] \to k$ implies that $K = k$.

(c) $\Longleftrightarrow$ (d). This is (8.6).

(c) $\Longrightarrow$ (b). Trivial.

(b) $\Longrightarrow$ (c). Since (a) and (d) hold over $k$ if and only if they hold over $\overline{k}$, it suffices to prove this in the case that $k = \overline{k}$. Write $\operatorname{spm} k[G]$ as a union of its irreducible components (AG 2.21). 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 (2.15), all points have this property, and so the irreducible components are disjoint. As $\operatorname{spm} k[G]$ is connected, there must be only one. □

EXAMPLE 8.20 The groups $\mathbb{G}_a$, $\mathrm{GL}_n$, $\mathbb{T}_n$ (upper triangular), $\mathbb{U}_n$ (strictly upper triangular), $\mathbb{D}_n$ are connected because in each case $k[G]$ is an integral domain. For example,

$$k[\mathbb{T}_n] = k[\mathrm{GL}_n]/(X_{ij} \mid i > j),$$

which is isomorphic to the polynomial ring in the symbols $X_{ij}$, $1 \le i \le j \le n$, with $X_{11} \cdots X_{nn}$ inverted.

EXAMPLE 8.21 For the group $G$ of monomial matrices (2.5), $\pi_0(k[G])$ 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 (2.14)), and $G^\circ = \mathbb{D}_n$.

EXAMPLE 8.22 The group $\mathrm{SL}_n$ is connected. Every invertible matrix $A$ can written uniquely in the form

$$A = A' \cdot \begin{pmatrix} a & 0 & & \\ 0 & 1 & & \\ & & \ddots & 0 \\ & & 0 & 1 \end{pmatrix}, \quad \det A' = 1.$$

Therefore $\mathrm{GL}_n \simeq \mathrm{SL}_n \times \mathbb{G}_m$ (isomorphism as set-valued functors, not as group-valued functors). Therefore $k[\mathrm{GL}_n] \simeq k[\mathrm{SL}_n] \otimes_k k[\mathbb{G}_m]$ (by the Yoneda lemma p13). In particular, $k[\mathrm{SL}_n]$ is a subring of $k[\mathrm{GL}_n]$, and so is an integral domain.

EXAMPLE 8.23 For any nondegenerate quadratic space $(V, q)$, the groups $\mathrm{Spin}(q)$ and $\mathrm{SO}(q)$ are connected. It suffices to prove this after replacing $k$ with $\overline{k}$, and so we may suppose that $q$ is the standard quadratic form $X_1^2 + \cdots + X_n^2$, in which case we write $\mathrm{SO}(q) = \mathrm{SO}_n$. The latter is shown to be connected in the exercise below.

The determinant defines a quotient map $O(q) \to \{\pm 1\}$ with kernel $\mathrm{SO}(q)$. Therefore $O(q)^\circ = \mathrm{SO}(q)$ and $\pi_0(O(q)) = \{\pm 1\}$ (constant algebraic group).

EXAMPLE 8.24 The symplectic group $\mathrm{Sp}_{2n}$ is connected (for some hints on how to prove this, see Springer 1998, 2.2.9).

EXAMPLE 8.25 Let $k$ be a field of characteristic $p \neq 0$, and let $n = p^r n_0$ with $n_0$ not divisible by

ASIDE 8.26 According to (8.9) and (8.19), 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 $\mathrm{GL}_n$ 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 $\mathrm{GL}_n$ is connected (of course, this requires the serious theorem stated in (8.9)).

**Warning:** For an algebraic group $G$ over $\mathbb{R}$, $G$ may be connected without $G(\mathbb{R})$ being connected, and conversely. For example, $\mathrm{GL}_2$ is connected as an algebraic group, but $\mathrm{GL}_2(\mathbb{R})$ is not connected for the real topology, and $\mu_3$ is not connected as an algebraic group, but $\mu_3(\mathbb{R}) = \{1\}$ is certainly connected for the real topology.

## Exact sequences and connectedness

PROPOSITION 8.27 *Let*

$$1 \to N \to G \to Q \to 1$$

*be an **exact** sequence of algebraic groups (i.e., $G \to Q$ is a quotient map with kernel $N$). If $N$ and $Q$ are connected, so also is $G$; conversely, if $G$ is connected, so also is $Q$.*

PROOF. Assume $N$ and $Q$ are connected. Then $N$ is contained in the kernel of $G \to \pi_0(G)$, so this map factors through $G \to Q$ (see 6.20), and therefore has image $\{1\}$. Conversely, since $G$ maps onto $\pi_0(Q)$, it must be trivial if $G$ is connected. □

### Exercises

8-1 What is the map $k[\mathrm{SL}_n] \to k[\mathrm{GL}_n]$ defined in example 8.22?

8-2 Prove directly that $\pi_0(k[O_n]) = k \times k$.

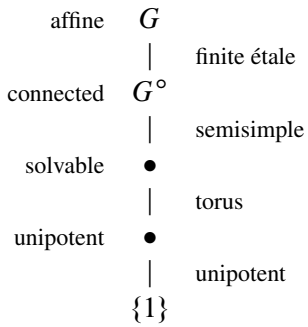
8-3 (Springer 1998, 2.2.2). For any $k$-algebra $R$, let $V(R)$ be the set of skew-symmetric matrices, i.e., the matrices such that $A^t = -A$.

(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 $\mathrm{SO}_n(\bar{k})$ onto an open subset of $V(\bar{k})$.
(c) Deduce that $\mathrm{SO}_n$ is a connected.

8-4 Let $A$ be a product 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 $S$.

## Where we are

As discussed in the first lecture, every affine algebraic group has a composition series with the quotients listed at right:




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.

# 9 Diagonalizable groups; tori

Recall for reference that

| | |
|---|---|
| $\mathbb{G}_m(R) = R^\times$ | $\mu_n(R) = \{\zeta \in R \mid \zeta^n = 1\}$ |
| $k[\mathbb{G}_m] = k[X, X^{-1}]$ | $k[\mu_n] = k[X]/(X^n - 1) = k[x]$ |
| $\Delta(X) = X \otimes X$ | $\Delta(x) = x \otimes x$ |
| $\epsilon(X) = 1$ | $\epsilon(x) = 1$ |
| $S(X) = X^{-1}$ | $S(x) = x^{n-1}$ |

## A remark about homomorphisms

9.1 Recall that a homomorphism $G \to H$ of groups is defined to be a map preserving products; it then automatically preserves neutral elements and inverses.

Now let $G$ and $H$ be algebraic groups. A homomorphism of $k$-algebras $\alpha: k[H] \to k[G]$ preserving $\Delta$ defines a natural map $G(R) \to H(R)$ preserving products, and hence also neutral elements and inverses. Therefore $\alpha$ preserves $\epsilon$ and $S$.

In other words, let $A$ and $B$ be $k$-bialgebras; in order to show that a homomorphism of $k$-algebras $A \to B$ is a homomorphism of $k$-bialgebras, it suffices to check that it sends $\Delta_A$ to $\Delta_B$; it then automatically sends $\epsilon_A$ to $\epsilon_B$ and $S_A$ and $S_B$.

## Group-like elements in a bialgebra

DEFINITION 9.2 A ***group-like*** element in a $k$-bialgebra $A$ is an invertible element $a$ of $A$ such that $\Delta(a) = a \otimes a$.

Note that if $a$ is group-like, then (see p31)

$$a = ((\epsilon, \mathrm{id}_A) \circ \Delta)(a) = (\epsilon, \mathrm{id}_A)(a \otimes a) = \epsilon(a)a,$$

and so $\epsilon(a) = 1$. Moreover,

$$\epsilon(a) = ((S, \mathrm{id}_A) \circ \Delta)(a) = (S, \mathrm{id}_A)(a \otimes a) = S(a)a$$

and so $S(a) = a^{-1}$.

The group-like elements form subgroup of $A^\times$. For example, if $a, a'$ are group-like, then

$$\begin{aligned} \Delta(aa') &= \Delta(a)\Delta(a') && (\Delta \text{ is a } k\text{-algebra homomorphism}) \\ &= (a \otimes a)(a' \otimes a') \\ &= aa' \otimes aa', \end{aligned}$$

and so $aa'$ is again group-like.

## The characters of an algebraic group

DEFINITION 9.3 A ***character*** of an algebraic group $G$ is a homomorphism $G \to \mathbb{G}_m$.

PROPOSITION 9.4 *There is a canonical one-to-one correspondence between the characters of $G$ and the group-like elements of $k[G]$.*

PROOF. According to (9.1), characters of $G$ correspond to homomorphisms of $k$-algebras $k[\mathbb{G}_m] \to k[G]$ respecting $\Delta$. To give a homomorphism of $k$-algebras $k[\mathbb{G}_m] \to k[G]$ amounts to giving an invertible element $a$ of $k[G]$ (the image of $X$), and the homomorphism respects $\Delta$ if and only if $a$ is group-like. □

For characters $\chi, \chi'$, define

$$\chi + \chi' : G(R) \to R^\times$$

by

$$(\chi + \chi')(g) = \chi(g) \cdot \chi'(g).$$

Then $\chi + \chi'$ is again a character, and the set of characters is an abelian group, denoted $X(G)$. The correspondence in the proposition is an isomorphism of groups.

## The algebraic group $D(M)$

Let $M$ be a finitely generated abelian group (written multiplicatively), and let $k[M]$ be the $k$-vector space with basis $M$. Thus, the elements of $k[M]$ are finite sums

$$\sum\nolimits_i a_i m_i, \quad a_i \in k, \quad m_i \in M,$$

and[37] $k[M]$ becomes a $k$-algebra (called the ***group algebra*** of $M$) when we set

$$\left(\sum\nolimits_i a_i m_i\right)\left(\sum\nolimits_j b_j n_j\right) = \sum\nolimits_{i,j} a_i b_j m_i n_j.$$

It becomes a bialgebra when we set

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1}.$$

Note that $k[M]$ is generated as a $k$-algebra by any set of generators for $M$, and so it is finitely generated.

EXAMPLE 9.5 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 $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, $S(e) = e$. Clearly, $k[M] \simeq k[\mathbb{G}_m]$.

(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 $S(e) = e^{n-1}$. Clearly, $k[M] \simeq k[\mu_n]$.

EXAMPLE 9.6 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 $(e_i \otimes f_j)_{(i,j)\in I\times J}$. This shows that if $M = M_1 \oplus M_2$, then

$$(m_1, m_2) \leftrightarrow m_1 \otimes m_2 : k[M] \leftrightarrow k[M_1] \otimes_k k[M_2]$$

is an isomorphism of $k$-vector spaces, and one checks easily that it respects the $k$-bialgebra structures.

[37] Bad notation — don't confuse this with the coordinate ring of an algebraic group.

PROPOSITION 9.7 *For any finitely generated abelian $M$, the functor $D(M)$*

$$R \mapsto \mathrm{Hom}(M, R^\times) \quad \textit{(homomorphisms of abelian groups)}$$

*is an algebraic group, with bialgebra $k[M]$. It is isomorphic to a finite product of copies of $\mathbb{G}_m$ and various $\mu_n$'s.*

PROOF. To give a $k$-linear map $k[M] \to R$ is to give a map $M \to R$. The map $k[M] \to R$ is a $k$-algebra homomorphism if and only if $M \to R$ has image in $R^\times$ and is a homomorphism $M \to R^\times$. This shows that $D(M)$ is represented by $k[M]$, and is therefore an algebraic group.

A decomposition of abelian groups

$$M \approx \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

defines a decomposition of $k$-bialgebras

$$k[M] \approx k[\mathbb{G}_m] \otimes_k \cdots \otimes_k k[\mathbb{G}_m] \otimes_k k[\mu_{n_1}] \otimes_k \cdots \otimes_k k[\mu_{n_r}]$$

(9.5,9.6). Since every finitely generated abelian group $M$ has such a decomposition, this proves the second statement. □

## Characterizing the groups $D(M)$

LEMMA 9.8 *The group-like elements in any $k$-bialgebra $A$ are linearly independent.*

PROOF. If not, it will be possible to express one group-like element $e$ in terms of other group-like elements $e_i \neq e$:

$$e = \sum\nolimits_i c_i e_i, \quad c_i \in k.$$

We may even assume the $e_i$ to be linearly independent. Now

$$\Delta(e) = e \otimes e = \sum\nolimits_{i,j} c_i c_j e_i \otimes e_j$$
$$\Delta(e) = \sum\nolimits_i c_i \Delta(e_i) = \sum\nolimits_i c_i e_i \otimes e_i.$$

The $e_i \otimes e_j$ are also linearly independent, and so this implies that

$$c_i c_j = \begin{cases} c_i & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Hence, each $c_i = 0$ or 1. But

$$\epsilon(e) = 1$$
$$\epsilon(e) = \sum c_i \epsilon(e_i) = \sum c_i.$$

Therefore exactly one of the $c_i = 1$, so $e = e_i$ for some $i$, contradicting our assumption. □

LEMMA 9.9 *The group-like elements of $k[M]$ are exactly the elements of $M$.*

PROOF. Let $a \in k[M]$ be group-like. Then

$$a = \sum c_i m_i \text{ for some } c_i \in k, m_i \in M.$$

The argument in the above proof shows that $a = m_i$ for some $i$. □

PROPOSITION 9.10 *An algebraic group $G$ is isomorphic to $D(M)$ for some $M$ if and only if the group-like elements in $k[G]$ span it (i.e., generate it as a $k$-vector space).*

PROOF. Certainly, the group-like elements of $k[M]$ span it. Conversely, suppose the group-like elements $M$ span $k[G]$. Then they form a basis for $k[G]$ (as a $k$-vector space), and so the inclusion $M \hookrightarrow k[G]$ extends to an isomorphism $k[M] \to k[G]$ of vector spaces. It is automatically a homomorphism of $k$-algebras, and it preserves $\Delta$ because the elements of $M$ are group-like. It is therefore an isomorphism of $k$-bialgebras (by 9.1). □

## Diagonalizable groups

DEFINITION 9.11 An algebraic group $G$ is ***diagonalizable*** if $k[G]$ is spanned by group-like elements.

THEOREM 9.12 *(a) The map $M \mapsto D(M)$ is a contravariant equivalence from the category of finitely generated abelian groups to the category of diagonalizable algebraic groups (with quasi-inverse $G \mapsto X(G)$).*
*(b) If*

$$0 \to M' \to M \to M'' \to 0$$

*is an exact sequence, then $D(M) \to D(M')$ is a quotient map with kernel $D(M'')$.*
*(c) Subgroups and quotients of diagonalizable algebraic groups are diagonalizable.*

PROOF. (a) Certainly, we have a contravariant functor

$$D\colon \{\text{finitely generated abelian groups}\} \to \{\text{diagonalizable groups}\}.$$

We show that $D$ is fully faithful, i.e., that

$$\mathrm{Hom}(M, M') \to \mathrm{Hom}(D(M'), D(M)) \tag{43}$$

is an isomorphism for all $M, M'$. As $D$ sends direct sums to products, it suffices to do this when $M, M'$ are cyclic. If, for example, $M$ and $M'$ are both infinite cyclic groups, then

$$\mathrm{Hom}(M, M') = \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z},$$

and

$$\mathrm{Hom}(D(M'), D(M)) = \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \{X^i \mid i \in \mathbb{Z}\} \simeq \mathbb{Z},$$

and so (43) is an isomorphism. The remaining cases are similarly easy.

Finally, (9.10) shows that the functor is essentially surjective, and so is an equivalence.

(b) The map $k[M'] \to k[M]$ is injective, and so $D(M) \to D(M')$ is a quotient map (by definition). Its kernel is represented by $k[M]/I_{k[M']}$, where $I_{k[M']}$ is the augmentation ideal of $k[M']$ (see 6.14). But $I_{k[M']}$ is the ideal generated the elements $m-1$ for $m \in M'$, and so $k[M]/I_{k[M']}$ is the quotient ring obtained by putting $m = 1$ for all $m \in M'$. Therefore $M \to M''$ defines an isomorphism $k[M]/I_{k[M']} \to k[M'']$.

(c) If $H$ is an algebraic subgroup of $G$, then $k[G] \to k[H]$ is surjective, and so if the group-like elements of $k[G]$ span it, the same is true of $k[H]$.

Let $D(M) \to Q$ be a quotient map, and let $H$ be its kernel. Then $H = D(M'')$ for some quotient $M''$ of $M$. Let $M'$ be the kernel of $M \to M''$. Then $D(M) \to D(M')$ and $D(M) \to Q$ are quotient maps with the same kernel, and so are isomorphic (6.21). □

## Diagonalizable groups are diagonalizable

Recall that $\mathbb{D}_n$ is the group of invertible diagonal $n \times n$ matrices; thus

$$\mathbb{D}_n \simeq \mathbb{G}_m \times \cdots \times \mathbb{G}_m \quad (n \text{ copies}).$$

THEOREM 9.13 *Let $V$ be a finite-dimensional vector space, and let $G$ be an algebraic subgroup of $\mathrm{GL}_V$. There exists a basis of $V$ for which $G \subset \mathbb{D}_n$ if and only if $G$ is diagonalizable.*

In more down-to-earth terms, the theorem says that for an algebraic subgroup $G$ of $\mathrm{GL}_n$, there exists an invertible matrix $P$ in $M_n(k)$ such that, for all $k$-algebras $R$ and all $g \in G(R)$,

$$PgP^{-1} \in \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}$$

if and only if $G$ is diagonalizable (according to definition 9.11).

PROOF. $\Longrightarrow$ : This follows from (9.12c).

$\Longleftarrow$ : Let $A = k[G]$, and let $\rho: V \to V \otimes_k A$ be the comodule corresponding to the representation $G \hookrightarrow \mathrm{GL}_V$ (see §3). We have to show that $V$ is a direct sum of one-dimensional representations or, equivalently, that there exists a basis for $V$ consisting of vectors $v$ such that $\rho(v) \in \langle v \rangle \otimes_k A$.

Let $(e_i)_{i \in I}$ be the basis for $A = k[G]$ of group-like elements, and write

$$\rho(v) = \sum\nolimits_i v_i \otimes e_i .$$

Applying the identity (see p31)

$$(\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_A) \circ \rho$$

to $v$ gives

$$\sum\nolimits_i v_i \otimes e_i \otimes e_i = \sum\nolimits_i \rho(v_i) \otimes e_i .$$

Hence

$$\rho(v_i) = v_i \otimes e_i \in \langle v_i \rangle \otimes_k A.$$

Since (see p31)

$$\begin{aligned} v &= (\mathrm{id}_V \otimes \epsilon) \circ \rho(v) \\ &= \sum v_i \epsilon(e_i) = \sum v_i \end{aligned}$$

is in the span of the $v_i$, we see that by taking enough $v$'s we get enough $v_i$'s to span $V$. □

## Split tori and their representations

DEFINITION 9.14 An algebraic group is a ***split torus*** if it is isomorphic to a product of copies of $\mathbb{G}_m$, and it is a ***torus*** if it becomes a split torus over $\overline{k}$.

In other words, the split tori are the diagonalizable groups $D(M)$ with $M$ torsion-free. The functor $M \mapsto D(M)$ is a contravariant equivalence from the category of free abelian groups of finite rank to the category of split tori, with quasi-inverse $T \mapsto X(T)$.

For example, let $T = \mathbb{G}_m \times \mathbb{G}_m$. Then $X(T) = \mathbb{Z} \oplus \mathbb{Z}$. The character corresponding to $(m_1, m_2) \in \mathbb{Z} \oplus \mathbb{Z}$ is

$$(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2} : T(R) \to \mathbb{G}_m(R).$$

A quotient group of a torus is again a torus (because it corresponds to a subgroup of a free abelian group of finite rank), but a subgroup of a torus need not be a torus. For example, $\mu_n$ is a subgroup of $\mathbb{G}_m$ (the map $\mu_n \to \mathbb{G}_m$ corresponds to $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$).

A character $\chi: T \to \mathbb{G}_m$ defines a representation of $T$ on any finite-dimensional space $V$: let $t \in T(R)$ act on $R \otimes_k V$ as multiplication by $\chi(t) \in R^\times$. For example, $\chi$ defines a representation of $T$ on $k^n$ by

$$t \mapsto \begin{pmatrix} \chi(t) & & 0 \\ & \ddots & \\ 0 & & \chi(t) \end{pmatrix}.$$

Let $\rho: T \to \mathrm{GL}_V$ be a representation of $T$. We say that $T$ ***acts on*** $V$ ***through*** $\chi$ if

$$\rho(t)v = \chi(t)v \text{ all } t \in T(R),\ v \in R \otimes_k V.$$

More precisely, this means that the image of $\rho$ is contained in the centre $\mathbb{G}_m$ of $\mathrm{GL}_V$ and is the composite of

$$T \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V .$$

If $V$ is 1-dimensional, then $\mathrm{GL}_V = \mathbb{G}_m$, and so $T$ always acts on $V$ through some character.

THEOREM 9.15 *Let $r: T \to \mathrm{GL}(V)$ be a representation of a split torus on a finite dimensional vector space $V$. For each character $\chi$, let $V_\chi$ be the largest subspace of $V$ on which $T$ acts through the character $\chi$. Then*

$$V = \bigoplus\nolimits_{\chi \in X(T)} V_\chi.$$

PROOF. Theorem 9.13 shows that $V = \bigoplus_{1 \le i \le r} V_{\chi_i}$ for certain characters $\chi_1, \dots, \chi_r$. Thus, $V = \sum_{\chi \in X(T)} V_\chi$, and (11.20) below shows that the sum is direct. □

For example, let $T = \mathbb{G}_m \times \mathbb{G}_m$, and let $r: T \to \mathrm{GL}(V)$ be a representation of $T$ on a finite-dimensional vector space $V$. Then $V$ 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 $t_1^{m_1} t_2^{m_2}$ (of course, all but a finite number of the $V_{(m_1,m_2)}$ are zero).

## Rigidity

By an action of algebraic group on another algebraic group, we mean natural actions

$$G(R) \times H(R) \to H(R)$$

such that the elements of $G(R)$ act on $H(R)$ by group homomorphisms. We shall need the following result:

THEOREM 9.16 *Every action of a connected algebraic group $G$ on a torus $T$ is trivial.*

The proof is based on the following result:

PROPOSITION 9.17 *Every action of a connected algebraic group $G$ on a product of copies of $\mu_m$ is trivial.*

PROOF. (SKETCH) Let $H$ be a product of copies of $\mu_m$, and let $A = k[H]$. The functor sending $R$ to

$$\underline{\mathrm{Aut}}(H)(R) \stackrel{\mathrm{df}}{=} \mathrm{Aut}_{R\text{-bialgebras}}(R \otimes_k A)$$

is an étale algebraic group (cf. exercise 9-1 below). The action of $G$ on $H$ defines a homomorphism $G \to \underline{\mathrm{Aut}}(H)$ of algebraic groups, which is trivial because $G$ is connected (see §8). □

We now sketch the proof of the theorem. It suffices to show that each element $g$ of $G(\overline{k})$ defines the trivial automorphism of $T_{\overline{k}}$. Thus, we can replace $k$ with $\overline{k}$ and take $k$ to be algebraically closed. The kernel of $x \mapsto x^m : T \to T$ is a product of copies of $\mu_m$, and so $G$ acts trivially on it. Because of the category equivalence $T \mapsto X(T)$, it suffices to show that $g$ acts trivially on the $X(T)$, and because $g$ acts trivially on the kernel of $m : T \to T$ it acts trivially on $X(T)/mX(T)$. We can now apply the following elementary lemma.

LEMMA 9.18 *Let $M$ be a free abelian group of finite rank, and let $\alpha : M \to M$ be a homomorphism such that*

$$\begin{array}{ccc} M & \longrightarrow & M \\ \downarrow & & \downarrow \\ M/mM & \xrightarrow{\mathrm{id}} & M/mM \end{array}$$

*commutes for all $m$. Then $\alpha = \mathrm{id}$.*

PROOF. 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 $m$,

$$(a_{ij}) \equiv I_n \mod m,$$

i.e., that $m | a_{ij}$ for $i \neq j$ and $m | a_{ii} - 1$. Clearly, this implies that $(a_{ij}) = I_n$. □

## Groups of multiplicative type

DEFINITION 9.19 An algebraic group $G$ is of ***multiplicative type*** if $G_{\overline{k}}$ is diagonalizable.

Assume (for simplicity) that $k$ is perfect. Let $M$ be a finitely generated abelian group, and let $\Gamma$ be the group of automorphisms of $\overline{k}$ over $k$. A ***continuous action*** of $\Gamma$ on $M$ is a homomorphism $\Gamma \to \mathrm{Aut}(M)$ factoring through $\mathrm{Gal}(K/k)$ for some finite Galois extension $K$ of $k$ contained in $\overline{k}$.

For an algebraic group $G$, we define

$$X^*(G) = \mathrm{Hom}(G_{\overline{k}}, \mathbb{G}_m).$$

Then $\Gamma$ acts continuously on $X^*(G)$, because $X^*(G)$ is finitely generators, and each of its generators is defined over a finite extension of $k$.

THEOREM 9.20 *The functor $G \to X^*(G)$ is a contravariant equivalence from the category of algebraic groups of multiplicative type over $k$ to the category of finitely generated abelian groups with a continuous action of $\Gamma$.*

PROOF. Omitted (for the present). See Waterhouse 7.3. □

Let $G$ be a group of multiplicative type over $k$. For any $K \subset \overline{k}$,

$$G(K) = \mathrm{Hom}(X^*(G), \overline{k}^\times)^{\Gamma_K}$$

where $\Gamma_K$ is the subgroup of $\Gamma$ of elements fixing $K$, and the notation means the $G(K)$ equals the group of homomorphisms $X^*(G) \to \overline{k}^\times$ commuting with the actions of $\Gamma_K$.

EXAMPLE 9.21 Take $k = \mathbb{R}$, so that $\Gamma$ is cyclic of order 2, and let $X^*(G) = \mathbb{Z}$. There are two possible actions of $\Gamma$ on $X^*(G)$.

(a) Trivial action. Then $G(\mathbb{R}) = \mathbb{R}^\times$, and $G \simeq \mathbb{G}_m$.
(b) The generator $\iota$ of $\Gamma$ acts on $\mathbb{Z}$ as $m \mapsto -m$. Then $G(\mathbb{R}) = \mathrm{Hom}(\mathbb{Z}, \mathbb{C}^\times)^\Gamma$ consists of the elements of $\mathbb{C}^\times$ fixed under the following action of $\iota$,

$$\iota z = \overline{z}^{-1}.$$

Thus $G(\mathbb{R}) = \{z \in \mathbb{C}^\times \mid z\overline{z} = 1\}$, which is compact.

EXAMPLE 9.22 Let $K$ be a finite extension of $k$. Let $T$ be the functor $R \mapsto (R \otimes_k K)^\times$. Then $T$ is an algebraic group, in fact, the group of multiplicative type corresponding to the $\Gamma$-module $\mathbb{Z}^{\mathrm{Hom}_k(K,\overline{k})}$ (families of elements of $\mathbb{Z}$ indexed by the $k$-homomorphisms $K \to \overline{k}$).

## Exercises

9-1 Show that $\underline{\mathrm{Aut}}(\mu_m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (constant group defined by the group of invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$). Hint: To recognize the elements of $\underline{\mathrm{Aut}}(\mu_m)(R)$ as complete systems of orthogonal idempotents, see the proof of (9.8).

# 10 Jordan decompositions

An endomorphism $\alpha$ of a finite-dimensionsl vector space $V$ over $k$ is ***semisimple*** if it becomes diagonalizable on $\overline{k} \otimes_k V$. For example, for an $n \times n$ matrix $A$, the endomorphism $x \mapsto Ax: k^n \to k^n$ is semisimple if and only if there exists an invertible matrix $P$ with entries in $\overline{k}$ such that $PAP^{-1}$ is diagonal.

From linear algebra, we know that $\alpha$ is semisimple if and only if its minimum polynomial $m_\alpha(T)$ has distinct roots; in other words, if and only if the subring $k[\alpha] \simeq k[T]/(m_\alpha(T))$ of $\mathrm{End}_k(V)$ generated by $\alpha$ is separable.

An endomorphism $\alpha$ of $V$ is ***nilpotent*** if $\alpha^m = 0$ for some $m > 0$, and it is ***unipotent*** if $\mathrm{id}_V - \alpha$ is nilpotent. Clearly, if $\alpha$ is nilpotent, then its minimum polynomial divides $T^m$ for some $m$, and so the eigenvalues of $\alpha$ are all zero, even in $\overline{k}$. From linear algebra, we know that the converse is also true, and so $\alpha$ is unipotent if and only if its eigenvalues in $\overline{k}$ all equal 1.

In this section, we prove the following theorem:

THEOREM 10.1 *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*

(a) $g = g_s g_u = g_u g_s$,

(b) *for all representations $\varphi: G \to \mathrm{GL}(V)$, $\varphi(g_s)$ is semisimple and $\varphi(g_u)$ is unipotent.*

Then $g_s$ and $g_u$ are called the ***semisimple*** and ***unipotent parts*** of $g$, and $g = g_s g_u$ is the ***Jordan decomposition*** of $g$.

## Jordan normal forms

Let $\alpha$ be an endomorphism of a finite-dimensional vector space $V$ over $k$. We say that $\alpha$ ***has all its eigenvalues*** in $k$ if the characteristic polynomial $P_\alpha(T)$ of $\alpha$ splits in $k[X]$,

$$P_\alpha(T) = (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}, \quad a_i \in k.$$

THEOREM 10.2 *Let $\alpha$ be an endomorphism of a finite-dimensional vector space $V$ with all its eigenvalues in $k$, and let $a_1, \dots, a_r$ be its distinct eigenvalues. Then there exists a basis for $V$ relative to which the matrix of $\alpha$ is*

$$A = \begin{pmatrix} A_1 & 0 & & \\ 0 & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \quad \text{where} \quad A_i = \begin{pmatrix} a_i & * & * \\ & \ddots & * \\ & & a_i \end{pmatrix}.$$

In fact, of course, one can even do a little better. This theorem is usually proved at the same time as the following theorem. For each eigenvalue $a$ of $\alpha$ in $k$, the ***generalized eigenspace*** is defined to be:

$$V_a = \{v \in V \mid (\alpha - a)^N v = 0, \quad N \text{ sufficiently divisible}\}.$$

THEOREM 10.3 *If $\alpha$ has all its eigenvalues in $k$, then $V$ is a direct sum of the generalized eigenspaces:*

$$V = \bigoplus\nolimits_i V_{a_i}.$$

To deduce this from the first theorem, note that $V_{a_i}$ is spanned by the basis vectors corresponding to $A_i$ (so $\alpha$ acts on $V_{a_i}$ through the matrix $A_i$). To deduce the first theorem from the second amounts to studying the action of the nilpotent endomorphism $\alpha - a_i$ on the subspace $V_{a_i}$.

## Jordan decomposition in $\mathrm{GL}_n(V)$ ($k = \overline{k}$)

In this subsection, $k$ is algebraically closed.

PROPOSITION 10.4 *For any automorphism $\alpha$ of a finite-dimensional vector space $V$, there exist unique automorphisms $\alpha_s$ and $\alpha_u$ such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$,

(b) *$\alpha_s$ is semisimple and $\alpha_u$ is unipotent.*

PROOF. According to (10.3), $V$ is a direct sum of its generalized eigenspaces of: $V = \bigoplus V_a$. Define $\alpha_s$ to be the automorphism of $V$ that acts as $a$ on $V_a$. Then $\alpha_s$ is a semisimple automorphism of $V$, and $\alpha_u =_{\mathrm{df}} \alpha \circ \alpha_s^{-1}$ commutes with $\alpha_s$ (because it does on each $V_a$) and is unipotent (because its eigenvalues are 1).

Let $\alpha = \beta_s \circ \beta_u$ be a second decomposition satisfying (a) and (b), and let $V = \bigoplus V_b$ be the decomposition of $V$ into the eigenspaces for $\beta_s$ (corresponding to distinct eigenvalues). Because $\beta_s$ and $\beta_u$ commute, each $V_b$ is stable under $\beta_u$,

$$v \in V_b \implies \beta_s(\beta_u(v)) = \beta_u\beta_s v = \beta_u b v = b(\beta_u v),$$

and hence under $\alpha$. Moreover, $V_b$ is a generalized eigenspace for $V$ with eigenvalue $b$, which shows that $V = \bigoplus V_b$ is *the* decomposition of $V$ into its generalized eigenspaces. Since $\beta_s$ acts on $V_b$ as multiplication by $b$, this proves that $\beta_s = \alpha_s$, and so $\beta_u = \alpha_u$. □

The automorphisms $\alpha_s$ and $\alpha_u$ are called the ***semisimple*** and ***unipotent parts*** of $\alpha$, and $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$ is the ***Jordan decompostion*** of $\alpha$.

PROPOSITION 10.5 *Let $\alpha$ and $\beta$ be automorphisms of $V$ and $W$ respectively, and let $\varphi\colon V \to W$ be a linear map such that $\varphi\circ\alpha = \beta\circ\varphi$. Then $\varphi\circ\alpha_s = \beta_s\circ\varphi$ and $\varphi\circ\alpha_u = \beta_u\circ\varphi$.*

PROOF. For each $a \in k$, $\varphi$ obviously maps $V_a$ into $W_a$, which implies that $\varphi \circ \alpha_s = \beta_s \circ \varphi$. Hence also

$$\varphi \circ \alpha_u = \varphi \circ (\alpha \circ \alpha_s^{-1}) = (\beta \circ \beta_s^{-1}) \circ \varphi = \beta_u \circ \varphi.$$ □

PROPOSITION 10.6 *Let $\alpha = \alpha_s \circ \alpha_u$ be the Jordan decomposition of $\alpha$. Then $\alpha_s \in k[\alpha]$, i.e., there exists a polyonomial $P(T) \in k[T]$ such that $\alpha_s = P(\alpha)$.*

PROOF. For each (distinct) eigenvalue $a_i$ of $\alpha$, let $n_i$ be such that $(\alpha - a)^{n_i} = 0$ on $V_{a_i}$. The polynomials $(T - a_i)^{n_{a_i}}$ are relatively prime, and so, according to the Chinese remainder theorem, there exists a $P \in k[T]$ such that

$$\begin{aligned} P(T) &\equiv a_1 \bmod (T - a_1)^{n_{a_1}} \\ P(T) &\equiv a_2 \bmod (T - a_2)^{n_{a_2}} \\ &\cdots \end{aligned}$$

Then $P(\alpha)$ acts as $a_i$ on $V_{a_i}$, and so $P(\alpha) = \alpha_s$. □

COROLLARY 10.7 *Every subspace $W$ of $V$ stable under $\alpha$ is stable under $\alpha_s$ and $\alpha_u$, 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 $\alpha_s$, and therefore also $\alpha_s^{-1}$ and $\alpha_u$. It is obvious that the decomposition $\alpha|W = \alpha_s|W \circ \alpha_u|W$ has the properties to be the Jordan decomposition. □

**For the remainder of this section, $k$ is perfect.**

## Jordan decomposition in $\mathrm{GL}(V)$, $k$ perfect

Let $\alpha$ be an automorphism of a finite-dimensional vector space $V$ over a perfect field $k$, and let $K$ be a splitting field for the minimum polyomial of $\alpha$ (so $K$ is generated by the eigenvalues of $\alpha$). 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 $\alpha$. Theorem 10.3 allows us to write $A = A_s A_u = A_u A_s$ with $A_s, A_u$ respectively semisimple and unipotent matrices with entries in $K$; moreover, this decomposition is unique.

Let $\sigma \in \mathrm{Gal}(K/k)$, and for a matrix $B = (b_{ij})$, define $\sigma B = (\sigma b_{ij})$. Because $A$ has entries in $k$, $\sigma A = A$. Now

$$A = (\sigma A_s)(\sigma A_u) = (\sigma A_u)(\sigma A_s)$$

is again a Jordan decomposition of $A$. By uniqueness, $\sigma A_s = A_s$ and $\sigma A_u = A_u$. Since this is true for all $\sigma \in \mathrm{Gal}(K/k)$, $A_s$ and $A_u$ have entries in $k$. This shows that Jordan decompositions exist over $k$.

THEOREM 10.8 *Let $\alpha$ be an automomorphism of a finite-dimensional vector space $V$ over a perfect field. Then $\alpha$ has a unique (Jordan) decomposition $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$ with $\alpha_s$ and $\alpha_u$ semisimple and unipotent respectively. Any subspace $W$ of $V$ stable under $\alpha$ is stable under $\alpha_s$ and $\alpha_u$, and $\alpha|W = (\alpha_s|W) \circ (\alpha_u|W) = (\alpha_u|W) \circ (\alpha_s|W)$.*

For the last sentence, one needs that $(K \otimes_k W) \cap V = W$. To prove this, choose a basis $(e_i)_{1 \le i \le m}$ for $W$, and extend it to a basis $(e_i)_{1 \le i \le n}$ for $V$. If $\sum a_i e_i$ ($a_i \in k$), lies in $K \otimes_k W$, then $a_i = 0$ for $i > m$.

LEMMA 10.9 *Let $\alpha$ and $\beta$ be automorphisms of vector spaces $V$ and $W$. Then*

$$\begin{array}{llll} (\alpha^{-1})_s = \alpha_s^{-1} & (\alpha \otimes \beta)_s = \alpha_s \otimes \beta_s & (\alpha^\vee)_s = \alpha_s^\vee & (\alpha \oplus \beta)_s = \alpha_s \oplus \beta_s \\ (\alpha^{-1})_u = \alpha_u^{-1} & (\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u & (\alpha^\vee)_u = \alpha_u^\vee & (\alpha \oplus \beta)_u = \alpha_u \oplus \beta_u \end{array}$$

PROOF. It is obvious that $\alpha^{-1} = (\alpha_u)^{-1}(\alpha_s)^{-1}$ is the Jordan decomposition of $\alpha^{-1}$. It suffices to prove the remaining statements in the top row, and it suffices to prove these after passing to the algebraic closure of the ground field. Thus, we may choose bases for which the matrices of $\alpha$ and $\beta$ are upper triangular. Note that the semisimple part of a triangular matrix (upper or lower) is obtained by putting all off-diagonal entries equal to zero. Thus, the equalities on the first row follow from the next statement. Let $A$ and $B$ be the matrices of $\alpha$ and $\beta$ relative some choice of bases for $V$ and $W$; relative to the obvious bases, $\alpha \otimes \beta$, $\alpha^\vee$, and $\alpha \oplus \beta$ have the following matrices:

$$\begin{pmatrix} Ab_{11} & Ab_{12} & \cdots \\ Ab_{21} & Ab_{22} & \\ \vdots & & \end{pmatrix} \qquad A^t \qquad \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

□

EXAMPLE 10.10 Let $k$ have characteristic 2 and be nonperfect, so that there exists an $a \in k$ that is not a square in $k$, and let $A = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$. In $k[\sqrt{a}]$, $A$ has the Jordan decomposition

$$A = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & 1/\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix}.$$

Since these matrices do not have coefficients in $k$, the uniqueness shows that $A$ does not have a Jordan decomposition in $M_2(k)$.

## Infinite-dimensional vector spaces

Let $V$ be a vector space, possibly infinite dimensional, over $k$. An endomorphism $\alpha$ of $V$ is ***locally finite*** if $V$ is a union of finite-dimensional subspaces stable under $\alpha$. 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 $\alpha$ be a locally finite automorphism of $V$. By assumption, every $v \in V$ is contained in a finite-dimensional subspace $W$ stable under $\alpha$, and we define $\alpha_s(v) = (\alpha|W)_s(v)$. According to (10.8), this is independent of the choice of $W$, and so in this way we get a semisimple automorphism of $V$. Similarly, we can define $\alpha_u$. Thus:

THEOREM 10.11 *For any locally finite automorphism $\alpha$ of $V$, there exist unique automorphisms $\alpha_s$ and $\alpha_u$ such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$,

(b) *$\alpha_s$ is semisimple and $\alpha_u$ is locally unipotent.*

*For any finite-dimensional subspace $W$ of $V$ stable under $\alpha$, $\alpha|W = (\alpha_s|W) \circ (\alpha_u|W) = (\alpha_u|W) \circ (\alpha_s|W)$ is the Jordan decomposition of $\alpha|W$.*

## The regular representation contains all

Let $G$ be an algebraic group and let $g \in G(k)$. For any representation $\varphi: G \to \mathrm{GL}_V$, we get a Jordan decomposition $\varphi(g) = \varphi(g)_s\varphi(g)_u$ in $\mathrm{GL}(V)$. We have to show that there is a decomposition $g = g_s g_u$ in $G(k)$ that gives the Jordan decomposition for *every* representation $\varphi$. One basic result we will need is that every representation of $G$ occurs already in a direct sum of copies of the regular representation, and so if we can find a decomposition $g = g_s g_u$ in $G(k)$ that works for the regular representation it should work for every representation.

PROPOSITION 10.12 *Let $V$ be a representation of $G$, and let $V_0$ denote the underlying vector space with the trivial representation. Then there is an injective homomorphism*[38]

$$V \to V_0 \otimes k[G]$$

[38]Compare the proposition with the following result for a finite group $G$ of order $n$. Let $k[G]$ be the group algebra, and let $V$ be a $k[G]$-module. Let $V_0$ be $V$ regarded as a vector space. Then

$$v \mapsto n^{-1} \sum_{g \in G} g \otimes g^{-1}v: V \to k[G] \otimes_k V_0$$

is a $G$-homomorphism whose composite with

$$g, v \mapsto gv: k[G] \otimes_k V_0 \to V$$

is the identity on $V$.

*of representations (i.e., $V$ embeds into a direct sum of copies of the regular representation).*

PROOF. Let $A = k[G]$. The $k$-vector space $V \otimes_k A$ becomes a comodule (isomorphic to a direct sum of copies of $A$) with the map

$$\mathrm{id}_V \otimes \Delta\colon V \otimes_k A \to V \otimes_k A \otimes_k A.$$

The commutative diagram (see p31)

$$\begin{array}{ccccc} V & \xrightarrow{\quad\rho\quad} & V_0 \otimes_k A & \approx & A^n \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \mathrm{id}_{V_0}\otimes\Delta} & & \downarrow{\scriptstyle \Delta^n} \\ V \otimes_k A & \xrightarrow{\rho\otimes 1} & V_0 \otimes_k A \otimes_k A & \approx & (A \otimes_k A)^n \end{array}$$

says exactly that the inclusion $\rho\colon V \to V \otimes_k A$ is homomorphism of comodules. □

## The Jordan decomposition in the regular representation

Let $G$ be an algebraic group. An element $g$ of $G(k) = \mathrm{Hom}_{k\text{-alg}}(A, k)$ defines a $k$-linear automorphism $\phi(g)\colon A \to A$, namely,

$$A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{a\otimes a' \mapsto a\cdot g(a')} A \tag{44}$$

($\phi$ is the regular representation). Moreover, $\phi(g)$ is locally finite (3.4), and so there is a decomposition $\phi(g) = \phi(g)_s\phi(g)_u$ whose restriction to any $\phi(g)$-stable subspace is the Jordan decomposition.

PROPOSITION 10.13 *Let $g \in \mathrm{GL}(V)$, and let $g = g_s g_u$ be its Jordan decomposition.*

(a) *Let $\phi$ be the regular representation of $\mathrm{GL}_V$ on $A = k[\mathrm{GL}_V]$; then $\phi(g) = \phi(g_s)\phi(g_u)$ is the Jordan decomposition of $\phi(g)$ (i.e., $\phi(g)_s = \phi(g_s)$ and $\phi(g)_u = \phi(g_u)$).*

(b) *Let $G$ be an algebraic subgroup of $\mathrm{GL}_V$; if $g \in G(k)$, then $g_s, g_u \in G(k)$.*

PROOF. (a) Let $G = \mathrm{GL}_V$ act on $V^\vee$ through the contragredient representation, i.e., $g$ acts as $(g^\vee)^{-1}$. The actions of $G$ on $V$ and $V^\vee$ define an injective map (compatible with the actions of $\mathrm{GL}(V)$)

$$\mathrm{GL}(V) \to \mathrm{End}(V) \times \mathrm{End}(V^\vee)$$

whose image consists of the pairs $(\alpha, \beta)$ such that $\alpha^\vee \circ \beta = \mathrm{id}_{V^\vee}$. When we choose a basis for $V$, this equality becomes a polynomial condition on the entries of the matrices of $\alpha$ and $\beta$, and so $\mathrm{GL}_V$ is a closed subvariety of $\mathrm{End}(V) \times \mathrm{End}(V^\vee)$ (regarded as an algebraic variety; cf. AG p55, affine space without coordinates). Therefore, there is a surjective map of coordinate rings:

$$\pi\colon \mathrm{Sym}(V^\vee \otimes V) \otimes_k \mathrm{Sym}(V \otimes V^\vee) \twoheadrightarrow k[G].$$

Let $\Phi$ be the natural representation of $\mathrm{GL}_V$ on $\mathrm{Sym}(V^\vee \otimes V) \otimes_k \mathrm{Sym}(V \otimes V^\vee)$. It follows from Lemma 10.9 that $\Phi(g)_s = \Phi(g_s)$. For any $h \in \mathrm{GL}(V)$, $\pi \circ \Phi(h) = \phi(h) \circ \pi$. In particular,

$$\begin{aligned} \pi \circ \Phi(g) &= \phi(g) \circ \pi \\ (\pi \circ \Phi(g)_s =) \quad \pi \circ \Phi(g_s) &= \phi(g_s) \circ \pi \end{aligned}$$

According to (10.5), the first of these implies that

$$\pi \circ \Phi(g)_s = \phi(g)_s \circ \pi.$$

Since $\pi$ is surjective, this shows that $\phi(g)_s = \phi(g_s)$.

(b) Let $k[G] = A/I$. An element $g$ of $\mathrm{GL}_V(k) = \mathrm{Hom}_{k\text{-alg}}(A, k)$ lies in $G(k)$ if and only if $g(I) = 0$. Thus, we have to show that

$$g(I) = 0 \implies g_s(I) = 0.$$

The composite of the maps in the top row of

$$\begin{array}{ccccc} A & \xrightarrow{\Delta_{\mathrm{GL}_V}} & A \otimes_k A & \xrightarrow{\mathrm{id}_A \otimes g} & A \otimes_k k \\ \downarrow & & \downarrow & & \downarrow \\ A/I & \xrightarrow{\Delta_G} & A/I \otimes_k A/I & \xrightarrow{\mathrm{id}_{A/I} \otimes g} & A/I \otimes_k k \end{array}$$

is $\phi(g)$ (see (44)). As the diagram commutes, we see that

$$\phi(g)(I) \subset I,$$

and so

$$\phi(g_s)(I) = \phi(g)_s(I) \subset I.$$

Because $A \to A/I$ is a homomorphism of bialgebras, $\epsilon_{\mathrm{GL}_V}(I) = 0$. According to the next lemma,

$$g_s = \epsilon \circ \phi(g_s),$$

and so $g_s$ sends $I$ to 0. □

LEMMA 10.14 *Let $G$ be an algebraic group, and let $\phi$ be the regular representation. An element $g \in G(k)$ can be recovered from $\phi(g)$ by the formula*

$$g = \epsilon \circ \phi(g).$$

PROOF. Let $A = k[G]$, and recall that $g$ is a homomorphism $A \to k$. When we omit the identification $A \otimes_k k \simeq k$, $\phi(g)$ is the composite,

$$\phi(g) = (\mathrm{id}_A \otimes g) \circ \Delta : A \to A \otimes_k A \to A \otimes_k k.$$

Therefore,

$$(\epsilon \otimes \mathrm{id}_k) \circ \phi(g) = (\epsilon \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes g) \circ \Delta.$$

Clearly,

$$\begin{aligned} (\epsilon \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes g) &= \epsilon \otimes g \qquad \text{(homomorphisms } A \otimes_k A \to k \otimes_k k\text{)} \\ &= (\mathrm{id}_k \otimes g) \circ (\epsilon \otimes \mathrm{id}_A). \end{aligned}$$

But $(\epsilon \otimes \mathrm{id}_A) \circ \Delta$ is the canonical isomorphism $i\colon A \simeq k \otimes_k A$ (see p31), and so

$$(\epsilon \otimes \mathrm{id}_k) \circ \phi(g) = \mathrm{id}_k \otimes g \circ i \qquad \text{(homomorphisms } A \to k \otimes k\text{)}.$$

When we ignore $i$'s, this becomes the required formula. □

**Proof of Theorem 10.1**

Let $G$ be an algebraic group over $k$, and choose an embedding

$$\varphi: G \to \mathrm{GL}_V$$

with $V$ a finite-dimensional vector space (we know $\varphi$ exists by 3.8). Let $g \in G(k)$. According to (10.13), there is a decomposition $g = g_s g_u$ in $G(k)$ giving the Jordan decomposition on $V$. Let $\varphi': G \to \mathrm{GL}_{V'}$ be a second representation, and consider the homomorphism

$$(\varphi, \varphi'): G \to \mathrm{GL}_{V \oplus V'}$$

defined by $\varphi, \varphi'$. According to (10.13), there is a decomposition $g = g'_s g'_u$ in $G(k)$ giving the Jordan decomposition on $V \oplus V'$, and in particular on $V$. Since $G(k) \to \mathrm{GL}(V)$ is injective, this shows that $g_s = g'_s$, $g_u = g'_u$, and that the decomposition $g = g_s g_u$ gives the Jordan decomposition on $V'$. This proves the existence, and the uniqueness is obvious.

REMARK 10.15 (a) To check that a decomposition $g = g_s g_u$ is the Jordan decomposition, it suffices to check that $\varphi(g) = \varphi(g_s)\varphi(g_u)$ is the Jordan decomposition of $\varphi(g)$ for a single faithful representation of $G$.

(b) Homomorphisms of groups preserve Jordan decompositions. [Let $\alpha: G \to G'$ be a homomorphism and $g = g_s g_u$ a Jordan decomposition in $G(k)$. For any representation $\varphi: G' \to \mathrm{GL}_V$, $\varphi \circ \alpha$ 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 $\varphi$ to be faithful, this implies that $\alpha(g) = \alpha(g_s) \cdot \alpha(g_u)$ is the Jordan decomposition of $\alpha(g)$.]

NOTES The above proof of the Jordan decomposition can probably be simplified.

# 11 Solvable algebraic groups

## Brief review of solvable groups (in the usual sense)

Let $G$ be a group (in the usual sense). 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 a commutator to a commutator, 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)

$$(x_1, y_1, \dots, x_n, y_n) \mapsto [x_1, y_1] \cdots [x_n, y_n] \colon G^{2n} \to G$$

has image the set of elements of $G$ that can be written as a product of (at most) $n$ commutators, and so $\mathcal{D}G$ is the union of the images of these maps. Note that $G^{2n-2} \to G$ factors through $G^{2n} \to G$,

$$(x_1, y_1, \dots, x_{n-1}, y_{n-1}) \mapsto (x_1, y_1, \dots, x_{n-1}, y_{n-1}, 1, 1) \mapsto [x_1, y_1] \cdots [x_{n-1}, y_{n-1}].$$

A group $G$ is said to be ***solvable***[39] 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'll define the derived subgroup of an algebraic group, and we'll call an algebraic group solvable if the similar sequence terminates with $\{1\}$. Then we'll study the structure of solvable groups.

## Remarks on algebraic subgroups

Recall that, when $k = \overline{k}$, $G(k) \simeq \operatorname{spm} k[G]$, and the Zariski topology on $\operatorname{spm} k[G]$ defines a Zariski topology on $G(k)$. For any embedding of $G$ into $\mathrm{GL}_n$, this is the topology on $G(k)$ induced by the natural Zariski topology on $\mathrm{GL}_n(k)$.

PROPOSITION 11.1 *For an algebraic group $G$ over an algebraically closed field $k$, $H \leftrightarrow H(k)$ is a one-to-one correspondence between the smooth algebraic subgroups of $G$ and the Zariski-closed subgroups of $G(k)$.*

PROOF. Both correspond to reduced quotients of $k[G]$ compatible with its bialgebra structure. □

PROPOSITION 11.2 *Let $G$ be an algebraic group over a perfect field $k$, and let $\Gamma$ be the Galois group of $\overline{k}$ over $k$. Then $\Gamma$ acts on $G(\overline{k})$, and $H \leftrightarrow H(\overline{k})$ is a one-to-one correspondence between the smooth algebraic subgroups of $G$ and the Zariski-closed subgroups of $G(\overline{k})$ stable under $\Gamma$ (i.e., such that $\sigma H(\overline{k}) = H(\overline{k})$ for all $\sigma \in \Gamma$).*

PROOF. Both correspond to radical ideals $\mathfrak{a}$ in the $\overline{k}$-bialgebra $\overline{k}[G]$ stable under the action of $\Gamma$ (see AG 16.7, 16.8). □

[39] Because a polynomial is solvable in terms of radicals if and only if its Galois group is solvable (FT 5.29).

## Commutative groups are triangulizable

We first prove a result in linear algebra.

PROPOSITION 11.3 *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 for $V$ for which $S$ is contained in the group of upper triangular matrices, i.e., a basis $e_1, \dots, e_n$ such that*

$$\alpha(\langle e_1, \dots, e_i\rangle) \subset \langle e_1, \dots, e_i\rangle \text{ for all } i. \tag{45}$$

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 $A \in S$.

PROOF. We prove this by induction on the dimension of $V$. If every $\alpha \in S$ is a scalar multiple of the identity map, there is nothing to prove. Otherwise, there exists an $\alpha \in S$ and an eigenvalue $a$ for $\alpha$ such that the eigenspace $V_a \neq V$. Because every element of $S$ commutes with $\alpha$, $V_a$ is stable under the action of the elements of $S$.[40] 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 $\overline{e}_{m+1}, \dots, \overline{e}_n$ for $V/V_a$ such that

$$\alpha(\langle e_1, \dots, e_i\rangle) \subset \langle e_1, \dots, e_i\rangle$$
$$\alpha(\langle \overline{e}_{m+1}, \dots, \overline{e}_{m+i}\rangle) \subset \langle \overline{e}_{m+1}, \dots, \overline{e}_{m+i}\rangle$$

for all $i$. Write $\overline{e}_{m+i} = e_{m+i} + V_a$. Then $e_1, \dots, e_n$ is a basis for $V$ satisfying (45). □

PROPOSITION 11.4 *Let $V$ be a finite-dimensional vector space over an algebraically closed field $k$, and let $G$ be a commutative smooth algebraic subgroup of $\mathrm{GL}_V$. There exists a basis for $V$ for which $G$ is contained in $\mathbb{T}_n$.*

PROOF. We deduce this from (11.3), using the following fact (4.8):

> Let $G$ be an algebraic subgroup of $\mathrm{GL}_n$; when $k = \overline{k}$ and $G$ is smooth, $k[G]$ consists of the functions $G(k) \to k$ defined by elements of $k[\mathrm{GL}_n] = k[\dots, X_{ij}, \dots, \det(X_{ij})^{-1}]$.

Consider:

$$\begin{array}{ccc} G(k) & \hookrightarrow & \mathrm{GL}(V) \\ \vdots & & \downarrow\approx \\ \mathbb{T}_n(k) & \hookrightarrow & \mathrm{GL}_n(k) \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} k[G] & \twoheadleftarrow & k[\mathrm{GL}_V] \\ \uparrow & & \uparrow\approx \\ k[\mathbb{T}_n] & \twoheadleftarrow & k[\mathrm{GL}_n] \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} G & \hookrightarrow & \mathrm{GL}_V \\ \vdots & & \downarrow\approx \\ \mathbb{T}_n & \hookrightarrow & \mathrm{GL}_n \end{array}$$

The first square is a diagram of groups and group homomorphisms. We have used (11.3) to choose a basis for $V$ (hence an isomorphism $V \to k^n$) so that the dotted arrow exists.

The second square is the diagram of bialgebras and bialgebra homomorphisms corresponding to the first (cf. 4.4); the dotted arrow in the first square defines a homomorphism from $k[\mathbb{T}_n]$ to the quotient $k[G]$ of $k[\mathrm{GL}_V]$.

The third square is the diagram of algebraic groups defined by the second square. □

[40] Let $\beta \in S$, and let $x \in V_a$. Then

$$\alpha(\beta x) = \beta(\alpha x) = \beta a x = a(\beta x).$$

## Decomposition of a commutative algebraic group

DEFINITION 11.5 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. $g = g_u$).

Thus, $g$ is semisimple (resp. unipotent) if and only if $\varphi(g)$ is semisimple (resp. unipotent) for all representations $\varphi$ of $G$.

Theorem 10.1 shows that

$$G(k) = G(k)_s \times G(k)_u \text{ (cartesian product of sets)} \tag{46}$$

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 don't 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 (10.15). Thus, in his case (46) realizes $G(k)$ as a product of subgroups. We can do better.

THEOREM 11.6 *Every commutative smooth algebraic group $G$ over an algebraically closed field is a direct product of two algebraic subgroups*

$$G \simeq G_s \times G_u$$

*such that $G_s(k) = G(k)_s$ and $G_u(k) = G(k)_u$.*

PROOF. Choose an embedding $G \hookrightarrow \mathbb{T}_n$ for some $n$, and let $G_s = G \cap \mathbb{D}_n$ and $G_u = G \cap \mathbb{U}_n$. Because $G$ is commutative,

$$G_s \times G_u \to G \tag{47}$$

is a homomorphism with kernel $G_s \cap G_u$ (cf. §6). Because $\mathbb{D}_n \cap \mathbb{U}_n = \{1\}$ as algebraic groups[41], $G_s \cap G_u = \{1\}$, and because $G_s(k)G_u(k) = G(k)$ and $G$ is smooth, $G_s \times G_u \to G$ is a quotient map (6.18). Thus, it is an isomorphism. □

REMARK 11.7 Let $G$ be a smooth algebraic group over an algebraically closed field $k$. 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 $\mathrm{GL}_n$ for some $n$. A matrix $A$ is unipotent if and only if 1 is its only eigenvalue, i.e., 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.

ASIDE 11.8 In fact every commutative algebraic group over a perfect field decomposes into a product of a group of multiplicative type and a unipotent group (Waterhouse 1979, 9.5)

[41] $\mathbb{D}_n$ is defined as a subgroup of $\mathrm{GL}_n$ by the equations $X_{ij} = 0$ for $i \neq j$; $\mathbb{U}_n$ is defined by the equations $X_{ii} = 1$ etc. When combined, the equations certainly define the subgroup $\{I\}$ (in any ring).

## The derived group of algebraic group

DEFINITION 11.9 The ***derived group*** $\mathcal{D}G$ (or $G'$ or $G^{\mathrm{der}}$) of an algebraic group $G$ is the intersection of the normal algebraic subgroups $N$ of $G$ such that $G/N$ is commutative.

Thus (cf. §6), $\mathcal{D}G$ is the smallest normal algebraic subgroup of $G$ such that $G/\mathcal{D}G$ is commutative. We shall need another description of it, analogous to the description of the derived group as that generated by commutators.

As for groups, there exist maps of functors

$$G^2 \to G^4 \to \cdots \to G^{2n} \to G.$$

Let $I_n$ be the kernel of the homomorphism $k[G] \to k[G^{2n}]$ of $k$-algebras (not $k$-bialgebras) defined by $G^{2n} \to G$. Then

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \cdots$$

and we let $I = \bigcap I_n$.

PROPOSITION 11.10 *The coordinate ring of $\mathcal{D}G$ is $k[G]/I$.*

PROOF. From the diagram of set-valued functors

$$\begin{array}{ccccc} G^{2n} & \times & G^{2n} & \to & G^{4n} \\ \downarrow & & \downarrow & & \downarrow \\ G & \times & G & \xrightarrow{\text{mult}} & G \end{array}$$

we get a diagram of $k$-algebras

$$\begin{array}{ccccc} k[G]/I_n & \otimes_k & k[G]/I_n & \leftarrow & k[G]/I_{2n} \\ \uparrow & & \uparrow & & \uparrow \\ k[G] & \otimes_k & k[G] & \xleftarrow{\Delta} & k[G] \end{array}$$

(because $k[G]/I_n$ is the image of $k[G]$ in $k[G^{2n}]$ ). It follows that $\Delta\colon k[G] \to k[G]/I \otimes_k k[G]/I$ factors through $k[G] \to k[G]/I$, and defines a $k$-bialgebra structure on $k[G]/I$, which corresponds to the smallest algebraic subgroup $G'$ of $G$ such that $G'(R)$ contains all the commutators for all $R$. Clearly, this is the smallest normal subgroup such that $G/G'$ is commutative. □

COROLLARY 11.11 *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 11.12 *If $G$ is connected (resp. smooth), then $\mathcal{D}G$ is connected (resp. smooth).*

PROOF. Recall that an algebraic group $G$ is connected if and only if $k[G]$ has no idempotent $\neq 0, 1$ (see p67), and that a product of connected algebraic groups is connected (8.16). Since $k[G]/I_n \hookrightarrow k[G^{2n}]$, the ring $k[G]/I_n$ has no idempotent $\neq 0, 1$, and this implies that the same is true of $k[G]/I = k[\mathcal{D}G]$. A similar argument works for "smooth". □

COROLLARY 11.13 PROPOSITION 11.14 *Let $G$ be a smooth connected algebraic group. Then $k[\mathcal{D}G] = k[G]/I_n$ for some $n$, and $(\mathcal{D}G)(\bar{k}) = \mathcal{D}(G(\bar{k}))$.*

PROOF. As $G$ is connected and smooth, so also is $G^{2n}$ (8.16, 2.20). Therefore, each ideal $I_n$ is prime, and an ascending sequence of prime ideals in a noetherian ring terminates. This proves the first part of the statement.

Let $V_n$ be the image of $G^{2n}(\bar{k})$ in $G(\bar{k})$. Its closure in $G(\bar{k})$ is the zero-set of $I_n$. Being the image of a regular map, $V_n$ contains a dense open subset $U$ of its closure (AG 10.2). Choose $n$ as in the first part, so that the zero-set of $I_n$ is $\mathcal{D}G(\bar{k})$. Then

$$U \cdot U^{-1} \subset V_n \cdot V_n \subset V_{2n} \subset \mathcal{D}(G(\bar{k})) = \bigcup\nolimits_m V_m \subset \mathcal{D}G(\bar{k}).$$

It remains to show that $U \cdot U^{-1} = \mathcal{D}G(\bar{k})$. Let $g \in \mathcal{D}G(\bar{k})$. Because $U$ is open and dense $\mathcal{D}G(\bar{k})$, so is $gU^{-1}$, which must therefore meet $U$, forcing $g$ to lie in $U \cdot U$. □

## Definition of a solvable algebraic group

Write $\mathcal{D}^2G$ for $\mathcal{D}(\mathcal{D}G)$, etc..

DEFINITION 11.15 An algebraic group $G$ is ***solvable*** if the ***derived series***

$$G \supset \mathcal{D}G \supset \mathcal{D}^2G \supset \cdots$$

terminates with 1.

LEMMA 11.16 *An algebraic group $G$ is solvable if and only if it has a sequence of algebraic subgroups*

$$G \supset G_1 \supset \cdots \supset G_n = \{1\} \tag{48}$$

*with $G_{i+1}$ normal in $G_i$ for each $i$, and $G_i/G_{i+1}$ commutative.*

PROOF. If $G$ is solvable, then the derived series is such a sequence. Conversely, $G_1 \supset \mathcal{D}G$, so $G_2 \supset \mathcal{D}^2G$, etc.. □

EXAMPLE 11.17 Let $F$ be a finite group, and let $\underline{F}$ be the associated constant algebraic group (2.14). Then $\underline{F}$ is solvable if and only if $F$ is solvable. In particular, the theory of solvable algebraic groups includes the theory of solvable finite groups, which is quite complicated.

EXAMPLE 11.18 The group $\mathbb{T}_n$ of upper triangular matrices is solvable. For example,

$$\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\} \supset \left\{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\right\} \supset \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$$

and

$$\left\{\left(\begin{smallmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{smallmatrix}\right)\right\} \supset \left\{\left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right)\right\} \supset \left\{\left(\begin{smallmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\right\} \supset \left\{\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\right\}$$

demonstrate that $\mathbb{T}_2$ and $\mathbb{T}_3$ are solvable. In the first case, the quotients are $\mathbb{G}_m \times \mathbb{G}_m$ and $\mathbb{G}_a$, and in the second the quotients are $\mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$, $\mathbb{G}_a \times \mathbb{G}_a$, and $\mathbb{G}_a$.

More generally, let $G_0$ be the subgroup of $\mathbb{T}_n$ consisting of the matrices $(a_{ij})$ with $a_{ii} = 1$. Let $G_r$ be the subgroup of $G_0$ of matrices $(a_{ij})$ such that $a_{ij} = 0$ for $0 < j - i \leq r$. The map

$$(a_{ij}) \mapsto (a_{1,r+2}, \ldots, a_{i,r+i+1}, \ldots)$$

is a homomorphism from $G_r$ onto $\mathbb{G}_a \times \mathbb{G}_a \times \cdots$ with kernel $G_{r+1}$.

Alternatively, we can work abstractly. A ***full flag*** $F$ in a vector space $V$ of dimension $n$ is a sequence of subspaces

$$V = V_n \supset \cdots \supset V_i \supset V_{i-1} \supset \cdots \supset V_1 \supset \{0\}$$

with $V_i$ of dimension $i$. Let $\mathbb{T}$ be the algebraic subgroup of $\mathrm{GL}_V$ such that $\mathbb{T}(k)$ consists of the automorphisms preserving the flag, i.e., such that $\alpha(V_i) \subset V_i$. When we take $F$ to be the obvious flag in $k^n$, $G = \mathbb{T}_n$. Let $G_0$ be the algebraic subgroup of $G$ of $\alpha$ acting as $\mathrm{id}$ on the quotients $V_i/V_{i-i}$; more precisely,

$$G_0 = \mathrm{Ker}(G \to \prod \mathrm{GL}_{V_i/V_{i-i}}).$$

Then $G_0$ is a normal algebraic subgroup of $\mathbb{T}$ with quotient isomorphic to $\mathbb{G}_m^n$. Now define $G_r$ to be the algebraic subgroup of $G_0$ of elements $\alpha$ acting as $\mathrm{id}$ 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 11.19 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).

## Independence of characters

Let $\mathbb{G}_m$ be the subgroup of $\mathrm{GL}_n$ of scalar matrices, i.e., it is the subgroup defined by the equations

$$X_{ij} = 0 \text{ for } i \neq j;$$
$$X_{11} = X_{22} = \cdots = X_{nn}.$$

Then $a \in \mathbb{G}_m(R) = R^\times$ acts on $R^n$ as $(x_1, \ldots, x_n) \mapsto (ax_1, \ldots, ax_n)$.

Similarly, $\mathrm{GL}_V$ contains a subgroup $\mathbb{G}_m$ such that $a \in \mathbb{G}_m(R)$ acts on $R \otimes_k V$ by the homothety $v \mapsto av$. Under the isomorphism $\mathrm{GL}_V \to \mathrm{GL}_n$ defined by any basis of $V$, the $\mathbb{G}_m$'s correspond. In fact, $\mathbb{G}_m$ is the centre of $\mathrm{GL}_V$.

Now let $\varphi\colon G \to \mathrm{GL}_V$ be a representation of $G$ on $V$. If $\varphi$ factors through the centre $\mathbb{G}_m$ of $\mathrm{GL}_V$,

$$G \xrightarrow{\varphi} \mathbb{G}_m \subset \mathrm{GL}_V$$

then $\varphi$ is a character of $G$, and we say that $G$ *acts on $V$ through the character $\varphi$* (cf. p75). More generally, we say that $G$ acts on a subspace $W$ of $V$ through a character $\chi$ if $W$ is stable under $G$ and $G$ acts on $W$ through $\chi$. 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 $g \in G(k)$, $\varphi(g)w$ is a scalar multiple of $w$. For this reason, we also call $V_\chi$ an *eigenspace for $G$ with character $\chi$*.

Let $\varphi\colon G \to \mathrm{GL}_V$ be a representation of $G$ on $V$. If $G$ acts on a subspaces $W$ and $W'$ through a character $\chi$, then it acts on $W + W'$ through $\chi$. Therefore, there is a largest subspace $V_\chi$ of $V$ on which $G$ acts through $\chi$.

PROPOSITION 11.20 *Assume $G$ is smooth. If $V$ is a sum of spaces $V_\chi$, then it is a direct sum. In other words, vectors lying in eigenspaces corresponding to $\chi$'s are linearly independent.*

PROOF. As we saw in §9, characters of $G$ correspond to group-like elements of $k[G]$. If $\chi \leftrightarrow a(\chi)$, then the representation $\rho$ of $G$ on $V_\chi$ is given by $\rho(v) = v \otimes a(\chi)$.

Suppose $V = V_{\chi_1} + \cdots + V_{\chi_r}$ with the $\chi_i$ distinct characters of $G$. If the sum is not direct, then there exists a relation

$$v_1 + \cdots + v_s = 0, \quad v_i \in V_{\chi_i}, \quad v_i \neq 0. \tag{49}$$

Then

$$0 = \sum \rho(v_i) = \sum v_i \otimes a(\chi_i)$$

which contradicts the linear independence of the $a(\chi_i)$ (see 9.8). □

REMARK 11.21 In characteristic zero, there is the following more direct proof. We may assume $k = \overline{k}$. On applying $g \in G(k)$ to (49), we get a new relation

$$\chi_1(g)v_1 + \cdots + \chi_{s-1}(g)v_{s-1} + \chi_s(g)v_s = 0. \tag{50}$$

As $\chi_s \neq \chi_{s-1}$, there exists a $g \in G(k)$ such that $\chi_s(g) \neq \chi_{s-1}(g)$. Multiply (50) by $\chi_s(g)^{-1}$ and subtract from (49). This will give us a new relation of the same form but with fewer terms. Continuing in this fashion, we arrive at a contradiction. [Perhaps this argument works more generally.]

We saw in §9 that if $G$ is a split torus, $V$ is always a sum of the eigenspace $V_\chi$. In general, this will be far from true. For example, $\mathrm{SL}_n$ has no nontrivial characters.

## The Lie-Kolchin theorem

THEOREM 11.22 *Let $G$ be an algebraic subgroup of $\mathrm{GL}_V$. If $G$ is connected, smooth, and solvable, and $k$ is algebraically closed, then there exists a basis for $V$ such that $G \subset \mathbb{T}_n$.*

Before proving this, it will be useful to see that the hypotheses are really needed.

**solvable** As $\mathbb{T}_n$ is solvable (11.18) and a subgroup of a solvable group is obviously solvable, this is necessary.

$k$ **algebraically closed** If $G(k) \subset \mathbb{T}_n(k)$, then the elements of $G(k)$ have a common eigenvector, namely, $e_1 = (1\ 0\ \cdots\ 0)^t$. Unless $k$ is algebraically closed, an endomorphism need not have an eigenvector, and, for example,

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R}, \quad a^2 + b^2 = 1 \right\}$$

is an commutative algebraic group over $\mathbb{R}$ that is not triangulizable over $\mathbb{R}$.

**connected** The group $G$ of monomial $2 \times 2$ matrices is solvable but no triagonalizable. The only common eigenvectors of $\mathbb{D}_2(k) \subset G(k)$ are $e_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $e_2 = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, but the monomial matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ interchanges $e_1$ and $e_2$, and so there is no common eigenvector for the elements of $G(k)$.

PROOF. By the argument in the proof of (11.4), it suffices to show that there exists a basis for $V$ such that $G(k) \subset \mathbb{T}_n(k)$.

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 11.3).

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 (11.4). Let $N = \mathcal{D}G$.

Its derived series is one shorter than that of $G$, and so we can assume that the elements of $N$ have a common eigenvector, i.e., for some character $\chi$ of $N$, the space $V_\chi$ (for $N$) is nonzero.

Let $W$ be the sum of the nonzero eigenspaces $V_\chi$ for $N$. According to (11.20), the sum is direct,

$$W = \bigoplus V_\chi$$

and so the set $\{V_\chi\}$ of nonzero eigenspaces for $N$ is finite.

Let $x \in V_\chi$ for some $\chi$, 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 $\chi' = (n \mapsto \chi(g^{-1}ng))$ of $N$. This shows that $G(k)$ permutes the finite set $\{V_\chi\}$.

Choose a $\chi$ and let $H$ be the stabilizer of $V_\chi$ in $G(k)$. Thus, $H$ is a subgroup of finite index in $G(k)$. Moreover, it is closed for the Zariski topology on $G(k)$ because it is the set where the characters $\chi$ and $\chi'$ coincide. But every closed subgroup of finite index of a topological group is open[42], and so $H$ is closed and open in $G(k)$. But $G(k)$ is connected for the Zariski topology (8.19), and so $G(k) = H$. This shows that $W = V_\chi$, and so $G(k)$ stabilizes $V_\chi$.

An element $n \in N(k)$ acts on $V_\chi$ as the homothety $x \mapsto \chi(n)x$, $\chi(n) \in k$. But each element $n$ of $N(k)$ is the commutator $n = [x, y]$ of two elements of $G(k)$ (see 11.14), and so $n$ acts on $V_\chi$ as an automorphism of determinant 1. This shows that $\chi(n)^{\dim V_\chi} = 1$, and so the image of $\chi\colon G \to \mathbb{G}_m$ is finite. Because $N$ is connected, this shows that $N(k)$ in fact acts trivially[43] on $V_\chi$. Hence $G(k)$ acts on $V_\chi$ through the quotient $G(k)/N(k)$, which is commutative. In this case, we know there is a common eigenvalue (11.3). □

## Unipotent groups

There is the following statement in linear algebra.

PROPOSITION 11.23 *Let $V$ be a finite-dimensional vector space, and let $G$ be a subgroup of $\mathrm{GL}(V)$ consisting of unipotent endomorphisms. Then there exists a basis for $V$ for which $G$ is contained in $\mathbb{U}_n$ (in particular, $G$ is solvable).*

PROOF. Waterhouse 1979, 8.2. □

PROPOSITION 11.24 *The following conditions on an algebraic group $G$ are equivalent:*

(a) *in 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 $k[G]$-comodule);*
(b) *$G$ is isomorphic to a subgroup of $\mathbb{U}_n$ for some $n$; and*
(c) *for smooth $G$, $G(\overline{k})$ consists of unipotent elements.*

PROOF. Waterhouse 1979, 8.3. [As in the proof of ((11.4), (c) implies that (b).] □

DEFINITION 11.25 An algebraic group $G$ is ***unipotent*** if it satisfies the equivalent conditions of (11.24).

[42] Because it is the complement of finite set of cosets, each of which is also closed.

[43] In more detail, the argument shows that the character $\chi$ takes values in $\mu_m \subset \mathbb{G}_m$ where $m = \dim V_\chi$. If $k$ has characteristic zero, or characteristic $p$ and $p \not| m$, then $\mu_m$ is étale, and so, because $N$ is connected, $\chi$ is trivial. If $p|m$, the argument only shows that $\chi$ takes values in $\mu_{p^r}$ 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.

## Structure of solvable groups

THEOREM 11.26 *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 $k = \overline{k}$. Embed $G$ into $\mathbb{T}_n$ for some $n$, and construct

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{U}_n & \longrightarrow & \mathbb{T}_n & \longrightarrow & \mathbb{D}_n & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & G_u & \longrightarrow & G & \longrightarrow & T & \longrightarrow & 1 \end{array}$$

where $G_u = \mathbb{U}_n \cap G$ and $T$ is the image of $G$ in $\mathbb{D}_n$. 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 (11.6)

$$Q \simeq Q_u \times Q_s.$$

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{D}G & \longrightarrow & G_u & \longrightarrow & \pi_0(G_u) & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathcal{D}G & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & T & \longrightarrow & Q/\pi G_u & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & 1 & & 1 & & \end{array}$$

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 (8.27)

$$Q_u, \mathcal{D}G \text{ connected} \implies G_u \text{ connected}.$$

For the uniqueness, note that $G_u$ is the largest connected normal unipotent subgroup of $G$, or that $G_u(\overline{k})$ consists of the unipotent elements of $G(\overline{k})$ (and apply (11.1)).

When $k$ is only perfect, the uniqueness of $(G_{\overline{k}})_u$ implies that it is stable under $\Gamma$, and hence arises from a unique algebraic subgroup $G_u$ of $G$ (11.2), which clearly has the required properties. □

## Tori in solvable groups

PROPOSITION 11.27 *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. Humphreys 1975, 19.2). □

PROPOSITION 11.28 *The centralizer of any torus in a connected smooth solvable group $G$ is connected.*

PROOF. Omitted for the present (cf. Humphreys 1975, 19.4). □

## The radical of an algebraic group

LEMMA 11.29 *(a) Algebraic subgroups and quotient groups of solvable algebraic groups are solvable.*

*(b) Let $N$ be a normal algebraic subgroup of $G$. If $N$ and $G/N$ are solvable, then so also is $G$.*

*(c) Let $N$ and $H$ be algebraic subgroups of $G$ with $N$ normal. If $H$ and $N$ are solvable (resp. connected), then $HN$ is solvable (resp. connected).*

PROOF. Only (c) is requires proof. The quotient $HN/N$ is solvable (resp. connected) because it is isomorphic to $H/H\cap N$ (see 6.24), and so this follows from (b) (resp. 8.27).□

It follows from (c) that for any algebraic algebraic group $G$ over a perfect field $k$, there exists a unique largest connected normal smooth solvable subgroup, which is called the ***radical*** $RG$ of $G$. The ***unipotent radical*** of $G$ is defined to be $R_uG = (RG)_u$.

## Structure of a general (affine) algebraic group

DEFINITION 11.30 A smooth connected algebraic group $G \neq 1$ is ***semisimple*** it has no smooth connected normal commutative subgroup other than the identity, and it is ***reductive*** if the only such subgroups are tori.

For example, $\mathrm{SL}_n$, $\mathrm{SO}_n$, $\mathrm{Sp}_n$ are semisimple, and $\mathrm{GL}_n$ is reductive.

PROPOSITION 11.31 *Let $G$ be a smooth connected algebraic group over a perfect field $k$.*

(a) *$G$ is semisimple if and only if $RG = 0$.*

(b) *$G$ is reductive if and only if $R_uG = 0$.*

PROOF. (a) If $RG = 0$, then obviously $G$ is semisimple. For the converse, we use that, for any algebraic group $G$, $RG$ and $\mathcal{D}G$ are ***characteristic subgroups***, i.e., every automorphism of $G$ maps $RG$ onto $RG$ and $\mathcal{D}G$ onto $\mathcal{D}G$. This is obvious from their definitions: $RG$ is the largest connected normal solvable algebraic subgroup and $\mathcal{D}G$ is the smallest normal algebraic subgroup such that $G/\mathcal{D}G$ is commutative. Therefore the chain

$$G \supset RG \supset \mathcal{D}(RG) \supset \mathcal{D}^2(RG) \supset \cdots \supset \mathcal{D}^r(RG) \supset 1$$

is preserved by every automorphism of $G$. In particular, the groups are normal in $G$.

(b) Similar. □

REMARK 11.32 If one of the conditions, commutative, connected, normal, smooth, is dropped, then a semisimple group may have such a subgroup. For example, $\mathrm{SL}_2$ has the commutative normal subgroup $\{\pm I\}$ and the commutative connected subgroup $\mathbb{U}_2$. Moreover, $\mathrm{SL}_2\times\mathrm{SL}_2$ is semisimple, but it has the connected normal subgroup $\{1\}\times\mathrm{SL}_2$. Finally, over a field of characteristic 2, $\mathrm{SL}_2$ has the connected normal commutative subgroup $\mu_2$.

EXAMPLE 11.33 Let $G$ be the group of invertible matrices $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$. The unipotent radical of $G$ is the subgroup of matrices $\begin{pmatrix} I & B \\ 0 & I \end{pmatrix}$. The quotient of $G$ by $R_uG$ is isomorphic to the reductive group of invertible matrices of the form $\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$, i.e., to $\mathrm{GL}_m \times \mathrm{GL}_n$. The radical of this is $\mathbb{G}_m \times \mathbb{G}_m$.

ASIDE 11.34 A representation $G \to \mathrm{GL}(V)$ is said to be ***semisimple*** (or ***completely reducible***) if every stable subspace $W$ has a stable complement $W'$ (so $V$ is a direct sum $V = W \oplus W'$ of representations), or, equivalently, if $V$ is a direct sum of ***simple*** (i.e., ***irreducible***) representations (those with no proper nonzero subrepresentations). For example, the action of $\mathbb{U}_2$ on $k^2$,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ay \\ y \end{pmatrix},$$

is not semisimple because the only stable one-dimensional subspace is the $x$-axis (the map is a shear). In general, representations of unipotent groups are not semisimple; nor should you expect the representations of a group containing a normal unipotent group to be semisimple. However, in characteristic zero, a connected algebraic group is reductive if and only if all of its representations are semisimple (15.6). In characteristic $p$, a connected algebraic group is reductive if and only if it is a torus.

## Exercises

11-1 Give a geometric proof that $G$ connected implies $\mathcal{D}G$ connected. [Show that the image of connected set under a continuous map is connected (for the Zariski topology, say), the closure of a connected set is connected, and a nested union of connected sets is connected sets is connected; then apply the criterion (8.19).]

11-2 Show that if $1 \to N \to G \to Q \to 1$ is exact, so also is $\pi_0(N) \to \pi_0(G) \to \pi_0(Q) \to 1$ (in an obvious sense). Give an example to show that $\pi_0(N) \to \pi_0(G)$ need not be injective.

# 12 The Lie algebra of an algebraic group: basics

According to any definition, an algebraic group gives a functor from $k$-algebras to groups. The Lie algebra of the algebraic group is detemined by the value of the functor on only the $k$-algebra of dual numbers, but nevertheless contains a surprisingly large amount of information about the group. Since the study of Lie algebras is little more than linear algebra, they are a valuable tool in the study of algebraic groups.

## Lie algebras: basic definitions

DEFINITION 12.1 A ***Lie algebra*** over a field $k$ is a finite-dimensional vector space $V$ over $k$ together with a $k$-bilinear map

$$[\ ,\ ]: L \times L \to L$$

(called the ***bracket***) such that

(a) $[x, x] = 0$ for all $x \in L$,

(b) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in L$.

A ***homomorphism of Lie algebras*** is a $k$-linear map $\alpha: L \to L'$ such that

$$[\alpha(x), \alpha(y)] = \alpha([x, y])$$

for all $x, y \in L$.

Condition (b) is called the ***Jacobi identity***. Note that (a) applied to $[x+y, x+y]$ implies that

$$[x, y] = -[y, x], \text{ for all } x, y \in L.$$

A ***Lie subalgebra*** of a Lie algebra $\mathfrak{g}$ is a $k$-subspace $\mathfrak{s}$ such that $[x, y] \in \mathfrak{s}$ whenever $x, y \in \mathfrak{s}$.

EXAMPLE 12.2 Let $\mathfrak{gl}_n$ be space of all $n \times n$ matrices with entries in $k$, and let

$$[A, B] = AB - BA.$$

Then obviously $[A, A] = 0$ and a calculation shows that it satisfies the Jacobi identity. 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 once with a minus sign.

A subspace $\mathfrak{a}$ of $\mathfrak{g}$ is an ***ideal*** if $[\mathfrak{g}, \mathfrak{a}] \subset \mathfrak{a}$, i.e., if $[x, a] \in \mathfrak{a}$ for all $x \in \mathfrak{g}$ and $a \in \mathfrak{a}$. The kernel of a homomorphism of Lie algebras is an ideal, and every ideal is the kernel of a homomorphism: given an ideal $\mathfrak{a}$ in $\mathfrak{g}$, define a bracket on the quotient vector space $\mathfrak{g}/\mathfrak{a}$ by setting

$$[x + \mathfrak{a}, y + \mathfrak{a}] = [x, y] + \mathfrak{a}.$$

The factorization theorem holds: every homomorphism of Lie algebras factors into a quotient map and an injection. Moreover, the isomorphism theorem holds: let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$ and $\mathfrak{a}$ an ideal in $\mathfrak{g}$; 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

$$x + \mathfrak{h} \cap \mathfrak{a} \mapsto x + \mathfrak{a}: \mathfrak{h}/\mathfrak{h} \cap \mathfrak{a} \to \mathfrak{h}\mathfrak{a}/\mathfrak{a}$$

is an isomorphism.

## 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***:

$$k[\varepsilon] = k[X]/(X^2).$$

Thus $k[\varepsilon] = k \oplus k\varepsilon$ as a $k$-vector space and $\varepsilon^2 = 0$. There are homomorphisms of $k$-algebras

$$k \xrightarrow{a \mapsto a+0\varepsilon} k[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} k$$

If $a \neq 0$, then $a + b\varepsilon = a(1 + \frac{b}{a}\varepsilon)$ has inverse $a^{-1}(1 - \frac{b}{a}\varepsilon)$, and so

$$k[\varepsilon]^\times = \{a + b\varepsilon \mid a \neq 0\}.$$

DEFINITION 12.3 For an algebraic group $G$ over $k$,

$$\mathrm{Lie}(G) = \mathrm{Ker}(G(k[\varepsilon]) \to G(k)).$$

Shortly we'll see that this has a natural structure of a Lie algebra.

EXAMPLE 12.4 Take $G = \mathrm{GL}_n$. Note that, for any $n \times n$ matrix $A$,

$$(I_n + \varepsilon A)(I_n - \varepsilon A) = I_n.$$

Thus, $I_n + \varepsilon A \in \mathrm{Lie}(\mathrm{GL}_n)$, and every element of $\mathrm{Lie}(\mathrm{GL}_n)$ is of this form. The map

$$I_n + \varepsilon A \mapsto A\colon \mathrm{Lie}(\mathrm{GL}_n) \to M_n(k)$$

is an isomorphism.

REMARK 12.5 An element of $\mathrm{Lie}(G)$ is a $k$-algebra homomorphism $\alpha\colon A \to k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0$ is $\epsilon$. Therefore, elements of $A$ not in the kernel $\mathfrak{m}$ of $\epsilon$ map to units in $k[\varepsilon]$, and so $\alpha$ factors uniquely through $A_{\mathfrak{m}}$. This shows that $\mathrm{Lie}(G)$ depends only on $A_{\mathfrak{m}}$. In particular, $\mathrm{Lie}(G^\circ) \simeq \mathrm{Lie}(G)$. Of course, experts will recognize $\mathrm{Lie}(G)$ as the tangent space to $G$ at the identity element.

### Description in terms of derivations

DEFINITION 12.6 Let $A$ be a $k$-algebra and $M$ an $A$-module. A $k$-***derivation*** is a $k$-linear map $D\colon A \to M$ such that

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad \text{(Leibniz rule)}.$$

For example, $D(1) = D(1 \times 1) = 2D(1)$and so $D(1) = 0$. By $k$-linearity, this implies that

$$D(c) = 0 \text{ for all } c \in k. \tag{51}$$

Conversely, every additive map $A \to M$ satisfying the Leibniz rule and zero on $k$ is a $k$-derivation.

Let $\alpha\colon A \to k[\varepsilon]$ be a $k$-algebra homomorphism, and write

$$\alpha(f) = \alpha_0(f) + \varepsilon\alpha_1(f).$$

From $\alpha(fg) = \alpha(f)\alpha(g)$, we find that

$$\alpha_0(fg) = \alpha_0(f)\alpha_0(g)$$
$$\alpha_1(fg) = \alpha_0(f)\alpha_1(g) + \alpha_0(g)\alpha_1(f).$$

When we use $\alpha_0$ to make $k$ into an $A$-module, the second condition says that $\alpha_1$ is a $k$-derivation $A \to k$.

By definition, the elements of $\mathrm{Lie}(G)$ are the $k$-algebra homomorphisms $k[G] \to k[\varepsilon]$ such that the composite

$$k[G] \xrightarrow{\alpha} k[\varepsilon] \xrightarrow{\varepsilon\mapsto 0} k$$

is $\epsilon$ (the $\epsilon$ that is part of the bialgebra structure on $k[G]$), i.e., such that $\alpha_0 = \epsilon$. Thus, we have proved the following statement.

PROPOSITION 12.7 *There is a natural one-to-one correspondence between the elements of* $\mathrm{Lie}(G)$ *and the $k$-derivations $A \to k$ ($A$ acting on $k$ through $\epsilon$).*

The correspondence is $\epsilon + \varepsilon D \leftrightarrow D$, and the Leibniz condition is

$$D(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f) \tag{52}$$

## The functor Lie

The description of $\mathrm{Lie}(G)$ in terms of derivations makes clear that it a functor from algebraic groups to $k$-vector spaces.

PROPOSITION 12.8 *There is a unique way of making $G \mapsto \mathrm{Lie}(G)$ into a functor to Lie algebras such that* $\mathrm{Lie}(\mathrm{GL}_n) = \mathfrak{gl}_n$.

Without the condition on $\mathrm{Lie}(\mathrm{GL}_n)$, we could, for example, take the bracket to be zero. It is clear from either description of Lie, that an embedding of algebraic groups $G \hookrightarrow H$ defines an injection $\mathrm{Lie}\, G \to \mathrm{Lie}\, H$. On applying this remark to an embedding of $G$ into $\mathrm{GL}_n$, we obtain the uniqueness assertion. The existence will be proved presently.

## Examples

EXAMPLE 12.9 When we expand out $\det(I + \varepsilon A)$ as a sum of $n!$ terms, the only nonzero term is

$$\prod(1 + \varepsilon a_{ii}) = 1 + \varepsilon \sum a_{ii}$$

because every other term includes at least two off-diagonal entries. Hence

$$\det(I + \varepsilon A) = 1 + \varepsilon \mathrm{trace}(A)$$

and so

$$\mathfrak{sl}_n \stackrel{\mathrm{df}}{=} \mathrm{Lie}(\mathrm{SL}_n) = \{I + \varepsilon A \mid \mathrm{trace}(A) = 0\}$$
$$\simeq \{A \in M_n(k) \mid \mathrm{trace}(A) = 0\}.$$

Certainly, $[A, B] = AB - BA$ has trace zero (even if $A$ and $B$ don't), and so $\mathfrak{sl}_n$ *is* a Lie subalgebra of $\mathfrak{gl}_n$.

EXAMPLE 12.10 As[44]

$$\mathbb{T}_n(k[\varepsilon]) = \left\{ \begin{pmatrix} a_1+* & * & \cdots & * & * \\ 0 & a_2+* & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n-1}+* & * \\ 0 & 0 & \cdots & 0 & a_n+* \end{pmatrix} \right\}$$

with $* \in \varepsilon k$, we see that

$$\mathfrak{t}_n \stackrel{\text{df}}{=} \text{Lie}(\mathbb{T}_n) \simeq \{(a_{ij}) \mid a_{ij} = 0 \text{ if } i > j\}.$$

Similarly,

$$\mathfrak{u}_n \stackrel{\text{df}}{=} \text{Lie}(\mathbb{U}_n) \simeq \{(a_{ij}) \mid a_{ij} = 0 \text{ if } i \geq j\}$$
$$\mathfrak{d}_n \stackrel{\text{df}}{=} \text{Lie}(\mathbb{D}_n) \simeq \{(a_{ij}) \mid a_{ij} = 0 \text{ if } i \neq j\}.$$

EXAMPLE 12.11 Assume the characteristic $\neq 2$, and let $\text{O}_n$ be orthogonal group:

$$\text{O}_n = \{A \in \text{GL}_n \mid A^t \cdot A = I\}$$

($A^t$ =transpose of $A$). This is the group of matrices preserving the quadratic form $X_1^2 + \cdots + X_n^2$. For $I + \varepsilon A \in M_n(k[\varepsilon])$,

$$(I + \varepsilon A)^t \cdot (I + \varepsilon A) = I + \varepsilon A^t + \varepsilon A,$$

and so

$$\begin{aligned} \text{Lie}(\text{O}_n) &= \{I + \varepsilon A \in M_n(k[\varepsilon]) \mid A^t + A = 0\} \\ &\simeq \{A \in M_n(k) \mid A^t + A = 0\}. \end{aligned}$$

Similarly, $\text{Lie}(\text{SO}_n)$ consists of the skew symmetric matrices with trace zero, but obviously the second condition is redundant, and so

$$\text{Lie}(\text{SO}_n) = \text{Lie}(O_n).$$

EXAMPLE 12.12 Let $G$ be a finite étale algebraic group, so $k[G]$ is a separable algebra. Every quotient of $k[G]$ is also separable, but the only separable subalgebra of $k[\varepsilon]$ is $k$. Therefore $G([k[\varepsilon]) = G(k)$, and $\text{Lie}(G) = 0$.

EXAMPLE 12.13 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 2.9). Thus $\alpha_p(k) = \{0\}$, and so

$$\text{Lie}(\alpha_p) = \alpha_p(k[\varepsilon]) = \{a\varepsilon \mid a \in k\} \simeq k.$$

Similarly, $\text{Lie}(\mu_p) \simeq k$.

[44]Recall that $\mathbb{T}_n$ is the subgroup of $\text{GL}_n$ defined by the equations $X_{ij} = 0$ for $i > j$.

EXAMPLE 12.14 Let $V$ be a vector space over $k$. Then $k[\varepsilon]\otimes_k V = V \oplus V\varepsilon$ as a $k$-vector space, with $\varepsilon$ acting as $x+\varepsilon y \mapsto \varepsilon x$, i.e., when we write $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ for $x+\varepsilon y$,

$$\varepsilon \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ x \end{smallmatrix}\right) = \varepsilon x.$$

Since

$$\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \beta & 0 \\ \delta & 0 \end{smallmatrix}\right)$$
$$\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ \alpha & \beta \end{smallmatrix}\right)$$

we see that the $k[\varepsilon]$-linear maps $k[\varepsilon]\otimes_k V \to k[\varepsilon]\otimes_k V$ are given by matrices $\left(\begin{smallmatrix} \alpha & 0 \\ \beta & \alpha \end{smallmatrix}\right)$, i.e., the $k[\varepsilon]$-linear maps are the maps $\alpha+\varepsilon\beta$ where $\alpha$ and $\beta$ are $k$-linear maps $V \to V$ and

$$(\alpha+\varepsilon\beta)(x+\varepsilon y) = \alpha(x) + \varepsilon(\alpha(y)+\beta(x)). \tag{53}$$

It follows that

$$\begin{aligned}\mathrm{Lie}(\mathrm{GL}_V) &= \{\mathrm{id}+\varepsilon\alpha \mid \alpha \in \mathrm{End}_{k\text{-lin}}(V)\}\\ &\simeq \mathrm{End}_{k\text{-lin}}(V).\end{aligned}$$

with the bracket

$$[\alpha,\beta] = \alpha\circ\beta - \beta\circ\alpha. \tag{54}$$

We denote this Lie algebra by $\mathfrak{gl}_V$.

Note that

$$(\mathrm{id}+\varepsilon\alpha)(x+\varepsilon y) = x+\varepsilon y+\varepsilon\alpha(x). \tag{55}$$

EXAMPLE 12.15 Let $\psi\colon V\times V \to k$ be a $k$-bilinear form, and let $G$ be the subgroup of $\mathrm{GL}_V$ of $\alpha$ preserving the form, i.e., such that

$$\psi(\alpha x,\alpha x') = \psi(x,x') \quad \text{all } x,x' \in V.$$

Then $\mathrm{Lie}(G)$ consists of the endomorphisms $\mathrm{id}+\varepsilon\alpha$ of $k[\varepsilon]\otimes_k V$ such that

$$\begin{aligned}\psi(x+\varepsilon y, x'+\varepsilon y') &= \psi((\mathrm{id}+\varepsilon\alpha)(x+\varepsilon y),(\mathrm{id}+\varepsilon\alpha)(x'+\varepsilon y'))\\ &= \psi(x+\varepsilon y+\varepsilon\cdot\alpha x, x'+\varepsilon y'+\varepsilon\cdot\alpha x')\\ &= \psi(x+\varepsilon y, x'+\varepsilon y') + \varepsilon(\psi(\alpha x,x')+\psi(x,\alpha x')),\end{aligned}$$

and so

$$\mathrm{Lie}(G) \simeq \{\alpha\in\mathrm{End}_{k\text{-lin}}(V) \mid \psi(\alpha x,x')+\psi(x,\alpha x') = 0 \text{ all } x,x'\in V\}.$$

The bracket is given by (54).

EXAMPLE 12.16 Let $G = D(M)$ (see p71), so that $G(R) = \mathrm{Hom}(M,R^\times)$. On applying $\mathrm{Hom}(M,-)$ to the exact sequence (of commutative groups)

$$0 \longrightarrow k \xrightarrow{a\mapsto 1+a\varepsilon} k[\varepsilon]^\times \xrightarrow{\varepsilon\mapsto 0} k^\times \longrightarrow 0,$$

we find that

$$\mathrm{Lie}(G) \simeq \mathrm{Hom}_{k\text{-lin}}(M,k) \simeq \mathrm{Hom}_{k\text{-lin}}(M,\mathbb{Z})\otimes_{\mathbb{Z}} k.$$

A split torus $T$ is the diagonalizable group associated with $M = X(T)$, and so

$$\mathrm{Lie}(T) \simeq \mathrm{Hom}_{k\text{-lin}}(X(T),k) \simeq \mathrm{Hom}_{k\text{-lin}}(X(T),\mathbb{Z})\otimes_{\mathbb{Z}} k.$$

Hence,

$$\mathrm{Hom}_{k\text{-lin}}(\mathrm{Lie}(T),k) \simeq k\otimes_{\mathbb{Z}} X(T).$$

## Extension of the base field

PROPOSITION 12.17 *For any extension $K$ of $k$, $\mathrm{Lie}(G_K) \simeq K \otimes_k \mathrm{Lie}(G)$.*

PROOF. We use the description of the Lie algebra in terms of derivations (12.8). Let $e_i$ be a basis for $A$ 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 $D: A \to k$ is a $k$-derivation, it suffices to check the Leibniz condition the elements of the basis. Therefore, $D$ is a $k$-derivation if and only if the scalars $c_i = D(e_i)$ satisfy

$$\sum\nolimits_k a_{ijk} c_k = \epsilon(e_i) c_j + \epsilon(e_j) c_i$$

for all $i, j$. This is a homogeneous system of linear equations in the $c_i$, and so[45] a basis for the solutions in $k$ is also a basis for the solutions in $K$. □

REMARK 12.18 Let $G$ be an algebraic group over $k$. For a $k$-algebra $R$, define

$$\mathfrak{g}(R) = \mathrm{Ker}(G(R[\varepsilon]) \to G(R))$$

where $R[\varepsilon] = R \otimes_k k[\varepsilon]$. Then, as in (12.7), $\mathfrak{g}(R)$ can be identified with the space of $k$-derivations $A \to R$ (with $R$ regarded as an $A$-module through $\epsilon$), and the argument in the proposition shows that

$$\mathfrak{g}(R) \simeq R \otimes_k \mathfrak{g}(k) \tag{56}$$

where $\mathfrak{g}(k) = \mathrm{Lie}(G)$.

## Definition of the bracket

An element $g \in G(k)$ defines an automorphism $\mathrm{inn}(g): x \mapsto gxg^{-1}$ of $G(R)$ for all $R$. In other words, there is a homomorphism

$$\mathrm{inn}: G(k) \to \mathrm{Aut}(G).$$

Because Lie is a functor, automorphisms of $G$ define automorphisms of $\mathrm{Lie}(G)$, and we get a homomorphism

$$\mathrm{Ad}: G(k) \xrightarrow{\mathrm{inn}} \mathrm{Aut}(G) \to \mathrm{Aut}(\mathrm{Lie}(G)).$$

Specifically, $g$ defines an element $g'$ of $G(k[\varepsilon])$ via $k \to k[\varepsilon]$, and the action of $\mathrm{inn}(g')$ on $G(k[\varepsilon])$ defines an automorphism of $\mathrm{Lie}(G) \subset G(k[\varepsilon])$.

[45] Let $S$ be the space of solutions of a system of homogeneous linear equations with coefficients in $k$. Then the space of solutions of the system of equations with coefficients in any $k$-algebra is $R \otimes_k S$. To see this, note that $S$ is the kernel of a linear map

$$0 \to S \to V \xrightarrow{\alpha} W$$

and that tensoring this sequence with $R$ gives an exact sequence

$$0 \to R \otimes_k S \to R \otimes_k V \xrightarrow{\mathrm{id}_R \otimes \alpha} R \otimes_k W.$$

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.

We can do this more generally: for any $k$-algebra $R$, an element $g \in G(R)$ defines an element $g'$ of $G(R[\varepsilon])$ via $R \to R[\varepsilon]$, and the action of $\mathrm{inn}(g')$ on $G(R[\varepsilon])$ defines an automorphism of $\mathfrak{g}(R)$. Therefore, we have a homomorphism

$$G(R) \to \mathrm{Aut}_{R\text{-lin}}(\mathfrak{g}(R)) \overset{(56)}{=} \mathrm{GL}_{\mathfrak{g}(k)}(R) \tag{57}$$

which is natural in $R$, i.e., a homomorphism of algebraic groups

$$G \to \mathrm{GL}_{\mathfrak{g}(k)}.$$

On applying the functor Lie to this, we get a homomorphism of $k$-vector spaces

$$\mathrm{ad}\colon \mathrm{Lie}\, G \to \mathrm{Lie}\, \mathrm{GL}_{\mathfrak{g}(k)} \overset{12.14}{\simeq} \mathrm{End}_{k\text{-lin}}(\mathfrak{g}(k)).$$

DEFINITION 12.19 For $A, X \in \mathrm{Lie}(G)$,

$$[A, X] = \mathrm{ad}(A)(X).$$

LEMMA 12.20 *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 $X + \varepsilon Y \in M_n \otimes_k k[\varepsilon]$ to give

$$(I + \varepsilon A)(X + \varepsilon Y)(I - \varepsilon A) = X + \varepsilon Y + \varepsilon(AX - XA).$$

On comparing this with (55), we see that $\mathrm{ad}(A)$ acts as $\mathrm{id} + \varepsilon\alpha$ where $\alpha(X) = AX - XA$. □

LEMMA 12.21 *The construction is functorial in $G$, i.e., the map $\mathrm{Lie}\, G \to \mathrm{Lie}\, H$ defined by a homomorphism of algebraic groups $G \to H$ is compatible with the two brackets.*

PROOF. The starting point of the proof is the observation that the homomorphisms (57) give a commutative diagram

$$\begin{array}{ccccc} G(R) & \times & \mathfrak{g}(R) & \to & \mathfrak{g}(R) \\ \downarrow & & \downarrow & & \downarrow \\ H(R) & \times & \mathfrak{h}(R) & \to & \mathfrak{h}(R). \end{array}$$

We leave the rest to the reader. □

Because the bracket $[A, X] = AX - XA$ on $\mathfrak{gl}_n$ satisfies the conditions in (12.1) and every $G$ can be embedded in $\mathrm{GL}_n$, the bracket on $\mathrm{Lie}(G)$ makes it into a Lie algebra. This completes the proof of (12.8).

## Alternative construction of the bracket.

Let $A = k[G]$, and consider the space $\mathrm{Der}_k(A, A)$ of $k$-derivations $A \to A$ (with $A$ regarded as an $A$-module in the obvious way). The composite of two $k$-derivations need not be a $k$-derivation, but their bracket

$$[D, D'] \overset{\mathrm{df}}{=} D \circ D' - D' \circ D$$

is, and it satisfies the Jacobi identity. One shows that the map $\mathrm{Der}_k(A, A) \to \mathrm{Der}_k(A, k)$ defined by $\epsilon\colon A \to k$ gives a bracket on $\mathrm{Der}_k(A, k)$ with the required properties (see Waterhouse 1979, Chapter 12).

## The unitary group

Let $K$ be a separable $k$-algebra of degree 2. There is a unique $k$-automorphism $a \mapsto \overline{a}$ of $K$ such that $a = \overline{a}$ if and only if $a \in k$. There are only two possibilities:

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

(b) $K = k \times k$ and $\overline{(a,b)} = (b,a)$.

For an $n \times n$ matrix $A = (a_{ij})$ with entries in $K$, define $\overline{A}$ to be $(\overline{a_{ij}})$ and $A^*$ to be the transpose of $\overline{A}$. 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 $\overline{a \otimes r} = \overline{a} \otimes r$ 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 $\mathrm{GL}_n$.

In case (a), let $e \in K \smallsetminus k$. Then $e$ satisfies a quadratic polynomial with coefficients in $k$. Assuming $\mathrm{char}(k) \neq 2$, we can "complete the square" and choose $e$ so that $e^2 \in k$ and $\overline{e} = -e$. 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

$$\begin{aligned} A^tA - e^2BB^t &= I \\ A^tB - B^tA &= 0. \end{aligned}$$

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

Note that, for a field extension $k \to k'$, $G_{k'}$ is the group obtained from the pair $(K' = K \otimes_k k', a \otimes c \mapsto \overline{a} \otimes c)$. In particular, $G_{\overline{k}} \simeq \mathrm{GL}_n$, and so is connected.

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 $K$.

When $k = \mathbb{R}$ and $K = \mathbb{C}$, $G$ is called the ***unitary group*** $U_n$. The subgroup of matrices with determinant 1 is the ***special unitary group*** $\mathrm{SU}_n$.

### Lie **preserves fibred products**

Recall (p15) that for any homomorphisms $G \to H \leftarrow G'$ of algebraic groups, there is an algebraic group $G \times_H G'$ such that $(G \times_H G')(R)$ consists of the pairs $g \in G(R)$, $g' \in G'(R)$ having the same image in $H(R)$. Thus, $\mathrm{Lie}(G \times_H G')$ consists of pairs $g \in G(k[\varepsilon])$, $g' \in G'(k[\varepsilon])$ having the same image in $H(k[\varepsilon])$ and mapping to 1 in $G(k)$ and $G'(k)$, i.e., of the pairs $g \in G(k[\varepsilon])$, $g' \in G'(k[\varepsilon])$ mapping to 1 in $G(k)$ and $G'(k)$ and having the same image in $H(k[\varepsilon])$. In other words,

$$\mathrm{Lie}(G \times_H G') = \mathrm{Lie}(G) \times_{\mathrm{Lie}(H)} \mathrm{Lie}(G'). \tag{58}$$

EXAMPLE 12.22 Let $k$ be a field of characteristic $p \neq 0$. Consider the homomorphisms

$$\mathbb{G}_m \xrightarrow{x \mapsto (1,x)} \mathbb{G}_m \times \mathbb{G}_m \xleftarrow{(y^p,y) \longleftarrow\!\shortmid\ y} \mathbb{G}_m.$$

They give the fibred product diagrams:

$$\begin{array}{ccc} \mu_p & \longrightarrow & \mathbb{G}_m \\ \downarrow & & \downarrow \\ \mathbb{G}_m & \longrightarrow & \mathbb{G}_m \times \mathbb{G}_m \end{array} \qquad \begin{array}{ccc} k & \xrightarrow{\mathrm{id}} & k \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle c \mapsto (0,c)} \\ k & \xrightarrow{c \mapsto (0,c)} & k \times k. \end{array}$$

EXAMPLE 12.23 Recall (6.14) that the kernel of a homomorphism $\alpha\colon G \to H$ of algebraic groups can be obtained as a fibred product:

$$\begin{array}{ccc} \mathrm{Ker}(\alpha) & \longrightarrow & \{1_H\} \\ \downarrow & & \downarrow \\ G & \xrightarrow{\alpha} & H \end{array}$$

Therefore (58) shows that

$$\mathrm{Lie}(\mathrm{Ker}(\alpha)) = \mathrm{Ker}(\mathrm{Lie}(\alpha)).$$

In other words, an exact sequence of algebraic groups $1 \to N \to G \to H$ gives rise to an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}\, N \to \mathrm{Lie}\, G \to \mathrm{Lie}\, H.$$

EXAMPLE 12.24 Let $G$ and $G'$ be algebraic subgroups of an algebraic group $H$. The algebraic subgroup $G \cap G'$ with $(G \cap G')(R) = G(R) \cap G'(R)$ (inside $H(R)$) is the fibred product of the inclusion maps, and so

$$\mathrm{Lie}(G \cap G') = \mathrm{Lie}(G) \cap \mathrm{Lie}(G').$$

For example, in (12.22), $\mathbb{G}_m$ and $\mathbb{G}_m$ can be regarded as subgroups of $\mathbb{G}_m \times \mathbb{G}_m$ with intersection $\mu_p$, and

$$\mathrm{Lie}(\mu_p) = \mathrm{Lie}(\mathbb{G}_m) \cap \mathrm{Lie}(\mathbb{G}_m)$$

(intersection inside $\mathbb{G}_m \times \mathbb{G}_m$).

REMARK 12.25 Example 12.22 shows that Lie does **not** preserve fibred products in the category of smooth algebraic groups.

### Commutative Lie algebras

A Lie algebra $\mathfrak{g}$ is said to be ***commutative*** (or ***abelian***) if $[x, y] = 0$ for all $x, y \in \mathfrak{g}$. Thus, to give a commutative Lie algebra amounts to giving a finite-dimensional vector space.

If $G$ is commutative, then $\mathrm{Lie}(G)$ is commutative. This can be seen directly from our definition of the bracket, or by observing that if $G$ is a commutative subgroup of $\mathrm{GL}_n$, then $\mathrm{Lie}(G)$ is a commutative subalgebra of $\mathrm{Lie}(\mathrm{GL}_n)$.

### Normal subgroups and ideals

A normal algebraic subgroup $N$ of an algebraic group $G$ is the kernel of a quotient map $G \to Q$ (see 6.22); therefore, $\mathrm{Lie}(N)$ is the kernel of a homomorphism of Lie algebras $\mathrm{Lie}\, G \to \mathrm{Lie}\, Q$ (see 12.23), and so is an ideal in $\mathrm{Lie}\, G$. Of course, this can also be proved directly.

# 13 The Lie algebra of an algebraic group

Following a standard convention, we usually write $\mathfrak{g}$ for $\mathrm{Lie}(G)$, $\mathfrak{h}$ for $\mathrm{Lie}(H)$, and so on.

### Some algebraic geometry

Recall the Noether normalization theorem:

THEOREM 13.1 *Every finitely generated algebra $A$ over a field $k$ contains a finite set $S$ of elements such that*

(a) *$k[S]$ is a polynomial ring in the elements of $S$, and*
(b) *$A$ is finitely generated as a $k[S]$-module.*

PROOF. For integral domains and infinite $k$'s, see AG 8.13; for the general case, see Waterhouse 1979, A.7. □

The number of elements of $S$ depends only on $A$. We define the ***dimension*** of $G$ to be this number for the ring $k[G]$.

REMARK 13.2 For any field $k'$ containing $k$, $\dim G = \dim G_{k'}$, and when $k$ is perfect, $\dim G = \dim G_{\mathrm{red}}$ (cf. 2.23). Thus, readers of AG may prefer the following equivalent definition: when $k$ is algebraically closed, the dimension of $G$ is the dimension of $\mathrm{Spm}\, k[G]/\mathfrak{N}$ in the sense of AG p40, and otherwise it is the dimension of $G_{\overline{k}}$.

THEOREM 13.3 *Let $H$ be an algebraic subgroup of a smooth connected algebraic group $G$. Then $\dim H \leq \dim G$, with equality if and only if $H = G$.*

PROOF. Since $k[G] \twoheadrightarrow k[H]$, $\dim H \leq \dim G$ (without the conditions on $G$). For a proof that $H \neq G$ implies $\dim H < \dim G$, see Waterhouse 1979, 12.4, or apply AG 2.26 noting that a connected algebraic group is automatically irreducible (8.19). □

THEOREM 13.4 *If*

$$1 \to N \to G \to Q \to 1$$

*is exact, then*

$$\dim G = \dim N + \dim Q.$$

PROOF. Note that $N \times G \simeq G \times_Q G$. Since $k[G \times_Q G] = k[G] \otimes_{k[Q]} k[G]$, it follows from the definition of dimension 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. Alternatively, apply AG 10.9(b). □

THEOREM 13.5 *For an algebraic group $G$, $\dim \mathrm{Lie}\, G \geq \dim G$, with equality if and only if $G$ is smooth.*

PROOF. We may suppose $k = \overline{k}$. Let $A = k[G]$. Then (cf. AG §5),

$$\mathrm{Lie}(G) \simeq \mathrm{Hom}_{k\text{-lin}}(\mathfrak{m}/\mathfrak{m}^2, k)$$

where $\mathfrak{m} = \mathrm{Ker}(A \xrightarrow{\epsilon} k)$. Therefore, $\dim \mathrm{Lie}(G) \geq \dim G$, with equality if and only if the local ring $A_{\mathfrak{m}}$ is regular (cf. 2.25). But (see 2.26, 2.27), $G$ is smooth if and only if $A_{\mathfrak{m}}$ is regular. □

## Applications

PROPOSITION 13.6 *Let $H$ be a smooth algebraic subgroup of a connected algebraic group $G$. If $\operatorname{Lie} H = \operatorname{Lie} G$, then $H = G$.*

PROOF. We have

$$\dim H \overset{H \text{ smooth}}{=} \dim \operatorname{Lie} H = \dim \operatorname{Lie} G \overset{13.5}{\geq} \dim G.$$

Now (13.3) implies that $\dim H = \dim \operatorname{Lie} G = \dim G$, and so $G$ is smooth (13.5) and $H = G$ (see 13.3). □

COROLLARY 13.7 *Assume $\operatorname{char}(k) = 0$ and $G$ is connected. A homomorphism $H \to G$ is a quotient map if $\operatorname{Lie} H \to \operatorname{Lie} G$ is surjective.*

PROOF. We know (6.22) that $H \to G$ factors into

$$H \to \overline{H} \to G$$

with $H \to \overline{H}$ a quotient map and $\overline{H} \to G$ an embedding. Correspondingly, we get a diagram

$$\operatorname{Lie} H \to \operatorname{Lie} \overline{H} \to \operatorname{Lie} G.$$

Because $\overline{H} \to G$ is an embedding, $\operatorname{Lie} \overline{H} \to \operatorname{Lie} G$ is injective (12.23) and hence is an isomorphism. As we are in characteristic zero, $\overline{H}$ is smooth (2.31), and so (13.6) shows that $\overline{H} = G$. □

COROLLARY 13.8 *Assume $\operatorname{char}(k) = 0$. If*

$$1 \to N \to G \to Q \to 1$$

*is exact and $Q$ is connected, then*

$$0 \to \operatorname{Lie}(N) \to \operatorname{Lie}(G) \to \operatorname{Lie}(Q) \to 0$$

*is exact.*

PROOF. The sequence $0 \to \operatorname{Lie}(N) \to \operatorname{Lie}(G) \to \operatorname{Lie}(Q)$ is exact (by 12.23), and the equality

$$\dim G \overset{13.4}{=} \dim N + \dim Q$$

implies a similar statement for the Lie algebras (by 2.31 and 13.5). This implies (by linear algebra) that $\operatorname{Lie}(G) \to \operatorname{Lie}(Q)$ is surjective. □

COROLLARY 13.9 *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* 1.

PROOF. We have seen that the Lie algebra of an étale group is zero (12.12). Conversely, if $\operatorname{Lie} G = 0$ then $\{1\} = G^\circ$ by (13.6), and so $G = \pi_0(G)$ (see 8.13). □

EXAMPLE 13.10 The embedding $\alpha_p \to \mathbb{G}_a$ defines an isomorphism $k \to k$ on Lie algebras. Thus, the condition that $H$ be smooth is necessary in the proposition, and the condition that $\mathrm{char}(k) = 0$ is necessary in the first two corollaries. The embedding $\mathrm{SO}_n \to O_n$ defines an isomorphism on the Lie algebras, and so it is necessary that $G$ be connected in the proposition.

PROPOSITION 13.11 *Assume* $\mathrm{char}(k) = 0$ *and $G$ is connected. The map $H \mapsto \mathrm{Lie}\, H$ from connected algebraic subgroups of $G$ to Lie subalgebras of* $\mathrm{Lie}\, G$ *is injective and inclusion preserving.*

PROOF. Let $H$ and $H'$ be connected algebraic subgroups of $G$. Then (see 12.24)

$$\mathrm{Lie}(H \cap H') = \mathrm{Lie}(H) \cap \mathrm{Lie}\, H').$$

If $\mathrm{Lie}(H) = \mathrm{Lie}(H')$, then

$$\mathrm{Lie}(H) = \mathrm{Lie}(H \cap H') = \mathrm{Lie}(H'),$$

and so (13.6)

$$H = H \cap H' = H'. \qquad \square$$

PROPOSITION 13.12 *Assume* $\mathrm{char}(k) = 0$. *Let $\alpha, \beta$ be homomorphisms of algebraic groups $G \to H$. If* $\mathrm{Lie}(\alpha) = \mathrm{Lie}(\beta)$ *and $G$ is connected, then $\alpha = \beta$.*

PROOF. The algebraic subgroup on which $\alpha$ and $\beta$ agree is

$$(\text{diagonal}) \cap G \times_H G.$$

The hypothesis implies that its Lie algebra is the Lie algebra of the diagonal, and so it equals the diagonal. $\square$

Thus, when $\mathrm{char}(k) = 0$, the functor $G \mapsto \mathrm{Lie}(G)$ from connected algebraic groups to Lie algebras is faithful. Of course, on étale algebraic groups (e.g., constant algebraic groups (2.14)), the functor is trivial.

## Stabilizers

LEMMA 13.13 *Let $G \to \mathrm{GL}_V$ be a representation of $G$, and let $W$ subspace of $V$. For a $k$-algebra $R$, define*

$$G_W(R) = \{g \in G(R) \mid g(W \otimes_k R) = W \otimes_k R\}.$$

*Then the functor $G_W$ is an algebraic subgroup of $G$.*

PROOF. Let $e_1, \dots, e_m$ be a basis for $W$, and extend it to a basis $e_1, \dots, e_n$ for $V$. Write

$$\rho(e_j) = \sum\nolimits_i e_i \otimes a_{ij}, \quad a_{ij} \in A.$$

For $g \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R)$,

$$ge_j = \sum e_i \otimes g(a_{ij})$$

(see (23)). Thus, $g(W \otimes_k R) \subset W \otimes_k R$ if and only if $g(a_{ij}) = 0$ for $j \le m, i > m$. Hence $G_W$ is represented by the quotient of $A$ by the ideal generated by $\{a_{ij} \mid j \le m, i > m\}$. $\square$

Recall that, for a finite-dimensional vector space $V$,

$$\mathfrak{gl}_V \stackrel{\text{df}}{=} \mathrm{Lie}(\mathrm{GL}_V) \simeq \mathrm{End}_{k\text{-lin}}(V).$$

A ***representation*** of a Lie algebra $\mathfrak{g}$ is a homomorphism $\alpha\colon \mathfrak{g} \to \mathfrak{gl}(V)$. Thus, for every $x \in \mathfrak{g}$, $\alpha(x)$ is a $k$-linear endomorphism of $V$, and

$$\alpha([x, y]) = \alpha(x)\alpha(y) - \alpha(y)\alpha(x).$$

Let $W$ be a subspace of $V$. The ***stabilizer*** $\mathfrak{g}_W$ of $W$ in $\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{g}$: if $\alpha(x)(W) \subset W$ and $\alpha(y)(W) \subset W$, then $\alpha([x, y])(W) \subset W$.

LEMMA 13.14 *For any representation $G \to \mathrm{GL}_V$,*

$$\mathrm{Lie}\, G_W = (\mathrm{Lie}\, G)_W.$$

PROOF. By definition, $\mathrm{Lie}\, G_W$ consists of the elements $\mathrm{id} + \varepsilon\alpha$ of $G(k[\varepsilon])$ such that

$$(\mathrm{id} + \varepsilon\alpha)(W + W\varepsilon) \subset W + W\varepsilon,$$

i.e., such that $\alpha(W) \subset W$. □

PROPOSITION 13.15 *If $W$ is stable under $G$, then it is stable under $\mathrm{Lie}(G)$, and the converse holds when $\mathrm{char}(k) = 0$ and $G$ is connected.*

PROOF. If $G = G_W$, then $(\mathrm{Lie}\, G)_W \stackrel{13.14}{=} \mathrm{Lie}\, G_W = \mathrm{Lie}\, G$. Conversely, if $W$ is stable under $\mathrm{Lie}(G)$, then

$$\mathrm{Lie}\, G_W \stackrel{13.14}{=} (\mathrm{Lie}\, G)_W = \mathrm{Lie}\, G,$$

and so $G_W = G$ provided $\mathrm{char}(k) = 0$ and $G$ is connected (13.6). □

## Isotropy groups

PROPOSITION 13.16 *Let $G \to \mathrm{GL}_V$ be a representation of $G$, and let $v \in V$. Let $G_v$ be the functor of $k$-algebras*

$$G_v(R) = \{g \in G(R) \mid g(v \otimes 1) = v \otimes 1\}.$$

*Then $G_v$ is an algebraic subgroup of $G$ (the **isotropy group** of $v$ in $G$), with Lie algebra*

$$\mathfrak{g}_v = \{x \in \mathfrak{g} \mid xv = 0\}.$$

*If $v$ is fixed by $G$, then it is fixed by $\mathfrak{g}$, and the converse holds when $\mathrm{char}(k) = 0$ and $G$ is connected.*

PROOF. The proofs are similar to those of (13.13,13.14,13.15). Note that $\mathrm{id} + \varepsilon\alpha \in \mathfrak{g}$ fixes $v \otimes 1 = v + 0\varepsilon \in V \otimes_k k[\varepsilon] = V \oplus V\varepsilon$ if and only if

$$\mathrm{id}(v) + \varepsilon\alpha(v) = v + 0\varepsilon,$$

i.e., if and only if $\alpha(v) = 0$. □

COROLLARY 13.17 *Let $W$ be a subspace of $V$. For a $k$-algebra $R$, define*

$$C_G(W)(R) = \{g \in G(R) \mid gw = w \text{ for all } w \in W\}.$$

*Then $C_G(W)$ is an algebraic subgroup of $G$ (the **centralizer** of $W$ in $G$), with Lie algebra*

$$c_{\mathfrak{g}}(W) = \{x \in \mathfrak{g} \mid xw = 0 \text{ for all } w \in W\}.$$

*If $G$ centralizes $W$ (i.e, $C_G(W) = G$), then $\mathfrak{g}$ centralizes it, and the converse holds when $\operatorname{char}(k) = 0$ and $G$ is connected.*

PROOF. For any (finite) set $S$ spanning $W$, $C_G(W) = \bigcap_{w\in S} G_w$, and so this follows from previous results. □

## Normalizers and centralizers

The ***centre*** of a Lie algebra $\mathfrak{g}$ is

$$z(\mathfrak{g}) = \{x \in \mathfrak{g} \mid [x, y] = 0 \text{ for all } y \in \mathfrak{g}\}.$$

If $x \in z(\mathfrak{g})$ and $y \in \mathfrak{g}$, then $[x, y] \in z(\mathfrak{g})$ because it is zero. Thus, $z(\mathfrak{g})$ is an ideal. For a subalgebra $\mathfrak{h}$ of $\mathfrak{g}$, the ***normalizer*** and ***centralizer*** of $\mathfrak{h}$ in $\mathfrak{g}$ are

$$n_{\mathfrak{g}}(\mathfrak{h}) = \{x \in \mathfrak{g} \mid [x, \mathfrak{h}] \subset \mathfrak{h}\}$$
$$c_{\mathfrak{g}}(\mathfrak{h}) = \{x \in \mathfrak{g} \mid [x, h] = 0 \text{ for all } h \in \mathfrak{h}\}.$$

PROPOSITION 13.18 *Let $G$ be an algebraic group. For an algebraic subgroup $H$ of $G$, let $N_G(H)$ and $C_G(H)$ be the functors*

$$N_G(H)(R) = N_{G(R)}(H(R)) \stackrel{df}{=} \{g \in G(R) \mid g \cdot H(R) \cdot g^{-1} = H(R)\}$$
$$C_G(H)(R) = C_{G(R)}(H(R)) \stackrel{df}{=} \{g \in G(R) \mid gh = hg \text{ for all } h \in H(R)\}.$$

(a) *The functors $N_G(H)$ and $C_G(H)$ are algebraic subgroups of $G$ (the **normalizer** and **centralizer** of $H$ in $G$).*
(b) *Assume $H$ is connected. Then*

$$\operatorname{Lie}(N_G(H)) \subset n_{\mathfrak{g}}(\mathfrak{h})$$
$$\operatorname{Lie}(C_G(H)) \subset c_{\mathfrak{g}}(\mathfrak{h})$$

*with equality when $\operatorname{char}(k) = 0$. If $H$ is normal in $G$, then $\mathfrak{h}$ is an ideal in $\operatorname{Lie}(G)$, and the converse holds when $\operatorname{char}(k) = 0$ and $G$ is connected. If $H$ lies in the centre of $G$, then $\mathfrak{h}$ lies in the centre of $\mathfrak{g}$, and the converse holds when $\operatorname{char}(k) = 0$ and $G$ is connected.*

PROOF. (a) Demazure and Gabriel 1970, II, §1, 3.7.
(b) Demazure and Gabriel 1970, II, §6, 2.1. □

COROLLARY 13.19 *For any connected algebraic group $G$, $\operatorname{Lie} Z(G) \subset z(\mathfrak{g})$, with equality when $\operatorname{char}(k) = 0$. If a connected algebraic group $G$ is commutative, then so also is $\mathfrak{g}$, and the converse holds when $\operatorname{char}(k) = 0$.*

PROOF. Since $Z(G) = C_G(G)$ and $z(\mathfrak{g}) = c_{\mathfrak{g}}(\mathfrak{g})$, the first statement follows from the proposition, and the second follows from the first. □

### A nasty example

Let $k$ be a field of characteristic $p \neq 0$. The following simple example illustrates some of the things that can go wrong in this case. Define $G$ to be the algebraic subgroup of $\mathrm{GL}_3$ 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 $G(\bar{k})$ is trivial. Thus,

$$\mathrm{Lie}(Z(G)_{\mathrm{red}}) \subsetneqq \mathrm{Lie}(Z(G)) \subsetneqq Z(\mathrm{Lie}(G)).$$

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

$$0 \times k = \mathrm{Lie}(Z(G)).$$

# 14 Semisimple algebraic groups and Lie algebras

Recall (11.30, 11.31) that a nontrivial smooth connected algebraic group is semisimple if it has no smooth connected normal commutative subgroup other than the identity, or, equivalently, if its radical is trivial.

## Semisimple Lie algebras

The ***derived series*** of a Lie algebra $\mathfrak{g}$ is

$$\mathfrak{g} \supset \mathfrak{g}' = [\mathfrak{g},\mathfrak{g}] \supset \mathfrak{g}'' = [\mathfrak{g}',\mathfrak{g}'] \supset \cdots .$$

A Lie algebra is said to be ***solvable*** if the derived series terminates with 0. Every Lie algebra contains a largest solvable ideal, called its ***radical*** $r(\mathfrak{g})$. A nonzero Lie algebra $\mathfrak{g}$ is ***semisimple*** if $r(\mathfrak{g}) = 0$, i.e., if $\mathfrak{g}$ has no nonzero solvable ideal. Similarly to the case of algebraic groups, this is equivalent to $\mathfrak{g}$ having no nonzero commutative ideal. (Humphreys 1972, 3.1.)

## Semisimple Lie algebras and algebraic groups

THEOREM 14.1 *Let $G$ be a connected algebraic group. If $\mathrm{Lie}(G)$ is semisimple, then $G$ is semisimple, and the converse is true when $\mathrm{char}(k) = 0$.*

PROOF. Suppose $\mathrm{Lie}(G)$ is semisimple, and let $N$ be a normal connected commutative subgroup of $G$ — we have to prove $N = 1$. But $\mathrm{Lie}(N)$ is a commutative ideal in $\mathrm{Lie}(G)$ (13.19), and so is zero. Hence $N = 1$ (see 13.9).

Conversely, suppose $G$ is semisimple, and let $\mathfrak{n}$ be a commutative ideal in $\mathfrak{g}$ — we have to prove $\mathfrak{n} = 0$. Let $G$ act on $\mathfrak{g}$ through the adjoint representation $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$, and let $H$ be the subgroup of $G$ whose elements fix those of $\mathfrak{n}$ (see 13.17). Then (ibid.), the Lie algebra of $H$ is

$$\mathfrak{h} = \{x \in \mathfrak{g} \mid [x,\mathfrak{n}] = 0\},$$

which contains $\mathfrak{n}$. Because $\mathfrak{n}$ is an ideal, so also is $\mathfrak{h}$:

$$[[h,x],n] = [h,[x,n]] - [x,[h,n]]$$

equals zero if $h \in \mathfrak{h}$ and $n \in \mathfrak{n}$. Therefore, $H^\circ$ is normal in $G$ (13.18), and so its centre $Z(H^\circ)$ is normal in $G$. Because $G$ is semisimple, $Z(H^\circ)^\circ = 1$, and so $z(\mathfrak{h}) = 0$ (13.19). But $z(\mathfrak{h}) \supset \mathfrak{n}$, which must therefore be zero. □

COROLLARY 14.2 *Assume $\mathrm{char}(k) = 0$. For a connected algebraic group $G$, $\mathrm{Lie}(R(G)) = r(\mathfrak{g})$.*

PROOF. From the exact sequence

$$1 \to RG \to G \to G/RG \to 1$$

we get an exact sequence (12.23)

$$1 \to \mathrm{Lie}(RG) \to \mathfrak{g} \to \mathrm{Lie}(G/RG) \to 1$$

in which $\mathrm{Lie}(RG)$ is solvable (obvious) and $\mathrm{Lie}(G/RG)$ is semisimple (14.1). Therefore $\mathrm{Lie}\, RG$ is the largest solvable ideal in $\mathfrak{g}$. □

## The map ad

For a $k$-vector space with a $k$-bilinear pairing

$$a, b \mapsto ab: C \times C \to C,$$

we write $\mathrm{Der}_k(C)$ for the space of $k$-derivations $C \to C$, i.e., $k$-linear maps $\delta: C \to C$ satisfying the Leibniz rule

$$\delta(ab) = a\delta(b) + \delta(a)b.$$

If $\delta$ and $\delta'$ are $k$-derivations, then $\delta \circ \delta'$ need not be, but $\delta \circ \delta' - \delta' \circ \delta$ is, and so $\mathrm{Der}_k(C)$ is a subalgebra of $\mathfrak{gl}(C)$, not $\mathrm{End}_{k\text{-lin}}(C)$.

For a Lie algebra $\mathfrak{g}$, the Jacobi identity says that the map $\mathrm{ad}(x) = (y \mapsto [x, y])$ is a derivation of $\mathfrak{g}$:

$$[x,[y,z]] = -[y,[z,x]] - [z,[x,y]] = [y,[x,z]] + [[x,y],z].$$

Thus, $\mathrm{ad}: \mathfrak{g} \to \mathrm{End}_{k\text{-lin}}(\mathfrak{g})$ maps into $\mathrm{Der}_k(\mathfrak{g})$. The kernel of ad is the centre of $\mathfrak{g}$.

THEOREM 14.3 *Let $k$ be of characteristic zero. If $\mathfrak{g}$ is semisimple, then* $\mathrm{ad}: \mathfrak{g} \to \mathrm{Der}_k(\mathfrak{g})$ *is surjective (and hence an isomorphism).*

The derivations of $\mathfrak{g}$ of the form $\mathrm{ad}(x)$ are often said to be ***inner*** (by analogy with the automorphisms of $G$ of the form $\mathrm{inn}(g)$). Thus the theorem says that all derivations of a semisimple Lie algebra are inner.

We discuss the proof of the theorem below (see Humphreys 1972, 5.3).

## The Lie algebra of $\mathrm{Aut}_k(C)$

Again, let $C$ be a finite-dimensional $k$-vector space with a $k$-bilinear pairing $C \times C \to C$.

PROPOSITION 14.4 *The functor*

$$R \mapsto \mathrm{Aut}_{k\text{-}alg}(R \otimes_k C)$$

*is an algebraic subgroup of* $\mathrm{GL}_C$.

PROOF. Choose a basis for $C$. Then an element of $\mathrm{Aut}_{k\text{-lin}}(R \otimes_k C)$ is represented by a matrix, and the condition that it preserve the algebra product is a polynomial condition on the matrix entries. [Of course, to be rigorous, one should write this out in terms of the bialgebra.] □

Denote this algebraic group by $\mathrm{Aut}_C$, so $\mathrm{Aut}_C(R) = \mathrm{Aut}_{k\text{-alg}}(R \otimes_k C)$.

PROPOSITION 14.5 *The Lie algebra of* $\mathrm{Aut}_C$ *is* $\mathfrak{gl}(C) \cap \mathrm{Der}_k(C)$.

PROOF. Let $\mathrm{id} + \varepsilon\alpha \in \mathrm{Lie}(\mathrm{GL}_C)$, and let $a + a'\varepsilon$, $b + b'\varepsilon$ be elements of $C \otimes_k k[\varepsilon] \simeq C \oplus C\varepsilon$. When we first apply $\mathrm{id} + \varepsilon\alpha$ 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 $\mathrm{id} + \varepsilon\alpha$ we get

$$ab + \varepsilon(ab' + a'b + \alpha(ab)).$$

These are equal if and only if $\alpha$ satisfies the Leibniz rule. □

## The map Ad

Let $G$ be a connected algebraic group. Recall (p102) that there is a homomorphism

$$\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}.$$

Specifically, $g \in G(R)$ acts on $\mathfrak{g} \otimes_k R \subset G(R[\varepsilon])$ as $\mathrm{inn}(g)$,

$$x \mapsto gxg^{-1}.$$

On applying Lie, we get a homomorphism

$$\mathrm{ad}\colon \mathrm{Lie}(G) \to \mathrm{Lie}(\mathrm{GL}_{\mathfrak{g}}) \simeq \mathrm{End}(\mathfrak{g}),$$

and we defined

$$[x, y] = \mathrm{ad}(x)(y).$$

LEMMA 14.6 *The homomorphism* Ad *has image in* $\mathrm{Aut}_{\mathfrak{g}}$*; in other words, for all* $g \in G(R)$*, the automorphism* $\mathrm{Ad}(g)$ *of* $\mathfrak{g} \otimes_k R$ *preserves the bracket. Therefore,* ad *maps into* $\mathrm{Der}_k(\mathfrak{g})$.

PROOF. Because of (3.8), it suffices to prove this for $G = \mathrm{GL}_n$. But $A \in \mathrm{GL}(R)$ acts on $\mathfrak{g} \otimes_k R = M_n(R)$ as

$$X \mapsto AXA^{-1}.$$

Now

$$\begin{aligned} A[X,Y]A^{-1} &= A(XY - YX)A^{-1} \\ &= AXA^{-1}AYA^{-1} - AYA^{-1}AXA^{-1} \\ &= [AXA^{-1}, AYA^{-1}]. \end{aligned}$$

□

LEMMA 14.7 *Let* $g \in G(k)$*. The functor* $C_G(g)$

$$R \mapsto \{g' \in G(R) \mid gg'g^{-1} = g'\}$$

*is an algebraic subgroup of* $G$ *with Lie algebra*

$$c_{\mathfrak{g}}(g) = \{x \in \mathfrak{g} \mid \mathrm{Ad}(g)(x) = x\}.$$

PROOF. Embed $G$ in $\mathrm{GL}_n$. If we can prove the statement for $\mathrm{GL}_n$, then we obtain it for $G$, because $C_G(g) = C_{\mathrm{GL}_n}(g) \cap G$ and $c_{\mathfrak{g}}(g) = c_{\mathfrak{gl}_n}(g) \cap \mathfrak{g}$.

Let $A \in \mathrm{GL}_n(k)$. Then

$$C_{\mathrm{GL}_n}(A)(R) = \{B \in \mathrm{GL}_n(R) \mid AB = BA\}.$$

Clearly this is a polynomial (even linear) condition on the entries of $B$. Moreover,

$$\begin{aligned} \mathrm{Lie}(C_{\mathrm{GL}_n}(A)) &= \{I + B\varepsilon \in \mathrm{Lie}(\mathrm{GL}_n) \mid A(I + B\varepsilon)A^{-1} = (I + B\varepsilon)\} \\ &\simeq \{B \in M_n \mid ABA^{-1} = B\}. \end{aligned}$$

□

PROPOSITION 14.8 *For a connected algebraic group $G$ over a field $k$ of characteristic zero, the kernel of* Ad *is the centre $Z(G)$ of $G$.*

PROOF. Clearly $Z \subset N = \mathrm{Ker}(\mathrm{Ad})$. It suffices[46] to prove $Z = N$ when $k = \overline{k}$. If $g \in N(k)$, then $c_{\mathfrak{g}}(g) = \mathfrak{g}$, and so $C_G(g) = G$ (by 14.7). Therefore $g \in Z(k)$. We have shown that $Z(k) = N(k)$, and this implies[47] that $Z = N$. □

THEOREM 14.9 *For a semisimple algebraic group $G$ over a field of characteristic zero, the sequence*

$$1 \to Z(G) \to G \to \mathrm{Aut}^\circ_{\mathfrak{g}} \to 1$$

*is exact.*

PROOF. On applying Lie to $\mathrm{Ad}: G \to \mathrm{Aut}_{\mathfrak{g}}$, we get

$$\mathrm{ad}: \mathfrak{g} \to \mathrm{Lie}(\mathrm{Aut}_{\mathfrak{g}}) \subset \mathrm{Der}(\mathfrak{g}).$$

But, according to (14.3), the map $\mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ is surjective, which shows that $\mathrm{ad}: \mathfrak{g} \to \mathrm{Lie}(\mathrm{Aut}_{\mathfrak{g}})$ is surjective, and implies that $\mathrm{Ad}: G \to \mathrm{Aut}^\circ_{\mathfrak{g}}$ is a quotient map (13.7). □

Recall that two semisimple groups $G_1$, $G_2$ are said to be isogenous if $G_1/Z(G_1) \approx G_2/Z(G_2)$. The theorem gives an inclusion

$$\{\text{semisimple algebraic groups}\}/\text{isogeny} \hookrightarrow \{\text{semisimple Lie algebras}\}/\text{isomorphism}.$$

In Humphreys 1972, there is a complete classification of the semisimple Lie algebras up to isomorphism over an algebraically closed field of characteristic zero, and all of them arise from algebraic groups. Thus this gives a complete classification of the semisimple algebraic groups up to isogeny. We will follow a slightly different approach which gives more information about the algebraic groups.

**For the remainder of this section, $k$ is of characteristic zero.**

## Interlude on semisimple Lie algebras

Let $\mathfrak{g}$ be a Lie algebra. A bilinear form $B: \mathfrak{g} \times \mathfrak{g} \to k$ on $\mathfrak{g}$ is said to be ***associative*** if

$$B([x, y], z) = B(x, [y, z]), \quad \text{all } x, y, z \in \mathfrak{g}.$$

LEMMA 14.10 *The orthogonal complement $\mathfrak{a}^\perp$ of an ideal $\mathfrak{a}$ in $\mathfrak{g}$ with respect to an associative form is again an ideal.*

PROOF. By definition

$$\mathfrak{a}^\perp = \{x \in \mathfrak{g} \mid B(a, x) = 0 \text{ for all } a \in \mathfrak{a}\} = \{x \in \mathfrak{g} \mid B(\mathfrak{a}, x) = 0\}.$$

Let $a' \in \mathfrak{a}^\perp$ and $g \in \mathfrak{g}$. Then, for $a \in \mathfrak{a}$,

$$B(a, [g, a']) = -B(a, [a', g]) = -B([a, a'], x) = 0$$

and so $[g, a'] \in \mathfrak{a}^\perp$. □

[46] Let $Q = N/Z$; if $Q_{\overline{k}} = 0$, then $Q = 0$.

[47] The map $k[N] \to \overline{k}[Z]$ is surjective — let $\mathfrak{a}$ be its kernel. Since $\cap \mathfrak{m} = 0$ in $k[N]$, if $\mathfrak{a} \neq 0$, then there exists a maximal ideal $\mathfrak{m}$ of $k[N]$ not containing $\mathfrak{a}$. Because $k = \overline{k}$, $k[N]/\mathfrak{m} \simeq k$ (AG 2.7), and the homomorphism $k[N] \to k[N]/\mathfrak{m} \to k$ is an element of $N(k) \smallsetminus Z(k)$.

The ***Killing form*** on $\mathfrak{g}$ is

$$\kappa(x,y) = \mathrm{Tr}_{\mathfrak{g}}(\mathrm{ad}(x)\circ\mathrm{ad}(y)).$$

That is, $\kappa(x,y)$ is the trace of the $k$-linear map

$$z \mapsto [x,[y,z]]\colon \mathfrak{g}\to\mathfrak{g}.$$

LEMMA 14.11 *The form*

$$\kappa(x,y) = \mathrm{Tr}_{\mathfrak{g}}(\mathrm{ad}(x)\circ\mathrm{ad}(y))$$

*is associative and symmetric.*

PROOF. It is symmetric because for matrices $A=(a_{ij})$ and $B=(b_{ij})$,

$$\mathrm{Tr}(AB) = \sum\nolimits_{i,j} a_{ij}b_{ji} = \mathrm{Tr}(BA).$$

By tradition, checking the associativity is left to the reader. □

EXAMPLE 14.12 The Lie algebra $\mathfrak{sl}_2$ consists of the $2\times 2$ matrices with trace zero. It has as basis the elements

$$x=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad h=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad y=\begin{pmatrix}0&0\\1&0\end{pmatrix},$$

and

$$[x,y]=h,\quad [h,x]=2x,\quad [h,y]=-2y.$$

Then

$$\mathrm{ad}x=\begin{pmatrix}0&-2&0\\0&0&1\\0&0&0\end{pmatrix},\quad \mathrm{ad}h=\begin{pmatrix}2&0&0\\0&0&0\\0&0&-2\end{pmatrix},\quad \mathrm{ad}y=\begin{pmatrix}0&0&0\\-1&0&0\\0&2&0\end{pmatrix}$$

and so the top row $(\kappa(x,x),\kappa(x,h),\kappa(x,y))$ of the matrix of $\kappa$ 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, $\kappa$ 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 $\kappa$ is $n^2-1\times n^2-1$, and so this is not something one would like to compute.

LEMMA 14.13 *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.,*

$$\kappa_{\mathfrak{g}}(x,y) = \kappa_{\mathfrak{a}}(x,y) \text{ all } x,y\in\mathfrak{a}.$$

PROOF. Let $\alpha$ be an endomorphism of a vector space $V$ such that $\alpha(V) \subset W$; then $\mathrm{Tr}_V(\alpha) = \mathrm{Tr}_W(\alpha|W)$, because when we choose a basis for $W$ and extend it to a basis for $V$, the matrix for $\alpha$ takes the form $\left(\begin{smallmatrix} A & B \\ 0 & 0 \end{smallmatrix}\right)$ where $A$ is the matrix of $\alpha|W$. If $x, y \in \mathfrak{a}$, then $\mathrm{ad}x \circ \mathrm{ad}y$ is an endomorphism of $\mathfrak{g}$ mapping $\mathfrak{g}$ into $\mathfrak{a}$, and so its trace (on $\mathfrak{g}$), $\kappa(x, y)$, equals

$$\mathrm{Tr}_{\mathfrak{a}}(\mathrm{ad}x \circ \mathrm{ad}y|\mathfrak{a}) = \mathrm{Tr}_{\mathfrak{a}}(\mathrm{ad}_{\mathfrak{a}}x \circ \mathrm{ad}_{\mathfrak{a}}y) = \kappa_{\mathfrak{a}}(x, y). \qquad \square$$

PROPOSITION 14.14 *(Cartan's Criterion). A Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}(V)$ is solvable if $\mathrm{Tr}_V(x \circ y) = 0$ for all $x \in [\mathfrak{g}, \mathfrak{g}]$ and $y \in \mathfrak{g}$.*

PROOF. If $\mathfrak{g}$ is solvable, then an analogue of the Lie-Kolchin theorem shows that, for some choice of a basis for $V$, $\mathfrak{g} \subset \mathfrak{t}_n$. Then $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{u}_n$ and $[[\mathfrak{g}, \mathfrak{g}], \mathfrak{g}] \subset \mathfrak{u}_n$, which implies the traces are zero. For the converse, which is what we'll need, see Humphreys 1972, 4.5, p20 (the proof is quite elementary, involving only linear algebra).[48] $\square$

COROLLARY 14.15 *If $\kappa([\mathfrak{g}, \mathfrak{g}], \mathfrak{g}) = 0$, then $\mathfrak{g}$ is solvable; in particular, if $\kappa(\mathfrak{g}, \mathfrak{g}) = 0$, then $\mathfrak{g}$ is solvable.*

PROOF. The map $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}(V)$ has kernel the centre $z(\mathfrak{g})$ of $\mathfrak{g}$, and the condition implies that its image is solvable. Therefore $\mathfrak{g}$ is solvable. $\square$

THEOREM 14.16 *(Cartan-Killing criterion). A nonzero Lie algebra $\mathfrak{g}$ is semisimple if and only if its Killing form is nondegenerate, i.e., the orthogonal complement of $\mathfrak{g}$ is zero.*

PROOF. $\Longrightarrow$ : Let $\mathfrak{a}$ be the orthogonal complement of $\mathfrak{g}$,

$$\mathfrak{a} = \{x \in \mathfrak{g} \mid \kappa(\mathfrak{g}, x) = 0\}.$$

It is an ideal (14.10), and certainly

$$\kappa(\mathfrak{a}, \mathfrak{a}) = 0$$

and so it is solvable by (14.13) and (14.15). Hence, $\mathfrak{a} = 0$ if $\mathfrak{g}$ is semisimple.

$\Longleftarrow$ : Let $\mathfrak{a}$ be a commutative ideal of $\mathfrak{g}$. Let $a \in \mathfrak{a}$ and $g \in \mathfrak{g}$. Then

$$\mathfrak{g} \xrightarrow{\mathrm{ad}g} \mathfrak{g} \xrightarrow{\mathrm{ad}a} \mathfrak{a} \xrightarrow{\mathrm{ad}g} \mathfrak{a} \xrightarrow{\mathrm{ad}a} 0.$$

Therefore, $(\mathrm{ad}a \circ \mathrm{ad}g)^2 = 0$, and so[49] $\mathrm{Tr}(\mathrm{ad}a \circ \mathrm{ad}g) = 0$. In other words, $\kappa(\mathfrak{a}, \mathfrak{g}) = 0$, and so $\mathfrak{a} = 0$ if $\kappa$ is nondegenerate. $\square$

A Lie algebra $\mathfrak{g}$ is said to be a ***direct sum*** of ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ if it is a direct sum of them as subspaces, in which case we write $\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$. 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 Lie subalgebras $\mathfrak{a}_i$. A nonzero Lie algebra is ***simple*** if it is not commutative and has no proper nonzero ideals.

In a semisimple Lie algebra, the minimal nonzero ideals are exactly the ideals that are simple as Lie subalgebras (but a simple Lie subalgebra need not be an ideal).

[48] In Humphreys 1972, this is proved only for algebraically closed fields $k$, but this condition is obviously unnecessary since the statement is true over $k$ if and only if it is true over $\overline{k}$.

[49] If $\alpha^2 = 0$, the minimum polynomial of $\alpha$ divides $X^2$, and so the eigenvalues of $\alpha$ are zero.

THEOREM 14.17 *Every semisimple Lie algebra is a direct sum*

$$\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$$

*of its minimal nonzero ideals. In particular, there are only finitely many such ideals. Every ideal in* $\mathfrak{a}$ *is a direct sum of certain of the* $\mathfrak{a}_i$.

PROOF. Let $\mathfrak{a}$ be an ideal in $\mathfrak{g}$. Then the orthogonal complement $\mathfrak{a}^\perp$ of $\mathfrak{a}$ is also an ideal (14.10, 14.11), and so $\mathfrak{a} \cap \mathfrak{a}^\perp$ is an ideal. By Cartan's criterion (14.15), 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 and $\mathfrak{a}$ and $\mathfrak{a}^\perp$ are not simple (as Lie subalgebras) we can decompose them 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 $[\mathfrak{a}, \mathfrak{g}]$ is an ideal contained in $\mathfrak{a}$, and it is nonzero because $z(\mathfrak{g}) = 0$, and so $[\mathfrak{a}, \mathfrak{g}] = \mathfrak{a}$. On the other hand,

$$[\mathfrak{a}, \mathfrak{g}] = [\mathfrak{a}, \mathfrak{a}_1] \oplus \cdots \oplus [\mathfrak{a}, \mathfrak{a}_r],$$

and so $\mathfrak{a} = [\mathfrak{a}, \mathfrak{a}_i]$ for exactly one $i$. Then $\mathfrak{a} \subset \mathfrak{a}_i$, and so $\mathfrak{a} = \mathfrak{a}_i$ (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 $\mathfrak{g}$. The same argument shows that $\mathfrak{a}$ is the direct sum of the minimal nonzero ideals contained in $\mathfrak{a}$. □

COROLLARY 14.18 *All nonzero ideals and quotients of a semisimple Lie algebra are semisimple.*

PROOF. Obvious from the theorem. □

COROLLARY 14.19 *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 also true for direct sums of simple algebras. □

REMARK 14.20 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 commutative 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.

LEMMA 14.21 *For any Lie algebra* $\mathfrak{g}$*, the space* $\{\mathrm{ad}(x) \mid x \in \mathfrak{g}\}$ *of inner derivations of* $\mathfrak{g}$ *is an ideal in* $\mathrm{Der}_k(\mathfrak{g})$.

PROOF. Recall that $\mathrm{Der}_k(\mathfrak{g})$ is the space of $k$-linear endomorphisms of $\mathfrak{g}$ satisfying the Leibniz condition; it is made into a Lie algebra by $[\delta,\delta'] = \delta\circ\delta' - \delta'\circ\delta$. For a derivation $\delta$ of $\mathfrak{g}$ and $x, y \in \mathfrak{g}$,

$$\begin{aligned}[\delta, \mathrm{ad}x](y) &= (\delta\circ\mathrm{ad}(x) - \mathrm{ad}(x)\circ\delta)(y)\\ &= \delta([x,y]) - [x,\delta(y)]\\ &= [\delta(x),y] + [x,\delta(y)] - [x,\delta(y)]\\ &= [\delta(x),y].\end{aligned}$$

Thus,

$$[\delta, \mathrm{ad}(x)] = \mathrm{ad}(\delta x) \tag{59}$$

is inner. □

THEOREM 14.22 *If $\mathfrak{g}$ is semisimple, then $\mathrm{ad}\colon \mathfrak{g}\to\mathrm{Der}(\mathfrak{g})$ is a bijection: every derivation of $\mathfrak{g}$ is inner.*

PROOF. Let $\mathrm{ad}\mathfrak{g}$ denote the (isomorphic) image of $\mathfrak{g}$ in $\mathrm{Der}(\mathfrak{g})$. It suffices to show that the orthogonal complement $(\mathrm{ad}\mathfrak{g})^\perp$ of $\mathrm{ad}\mathfrak{g}$ in $D$ for $\kappa_D$ is zero.

Because $\mathrm{ad}\mathfrak{g}$ and $(\mathrm{ad}\mathfrak{g})^\perp$ are ideals in $\mathrm{Der}(\mathfrak{g})$ (see 14.21, 14.10),

$$[\mathrm{ad}\mathfrak{g}, (\mathrm{ad}\mathfrak{g})^\perp] \subset \mathrm{ad}\mathfrak{g}\cap(\mathrm{ad}\mathfrak{g})^\perp.$$

Because $\kappa_D|\mathrm{ad}\mathfrak{g} = \kappa_{\mathrm{ad}\mathfrak{g}}$ is nondegenerate (14.16),

$$\mathrm{ad}\mathfrak{g}\cap(\mathrm{ad}\mathfrak{g})^\perp = 0.$$

Let $\delta\in(\mathrm{ad}\mathfrak{g})^\perp$. For $x\in\mathfrak{g}$,

$$\mathrm{ad}(\delta x)\overset{(59)}{=}[\delta,\mathrm{ad}(x)] = 0.$$

As $\mathrm{ad}\colon\mathfrak{g}\to\mathrm{Der}(\mathfrak{g})$ is injective, this shows that $\delta x = 0$. Since this is true for all $x\in\mathfrak{g}$, $\delta = 0$. □

## Semisimple algebraic groups

A connected algebraic group $G$ is ***simple*** if it is noncommutative and has no normal algebraic subgroup except $G$ and 1, and it is ***almost simple*** if it is noncommutative and has no proper normal algebraic subgroup of dimension $> 0$. Thus, for $n > 1$, $\mathrm{SL}_n$ is almost simple and $\mathrm{PSL}_n =_{\mathrm{df}} \mathrm{SL}_n/\mu_n$ is simple. An algebraic group $G$ is said to be the ***almost direct product*** of its algebraic subgroups $G_1,\dots,G_n$ if the map

$$(g_1,\dots,g_n)\mapsto g_1\cdots g_n\colon G_1\times\cdots\times G_n\to G$$

is a quotient map (in particular, a homomorphism) with finite kernel. In particular, this means that the $G_i$ commute and each $G_i$ is normal.

THEOREM 14.23 *Every semisimple group $G$ is an almost direct product*

$$G_1\times\cdots\times G_r\to G$$

*of its minimal connected normal algebraic subgroups of dimension $> 0$. In particular, there are only finitely many such subgroups. Every connected normal algebraic subgroup of $G$ is a product of those $G_i$ that it contains, and is centralized by the remaining ones.*

PROOF. Write

$$\mathrm{Lie}(G) = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r$$

with the $\mathfrak{g}_i$ simple ideals. Let $G_1$ be the identity component of $C_G(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r)$ (notation as in 13.17). Then $\mathrm{Lie}(G_1) \overset{13.17}{=} c_{\mathfrak{g}}(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r) = \mathfrak{g}_1$, and so it is normal in $G$ (13.18). 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 (13.18). The subgroup $G_1 \cdots G_r$ of $G$ has Lie algebra $\mathfrak{g}$, and so equals $G$ (13.6). Finally,

$$\mathrm{Lie}(G_1 \cap \ldots \cap G_r) \overset{12.24}{=} \mathfrak{g}_1 \cap \ldots \cap \mathfrak{g}_r = 0$$

and so $G_1 \cap \ldots \cap G_r$ is étale (13.9).

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. □

COROLLARY 14.24 *All nontrivial connected normal subgroups and quotients of a semisimple algebraic group are semisimple.*

PROOF. Obvious from the theorem. □

COROLLARY 14.25 *If $G$ is semisimple, then $\mathcal{D}G = G$, i.e., a semisimple group has no commutative quotients.*

PROOF. This is obvious for simple groups, and the theorem then implies it for semisimple groups. □

# 15 Reductive algebraic groups

Throughout this section, $k$ has characteristic zero.

Recall (11.30, 11.31) that a nontrivial connected algebraic group is reductive if it has no connected normal commutative subgroup except tori, or, equivalently, if its unipotent radical is trivial.

## Structure of reductive groups

THEOREM 15.1 *If $G$ is reductive, then the derived group $G^{\mathrm{der}}$ of $G$ is semisimple, the connected centre $Z(G)^\circ$ of $G$ is a torus, and $Z(G) \cap G^{\mathrm{der}}$ is the (finite) centre of $G^{\mathrm{der}}$; moreover, $Z(G)^\circ \cdot G^{\mathrm{der}} = G$.*

PROOF. It suffices to prove this with $k = \overline{k}$. By definition, $(RG)_u = 0$, and so (11.26) shows that $RG$ is a torus $T$. Rigidity (9.16) 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 $Z(G)^\circ \cap G^{\mathrm{der}}$ is finite. Choose an embedding $G \hookrightarrow \mathrm{GL}_V$, 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 9.15). 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,[50] and so its centralizer in $\mathrm{GL}_V$ consists of the matrices of this shape with the $A_i$ arbitrary. Since $G^{\mathrm{der}}(k)$ consists of commutators (11.14), it consists of such matrices with determinant 1. As $\mathrm{SL}(V_i)$ contains only finitely many scalar matrices, this shows that $Z(G)^\circ \cap G^{\mathrm{der}}$ is finite.

Note that $Z(G)^\circ \cdot G^{\mathrm{der}}$ is a normal algebraic subgroup of $G$ such that $G/(Z(G)^\circ \cdot G^{\mathrm{der}})$ is commutative (being a quotient of $G/G^{\mathrm{der}}$) and semisimple (being a quotient of $G/R(G)$). Now (14.25) shows that

$$G = Z(G)^\circ \cdot G^{\mathrm{der}}.$$

Therefore

$$G^{\mathrm{der}} \to G/R(G)$$

is surjective with finite kernel. As $G/R(G)$ is semisimple, so also is $G^{\mathrm{der}}$.

Certainly $Z(G) \cap G^{\mathrm{der}} \subset Z(G^{\mathrm{der}})$, but, because $G = Z(G)^\circ \cdot G^{\mathrm{der}}$ and $Z(G)^\circ$ is commutative, $Z(G^{\mathrm{der}}) \subset Z(G)$. □

REMARK 15.2 From a reductive group $G$, we obtain a semisimple group $G'$ (its derived group), a group $Z$ of multiplicative type (its centre), and a homomorphism $\varphi\colon Z(G') \to Z$. Moreover, $G$ can be recovered from $(G', Z, \varphi)$ as the quotient

$$Z(G') \xrightarrow{z \mapsto (\varphi(z)^{-1}, z)} Z \times G' \to G \to 1. \tag{60}$$

[50] That is, of the form $\mathrm{diag}(a, \dots, a)$ with $a \neq 0$.

Clearly, every reductive group arises from such a triple $(G', Z, \varphi)$ (and $G'$ can even be chosen to be simply connected).

### Generalities on semisimple modules

Let $k$ be a field, and let $A$ be a $k$-algebra (not necessarily commutative). An $A$-module is ***simple*** if it does not contain a nonzero proper submodule.

PROPOSITION 15.3 *The following conditions on an $A$-module $M$ of finite dimension*[51] *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). □

DEFINITION 15.4 An $A$-module is ***semisimple*** if it satisfies the equivalent conditions of the proposition.

## Representations of reductive groups

Throughout this subsection, $k$ is algebraically closed. Representations are always on finite-dimensional $k$-vector spaces. We shall sometimes refer to a vector space with a representation of $G$ on it as a $G$-module. The definitions and result of the last subsection carry over to $G$-modules.

Our starting point is the following result.

THEOREM 15.5 *If $\mathfrak{g}$ is semisimple, then all $\mathfrak{g}$-modules are semisimple.*

PROOF. Omitted — see Humphreys 1972, pp25–28 (the proof is elementary but a little complicated). □

THEOREM 15.6 *Let $G$ be an algebraic group. All representations of $G$ are semisimple if and only if $G^\circ$ is reductive.*

LEMMA 15.7 *The restriction to any normal algebraic subgroup of a semisimple representation is again semisimple.*

[51] I assume this only to avoid using Zorn's lemma in the proof.

PROOF. Let $G \to \mathrm{GL}_V$ be a representation of $G$, which we may assume to be simple, and let $N$ be a normal algbraic subgroup of $G$. 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 $V$). □

LEMMA 15.8 *All representations of $G$ are semisimple if and only if all representations of $G^\circ$ are semisimple*

PROOF. $\Longrightarrow$ : Since $G^\circ$ is a normal algebraic subgroup of $G$ (8.13), this follows from the preceding lemma.

$\Longleftarrow$ : Let $V$ be a $G$-module, and let $W$ be a sub $G$-module (i.e., a subspace stable under $G$). Then $W$ is also stable under $G^\circ$, and so $V = W \oplus W'$ for some $G^\circ$-stable subspace $W'$. Let $p$ be the projection map $V \to W$; it is a $G^\circ$-equivariant[52] map whose restriction to $W$ is $\mathrm{id}_W$. Define

$$q\colon V \to W, \quad q = \frac{1}{n}\sum\nolimits_g gpg^{-1},$$

where $n = (G(k)\colon G^\circ(k))$ and $g$ runs over a set of coset representatives for $G^\circ(k)$ in $G(k)$. One checks directly that $q$ has the following properties:

(a) it is independent of the choice of the coset representatives;
(b) for all $w \in W$, $q(w) = w$;
(c) it is $G$-equivariant.

Now (b) implies that $V = W \oplus W''$, where $W'' = \mathrm{Ker}(q)$, and (c) implies that $W''$ is stable under $G$. □

REMARK 15.9 The lemma implies that the representations of a finite group are semisimple. This would fail if we allowed the characteristic to divide the order of the finite group.

LEMMA 15.10 *Every representation of a semisimple algebraic group is semisimple.*

PROOF. From a representation $G \to \mathrm{GL}_V$ of $G$ on $V$ we get a representation $\mathfrak{g} \to \mathfrak{gl}_V$ of $\mathfrak{g}$ on $V$, and a subspace $W$ of $V$ is stable under $G$ if and only if it is stable under $\mathfrak{g}$ (see 13.15). Therefore, the statement follows from (15.5). □

**Proof of Theorem 15.6**

Lemma 15.8 allows us to assume $G$ is connected.

$\Longrightarrow$ : Let $G \to \mathrm{GL}_V$ be a faithful semisimple representation of $G$, and let $N$ be the unipotent radical of $G$. Lemma 15.7 shows $V$ is semisimple as an $N$-module, say $V = \bigoplus V_i$ with $V_i$ simple. Because $N$ is solvable, the Lie-Kolchin theorem (11.22) shows that the elements of $N$ have a common eigenvector in $V_i$ (cf. the proof of the theorem) and so $V_i$ has dimension 1, and because $N$ is unipotent it must act trivially on $V_i$. Therefore, $N$ acts trivially on $V$, but we chose $V$ to be faithful. Hence $N = 0$.

$\Longleftarrow$ : If $G$ is reductive, then $G = Z^\circ \cdot G'$ where $Z^\circ$ is the connected centre of $G$ (a torus) and $G'$ is the derived group of $G$ (a semisimple group) — see (15.1). Let $G \to \mathrm{GL}_V$ be a representation of $G$. Then $V = \bigoplus_i V_i$ where $V_i$ is the subspace of $V$ on which $Z^\circ$ acts through a character $\chi_i$ (see 9.15). Because $Z^\circ$ and $G'$ commute, each space $V_i$ is

[52] That is, it is a homomorphism of $G^\circ$-representations.

stable under $G'$, and because $G'$ is semisimple, $V_i = \bigoplus_j V_{ij}$ with each $V_{ij}$ simple as a $G'$-module (15.10). Now $V = \bigoplus_{i,j} V_{ij}$ is a decomposition of $V$ into a direct sum of simple $G$-modules.

REMARK 15.11 It is not necessary to assume $k$ is algebraically closed. In fact, for an algebraic group $G$ over $k$ of characteristic zero, all representations of $G$ are semisimple if and only if all representations of $G_{\overline{k}}$ are semisimple (Deligne and Milne 1982, 2.25)[53]. However, as noted earlier (11.34), it is necessary to assume that $k$ has characteristic zero, even when $G$ is connected.

REMARK 15.12 Classically, the proof was based on the following two results:

> Every semisimple algebraic group $G$ over $\mathbb{C}$ has a (unique) model $G_0$ over $\mathbb{R}$ such that $G_0(\mathbb{R})$ is compact, and $\mathrm{Hom}_{\mathbb{R}}(G_0, \mathrm{GL}_V) \simeq \mathrm{Hom}_{\mathbb{C}}(G, \mathrm{GL}_V)$.

For example, $\mathrm{SL}_n = (G_0)_{\mathbb{C}}$ where $G_0$ is the special unitary group (see p103).

> Every representation of an algebraic group $G$ over $\mathbb{R}$ such that $G(\mathbb{R})$ is compact is semisimple.

To prove this, let $\langle\ ,\ \rangle$ be a positive definite form on $V$. Then $\langle\ ,\ \rangle_0 = \int_{G(\mathbb{R})} \langle x, y\rangle dg$ is a $G(\mathbb{R})$-invariant positive definite form on $V$. For any $G$-stable subspace $W$, the orthogonal complement of $W$ is a $G$-stable complement.

## A criterion to be reductive

There is an isomorphism of algebraic groups $\mathrm{GL}_n \to \mathrm{GL}_n$ sending an invertible matrix $A$ to the transpose $(A^{-1})^t$ of its inverse. The image of an algebraic subgroup $H$ of $\mathrm{GL}_n$ under this map is the algebraic subgroup $H^t$ of $\mathrm{GL}_n$ such that $H^t(R) = \{A^t \mid A \in H(R)\}$ for all $k$-algebras $R$.

Now consider $\mathrm{GL}_V$. The choice of a basis for $V$ determines an isomorphism $\mathrm{GL}_V \approx \mathrm{GL}_n$ and hence a transpose map on $\mathrm{GL}_V$, *which depends on the choice of the basis.*

PROPOSITION 15.13 *Every connected algebraic subgroup $G$ of $\mathrm{GL}_V$ such that $G = G^t$ for all choices of a basis for $V$ is reductive.*

PROOF. We have to show that $(RG)_u = 0$. It suffices to check this after passing to the algebraic closure[54] $\overline{k}$ of $k$. Recall that the radical of $G$ is the largest connected normal solvable subgroup of $G$. It follows from (11.29c) that $RG$ is contained in every maximal connected solvable subgroup of $G$. Let $B$ be such a subgroup, and choose a basis for $V$ such that $B \subset \mathbb{T}_n$ (Lie-Kolchin theorem 11.22). 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. □

EXAMPLE 15.14 The group $\mathrm{GL}_V$ itself is reductive.

[53] Deligne, P., and Milne, J., Tannakian Categories. In Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Math. 900 (1982), Springer, Heidelberg, 101-228.

[54] More precisely, one can prove that $R(G_{\overline{k}}) = (RG)_{\overline{k}}$ and similarly for the unipotent radial (provided $k$ is perfect).

EXAMPLE 15.15 Since the transpose of a matrix of determinant 1 has determinant 1, $\mathrm{SL}_V$ is reductive.

It is possible to verify that $\mathrm{SO}_n$ and $\mathrm{Sp}_n$ are reductive using this criterion (to be added; cf. Humphreys 1972, Exercise 1-12, p6). They are semisimple because their centres are finite (this can be verified directly, or by studying their roots — see below).

# 16 Split reductive groups: the program

In this, and all later sections, $k$ is of characteristic zero.

## 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 $\mathbb{G}_m$. A torus over $k$ is an algebraic group that becomes isomorphic to a split torus over $\overline{k}$. A torus in $\mathrm{GL}_V$ 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 $k$.

Recall (§9) that $\mathrm{End}(\mathbb{G}_m) \simeq \mathbb{Z}$: the only group-like elements in $k[\mathbb{G}_m] = k[X, X^{-1}]$ are the powers of $X$, and the only homomorphisms $\mathbb{G}_m \to \mathbb{G}_m$ are the maps $t \mapsto t^n$ for $n \in \mathbb{Z}$. For a split torus $T$, we set

$$X^*(T) = \mathrm{Hom}(T, \mathbb{G}_m) = \text{group of characters of } T,$$
$$X_*(T) = \mathrm{Hom}(\mathbb{G}_m, T) = \text{group of cocharacters of } T.$$

There is a pairing

$$\langle\ ,\ \rangle : X^*(T) \times X_*(T) \to \mathrm{End}(\mathbb{G}_m) \simeq \mathbb{Z}, \quad \langle \chi, \lambda \rangle = \chi \circ \lambda. \tag{61}$$

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 $\langle\ ,\ \rangle$ 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 $\chi_1, \dots, \chi_n$, where

$$\chi_i(\mathrm{diag}(a_1, \dots, a_n)) = a_i,$$

and $X_*(T)$ has basis $\lambda_1, \dots, \lambda_n$, where

$$\lambda_i(t) = \mathrm{diag}(1, \dots, \overset{i}{t}, \dots, 1).$$

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 $a = \operatorname{diag}(a_1, a_2, a_3)$, 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 exponentional notation $\chi(a) = a^\chi$. With this notation, the preceding equation becomes

$$a^{5\chi_2 + 7\chi_3} = a^{5\chi_2} a^{7\chi_3} = a_2^5 a_3^7.$$

## Split reductive groups

Let $G$ be an algebraic group over a field $k$. When $k = \overline{k}$, a torus $T \subset G$ is ***maximal*** if it is not properly contained in any other torus. For example, $\mathbb{D}_n$ is a maximal torus in $\mathrm{GL}_n$ because it is equal to own centralizer in $\mathrm{GL}_n$. In general, $T \subset G$ is said to be ***maximal*** **if** $T_{\overline{k}}$ **is maximal in** $G_{\overline{k}}$. A reductive group is ***split*** if it contains a split maximal torus.

Let $G$ a reductive group over $\overline{k}$. Since all tori over $\overline{k}$ are split, $G$ is automatically split. As we discuss below, there exists a split reductive group $G_0$ over $k$, unique up to isomorphism, such that $G_{0\overline{k}} \approx G$.

EXAMPLE 16.1 The group $\mathrm{GL}_n$ 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

$$i^2 = -1, \quad j^2 = -1, ij = -ji.$$

It is a division algebra with centre $\mathbb{R}$. There is an algebraic group $G$ over $\mathbb{R}$ such that

$$G(R) = (R \otimes_k \mathbb{H})^\times.$$

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 $\mathrm{GL}_2$ over $\mathbb{C}$, but as an algebraic group over $\mathbb{R}$ it is not split.[55]

EXAMPLE 16.2 The group $\mathrm{SL}_n$ is a split reductive (in fact, semisimple) group, with split maximal torus the diagonal matrices of determinant 1.

EXAMPLE 16.3 Let $(V, q)$ be a nondegenerate quadratic space (see §5), i.e., $V$ is a finite-dimensional vector space and $q$ is a nondegenerate quadratic form on $V$ with associated symmetric form $\phi$. Recall (5.7) 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

$$V = H_1 \perp \ldots \perp H_r \perp V_1 \quad \text{(Witt decomposition)}$$

[55] Its derived group $G'$ is the subgroup of elements of norm 1. As $G'(\mathbb{R})$ is compact, it can't contain a split torus.

where each $H_i$ is a hyperbolic plane and $V_1$ is anisotropic (5.9). It can be shown that the associated algebraic group $\mathrm{SO}(q)$ is split if and only if its Witt index is as large as possible.

(a) Case $\dim V = n$ is even. When the Witt index is as large as possible, $n = 2r$, and there is a basis for which the matrix[56] of the form is $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$, and so

$$q(x_1, \dots, x_n) = x_1 x_{r+1} + \cdots + x_r x_{2r}.$$

Note that the subspace of vectors

$$(*, \dots, \overset{r}{*}, 0, \dots, 0)$$

is totally isotropic. The algebraic subgroup consisting of the diagonal matrices of the form

$$\mathrm{diag}(a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in $\mathrm{SO}(q)$.

(b) Case $\dim V = n$ is odd. When the Witt index is as large as possible, $n = 2r + 1$, and 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

$$q(x_0, x_1, \dots, x_n) = x_0^2 + x_1 x_{r+1} + \cdots + x_r x_{2r}.$$

The algebraic subgroup consisting of the diagonal matrices of the form

$$\mathrm{diag}(1, a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in $\mathrm{SO}(q)$.

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 $\mathrm{SO}_n$s.**

EXAMPLE 16.4 Let $V = k^{2n}$, and let $\psi$ be the skew-symmetric form with matrix $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, so

$$\psi(\vec{x}, \vec{y}) = x_1 y_{n+1} + \cdots + x_n y_{2n} - x_{n+1} y_1 - \cdots - x_{2n} y_n.$$

The corresponding symplectic group $\mathrm{Sp}_n$ is split, and the algebraic subgroup consisting of the diagonal matrices of the form

$$\mathrm{diag}(a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1})$$

is a split maximal torus in $\mathrm{Sp}_n$.

[56] Moreover, $\mathrm{SO}(q)$ consists of the automorphs of this matrix with determinant 1, i.e., $\mathrm{SO}(q)(R)$ consists of the $n \times n$ matrices $A$ with entries in $R$ and determinant 1 such that $A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

## Program

Let $G$ be a split reductive group over $k$. Then any two split maximal tori are conjugate by an element of $G(k)$. Rather than working with split reductive groups $G$, it turns out to be better to work with pairs $(G,T)$ with $T$ a split maximal torus in $G$.

16.5 To each pair $(G,T)$ consisting of a split reductive group and a maximal torus, we associate a more elementary object, namely, its root datum $\Psi(G,T)$. The root datum $\Psi(G,T)$ determines $(G,T)$ up to isomorphism, and every root datum arises from a pair $(G,T)$ (see §§17,20).

16.6 Classify the root data (see §§18,19).

16.7 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 (see §§21,22,23).

16.8 The root data have nothing to do with the field! In particular, we see that for each reductive group $G$ over $\overline{k}$, there is (up to isomorphism) exactly one split reductive group over $k$ that becomes isomorphic to $G$ over $\overline{k}$. However, there will in general be many nonsplit groups, and so we are left with the problem of understanding them (§§26,27).

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 are ensuring that there are enough eigenvalues without requiring the ground field to be algebraically closed.

**Example: the forms of $\mathrm{GL}_2$.** What are the groups $G$ over a field $k$ such that $G_{\overline{k}} \approx \mathrm{GL}_2$? 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

$$i^2 = a,\ j^2 = b,\ ij = -ji.$$

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 $\mathrm{GL}_2$ over $\overline{k}$, 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 $\mathrm{GL}_2$ 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 $\mathrm{GL}_2$ over $\mathbb{Q}$, exactly one of which, $\mathrm{GL}_2$, is split.

# 17 The root datum of a split reductive group

Recall that $k$ has characteristic zero.

### Roots

Let $G$ be a split reductive group and $T$ a split maximal torus. Then $G$ acts on $\mathfrak{g} = \mathrm{Lie}(G)$ via the adjoint representation

$$\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}.$$

In particular, $T$ acts on $\mathfrak{g}$, and so it decomposes as

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus \mathfrak{g}_\chi$$

where $\mathfrak{g}_0$ is the subspace on which $T$ acts trivially, and $\mathfrak{g}_\chi$ is the subspace on which $T$ acts through the nontrivial character $\chi$ (see 9.15). The nonzero $\chi$ occurring in this decomposition are called the ***roots*** of $(G,T)$. They form a finite subset $\Phi$ of $X^*(T)$.

### Example: $\mathrm{GL}_2$

Here

$$\begin{aligned} T &= \left\{ \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \;\middle|\; x_1x_2 \neq 0 \right\}, \\ X^*(T) &= \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2, \quad \left(\begin{smallmatrix} x_1 & 0 \\ 0 & x_2 \end{smallmatrix}\right) \overset{a\chi_1+b\chi_2}{\longrightarrow} x_1^a x_2^b, \\ \mathfrak{g} &= M_2(k), \end{aligned}$$

and $T$ acts on $\mathfrak{g}$ by conjugation,

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1^{-1} & 0 \\ 0 & x_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{x_1}{x_2}b \\ \frac{x_2}{x_1}c & d \end{pmatrix}.$$

Write $E_{ij}$ for the matrix with a 1 in the $ij^{\text{th}}$-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, $\Phi = \{\alpha, -\alpha\}$ where $\alpha = \chi_1 - \chi_2$. When we use $\chi_1$ and $\chi_2$ to identify $X^*(T)$ with $\mathbb{Z} \oplus \mathbb{Z}$, $\Phi$ becomes identified with $\{\pm(e_1 - e_2)\}$.

### Example: $\mathrm{SL}_2$

Here

$$\begin{aligned} T &= \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \right\}, \\ X^*(T) &= \mathbb{Z}\chi, \quad \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right) \overset{\chi}{\longmapsto} x, \\ \mathfrak{g} &= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(k) \mid a + d = 0\}. \end{aligned}$$

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 $\chi$ to identify $X^*(T)$ with $\mathbb{Z}$, $\Phi$ becomes identified with $\{2, -2\}$.

**Example:** $\mathrm{PGL}_2$

Recall that this is the quotient of $\mathrm{GL}_2$ by its centre: $\mathrm{PGL}_2 = \mathrm{GL}_2/\mathbb{G}_m$. One can prove that for all rings $R$, $\mathrm{PGL}_2(R) = \mathrm{GL}_2(R)/R^\times$. Here

$$\begin{aligned} T &= \left\{ \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \;\middle|\; x_1 x_2 \neq 0 \right\} \Big/ \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \mid x \neq 0 \right\}, \\ X^*(T) &= \mathbb{Z}\chi, \quad \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \overset{\chi}{\longmapsto} \frac{x_1}{x_2}, \\ \mathfrak{g} &= M_2(k)/\{aI\} \quad \text{(quotient as a } \textit{vector space)}. \end{aligned}$$

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 $\chi$ to identify $X^*(T)$ with $\mathbb{Z}$, $\Phi$ becomes identified with $\{1, -1\}$.

**Example:** $\mathrm{GL}_n$

Here

$$\begin{aligned} T &= \left\{ \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \;\middle|\; x_1 \cdots x_n \neq 0 \right\}, \\ X^*(T) &= \bigoplus\nolimits_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \overset{\chi_i}{\longmapsto} x_i, \\ \mathfrak{g} &= M_n(k), \end{aligned}$$

and $T$ acts on $\mathfrak{g}$ by conjugation:

$$\begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & a_{ij} & \vdots \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1^{-1} & & 0 \\ & \ddots & \\ 0 & & x_n^{-1} \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & \cdots & \frac{x_1}{x_n} a_{1n} \\ \vdots & & \frac{x_i}{x_j} a_{ij} & \vdots \\ \vdots & & & \vdots \\ \frac{x_n}{x_1} a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}.$$

Write $E_{ij}$ for the matrix with a 1 in the $ij^{\text{th}}$-position, and zeros elsewhere. Then $T$ acts trivially on $\mathfrak{g}_0 = \langle E_{11}, \ldots, E_{nn} \rangle$ and through the character $\alpha_{ij} = \chi_i - \chi_j$ on $\mathfrak{g}_{\alpha_{ij}} = \langle E_{ij} \rangle$, and so

$$\Phi = \{\alpha_{ij} \mid 1 \leq i, j \leq n, \quad i \neq j\}.$$

When we use the $\chi_i$ to identify $X^*(T)$ with $\mathbb{Z}^n$, then $\Phi$ becomes identified with

$$\{e_i - e_j \mid 1 \leq i, j \leq n, \quad i \neq j\}$$

where $e_1, \ldots, e_n$ is the standard basis for $\mathbb{Z}^n$.

## Definition of a root datum

DEFINITION 17.1 A ***root datum*** is a quadruple $\Psi = (X, \Phi, X^\vee, \Phi^\vee)$ where

- $X, X^\vee$ are free $\mathbb{Z}$-modules of finite rank in duality by a pairing $\langle\ ,\ \rangle\colon X \times X^\vee \to \mathbb{Z}$,
- $\Phi, \Phi^\vee$ are finite subsets of $X$ and $X^\vee$ in bijection by a map $\alpha \leftrightarrow \alpha^\vee$,

[57]satisfying the following conditions

**rd1** $\langle \alpha, \alpha^\vee \rangle = 2$,

**rd2** $s_\alpha(\Phi) \subset \Phi$ where $s_\alpha$ is the homomorphism $X \to X$ defined by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad x \in X, \alpha \in \Phi,$$

**rd3** the group of automorphisms of $X$ generated by the $s_\alpha$ for $\alpha \in \Phi$ is finite.

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, $s_\alpha$ should be considered an "abstract reflection in the hyperplane orthogonal to $\alpha$".

The elements of $\Phi$ and $\Phi^\vee$ are called the ***roots*** and ***coroots*** of the root datum (and $\alpha^\vee$ is the ***coroot*** of $\alpha$). The group $W = W(\Psi)$ of automorphisms of $X$ generated by the $s_\alpha$ for $\alpha \in \Phi$ 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

$$\begin{aligned} X &= X^*(T), \\ \Phi &= \text{roots}, \\ X^\vee &= X_*(T) \text{ with the pairing } X^*(T) \times X_*(T) \to \mathbb{Z} \text{ in (61)}, \\ \Phi^\vee &= \text{coroots (to be defined)}. \end{aligned}$$

## First examples of root data

EXAMPLE 17.2 Let $G = \mathrm{SL}_2$. Here

$$\begin{aligned} X = X^*(T) = \mathbb{Z}\chi, &\quad \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right) \overset{\chi}{\longmapsto} x \\ X^\vee = X_*(T) = \mathbb{Z}\lambda, &\quad t \overset{\lambda}{\longmapsto} \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \\ \Phi = \{\alpha, -\alpha\}, &\quad \alpha = 2\chi \\ \Phi^\vee = \{\alpha^\vee, -\alpha^\vee\}, &\quad \alpha^\vee = \lambda. \end{aligned}$$

[57]Thus, a root datum is really an ordered sextuple,

$$X, X^\vee, \langle\ ,\ \rangle, \Phi, \Phi^\vee, \Phi \to \Phi^\vee,$$

but everyone says quadruple.

Note that

$$t \overset{\lambda}{\longmapsto} \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \overset{2\chi}{\longmapsto} t^2$$

and so

$$\langle \alpha, \alpha^\vee \rangle = 2.$$

As always,

$$s_\alpha(\alpha) = -\alpha, \quad s_\alpha(-\alpha) = \alpha$$

etc., and so $s_{\pm\alpha}(\Phi) \subset \Phi$. Finally, $W(\Psi) = \{1, s_\alpha\}$ is finite, and so $\Psi(\mathrm{SL}_2, T)$ 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 17.3 Let $G = \mathrm{PGL}_2$. Here

$$\Phi^\vee = \{\alpha^\vee, -\alpha^\vee\}, \quad \alpha^\vee = 2\lambda.$$

In this case $\Psi(\mathrm{PGL}_2, T)$ is a root system, isomorphic to

$$(\mathbb{Z}, \{1, -1\}, \mathbb{Z}, \{2, -2\}).$$

REMARK 17.4 If $\alpha$ is a root, so also is $-\alpha$, and there exists an $\alpha^\vee$ 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 $\Phi$ 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 17.5 Let $G = \mathrm{GL}_n$. Here

$$\begin{aligned}
X = X^*(\mathbb{D}_n) &= \bigoplus\nolimits_i \mathbb{Z}\chi_i, \quad \mathrm{diag}(x_1, \dots, x_n) \overset{\chi_i}{\longmapsto} x_i \\
X^\vee = X_*(\mathbb{D}_n) &= \bigoplus\nolimits_i \mathbb{Z}\lambda_i, \quad t \overset{\lambda_i}{\longmapsto} \mathrm{diag}(1, \dots, 1, \overset{i}{t}, 1, \dots, 1) \\
\Phi &= \{\alpha_{ij} \mid i \neq j\}, \quad \alpha_{ij} = \chi_i - \chi_j \\
\Phi^\vee &= \{\alpha_{ij}^\vee \mid i \neq j\}, \quad \alpha_{ij}^\vee = \lambda_i - \lambda_j.
\end{aligned}$$

Note that

$$t \overset{\lambda_i - \lambda_j}{\longmapsto} \mathrm{diag}(1, \dots, \overset{i}{t}, \dots, \overset{j}{t^{-1}}, \dots) \overset{\chi_i - \chi_j}{\longmapsto} t^2$$

and so

$$\langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = 2.$$

Moreover, $s_\alpha(\Phi) \subset \Phi$ for all $\alpha \in \Phi$. 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 $i^{\text{th}}$ and $j^{\text{th}}$ rows have been swapped. The action

$$A \mapsto E(ij) \cdot A \cdot E(ij)^{-1}$$

of $E_{ij}$ on $\mathrm{GL}_n$ 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 $\mathrm{GL}_n$ 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

$$(\mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}, \mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}$$

where $e_i = (0, \dots, \overset{i}{1}, \dots, 0)$, the pairing is the standard one $\langle e_i, e_j \rangle = \delta_{ij}$, and $(e_i - e_j)^\vee = e_i - e_j$.

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.

## 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 $G_{\overline{k}}$ contains a subgroup isomorphic to $\mathbb{G}_m^r$. Since all maximal tori in $G_{\overline{k}}$ are conjugate (see 17.17 below), the rank is well-defined.

THEOREM 17.6 *(a) Every semisimple group of rank* 0 *is trivial.*
*(b) Every semisimple group of rank* 1 *is isomorphic to* $\mathrm{SL}_2$ *or* $\mathrm{PGL}_2$.

PROOF. (SKETCH) (a) Take $k = \overline{k}$. If all the elements of $G(k)$ are unipotent, then $G$ is solvable (11.23), hence trivial. Otherwise, $G(k)$ contains a semisimple element (10.1). The smallest algebraic subgroup $H$ containing the element is commutative, and therefore decomposes into $H_s \times H_u$ (see 11.6). If all semisimple elements of $G(k)$ are of finite order, then $G$ is finite (hence trivial, being connected). If $G(k)$ contains a semisimple element of infinite order, $H_s^\circ$ 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 $G \to \mathrm{Aut}(\mathbb{P}^1) \simeq \mathrm{PGL}_2$. □

## Centralizers and normalizers

Let $T$ be a torus in an algebraic group $G$. Recall (13.18) that the ***centralizer*** of $T$ in $G$ is the algebraic subgroup $C = C_G(T)$ of $G$ such that, for all $k$-algebras $R$,

$$C(R) = \{g \in G(R) \mid gt = tg \text{ for all } t \in T(R)\}.$$

Similarly, the ***normalizer*** of $T$ in $G$ is the algebraic subgroup $N = N_G(T)$ of $G$ such that, for all $k$-algebras $R$,

$$N(R) = \{g \in G(R) \mid gtg^{-1} \in T(R) \text{ for all } t \in T(R)\}.$$

THEOREM 17.7 *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 connected.*
(b) *The identity component of the normalizer $N_G(T)$ of $T$ in $G$ is $C_G(T)$; in particular, $N_G(T)/C_G(T)$ is a finite étale group.*
(c) *The torus $T$ is maximal if and only if $T = C_G(T)$.*

PROOF. (a) Omitted. (When $k = \overline{k}$, the statement is proved in Humphreys 1975, 26.2.)

(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 (9.16). For the second statement, see §8.

(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 (15.1) containing $T$ and therefore equal to it. Hence $C_G(T)/T$ is a semisimple group (15.1) of rank 0, and hence is trivial. Thus $C_G(T) = Z(C_G(T))^\circ = T$. □

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 group[58] when $T$ is split, and so may be regarded simply as a finite group.

## Definition of the coroots

LEMMA 17.8 *Let $G$ be a split reductive group with split maximal torus $T$. The action of $W(G,T)$ on $X^*(T)$ stabilizes $\Phi$.*

PROOF. Take $k = \overline{k}$. 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 $\alpha$ 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. □

For a root $\alpha$ of $(G,T)$, let $T_\alpha = \mathrm{Ker}(\alpha)^\circ$, and let $G_\alpha$ be centralizer of $T_\alpha$.

THEOREM 17.9 *Let $G$ be a split reductive group with split maximal torus $T$.*
(a) *For each $\alpha \in \Phi$, $W(G_\alpha, T)$ contains exactly one nontrivial element $s_\alpha$, and there is a unique $\alpha^\vee \in X_*(T)$ such that*

$$s_\alpha(x) = x - \langle x, \alpha^\vee\rangle\alpha, \quad \text{for all } x \in X^*(T). \tag{62}$$

*Moreover, $\langle \alpha, \alpha^\vee\rangle = 2$.*
(b) *The system $(X^*(T), \Phi, X_*(T), \Phi^\vee)$ with $\Phi^\vee = \{\alpha^\vee \mid \alpha \in \Phi\}$ and the map $\alpha \mapsto \alpha^\vee\colon \Phi \to \Phi^\vee$ is a root datum.*

[58] That 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).

PROOF. (SKETCH) (a) The key point is that the derived group of $G_\alpha$ is a semisimple group of rank one and $T$ is a maximal torus of $G_\alpha$. Thus, we are essentially in the case of $\mathrm{SL}_2$ or $\mathrm{PGL}_2$, where everything is obvious (see below). Note that the uniqueness of $\alpha^\vee$ follows from that of $s_\alpha$.

(b) We noted in (a) that (rd1) holds. The $s_\alpha$ attached to $\alpha$ lies in $W(G_\alpha, T) \subset W(G, T)$, and so stabilizes $\Phi$ by the lemma. Finally, all $s_\alpha$ lie in the Weyl group $W(G, T)$, and so they generate a finite group (in fact, the generate exactly $W(G, T)$). □

EXAMPLE 17.10 Let $G = \mathrm{SL}_2$, and let $\alpha$ be the root $2\chi$. 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 $\alpha^\vee$ for which (62) holds is $\lambda$.

EXAMPLE 17.11 Let $G = \mathrm{GL}_n$, and let $\alpha = \alpha_{12} = \chi_1 - \chi_2$. Then

$$T_\alpha = \{\mathrm{diag}(x, x, x_3, \dots, x_n) \mid xxx_3 \dots x_n \neq 1\}$$

and $G_\alpha$ consists of the invertible matrices of the form

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

Clearly

$$n_\alpha = \begin{pmatrix} 0 & 1 & 0 & & 0 \\ 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

represents the unique nontrivial element $s_\alpha$ of $W(G_\alpha, T)$. It acts on $T$ by

$$\mathrm{diag}(x_1, x_2, x_3, \dots, x_n) \longmapsto \mathrm{diag}(x_2, x_1, x_3, \dots, x_n).$$

For $x = m_1\chi_1 + \cdots + m_n\chi_n$,

$$\begin{aligned} s_\alpha x &= m_2\chi_1 + m_1\chi_2 + m_3\chi_3 + \cdots + m_n\chi_n \\ &= x - \langle x, \lambda_1 - \lambda_2\rangle(\chi_1 - \chi_2). \end{aligned}$$

and

$$x - \langle x, \lambda_1 - \lambda_2\rangle\alpha = x - (2$$

Thus (62) holds if and only if $\alpha^\vee$ is taken to be $\lambda_1 - \lambda_2$.

## Computing the centre

PROPOSITION 17.12 *Every maximal torus $T$ in a reductive algebraic group $G$ contains the centre $Z = Z(G)$ of $G$.*

PROOF. Clearly $Z \subset C_G(T)$, but (see 17.7), $C_G(T) = T$. □

Recall (14.8) that the kernel of the adjoint map $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$ is $Z(G)$, and so the kernel of $\mathrm{Ad}\colon T \to \mathrm{GL}_{\mathfrak{g}}$ is $Z(G) \cap T = Z(G)$. Therefore

$$Z(G) = \mathrm{Ker}(\mathrm{Ad}\,|T) = \bigcap\nolimits_{\alpha\in\Phi} \mathrm{Ker}(\alpha).$$

We can use this to compute the centres of groups. For example,

$$Z(\mathrm{GL}_n) = \bigcap\nolimits_{i\neq j} \mathrm{Ker}(\chi_i - \chi_j) = \left\{ \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix} \;\middle|\; x_1 = x_2 = \cdots = x_n \neq 0 \right\},$$

$$Z(\mathrm{SL}_2) = \mathrm{Ker}(2\chi) = \left\{ \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right) \mid x^2 = 1 \right\} = \mu_2,$$

$$Z(\mathrm{PGL}_2) = \mathrm{Ker}(\chi) = 1.$$

On applying $X^*$ to the exact sequence

$$0 \to Z(G) \to T \xrightarrow{t\mapsto(\ldots,\alpha(t),\ldots)} \prod\nolimits_{\alpha\in\Phi} \mathbb{G}_m \tag{63}$$

we get (see 9.12) an exact sequence

$$\bigoplus\nolimits_{\alpha\in\Phi} \mathbb{Z} \xrightarrow{(\ldots,m_\alpha,\ldots)\mapsto\sum m_\alpha\alpha} X^*(T) \to X^*(Z(G)) \to 0,$$

and so

$$X^*(Z(G)) = X^*(T)/\{\text{subgroup generated by } \Phi\}. \tag{64}$$

For example,

$$X^*(Z(\mathrm{GL}_n)) \simeq \mathbb{Z}^n/\langle e_i - e_j \mid i \neq j\rangle \xrightarrow[\simeq]{(a_1,\ldots,a_n)\mapsto\sum a_i} \mathbb{Z},$$

$$X^*(Z(\mathrm{SL}_2)) \simeq \mathbb{Z}/(2),$$

$$X^*(Z(\mathrm{PGL}_2)) \simeq \mathbb{Z}/\mathbb{Z} = 0.$$

## Semisimple and toral root data

DEFINITION 17.13 A root datum is ***semisimple*** if $\Phi$ generates a subgroup of finite index in $X$.

PROPOSITION 17.14 *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 (64). □

DEFINITION 17.15 A root datum is ***toral*** if $\Phi$ is empty.

PROPOSITION 17.16 *A split reductive group is a torus if and only if its root datum is toral.*

PROOF. If the root datum is toral, then (64) 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 $\mathfrak{g} = \mathfrak{g}_0$. □

## The main theorems.

From $(G,T)$ we get a root datum $\Psi(G,T)$.

THEOREM 17.17 *Let $T, T'$ be split maximal tori in $G$. Then there exists a $g \in G(k)$ such that $T' = gTg^{-1}$ (i.e., $\mathrm{inn}(g)(T) = T'$).*

PROOF. Omitted for the present. □

EXAMPLE 17.18 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 $\mathrm{GL}_V$.

It follows that the root datum attached to $(G,T)$ depends only on $G$ (up to isomorphism).

THEOREM 17.19 (ISOMORPHISM) *Every isomorphism $\Psi(G,T) \to \Psi(G',T')$ of root data arises from an isomorphism $\varphi: G \to G'$ such that $\varphi(T) = T'$.*

PROOF. Springer 1998, 16.3.2. □

Later we shall define the notion of a base for a root datum. If bases are fixed for $(G,T)$ and $(G',T')$, then $\varphi$ 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 $t \in T(\bar{k})$ and $\alpha(t) \in k$ for all $\alpha$.

THEOREM 17.20 (EXISTENCE) *Every reduced root datum arises from a split reductive group.*

PROOF. Springer 1998, 16.5. □

A root datum is ***reduced*** if the only multiples of a root $\alpha$ that can also be a root are $\pm\alpha$.

## 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 $\mathrm{GL}_n$. We first compute the weights of the split maximal torus on $\mathfrak{gl}_n$, and then check that each nonzero weight occurs in $\mathfrak{g}$ (in fact, with multiplicity 1). Then for each $\alpha$ we find a natural copy of $\mathrm{SL}_2$ (or $\mathrm{PGL}_2$) centralizing $T_\alpha$, and use it to find the coroot $\alpha^\vee$.

**Example ($\mathbf{A}_n$): $\mathrm{SL}_{n+1}$.**

Let $G$ be $\mathrm{SL}_{n+1}$ and let $T$ be the algebraic subgroup of diagonal matrices:

$$\{\mathrm{diag}(t_1,\dots,t_{n+1}) \mid t_1\cdots t_{n+1} = 1\}.$$

Then

$$X^*(T) = \bigoplus \mathbb{Z}\chi_i \Big/ \mathbb{Z}\chi, \quad \begin{cases} \mathrm{diag}(t_1,\dots,t_{n+1}) \overset{\chi_i}{\longmapsto} t_i \\ \chi = \sum \chi_i \end{cases}$$

$$X_*(T) = \{\sum a_i\lambda_i \mid \sum a_i = 0\}, \quad t \overset{\sum a_i\lambda_i}{\longmapsto} \mathrm{diag}(t^{a_1},\dots,t^{a_n}), \quad a_i \in \mathbb{Z},$$

with the obvious pairing $\langle\ ,\ \rangle$. Write $\overline{\chi}_i$ for the class of $\chi_i$ in $X^*(T)$. Then all the characters $\overline{\chi}_i - \overline{\chi}_j$, $i \neq j$, 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 $\mathrm{GL}_n$.

**Example ($\mathbf{B}_n$):** $\mathrm{SO}_{2n+1}$ .

Consider the symmetric bilinear form $\phi$ 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 $\mathrm{SO}_{2n+1} =_{\mathrm{df}} \mathrm{SO}(\phi)$ 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 $\mathrm{SO}_{2n+1}$ consists of the $2n+1 \times 2n+1$ matrices $A$ of trace 0 such that

$$\phi(A\vec{x},\vec{y}) = -\phi(\vec{x},A\vec{y}),$$

(12.15), 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

$$\mathrm{diag}(1,t_1,\dots,t_n,t_1^{-1},\dots,t_n^{-1})$$

Then

$$X^*(T) = \bigoplus\nolimits_{1\le i\le n}\mathbb{Z}\chi_i, \quad \mathrm{diag}(1,t_1,\dots,t_n,t_1^{-1},\dots,t_n^{-1}) \overset{\chi_i}{\longmapsto} t_i$$
$$X_*(T) = \bigoplus\nolimits_{1\le i\le n}\mathbb{Z}\lambda_i, \quad t \overset{\lambda_i}{\longmapsto} \mathrm{diag}(1,\dots,\overset{i+1}{t},\dots,1)$$

with the obvious pairing $\langle\ ,\ \rangle$. All the characters

$$\pm\chi_i, \quad \pm\chi_i \pm \chi_j, \quad i \ne j$$

occur as roots, and their coroots are, respectively,

$$\pm 2\lambda_i, \quad \pm\lambda_i \pm \lambda_j, \quad i \ne j.$$

**Example ($\mathbf{C}_n$):** $\mathrm{Sp}_{2n}$ .

Consider the skew symmetric bilinear form $k^{2n} \times k^{2n} \to k$,

$$\phi(\vec{x},\vec{y}) = x_1y_{n+1} - x_{n+1}y_1 + \cdots + x_ny_{2n} - x_{2n}y_n.$$

Then $\mathrm{Sp}_{2n}$ 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 $\mathrm{Sp}_n$ 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

$$X^*(T) = \bigoplus\nolimits_{1 \le i \le n} \mathbb{Z}\chi_i, \quad \mathrm{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \overset{\chi_i}{\longmapsto} t_i$$
$$X_*(T) = \bigoplus\nolimits_{1 \le i \le n} \mathbb{Z}\lambda_i, \quad t \overset{\lambda_i}{\longmapsto} \mathrm{diag}(1, \dots, \overset{i}{t}, \dots, 1)$$

with the obvious pairing $\langle\ ,\ \rangle$. All the characters

$$\pm 2\chi_i, \quad \pm\chi_i \pm \chi_j, \quad i \ne j$$

occur as roots, and their coroots are, respectively,

$$\pm\lambda_i, \quad \pm\lambda_i \pm \lambda_j, \quad i \ne j.$$

**Example ($\mathbf{D}_n$):** $\mathrm{SO}_{2n}$ .

Consider the symmetric bilinear form $k^{2n} \times k^{2n} \to k$,

$$\phi(\vec{x}, \vec{y}) = x_1 y_{n+1} + x_{n+1} y_1 + \cdots + x_n y_{2n} + x_{2n} y_{2n}.$$

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 $\mathrm{SO}_n$ 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 $\chi_i$, $1 \le i \le r$, be the character

$$\mathrm{diag}(t_1,\dots,t_n,t_1^{-1},\dots,t_n^{-1}) \mapsto t_i.$$

All the characters

$$\pm\chi_i \pm \chi_j, \quad i \ne j$$

occur, and their coroots are, respectively,

$$\pm\lambda_i \pm \lambda_j, \quad i \ne j.$$

REMARK 17.21 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.

# 18 Generalities on root data

## Definition

The following is the standard definition.

DEFINITION 18.1 A root datum is an ordered quadruple $\Psi = (X, \Phi, X^\vee, \Phi^\vee)$ where
- $\diamond$ $X, X^\vee$ are free $\mathbb{Z}$-modules of finite rank in duality by a pairing $\langle\ ,\ \rangle\colon X \times X^\vee \to \mathbb{Z}$,
- $\diamond$ $\Phi, \Phi^\vee$ 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** $s_\alpha(\Phi) \subset \Phi$, $s_\alpha^\vee(\Phi^\vee) \subset \Phi^\vee$, where

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad \text{for } x \in X, \alpha \in \Phi,$$
$$s_\alpha^\vee(y) = y - \langle \alpha, y \rangle \alpha^\vee, \quad \text{for } y \in X^\vee, \alpha \in \Phi.$$

Recall that RD1 implies that $s_\alpha(\alpha) = -\alpha$ and $s_\alpha^2 = 1$.

Set[59]

$$Q = \mathbb{Z}\Phi \subset X \qquad Q^\vee = \mathbb{Z}\Phi^\vee \subset X^\vee$$
$$V = \mathbb{Q} \otimes_{\mathbb{Z}} Q \qquad V^\vee = \mathbb{Q} \otimes_{\mathbb{Z}} Q^\vee.$$
$$X_0 = \{x \in X \mid \langle x, \Phi^\vee \rangle = 0\}$$

By $\mathbb{Z}\Phi$ we mean the $\mathbb{Z}$-submodule of $X$ generated by the $\alpha \in \Phi$.

LEMMA 18.2 *For $\alpha \in \Phi$, $x \in X$, and $y \in X^\vee$,*

$$\langle s_\alpha(x), y \rangle = \langle x, s_\alpha^\vee(y) \rangle, \tag{65}$$

*and so*

$$\langle s_\alpha(x), s_\alpha^\vee(y) \rangle = \langle x, y \rangle. \tag{66}$$

PROOF. We have

$$\langle s_\alpha(x), y \rangle = \langle x - \langle x, \alpha^\vee \rangle \alpha, y \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle$$
$$\langle x, s_\alpha^\vee(y) \rangle = \langle x, y - \langle \alpha, y \rangle \alpha^\vee \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle,$$

which gives the first formula, and the second is obtained from the first by replacing $y$ with $s_\alpha^\vee(y)$. □

In other words, as the notation suggests, $s_\alpha^\vee$ (which is sometimes denoted $s_{\alpha^\vee}$) is the transpose of $s_\alpha$.

LEMMA 18.3 *The following hold for the mapping*

$$p\colon X \to X^\vee, \quad p(x) = \sum_{\alpha \in \Phi} \langle x, \alpha^\vee \rangle \alpha^\vee.$$

*(a) For all $x \in X$,*

$$\langle x, p(x) \rangle = \sum\nolimits_{\alpha \in \Phi} \langle x, \alpha^\vee \rangle^2 \geq 0, \tag{67}$$

*with strict inequality holding if $x \in \Phi$.*

[59] The notation $Q^\vee$ is a bit confusing, because $Q^\vee$ is not in fact the dual of $Q$.

*(b) For all $x \in X$ and $w \in W$,*

$$\langle wx, p(wx)\rangle = \langle x, p(x)\rangle. \tag{68}$$

*(c) For all $\alpha \in \Phi$,*

$$\langle \alpha, p(\alpha)\rangle \alpha^\vee = 2p(\alpha), \quad \text{all } \alpha \in \Phi. \tag{69}$$

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 (67) 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

$$\begin{aligned} -\langle \alpha, y\rangle &= \langle s_\alpha(\alpha), y\rangle \\ &\overset{(65)}{=} \langle \alpha, s_\alpha^\vee(y)\rangle \end{aligned}$$

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 $\Phi^\vee$, so also does $s_\alpha^\vee(y)$, and so when we sum over $y \in \Phi^\vee$, we obtain (69). □

REMARK 18.4 Suppose $m\alpha$ is also a root. On replacing $\alpha$ with $m\alpha$ in (69) and using that $p$ is a homomorphism of $\mathbb{Z}$-modules, we find that

$$m\langle \alpha, p(\alpha)\rangle (m\alpha)^\vee = 2p(\alpha), \quad \text{all } \alpha \in \Phi.$$

Therefore,

$$(m\alpha)^\vee = m^{-1}\alpha^\vee. \tag{70}$$

In particular,

$$(-\alpha)^\vee = -(\alpha^\vee). \tag{71}$$

LEMMA 18.5 *The map $p\colon X \to X^\vee$ defines an isomorphism*

$$1 \otimes p\colon V \to V^\vee.$$

*In particular,* $\dim V = \dim V^\vee$.

PROOF. As $\langle \alpha, p(\alpha)\rangle \neq 0$, (69) shows that $p(Q)$ has finite index in $Q^\vee$. Therefore, when we tensor $p\colon Q \to Q^\vee$ with $\mathbb{Q}$, we get a surjective map $1 \otimes p\colon V \to V^\vee$; in particular, $\dim V \geq \dim V^\vee$. The definition of a root datum is symmetric between $(X, \Phi)$ and $(X^\vee, \Phi^\vee)$, and so the symmetric argument shows that $\dim V^\vee \leq \dim V$. Hence

$$\dim V = \dim V^\vee,$$

and $1 \otimes p\colon V \to V^\vee$ is an isomorphism. □

LEMMA 18.6 *The kernel of $p: X \to X^\vee$ is $X_0$.*

PROOF. Clearly, $X_0 \subset \mathrm{Ker}(p)$, but (67) proves the reverse inclusion. □

PROPOSITION 18.7 *We have*

$$Q \cap X_0 = 0$$
$$Q + X_0 \text{ is of finite index in } X.$$

*Thus, there is an exact sequence*

$$0 \to Q \oplus X_0 \xrightarrow{(q,x)\mapsto q+x} X \to \text{finite group} \to 0.$$

PROOF. The map

$$1 \otimes p: \mathbb{Q} \otimes X \to V^\vee$$

has kernel $\mathbb{Q} \otimes X_0$ (see 18.6) and maps the subspace $V$ of $\mathbb{Q} \otimes X$ isomorphically onto $V^\vee$ (see 18.5). This implies that

$$(\mathbb{Q} \otimes_{\mathbb{Z}} X_0) \oplus V \simeq \mathbb{Q} \otimes X,$$

from which the proposition follows. □

LEMMA 18.8 *The bilinear form $\langle\ ,\ \rangle$ defines a nondegenerate pairing $V \times V^\vee \to \mathbb{Q}$.*

PROOF. Let $x \in X$. If $\langle x, \alpha^\vee\rangle = 0$ for all $a^\vee \in \Phi^\vee$, then $x \in \mathrm{Ker}(p) = X_0$. □

LEMMA 18.9 *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. □

Recall that the Weyl group $W = W(\Psi)$ of $\Psi$ is the subgroup of $\mathrm{Aut}(X)$ generated by the $s_\alpha$, $\alpha \in \Phi$. 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 $s_\alpha$ act on $X^\vee$ as $(s_\alpha^\vee)^{-1} = s_\alpha^\vee$ (see 65).

PROPOSITION 18.10 *The Weyl group $W$ acts faithfully on $\Phi$ (and so is finite).*

PROOF. By symmetry, it is equivalent to show that $W$ acts faithfully on $\Phi^\vee$. Let $w$ be an element of $W$ such that $w(\alpha) = \alpha$ for all $\alpha \in \Phi^\vee$. 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 $\Phi^\vee$. As it lies in $Q$ (see 18.9), this implies that it is zero (18.8), and so $w = 1$. □

Thus, a root datum in the sense of (18.1) is a root datum in the sense of (17.1), and the next proposition proves the converse.

PROPOSITION 18.11 *Let $\Psi = (X, \Phi, X^\vee, \Phi^\vee)$ be a system satisfying the conditions (rd1), (rd2), (rd3) of (17.1). Then $\Psi$ is a root datum.*

PROOF. We have to show that

$$s_\alpha^\vee(\Phi^\vee) \subset \Phi^\vee \text{ where } s_\alpha^\vee(y) = y - \langle \alpha, y\rangle \alpha^\vee.$$

As in Lemma 18.2, $\langle s_\alpha(x), s_\alpha^\vee(y)\rangle = \langle x, y\rangle$.

Let $\alpha, \beta \in \Phi$, and let $t = s_{s_\alpha(\beta)} s_\alpha s_\beta s_\alpha$. An easy calculation[60] 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 $t(s_a(\beta)) = s_\alpha(\beta)$. Thus,

$$(t-1)^2 = 0,$$

and so the minimum polyonomial 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

$$s_\alpha^\vee(\beta^\vee) = s_\alpha(\beta)^\vee \in \Phi^\vee. \qquad \square$$

REMARK 18.12 To give a root datum amounts to giving a triple $(X, \Phi, f)$ where

- $\diamond$ $X$ is a free abelian group of finite rank,
- $\diamond$ $\Phi$ is a finite subset of $X$, and
- $\diamond$ $f$ is an injective map $\alpha \mapsto \alpha^\vee$ from $\Phi$ into the dual $X^\vee$ of $X$

satisfying the conditions (rd1), (rd2), (rd3) of (17.1).

[60] Or so it is stated in Springer 1979, 1.4 (Corvallis).

# 19 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

Let $V$ be a finite-dimensional vector space over $F$, and let $\alpha$ be a nonzero element of $V$. A ***symmetry with vector*** $\alpha$ is an automorphism 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 $\mathrm{Hom}_{\mathbb{Q}\text{-lin}}(V, F)$ of $V$, and write $\langle x, f\rangle$ for $f(x)$. The composite

$$V \to V/H \overset{\alpha+H\mapsto 2}{\longrightarrow} F$$

is the unique element $\alpha^\vee$ of $V^\vee$ such that $\alpha(H) = 0$ and $\langle\alpha, \alpha^\vee\rangle = 2$; moreover,

$$s(x) = x - \langle x, \alpha^\vee\rangle\alpha \quad \text{all } x \in V. \tag{72}$$

In this way, symmetries with vector $\alpha$ are in one-to-one correspondence with vectors $\alpha^\vee$ such that $\langle\alpha, \alpha^\vee\rangle = 2$.

LEMMA 19.1 *Let $\Phi$ be a finite subset of $V$ that spans $V$. Then, for any nonzero vector $\alpha$ in $V$, there exists at most one symmetry $s$ with vector $\alpha$ such that $\alpha(\Phi) \subset \Phi$.*

PROOF. Let $s, s'$ be such symmetries, and let $t = ss'$. Then $t$ defines the identity map on both $F\alpha$ and on $V/F\alpha$, and so

$$(t-1)^2V \subset (t-1)F\alpha = 0.$$

Thus the minimum polynomial of $t$ divides $(T-1)^2$. On the other hand, because $\Phi$ is finite, there exists an integer $m \geq 1$ such that $t^m(x) = x$ for all $x \in \Phi$ and hence for all $x \in V$. Therefore the minimum polyomial of $t$ divides $T^m - 1$, and hence also

$$\gcd((T-1)^2, T^m - 1) = T - 1.$$

This shows that $t = 1$. □

LEMMA 19.2 *Let $(\ ,\ )$ be an inner product on a real vector space $V$. Then, for any nonzero vector $\alpha$ in $V$, there exists a unique symmetry $s$ with vector $\alpha$ that is orthogonal for $(\ ,\ )$, i.e., such that $(sx, sy) = (x, y)$ for all $x, y \in V$, namely*

$$s(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha. \tag{73}$$

PROOF. Certainly, (73) does define an orthogonal symmetry with vector $\alpha$. 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 $s$. □

## Generalities on lattices

In this subsection $V$ is a finite-dimensional vector space over $F$.

DEFINITION 19.3 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 $F \otimes_{\mathbb{Z}} X \to V$ is an isomorphism.

REMARK 19.4 (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 19.5 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 $\pm 1$.

PROPOSITION 19.6 *Let*

$$\langle\ ,\ \rangle : V \times V^\vee \to k$$

*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*

$$X \times Y \to \mathbb{Z}.$$

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

$$Y = \mathbb{Z}e_1' + \cdots + \mathbb{Z}e_n',$$

and so it is a lattice, and it is clear that $\langle\ ,\ \rangle$ restricts to a perfect pairing $X \times Y \to \mathbb{Z}$.

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 $X \times Y' \to \mathbb{Z}$ is $\pm(Y : Y')$, and so the pairing on $X \times Y'$ is perfect if and only if $Y' = Y$. □

## Root systems

DEFINITION 19.7 A ***root system*** is a pair $(V, \Phi)$ with $V$ a finite-dimensional vector space over $F$ and $\Phi$ a finite subset of $V$ such that

**RS1** $\Phi$ spans $V$ and does not contain 0;
**RS2** for each $\alpha \in \Phi$, there exists a symmetry $s_\alpha$ with vector $\alpha$ such that $s_\alpha(\Phi) \subset \Phi$;
**RS3** for all $\alpha, \beta \in \Phi$, $\langle \beta, \alpha^\vee\rangle \in \mathbb{Z}$.

In (RS3), $\alpha^\vee$ is the element of $V^\vee$ corresponding to $s_\alpha$. Note that (19.1) shows that $s_\alpha$ (hence also $\alpha^\vee$) is uniquely determined by $\alpha$.

The elements of $\Phi$ are called the ***roots*** of the root system. If $\alpha$ is a root, then $s_\alpha(\alpha) = -\alpha$ is also a root. If $t\alpha$ is also a root, then (RS3) shows that $t = \frac{1}{2}$ or 2. A root system $(V, \Phi)$ is ***reduced*** if no multiple of a root except its negative is a root.

The ***Weyl group*** $W = W(\Phi)$ of $(V, \Phi)$ is the subgroup of $\mathrm{GL}(V)$ generated by the symmetries $s_\alpha$ for $\alpha \in \Phi$. Because $\Phi$ spans $V$, $W$ acts faithfully on $\Phi$; in particular, it is finite.

PROPOSITION 19.8 *Let $(V, \Phi)$ be a root system over $F$, and let $V_0$ be the $\mathbb{Q}$-vector space generated by $\Phi$. Then*

(a) *the natural map $F \otimes_{\mathbb{Q}} V_0 \to V$ is an isomorphism;*
(b) *the pair $(V_0, \Phi)$ is a root system over $\mathbb{Q}$.*

PROOF. For a proof of the proposition, see Serre 1987, p42. □

Thus, to give a root system over $\mathbb{R}$ or $\mathbb{C}$ amounts to giving a root system over $\mathbb{Q}$.

## Root systems and semisimple root data

Compare (18.12; 19.7):

| Semisimple root datum | Root system (over $\mathbb{Q}$) |
|---|---|
| $X, \Phi, \alpha \mapsto \alpha^\vee : \Phi \hookrightarrow X^\vee$ | $V, \Phi$ |
| $\Phi$ is finite | $\Phi$ is finite |
| $(X : \mathbb{Z}\Phi)$ finite | $\Phi$ spans $V$ |
| | $0 \notin \Phi$ |
| $\langle \alpha, \alpha^\vee \rangle = 2$, $s_\alpha(\Phi) \subset \Phi$ | $\exists s_\alpha$ such that $s_\alpha(\Phi) \subset \Phi$ |
| | $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$, all $\alpha, \beta \in \Phi$ |
| Weyl group finite | |

For a root system $(V, \Phi)$, let $Q = \mathbb{Z}\Phi$ be the $\mathbb{Z}$-submodule of $V$ generated by $\Phi$ and let $Q^\vee$ be the $\mathbb{Z}$-submodule of $V^\vee$ generated by the $\alpha^\vee$, $\alpha \in \Phi$. Then, $Q$ and $Q^\vee$ are lattices[61] 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 19.6), and because of (RS3),

$$Q \subset P. \tag{74}$$

PROPOSITION 19.9 *If $(X, \Phi, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum, then $(\mathbb{Q} \otimes_{\mathbb{Z}} X, \Phi)$ is a root system over $\mathbb{Q}$. Conversely, if $(V, \Phi)$ is root system over $\mathbb{Q}$, then for any choice $X$ of a lattice in $V$ such that*

$$Q \subset X \subset P \tag{75}$$

*$(X, \Phi, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum.*

PROOF. If $(X, \Phi, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum, then $0 \notin \Phi$ because $\langle \alpha, \alpha^\vee \rangle = 2$, and $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$ because $\alpha^\vee \in X^\vee$. Therefore $(\mathbb{Q} \otimes_{\mathbb{Z}} X, \Phi)$ is a root system.

Conversely, let $(V, \Phi)$ be a root system. Let $X$ satisfy (75), and let $X^\vee$ denote the lattice in $V^\vee$ in duality with $X$ (see 19.6). For each $\alpha \in \Phi$, there exists an $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and $s_\alpha(\Phi) \subset \Phi$ (because $(V, \Phi)$ is a root datum), and (19.1) shows that it is unique. Therefore, we have a function $\alpha \mapsto \alpha^\vee : \Phi \to V^\vee$ which takes its values in $X^\vee$ (because $X \subset P$ implies $X^\vee \supset \Phi^\vee$), and is injective. The Weyl group of $(X, \Phi, \alpha \mapsto \alpha^\vee)$ is the Weyl group of $(V, \Phi)$, which, as we noted above, is finite. Therefore $(X, \Phi, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum. □

[61] They are finitely generated, and $\Phi^\vee$ spans $V^\vee$ by Serre 1987, p28.

## The big picture

Recall that the base field $k$ (for $G$) has characteristic zero.

$$\begin{array}{ccc} \text{Split reductive groups} & \leftrightarrow & \text{Reduced root data} \\ \vdots & & \vdots \\ \text{Split semisimple groups} & \leftrightarrow & \text{Reduced semisimple root data} \\ \downarrow & & \downarrow \\ \text{Lie algebras} & \overset{k=\bar{k}}{\leftrightarrow} & \text{Reduced root systems} \end{array}$$

19.10 As we discussed in (§17), the reduced root data classify the split reductive groups over $k$.

19.11 As we discussed in (15.1), from a reductive group $G$, we get semisimple groups $\mathcal{D}G$ and $G/Z(G)$ together with an isogeny $\mathcal{D}G \to G/Z(G)$. Conversely, every reductive group $G$ can be built up from a semisimple group and a torus (15.2).

19.12 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.

19.13 From a semisimple group $G$ we get a semisimple Lie algebra $\mathrm{Lie}(G)$ (see 14.1), and from $\mathrm{Lie}(G)$ we can recover $G/Z(G)$ (see 14.9). Passing from $G$ to $\mathrm{Lie}(G)$ amounts to forgetting the centre of $G$.

19.14 From a semisimple root datum $(X, \Phi, \alpha \mapsto \alpha^\vee)$, we get a root system $(V = \mathbb{Q} \otimes_{\mathbb{Z}} X, \Phi)$. Passing from the semisimple root datum to the root system amounts to forgetting the lattice $X$ in $V$.

19.15 Take $k = \bar{k}$, 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 $\mathrm{ad}\colon \mathfrak{h} \to \mathrm{End}(\mathfrak{g})$, i.e., for $h \in \mathfrak{h}$, $x \in \mathfrak{g}$, $\mathrm{ad}(h)(x) = [h, x]$. One shows that $\mathfrak{g}$ decomposes as a sum

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus\nolimits_{\alpha \in \mathfrak{h}^\vee} \mathfrak{g}_\alpha$$

where $\mathfrak{g}_0$ is the subspace on which $\mathfrak{h}$ acts trivially, and hence equals $\mathfrak{h}$, and $\mathfrak{g}_\alpha$ is the subspace on which $\mathfrak{h}$ acts through the linear form $\alpha\colon \mathfrak{h} \to k$, i.e., for $h \in \mathfrak{h}$, $x \in \mathfrak{g}_\alpha$, $[h, x] = \alpha(h)x$. The nonzero $\alpha$ occurring in the above decomposition form a reduced root system $\Phi$ in $\mathfrak{h}^\vee$ (and hence in the $\mathbb{Q}$-subspace of $\mathfrak{h}^\vee$ spanned by $\Phi$ — see 19.8). In this way, the semisimple Lie algebras over $k$ are classified by the reduced root systems (see Serre 1987, VI).

## Classification of the reduced root system

After (19.8), we may as well work with root systems over $\mathbb{R}$.

PROPOSITION 19.16 *For any root system $(V, \Phi)$, there exists an inner product $(\ ,\ )$ on $V$ such that the $s_\alpha$ act as orthogonal transformations, i.e., such that*

$$(s_\alpha x, s_\alpha y) = (x, y), \quad \text{all } \alpha \in \Phi, \quad x, y \in V.$$

PROOF. Let $(\ ,\ )'$ be any inner product $V \times V \to \mathbb{R}$, 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 $ww_0$. □

REMARK 19.17 There is in fact a canonical inner product on $V$, namely, the form induced by $x, y \mapsto (x, p(x))$ (see 18.3).

Thus, we may as well equip $V$ with an inner product $(\ ,\ )$ as in the proposition. On comparing (73) with (72)

$$\begin{aligned}s_\alpha(x) &= x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha, \\ s_\alpha(x) &= x - \langle x, \alpha^\vee\rangle\alpha,\end{aligned}$$

we see that

$$\langle x, \alpha^\vee\rangle = 2\frac{(x,\alpha)}{(\alpha,\alpha)}. \tag{76}$$

Thus (RS3) becomes the condition:

$$2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}, \text{ all } \alpha, \beta \in \Phi.$$

**Study of two roots**

Let $\alpha, \beta \in \Phi$, and let $n(\beta,\alpha) = 2\frac{(\beta,\alpha)}{(\alpha,\alpha)}$. We wish to examine the significance of the condition $n(\beta,\alpha) \in \mathbb{Z}$. Write

$$n(\beta,\alpha) = 2\frac{|\beta|}{|\alpha|}\cos\phi$$

where $|\cdot|$ denotes the length of a vector and $\phi$ is the angle between $\alpha$ and $\beta$. Then

$$n(\beta,\alpha)\cdot n(\alpha,\beta) = 4\cos^2\phi \in \mathbb{Z}. \tag{77}$$

Excluding the possibility that $\beta$ is a multiple of $\alpha$, there are only the following possibilities (in the table, we have chosen $\beta$ to be the longer root).

| $n(\beta,\alpha)\cdot n(\alpha,\beta)$ | $n(\alpha,\beta)$ | $n(\beta,\alpha)$ | $\phi$ | $\lvert\beta\rvert/\lvert\alpha\rvert$ |
|---|---|---|---|---|
| 0 | 0 | 0 | $\pi/2$ | |
| 1 | 1 | 1 | $\pi/3$ | 1 |
| | $-1$ | $-1$ | $2\pi/3$ | |
| 2 | 1 | 2 | $\pi/4$ | $\sqrt{2}$ |
| | $-1$ | $-2$ | $3\pi/4$ | |
| 3 | 1 | 3 | $\pi/6$ | $\sqrt{3}$ |
| | $-1$ | $-3$ | $5\pi/6$ | |

The proof of this is an exercise for the reader, who should also draw the appropriate pictures.

REMARK 19.18 Let $\alpha$ and $\beta$ be roots with neither a multiple of the other. Clearly, $n(\alpha,\beta)$ and $n(\beta,\alpha)$ are either both positive or both negative. From the table, we see that in the first case at least one of $n(\alpha,\beta)$ or $n(\beta,\alpha)$ equals 1. If it is, say, $n(\beta,\alpha)$, then

$$s_\alpha(\beta) = \beta - n(\beta,\alpha)\alpha = \beta - \alpha,$$

and so $\pm(\alpha-\beta)$ are roots.

**Bases**

DEFINITION 19.19 A ***base*** for $\Phi$ is a subset $S$ such that

(a) $S$ is a basis for $V$ (as an $\mathbb{R}$-vector space), and

(b) when we express a root $\beta$ as a linear combination of elements of $S$,

$$\beta = \sum\nolimits_{\alpha\in S} m_\alpha\alpha,$$

the $m_\alpha$ are 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 $S$ are often called the ***simple roots***(for the base).

PROPOSITION 19.20 *There exists a base $S$ for $\Phi$.*

PROOF. Serre 1987, V 8. The idea of the proof is the following. Choose a vector $t$ in the dual vector space $V^\vee$ such that, for all $\alpha\in\Phi$, $\langle\alpha,t\rangle\neq 0$, and set

$$\Phi^+ = \{\alpha \mid \langle\alpha,t\rangle > 0\}$$
$$\Phi^- = \{\alpha \mid \langle\alpha,t\rangle < 0\}$$

(so $\Phi = \Phi^- \sqcup \Phi^+$). Say that an $\alpha\in\Phi^+$ is ***decomposable*** if it can be written as a sum $\alpha=\beta+\gamma$ with $\beta,\gamma\in\Phi^+$, and otherwise is ***indecomposable***. One shows that the indecomposable elements form base. □

REMARK 19.21 Let $\alpha$ and $\beta$ be simple roots, and suppose $n(\alpha,\beta)$ and $n(\beta,\alpha)$ are positive (i.e., the angle between $\alpha$ and $\beta$ is acute). Then (see 19.18), both of $\alpha-\beta$ and $\beta-\alpha$ are roots, and one of them, say, $\alpha-\beta$, will be in $\Phi^+$. But then $\alpha = (\alpha-\beta)+\beta$, contradicting the simplicity of $\alpha$. We conclude that $n(\beta,\alpha)$ and $n(\alpha,\beta)$ are negative.

EXAMPLE 19.22 Consider the root system of type $A_n$, i.e., that attached to $\mathrm{SL}_{n+1}$ (see p124). We can take $V$ to be the subspace[62] of $\mathbb{R}^{n+1}$ of $n+1$-tuples such that $\sum x_i = 0$ with the usual inner product, and $\Phi = \{e_i - e_j \mid i\neq j\}$ with $e_1,\dots,e_{n+1}$ the standard basis of $\mathbb{R}^{n+1}$. When we choose $t = ne_1+\cdots+e_n$,

$$\Phi^+ = \{e_i - e_j \mid i > j\}.$$

For $i > j+1$,

$$e_i - e_j = (e_i - e_{i-1}) + \cdots + (e_{j+1} - e_j)$$

is decomposable, and so the indecomposable elements are $e_1-e_2,\dots,e_n-e_{n+1}$. They obviously form a base.

[62]The naturally occurring space is $\mathbb{R}^{n+1}$ modulo the line $\mathbb{R}(e_1+\cdots+e_{n+1})$, but $V$ is the hyperplane orthogonal to this line and contains the roots, and so this gives an isomorphic root system. Alternatively, it is naturally the dual $\Phi^\vee$.

### Action of the Weyl group

Recall that $W = W(\Phi)$ is the subgroup of $\mathrm{GL}(V)$ generated by $\{s_\alpha \mid \alpha \in \Phi\}$.

PROPOSITION 19.23 *Let $S$ be a base for $\Phi$. Then*
(a) *$W$ is generated by the $s_\alpha$ for $\alpha \in S$;*
(b) *$W \cdot S = \Phi$;*
(c) *if $S'$ is a second base for $\Phi$, then $S' = wS$ for some $w \in W$.*

PROOF. Serre 1987, V 10. □

EXAMPLE 19.24 For the root system $A_n$,

$$\begin{aligned} s_{\alpha_{ij}}(\vec{x}) &= \vec{x} - 2\frac{(\vec{x}, \alpha_{ij})}{(\alpha_{ij}, \alpha_{ij})}\alpha_{ij}, \quad \alpha_{ij} = e_i - e_j, \\ &= \vec{x} + (0, \dots, 0, x_j \overset{i}{-} x_i, 0, \dots, 0, x_i \overset{j}{-} x_j, 0, \dots, 0) \\ &= (x_1, \dots, \overset{i}{x_j}, \dots, \overset{j}{x_i}, \dots, x_{n+1}). \end{aligned}$$

Thus, $s_{\alpha_{ij}}$ switches the $i^{\text{th}}$ and $j^{\text{th}}$ coordinates. It follows that $W$ has a natural identification with the symmetric group $S_{n+1}$, and it is certainly generated by the elements $s_{\alpha_{ii+1}}$. Moreover, $W \cdot S = \Phi$.

### Cartan matrix

For a choice $S$ of a base, the ***Cartan matrix*** is $(n(\alpha, \beta))_{\alpha,\beta \in S}$. Thus, its diagonal terms equal 2 and its off-diagonal terms are negative or zero (19.21).

PROPOSITION 19.25 *The Cartan matrix doesn't depend on the choice of $S$, and it determines the root system up to isomorphism.*

PROOF. The first assertion follows from (19.23c). For the second, let $(V, \Phi)$ and $(V', \Phi')$ be root systems such that for some bases $S$ and $S'$ there is a bijection $\alpha \mapsto \alpha' : S \to S'$ such that $n(\alpha, \beta) = n(\alpha', \beta')$. The bijection $\alpha \mapsto \alpha'$ extends uniquely to an isomorphism of vector spaces $x \mapsto x' : V \to V'$. Because

$$s_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha,$$

this isomorphism sends $s_\alpha$ to $s_{\alpha'}$ for $\alpha \in S$. Because of (19.23a), it maps $W$ onto $W'$, which (by 19.23b) implies that it maps $\Phi$ onto $\Phi'$. □

EXAMPLE 19.26 For the root system $A_n$ and the obvious base $S$, the Cartan matrix 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

$$2\frac{(e_i - e_{i+1}, e_{i+1} - e_{i+2})}{(e_i - e_{i+1}, e_i - e_{i+1})} = -1,$$

for example.

## The Coxeter graph

This is the graph with nodes indexed by the elements of a base $S$ for $\Phi$ and with two nodes joined by $n(\alpha,\beta)\cdot n(\beta,\alpha)$ edges.

We can define the direct sum of two root systems

$$(V,\Phi) = (V_1,\Phi_1)\oplus(V_2,\Phi_2)$$

by taking $V = V_1 \oplus V_2$ (as vector spaces with inner product) and by taking $\Phi = \Phi_1 \cup \Phi_2$. A root system is ***indecomposable*** if it can't be written as a direct sum of two nonzero root systems.

PROPOSITION 19.27 *A root system is indecomposable if and only if its Coxeter graph is connected.*

PROOF. One shows that a root system is decomposable if and only if $\Phi$ can be written as a disjoint union $\Phi = \Phi_1 \sqcup \Phi_2$ with each root in $\Phi_1$ orthogonal to each root in $\Phi_2$. Since roots $\alpha,\beta$ are orthogonal if and only $n(\alpha,\beta)\cdot n(\beta,\alpha) = 4\cos^2\phi = 0$, this is equivalent to the Coxeter graph being disconnected. □

Clearly, it suffices to classify the indecomposable root systems.

### The Dynkin diagram

The Coxeter graph doesn't determine the root system because for any two base roots $\alpha,\beta$, 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

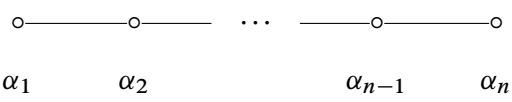
$$\{n(\alpha,\beta), n(\beta,\alpha)\} = \{2\frac{|\alpha|}{|\beta|}\cos\phi, 2\frac{|\beta|}{|\alpha|}\cos\phi\}.$$

Thus, if we know in addition which is the longer root, then we know the ***ordered*** pair. The ***Dynkin diagram*** is the Coxeter graph with an arrow added pointing towards the shorter root (if the roots have different lengths). It determines the Cartan matrix and hence the root system. Specifically, to compute the Cartan matrix from the Dynkin diagram, number the simple roots $\alpha_1,\dots,\alpha_n$, and let $a_{ij} = n(\alpha_i,\beta_j)$ be the $ij^{\text{th}}$ coefficient of the Cartan matrix; then

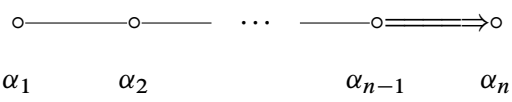
for all $i$, $a_{ii} = 2$;
if $\alpha_i$ and $\alpha_j$ are not joined by an edge, then $a_{ij} = 0 = a_{ji}$;
if $\alpha_i$ and $\alpha_j$ are joined by an edge and $|\alpha_i| \le |\alpha_j|$, then $a_{ij} = -1$;
if $\alpha_i$ and $\alpha_j$ are joined by $r$ edges and $|\alpha_i| > |\alpha_j|$, then $a_{ij} = -r$.

THEOREM 19.28 *The Dynkin diagrams arising from reduced indecomposable root systems are exactly those listed below.*

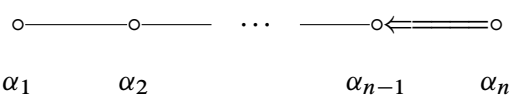
PROOF. See Humphreys 1979, 11.4, pp 60–62. □

$A_n$:  $n \geq 1$

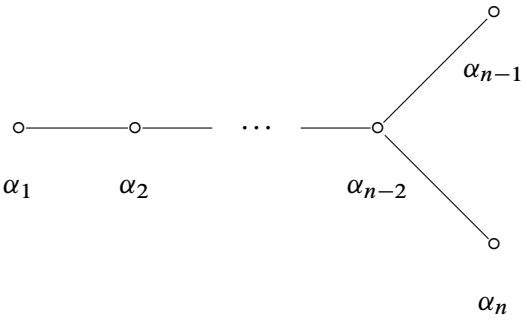


$B_n$:  $(n \geq 2)$

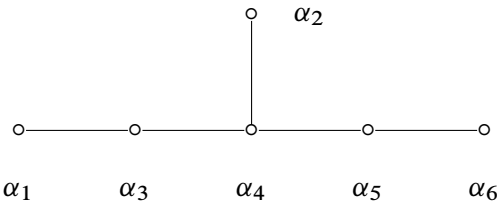


$C_n$:  $(n \geq 3)$

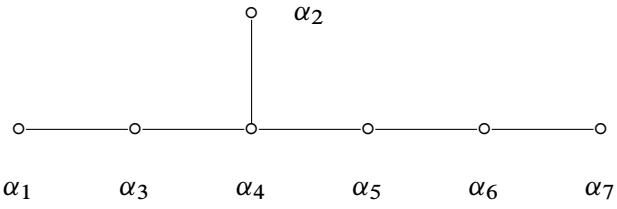


$D_n$:  $(n \geq 4)$

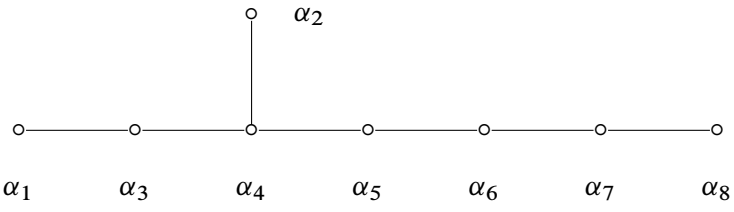


$E_6$: 

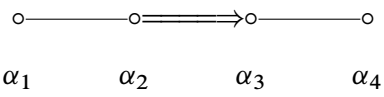


$E_7$: 



$E_8$: 



$F_4$: 



$G_2$:Omitted for the present.

# 20 The construction of all split reductive groups

Throughout this section, $k$ is a field of characteristic zero.

### Preliminaries on root data/systems

Recall (19.9) that semisimple root data (hence semisimple algebraic groups) correspond to reduced root systems $(V, \Phi)$ together with a choice of a lattice $X$,

$$Q \subset X \subset P$$

where $Q = \mathbb{Z}\Phi$ and $P$ is the lattice in duality with $\mathbb{Z}\Phi^\vee$. Thus

$$P = \{x \in V \mid \langle x, \alpha^\vee\rangle \in \mathbb{Z}, \quad \text{all } \alpha \in \Phi\}.$$

When we take $V$ to be a real vector space and choose an inner product as in (19.16), this becomes

$$P = \left\{ x \in V \;\middle|\; 2\frac{(x,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}, \quad \text{all } \alpha \in \Phi \right\}.$$

Choose a base $S = \{\alpha_1, \dots, \alpha_n\}$ for $\Phi$ (see 19.19). Then

$$Q = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n,$$

and we want to find a basis for $P$. Let $\{\lambda_1, \dots, \lambda_n\}$ be the basis of $V$ dual to the basis

$$\left\{ \frac{2}{(\alpha_1,\alpha_1)}\alpha_1, \dots, \frac{2}{(\alpha_i,\alpha_i)}\alpha_i, \dots, \frac{2}{(\alpha_n,\alpha_n)}\alpha_n \right\},$$

i.e., $(\lambda_i)_{1\le i\le n}$ is characterized by

$$2\frac{(\lambda_i,\alpha_j)}{(\alpha_j,\alpha_j)} = \delta_{ij} \quad \text{(Kronecker delta)}.$$

PROPOSITION 20.1 *The set $\{\lambda_1, \dots, \lambda_n\}$ is a basis for $P$, i.e.,*

$$P = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n.$$

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 20.2 *Let $\Phi$ be a reduced root system, and let $\Phi'$ be the root system consisting of the vectors $\alpha' = \frac{2}{(\alpha,\alpha)}\alpha$ for $\alpha \in \Phi$. For any base $S$ for $\Phi$, the set $S' = \{\alpha' \mid \alpha \in S\}$ is a base for $\Phi'$.*

PROOF. See Serre 1987, V 9, Proposition 7. □

PROPOSITION 20.3 *For each $j$,*

$$\alpha_j = \sum\nolimits_{1\le i\le n} 2\frac{(\alpha_i,\alpha_j)}{(\alpha_i,\alpha_i)}\lambda_i.$$

PROOF. This follows from the calculation in the above proof. □

Thus, we have

$$P = \bigoplus\nolimits_i \mathbb{Z}\lambda_i \supset Q = \bigoplus\nolimits_i \mathbb{Z}\alpha_i$$

and when we express the $\alpha_i$ in terms of the $\lambda_i$, the coefficients are the entries of the Cartan matrix. Replacing the $\lambda_i$'s and $\alpha_i$'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 $\lambda_i$'s in terms of the $\alpha_i$'s. Cf. Humphreys 1972, p69.

## Brief review of diagonalizable groups

Recall from §9 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

$$D \mapsto X(D) =_{\mathrm{df}} \mathrm{Hom}(D, \mathbb{G}_m).$$

Moreover, these functors are exact. For example, an exact sequence

$$0 \to D' \to D \xrightarrow{\pi} D'' \to 0$$

of diagonalizable groups corresponds to an exact sequence

$$0 \to X(D'') \to X(D) \to X(D') \to 0$$

of abelian groups. Under this correspondence,

$$D' = \mathrm{Ker}(D \to D'' \overset{\chi}{\hookrightarrow} \prod\nolimits_{\chi\in X(D'')} \mathbb{G}_m)$$

i.e.,

$$D' = \bigcap\nolimits_{\chi\in X(D'')} \mathrm{Ker}(D \xrightarrow{\pi\circ\chi} \mathbb{G}_m). \tag{78}$$

## 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 20.4 *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 $\mathrm{SL}_{n+1}$ and for $C_n$ it $\mathrm{Sp}_{2n}$. For $B_n$ and $D_n$ one tries $\mathrm{SO}_{2n+1}$ and $\mathrm{SO}_{2n}$ (as defined in 16.3), but their centres are too small. In fact the centre of $O_m$ is $\pm I$, and so $\mathrm{SO}_{2n+1}$ has trivial centre and $O_{2n}$ has centre of order 2. The group one needs is the corresponding spin group (see §5). 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 discussed earlier (p137), 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

$$N = \bigcap\nolimits_{\chi \in X/Q} \mathrm{Ker}(\chi\colon Z(G) \to \mathbb{G}_m)$$

has centre with character group $X/Q$ (cf. (78)), 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 $X \neq X'$.

## 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).

## Split reductive groups

Let $G'$ be a split semisimple group, $D$ a diagonalizable group, and $Z(G') \to D$ a homomorphism from $Z(G')$ to $D$. Define $G$ to be the quotient

$$Z(G') \to G' \times D \to G \to 1.$$

All split reductive groups arise in this fashion (15.1).

ASIDE 20.5 With only minor changes, the above description works over fields of nonzero characteristic.

## Exercise

20-1 Assuming Theorem 20.4, show that the split reductive groups correspond exactly to the reduced root data.

# 21 Borel fixed point theorem and applications

## Brief review of algebraic geometry

We need the notions of an affine algebraic variety, a projective algebraic variety, and a quasi-projective algebraic variety as, for example, in my notes AG. 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.

21.1 Let $V$ be a vector space of dimension $n$ over $k$.

(a) The set $\mathbb{P}(V)$ of lines in $V$ 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).

(c) For any sequence of integers $n > d_r > d_{r-1} > \cdots > d_1 > 0$ the set of flags

$$V \supset V_r \supset \cdots \supset V_1 \supset \{0\}$$

with $V_i$ a subspace of $V$ of dimenision $d_i$ has a natural structure of a projective algebraic variety (called a ***flag variety***; AG p114).

21.2 If $X$ is an affine algebraic variety, then the ring of regular functions on $X$ is finite over a polynomial ring in $\dim X$ symbols (Noether normalization theorem, AG 8.13). On the other hand, the ring of regular functions on a connected projective variety consists only of the constant functions (AG 7.7, 7.3e). Thus an affine algebraic variety isomorphic to a projective algebraic variety has dimension zero.

21.3 Let $f: X \to Y$ be a regular map. Then $f(X)$ contains an open subset of its closure $\overline{f(X)}$ (AG 10.2). If $X$ is projective, then $f(X)$ is closed (AG 7.7, 7.3c).

21.4 A bijective regular map of algebraic varieties need not be an isomorphism. For example, $x \mapsto x^p: \mathbb{A}^1 \to \mathbb{A}^1$ in characteristic $p$ corresponds to the map of $k$-algebras $T \mapsto T^p: k[T] \to k[T]$, which is not an isomorphism, and

$$t \mapsto (t^2, t^3): \mathbb{A}^1 \to \{y^2 = x^3\} \subset \mathbb{A}^2$$

corresponds to the map $k[t^2, t^3] \hookrightarrow k[t]$, which is not an isomorphism. However, every bijective regular map $X \to Y$ of varieties in characteristic zero with $Y$ nonsingular is an isomorphism (cf. AG 8.19).

21.5 The set of nonsingular points of a variety is dense and open (AG 5.18). Therefore, a variety on which a group acts transitively by regular maps is nonsingular (cf. AG 5.20).

In order to be able to use algebraic geometry in its most naive form, for the remainder of this section **I take $k$ to be algebraically closed of characteristic zero.** This allows us to regard algebraic groups as affine algebraic varieties (in the sense of AG) endowed with a group structure defined by regular maps (2.24).

## The Borel fixed point theorem

THEOREM 21.6 (BOREL FIXED POINT THEOREM) *Any connected solvable affine algebraic group acting*[63] *on a projective variety has a fixed point.*

PROOF. Let $G \times X \to X$ be the action. We use induction on the dimension of $G$.

Suppose $G$ has dimension 1, and let $O = Gx$ be an orbit in $X$. There are three possibilities to consider:

(a) $O$ has dimension 0;
(b) $O$ has dimension 1, and is not closed;
(c) $O$ has dimension 1, and is closed.

In case (a), $O$ consists of a single point (because $G$ is connected), which is a fixed point. In case (b), $\overline{O}$ is stable under $G$, and so $\overline{O} \smallsetminus O$ is a finite set of fixed points. Case (c) doesn't occur: the orbit $O$ is nonsingular (21.5), and if it is closed then it is projective; the subgroup $N$ of $G$ fixing $x$ is normal (because $G$ is commutative), and $G/N \to O$ is bijective, and is therefore an isomorphism (21.4); this contradicts (21.2) because $G/N$ is affine (6.22).

In the general case, $G$ has a normal subgroup $H$ with $G/H$ of dimension 1 — this follows from the Lie-Kolchin theorem, or can be proved directly. The subvariety $X^H$ of points fixed by $H$ is nonempty by induction, and it is closed because $X^H = \bigcap_{h\in H} X^h$, where $X^h$ is the set on which the regular maps $x \mapsto hx$ and $x \mapsto x$ agree. Therefore $X^H$ is a projective variety on which $G$ acts through its quotient $G/H$, which has a fixed point by the first part of the proof. □

REMARK 21.7 It is possible to recover the Lie-Kolchin theorem from the Borel fixed point theorem. Let $G$ be a connected solvable subgroup of $\mathrm{GL}_V$, and let $X$ be the collection of full flags in $V$ (i.e., the flags corresponding to the sequence $\dim V = n > n-1 > \cdots > 1 > 0$). As noted in (21.1), this has a natural structure of a projective variety, and $G$ acts on it by a regular map

$$g, F \mapsto gF\colon G \times X \to X$$

where

$$g(V_n \supset V_{n-1} \supset \cdots) = gV_n \supset gV_{n-1} \supset \cdots .$$

According to the theorem, there is a fixed point, i.e., a full flag such that $gF = F$ for all $g \in G(k)$. Relative to a basis $e_1, \dots, e_n$ adapted to the flag,[64] $G \subset \mathbb{T}_n$.

## Quotients

Earlier we discussed 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 subgroup $H$. Let $\pi\colon G \to G/H$ be the quotient map (of sets). Endow $G/H$ with the quotient topology, and for $U$ an open subset of $G/H$, let $\mathcal{O}_{G/H}(U)$ be the $k$-algebra of functions $f\colon U \to k$ such that $f \circ \pi$ is regular on $\pi^{-1}(U)$. Then one can show that the ringed space so defined is a quasi-projective algebraic variety. Moreover, it has the following universal property: every regular map $G \to Y$ that is constant on each left coset of $H$ in $G$ factors uniquely through $\pi$.

[63] By this we mean that there is a regular map $G \times X \to X$ defining an action of the group $G(k)$ on the set $X(k)$ in the usual sense.

[64] That is, such that $e_1, \dots, e_i$ is a basis of $V_i$.

As in the case of a normal subgroup, a key tool in the proof Chevalley's theorem (3.13): there exists a representation $G \to \mathrm{GL}_V$ and a one-dimensional subspace $L$ in $V$ such that

$$H(k) = \{g \in G(k) \mid gL = L\}.$$

Then, the map $g \mapsto gL$ defines an injection (of sets) $G/H \to \mathbb{P}(V)$, and one shows that the image of the map is a quasi-projective subvariety of $\mathbb{P}(V)$ and that the bijection endows $G/H$ with the structure of a quasi-projective variety having the correct properties. See Humphreys 1975, Chapter IV.

EXAMPLE 21.8 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 $\begin{pmatrix} * \\ 0 \end{pmatrix}$. Since $G$ acts transitively on the set of lines, there is a bijection $G/H \to \mathbb{P}^1$, which endows $G/H$ with the structure of a projective variety.

ASIDE 21.9 When $k$ and $G$ are arbitrary, quotients still exist. Let $H$ be an algebraic subgroup of $G$. Then there exists an algebraic space $G/H$ and a map $\pi: G \to H$ such that

(a) for all $k$-algebras $R$, the fibres of the map $G(R) \to (G/H)(R)$ are the cosets of $H(R)$;
(b) for all $k$-algebras $R$ and $x \in (G/H)(R)$, there exists a finitely generated faithfully flat $R$-algebra $R'$ and an $y \in G(R')$ such that $x$ and $y$ have the same image in $(G/H)(R')$.

See Demazure and Gabriel 1970, III §3 5.4.

## Borel subgroups

DEFINITION 21.10 A ***Borel subgroup*** of an algebraic group $G$ is a maximal connected solvable algebraic subgroup.

For example, $\mathbb{T}_2$ is a Borel subgroup of $\mathrm{GL}_2$ (it is certainly connected and solvable, and the only connected subgroup properly containing it is $\mathrm{GL}_2$, which isn't solvable).

For the remainder of this section, $G$ is a **connected** algebraic group.

THEOREM 21.11 *If $B$ is a Borel subgroup of $G$, then $G/B$ is projective.*

THEOREM 21.12 *Any two Borel subgroups of $G$ are conjugate, i.e., $B' = gBg^{-1}$ for some $g \in G(k)$.*

PROOF. We first prove Theorem 21.11 for $B$ a connected solvable algebraic subgroup of $G$ of largest possible dimension. Apply the theorem of Chevalley quoted above to obtain a representation $G \to \mathrm{GL}_V$ 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 full flag in $V/L$ stabilized by $B$. On pulling this back to $V$, we get a full 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 $V_1$),

$$H(k) = \{g \in G(k) \mid gF = F\}.$$

Thus $G/B \to G \cdot F$ is bijective. This shows that, when we let $G$ act on the variety of full flags, $G \cdot F$ is the orbit of smallest dimension, because for any other full flag $F'$, the stabilizer $H$ of $F'$ is a solvable algebraic subgroup of dimension at most that of $B$, and so

$$\dim G \cdot F' = \dim G - \dim H \geq \dim G - \dim B = \dim G \cdot F.$$

This implies that $G \cdot F$ is closed, because otherwise $\overline{G \cdot F} \smallsetminus G \cdot F$ would be a union of orbits of lower dimension. As a closed subset of the projective variety of full flags in $V$, $G \cdot F$ is projective. By the universal property of quotients, $G/B \to G \cdot F$ is regular, and hence is an isomorphism (21.4, 21.5). Therefore, $G/B$ is also projective.

We now complete the proof of the theorems by showing that for any Borel subgroups $B$ and $B'$ with $B$ of largest possible dimension, $B' \subset gBg^{-1}$ for some $g \in G(k)$.[65] 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. □

THEOREM 21.13 *All maximal tori in $G$ are conjugate.*

PROOF. Let $T$ and $T'$ be maximal tori. Being 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 (11.27). □

THEOREM 21.14 *For any Borel subgroup $B$ of $G$, $G = \bigcup_{g \in G(k)} gBg^{-1}$.*

PROOF. (BRIEF SKETCH) 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 $B$ (21.12). □

THEOREM 21.15 *For any torus $T$ in $G$, $C_G(T)$ is connected.*

PROOF. 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 21.14), 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 (11.28). Therefore $x \in C_G(T)^\circ$. □

[65] The maximality of $B'$ implies that $B' = gBg^{-1}$.

## Parabolic subgroups

DEFINITION 21.16 An algebraic subgroup $P$ of $G$ is ***parabolic*** if $G/P$ is projective.

THEOREM 21.17 *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. $\Longrightarrow$ : 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 $g^{-1}Bg \subset P$.

$\Longleftarrow$ : Suppose $P$ contains the Borel subroup $B$. Then there is quotient map $G/B \to G/P$. 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 $G/B \to G/P \to \mathbb{P}^N$ has closed image (see 21.3), but this image is $G/P$, which is therefore projective. □

COROLLARY 21.18 *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. □

## Examples of Borel and parabolic subgroups

**Example:** $\mathrm{GL}_V$

Let $G = \mathrm{GL}_V$ with $V$ of dimension $n$. Let $F$ be a full flag

$$F\colon V = V_n \supset V_{n-1} \supset \cdots \supset V_1 \supset 0$$

and let $G(F)$ be the stabilizer of $F$,

$$G(F)(k) = \{g \in \mathrm{GL}(V) \mid gV_i \subset V_i \text{ for all } i\}.$$

Then $G(F)$ is connected and solvable (because the choice of a basis adapted to $F$ defines an isomorphism $G(F) \to \mathbb{T}_n$), and $\mathrm{GL}_V/G(F)$ is projective (because $\mathrm{GL}(V)$ acts transitively on the space of all full flags in $V$). Therefore, $G(F)$ is a Borel subgroup (21.18). For $g \in \mathrm{GL}(V)$,

$$G(gF) = g \cdot G(F) \cdot g^{-1}.$$

Since all Borel subgroups are conjugate, we see that the Borel subgroups of $\mathrm{GL}_V$ are precisely the groups of the form $G(F)$ with $F$ a full flag.

Now consider $G(F)$ with $F$ a (not necessarily full) flag. Clearly $F$ can be refined to a full flag $F'$, and $G(F)$ contains the Borel subgroup $G(F')$. Therefore it is parabolic. Later we'll see that all parabolic subgroups of $\mathrm{GL}_V$ are of this form.

**Example:** $\mathrm{SO}_{2n}$

Let $V$ be a vector space of dimension $2n$, and let $\phi$ 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 ***full*** if it has the maximum length $n$.

Let

$$F: V_n \supset V_{n-1} \supset \cdots \supset V_1 \supset 0$$

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 dimension[66] $n+1$, 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 $\phi$ is $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

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 full totally isotropic subspaces of $V$. One shows that $X$ is closed (for the Zariski topology) in the flag variety consisting of all flags $V_n \supset \cdots \supset V_1 \supset 0$ with $\dim V_n = n$, and is therefore a projective variety. It may fall into two connected components which are the orbits of $\mathrm{SO}(\phi)$.[67]

Let $G = \mathrm{SO}(\phi)$. 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 full totally isotropic flags.

**Example:** $\mathrm{Sp}_{2n}$

Again the stabilizers of totally isotropic flags are parabolic subgroups, and the Borel subgroups are exactly the stabilizers of full totally isotropic flags.

**Example:** $\mathrm{SO}_{2n+1}$

Same as the last two cases.

**Exercise**

21-1 Write out a proof that the Borel subgroups of $\mathrm{SO}_{2n}$, $\mathrm{Sp}_{2n}$, and $\mathrm{SO}_{2n+1}$ are those indicated above.

[66] Recall that in a nondegenerate quadratic space $(V, \phi)$,

$$\dim W + \dim W^\perp = \dim V.$$

[67] Let $(V, \phi)$ be a hyperbolic plane with its standard basis $e_1, e_2$. Then the flags

$$F_1: \langle e_1, e_2 \rangle \supset \langle e_1 \rangle \supset 0$$
$$F_2: \langle e_1, e_2 \rangle \supset \langle e_2 \rangle \supset 0$$

fall into different $\mathrm{SO}(\phi)$ orbits.

# 22 Parabolic subgroups and roots

Throughout this section, $k$ is algebraically closed of characteristic zero.

Recall (9.15) that for a representation $T \to \mathrm{GL}_V$ of a (split) torus $T$,

$$V = \bigoplus\nolimits_{\chi \in X^*(T)} V_\chi$$

where $V_\chi$ is the subspace on which $T$ acts through the character $\chi$. The $\chi$ for which $V_\chi \neq 0$ are called the ***weights*** of $T$ in $V$, and the corresponding $V_\chi$ are called the ***weight spaces***. Clearly

$$\mathrm{Ker}(T \to \mathrm{GL}_V) = \bigcap\nolimits_{\chi \text{ a weight}} \mathrm{Ker}(\chi).$$

Therefore $T$ acts faithfully on $V$ if and only if the weights generate $X^*(T)$ (by 9.12).

We wish to understand the Borel and parabolic subgroups in terms of root systems. We first state a weak result.

THEOREM 22.1 *Let $G$ be a connected reductive group, $T$ a maximal torus in $G$, and $(V, \Phi)$ the corresponding root system (so $V = \mathbb{R} \otimes_{\mathbb{Q}} Q$ where $Q$ is the $\mathbb{Z}$-module generated by $\Phi$).*

*(a) The Borel subgroups of $G$ containing $T$ are in one-to-one correspondence with the bases of $\Phi$.*

*(b) Let $B$ be the Borel subgroup of $G$ corresponding to a base $S$ for $\Phi$. The number of parabolic subgroups of $G$ containing $B$ is $2^{|S|}$.*

We examine this statement for $G = \mathrm{GL}_V$. Let $n = \dim V$.

22.2 *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 $\mathrm{GL}_V$. 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 $V$.

22.3 *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 full flags

$$F\colon V = W_n \supset W_{n-1} \supset \cdots$$

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 $j_n > \cdots > j_1$ 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 full flag.

22.4 *The bases for $\Phi$ are in natural one-to-one correspondence with the orderings of $J$.*

The vector space $V$ has basis $(\chi_j)_{j\in J}$, and $\Phi = \{\chi_i - \chi_j \mid i \neq j\}$. 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 $\Phi^+ = \{\chi_i - \chi_j \mid \langle \chi_i - \chi_j, t\rangle > 0\}$. Clearly, specifying $\Phi^+$ in this way amounts to choosing an ordering on $J$.[68]

22.5 *Fix a Borel subgroup $B$ of $G$ containing $T$, and hence a base $S$ for $\Phi$. 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

$$V \supset V_r \supset \cdots \supset V_1 \supset 0$$

with $V_j = \bigoplus_{i\le a_1+\cdots+a_j} V_i$. Since the number of such sequences[69] is $2^{n-1}$, the theorem implies that this is a complete list of parabolic subgroups.

## Lie algebras

Recall that $\mathfrak{sl}_2$ consists of the $2\times 2$ 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 $\mathrm{ad}x$ is semisimple. Then

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus\nolimits_{\alpha\in\Phi} \mathfrak{g}_\alpha$$

where $\mathfrak{g}_0$ is the subspace of $\mathfrak{g}$ on which $\mathfrak{h}$ acts trivially, and $\mathfrak{g}_\alpha$ is the subspace on which $\mathfrak{h}$ acts through the nonzero linear form $\alpha$. The $\alpha$ occurring in the decomposition are called the ***roots*** of $\mathfrak{g}$ (relative to $\mathfrak{h}$).

THEOREM 22.6 *For each $\alpha \in \Phi$, the spaces $\mathfrak{g}_\alpha$ and $\mathfrak{h}_\alpha = _{\mathrm{df}} [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}]$ 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 $y_\alpha$ such that*

$$[x_\alpha, y_\alpha] = h_\alpha, \quad [h_\alpha, x_\alpha] = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -2y_\alpha.$$

*Hence $\mathfrak{g}_\alpha = \mathfrak{g}_{-\alpha} \oplus \mathfrak{h}_\alpha \oplus \mathfrak{g}_\alpha$ is isomorphic to $\mathfrak{sl}_2$.*

PROOF. Serre 1987, Chapter VI. □

[68] Let $(f_i)_{i\in I}$ 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 $\Phi^+$ depends only on ordering of the $a_i$ (relative to the natural order on $\mathbb{R}$), and it determines this ordering.

[69] Such sequences correspond to functions $\mu\colon \{1, \dots, n\} \to \{0, 1\}$ with $\mu(0) = 1$ — the $a_i$ are the lengths of the strings of zeros or ones.

## Algebraic groups

Let $G$ be a reductive group containing a split maximal torus $T$. Let $\mathrm{Lie}(G,T) = (\mathfrak{g},\mathfrak{h})$. Then

$$\mathrm{Hom}_{k\text{-lin}}(\mathfrak{h},k) \simeq k \otimes_{\mathbb{Z}} X^*(T)$$

(see 12.16), and so each $\alpha \in \Phi$ defines a linear form $\alpha'$ 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 22.7 *For each $\alpha \in \Phi$ there is a unique homomorphism $\exp_\alpha\colon \mathfrak{g}_\alpha \to G$ of algebraic groups such that*

$$t\exp_\alpha(x)t^{-1} = \exp(\alpha(t)x)$$
$$\mathrm{Lie}(\exp_\alpha) = (\mathfrak{g}_\alpha \hookrightarrow \mathfrak{g}).$$

PROOF. Omitted. □

EXAMPLE 22.8 Let $G = \mathrm{GL}_n$, 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 $U_\alpha$ denote the image of $\exp_\alpha$.

THEOREM 22.9 *For any base $S$ for $\Phi$, the subgroup of $G$ generated by $T$ and the $U_\alpha$ for $\alpha \in \Phi^+$ 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*

$$\Phi^+ = \{\alpha \in \Phi \mid U_\alpha \in B\}$$

*is the set of positive roots (so $S$ is the set of indecomposable elements in $\Phi^+$).*

PROOF. Omitted. □

THEOREM 22.10 *Let $S$ be a base for $\Phi$ and let $B$ be the corresponding Borel subgroup. For each subset $I$ of $\Phi$, 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 $\mathrm{GL}_5$ is

$$\left\{\begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \end{pmatrix}\right\}.$$

# 23 Representations of split reductive groups

Throughout this section, $k$ is algebraically closed of characteristic zero.

### The dominant weights of a root datum

Let $(X, \Phi, X^\vee, \Phi^\vee)$ be a root datum. We make the following definitions:

- $Q = \mathbb{Z}\Phi$ (***root lattice***) is the $\mathbb{Z}$-submodule of $X$ generated by the roots;
- $X_0 = \{x \in X \mid \langle x, \alpha^\vee\rangle = 0 \text{ for all } \alpha \in \Phi\}$;
- $V = \mathbb{R} \otimes_{\mathbb{Z}} Q \subset \mathbb{R} \otimes_{\mathbb{Z}} X$;
- $P = \{\lambda \in V \mid \langle \lambda, \alpha^\vee\rangle \in \mathbb{Z} \text{ for all } \alpha \in \Phi\}$ (***weight lattice***).

Now choose a base $S = \{\alpha_1, \dots, \alpha_n\}$ for $\Phi$, so that:

- $\Phi = \Phi^+ \sqcup \Phi^-$ where $\Phi^+ = \{\sum m_i\alpha_i \mid m_i \geq 0\}$ and $\Phi^- = \{\sum m_i\alpha_i \mid m_i \leq 0\}$;
- $Q = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset V = \mathbb{R}\alpha_1 \oplus \cdots \oplus \mathbb{R}\alpha_n$,
- $P = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n$ where $\lambda_i$ is defined by $\langle \lambda_i, \alpha_j^\vee\rangle = \delta_{ij}$.

The $\lambda_i$ are called the ***fundamental (dominant) weights***. Define

- $P^+ = \{\lambda \in P \mid \langle \lambda, \alpha^\vee\rangle \geq 0 \text{ all } \alpha \in \Phi^\vee\}$.

An element $\lambda$ of $X$ is ***dominant*** if $\langle \lambda, \alpha^\vee\rangle \geq 0$ for all $\alpha \in \Phi^+$. Such a $\lambda$ can be written uniquely

$$\lambda = \sum\nolimits_{1 \leq i \leq n} m_i\lambda_i + \lambda_0 \tag{79}$$

with $m_i \in \mathbb{N}$, $\sum m_i\lambda_i \in X$, and $\lambda_0 \in X_0$.

### The dominant weights of a semisimple root datum

Recall (19.9) that to give a semisimple root datum amounts to giving a root system $(V, \Phi)$ and a lattice $X$,

$$P \supset X \supset Q.$$

Choose an inner product $(\ ,\ )$ on $V$ for which the $s_\alpha$ act as orthogonal transformations (19.16). Then, for $\lambda \in V$

$$\langle \lambda, \alpha^\vee\rangle = 2\frac{(\lambda, \alpha)}{(\alpha, \alpha)}$$

(see p150). Since in this case $X_0 = 0$, the above definitions become:

- $Q = \mathbb{Z}\Phi = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$,
- $P = \{\lambda \in V \mid 2\frac{(\lambda,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z} \text{ all } \alpha \in \Phi\} = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n$ where $\lambda_i$ is defined by

$$2\frac{(\lambda_i, \alpha)}{(\alpha, \alpha)} = \delta_{ij}.$$

- $P^+ = \{\lambda = \sum_i m_i\lambda_i \mid m_i \geq 0\} = \{\text{dominant weights}\}$.

### 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 $(X, \Phi, X^\vee, \Phi^\vee)$ and a base $S$ for $\Phi$). As every representation of $G$ is (uniquely) a sum of simple representations (15.6), we only need to classify them.

THEOREM 23.1 *Let $r\colon G \to \mathrm{GL}_W$ 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 $\lambda_r$ in (b) is dominant.*
(d) *If $\lambda$ 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 (11.22) 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), $\lambda_r$ is called the ***heighest weight*** of the simple representation $r$.

THEOREM 23.2 *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. □

## 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 $\mathrm{SL}_2$ on the homogeneous polynomials of degree $m$ is simple, and every simple representation is isomorphic to exactly one of these.

## Example: $\mathrm{GL}_n$

As usual, let $T$ be $\mathbb{D}_n$, and let $B$ the standard Borel subgroup. The characters of $T$ are $\chi_1, \ldots, \chi_n$. Note that $\mathrm{GL}_n$ 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 $\mathrm{GL}_n$ we can shift its weights by any integer multiple of $\chi_1 + \cdots + \chi_n$.

In this case, the simple roots are $\chi_1 - \chi_2, \ldots, \chi_{n-1} - \chi_n$, 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 $e_1 - e_2, \ldots, e_{n-1} - e_n$, and the fundamental dominant weights are $\lambda_1, \ldots, \lambda_{n-1}$ with

$$\lambda_i = e_1 + \cdots + e_i - n^{-1}i\,(e_1 + \cdots + e_n).$$

According to (79), the dominant weights are the expressions

$$a_1\lambda_1 + \cdots + a_{n-1}\lambda_{n-1} + m(e_1 + \cdots + e_n), \quad a_i \in \mathbb{N}, \quad m \in \mathbb{Z}.$$

These are the expressions

$$m_1e_1 + \cdots + m_ne_n$$

where the $m_i$ are integers with $m_1 \geq \cdots \geq m_n$. The simple representation with highest weight $e_1$ is the representation of $\mathrm{GL}_n$ on $k^n$ (obviously), and the simple representation with highest weight $e_1 + \cdots + e_i$ is the representation on $\bigwedge^i(k^n)$ (Springer, Linear algebraic groups, Survey article, 1993, 4.6.2).

### Example: $\mathrm{SL}_n$

Let $T_1$ be the diagonal in $\mathrm{SL}_n$. Then $X^*(T_1) = X^*(T)/\mathbb{Z}(\chi_1 + \cdots + \chi_n)$ with $T = \mathbb{D}_n$. The root datum for $\mathrm{SL}_n$ is isomorphic to $(\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n), \{\varepsilon_i - \varepsilon_j \mid i \neq j\}, \ldots)$ where $\varepsilon_i$ is the image of $e_i$ in $\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n)$. It follows from the $\mathrm{GL}_n$ case that the fundamental dominant weights are $\lambda_1, \ldots, \lambda_{n-1}$ with

$$\lambda_i = \varepsilon_1 + \cdots + \varepsilon_i.$$

Again, the simple representation with highest weight $\varepsilon_1$ is the representation of $\mathrm{SL}_n$ on $k^n$, and the simple representation with highest weight $\varepsilon_1 + \cdots + \varepsilon_i$ is the representation $\mathrm{SL}_n$ on $\bigwedge^i(k^n)$ (ibid.).

# 24 Tannaka duality

By a character of a topological group, I mean a continuous homomorphism to the circle group $\{z \in \mathbb{C} \mid z\overline{z} = 1\}$. A finite abelian group $G$ can be recovered from its group $G^\vee$ of characters because the canonical homomorphism $G \to G^{\vee\vee}$ is an isomorphism.

More generally, a locally compact abelian topological group $G$ can be recovered from its character group because, again, the canonical homomorphism $G \to G^{\vee\vee}$ is an isomorphism (Pontryagin duality). Moreover, the dual of a compact abelian group is a discrete abelian group, and so, the study of compact abelian topological groups is equivalent to that of discrete abelian groups.

Clearly, "abelian" 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 nonabelian group from its category of unitary reprsesentations.

In this section, I discuss an analogue of this for algebraic groups, which is usually called Tannaka duality. For more details, see Deligne and Milne, Tannakian categories, in Hodge Cycles, Motives, and Shimura Varieties, 1982 (available on my website).

Throughout this section, all vector spaces are finite-dimensional, and all representations are on finite-dimensional vector spaces. The ground field $k$ is of arbitrary characteristic.

## Recovering a group from its representations

PROPOSITION 24.1 *Let $G$ be an algebraic group, and let $R$ be a $k$-algebra. Suppose that we are given, for each representation $r_V\colon G \to \mathrm{GL}_V$ of $G$, an element $\lambda_V$ of $\mathrm{Aut}_{R\text{-}lin}(R \otimes_k V)$. If the family $(\lambda_V)$ satisfies the conditions,*

(a) *for all representations $V, W$,*

$$\lambda_{V\otimes W} = \lambda_V \otimes \lambda_W,$$

(b) $\lambda_{\mathbb{1}} = \mathrm{id}_{\mathbb{1}}$ *(here $\mathbb{1} = k$ with the trivial action),*

(c) *for all $G$-equivariant maps $\alpha\colon V \to W$,*

$$\lambda_W \circ (\mathrm{id}_R \otimes \alpha) = (\mathrm{id}_R \otimes \alpha) \circ \lambda_V,$$

*then there exists a $g \in G(R)$ such that $\lambda_X = r_X(g)$ for all $X$.*

PROOF. To be added (one page; cf. Deligne and Milne 1982, 2.8). □

Because there exists a faithful representation (3.8), $g$ is uniquely determined by the family $(\lambda_V)$. Moreover, each $g \in G(R)$ of course defines such a family. Thus, from the category $\mathsf{Rep}_k(G)$ 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.

## Properties of $G$ versus those of $\mathsf{Rep}_k(G)$

Since each of $G$ and $\mathsf{Rep}_k(G)$ determines the other, we should be able to see properties of one reflected in the other.

PROPOSITION 24.2 *An algebraic group $G$ is finite if and only if there exists a representation $(r, V)$ such that every representation of $G$ is a subquotient[70] of $V^n$ for some $n \geq 0$.*

[70]Here $V^n$ 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).

PROOF. See Deligne and Milne 1982, 2.20. □

PROPOSITION 24.3 *Let $k$ be an algebraically closed field. A smooth algebraic group over $k$ is unipotent (resp. solvable) if and only if every nonzero representation of the group has a nonzero fixed vector (resp. stable one-dimensional subspace).*

PROOF. See (11.24) and (11.22). □

PROPOSITION 24.4 *The identity component $G^\circ$ of an algebraic group $G$ over a field of characteristic zero is reductive if and only if $\mathsf{Rep}_k(G)$ is semisimple.*

PROOF. See (15.6, 15.11). □

PROPOSITION 24.5 *Let $G$ and $G'$ be algebraic groups over a field $k$ of characteristic zero, and assume $G^\circ$ is reductive. Let $f: G \to G'$ be a homomorphism, and let $\omega^f: \mathsf{Rep}(G') \to \mathsf{Rep}(G)$ be the functor $(r, V) \mapsto (r \circ \lambda, V)$. Then:*

(a) *$f$ is a quotient map if and only if $\omega^f$ is fully faithful;*
(b) *$f$ is an embedding if and if every object of $\mathsf{Rep}_k(G)$ is isomorphic to a direct factor of an object of the form $\omega^f(V)$.*

PROOF. See Deligne and Milne 1982, 2.21, 2.29. □

## (Neutralized) Tannakian categories

For $k$-vector spaces $U, V, W$, there are canonical isomorphisms

$$\begin{aligned} &\phi_{U,V,W}: U \otimes_k (V \otimes_k W) \to (U \otimes_k V) \otimes_k W, && u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w \\ &\phi_{U,V}: U \otimes_k V \to V \otimes U, && u \otimes v \mapsto v \otimes u. \end{aligned}$$

Let $V^\vee = \mathrm{Hom}_{k\text{-lin}}(V, k)$ be the dual of $V$. Then there are canonical linear maps

$$\begin{aligned} &\mathrm{ev}_X: V^\vee \otimes_k V \to k, && f \otimes v \mapsto f(v) \\ &\delta_X: k \to V \otimes V^\vee, && 1 \mapsto \textstyle\sum e_i \otimes f_i \end{aligned}$$

where $(e_i)$ is any basis for $V$ and $(f_i)$ is the dual basis. Let $\mathsf{Vec}_k$ denote the category of finite-dimensional $k$-vector spaces.

DEFINITION 24.6 A neutralized ***Tannakian category*** over $k$ is a triple $(\mathsf{C}, \otimes, \omega)$ consisting of

- $k$-linear category $\mathsf{C}$ in which all morphisms have kernels and cokernels,
- $\otimes$ is a $k$-bilinear functor $\mathsf{C} \times \mathsf{C} \to \mathsf{C}$, and
- $\omega$ is an exact faithful $k$-linear functor $\mathsf{C} \to \mathsf{Vec}_k$ such that $\alpha$ is an isomorphism if $\omega(\alpha)$ is,

satisfying the following conditions

(a) for all $X, Y$, $\omega(X \otimes Y) = \omega(X) \otimes_k \omega(Y)$;
(b) for all $X, Y, Z$, the isomorphisms $\phi_{\omega X, \omega Y, \omega Z}$ and $\phi_{\omega X, \omega Y}$ live in $\mathsf{C}$;
(c) there exists an object $\mathbb{1}$ in $\mathsf{C}$ such that $\omega(\mathbb{1}) = k$ and the canonical isomorphisms

$$\omega(\mathbb{1}) \otimes \omega(X) \simeq \omega(X) \simeq \omega(X) \otimes \omega(\mathbb{1})$$

live in $\mathsf{C}$;

(d) for each $X$, there exists an $X^\vee$ in $\mathsf{C}$ such that $\omega(X^\vee) = \omega(X)^\vee$ and $\delta_{\omega X}$ and $\mathrm{ev}_{\omega X}$ live in $\mathsf{C}$.

We say that $\mathsf{C}$ is ***algebraic*** if there exists an object $X$ such that every other object can be constructed by forming tensor products, direct sums, duals, and subquotients.

REMARK 24.7 (a) A category is $k$-***linear*** if
i) every pair of objects has a direct sum and a direct product,
ii) the Hom sets are vector spaces over $k$ and composition is $k$-bilinear, and
iii) there exists a zero object (object with $\mathrm{id} = 0$).

(b) A $k$-linear category is ***abelian*** if each morphism $\alpha\colon X \to Y$ has a kernel and cokernel and the morphism $X/\operatorname{Ker}(\alpha) \to \operatorname{Ker}(Y \to \operatorname{Coker}(\alpha))$ is an isomorphism.

(c) By $\omega$ being exact, I mean that it preserves kernels and cokernels. Notice that the conditions imply that $\mathsf{C}$ is an abelian category.

(d) By a map $\alpha\colon \omega(X) \to \omega(Y)$ in $\mathsf{Vec}_k$ "***living in*** $\mathsf{C}$", I mean that it lie in $\operatorname{Hom}(X, Y) \subset \operatorname{Hom}(\omega X, \omega Y)$. For example, by $\phi_{\omega X,\omega Y}$ living in $\mathsf{C}$, I mean that $\phi_{\omega X,\omega Y} = \omega(\phi_{X,Y})$ for some isomorphism $\phi_{X,Y}\colon X \otimes Y \to Y \otimes X$.

From now on "Tannakian category" means "neutralized Tannakian category".

EXAMPLE 24.8 For every algebraic group $G$, $\mathsf{Rep}_k(G)$ is obviously a Tannakian category over $k$, and (3.9) shows that it is algebraic.

EXAMPLE 24.9 For every Lie algebra $\mathfrak{g}$, the category of representations of $\mathfrak{g}$ on finite-dimensional vector spaces is Tannakian.

THEOREM 24.10 *Every algebraic Tannakian category is the category of representations of an algebraic group $G$.*

PROOF. For a proof (and more precise statement), see Deligne and Milne 1982, 2.11. □

ASIDE 24.11 We have seen that algebraic Tannakian categories correspond to algebraic groups. Without "algebraic" the categories correspond to functors from $k$-algebras to groups that are represented by $k$-algebras, but not necessarily by finitely generated $k$-algebras. Such a functor will be called a ***pro-algebraic group*** (they are, in fact, the projective limits of algebraic groups).

## Applications

We now take $k$ to be of characteristic zero. Then Ado's theorem says that every Lie algebra (meaning, of course, finite-dimensional) has a faithful representation (N. Jacobson, Lie Algebras, Wiley, 1962, Chapter VI). A representation $\rho\colon G \to \mathrm{GL}_V$ of an algebraic group defines a representation $d\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ of its Lie algebra (cf. 12.14).

PROPOSITION 24.12 *Let $\mathfrak{g} = \mathrm{Lie}(G)$. Then the functor $\mathsf{Rep}_k(G) \to \mathsf{Rep}_k(\mathfrak{g})$ is fully faithful.*

PROOF. Let $(r_1, V_1)$ and $(r_2, V_2)$ be representations of $G$. Let $\alpha\colon V_1 \to V_2$ be a $k$-linear map, and let $t$ be the corresponding element of $V_1^\vee \otimes_k V_2$. Then

the map $\alpha$ is a homomorphism of representations of $G$ $\iff$
$t$ is fixed by $G$ $\iff$
$t$ is fixed by $\mathfrak{g}$ (see 13.16) $\iff$
$\alpha$ is a homomorphism of representations of $\mathfrak{g}$. □

For any Lie algebra $\mathfrak{g}$, $\mathsf{Rep}_k(\mathfrak{g})$ is obviously Tannakian. When it is algebraic, we let $T(\mathfrak{g})$ denote the algebraic group attached to it by Theorem 24.10 (so $\mathsf{Rep}_k(T(\mathfrak{g})) \simeq \mathsf{Rep}_k(\mathfrak{g})$).

In any Lie algebra $\mathfrak{g}$, there is a largest solvable ideal, called the ***radical*** of $\mathfrak{g}$. When the radical of $\mathfrak{g}$ is commutative, $\mathfrak{g}$ is said to be ***reductive***.

PROPOSITION 24.13 *If $\mathfrak{g}$ is reductive, then $\mathsf{Rep}_k(\mathfrak{g})$ is algebrac, and $T(\mathfrak{g})$ is a reductive algebraic group with the property that every algebraic group with Lie algebra $\mathfrak{g}$ is canonically a quotient of $T(\mathfrak{g})$.*

PROOF. It follows from the representation theory of reductive Lie algebras that $\mathsf{Rep}_k(\mathfrak{g})$ has the following properties:

(a) it is a semisimple,
(b) it is algebraic,
(c) if $V$ is an object on which $\mathfrak{g}$ acts nontrivially, then the full subcategory of $\mathsf{Rep}_k(\mathfrak{g})$ whose objects are the direct factors of $V^n$ for some $n$ is not stable under $\otimes$.

According to (24.10), (b) implies that there exists an algebraic group $T(\mathfrak{g})$ with $\mathsf{Rep}_k(T(\mathfrak{g})) \simeq \mathsf{Rep}_k(\mathfrak{g})$, and (a) implies that $T(\mathfrak{g})^\circ$ is reductive (15.6). Also (c) implies that $T(\mathfrak{g})$ has no finite quotient (24.2), and so it is connected. That every algebraic group with Lie algebra $\mathfrak{g}$ is a quotient of $T(\mathfrak{g})$ follows from (24.12) and (24.5). □

PROPOSITION 24.14 *If $\mathfrak{g}$ is semisimple, then $T(\mathfrak{g})$ is the simply connected semisimple algebraic group with Lie algebra $\mathfrak{g}$.*

PROOF. The category $\mathsf{Rep}_k(\mathfrak{g})$ is a semisimple category whose simple objects are indexed by the dominant weights (Serre 1987, VII). Let $G$ be the simply connected semisimple algebraic group with Lie algebra $\mathfrak{g}$. Then $\mathsf{Rep}_k(G) \to \mathsf{Rep}_k(\mathfrak{g})$ is fully faithful (24.12), and (23.2) shows that it is essentially surjective. Hence $G = T(\mathfrak{g})$. □

REMARK 24.15 Let $\mathfrak{g}$ be a semisimple Lie algebra. We have $P \supset Q$ and $P^+$. The simple objects in $\mathsf{Rep}_k(\mathfrak{g})$ are indexed by the elements of $P^+$. Let $X$ be a lattice $P \supset X \supset Q$, and let $\mathsf{Rep}_k(\mathfrak{g})_X$ be the tensor subcategory of $\mathsf{Rep}_k(\mathfrak{g})$ whose simple objects are those indexed by the elements of $P^+ \cap X$. Then $\mathsf{Rep}_k(\mathfrak{g})_X = \mathsf{Rep}(G_X)$ where $G_X$ is the group corresponding to $X$. In other words, every representation of $\mathfrak{g}$ arises from a representation of $G_P$, and the simple representations with heighest weight in $X$ are exactly those for which the representation factors through the quotient $G_X$ of $G_P$.

ASIDE 24.16 Suppose that, for every split semisimple Lie algebra over a field $k$ in characteristic zero, we know that there is $P/Q$-grading on the Tannakian category $\mathsf{Rep}(\mathfrak{g})$, but no grading by any abelian group properly containing $P/Q$ (cf. Deligne and Milne 1982, §5).

Then we can deduce that $G = T(\mathfrak{g})$ is a semisimple algebraic group such that:

- $\mathrm{Lie}(G) = \mathfrak{g}$, and every other algebraic group with this property is a quotient of $G$;
- the centre of $G$ is the group of multiplicative type with character group $P/Q$ (ibid.);
- $\mathsf{Rep}_k(G) \simeq \mathsf{Rep}_k(\mathfrak{g})$.

From this we can read off the existence and uniqueness theorems for split reductive groups and their representations from the similar results for semisimple Lie algebras.

# 25 Algebraic groups over $\mathbb{R}$ and $\mathbb{C}$; relation to 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 section, $k = \mathbb{R}$ or $\mathbb{C}$.

## The Lie group attached to an algebraic group

DEFINITION 25.1 (a) A ***real Lie group*** is a smooth manifold $G$ with a group structure such that both the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are smooth.

(b) A ***complex Lie group*** is a complex manifold $G$ with a group structure such that both the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are holomorphic.

Here "smooth" means infinitely differentiable.

THEOREM 25.2 *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 $\mathrm{GL}_n$ to $\mathrm{GL}_n(\mathbb{R})$ (resp. $\mathrm{GL}_n(\mathbb{C})$) 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 $G \hookrightarrow \mathrm{GL}_n$. Then $G(k)$ is a closed subgroup of $\mathrm{GL}_n(\mathbb{C})$, 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 is a real or complex Lie group). 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 (I. Shafarevich, Basic Algebraic Geometry, 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 (13.12). In the complex case, use §4.

## Negative results

25.3 *In the real case, the functor is not faithful on nonconnected algebraic groups.*

Let $G = H = \mu_3$. The real Lie group attached to $\mu_3$ is $\mu_3(\mathbb{R}) = \{1\}$, and so $\mathrm{Hom}(L(G), L(H)) = 1$, but $\mathrm{Hom}(\mu_3, \mu_3)$ is cyclic of order 3.

25.4 *The functor is not full.*

For example, the $z \mapsto e^z : \mathbb{C} \to \mathbb{C}^\times$ is a homomorphism of Lie groups not arising from a homomorphism of algebraic groups $\mathbb{G}_a \to \mathbb{G}_m$.

For another example, consider the quotient map of algebraic groups $\mathrm{SL}_3 \to \mathrm{PSL}_3$. It is not an isomorphism of algebraic groups because its kernel is $\mu_3$, but it does give an isomorphism $\mathrm{SL}_3(\mathbb{R}) \to \mathrm{PSL}_3(\mathbb{R})$ of Lie groups. The inverse of this isomorphism is not algebraic.

25.5 *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 $\mathbb{R}^m \to \mathbb{R}^n$), these problems don't arise, and the theory of Lie groups quite closely parallels that of algebraic groups.

25.6 *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 has a natural structure of a Lie group. Every representation of this covering group on a finite-dimensional vector space factors through $\mathrm{SL}_2(\mathbb{R})$. Another (standard) example is the Lie group $\mathbb{R}^1 \times \mathbb{R}^1 \times S^1$ with the group structure

$$(x_1, y_1, u_1) \cdot (x_2, y_2, u_2) = (x_1 + x_2, y_1 + y_2, e^{ix_1y_2}u_1u_2).$$

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).

25.7 *Even when a Lie group has a faithful representation, it need not be algebraic.*

For example, the identity component of $\mathrm{GL}_2(\mathbb{R})$ is not algebraic.

25.8 *Let $G$ be an algebraic group over $\mathbb{C}$. Then the Lie group $G(\mathbb{C})$ may have many more representations than $G$.*

Consider $\mathbb{G}_a$. Then the homomorphisms $z \mapsto e^{cz}: \mathbb{C} \to \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$ and $z \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}: \mathbb{C} \to \mathrm{GL}_2(\mathbb{C})$ are representations of the Lie group $\mathbb{C}$, but only the second is algebraic.

## Complex groups

A Lie group (real or complex) is said to be ***linear*** if it admits a faithful representation (on a finite-dimensional vector space, of course). For any complex Lie group $G$, the category $\mathsf{Rep}_{\mathbb{C}}(G)$ is obviously Tannakian.

THEOREM 25.9 *For a complex linear Lie group $G$, the following conditions are equivalent:*

(a) *the Tannakian category $\mathsf{Rep}_{\mathbb{C}}(G)$ is algebraic;*
(b) *there exists an algebraic group $T(G)$ over $\mathbb{C}$ and a homomorphism $G \to T(G)(\mathbb{C})$ inducing an equivalence of categories $\mathsf{Rep}_{\mathbb{C}}(T(G)) \to \mathsf{Rep}_{\mathbb{C}}(G)$.*
(c) *$G$ is the semidirect product of a reductive subgroup and the radical of its derived group.*

*Moreover, when these conditions hold, the homomorphism $G \to T(G)(\mathbb{C})$ is an isomorphism.*

PROOF. The equivalence of (a) and (b) follows from (24.8) and (24.10). For the remaining statements, see Dong Hong Lee, The structure of complex Lie groups, Chapman and Hall, 2002, Theorem 5.20. □

COROLLARY 25.10 *Let $G$ be a complex analytic subgroup of $\mathrm{GL}(V)$ for some complex vector space $V$. If $\mathsf{Rep}_{\mathbb{C}}(G)$ is algebraic, then $G$ is an algebraic subgroup of $\mathrm{GL}_V$, and every complex analytic representation of $G$ is algebraic.*

PROOF. Ibid. 5.22. □

COROLLARY 25.11 *The functors $T$ and $L$ are inverse equivalences between the categories of complex reductive Lie groups and complex reductive algebraic groups (in particular, every complex reductive Lie group has a faithful representation).*

PROOF. Only the parenthetical statement requires proof (omitted for the moment). □

EXAMPLE 25.12 The Lie group $\mathbb{C}$ is algebraic, but nevertheless the conditions in (25.9) fail for it — see (25.8).

## Real groups

We say that a real Lie group $G$ is ***algebraic*** if $G^+ = H(\mathbb{R})^+$ for some algebraic group $H$ (as usual, $^+$ denotes the identity component for the real topology).

THEOREM 25.13 *For every reductive real Lie group $G$, there exists an algebraic group $T(G)$ and a homomorphism $G \to T(G)(\mathbb{R})$ inducing an equivalence of categories $\mathsf{Rep}_{\mathbb{R}}(G) \to \mathsf{Rep}_{\mathbb{R}}(T(G))$. 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. For the first statement, one only has to prove that the Tannakian category $\mathsf{Rep}_{\mathbb{R}}(G)$ is algebraic. For the last statement, see Dong Hoon Lee, J. Lie Theory, 9 (1999), 271-284.□

THEOREM 25.14 *For every compact connected real Lie group $K$, there exists a semisimple algebraic group $T(K)$ and an isomorphism $K \to T(K)(\mathbb{R})$ which induces an equivalence of categories $\mathsf{Rep}_{\mathbb{R}}(K) \to \mathsf{Rep}_{\mathbb{R}}(T(K))$. Moreover, for any reductive algebraic group $G'$ over $\mathbb{C}$,*

$$\mathrm{Hom}_{\mathbb{C}\ \textit{algebraic groups}}(T(K)_{\mathbb{C}}, G') \simeq \mathrm{Hom}_{\mathbb{R}\ \textit{Lie groups}}(K, G'(\mathbb{C}))$$

PROOF. See C. Chevalley, Theory of Lie groups, Princeton, 1946, Chapter 6, §§8–12, and J-P. Serre, Gèbres, L'Enseignement Math., 39 (1993), pp33-85. □

# 26 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.

Let $A$ be a set with an equivalence relation $\sim$, and let $B$ be a second set. When there exists a canonical surjection $A \to B$ whose fibres are the equivalence classes, I say that $B$ ***classifies*** the $\sim$-classes of elements of $A$.

## Introduction

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 anistropic groups (those with no split torus). We give a different approach to describing nonsplit reductive algebraic groups. In this section, we show that they are classified by certain cohomology groups, and in the next section we show that certain algebras with involution are classified by the same cohomology groups. In this way we obtain a description of the groups in terms of algebras.

## Non-commutative cohomology.

Let $\Gamma$ be a group. A $\Gamma$-***set*** is a set $A$ with an action

$$(\sigma, a) \mapsto \sigma a \colon \Gamma \times A \to A$$

of $\Gamma$ 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 $G$ respects this structure (i.e., $\sigma(aa') = \sigma a \cdot \sigma a'$), then we say $A$ is a $G$-***group***.

### Definition of $H^0(\Gamma, A)$

For a $\Gamma$-set $A$, $H^0(\Gamma, A)$ is defined to be the set $A^\Gamma$ of elements left fixed by the operation of $\Gamma$ 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 $\Gamma$-group, then $H^0(\Gamma, A)$ is a group.

### Definition of $H^1(\Gamma, A)$

Let $A$ be a $\Gamma$-group. A mapping $\sigma \mapsto a_\sigma$ of $\Gamma$ into $A$ is said to be a 1-***cocycle*** of $\Gamma$ in $A$ if the relation $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ holds for all $\sigma, \tau \in \Gamma$. Two 1-cocycles $(a_\sigma)$ and $(b_\sigma)$ 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 $\Gamma$ 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 $\sigma \mapsto b^{-1} \cdot \sigma b$, $b \in A$.

### Homomorphisms

Let $A$ be $\Gamma$-group and $B$ an $\Delta$-group. Two homomorphisms $f\colon A \to B$ and $g\colon \Delta \to \Gamma$ are said to be ***compatible*** if

$$f(g(\sigma)a) = \sigma(f(a)) \text{ for all } \sigma \in \Delta, a \in A.$$

When $\Delta = \Gamma$ and $g$ is the identity, then $f$ is said to be a $\Gamma$-***homomorphism*** (or be $\Gamma$-***equivariant***). If $(a_\sigma)$ is a 1-cocycle for $A$, then

$$b_\sigma = f(a_{g(\sigma)})$$

is a 1-cocycle of $\Delta$ in $B$, and this defines a mapping $H^1(\Gamma, A) \to H^1(\Delta, B)$, which is a homomorphism if $A$ and $B$ are commutative.

### Exact sequences

PROPOSITION 26.1 *An exact sequence*

$$1 \to A' \to A \to A'' \to 1$$

*of $\Gamma$-groups gives rise to an exact sequence of cohomology sets*

$$1 \to H^0(\Gamma, A') \to H^0(\Gamma, A) \to H^0(\Gamma, A'') \to H^1(\Gamma, A') \to H^1(\Gamma, A) \to H^1(\Gamma, A'')$$

Exactness at $H^0(\Gamma, A'')$ means that the fibres of $H^0(\Gamma, A'') \to H^1(\Gamma, A')$ are the orbits of $H^0(\Gamma, A)$ acting on $H^0(\Gamma, A'')$. Exactness at $H^1(\Gamma, A')$ means that fibre of $H^1(\Gamma, A') \to H^1(\Gamma, A)$ over the distinguished element is the image of $H^0(\Gamma, A'')$.

We now define the boundary map $H^0(\Gamma, A'') \to H^1(\Gamma, A')$. For simplicity, regard $A'$ as a subgroup of $A$ with quotient $A''$. Let $a''$ be an element of $A''$ fixed by $\Gamma$, and choose an $a$ in $A$ mapping to it. Because $a''$ is fixed by $\Gamma$, $a^{-1} \cdot \sigma a$ is an element of $A'$, which we denote $a_\sigma$. 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.

### Classification of bilinear forms

Let $K$ be a finite Galois extension of $k$ with Galois group $\Gamma$. Let $V$ be a finite-dimensional $K$-vector space. By a ***semi-linear action*** of $\Gamma$ on $V$, I mean a homomorphism $\Gamma \to \mathrm{Aut}_{k\text{-lin}}(V)$ 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 $\Gamma$ 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 26.2 *The functor $V \mapsto K \otimes_k V$ from $k$-vector spaces to $K$-vector spaces endowed with a semi-linear action of $\Gamma$ is an equivalence of categories with quasi-inverse $V \mapsto V^\Gamma$.*

LEMMA 26.3 *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.*

PROOF. Note that $S$ is a simple $M_n(k)$-module. Since

$$\mathrm{End}_{k\text{-lin}}(k) = k = \mathrm{End}_{M_n(k)}(k^n)$$

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:

$$M_n(k) = \bigoplus\nolimits_{1\le i\le n} L(i) \quad \text{(as a left } M_n(k)\text{-module)}$$

where $L(i)$ is the set of matrices whose entries are zero except for those in the $i^{\text{th}}$ 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 15.3). □

LEMMA 26.4 *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 $\mathrm{End}_k(W)$-modules.*

PROOF. When we choose a basis for $W$, this becomes the previous lemma. □

PROOF. (OF THE PROPOSITION) Let $K[\Gamma]$ be the $K$-vector space with basis the elements of $\Gamma$, 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

$$(\textstyle\sum a_\sigma\sigma)c = \sum a_\sigma\sigma c,$$

and the resulting homomorphism

$$K[\Gamma] \to \mathrm{End}_k(K)$$

is injective by Dedekind's theorem on the independence of characters (FT 5.14). Since $K[\Gamma]$ and $\mathrm{End}_k(K)$ 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 $\mathrm{End}_k(K) \simeq K[\Gamma]$. This is the statement of the proposition. □

Let $(V_0,\phi_0)$ be a $k$-vector space with a bilinear form $V\times V\to k$, and write $(V_0,\phi_0)_K$ for the similar pair over $K$ obtained by extending scalars. Let $\mathcal{A}(K)$ denote the set of automorphisms of $(V_0,\phi_0)_K$.[71]

THEOREM 26.5 *The cohomology set $H^1(\Gamma,\mathcal{A}(K))$ classifies the isomorphism classes of pairs $(V,\phi)$ over $k$ that become isomorphic to $(V_0,\phi_0)$ over $K$.*

[71] In more detail: $(V_0,\phi_0)_K = (V_{0K},\phi_{0K})$ where $V_{0K} = K\otimes_k V_0$ and $\phi_{0K}$ is the unique $K$-bilinear map $V_{0K}\times V_{0K}\to K$ extending $\phi_0$; an element of $\mathcal{A}(K)$ is a $K$-linear isomorphism $\alpha\colon V_{0K}\to V_{0K}$ such that $\phi_{0K}(\alpha x,\alpha y) = \phi_{0K}(x,y)$ for all $x,y\in V_{0K}$.

PROOF. Suppose $(V,\phi)_K \approx (V_0,\phi_0)_K$, and choose an isomorphism

$$f\colon (V_0,\phi_0)_K \to (V,\phi)_K.$$

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 $f'\colon (V_0,\phi_0)_K \to (V,\phi)_K$ 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 $(V,\phi)$. It is easy to see that, in fact, it depends only on the isomorphism class of $(V,\phi)$, and that two pairs $(V,\phi)$ and $(V',\phi')$ giving rise to the same class are isomorphic. It remains to show that every cohomology class arises from a pair $(V,\phi)$. Let $(a_\sigma)_{\sigma\in\Gamma}$ be a 1-cocycle, and use it to define a new action of $\Gamma$ on $V_K =_{\text{df}} K\otimes_k V$:

$$^\sigma x = a_\sigma\cdot\sigma x,\quad \sigma\in\Gamma,\quad x\in V_K.$$

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,

$$V_1 \stackrel{\text{df}}{=} \{x\in V_K \mid {}^\sigma x = x\}$$

is a subspace of $V_K$ such that $K\otimes_k V_1 \simeq V_K$ (by 26.2). Because $\phi_{0K}$ 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 $\phi_{0K}$ induces a $k$-bilinear pairing on $V_1$. □

## Applications

Again let $K$ be a finite Galois extension of $k$ with Galois group $\Gamma$.

PROPOSITION 26.6 *For all $n$, $H^1(\Gamma,\mathrm{GL}_n(K)) = 1$.*

PROOF. Apply Theorem 26.5 with $V_0 = k^n$ and $\phi_0$ 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. □

PROPOSITION 26.7 *For all $n$, $H^1(\Gamma, \mathrm{SL}_n(K)) = 1$*

PROOF. Because the determinant map $\det\colon \mathrm{GL}_n(K) \to K^\times$ is surjective,

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^\times \to 1$$

is an exact sequence of $\Gamma$-groups. It gives rise to an exact sequence

$$\mathrm{GL}_n(k) \xrightarrow{\det} k^\times \to H^1(\Gamma, \mathrm{SL}_n) \to H^1(\Gamma, \mathrm{GL}_n)$$

from which the statement follows. □

PROPOSITION 26.8 *Let $\phi_0$ be a nondegenerate alternating bilinear form on $V_0$, and let* Sp *be the associated symplectic group*[72]*. Then $H^1(\Gamma, \mathrm{Sp}(K)) = 1$.*

PROOF. According to Theorem 26.5, $H^1(\Gamma, \mathrm{Sp}(K))$ classifies isomorphism classes of pairs $(V, \phi)$ over $k$ that become isomorphic to $(V_0, \phi_0)$ over $K$. But this condition implies that $\phi$ is a nondegenerate alternating form and that $\dim V = \dim V_0$. All such pairs $(V, \phi)$ are isomorphic. □

REMARK 26.9 Let $\phi_0$ be a nondegenerate bilinear symmetric form on $V_0$, and let $O$ be the associated orthogonal group. Then $H^1(\Gamma, O(K))$ classifies the isomorphism classes of quadratic spaces over $k$ that become isomorphic to $(V, \phi)$ over $K$. This is commonly a large set.

## Classifying the forms of an algebraic group

Again let $K$ be a finite Galois extension of $k$ with Galois group $\Gamma$. Let $G_0$ be an algebraic group over $k$, and let $\mathcal{A}(K)$ be the group of automorphisms $\alpha\colon G_K \to G_K$. Then $\Gamma$ acts on $\mathcal{A}(K)$ in a natural way:

$$\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}.$$

THEOREM 26.10 *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 $K$.*

PROOF. Let $G$ be such an algebraic group over $k$, choose an isomorphism

$$f\colon G_{0K} \to G_K,$$

and write

$$a_\sigma = f^{-1} \circ \sigma f.$$

As in the proof of Theorem 26.5, $(a_\sigma)_{\sigma\in\Gamma}$ is a 1-cocycle, and the map

$$G \mapsto \text{class of } (a_\sigma)_{\sigma\in\Gamma} \text{ in } H^1(\Gamma, A(K))$$

[72] So $\mathrm{Sp}(R) = \{a \in \mathrm{End}_{R\text{-lin}}(R \otimes_k V) \mid \phi(ax, ay) = \phi(x, y)\}$

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 bialgebra $K[G_{0K}] = K \otimes_k k[G_0]$. Let $A_0 = k[G_0]$ and $A = K \otimes_k A_0$. As in the proof of Theorem 26.5, we use a 1-cocycle $(a_\sigma)_{\sigma\in\Gamma}$ to twist the action of $\Gamma$ on $A$; specifically, we define

$$^\sigma a = a_\sigma \circ \sigma a, \quad \sigma \in \Gamma, \quad a \in A.$$

Proposition 26.2 in fact holds for infinite dimensional vector spaces $V$ with the same[73] 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 bialgebra structure on $A$ induces a bialgebra structure on $B$. Consider for example the comultiplication. The $k$-linear map

$$\Delta_0 \colon A_0 \to A_0 \otimes_k A_0$$

has a unique extension to a $K$-linear map

$$\Delta \colon A \to A \otimes_K A.$$

This map commutes with the action of $\Gamma$:

$$\Delta(\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Because $a_\sigma$ is a bialgebra 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 $\Delta$ maps $B$ into $(A \otimes_K A)^\Gamma$, which equals $B \otimes_k B$ because the functor in (26.2) preserves tensor products. Similarly, all the maps defining the bialgebra structure on $A$ preserve $B$, and therefore define a bialgebra structure on $B$. Finally, one checks that the 1-cocycle attached to $B$ and the given isomorphism $K \otimes_k B \to A$ is $(a_\sigma)$.□

## Infinite Galois groups

For simplicity, we now assume $k$ to be perfect. Let $\Gamma = \mathrm{Gal}(\overline{k}/k)$ where $\overline{k}$ is the algebraic closure of $k$. For any subfield $K$ of $\overline{k}$ finite over $k$, we let

$$\Gamma_K = \{\sigma \in \Gamma \mid \sigma x = x \text{ for all } x \in K\}.$$

We consider only $\Gamma$-groups $A$ for which

$$A = \bigcup A^{\Gamma_K} \tag{80}$$

[73] Except that the last step of the proof of (26.3) requires Zorn's lemma.

and we define $H^1(\Gamma, A)$ to be the equivalence classes of 1-cocycles that factor through $\mathrm{Gal}(K/k)$ for some subfield $K$ of $\overline{k}$ finite and Galois over $k$. With these definitions,[74]

$$H^1(\Gamma, A) = \varinjlim H^1(\mathrm{Gal}(K/k), A^{\Gamma_K}) \tag{81}$$

where $K$ runs through the subfields $K$ of $\overline{k}$ finite and Galois over $k$.

When $G$ is an algebraic group over $k$,

$$G(\overline{k}) = \bigcup G(K), \quad G(K) = G(\overline{k})^{\Gamma_K},$$

and so $G(\overline{k})$ satisfies (80). We write $H^i(k, G)$ for $H^i(\mathrm{Gal}(\overline{k}/k), G(\overline{k}))$.

## Exact sequences

An exact sequence

$$1 \to G' \to G \to G'' \to 1$$

of algebraic groups over $k$ gives rise to an exact

$$1 \to G'(\overline{k}) \to G(\overline{k}) \to G''(\overline{k}) \to 1$$

and hence (see 26.1) an exact sequence

$$1 \to G'(k) \to G(k) \to G''(k) \to H^1(k, G') \to H^1(k, G) \to H^1(k, G'')$$

## Examples

26.11 *For all $n$, $H^1(k, \mathrm{GL}_n) = 1$.*

This follows from (26.6) and (81).

26.12 *For all $n$, $H^1(k, \mathrm{SL}_n) = 1$.*

26.13 *For all $n$, $H^1(k, \mathrm{Sp}_n) = 1$.*

26.14 *Let $(V, \phi)$ 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 $\overline{k}$, all nondegenerate quadratic spaces of the same dimension are isomorphic. □

26.15 *Let $G$ be an algebraic group of $k$. The isomorphism classes of algebraic groups over $k$ that become isomorphic to $G_{\overline{k}}$ over $\overline{k}$ are classified by $H^1(\Gamma, \mathcal{A}(\overline{k}))$. Here $\Gamma = \mathrm{Gal}(\overline{k}/k)$ and $\mathcal{A}(\overline{k})$ is the automorphism group of $G_{\overline{k}}$.*

[74] Equivalently, we consider only $\Gamma$-groups $A$ for which the pairing $\Gamma \times A \to A$ is continuous relative to the Krull topology on $\Gamma$ and the discrete topology on $A$, and we require that the 1-cocycles be continuous for the same topologies.

## (Weil) restriction of the base field

Before considering the classification of algebraic groups, we need one more construction. Let $K$ be a finite extension of $k$, and let $G$ be an algebraic group over $K$. Define a functor

$$G_*(R) = G(K \otimes_k R)$$

from $k$-algebras to groups.

PROPOSITION 26.16 *The functor $G_*$ is an algebraic group over $k$ (i.e., it is represented by a finitely generated $k$-algebra).*

PROOF. Omitted (cf. AG 16.26). □

PROPOSITION 26.17 *There is a canonical isomorphism*

$$G_{*\overline{k}} \simeq \prod_{\rho: K \to \overline{k}} \rho G. \tag{82}$$

PROOF. The product is over the $k$-homomorphisms $K \to \overline{k}$, and by $\rho G$, we mean the algebraic group over $\overline{k}$ such that, for a $\overline{k}$-algebra $R$,

$$(\rho G)(R) = G(R)$$

— on the right, $R$ is regarded as a $k$-algebra via $\rho$. For a $\overline{k}$-algebra $R$,

$$\begin{aligned} K \otimes_k R &\simeq K \otimes_k (\overline{k} \otimes_{\overline{k}} R) \\ &\simeq (K \otimes_k \overline{k}) \otimes_{\overline{k}} R \\ &\simeq \left(\prod_{\rho: K \to \overline{k}} \overline{k}\right) \otimes_{\overline{k}} R. \end{aligned}$$

Thus, $G_{*\overline{k}} \simeq \prod_{\rho: K \to \overline{k}} \rho G$ as functors, and therefore as algebraic groups. □

From now on, **we assume that $k$ has characteristic zero.**

## Reductive algebraic groups

According to (15.2), 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 $Z(G) \to Z$. Because $k$ has characteristic zero, $Z(G)$ is of multiplicative type (even étale), and according to Theorem 9.20, 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 $\Gamma$. 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.

## Simply connected semisimple groups

Let $G$ be a simply connected semisimple group over $k$. Then, according to Theorem 14.23, $G_{\overline{k}}$ decomposes into a product

$$G_{\overline{k}} = G_1 \times \cdots \times G_r \tag{83}$$

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 $\sigma \in \Gamma$, equation (83) becomes

$$G_{\overline{k}} = \sigma G_{\overline{k}} = \sigma G_1 \times \cdots \times \sigma G_r$$

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 $\Gamma$. Then $\sigma H_i = H_i$, and so $H_i$ is defined over $k$ (11.2), 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 $\Gamma$ acts transitively on the $G_i$ in (83). Let

$$\Delta = \{\sigma \in \Gamma \mid \sigma G_1 = G_1\}.$$

Then $G_1$ is defined over the subfield $K = \overline{k}^{\Delta}$ of $\overline{k}$ (11.2).

PROPOSITION 26.18 *We have $G \simeq G_{1*}$.*

PROOF. We can rewrite (83) as

$$G_{\overline{k}} = \prod \sigma G_{1\overline{k}}$$

where $\sigma$ runs over a set of cosets for $\Delta$ in $\Gamma$. On comparing this with (82), we see that there is a canonical isomorphism

$$G_{\overline{k}} \simeq G_{1*\overline{k}}.$$

In particular, it commutes with the action of $\Gamma$, and so is defined over $k$ (AG 16.9). □

The group $G_1$ over $K$ is ***absolutely almost-simple***, i.e., it remains almost-simple over $\overline{k}$. 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 $G^{\mathrm{ad}} = G/Z(G)$.

PROPOSITION 26.19 *For any simply connected semisimple group $G$, there is an exact sequence*

$$1 \to G^{\mathrm{ad}}(\overline{k}) \to \mathcal{A}(\overline{k}) \to Sym(D) \to 1.$$

*When $G$ is split, $\Gamma$ acts trivially on $Sym(D)$, and the sequence is split, i.e., there is a subgroup of $\mathcal{A}(\overline{k})$ on which $\Gamma$ acts trivially and which maps isomorphically onto $Sym(D)$.*

PROOF. An element of $G^{\mathrm{ad}}(\overline{k}) = G(\overline{k})/Z(\overline{k})$ acts on $G_{\overline{k}}$ by an inner automorphism. Here $D$ is the Dynkin diagram of $G$, and $Sym(D)$ 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 (17.19). □

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 26.20 *For each indecomposable Dynkin diagram $D$, there is a split, absolutely almost-simple, simply connected algebraic group $G$ over $k$ such that $G_{\overline{k}}$ 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 $\overline{k}$ are classified by $H^1(k, \mathcal{A}(\overline{k}))$ where $\mathcal{A}(\overline{k})$ is the automorphism group of $G_{\overline{k}}$. For the split group $G$, $X^*(Z(G)) = P(D)/Q(D)$ with $\Gamma$ acting trivially. For the form $G'$ of $G$ defined by a 1-cocycle $(a_\sigma)$, $Z(G') = Z(G)$ but with $\Gamma$ acting through $a_\sigma$.*

We illustrate this last point. For $A_n$, the split group is $\mathrm{SL}_n$. This has centre $\mu_n$, which is the group of multiplicative type corresponding to $\mathbb{Z}/n\mathbb{Z}$ with the trivial action of $\Gamma$. Let $G_0$ and $G$ be groups over $k$, and let $f: G_{0\overline{k}} \to G_{\overline{k}}$ be an isomorphism over $\overline{k}$. Write $a_\sigma = f^{-1} \circ \sigma f$. Then $f$ defines an isomorphism

$$f: Z_0(\overline{k}) \to Z(\overline{k})$$

on the points of their centres, and

$$f(a_\sigma \sigma x) = \sigma(f(x)).$$

When use $f$ to identify $Z_0(\overline{k})$ with $Z(\overline{k})$, this says that $\Gamma$ acts on $Z(\overline{k})$ by the twisted action ${}^\sigma x = a_\sigma \sigma x$.

REMARK 26.21 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 $c \in H^1(k, G^{\mathrm{ad}})$, then $G$ is called an ***inner form*** of $G$. In general, $c$ will map to a nontrivial element of

$$H^1(k, Sym(D)) = \mathrm{Hom}_{\mathrm{continuous}}(\Gamma, Sym(D)).$$

Let $\Delta$ be the kernel of this homomorphism, and let $L$ be the corresponding exension field of $k$. Let $z = (\Gamma : \Delta)$. Then we say $G$ is of type ${}^z X_y$.

## 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.

26.22 *Let $k$ be finite. If $G$ is connected, then $H^1(k, G) = 1$.*

26.23 *Let $k$ be a finite extension of the field of $p$-adic numbers $\mathbb{Q}_p$. If $G$ is simply connected and semisimple, then $H^1(k, G) = 1$.*

26.24 *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 $(V, \phi)$, then*

$$H^1(\mathbb{Q}, G) \to \prod\nolimits_{p=2,3,5,\ldots,\infty} H^1(\mathbb{Q}_p, G)$$

*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.

The last statements extend in an obvious way (for those who know the language) to finite extensions of $K$.

NOTES For more on the cohomology of algebraic groups, see Platonov and Rapinchuk 1994 or Kneser, Lectures on Galois cohomology of classical groups, Tata, Bombay, 1969.

# 27 Classical groups and algebras with involution

An absolutely almost-simple simply connected algebraic group is said to be ***classical*** if it is of type $A_n$, $B_n$, $C_n$, or $D_n$ and becomes an inner form of the split form over a quadratic extension of $k$. For all but groups of type $D_4$, this last condition is automatic (see 26.19 et seq.). A semisimple group $G$ is ***classical*** if, in the decomposition of its simply connected covering, only classical groups occur. In this section, I will list all the absolutely almost-simple, simply connected, classical groups over a field $k$ of characteristic zero.

By a $k$-algebra $A$ I will 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*** $[A\colon k]$ of $A$).

## The forms of $M_n(k)$

DEFINITION 27.1 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 27.2 (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 (see p115). It is either a division algebra, or it is isomorphic to $M_2(k)$.

THEOREM 27.3 (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 my notes on Class Field Theory, IV 1.9 (Chapter IV can be read independently of the rest of the notes, and is fairly elementary). □

COROLLARY 27.4 *If $k$ 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 27.5 *The $k$-algebras becoming isomorphic to $M_n(k)$ over $\overline{k}$ 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 $\overline{k} \otimes_k A$ is again central simple (CFT 2.15), and so is isomorphic to $M_n(k)$ (27.4). Conversely, if $A$ is a $k$-algebra that becomes isomorphic to $M_n(\overline{k})$ over $\overline{k}$, then it is certainly central and simple, and has degree $n^2$. □

PROPOSITION 27.6 *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 the proof of 26.3). Let $\alpha$ 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 $f: S \to S'$. 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

$$\alpha(X) = YXY^{-1}.$$

□

COROLLARY 27.7 *The isomorphism classes of $k$-algebras becoming isomorphic to $M_n(k)$ over $\overline{k}$ are classified by $H^1(k, \mathrm{PGL}_n)$.*

PROOF. The proposition shows that

$$\mathrm{Aut}_{\overline{k}\text{-alg}}(M_n(\overline{k})) = \mathrm{PGL}_n(\overline{k}).$$

Let $A$ be a $k$-algebra for which there exists an isomorphism $f: M_n(\overline{k}) \to \overline{k} \otimes_k A$, and let

$$a_\sigma = f^{-1} \circ \sigma f.$$

Then $a_\sigma$ is a 1-cocycle, depending only on the $k$-isomorphism class of $A$.

Conversely, given a 1-cocycle, define

$${}^\sigma X = a_\sigma \cdot \sigma X, \quad \sigma \in \Gamma, X \in M_n(\overline{k}).$$

This defines an action of $\Gamma$ on $M_n(\overline{k})$ and $M_n(\overline{k})^\Gamma$ is a $k$-algebra becoming isomorphic to $M_n(k)$ over $\overline{k}$ (cf. the proof of 26.5). □

REMARK 27.8 Let $A$ be a central simple algebra over $k$. For some $n$, there exists an isomorphism $f: \overline{k} \otimes_k A \to M_n(\overline{k})$, unique up to an inner automorphism (27.5, 27.6). Let $a \in A$, and let $\mathrm{Nm}(a) = \det(f(a))$. Then $\mathrm{Nm}(a)$ does not depend on the choice of $f$. Moreover, it is fixed by $\Gamma$, and so lies in $k$. It is called the ***reduced norm*** of $a$.

## The inner forms of $\mathrm{SL}_n$

Consider

$$X \mapsto X: \mathrm{SL}_n(\overline{k}) \to M_n(\overline{k}).$$

The action of $\mathrm{PGL}_n(\overline{k})$ on $M_n(\overline{k})$ by inner automorphisms preserves $\mathrm{SL}_n(\overline{k})$, and is the full group of inner automorphisms of $\mathrm{SL}_n$.

THEOREM 27.9 *The inner forms of $\mathrm{SL}_n$ are the groups $\mathrm{SL}_m(D)$ for $D$ a division algebra of degree $n/m$.*

PROOF. The inner forms of $\mathrm{SL}_n$ and the forms of $M_n(k)$ are both classified by $H^1(k, \mathrm{PGL}_n)$, and so correspond. The forms of $M_n(k)$ are the $k$-algebras $M_m(D)$ (by 27.5, 27.3), and the form of $\mathrm{SL}_n$ is related to it exactly as $\mathrm{SL}_n$ is related to $M_n$. □

Here $\mathrm{SL}_m(D)$ is the group

$$R \mapsto \{a \in M_m(R \otimes_k D) \mid \mathrm{Nm}(a) = 1\}.$$

## Involutions of $k$-algebras

DEFINITION 27.10 Let $A$ be a $k$-algebra. An ***involution*** of $k$ is a $k$-linear map $a \mapsto a^*: A \to A$ such that

$$(ab)^* = b^*a^* \quad \text{all } a, b \in A,$$
$$a^{**} = a.$$

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 27.11 (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 27.12 *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 $\mathrm{inn}(a)$ commutes with $*$ means that the two maps

$$x \mapsto axa^{-1} \mapsto (a^*)^{-1}x^*a^*$$
$$x \mapsto x^* \mapsto ax^*a^{-1}$$

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 $a$. □

REMARK 27.13 Let $A$ have centre $k$. We can replace $a$ with $ca$, $c \in k^\times$, without changing $\mathrm{inn}(a)$. 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 $a^*a = 1$.

## All the forms of $\mathrm{SL}_n$

According to (26.19), there is an exact sequence

$$1 \to \mathrm{PGL}_n(\bar{k}) \to \mathrm{Aut}(\mathrm{SL}_{n\bar{k}}) \to Sym(D) \to 1,$$

and $Sym(D)$ has order 2. In fact, $X \mapsto (X^{-1})^t = (X^t)^{-1}$ is an outer automorphism of $\mathrm{SL}_n$.

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 $(X, Y) \mapsto (Y, X)$.[75] According to (27.12), the inner automorphism by

[75] This 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 $\overline{k}$, we can scale $a$ so that $a^*a = 1$ (27.13): if $a = (X, Y)$, then

$$1 = a^*a = (Y^tX, X^tY),$$

and so $a = (X, (X^t)^{-1})$. Thus, the automorphisms of $(M_n(\overline{k}) \times M_n(\overline{k}), *)$ are the inner automorphisms by elements $(X, (X^t)^{-1})$ and composites of such automorphisms with $(X, Y) \mapsto (Y, X)$. When we embed

$$X \mapsto (X, (X^t)^{-1}) : \mathrm{SL}_n(\overline{k}) \hookrightarrow M_n(\overline{k}) \times M_n(\overline{k}), \tag{84}$$

the image it is stable under the automorphisms of $(M_n(\overline{k}) \times M_n(\overline{k}), *)$, and this induces an isomorphism

$$\mathrm{Aut}(M_n(\overline{k}) \times M_n(\overline{k}), *) \simeq \mathrm{Aut}(\mathrm{SL}_{n\overline{k}}).$$

Thus, the forms of $\mathrm{SL}_n$ 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 (84) identifies $\mathrm{SL}_n(\overline{k})$ with the subgroup of $M_n(\overline{k}) \times M_n(\overline{k})$ of elements such that

$$a^*a = 1, \quad \mathrm{Nm}(a) = 1.$$

Therefore, the form of $\mathrm{SL}_n$ attached to the form $(A, *)$ is the group $G$ such that $G(R)$ consists of the $a \in R \otimes_k A$ such that

$$a^*a = 1, \quad \mathrm{Nm}(a) = 1.$$

There is a commutative diagram

$$\begin{array}{ccc} \mathrm{Aut}(\mathrm{SL}_{n\overline{k}}) & \longrightarrow & Sym(D) \\ \| & & \| \\ \mathrm{Aut}(M_n(\overline{k}) \times M_n(\overline{k}), *) & \longrightarrow & \mathrm{Aut}_{k\text{-alg}}(\overline{k} \times \overline{k}). \end{array}$$

The centre $K$ of $A$ is the form of $\overline{k} \times \overline{k}$ corresponding to the image of the cohomology class of $G$ in $Sym(D)$. Therefore, we see that $G$ is an outer form if and only if $K$ is a field.

## Forms of $\mathrm{Sp}_{2n}$

Here we use the $k$-algebra with involution of the first kind

$$M_{2n}(k), \quad X^* = SX^tS^{-1}, \quad S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The inner automorphism defined by an invertible matrix $U$ commutes with $*$ if and only if $U^*U \in k$ (see 27.12). When we pass to $\overline{k}$, we may suppose $U^*U = I$, i.e., that

$$SU^tS^{-1}U = I.$$

Because $S^{-1} = -S$, this says that

$$U^tSU = S$$

i.e., that $U \in \mathrm{Sp}_{2n}(\overline{k})$. Since there are no symmetries of the Dynkin diagram $C_n$, we see that the inclusion

$$X \mapsto X\colon \mathrm{Sp}_{2n}(\overline{k}) \hookrightarrow M_{2n}(\overline{k}) \tag{85}$$

induces an isomorphism

$$\mathrm{Aut}(\mathrm{Sp}_{2n\overline{k}}) \simeq \mathrm{Aut}(M_{2n}(\overline{k}), *).$$

Therefore, the forms of $\mathrm{Sp}_{2n}$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 (85) identifies $\mathrm{Sp}_{2n}(\overline{k})$ with the subgroup of $M_{2n}(\overline{k})$ of elements such that

$$a^*a = 1.$$

Therefore, the form of $\mathrm{Sp}_{2n}$ attached to $(A, *)$ is the group $G$ such that $G(R)$ consists of the $a \in R \otimes_k A$ for which

$$a^*a = 1.$$

### The forms of $\mathrm{Spin}(\phi)$

Let $(V, \phi)$ 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 $\mathrm{Spin}(\phi)$ given by (5.28). These actions are compatible with the natural homomorphism

$$\mathrm{Spin}(\phi) \to \mathrm{SO}(\phi)$$

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 $\phi$ relative to some basis for $V$. We use the $k$-algebra with involution of the first kind

$$M_n(k), \quad X^* = MX^tM^{-1}.$$

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

$$a^*a = 1.$$

### 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 27.14 *If a central simple algebra $A$ over $k$ admits an involution of the first kind, then*

$$A \otimes_k A \approx M_{n^2}(k), \quad n^2 = [A\colon k]. \tag{86}$$

PROOF. Recall that the opposite algebra $A^{\text{opp}}$ 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 $A^{\text{opp}}$ on $A_0$, namely, $A$ acts by left multiplication and $A^{\text{opp}}$ by right multiplication, and hence a homomorphism

$$A \otimes_k A^{\text{opp}} \to \text{End}_{k\text{-lin}}(A_0).$$

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 $A \to A^{\text{opp}}$, the proposition follows from this. □

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 $k$:

27.15 *the only central division algebras over $k$ or a finite extension of $k$ satisfying (86) are the quaternion algebras and the field itself (i.e., they have degree 4 or 1).*

THEOREM 27.16 *The following fields satisfy (27.15): 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 (27.4); for $\mathbb{Q}$ it requires the full force of class field theory (CFT).□

## 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 27.17 (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*

$$x^* = ax^\dagger a^{-1}, \quad \text{all } x \in A. \tag{87}$$

PROOF. See CFT 2.10. □

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 (87) 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 (87) holds with $a$ satisfying $a^\dagger = a$.

## 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
- $\phi: V \times V \to D$ 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 $\phi$ 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 27.18 (a) Let $D = k$ with $* = \mathrm{id}_k$. 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 $(V, \phi)$, and the special group of automorphisms of $\phi$ (the automorphisms with determinant 1, if this is not automatic).

## The groups attached to algebras with involution

We assume the ground field $k$ satisfies the condition (27.15), 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.

## Conclusion.

Let $k$ be a field satisfying the condition (27.15). Then the absolutely almost-simple, simply connected, classical groups over $k$ are the following:

**(A)** The groups $\mathrm{SL}_m(D)$ for $D$ a central division algebra over $k$ (the inner forms of $\mathrm{SL}_n$); the groups attached to a hermitian form for a quadratic field extension $K$ of $k$ (the outer forms of $\mathrm{SL}_n$).

**(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.

# 28 Arithmetic subgroups

## 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, $1\mathbb{Z}$ 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 $H_3$.

## Definitions and examples

Let $G$ be an algebraic group over $\mathbb{Q}$. Let $\rho\colon G \to \mathrm{GL}_V$ 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

$$\Gamma(N)_L = \{g \in G(\mathbb{Q})_L \mid g \text{ acts as 1 on } L/NL\}.$$

In other words, $\Gamma(N)_L$ is the kernel of

$$G(\mathbb{Q})_L \to \mathrm{Aut}(L/NL).$$

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 28.1 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,

$$\begin{aligned}\Gamma(N) &= \{A \in \mathrm{GL}_n(\mathbb{Z}) \mid A \equiv I \bmod N\}\\ &= \{(a_{ij}) \in \mathrm{GL}_n(\mathbb{Z}) \mid N \mid (a_{ij} - \delta_{ij})\},\end{aligned}$$

which is the kernel of

$$\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z}).$$

EXAMPLE 28.2 Consider a triple $(G, \rho, L)$ as in the definition of arithmetic subgroups. The choice of a basis for $L$ identifies $G$ with a subgroup of $\mathrm{GL}_n$ 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 $\mathrm{GL}_n$, one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. By abuse of notation, given a triple $(G, \rho, L)$, one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q})_L$.

EXAMPLE 28.3 Let

$$\mathrm{Sp}_{2n}(\mathbb{Z}) = \left\{A \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid A^t \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right) A = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)\right\}$$

is an arithmetic subgroup of $\mathrm{Sp}_{2n}(\mathbb{Q})$, and all arithmetic subgroups are commensurable with it.

EXAMPLE 28.4 Let $(V, \Phi)$ be a root system and $X$ a lattice $P \supset X \supset Q$. Chevalley showed that $(V, \Phi, X)$ defines an "algebraic group $G$ over $\mathbb{Z}$" which over $\mathbb{Q}$ becomes the split semisimple algebraic group associated with $(V, \Phi, X)$, and $G(\mathbb{Z})$ is a canonical arithmetic group in $G(\mathbb{Q})$.

EXAMPLE 28.5 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 28.6 (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 $T$ over $\mathbb{Q}$ such that $T(R) = (R \otimes_{\mathbb{Q}} K)^\times$, $T(\mathbb{Z}) = U$.

## 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 $\rho$ 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?

## Independence of $\rho$ and $L$.

LEMMA 28.7 *Let $G$ be a subgroup of $\mathrm{GL}_n$. For any representation $\rho\colon G \to \mathrm{GL}_V$ 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 $L$, $\rho$ becomes a homomorphism of algebraic groups $G \to \mathrm{GL}_{n'}$. The entries of the matrix $\rho(g)$ are polynomials in the entries of the matrix $g = (g_{ij})$, i.e., there exist polynomials $P_{\alpha,\beta} \in \mathbb{Q}[\ldots, X_{ij}, \ldots]$ such that

$$\rho(g)_{\alpha\beta} = P_{\alpha,\beta}(\ldots, g_{ij}, \ldots).$$

After a minor change of variables, this equation becomes

$$\rho(g)_{\alpha\beta} - \delta_{\alpha,\beta} = Q_{\alpha,\beta}(\ldots, g_{ij} - \delta_{ij}, \ldots)$$

with $Q_{\alpha,\beta} \in \mathbb{Q}[\ldots, X_{ij}, \ldots]$ and $\delta$ 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 $Q_{a,\beta}$, so that

$$mQ_{\alpha,\beta} \in \mathbb{Z}[\ldots, X_{ij}, \ldots].$$

If $g \equiv I \bmod m$, then

$$Q_{\alpha,\beta}(\ldots, g_{ij} - \delta_{ij}, \ldots) \in \mathbb{Z}.$$

Therefore, $\rho(g)\mathbb{Z}^{n'} \subset \mathbb{Z}^{n'}$, and, as $g^{-1}$ also lies in $\Gamma(m)$, $\rho(g)\mathbb{Z}^{n'} = \mathbb{Z}^{n'}$. □

PROPOSITION 28.8 *For any faithful representations $G \to \mathrm{GL}_V$ and $G \to \mathrm{GL}_{V'}$ 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 $\Gamma$ 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,

$$(G(\mathbb{Q})_{L'} : G(\mathbb{Q})_L \cap G(\mathbb{Q})_{L'}) < \infty.$$ □

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 (28.7) shows that, for any $N$, there exists an $m$ such that $\Gamma(Nm) \subset \Gamma_L(N)$.

## Behaviour with respect to homomorphisms

PROPOSITION 28.9 *Let $\Gamma$ be an arithmetic subgroup of $G(\mathbb{Q})$, and let $\rho: G \to \mathrm{GL}_V$ be a representation of $G$. Every lattice $L$ of $V$ is contained in a lattice stable under $\Gamma$.*

PROOF. According to (28.7), there exists a subgroup $\Gamma'$ leaving $L$ stable. Let

$$L' = \sum \rho(g)L$$

where $g$ runs over a set of coset representatives for $\Gamma'$ in $\Gamma$. The sum is finite, and so $L'$ is again a lattice in $V$, and it is obviously stable under $\Gamma$. □

PROPOSITION 28.10 *Let $\varphi: G \to G'$ be a homomorphism of algebraic groups over $\mathbb{Q}$. For any arithmetic subgroup $\Gamma$ of $G(\mathbb{Q})$, $\varphi(\Gamma)$ is contained in an arithmetic subgroup of $G'(\mathbb{Q})$.*

PROOF. Let $\rho: G' \to \mathrm{GL}_V$ be a faithful representation of $G'$, and let $L$ be a lattice in $V$. According to (28.9), there exists a lattice $L' \supset L$ stable under $(\rho \circ \varphi)(\Gamma)$, and so $G'(\mathbb{Q})_L \supset \varphi(\Gamma)$. □

REMARK 28.11 If $\varphi: G \to G'$ is a quotient map and $\Gamma$ 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 1979, 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.)

### 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 $\ell$ runs over the finite primes of $\mathbb{Q}$. Thus, $\mathbb{A}_f$ is the subring of $\prod\mathbb{Q}_\ell$ consisting of the $(a_\ell)$ such that $a_\ell \in \mathbb{Z}_\ell$ for almost all $\ell$, and it is endowed with the topology for which $\prod\mathbb{Z}_\ell$ is open and has the product topology.

Let $V = \operatorname{Spm} A$ be an affine variety over $\mathbb{Q}$. The set of points of $V$ with coordinates in a $\mathbb{Q}$-algebra $R$ is

$$V(R) = \operatorname{Hom}_{\mathbb{Q}}(A, R).$$

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

$$V(\mathbb{Z}_\ell) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_m], \mathbb{Z}_\ell) = V(\mathbb{Q}_\ell) \cap \mathbb{Z}_\ell^m \qquad \text{(inside } \mathbb{Q}_\ell^m\text{)}.$$

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

$$\mathbb{Z}[\tfrac{1}{d}][x_1, \dots, x_m] = \mathbb{Z}[\tfrac{1}{d}][y_1, \dots, y_n] \qquad \text{(inside } A\text{)}.$$

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.[76] For example,

$$\mathbb{G}_m(\mathbb{A}_f) = \prod(\mathbb{Q}_\ell^\times : \mathbb{Z}_\ell^\times) = \mathbb{A}_f^\times.$$

PROPOSITION 28.12 *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.*[77]

[76] The choice of generators determines a group structure on $G(\mathbb{Z}_\ell)$ for almost all $\ell$, etc..

[77] To 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 $\Gamma$ 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 $\mathbb{Q}[\mathrm{GL}_n] \to \mathbb{Q}[G]$ (of $\mathbb{Q}$-algebras of regular functions), i.e., a surjection

$$\mathbb{Q}[X_{11}, \dots, X_{nn}, T]/(\det(X_{ij})T - 1) \to \mathbb{Q}[G],$$

and hence $\mathbb{Q}[G] = \mathbb{Q}[x_{11}, \dots, x_{nn}, t]$. For this presentation of $\mathbb{Q}[G]$,

$$G(\mathbb{Z}_\ell) = G(\mathbb{Q}_\ell) \cap \mathrm{GL}_n(\mathbb{Z}_\ell) \qquad (\text{inside } \mathrm{GL}_n(\mathbb{Q}_\ell)).$$

For an integer $N > 0$, let

$$K(N) = \textstyle\prod_\ell K_\ell, \quad \text{where} \quad K_\ell = \begin{cases} G(\mathbb{Z}_\ell) & \text{if} \quad \ell \nmid N \\ \{g \in G(\mathbb{Z}_\ell) \mid g \equiv I_n \bmod \ell^{r_\ell}\} & \text{if} \quad r_\ell = \mathrm{ord}_\ell(N). \end{cases}$$

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. □

## 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 $\Gamma$ 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 (J. Lee, Introduction to smooth manifolds, 2003, 9.22).

THEOREM 28.13 *For any discrete torsion-free subgroup $\Gamma$ of $G(\mathbb{R})$, $\Gamma$ acts freely on $M$, and $\Gamma\backslash M$ is a smooth manifold.*

PROOF. Standard; see for example Lee 2003, Chapter 9, or 3.1 of my notes, Introduction to Shimura varieties. □

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.

## 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 28.14 *Every arithmetic group contains a torsion-free subgroup of finite index.*

For this, it suffices to prove the following statement.

LEMMA 28.15 *For any prime $p \geq 3$, the subgroup $\Gamma(p)$ of $\mathrm{GL}_n(\mathbb{Z})$ is torsion-free.*

PROOF. If not, it will contain an element of order a prime $\ell$, 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

$$\ell p^m A = -\sum\nolimits_{i=2}^{\ell} \binom{\ell}{i} p^{mi} A^i.$$

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 $2 \leq i < p$, $p^{2m+1} | \binom{p}{i} p^{mi}$ because $p | \binom{p}{i}$, and $p^{2m+1} | p^{mp}$ because $p \geq 3$. Again we have a contradiction. □

## A fundamental domain for $\mathrm{SL}_2$

Let $\mathcal{H}$ be the complex upper half plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$,

$$\Im\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\Im(z)}{|cz+d|^2}. \tag{88}$$

Therefore, $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ by holomorphic maps

$$\mathrm{SL}_2(\mathbb{R}) \times \mathcal{H} \to \mathcal{H}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

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

$$O = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a^2 + b^2 = 1 \right\}$$

(compact circle group). Thus

$$\mathcal{H} \simeq (\mathrm{SL}_2(\mathbb{R})/O) \cdot i$$

as a smooth manifold.

PROPOSITION 28.16 *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 (88)) 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 $\gamma$.

The proof of the second part of the statement is omitted. □

## Application to quadratric 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

$$q(x, y) = (x, y) \cdot Q \cdot \begin{pmatrix} x \\ y \end{pmatrix}, \qquad q'(x, y) = (x, y) \cdot Q' \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

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

$$q(x, y) = a(x - \omega y)(x - \overline{\omega} y), \, a \in \mathbb{R}_{>0}, \, \omega \in \mathcal{H}.$$

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

$$-a < b \le a < c \text{ or}$$
$$0 \le b \le a = c.$$

Theorem 28.16 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

$$4a^2 \le 4ac = b^2 - \Delta \le a^2 - \Delta$$

we see that there are only finitely many values of $a$ for a fixed $\Delta$. Since $|b| \le a$, 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, Number theory, 1966, especially Chapter 3, §6).

## "Large" discrete subgroups

Let $\Gamma$ be a subgroup of a locally compact group $G$. A discrete subgroup $\Gamma$ of a locally compact group $G$ is said to ***cocompact*** (or ***uniform***) if $G/\Gamma$ is compact. This is a way of saying that $\Gamma$ 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***[78], which induces a measure $\mu$ on $\Gamma\backslash G$. If $\mu(\Gamma\backslash G) < \infty$, then one says that $\Gamma$ has ***finite covolume***, or that $\Gamma$ 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 28.17 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 $i < n$, $\Gamma$ does not have finite covolume. (The left-invariant measure on $\mathbb{R}^n$ is just the usual Lebesgue measure.)

EXAMPLE 28.18 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 $\frac{dxdy}{y^2}$, and

$$\int_{\Gamma\backslash\mathcal{H}} \frac{dxdy}{y^2} = \iint_D \frac{dxdy}{y^2} \le \int_{\sqrt{3}/2}^{\infty} \int_{-1/2}^{1/2} \frac{dxdy}{y^2} = \int_{\sqrt{3}/2}^{\infty} \frac{dy}{y^2} < \infty.$$

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).

[78]For real Lie groups, the proof of the existence is much more elementary than in the general case (cf. Boothby 1975, VI 3.5).

EXAMPLE 28.19 Consider $G = \mathbb{G}_m$. The left-invariant measure[79] 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**

28-1 Show that, if a subgroup $\Gamma$ of a locally compact group is discrete (resp. is cocompact, resp. has finite covolume), then so also is every subgroup commensurable with $\Gamma$.

## Reduction theory

In this section, I can only summarize the main definitions and results from A. Borel, Introduction aux groupes arithmétiques, Hermann, 1969.

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

$$\vec{y} = \begin{pmatrix} \sqrt{t_1} & 0 & & 0 \\ 0 & \sqrt{t_2} & & 0 \\ & & \ddots & \\ 0 & 0 & & \sqrt{t_n} \end{pmatrix} \begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ 0 & 1 & \cdots & u_{2n} \\ & & \ddots & \vdots \\ 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \tag{89}$$

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

$$B, Q \mapsto B^t Q B \colon \mathrm{GL}_n(\mathbb{R}) \times \mathcal{Q}_n \to \mathcal{Q}_n.$$

The action is transitive, and the subgroup fixing the form $I$ is[80] $O_n(\mathbb{R}) = \{A \mid A^t A = I\}$, and so we can read off from (89) a set of representatives for the cosets of $O_n(\mathbb{R})$ in $\mathrm{GL}_n(\mathbb{R})$. We find that

$$\mathrm{GL}_n(\mathbb{R}) \simeq A \cdot N \cdot K$$

where

- $K$ is the compact group $O_n(\mathbb{R})$,
- $A = T(\mathbb{R})^+$ for $T$ the split maximal torus in $\mathrm{GL}_n$ of diagonal matrices,[81] and

[79] Because $\frac{dax}{ax} = \frac{dx}{x}$; alternatively,

$$\int_{t_1}^{t_2} \frac{dx}{x} = \log(t_2) - \log(t_1) = \int_{at_1}^{at_2} \frac{dx}{x}.$$

[80] So we are reverting to using $O_n$ for the orthogonal group of the form $x_1^2 + \cdots + x_n^2$.

[81] The $^+$ denotes the identity component of $T(\mathbb{R})$ for the real topology. Thus, for example,

$$(\mathbb{G}_m(\mathbb{R})^r)^+ = (\mathbb{R}^r)^+ = (\mathbb{R}_{>0})^r.$$

◇ $N$ is the group $\mathbb{U}_n(\mathbb{R})$.

Since $A$ normalizes $N$, we can rewrite this as

$$\mathrm{GL}_n(\mathbb{R}) \simeq N \cdot A \cdot K.$$

For any compact neighbourhood $\omega$ of 1 in $N$ and real number $t > 0$, let

$$\mathfrak{S}_{t,\omega} = \omega \cdot A_t \cdot K$$

where

$$A_t = \{a \in A \mid a_{i,i} \le t a_{i+1,i+1}, \quad 1 \le i \le n-1\}. \tag{90}$$

Any set of this form is called a ***Siegel set***.

THEOREM 28.20 *Let $\Gamma$ be an arithmetic subgroup in $G(\mathbb{Q}) = \mathrm{GL}_n(\mathbb{Q})$. 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 $\Gamma$ 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 1969, 11.4, 11.9). The definition of the ***Siegel sets*** is the same except now[82]

$$A_t = \{a \in A \mid \alpha(a) \le t \text{ for all } \alpha \in S\}. \tag{91}$$

Then Theorem 28.20 continues to hold in this more general situation (Borel 1969, 13.1, 15.4).

EXAMPLE 28.21 The images of the Siegel sets for $\mathrm{SL}_2$ in $\mathcal{H}$ are the sets

$$\mathfrak{S}_{t,u} = \{z \in \mathcal{H} \mid \Im(z) \ge t, \quad |\Re(z)| \le u\}.$$

THEOREM 28.22 *If $\mathrm{Hom}_k(G, \mathbb{G}_m) = 0$, then every Siegel set has finite measure.*

PROOF. Borel 1969, 12.5. □

[82]Recall that, with the standard choices, $\chi_1 - \chi_2, \dots, \chi_{n-1} - \chi_n$ is a base for the roots of $T$ in $\mathrm{GL}_n$, so this definition agrees with that in (90).

THEOREM 28.23 *Let $G$ be a reductive group over $\mathbb{Q}$, and let $\Gamma$ 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 (28.19). The sufficiency follows from (28.21) and (28.22).

(b) See Borel 1969, 8.4. □

EXAMPLE 28.24 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 28.28 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 ($\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ 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 28.25 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 1969, 8.6).

## Presentations

In this section, I assume some familiarity with free groups and presentations (see, for example, §2 of my notes on Group Theory).

PROPOSITION 28.26 *The group $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is generated by $S = \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$.*

PROOF. Let $\Gamma'$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ generated by $S$ and $T$. The argument in the proof of (28.16) 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 28.16). □

In fact $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ has a presentation $\langle S, T | S^2, (ST)^3\rangle$. It is known that every torsion-free subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ is free on $1 + \frac{(\mathrm{SL}_2(\mathbb{Z}):\Gamma)}{12}$ generators.[83] For example, the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z})$ has index 12, and is the free group on the generators $\left(\begin{smallmatrix}2&1\\1&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$.

For a general algebraic group $G$ over $\mathbb{Q}$, choose $\mathfrak{S}$ and $C$ as in (28.20a), and let

$$D = \bigcup\nolimits_{g\in C} g\mathfrak{S}/K.$$

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 $\Gamma$, and that, moreover, $\Gamma$ has a finite presentation.

[83] Contrary to appearances, this statement is correct.

## The congruence subgroup problem

Consider an algebraic subgroup $G$ of $\mathrm{GL}_n$. Is every arithmetic subgroup congruence? That is, does every subgroup commensurable with $G(\mathbb{Z})$ contain

$$\Gamma(N) =_{\mathrm{df}} \mathrm{Ker}(G(\mathbb{Z}) \to G(\mathbb{Z}/N\mathbb{Z}))$$

for some $N$.

That $\mathrm{SL}_2(\mathbb{Z})$ has noncongruence arithmetic subgroups was noted by Klein as early as 1880. For a proof that $\mathrm{SL}_2(\mathbb{Z})$ has infinitely many subgroups of finite index that are not congruence subgroups see B. Sury, The congruence subgroup problem, Hindustan, 2003, 3-4.1. The proof proceeds by showing that the groups occurring as quotients of $\mathrm{SL}_2(\mathbb{Z})$ by principal congruence subgroups are of a rather special type, and then exploits the known structure of $\mathrm{SL}_2(\mathbb{Z})$ 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 $\mathrm{SL}_2(\mathbb{Z})$ of index $\leq m$ and $N'(m)$ the number of arithmetic subgroups, then $N(m)/N'(m) \to 0$ as $m \to \infty$.

However, $\mathrm{SL}_2$ is unusual. For split simply connected almost-simple groups other than $\mathrm{SL}_2$, for example, for $\mathrm{SL}_n$ ($n \geq 3$), $\mathrm{Sp}_{2n}$ ($n \geq 2$), 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 and we denote the corresponding completions by $\widehat{G}$ and $\overline{G}$. Because every congruence group is arithmetic, the identity map on $G(\mathbb{Q})$ gives a surjective homomorphism $\widehat{G} \to \overline{G}$, 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 $C(\mathrm{SL}_2)$ 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:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C(G) & \longrightarrow & \widehat{G} & \longrightarrow & \overline{G} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \widehat{\pi}} & & \downarrow{\scriptstyle \overline{\pi}} & & \\ 1 & \longrightarrow & C(G') & \longrightarrow & \widehat{G}' & \longrightarrow & \overline{G}' & \longrightarrow & 1. \end{array}$$

It is known that $\overline{G} = G(\mathbb{A}_f)$, and that the kernel of $\widehat{\pi}$ is $N(\mathbb{Q})$, which is finite. On the other hand, the kernel of $\overline{\pi}$ is $N(\mathbb{A}_f)$, which is infinite. Because $\mathrm{Ker}(\overline{\pi}) \neq N(\mathbb{Q})$, $\pi\colon G(\mathbb{Q}) \to G'(\mathbb{Q})$ 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 is contained in the centre of $\widehat{G(\mathbb{Q})}$. For an absolutely 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 $\mathrm{SL}_n$) and equal to it many cases (work of Gopal Prasad, Raghunathan, Rapinchuk, and others).

## The theorem of Margulis

DEFINITION 28.27 Let $H$ be a semisimple algebraic group over $\mathbb{R}$. A subgroup $\Gamma$ of $H(\mathbb{R})$ is ***arithmetic*** if there exists an algebraic group $G$ over $\mathbb{Q}$, a surjective map $G_{\mathbb{R}} \to H$ such that the kernel of $\varphi(\mathbb{R})\colon G(\mathbb{R}) \to H(\mathbb{R})$ is compact, and an arithmetic subgroup $\Gamma'$ of $G(\mathbb{R})$ such that $\varphi(\Gamma')$ is commensurable with $\Gamma$.

EXAMPLE 28.28 Let $B$ be a quaternion algebra over a finite extension $F$ of $\mathbb{Q}$,

$$B = F + Fi + Fj + Fk$$
$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji.$$

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 $R$,

$$G(R) = \{b \in R \otimes_{\mathbb{Q}} B \mid \mathrm{Nm}(b) = 1\}.$$

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

$$G(\mathbb{R}) \approx \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H}^1 \times \cdots \times \mathbb{H}^1$$
$$\mathbb{H}^1 = \{w + xi + yj + zk \in \mathbb{H} \mid w^2 + x^2 + y^2 + z^2 = 1\}.$$

Nonisomorphic $B$'s define different commensurability classes of arithmetic subgroups of $\mathrm{SL}_2(\mathbb{R})$, and all such classes arise in this way.

Not every discrete subgroup in $\mathrm{SL}_2(\mathbb{R})$ (or $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$) 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 $\mathrm{Aut}(\mathcal{H}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ 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 $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ (therefore also in $\mathrm{SL}_2(\mathbb{R})$), but there only countably many arithmetic subgroups.

The following amazing theorem of Margulis shows that $\mathrm{SL}_2$ is exceptional in this regard:

THEOREM 28.29 *Let $\Gamma$ be a discrete subgroup of finite covolume in a noncompact almost-simple real algebraic group $H$; then $\Gamma$ is arithmetic unless $H$ is isogenous to* $\mathrm{SO}(1, n)$ *or* $\mathrm{SU}(1, n)$.

PROOF. The proof is given in G. Margulis, Discrete subgroups of semisimple Lie groups, Springer, 1991. For a disussion of it, see D. Witte, Introduction to arithmetic groups, arXiv:math.DG/0106063. □

Here
$\mathrm{SO}(1, n)$ correspond to $x_1^2 + \cdots + x_n^2 - x_{n+1}^2$
$SU(1, n)$ corresponds to $z_1\overline{z}_1 + \cdots + z_n\overline{z}_n - z_{n+1}\overline{z}_{n+1}$.
Note that, because $\mathrm{SL}_2(\mathbb{R})$ is isogenous to $\mathrm{SO}(1, 2)$, the theorem doesn't apply to it.

## Shimura varieties

Let $U_1 = \{z \in \mathbb{C} \mid z\overline{z} = 1\}$. Recall that for a group $G$, $G^{\mathrm{ad}} = G/Z(G)$ and that $G$ is said to be adjoint if $G = G^{\mathrm{ad}}$ (i.e., if $Z(G) = 1$).

THEOREM 28.30 *Let $G$ be a semisimple adjoint group over $\mathbb{R}$, and let $u\colon U_1 \to G(\mathbb{R})$ be a homomorphism such that*

(a) *only the characters $z^{-1}, 1, z$ occur in the representation of $U_1$ on $\mathrm{Lie}(G)_{\mathbb{C}}$;*

(b) *the subgroup*

$$K_{\mathbb{C}} = \{g \in G(\mathbb{C}) \mid g = \mathrm{inn}(u(-1))(\overline{g})\}$$

*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. S. Helgason, Differential geometry, Lie groups, and symmetric spaces, Academic, 1978, VIII; see also my notes Introduction to Shimura varieties (ISV), 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 28.31 *Let $G$ be a simply connected semisimple algebraic group over $\mathbb{Q}$ having no simple factor $H$ with $H(\mathbb{R})$ compact. Let $u\colon U_1 \to G^{\mathrm{ad}}(\mathbb{R})$ be a homomorphism satisfying (a) and (b) of (28.30), and let $X = G^{\mathrm{ad}}(\mathbb{R})^+/K$ with its structure as a complex manifold. For each torsion-free arithmetic subgroup $\Gamma$ 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 ISV 3.12 for a discussion of the theorem. □

EXAMPLE 28.32 Let $G = \mathrm{SL}_2$. For $z \in \mathbb{C}$, choose a square root $a + ib$, and map $z$ to $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$. For example, $u(-1) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and

$$K_{\mathbb{C}} = \{\left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{C}) \mid |a|^2 + |b|^2 = 1\},$$

which is compact. Moreover,

$$K \stackrel{\mathrm{df}}{=} K_{\mathbb{C}} \cap \mathrm{SL}_2(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R}) \mid a^2 + b^2 = 1\}.$$

Therefore $G(\mathbb{R})/K \approx \mathcal{H}$.

THEOREM 28.33 *Let $G$, $u$, and $X$ be as in (28.31). If $\Gamma$ is a congruence subgroup, then $\Gamma\backslash X$ has a canonical model over a specific finite extension $\mathbb{Q}_\Gamma$ of $\mathbb{Q}$.*

PROOF. For a discussion of the theorem, see ISV §§12–14.Reference to be added. □

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 $\mathrm{SL}_2(\mathbb{Q})$ consisting of matrices the $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ 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 $Y_0(N) \to E$ for some $N$, and that from this Fermat's last theorem follows.

## Index of definitions