Lie Algebras, Algebraic Groups,

and

Lie Groups

J.S. Milne

Version 2.00
May 5, 2013

These notes are an introduction to Lie algebras, algebraic groups, and Lie groups in characteristic zero, emphasizing the relationships between these objects visible in their categories of representations. Eventually these notes will consist of three chapters, each about 100 pages long, and a short appendix.

BibTeX information:

```
@misc{milneLAG,
author={Milne, James S.},
title={Lie Algebras, Algebraic Groups, and Lie Groups},
year={2013},
note={Available at www.jmilne.org/math/}
}
```

v1.00 March 11, 2012; 142 pages.
V2.00 May 1, 2013; 186 pages.

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

The photo is of a grotto on The Peak That Flew Here, Hangzhou, Zhejiang, China.

Table of Contents

Preface

[Lie] did not follow the accepted paths... I would compare him rather to a pathfinder in a primal forest who always knows how to find the way, whereas others thrash around in the thicket... moreover, his pathway always leads past the best vistas, over unknown mountains and valleys.

Friedrich Engel.

Lie algebras are an essential tool in studying both algebraic groups and Lie groups. **Chapter I** develops the basic theory of Lie algebras, including the fundamental theorems of Engel, Lie, Cartan, Weyl, Ado, and Poincaré-Birkhoff-Witt. The classification of semisimple Lie algebras in terms of the Dynkin diagrams is explained, and the structure of semisimple Lie algebras and their representations described.

In **Chapter II** we apply the theory of Lie algebras to the study of algebraic groups in characteristic zero. As Cartier (1956) noted, the relation between Lie algebras and algebraic groups in characteristic zero is best understood through their categories of representations.

For example, when $\mathfrak{g}$ is a semisimple Lie algebra, the representations of $\mathfrak{g}$ form a tannakian category $\mathsf{Rep}(\mathfrak{g})$ whose associated affine group G is the simply connected semisimple algebraic group G with Lie algebra $\mathfrak{g}$. In other words,

$$\mathsf{Rep}(G) = \mathsf{Rep}(\mathfrak{g}) \tag{1}$$

with G a simply connected semisimple algebraic group having Lie algebra $\mathfrak{g}$. It is possible to compute the centre of G from $\mathsf{Rep}(\mathfrak{g})$, and to identify the subcategory of $\mathsf{Rep}(\mathfrak{g})$ corresponding to each quotient of G by a finite subgroup. This makes it possible to read off the entire theory of semisimple algebraic groups and their representations from the (apparently simpler) theory of semisimple Lie algebras.

For a general Lie algebra $\mathfrak{g}$, we consider the category $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ of representations of $\mathfrak{g}$ such that the elements in the largest nilpotent ideal of $\mathfrak{g}$ act as nilpotent endomorphisms. Ado's theorem assures us that $\mathfrak{g}$ has a faithful such representation, and from this we are able to deduce a correspondence between algebraic Lie algebras and algebraic groups with unipotent centre.

Let G be a reductive algebraic group with a split maximal torus T. The action of T on the Lie algebra $\mathfrak{g}$ of G induces a decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha}, \quad \mathfrak{h} = \mathrm{Lie}(T),$$

of $\mathfrak{g}$ into eigenspaces $\mathfrak{g}^{\alpha}$ indexed by certain characters α of T, called the roots. A root α determines a copy $\mathfrak{s}_{\alpha}$ of $\mathfrak{sl}_2$ in $\mathfrak{g}$. From the composite of the exact tensor functors

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{s}_{\alpha}) \overset{(1)}{=} \mathsf{Rep}(S_{\alpha}),$$

we obtain a homomorphism from a copy S_{α} of SL_2 into G. Regard α as a root of S_{α}; then its coroot $\alpha^{\vee}$ can be regarded as an element of $X_*(T)$. The system $(X^*(T), R, \alpha \mapsto \alpha^{\vee})$ is a root datum. From this, and the Borel fixed point theorem, the entire theory of split reductive groups over fields of characteristic zero follows easily.

Although there are many books on algebraic groups, and even more on Lie groups, there are few that treat both. In fact it is not easy to discover in the expository literature what the precise relation between the two is. In **Chapter III** we show that all connected complex semisimple Lie groups are algebraic groups, and that all connected real semisimple Lie groups arise as covering groups of algebraic groups. Thus readers who understand the theory of algebraic groups and their representations will find that they also understand much of the theory of Lie groups. Again, the key tool is tannakian duality.

Realizing a Lie group as an algebraic group is the first step towards understanding the discrete subgroups of the Lie group. We discuss the discrete groups that arise in this way in an appendix.

At present, only the split case is covered in Chapter I, only the semisimple case is covered in detail in Chapter II, and only a partial summary of Chapter III is available.

Notations; terminology

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

Throughout k is the ground field, usually of characteristic zero, and R always denotes a commutative k-algebra. A k-algebra A is a k-module equipped with a k-bilinear (multiplication) map $A \times A \to k$. Associative k-algebras are required to have an element 1, and $\{c1 \mid c \in k\}$ is contained in the centre of the algebra. Unadorned tensor products are over k. Notations from commutative algebra are as in my primer. When k is a field, k^{sep} denotes a separable algebraic closure of k and k^{al} an algebraic closure of k. The dual $\mathrm{Hom}_{k\text{-linear}}(V, k)$ of a k-module V is denoted by $V^\vee$. The transpose of a matrix M is denoted by M^t. We define the eigenvalues of an endomorphism of a vector space to be the roots of its characteristic polynomial.

We use the terms "morphism of functors" and "natural transformation of functors" interchangeably. When F and F' are functors from a category, we say that "a homomorphism $F(a) \to F'(a)$ is natural in a" when we have a family of such maps, indexed by the objects a of the category, forming a natural transformation $F \to F'$. For a natural transformation $\alpha: F \to F'$, we often write α_R for the morphism $\alpha(R): F(R) \to F'(R)$. When its action on morphisms is obvious, we usually describe a functor F by giving its action $R \rightsquigarrow F(R)$ on objects. Categories are required to be locally small (i.e., the morphisms between any two objects form a set), except for the category $\mathsf{A}^\vee$ of functors $\mathsf{A} \to \mathsf{Set}$. A diagram $A \to B \rightrightarrows C$ is said to be exact if the first arrow is the equalizer of the pair of arrows; in particular, this means that $A \to B$ is a monomorphism.

The symbol $\twoheadrightarrow$ denotes a surjective map, and $\hookrightarrow$ an injective map.

We use the following conventions:

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

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

ASIDES may be skipped; NOTES are often reminders to the author.

Prerequisites

The only prerequisite for Chapter I (Lie algebras) is the algebra normally taught in first-year graduate courses and in some advanced undergraduate courses. Chapter II (algebraic groups) makes use of some algebraic geometry from the first 11 chapters of my notes AG, and Chapter III (Lie groups) assumes some familiarity with manifolds.

References

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

GT Group Theory (v3.13, 2013).
CA A Primer of Commutative Algebra (v2.23, 2013).
AG Algebraic Geometry (v5.22, 2012).
AGS Basic Theory of Affine Group Schemes (v1.00, 2012).

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

Also, I use the following abbreviations:

Bourbaki A Bourbaki, Algèbre.
Bourbaki LIE Bourbaki, Groupes et Algèbres de Lie (I 1972; II–III 1972; IV–VI 1981).
DG Demazure and Gabriel, Groupes Algébriques, Tome I, 1970.
Sophus Lie Séminaire “Sophus Lie”, Paris, 1954–56.
monnnn http://mathoverflow.net/questions/nnnn/

The works of Casselman cited can be found on his home page under “Essays on representations and automorphic forms”.

Acknowledgements

I thank the following for providing comments and corrections for earlier versions of these notes: Lyosha Beshenov; Roland Loetscher; Bhupendra Nath Tiwari, and others.

DRAMATIS PERSONÆ

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

RIEMANN (1826–1866). Defined the spaces that bear his name. The study of these spaces led to the introduction of local Lie groups and Lie algebras.

LIE (1842–1899). Founded and developed the subject that bears his name with the original intention of finding a "Galois theory" for systems of differential equations.

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

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

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

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

WEYL (1885–1955). He was a pioneer in the application of Lie groups to physics. He proved that the finite-dimensional representations of semisimple Lie algebras and semisimple Lie groups are semisimple (completely reducible).

NOETHER (1882–1935).
HASSE (1898–1979).
BRAUER (1901–1977).
ALBERT (1905–1972).
They found a classification of semisimple algebras over number fields, which leads to a classification of the classical algebraic groups over the same fields.

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

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

WEIL (1906–1998). Foundational work on algebraic groups over arbitrary fields. Classified the classical algebraic groups over arbitrary fields in terms of semisimple algebras with involution (thereby winning the all India cocycling championship for 1960). Introduced adéles into the study of arithmetic problems on algebraic groups.

CHEVALLEY (1909–1984). He proved the existence of the simple Lie algebras and of their representations without using a case-by-case argument. Was the leading pioneer in the development of the theory algebraic groups over arbitrary fields. Classified the split semisimple algebraic groups over any field, and in the process found new classes of finite simple groups.

JACOBSON (1910–1999). Proved that most of the classical results on Lie algebras remain true over any field of characteristic zero (at least for split algebras).

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

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

HARISH-CHANDRA (1923–1983). Independently of Chevalley, he showed the existence of the simple Lie algebras and of their representations without using a case-by-case argument. With Borel he proved some basic results on arithmetic groups. Was one of the founders of the theory of infinite-dimensional representations of Lie groups.

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

SATAKE (1927–). He classified reductive algebraic groups over perfect fields (independently of Tits).

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

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

CHAPTER **I**

Lie Algebras

The Lie algebra of an algebraic group or Lie group is the first linear approximation of the group. The study of Lie algebras is much more elementary than that of the groups, and so we begin with it. Beyond the basic results of Engel, Lie, and Cartan on nilpotent and solvable Lie algebras, the main theorems in this chapter attach a root system to each split semisimple Lie algebra and explain how to deduce the structure of the Lie algebra (for example, its Lie subalgebras) and its representations from the root system.

The first nine sections are almost complete except that a few proofs are omitted (references are given). The remaining sections are not yet written. They will extend the theory to nonsplit Lie algebras. Specifically, they will cover the following topics.

- ◇ Classification of Lie algebras over $\mathbb{R}$ their representations in terms of "enhanced" Dynkin diagrams; Cartan involutions.
- ◇ Classification of forms of a (split) Lie algebra by Galois cohomology groups.
- ◇ Description of all classical Lie algebras in terms of semisimple algebras with involution.
- ◇ Relative root systems, and the classification of Lie algebras and their representations in terms relative root systems and the anisotropic kernel.

In this chapter, we follow Bourbaki's terminology and exposition quite closely, extracting what we need for the remaining two chapters.

Throughout this chapter k is a field.

1 Definitions and basic properties

Basic definitions

DEFINITION 1.1 A ***Lie algebra*** over a field k is a vector space $\mathfrak{g}$ over k together with a k-bilinear map

$$[\ ,\ ]\colon \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$$

(called the ***bracket***) such that

(a) $[x,x]=0$ for all $x\in\mathfrak{g}$,
(b) $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ for all $x,y,z\in\mathfrak{g}$.

A ***homomorphism of Lie algebras*** is a k-linear map $\alpha\colon \mathfrak{g} \to \mathfrak{g}'$ such that

$$\alpha([x,y]) = [\alpha(x),\alpha(y)] \quad \text{for all } x,y \in \mathfrak{g}.$$

Condition (b) is called the ***Jacobi identity***. Note that (a) applied to $[x+y,x+y]$ shows that the Lie bracket is skew-symmetric,

$$[x,y] = -[y,x], \text{ for all } x,y \in \mathfrak{g}, \tag{2}$$

and that (2) allows us to rewrite the Jacobi identity as

$$[x,[y,z]] = [[x,y],z] + [y,[x,z]] \tag{3}$$

or

$$[[x,y],z] = [x,[y,z]] - [y,[x,z]] \tag{4}$$

A ***Lie subalgebra*** of a Lie algebra $\mathfrak{g}$ is a k-subspace $\mathfrak{s}$ such that $[x,y] \in \mathfrak{s}$ whenever $x,y \in \mathfrak{s}$ (i.e., such that[1] $[\mathfrak{s},\mathfrak{s}] \subset \mathfrak{s}$). With the bracket, it becomes a Lie algebra.

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.

An injective homomorphism is sometimes called an ***embedding***, and a surjective homomorphism is sometimes called a ***quotient map***.

We shall be mainly concerned with finite-dimensional Lie algebras. Suppose that $\mathfrak{g}$ has a basis $\{e_1,\ldots,e_n\}$, and write

$$[e_i,e_j] = \sum_{l=1}^{n} a_{ij}^l e_l, \quad a_{ij}^l \in k, \quad 1 \le i,j \le n. \tag{5}$$

The a_{ij}^l, $1 \le i,j,l \le n$, are called the ***structure constants*** of $\mathfrak{g}$ relative to the given basis. They determine the bracket on $\mathfrak{g}$.

DEFINITION 1.2 An ***ideal*** in a Lie algebra $\mathfrak{g}$ is a subspace $\mathfrak{a}$ such that $[x,a] \in \mathfrak{a}$ for all $x \in \mathfrak{g}$ and $a \in \mathfrak{a}$ (i.e., such that $[\mathfrak{g},\mathfrak{a}] \subset \mathfrak{a}$).

Notice that, because of the skew-symmetry of the bracket

$$[\mathfrak{g},\mathfrak{a}] \subset \mathfrak{a} \iff [\mathfrak{a},\mathfrak{g}] \subset \mathfrak{a} \iff [\mathfrak{g},\mathfrak{a}] \subset \mathfrak{a} \text{ and } [\mathfrak{a},\mathfrak{g}] \subset \mathfrak{a}$$

— all left (or right) ideals are two-sided ideals.

Examples

1.3 Up to isomorphism, the only noncommutative Lie algebra of dimension 2 is that with basis x,y and bracket determined by $[x,y] = x$ (exercise).

1.4 Let A be an associative k-algebra. The bracket

$$[a,b] = ab - ba \tag{6}$$

[1]We write $[\mathfrak{s},\mathfrak{t}]$ for the k-subspace of $\mathfrak{g}$ spanned by the brackets $[x,y]$ with $x \in \mathfrak{s}$ and $y \in \mathfrak{t}$.

is k-bilinear, and it makes A into a Lie algebra $[A]$ because $[a,a]$ is obviously 0 and the Jacobi identity can be proved by a direct calculation. In fact, on expanding out the left side of the Jacobi identity for a,b,c one obtains a sum of 12 terms, 6 with plus signs and 6 with minus signs; by symmetry, each permutation of a,b,c must occur exactly once with a plus sign and exactly once with a minus sign.

1.5 In the special case of (1.4) in which $A = M_n(k)$, we obtain the Lie algebra $\mathfrak{gl}_n$. Thus $\mathfrak{gl}_n$ consists of the $n \times n$ matrices A with entries in k endowed with the bracket

$$[A,B] = AB - BA.$$

Let E_{ij} be the matrix with 1 in the ijth position and 0 elsewhere. These matrices form a basis for $\mathfrak{gl}_n$, and

$$[E_{ij}, E_{i'j'}] = \begin{cases} E_{ij'} & \text{if } j = i' \\ -E_{i'j} & \text{if } i = j' \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

More generally, let V be a k-vector space. From $A = \mathrm{End}_{k\text{-linear}}(V)$ we obtain the Lie algebra $\mathfrak{gl}_V$ of endomorphisms of V with

$$[\alpha,\beta] = \alpha \circ \beta - \beta \circ \alpha.$$

1.6 Let A be an associative k-algebra such that $k = k1$ is contained the centre of A. An ***involution*** of A is a k-linear map $a \mapsto a^*: A \to A$ such that

$$(a+b)^* = a^* + b^*, \quad (ab)^* = b^* a^*, \quad a^{**} = a$$

for all $a,b \in A$. When $*$ is an involution of A,

$$[A,*] \stackrel{\text{def}}{=} \{a \in A \mid a + a^* = 0\}$$

is a Lie k-subalgebra of $[A]$, because it is a k-subspace and

$$[a,b]^* = (ab - ba)^* = b^*a^* - a^*b^* = ba - ab = -[b,a].$$

1.7 Let V be a finite-dimensional vector space over k, and let

$$\beta: V \times V \to k$$

be a nondegenerate k-bilinear form. Define $*: \mathrm{End}(V) \to \mathrm{End}(V)$ by

$$\beta(av, v') = \beta(v, a^* v'), \quad a \in \mathrm{End}(V),\ v, v' \in V.$$

Then $(a+b)^* = a^* + b^*$ and $(ab)^* = b^*a^*$. If β is symmetric or skew-symmetric, then $*$ is an involution, and $[\mathrm{End}(V), *]$ is the Lie algebra

$$\mathfrak{g} = \left\{x \in \mathfrak{gl}_V \mid \beta(xv, v') + \beta(v, xv') = 0 \text{ all } v, v' \in V\right\}.$$

1.8 The following are all Lie subalgebras of $\mathfrak{gl}_n$:

$$\begin{aligned}
\mathfrak{sl}_n &= \{A \in M_n(k) \mid \text{trace}(A) = 0\}, \\
\mathfrak{o}_n &= \{A \in M_n(k) \mid A \text{ is skew symmetric, i.e., } A + A^t = 0\}, \\
\mathfrak{sp}_n &= \left\{A \in M_n(k) \;\middle|\; \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right) A + A^t \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right) = 0\right\}, \\
\mathfrak{b}_n &= \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i > j\} \quad \text{(upper triangular matrices)}, \\
\mathfrak{n}_n &= \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\} \quad \text{(strictly upper triangular matrices)}, \\
\mathfrak{d}_n &= \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \neq j\} \quad \text{(diagonal matrices)}.
\end{aligned}$$

To see that $\mathfrak{sl}_n$ is a Lie subalgebra of $\mathfrak{gl}_n$, note that, for $n \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$,

$$\text{trace}(AB) = \sum\nolimits_{1 \leq i,j \leq n} a_{ij} b_{ji} = \text{trace}(BA). \tag{8}$$

Therefore $[A, B] = AB - BA$ has trace zero. Similarly, the endomorphisms with trace 0 of a finite-dimensional vector space V form a Lie subalgebra $\mathfrak{sl}_V$ of $\mathfrak{gl}_V$. Both $\mathfrak{o}_n$ and $\mathfrak{sp}_n$ are special cases of (1.7).

NOTATION 1.9 We write $\langle a, b, \ldots\rangle$ for $\text{Span}(a, b, \ldots)$, and we write $\langle a, b, \ldots | R\rangle$ for the Lie algebra with basis $a, b, \ldots$ and the bracket given by the rules R. For example, the Lie algebra in (1.3) can be written $\langle x, y \mid [x, y] = x\rangle$.

NOTES Although Lie algebras have been studied since the 1880s, the term "Lie algebra" was introduced by Weyl only in 1934. Previously people had spoken of "infinitesimal groups" or used even less precise terms. See Bourbaki LIE, Historical Note to Chapters 1–3, IV.

Derivations; the adjoint map

DEFINITION 1.10 Let A be a k-algebra (not necessarily associative). A ***derivation*** of A is a k-linear map $D: A \to A$ such that

$$D(ab) = D(a)b + a\,D(b) \quad \text{for all } a, b \in A. \tag{9}$$

The composite of two derivations need not be a derivation, but their bracket

$$[D, E] = D \circ E - E \circ D$$

is, and so the set of k-derivations $A \to A$ is a Lie subalgebra $\text{Der}_k(A)$ of $\mathfrak{gl}_A$. For example, if the product on A is trivial, then the condition (9) is vacuous, and so $\text{Der}_k(A) = \mathfrak{gl}_A$.

DEFINITION 1.11 Let $\mathfrak{g}$ be a Lie algebra. For a fixed x in $\mathfrak{g}$, the linear map

$$y \mapsto [x, y]: \mathfrak{g} \to \mathfrak{g}$$

is called the ***adjoint (linear) map*** of x, and is denoted $\text{ad}_{\mathfrak{g}}(x)$ or $\text{ad}(x)$ (we sometimes omit the parentheses) .

For each x, the map $\text{ad}_{\mathfrak{g}}(x)$ is a k-derivation of $\mathfrak{g}$ because (3) can be rewritten as

$$\text{ad}(x)[y, z] = [\text{ad}(x)y, z] + [y, \text{ad}(x)z].$$

Moreover, $\mathrm{ad}_{\mathfrak{g}}$ is a homomorphism of Lie algebras $\mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ because (4) can be rewritten as

$$\mathrm{ad}([x,y])z = \mathrm{ad}(x)(\mathrm{ad}(y)z) - \mathrm{ad}(y)(\mathrm{ad}(x)z).$$

The kernel of $\mathrm{ad}_{\mathfrak{g}}\colon \mathfrak{g} \to \mathrm{Der}_k(\mathfrak{g})$ is the ***centre*** of $\mathfrak{g}$,

$$z(\mathfrak{g}) = \{x \in \mathfrak{g} \mid [x,\mathfrak{g}] = 0\}.$$

The derivations of $\mathfrak{g}$ of the form $\mathrm{ad}\,x$ are said to be ***inner*** (by analogy with the inner automorphisms of a group).

An ideal in $\mathfrak{g}$ is a subspace stable under all inner derivations of $\mathfrak{g}$. A subspace stable under *all* derivations is called a ***characteristic ideal.*** For example, the centre $z(\mathfrak{g})$ of $\mathfrak{g}$ is a characteristic ideal of $\mathfrak{g}$. An ideal $\mathfrak{a}$ in $\mathfrak{g}$ is, in particular, a subalgebra of $\mathfrak{g}$; if $\mathfrak{a}$ is characteristic, then every ideal in $\mathfrak{a}$ is also an ideal in $\mathfrak{g}$.

The isomorphism theorems

When $\mathfrak{a}$ is an ideal in a Lie algebra $\mathfrak{g}$, the quotient vector space $\mathfrak{g}/\mathfrak{a}$ becomes a Lie algebra with the bracket

$$[x+\mathfrak{a}, y+\mathfrak{a}] = [x,y] + \mathfrak{a}.$$

The following statements are straightforward consequences of the similar statements for vector spaces.

1.12 (Existence of quotients). The kernel of a homomorphism $\mathfrak{g} \to \mathfrak{g}'$ of Lie algebras is an ideal, and every ideal $\mathfrak{a}$ is the kernel of a quotient map $\mathfrak{g} \to \mathfrak{q}$.

1.13 (Homomorphism theorem). The image of a homomorphism $\alpha\colon \mathfrak{g} \to \mathfrak{g}'$ of Lie algebras is a Lie subalgebra $\alpha\mathfrak{g}$ of $\mathfrak{g}'$, and α defines an isomorphism of $\mathfrak{g}/\mathrm{Ker}(\alpha)$ onto $\alpha\mathfrak{g}$; in particular, every homomorphism of Lie algebras is the composite of a surjective homomorphism with an injective homomorphism.

1.14 (Isomorphism theorem). Let $\mathfrak{h}$ and $\mathfrak{a}$ be Lie subalgebras of $\mathfrak{g}$. If $[\mathfrak{h},\mathfrak{a}] \subset \mathfrak{a}$, then $\mathfrak{h}+\mathfrak{a}$ is a Lie subalgebra of $\mathfrak{g}$, $\mathfrak{h} \cap \mathfrak{a}$ is an ideal in $\mathfrak{h}$, and the map

$$x + \mathfrak{h}\cap\mathfrak{a} \mapsto x + \mathfrak{a}\colon \mathfrak{h}/\mathfrak{h}\cap\mathfrak{a} \to (\mathfrak{h}+\mathfrak{a})/\mathfrak{a}$$

is an isomorphism.

1.15 (Correspondence theorem). Let $\mathfrak{a}$ be an ideal in a Lie algebra $\mathfrak{g}$. The map $\mathfrak{h} \mapsto \mathfrak{h}/\mathfrak{a}$ is a bijection from the set of Lie subalgebras of $\mathfrak{g}$ containing $\mathfrak{a}$ to the set of Lie subalgebras of $\mathfrak{g}/\mathfrak{a}$. A Lie subalgebra $\mathfrak{h}$ containing $\mathfrak{a}$ is an ideal if and only if $\mathfrak{h}/\mathfrak{a}$ is an ideal in $\mathfrak{g}/\mathfrak{a}$, in which case the map

$$\mathfrak{g}/\mathfrak{h} \to (\mathfrak{g}/\mathfrak{a})/(\mathfrak{h}/\mathfrak{a})$$

is an isomorphism.

Normalizers and centralizers

For a subalgebra $\mathfrak{h}$ of $\mathfrak{g}$, the ***normalizer*** and ***centralizer*** of $\mathfrak{h}$ in $\mathfrak{g}$ are

$$n_{\mathfrak{g}}(\mathfrak{h}) = \{x \in \mathfrak{g} \mid [x,\mathfrak{h}] \subset \mathfrak{h}\}$$
$$c_{\mathfrak{g}}(\mathfrak{h}) = \{x \in \mathfrak{g} \mid [x,\mathfrak{h}] = 0\}.$$

These are both subalgebras of $\mathfrak{g}$, and $n_{\mathfrak{g}}(\mathfrak{h})$ is the largest subalgebra containing $\mathfrak{h}$ as an ideal. When $\mathfrak{h}$ is commutative, $c_{\mathfrak{g}}(\mathfrak{h})$ is the largest subalgebra of $\mathfrak{g}$ containing $\mathfrak{h}$ in its centre.

Extensions; semidirect products

An exact sequence of Lie algebras

$$0 \to \mathfrak{a} \to \mathfrak{g} \to \mathfrak{b} \to 0$$

is called an ***extension*** of $\mathfrak{b}$ by $\mathfrak{a}$. The extension is said to be ***central*** if $\mathfrak{a}$ is contained in the centre of $\mathfrak{g}$, i.e., if $[\mathfrak{g},\mathfrak{a}] = 0$.

Let $\mathfrak{a}$ be an ideal in a Lie algebra $\mathfrak{g}$. Each element g of $\mathfrak{g}$ defines a derivation $a \mapsto [g,a]$ of $\mathfrak{a}$, and this defines a homomorphism

$$\phi\colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{a}), \quad g \mapsto \mathrm{ad}(g)|\mathfrak{a}.$$

If there exists a Lie subalgebra $\mathfrak{q}$ of $\mathfrak{g}$ such that $\mathfrak{g} \to \mathfrak{g}/\mathfrak{a}$ maps $\mathfrak{q}$ isomorphically onto $\mathfrak{g}/\mathfrak{a}$, then I claim that we can reconstruct $\mathfrak{g}$ from $\mathfrak{a}$, $\mathfrak{q}$, and $\phi|\mathfrak{q}$. Indeed, each element g of $\mathfrak{g}$ can be written uniquely in the form

$$g = a + q, \quad a \in \mathfrak{a}, \quad q \in \mathfrak{q};$$

— here q must be the unique element of Q mapping to $g + \mathfrak{a}$ in $\mathfrak{g}/\mathfrak{a}$ and a must be $g - q$. Thus we have a one-to-one correspondence of sets

$$\mathfrak{g} \overset{\text{1-1}}{\longleftrightarrow} \mathfrak{a} \times \mathfrak{q},$$

which is, in fact, an isomorphism of k-vector spaces. If $g = a + q$ and $g' = a' + q'$, then

$$\begin{aligned}[g,g'] &= [a+q, a'+q'] \\ &= [a,a'] + [a,q'] + [q,a'] + [q,q'] \\ &= \left([a,a'] + \phi_q a' - \phi_{q'} a\right) + [q,q'],\end{aligned}$$

which proves the claim.

DEFINITION 1.16 A Lie algebra $\mathfrak{g}$ is a ***semidirect product*** of subalgebras $\mathfrak{a}$ and $\mathfrak{q}$, denoted $\mathfrak{g} = \mathfrak{a} \rtimes \mathfrak{q}$, if $\mathfrak{a}$ is an ideal in $\mathfrak{g}$ and the quotient map $\mathfrak{g} \to \mathfrak{g}/\mathfrak{a}$ induces an isomorphism $\mathfrak{q} \to \mathfrak{g}/\mathfrak{a}$.

We have seen that, from a semidirect product $\mathfrak{g} = \mathfrak{a} \rtimes \mathfrak{q}$, we obtain a triple

$$(\mathfrak{a}, \mathfrak{q}, \phi\colon \mathfrak{q} \to \mathrm{Der}_k(\mathfrak{a})),$$

and that the triple determines $\mathfrak{g}$. We now show that every triple $(\mathfrak{a},\mathfrak{q},\phi)$ consisting of two Lie algebras $\mathfrak{a}$ and $\mathfrak{q}$ and a homomorphism $\phi\colon \mathfrak{q} \to \mathrm{Der}_k(\mathfrak{a})$ arises from a semidirect product. As a k-vector space, we let $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{q}$, and we define

$$[(a,q),(a',q')] = \left([a,a'] + \phi_q a' - \phi_{q'} a, [q,q']\right). \tag{10}$$

PROPOSITION 1.17 *The bracket (10) makes $\mathfrak{g}$ into a Lie algebra.*

PROOF. Routine verification. □

We denote $\mathfrak{g}$ by $\mathfrak{a} \rtimes_\phi \mathfrak{q}$. The extension

$$0 \to \mathfrak{a} \to \mathfrak{a} \rtimes_\phi \mathfrak{q} \to \mathfrak{q} \to 0$$

is central if and only if $\mathfrak{a}$ is commutative and ϕ is the zero map.

Examples

1.18 Let D be a derivation of a Lie algebra $\mathfrak{a}$. Let $\mathfrak{q}$ be the one-dimensional Lie algebra k, and let

$$\mathfrak{g} = \mathfrak{a} \rtimes_\phi \mathfrak{q},$$

where ϕ is the map $c \mapsto cD\colon \mathfrak{q} \to \mathrm{Der}_k(\mathfrak{a})$. For the element $x = (0,1)$ of $\mathfrak{g}$, $\mathrm{ad}_\mathfrak{g}(x)|\mathfrak{a} = D$, and so the derivation D of $\mathfrak{a}$ has become an inner derivation in $\mathfrak{g}$.

1.19 Let V be a finite-dimensional k-vector space. When we regard V as a commutative Lie algebra, $\mathrm{Der}_k(V) = \mathfrak{gl}_V$. Let ϕ be the identity map $\mathfrak{gl}_V \to \mathrm{Der}_k(V)$. Then $V \rtimes_\phi \mathfrak{gl}_V$ is a Lie algebra, denoted $\mathfrak{af}(V)$.[2] An element of $\mathfrak{af}(V)$ is a pair (v,x) with $v \in V$ and $u \in \mathfrak{gl}_V$, and the bracket is

$$[(v,u),(v',u')] = (u(v') - u'(v), [u,u']).$$

Let $\mathfrak{h}$ be a Lie algebra, and let $\theta\colon \mathfrak{h} \to \mathfrak{af}(V)$ be a k-linear map. We can write $\theta = (\zeta,\eta)$ with $\zeta\colon \mathfrak{h} \to V$ and $\eta\colon \mathfrak{h} \to \mathfrak{gl}_V$ linear maps, and θ is a homomorphism of Lie algebras if and only if η is a homomorphism of Lie algebras and

$$\zeta([x,y]) = \eta(x)\cdot\zeta(y) - \eta(y)\cdot\zeta(x) \tag{11}$$

for all $x,y \in \mathfrak{h}$ (we have written $a \cdot v$ for $a(v)$, $a \in \mathfrak{gl}_V$, $v \in V$).

Let $V' = V \oplus k$, and let

$$\mathfrak{h} = \{w \in \mathfrak{gl}_{V'} \mid w(V') \subset V\}.$$

Then $\mathfrak{h}$ is a Lie subalgebra of $\mathfrak{gl}_{V'}$. Define

$$\eta\colon \mathfrak{h} \to \mathfrak{gl}_V, \quad \eta(w) = w|V,$$
$$\zeta\colon \mathfrak{h} \to V, \quad \zeta(w) = w(0,1).$$

Then η is a homomorphism of Lie algebras, and (ζ,η) satisfies (11), and so

$$\theta\colon \mathfrak{h} \to \mathfrak{af}(V), \quad w \mapsto (\zeta(w),\eta(w))$$

is a homomorphism of Lie algebras. The map θ is bijective, and its inverse sends $(v,u) \in \mathfrak{af}(V)$ to the element

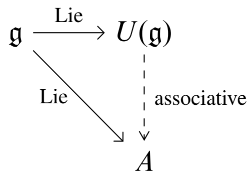
$$(v',c) \mapsto (u(v') + cv, 0)$$

of $\mathfrak{h}$. See Bourbaki LIE, I, §1, 8, Ex. 2.

[2] It is the Lie algebra of the group of affine transformations of V — see Chapter II.

The universal enveloping algebra

Recall (1.4) that an associative k-algebra A becomes a Lie algebra $[A]$ with the bracket $[a,b] = ab - ba$. Let $\mathfrak{g}$ be a Lie algebra. Among the pairs consisting of an associative k-algebra A and a Lie algebra homomorphism $\mathfrak{g} \to [A]$, there is one, $\rho\colon \mathfrak{g} \to [U(\mathfrak{g})]$, that is universal:



$$\begin{cases} \mathrm{Hom}(\mathfrak{g},[A]) & \simeq & \mathrm{Hom}(U(\mathfrak{g}),A). \\ \alpha\circ\rho & \leftrightarrow & \alpha \end{cases}$$

In other words, every Lie algebra homomorphism $\mathfrak{g} \to [A]$ extends uniquely to a homomorphism of associative algebras $A \to U(\mathfrak{g})$. The pair $(U(\mathfrak{g}),\rho)$ is called the ***universal enveloping algebra*** of $\mathfrak{g}$.

The algebra $U(\mathfrak{g})$ can be constructed as follows. Recall that the tensor algebra $T(V)$ of a k-vector space V is

$$T(V) = k \oplus V \oplus (V\otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$$

with the k-algebra structure

$$(x_1 \otimes \cdots \otimes x_r)\cdot(y_1 \otimes \cdots \otimes y_s) = x_1 \otimes \cdots \otimes x_r \otimes y_1 \otimes \cdots \otimes y_s.$$

It has the property that every k-linear map $V \to A$ with A an associative k-algebra extends uniquely to a k-algebra homomorphism $T(V) \to A$. We define $U(\mathfrak{g})$ to be the quotient of $T(\mathfrak{g})$ by the two-sided ideal generated by the tensors

$$x\otimes y - y \otimes x - [x,y], \quad x,y \in \mathfrak{g}. \tag{12}$$

Every k-linear map $\alpha\colon \mathfrak{g} \to A$ with A an associative k-algebra extends uniquely to k-algebra homomorphism $T(\mathfrak{g}) \to A$, which factors through $U(\mathfrak{g})$ if and only if α is a Lie algebra homomorphism $\mathfrak{g} \to [A]$.

If $\mathfrak{g}$ is commutative, then (12) is just the relation $x\otimes y = y \otimes x$, and so $U(\mathfrak{g})$ is the symmetric algebra on $\mathfrak{g}$.

Assume that $\mathfrak{g}$ is finite-dimensional, and let $(a_{ij}^l)_{1\le i,j,l\le n}$ be the family of structure constants of $\mathfrak{g}$ relative to a basis $\{e_1,\ldots,e_n\}$ (see (5)); let ε_i be the image of e_i in $U(\mathfrak{g})$; then $U(\mathfrak{g})$ is the associative k-algebra with generators $\varepsilon_1,\ldots,\varepsilon_n$ and relations

$$\varepsilon_i\varepsilon_j - \varepsilon_j\varepsilon_i = \sum_{l=1}^{n} a_{ij}^l \varepsilon_l. \tag{13}$$

We study the structure of $U(\mathfrak{g})$ later in this section (Theorems 1.30, 1.31).

Representations

A ***representation*** of a Lie algebra $\mathfrak{g}$ on a k-vector space V is a homomorphism $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$. Thus ρ sends $x \in \mathfrak{g}$ to a k-linear endomorphism $\rho(x)$ of V, and

$$\rho([x,y]) = \rho(x)\rho(y) - \rho(y)\rho(x).$$

We often call V a $\mathfrak{g}$-***module*** and write xv or $x_V v$ for $\rho(x)(v)$. With this notation

$$[x,y]v = x(yv) - y(xv). \tag{14}$$

A representation ρ is said to be ***faithful*** if it is injective. The representation

$$x \mapsto \operatorname{ad} x \colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$$

is called the ***adjoint representation*** of $\mathfrak{g}$ (see 1.11).

Let W be a subspace of V. The ***stabilizer*** of W in $\mathfrak{g}$ is

$$\mathfrak{g}_W \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xW \subset W\}.$$

It is clear from (14) that $\mathfrak{g}_W$ is a Lie subalgebra of $\mathfrak{g}$.

Let $v \in V$. The ***isotropy algebra*** of v in $\mathfrak{g}$ is

$$\mathfrak{g}_v \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xv = 0\}.$$

It is a Lie subalgebra of $\mathfrak{g}$. An element v of V is said to be ***fixed*** by $\mathfrak{g}$, or ***invariant*** under $\mathfrak{g}$, if $\mathfrak{g} = \mathfrak{g}_v$, i.e., if $\mathfrak{g}v = 0$.

Let $\mathfrak{g}$ be a Lie algebra over a field k. The representations of $\mathfrak{g}$ on finite-dimensional k-vector spaces form an abelian category, which we denote $\mathsf{Rep}(\mathfrak{g})$.

Every homomorphism $\mathfrak{g} \to \mathfrak{gl}_V$ of Lie algebras extends uniquely to a homomorphism $U(\mathfrak{g}) \to \operatorname{End}_{k\text{-linear}}(V)$ of associative algebras. It follows that the functor sending a representation $\rho \colon U(\mathfrak{g}) \to \operatorname{End}_{k\text{-linear}}(V)$ of $U(\mathfrak{g})$ to $\rho|\mathfrak{g}$ is an isomorphism(!) of categories

$$\mathsf{Rep}(U(\mathfrak{g})) \to \mathsf{Rep}(\mathfrak{g}).$$

1.20 Let V and W be finite-dimensional $\mathfrak{g}$-modules.

(a) There is a unique $\mathfrak{g}$-module structure on $V \otimes W$ such that

$$x(v \otimes w) = x_V v \otimes w + v \otimes x_W w, \quad x \in \mathfrak{g},\ v \in V,\ w \in W.$$

(b) The following formula defines a $\mathfrak{g}$-module structure on $\operatorname{Hom}(V,W)$:

$$xf = x_W f - f x_V, \quad x \in \mathfrak{g},\ f \in \operatorname{Hom}(V,W),$$

i.e.,

$$(xf)(v) = x \cdot f(v) - f(x \cdot v), \quad \text{for } v \in V.$$

In particular, $V^\vee$ has natural $\mathfrak{g}$-module structure:

$$(xf)(v) = f(v) - f(x \cdot v), \quad v \in V.$$

These statements can be proved directly, or they can be deduced from similar statements for the enveloping algebras. For example, $\operatorname{Hom}(V,W)$ is a $U(\mathfrak{g})^{\text{opp}} \otimes U(\mathfrak{g})$-module, and the map

$$x \mapsto -x \otimes 1 + 1 \otimes x \colon \mathfrak{g} \to U(\mathfrak{g})^{\text{opp}} \otimes U(\mathfrak{g})$$

preserves the bracket, and so $\operatorname{Hom}(V,W)$ acquires a $\mathfrak{g}$-module structure, which is that in (b).

We sometimes write $\rho_V \otimes \rho_W$ for the representation in (a) and $\underline{\operatorname{Hom}}(\rho_V, \rho_W)$ for that in (b).

See Bourbaki LIE, I, §3, for much more on such things.

Jordan decompositions

1.21 Let α be an endomorphism of a finite-dimensional k-vector space. For an eigenvalue a of α, the ***primary space*** V^a is

$$\{v \in V \mid (\alpha - a)^m v = 0 \text{ some } m \geq 1\}.$$

If α has all of its eigenvalues in k, i.e., if its characteristic polynomial splits in $k[X]$,[3] then $V = \bigoplus_{a \in I} V^a$, where I is the set of eigenvalues of α (see AGS, X, 2.1).

PROPOSITION 1.22 *Let V be a finite-dimensional vector space over a perfect field. For any endomorphism α of V, there exist unique endomorphisms α_s and α_n of V such that*

(a) $\alpha = \alpha_s + \alpha_n$,
(b) $\alpha_s \circ \alpha_n = \alpha_n \circ \alpha_s$, *and*
(c) α_s *is semisimple and* α_n *is nilpotent.*

Moreover, each of α_s and α_n is a polynomial in α.

PROOF. Assume first that α has all of its eigenvalues in k, so that V is a direct sum of the primary spaces, say, $V = \bigoplus_{a \in I} V^a$. Define α_s to be the endomorphism of V that acts as a on V^a for each $a \in I$. Then α_s is a semisimple endomorphism of V, and $\alpha_n \overset{\text{def}}{=} \alpha - \alpha_s$ commutes with α_s (because it does on each V^a) and is nilpotent (because it is so on each V^a). Thus α_s and α_n satisfy the conditions (a,b,c).

Let n_a denote the multiplicity of the eigenvalue a. Because the polynomials $(T-a)^{n_a}$, $a \in I$, are relatively prime, the Chinese remainder theorem shows that there exists a $Q(T) \in k[T]$ such that

$$Q(T) \equiv a \bmod (T-a)^{n_a}$$

for all $a \in I$. Then $Q(\alpha)$ acts as a on V_a for each i, and so $\alpha_s = Q(\alpha)$. Moreover, $\alpha_n = \alpha - Q(\alpha)$.

In the general case, because k is perfect, there exists a finite Galois extension k' of k such that α has all of its eigenvalues in k'. Choose a basis for V, and use it to attach matrices to endomorphisms of V and $k' \otimes_k V$. Let A be the matrix of α. The first part of the proof allows us to write A as the sum $A = A_s + A_n$ of a semisimple matrix A_s and commuting nilpotent matrix A_n with entries in k'; moreover, this decomposition is unique.

Let $\sigma \in \mathrm{Gal}(k'/k)$, and for a matrix $B = (b_{ij})$, define σB to be (σb_{ij}). Because A has entries in k, $\sigma A = A$. Now

$$A = \sigma A_s + \sigma A_n$$

is again a decomposition of A into commuting semisimple and nilpotent matrices. By the uniqueness of the decomposition, $\sigma A_s = A_s$ and $\sigma A_n = A_n$. Since this is true for all $\sigma \in \mathrm{Gal}(k'/k)$, the matrices A_s and A_n have entries in k. Now $\alpha = \alpha_s + \alpha_n$, where α_s and α_n are the endomorphisms with matrices A_s and A_n, is a decomposition of α satisfying (a) and (b).

Finally, the first part of the proof shows that there exist $a_i \in k'$ such that

$$A_s = a_0 + a_1 A + \cdots + a_{n-1} A^{n-1} \qquad (n = \dim V).$$

[3] Or, as Bourbaki likes to put it, α is trigonalizable over k.

The a_i are unique, and so, on applying σ, we find that they lie in k. Therefore,

$$\alpha_s = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in k[\alpha].$$

Similarly, $\alpha_u \in k[\alpha]$. □

REMARK 1.23 (a) If 0 is an eigenvalue of α, then the polynomial $Q(T)$ has no constant term. Otherwise, we can choose it to satisfy the additional congruence

$$Q(T) \equiv 0 \bmod T$$

in order to achieve the same result. Similarly, we can express α_n as a polynomial in α without constant term.

(b) Suppose $k = \mathbb{C}$, and let $\overline{a}$ denote the complex conjugate of a. There exists a $Q(T) \in \mathbb{C}[T]$ such that

$$Q(T) \equiv \overline{a} \bmod (T-a)^{n_a}$$

for all $a \in I$. Then $Q(\alpha)$ is an endomorphism of V that acts on V_a as $\overline{a}$. Again, we can choose $Q(T)$ to have no constant term.

A pair (α_s, α_n) of endomorphisms satisfying the conditions (a,b,c) of (1.22) is called an ***(additive) Jordan decomposition*** of α. The endomorphisms α_s and α_n are called the ***semisimple*** and ***nilpotent parts*** of α.

PROPOSITION 1.24 *Let α be an endomorphism of a finite-dimensional vector space V over a perfect field, and let $\alpha = \alpha_s + \alpha_n$ be its Jordan decomposition. The Jordan decomposition of*

$$\mathrm{ad}(\alpha)\colon \mathrm{End}(V) \to \mathrm{End}(V), \quad \beta \mapsto [\alpha,\beta] = \alpha\beta - \beta\alpha,$$

is

$$\mathrm{ad}(\alpha) = \mathrm{ad}(\alpha_s) + \mathrm{ad}(\alpha_n).$$

In particular, $\mathrm{ad}(\alpha)$ *is semisimple (resp. nilpotent) if α is.*

PROOF. Suppose first that α is semisimple. After a field extension, there exists a basis $(e_i)_{1\le i\le n}$ of V for which the matrix of α is diagonal, say, equal to $\mathrm{diag}(a_1,\ldots,a_n)$. If $(e_{ij})_{1\le i,j\le n}$ is the corresponding basis for $\mathrm{End}(V)$, then $\mathrm{ad}(\alpha)e_{ij} = (a_i - a_j)e_{ij}$ for all i,j. Therefore $\mathrm{ad}(\alpha)$ is semisimple.

Next suppose that α is nilpotent. Let $\beta \in \mathrm{End}(V)$. Then

$$\begin{aligned}
[\alpha,\beta] &= \alpha\circ\beta - \beta\circ\alpha \\
[\alpha,[\alpha,\beta]] &= \alpha^2\circ\beta - 2\alpha\circ\beta\circ\alpha + \beta\circ\alpha^2 \\
[\alpha,[\alpha,[\alpha,\beta]]] &= \alpha^3\circ\beta - 3\alpha^2\circ\beta\circ\alpha + 3\alpha\circ\beta\circ\alpha^2 - \beta\circ\alpha^3 \\
&\cdots.
\end{aligned}$$

In general, $(\mathrm{ad}\alpha)^m(\beta)$ is a sum of terms $\pm\alpha^j\circ\beta\circ\alpha^{m-j}$ with $0\le j\le m$. Therefore, if $\alpha^n = 0$, then $(\mathrm{ad}\alpha)^{2n} = 0$.

For a general α, the Jordan decomposition $\alpha = \alpha_s + \alpha_n$ gives a decomposition $\mathrm{ad}(\alpha) = \mathrm{ad}(\alpha_s) + \mathrm{ad}(\alpha_n)$. We have shown that $\mathrm{ad}(\alpha_s)$ is semisimple and that $\mathrm{ad}(\alpha_n)$ is nilpotent; the two commute because

$$[\mathrm{ad}(\alpha_s),\mathrm{ad}(\alpha_n)] = \mathrm{ad}([\alpha_s,\alpha_n]) = 0.$$

Therefore $\mathrm{ad}(\alpha) = \mathrm{ad}(\alpha_s) + \mathrm{ad}(\alpha_n)$ is a Jordan decomposition. □

1.25 Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}_V$. If $\alpha \in \mathfrak{g}$, it need not be true that α_s and α_n lie in $\mathfrak{g}$. For example, the following rules define a five-dimensional (solvable) Lie algebra $\mathfrak{g} = \bigoplus_{1 \le i \le 5} k x_i$:

$$[x_1, x_2] = x_5, [x_1, x_3] = x_3, [x_2, x_4] = x_4, [x_1, x_4] = [x_2, x_3] = [x_3, x_4] = [x_5, \mathfrak{g}] = 0$$

(Bourbaki LIE, I, §5, Exercise 6). For every injective homomorphism $\mathfrak{g} \hookrightarrow \mathfrak{gl}_V$, there exists an element of $\mathfrak{g}$ whose semisimple and nilpotent components (as an endomorphism of V) do not lie in $\mathfrak{g}$ (ibid., VII, §5, Exercise 1).

Extension of the base field

Let k' be a field containing k. If $\mathfrak{g}$ is a Lie algebra over k, then $\mathfrak{g}_{k'} \overset{\text{def}}{=} k' \otimes \mathfrak{g}$ becomes a Lie algebra over k' with the obvious bracket. Since much of the theory of Lie algebras is linear, most things extend in an obvious way under $k \to k'$. For example, if $\mathfrak{a}$ is a Lie subalgebra of $\mathfrak{g}$, then $\mathfrak{a}_{k'}$ is a Lie subalgebra of $\mathfrak{g}_{k'}$, and

$$n_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = n_{\mathfrak{g}}(\mathfrak{a})_{k'} \tag{15}$$
$$c_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = c_{\mathfrak{g}}(\mathfrak{a})_{k'}. \tag{16}$$

Moreover, when $\mathfrak{g}$ is finite-dimensional,

$$U(\mathfrak{g}_{k'}) \simeq U(\mathfrak{g})_{k'}. \tag{17}$$

The filtration on the universal enveloping algebra

Let $\mathfrak{g}$ be a Lie algebra over k. The universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$ is not graded (the tensor (12) is not homogeneous), but it is filtered.

Let T^n be the k-subspace of $T(\mathfrak{g})$ of homogeneous tensors of degree n, and let $T_n = \sum_{i \le n} T^i$. The T_n's make $T(\mathfrak{g})$ into a filtered k-algebra:

$$T_n T_m \subset T_{n+m} \quad \text{all } n, m \in \mathbb{N},$$

and

$$T(\mathfrak{g}) = \bigcup T_n \supset \cdots \supset T_{n+1} \supset T_n \supset \cdots \supset T_0 \supset T_{-1} = \{0\}.$$

Let U_n be the image of T_n in $U(\mathfrak{g})$. Then the U_n's make $U(\mathfrak{g})$ into a filtered k-algebra.

Let G be the graded algebra defined by the filtration $(U_n)_{n \ge -1}$ on $U(\mathfrak{g})$. Thus,

$$G = \bigoplus_n G^n, \quad G^n = U_n / U_{n-1}$$

with the obvious product structure, namely, for $u_n + U_{n-1} \in G^n$ and $u'_m + U_{m-1} \in G^m$,

$$(u_n + U_{n-1})(u'_m + U_{m-1}) = u_n u'_m + U_{n+m-1}.$$

For each n, we have a canonical map ϕ_n

$$T^n \to U_n \twoheadrightarrow U_n / U_{n-1} \overset{\text{def}}{=} G^n,$$

and hence k-linear map $\phi \colon T(\mathfrak{g}) = \bigoplus_n T^n \xrightarrow{\oplus \phi_n} \bigoplus_n G^n = G$.

PROPOSITION 1.26 *The map ϕ is a surjective homomorphism of k-algebras, and it is zero on the two-sided ideal generated by the elements $x \otimes y - y \otimes x$, $x, y \in \mathfrak{g}$.*

PROOF. Each map ϕ_n is surjective, and so ϕ is surjective. That $\phi(tt') = \phi(t)\phi(t')$ for $t \in T_n, t' \in T_m$, follows from the definition of the product in G. The image of $x \otimes y - y \otimes x$ in $U_2 \subset U(\mathfrak{g})$ is equal to that of $[x, y]$, which lies in $U_1 \subset U_2$. Therefore the image of $x \otimes y - y \otimes x$ in $U_2/U_1 \stackrel{\text{def}}{=} G^1$ is zero. □

By definition, the symmetric algebra of $\mathfrak{g}$ (as a k-vector space) is the quotient of $T(\mathfrak{g})$ by the two-sided ideal generated by the elements $x \otimes y - y \otimes x$, $x, y \in \mathfrak{g}$. The proposition shows that ϕ defines a surjective homomorphism

$$\omega: S(\mathfrak{g}) \to G. \tag{18}$$

PROPOSITION 1.27 *If $\mathfrak{g}$ is finite-dimensional, then the k-algebra $U(\mathfrak{g})$ is left and right noetherian.*

PROOF. The symmetric algebra of a vector space of dimension r is a polynomial algebra in r symbols, and so it is noetherian (Hilbert basis theorem). Quotients of noetherian rings are (obviously) noetherian, and so G is noetherian. The filtration $(U_n)_{n \geq -1}$ on $U(\mathfrak{g})$ is exhaustive, i.e., $U(\mathfrak{g}) = \bigcup_{n \geq -1} U_n$, and it defines discrete topology on $U(\mathfrak{g})$). We can now apply the following standard result. [Actually, it would be easy to write out a direct proof.]□

LEMMA 1.28 *Let A be a complete separated filtered ring whose filtration is exhaustive. If the associated graded ring of A is left noetherian, then so also is A.*

PROOF. Bourbaki AC, III, §2, 9, Cor. 2 to Proposition 12. □

COROLLARY 1.29 *Let $I_1, \ldots, I_m$ be left ideals in $U(\mathfrak{g})$. If each I_i is of finite codimension in $U(\mathfrak{g})$, then so also is $I_1 \cdots I_m$.*

PROOF. Since $I_1 \cdots I_m = I_1(I_2 \cdots I_m)$, it suffices to prove this for $m = 2$. Let $u_1, \ldots, u_m$ be elements of $U(\mathfrak{g})$ generating $U(\mathfrak{g})/I_1$ as a k-vector space, and let $v_1, \ldots, v_n$ be elements of I_2 generating I_2 as a left $U(\mathfrak{g})$-module. Then the elements $u_i v_j + I_1 I_2$ generate $I_1/I_1 I_2$ as a k-vector space. Now

$$\dim_k(U/I_1 I_2) = \dim_k(U/I_1) + \dim_k(I_1/I_1 I_2) < \infty.$$ □

The Poincaré-Birkhoff-Witt theorem

Throughout this subsection, $\mathfrak{g}$ is a finite-dimensional Lie algebra over a field k of characteristic zero.

THEOREM 1.30 (POINCARÉ, BIRKHOFF, WITT) *Let $\{e_1, \ldots, e_r\}$ be a basis for $\mathfrak{g}$ as a k-vector space, and let $\varepsilon_i = \rho(e_i)$. Then the set*

$$\{\varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_r^{m_r} \mid m_1, \ldots, m_r \in \mathbb{N}\} \tag{19}$$

is a basis for $U(\mathfrak{g})$ as a k-vector space.

For example, if $\mathfrak{g}$ is commutative, then $U(\mathfrak{g})$ is the polynomial algebra in the symbols $\varepsilon_1, \ldots, \varepsilon_r$.

As $U(\mathfrak{g})$ is generated as a k-algebra by $\varepsilon_1, \ldots, \varepsilon_r$, it is generated as a k-vector space by the elements $\varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_m}$, $1 \le i_j \le r$, $m \in \mathbb{N}$. The relations (13) allow one to "reorder" the factors in such a term, and deduce that the set (19) spans $U(\mathfrak{g})$; the import of the theorem is that the set is linearly independent. In particular, the set $\{\varepsilon_1, \ldots, \varepsilon_r\}$ is linearly independent.

For each family $M = (m_i)_{1 \le i \le r}$, $m_i \in \mathbb{N}$, let

$$\begin{aligned} |M| &= m_1 + \cdots + m_r \\ e^M &= e_1^{\otimes m_1} \otimes \cdots \otimes e_r^{m_r} \in T(\mathfrak{g}) \\ \varepsilon^M &= \varepsilon_1^{\otimes m_1} \otimes \cdots \otimes \varepsilon_r^{m_r} \in U(\mathfrak{g}). \end{aligned}$$

The theorem says that the elements ε^M form a basis for $U(\mathfrak{g})$ as a k-vector space.

We defer the proof of Theorem 1.30 to the end of the subsection.

THEOREM 1.31 *The homomorphism $\omega\colon S(\mathfrak{g}) \to G$ (see (18)) is an isomorphism of graded k-algebras.*

PROOF. The elements ε^M with $|M| \le n$ span U_n, and (1.30) shows that they form a basis for U_n. Therefore, the elements $\varepsilon^M + U_{n-1}$ with $|M| = n$ form a basis of G^n. Let s^M denote the image of ε^M in $S(\mathfrak{g})$. Then the elements s^M with $|M| = n$ form a basis for the k-vector space of homogeneous elements in $S(\mathfrak{g})$ of degree n. As ω maps s^N to ε^M, we see that it is an isomorphism. □

The following are all immediate consequences of Theorem 1.30.

1.32 *The map $\rho\colon \mathfrak{g} \to U(\mathfrak{g})$ is an isomorphism of $\mathfrak{g}$ onto its image.*

1.33 *For any Lie subalgebra $\mathfrak{g}'$ of $\mathfrak{g}$, the homomorphism $U(\mathfrak{g}') \to U(\mathfrak{g})$ is injective.*

1.34 *If $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ with $\mathfrak{g}_1$ and $\mathfrak{g}_2$ subalgebras of $\mathfrak{g}$, then $U(\mathfrak{g}) \simeq U(\mathfrak{g}_1) \otimes U(\mathfrak{g}_2)$ as k-vector spaces (not algebras).*

1.35 *The only invertible elements of $U(\mathfrak{g})$ are the nonzero scalars.*

1.36 *The algebra $U(\mathfrak{g})$ has no nonzero zero divisors.*

Proof of Theorem 1.30

The following is the key lemma.

LEMMA 1.37 *Let $\{e_1, \ldots, e_r\}$ be a basis for $\mathfrak{g}$ as a k-vector space, and let $\varepsilon_i = \rho(e_i)$. If $\rho\colon \mathfrak{g} \to U(\mathfrak{g})$ is injective, then the set $\{\varepsilon^M \mid M \in \mathbb{N}^r\}$ is a basis for $U(\mathfrak{g})$.*

PROOF. The following is copied verbatim from Sophus Lie Exposé 1 (Cartier).

We have to show that, if the ε_i are linearly independent, then so also are ε^M. As ρ is injective, we can use the same letter for an element of $\mathfrak{g}$ and its image in $U(\mathfrak{g})$.

The map

$$x \mapsto x \otimes 1 + 1 \otimes x : \mathfrak{g} \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$$

is a Lie algebra homomorphism, and so it extends to a homomorphism of associative k-algebras

$$H : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g}).$$

We have

$$H(x^m) = (x \otimes 1 + 1 \otimes x)^m = \sum\nolimits_{p+q=m} \binom{m}{p} x^p \otimes x^q$$

because $x \otimes 1$ and $1 \otimes x$ commute. Moreover, for $M \in \mathbb{N}^r$,

$$t^M = (\varepsilon^M) - 1 \otimes \varepsilon^M - \varepsilon^M \otimes 1 = \sum_{P+Q=M,\ P,Q \neq \emptyset} \binom{M}{P} \varepsilon^P \otimes \varepsilon^Q \tag{20}$$

where

$$\binom{M}{P} = \prod\nolimits_{i \in I} \binom{m_i}{p_i}.$$

The proof proceeds by induction on $|M|$. By hypothesis, the ε^N are linearly independent if $|N| = 1$; suppose that they are linearly independent for $|N| \leq m$ and $|M| \leq m+1$. Then the $y^{P,Q} \overset{\text{def}}{=} \varepsilon^P \otimes \varepsilon^Q$ occurring in the expression for t^M are linearly independent in $U_m \otimes U_m$. No t^M is zero if $m > 1$ (we are in characteristic 0!), and if $M \neq M'$ $(m > 1)$, then t^M and $t^{M'}$ do not involve the same $y^{P,Q}$ because t^M involves only $y^{P,Q}$ with $P + Q = M$ and $t^{M'}$ involves only $y^{P,Q}$ with $P + Q = M' \neq M$; they are therefore linearly independent.

Suppose that there exists a linear relation $\sum a_M \varepsilon^M = 0$ between the ε^M. We deduce that

$$\sum a_M t^M = \sum a_M H(\varepsilon^M) - 1 \otimes \sum a_M \varepsilon^M - \sum a_M \varepsilon^M \otimes 1,$$

which implies that $a_M = 0$ unless $|M| = 1$. But then $\varepsilon^M = \varepsilon_i$ for some i, and we are assuming that the ε_i are linearly independent. Therefore all the a_M are zero, and the ε^M are linearly independent. □

NOTES

1.38 Suppose that $\mathfrak{g}$ admits a faithful representation $\gamma : \mathfrak{g} \to \mathfrak{gl}_n = [M_n]$. Then $\gamma = a \circ \rho$ for some homomorphism $a : U(\mathfrak{g}) \to M_n$ of associative k-algebras. As γ is injective, so also as ρ. Therefore, Theorem 1.30 for $\mathfrak{g}$ follows from Lemma 1.37. As Ado's theorem (6.27 below), shows that every finite-dimensional Lie algebra admits a faithful representation, this completes the proof of Theorem 1.30. (Corollary 1.29 is used in the proof of Ado's theorem, specifically, in the proof of the Zassenhaus extension theorem (6.28), but nothing from this subsection.)

1.39 The Poincaré-Birkhoff-Witt theorem holds also for infinite-dimensional Lie algebras: for any totally ordered basis $(e_i)_{i \in I}$ for $\mathfrak{g}$, the elements ε^M, $M \in \mathbb{N}^{(I)}$, form a basis for $U(\mathfrak{g})$ as a k-vector space. Lemma 1.37 (and its proof) hold for infinite-dimensional Lie algebras, and so the infinite-dimensional theorem follows from the next two statements: if the PBW theorem holds for a Lie algebra $\mathfrak{g}$, then it holds for every quotient of $\mathfrak{g}$; if $\mathfrak{g}$ is a free Lie algebra, then the map $\rho : \mathfrak{g} \to U(\mathfrak{g})$ is injective. See Sophus Lie Exposé 1, Lemme 1, Lemme 3.

1.40 In the form (1.31), the PBW theorem holds for all Lie algebras $\mathfrak{g}$ over a commutative ring k such that $\mathfrak{g}$ is free as a k-module. See Bourbaki LIE, I, §2, 7.

1.41 For the proof of the PBW theorem, see Casselman, Introduction to Lie algebras, §15, and the discussion in mo87402.

Nilpotent, solvable, and semisimple Lie algebras

A Lie algebra is ***nilpotent*** if it can be obtained from commutative Lie algebras by successive central extensions, and it is ***solvable*** if it can be obtained from commutative Lie algebras by successive extensions, not necessarily central. For example, the Lie algebra $\mathfrak{n}_n$ of strictly upper triangular matrices is nilpotent, and the Lie algebra $\mathfrak{b}_n$ of upper triangular matrices is solvable. The Lie algebra

$$\langle x, y \mid [x,y] = x \rangle$$

is solvable but not nilpotent (the extension

$$0 \to \langle x \rangle \to \langle x, y \rangle \to \langle x, y \rangle / \langle x \rangle \to 0$$

is not central), and the Lie algebra

$$\langle x, y, z \mid [x,y] = z, [x,z] = [y,z] = 0 \rangle$$

is nilpotent, hence also solvable (the extension

$$0 \to \langle z \rangle \to \langle x, y, z \rangle \to \langle x, y, z \rangle / \langle z \rangle \to 0$$

is central and the quotient is commutative).

The centre of a nontrivial nilpotent Lie algebra is nontrivial. By contrast, a Lie algebra whose centre is trivial is said to be ***semisimple***. Such a Lie algebra is a product of simple Lie algebras. In the next three sections, we study nilpotent, solvable, and semisimple Lie algebras respectively.

2 Nilpotent Lie algebras: Engel's theorem

In this section, all Lie algebras and all representations are finite dimensional over a field k.

Generalities

DEFINITION 2.1 A Lie algebra $\mathfrak{g}$ is said to be ***nilpotent*** if it admits a filtration

$$\mathfrak{g} = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_r = 0 \tag{21}$$

by ideals such that $[\mathfrak{g}, \mathfrak{a}_i] \subset \mathfrak{a}_{i+1}$ for $0 \leq i \leq r-1$. Such a filtration is called a ***nilpotent series***.

The condition for (21) to be a nilpotent series is that $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ be in the centre of $\mathfrak{g}/\mathfrak{a}_{i+1}$ for $0 \leq i \leq r-1$. Thus the nilpotent Lie algebras are exactly those that can be obtained from commutative Lie algebras by successive *central* extensions

$$\begin{aligned} 0 &\to \mathfrak{a}_1/\mathfrak{a}_2 \to \mathfrak{g}/\mathfrak{a}_2 \to \mathfrak{g}/\mathfrak{a}_1 \to 0 \\ 0 &\to \mathfrak{a}_2/\mathfrak{a}_3 \to \mathfrak{g}/\mathfrak{a}_3 \to \mathfrak{g}/\mathfrak{a}_2 \to 0 \\ &\cdots \end{aligned}$$

In other words, the nilpotent Lie algebras form the smallest class containing the commutative Lie algebras and closed under *central* extensions.

The ***lower central series*** of $\mathfrak{g}$ is

$$\mathfrak{g} \supset \mathfrak{g}^1 \supset \mathfrak{g}^2 \supset \cdots \supset \mathfrak{g}^{i+1} \supset \cdots$$

with $\mathfrak{g}^1 = [\mathfrak{g},\mathfrak{g}]$, $\mathfrak{g}^2 = [\mathfrak{g},\mathfrak{g}^1]$, ..., $\mathfrak{g}^{i+1} = [\mathfrak{g},\mathfrak{g}^i]$,....

PROPOSITION 2.2 *A Lie algebra $\mathfrak{g}$ is nilpotent if and only if its lower central series terminates with zero.*

PROOF. If the lower central series terminates with zero, then it is a nilpotent series. Conversely, if $\mathfrak{g} \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_r = 0$ is a nilpotent series, then $\mathfrak{a}_1 \supset \mathfrak{g}^1$ because $\mathfrak{g}/\mathfrak{a}_1$ is commutative, $\mathfrak{a}_2 \supset [\mathfrak{g},\mathfrak{a}_1] \supset [\mathfrak{g},\mathfrak{g}^1] = \mathfrak{g}^2$, and so on, until we arrive at $0 = \mathfrak{a}_r \supset \mathfrak{g}^r$. □

Let V be a vector space of dimension n, and let

$$F\colon V = V_0 \supset V_1 \supset \cdots \supset V_n = 0, \quad \dim V_i = n - i,$$

be a maximal flag in V. Let $\mathfrak{n}(F)$ be the Lie subalgebra of $\mathfrak{gl}_V$ consisting of the elements x such that $x(V_i) \subset V_{i+1}$ for all i. The lower central series for $\mathfrak{n}(F)$ has

$$\mathfrak{n}(F)^j = \{x \in \mathfrak{gl}_V \mid x(V_i) \subset V_{i+1+j}\}$$

for $j = 1,\ldots,n$. In particular, $\mathfrak{n}(F)$ is nilpotent. For example,

$$\mathfrak{n}_3 = \left\{\begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\} \supset \{0\},$$

is a nilpotent series for $\mathfrak{n}_3$.

2.3 An extension of nilpotent algebras is solvable, but not necessarily nilpotent. For example, $\mathfrak{n}_3$ is nilpotent and $\mathfrak{b}_3/\mathfrak{n}_3$ is commutative, but $\mathfrak{b}_3$ is not nilpotent when $n \geq 3$.

PROPOSITION 2.4 *Let k' be a field containing k. A Lie algebra $\mathfrak{g}$ over k is nilpotent if and only if $\mathfrak{g}_{k'} \overset{\text{def}}{=} k' \otimes_k \mathfrak{g}$ is nilpotent.*

PROOF. Obviously, for any subalgebras $\mathfrak{h}$ and $\mathfrak{h}'$ of $\mathfrak{g}$, $[\mathfrak{h},\mathfrak{h}']_{k'} = [\mathfrak{h}_{k'},\mathfrak{h}'_{k'}]$, and so extension of the base field maps the lower central series of $\mathfrak{g}$ to that of $\mathfrak{g}_{k'}$. □

PROPOSITION 2.5 *(a) Subalgebras and quotient algebras of nilpotent Lie algebras are nilpotent.*

(b) A Lie algebra $\mathfrak{g}$ is nilpotent if $\mathfrak{g}/\mathfrak{a}$ is nilpotent for some ideal $\mathfrak{a}$ contained in $z(\mathfrak{g})$.

(c) A nonzero nilpotent Lie algebra has nonzero centre.

PROOF. (a) The intersection of a nilpotent series for $\mathfrak{g}$ with a Lie subalgebra $\mathfrak{h}$ is a nilpotent series for $\mathfrak{h}$, and the image of a nilpotent series for $\mathfrak{g}$ in a quotient algebra $\mathfrak{q}$ is a nilpotent series for $\mathfrak{q}$.

(b) For any ideal $\mathfrak{a} \subset z(\mathfrak{g})$, the inverse image of a nilpotent series for $\mathfrak{g}/\mathfrak{a}$ becomes a nilpotent series for $\mathfrak{g}$ when extended by 0.

(c) If $\mathfrak{g}$ is nilpotent, then the last nonzero term $\mathfrak{a}$ in a nilpotent series for $\mathfrak{g}$ is contained in $z(\mathfrak{g})$. □

PROPOSITION 2.6 *Let $\mathfrak{h}$ be a proper Lie subalgebra of a nilpotent Lie algebra $\mathfrak{g}$; then $\mathfrak{h} \neq n_{\mathfrak{g}}(\mathfrak{h})$.*

PROOF. We use induction on the dimension of $\mathfrak{g}$. Because $\mathfrak{g}$ is nilpotent and nonzero, its centre $z(\mathfrak{g})$ is nonzero. If $z(\mathfrak{g}) \not\subset \mathfrak{h}$, then $n_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h}$ because $z(\mathfrak{g})$ normalizes $\mathfrak{h}$. If $z(\mathfrak{g}) \subset \mathfrak{h}$, then we can apply induction to the Lie subalgebra $\mathfrak{h}/z(\mathfrak{g})$ of $\mathfrak{g}/z(\mathfrak{g})$. □

ASIDE 2.7 The proposition is the analogue of the following statement in the theory of finite groups: let H be a proper subgroup of a nilpotent finite group G; then $H \neq N_G(H)$ (GT 6.20).

Engel's theorem

THEOREM 2.8 (ENGEL) *Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$. If $\rho(x)$ is nilpotent for all $x \in \mathfrak{g}$, then there exists a basis of V for which $\rho(\mathfrak{g})$ is contained in $\mathfrak{n}_n$, $n = \dim V$; in particular, $\rho(\mathfrak{g})$ is nilpotent.*

In other words, there exists a basis $e_1, \ldots, e_n$ for V such that

$$\mathfrak{g}e_i \subset \langle e_1, \ldots, e_{i-1} \rangle, \text{ all } i. \tag{22}$$

Before proving Theorem 2.8, we list some consequences.

COROLLARY 2.9 *Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of $\mathfrak{g}$ on a nonzero vector space V. If $\rho(x)$ is nilpotent for all $x \in \mathfrak{g}$, then ρ has a fixed vector, i.e., there exists a nonzero vector v in V such that $\mathfrak{g}v = 0$.*

PROOF. Clearly e_1 is a nonzero fixed vector. □

2.10 Let $\mathfrak{g}$ be a Lie algebra over k. If the $n+1$st term $\mathfrak{g}^{n+1}$ of the lower central series of $\mathfrak{g}$ is zero, then

$$[x_1, [x_2, \ldots [x_n, y] \ldots]] = 0$$

for all $x_1, \ldots, x_n, y \in \mathfrak{g}$. In other words, $\mathrm{ad}(x_1) \circ \cdots \circ \mathrm{ad}(x_n) = 0$, and, in particular, $\mathrm{ad}(x)^n = 0$. Therefore, if $\mathfrak{g}$ is nilpotent, then $\mathrm{ad}(x)$ is nilpotent for all $x \in \mathfrak{g}$. The converse to this statement is also true.

COROLLARY 2.11 *A Lie algebra $\mathfrak{g}$ is nilpotent if* $\mathrm{ad}(x)\colon \mathfrak{g} \to \mathfrak{g}$ *is nilpotent for every* $x \in \mathfrak{g}$.

PROOF. We may assume that $\mathfrak{g} \neq 0$. On applying (2.9) to the representation $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$, we see that there exists a nonzero $x \in \mathfrak{g}$ such that $[\mathfrak{g}, x] = 0$. Therefore $z(\mathfrak{g}) \neq 0$. The quotient Lie algebra $\mathfrak{g}/z(\mathfrak{g})$ satisfies the hypothesis of (2.11) and has smaller dimension than $\mathfrak{g}$. Using induction on the dimension of $\mathfrak{g}$, we find that $\mathfrak{g}/z(\mathfrak{g})$ is nilpotent, which implies that $\mathfrak{g}$ is nilpotent by (2.5b). □

2.12 Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$. If $\rho(\mathfrak{g})$ consists of nilpotent endomorphisms of V, then $\rho(\mathfrak{g}) \subset \mathfrak{n}(F)$ for some maximal flag F in V and $\rho(\mathfrak{g})$ is nilpotent (2.8). Conversely, if $\mathfrak{g}$ is nilpotent *and ρ is the adjoint representation*, then $\rho(\mathfrak{g})$ consists of nilpotent endomorphisms (2.10), but for other representations $\rho(\mathfrak{g})$ *need not* consist of nilpotent endomorphisms and $\rho(\mathfrak{g})$ *need not* be contained in $\mathfrak{n}(F)$ for any maximal flag. For example, if V has dimension 1, then $\mathfrak{g} = \mathfrak{gl}_V$ is nilpotent (even commutative), but there is no basis for which the elements of $\mathfrak{g}$ are represented by *strictly* upper triangular matrices.

2.13 Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$. The set of $x \in \mathfrak{g}$ such that $\rho(x)$ is nilpotent need not be an ideal in $\mathfrak{g}$, but in Corollary 2.22 below we show that, there exists a largest ideal $\mathfrak{n}$ in $\mathfrak{g}$ such that $\rho(\mathfrak{n})$ consists of nilpotent elements.

Proof of Engel's Theorem

We first show that it suffices to prove 2.9. Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ satisfy the hypothesis of (2.8). If $V \neq 0$, then (2.9) applied to ρ shows that there exists a vector $e_1 \neq 0$ such that $\mathfrak{g}e_1 = 0$; if $V \neq \langle e_1 \rangle$, then (2.9) applied to $\mathfrak{g} \to \mathfrak{gl}_{V/\langle e_1 \rangle}$ shows that there exists a vector $e_2 \notin \langle e_1 \rangle$ such that $\mathfrak{g}e_2 \subset \langle e_1 \rangle$. Continuing in this fashion, we obtain a basis $e_1, \ldots, e_n$ for V satisfying (22).

We now prove (2.9). For a single $x \in \mathfrak{g}$, there is no difficulty finding a fixed vector: choose any nonzero vector v_0 in V, and let $v = x^m v_0$ with m the last element of $\mathbb{N}$ such that $x^m v_0 \neq 0$. The problem is to find a vector that is simultaneously fixed by all elements x of $\mathfrak{g}$.

By induction, we may assume that the statement holds for Lie algebras of dimension less than $\dim \mathfrak{g}$. Also, we may replace $\mathfrak{g}$ with its image in $\mathfrak{gl}_V$, and so assume that $\mathfrak{g} \subset \mathfrak{gl}_V$.

Let $\mathfrak{h}$ be a *maximal* proper subalgebra of $\mathfrak{g}$. Then $n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$ (2.6), and so $\mathfrak{h}$ is an ideal in $\mathfrak{g}$. Let $x_0 \in \mathfrak{g} \smallsetminus \mathfrak{h}$; then $\mathfrak{h} + \langle x_0 \rangle$ is a Lie subalgebra of $\mathfrak{g}$ properly containing $\mathfrak{h}$, and so it equals $\mathfrak{g}$.

Let $W = \{v \in V \mid \mathfrak{h}v = 0\}$; then $W \neq 0$ by induction ($\dim \mathfrak{h} < \dim \mathfrak{g}$). For $h \in \mathfrak{h}$ and $w \in W$,

$$h(x_0 w) = [h, x_0]w + x_0(hw) = 0,$$

and so $x_0 W \subset W$. Because x_0 acts nilpotently on W, there exists a nonzero $v \in W$ such that $x_0 v = 0$. Now $\mathfrak{g}v = (\mathfrak{h} + \langle x_0 \rangle)v = 0$.

ASIDE 2.14 Engel sketched a proof of his theorem in a letter to Killing in 1890, and his student Umlauf gave a complete proof in his 1891 dissertation (Wikipedia; Hawkins 2000, pp.176–177). The statement 2.11 is also referred to as Engel's theorem.

Representations of nilpotent Lie algebras

Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of Lie algebra $\mathfrak{g}$. For a linear form λ on $\mathfrak{g}$, the ***primary space*** V^λ is defined to be the set of $v \in V$ such that, for every $g \in \mathfrak{g}$,

$$(\rho(g) - \lambda(g))^n v = 0$$

for all sufficiently large n.

THEOREM 2.15 *Assume that k is algebraically closed. If $\mathfrak{g}$ is nilpotent, then each space V^λ is stable under $\mathfrak{g}$, and*

$$V = \bigoplus_{\lambda:\mathfrak{g}\to k} V^\lambda.$$

PROOF. When $\mathfrak{g}$ is commutative, the elements $\rho(g)$ form a commuting family of endomorphisms of V, and this is obvious from linear algebra. In the general case, the $\rho(g)$ are "almost commuting". For the proof in the general case, see Bourbaki LIE, I, §5, Exercise 12; Bourbaki LIE VII, §1, 3, Proposition 9; Jacobson 1962, II, Theorem 7; Casselman, Introduction to Lie algebras, 10.8 (or the next version of the notes). □

NOTES It is not necessary for k to be algebraically closed — it suffices that every endomorphism $\rho(g)$, $g \in \mathfrak{g}$, have all of its eigenvalues in k (i.e., that each endomorphism $\rho(g)$ be trigonalizable).

NOTES As an exercise, compute the affine group scheme attached to the tannakian category $\mathsf{Rep}(\mathfrak{g})$, $\mathfrak{g}$ nilpotent. For the case that $\mathfrak{g}$ is one-dimensional, see II, 4.17 below.

Nilpotency ideals and the largest nilpotent ideal

Review of Jacobson radicals

Let A be an associative ring. The ***Jacobson radical*** $R(A)$ of A is the intersection of the maximal left ideals of A. A ***nilideal*** in A is an ideal whose elements are all nilpotent.

2.16 *The following conditions on an element x of A are equivalent:*

(a) *x lies in the radical $R(A)$ of A;*
(b) *$1 - ax$ has a left inverse for all $a \in A$;*
(c) *$xM = 0$ for every simple left A-module M.*

(a) $\Rightarrow$(b): Let $x \in R(A)$. If $1 - ax$ does not have a left inverse, then it lies in some maximal left ideal $\mathfrak{m}$ (by Zorn's lemma). Now $1 = (1 - ax) + ax \in \mathfrak{m}$, which is a contradiction.

(b) $\Rightarrow$(c): Let M a simple left A-module. If $xM \neq 0$, then $xm \neq 0$ for some $m \in M$. Because M is simple, $Axm = M$; in particular, $axm = m$ for some $a \in A$. Now $(1 - ax)m = 0$. But $(1 - ax)$ has a left inverse, and so this contradicts the fact that $m \neq 0$.

(c) $\Rightarrow$(a): Let $\mathfrak{m}$ be a maximal left ideal in A. Then $A/\mathfrak{m}$ is a simple left A-module, and so $x(A/\mathfrak{m}) = 0$. Therefore $x \in \mathfrak{m}$.

2.17 (NAKAYAMA'S LEMMA) *Let M be a finitely generated A-module. If $R(A) \cdot M = M$, then $M = 0$.*

Suppose $M \neq 0$. Choose a minimal set of generators $\{e_1, \ldots, e_n\}$, $n \geq 1$, for M and write

$$e_1 = a_1 e_1 + \cdots + a_n e_n, \quad a_i \in R(A).$$

Then

$$(1 - a_1)e_1 = a_2 e_2 + \cdots + a_n e_n.$$

As $1 - a_1$ has a left inverse, this shows that $\{e_2, \ldots, e_n\}$ generates M, which contradicts the minimality of the original set.

2.18 *$R(A)$ contains every left nilideal of A.*

Let $\mathfrak{n}$ be a left nilideal, and let $x \in \mathfrak{n}$. For $a \in A$, ax is nilpotent, say $(ax)^n = 0$, and

$$(1 + ax + \cdots + (ax)^{n-1})(1 - ax) = 1.$$

Therefore $(1 - ax)$ has a left inverse for all $a \in A$, and so $x \in R(A)$ (by 2.16).

2.19 *If A is a finite k-algebra, then $R(A)^n = 0$ for some n.*

Let $R = R(A)$. As A is artinian, the sequence of ideals $R \supset R^2 \supset \cdots$ becomes stationary, say $R^n = R^{n+1} = \cdots$. The ideal R^n is finitely generated (even as a k-module), and so Nakayama's lemma shows that it is zero.

Nilpotency ideals

DEFINITION 2.20 Let $\rho \colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$. A ***nilpotency ideal*** of $\mathfrak{g}$ with respect to ρ is an ideal $\mathfrak{a}$ such that $\rho(x)$ is nilpotent for all x in $\mathfrak{a}$.

When we regard V as a $\mathfrak{g}$-module, the condition becomes that x_V is nilpotent for all $x \in \mathfrak{a}$ (and we refer to $\mathfrak{a}$ as a nilpotency ideal of $\mathfrak{g}$ with respect to V).

PROPOSITION 2.21 *Let $\rho \colon \mathfrak{g} \to \mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$. The following conditions on an ideal $\mathfrak{a}$ of $\mathfrak{g}$ are equivalent:*

(a) *$\mathfrak{a}$ is a nilpotency ideal with respect to ρ;*
(b) *for all simple subquotients M of V, $\mathfrak{a}M = 0$;*
(c) *let A be the associative k-subalgebra of* End(V) *generated by $\rho(\mathfrak{a})$; then $\rho(\mathfrak{a}) \subset R(A)$.*

PROOF. (a)⇒(b). Let M be a simple subquotient of V, and let

$$N = \{m \in M \mid \mathfrak{a}m = 0\}$$

(k-subspace of M). The elements of $\mathfrak{a}$ act nilpotently on V, and hence on M, and so (2.9) shows that $N \neq 0$. The subspace N of M is stable under $\mathfrak{g}$, because

$$a(xn) = [a, x]n + x(an) = 0$$

for $a \in \mathfrak{a}$, $x \in \mathfrak{g}$, and $n \in N$. As M is simple, $N = M$.

(b)⇒(c). By definition, A is the associative k-subalgebra of $\mathrm{End}(V)$ generated by $\{x_V \mid x \in \mathfrak{a}\}$. Let

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

be a filtration of V by $\mathfrak{g}$-submodules such that each quotient V_i/V_{i+1} is simple. If $x \in \mathfrak{a}$, then $x_V V_i \subset V_{i+1}$ for all $0 \le i \le n-1$, and so $x_V^n = 0$. It follows that, for any $x \in \mathfrak{a}$, Ax_V is a left nilideal in A, and so $Ax_V \subset R(A)$ (2.18).

(c)⇒(a). According to (2.19), some power $R(A)$ is zero; therefore x_V is nilpotent for all $x \in \mathfrak{a}$. □

COROLLARY 2.22 *Let (V,ρ) be a representation of $\mathfrak{g}$, and let*

$$\mathfrak{n} = \{x \in \mathfrak{g} \mid xM = 0 \text{ for all simple subquotients } M \text{ of } V\}.$$

Then $\mathfrak{n}$ is a nilpotency ideal of $\mathfrak{g}$ with respect to V, and it contains all other nilpotency ideals.

PROOF. Obviously $\mathfrak{n}$ is an ideal in $\mathfrak{g}$, and the remaining statements follow from the proposition. □

The ideal $\mathfrak{n}$ in (2.22) is the largest nilpotency ideal of $\mathfrak{g}$ with respect to ρ. We denote it by $n_\rho(\mathfrak{g})$. It contains the kernel of ρ, and equals it when V is semisimple (obviously), but not in general otherwise. It need not contain all $x \in \mathfrak{g}$ such that $\rho(x)$ is nilpotent, because the set of such x need not form an ideal.

The largest nilpotent ideal in a Lie algebra

We say that an ideal $\mathfrak{a}$ in a Lie algebra $\mathfrak{g}$ is ***nilpotent*** if it is nilpotent as a Lie algebra.

PROPOSITION 2.23 *The nilpotent ideals of $\mathfrak{g}$ are exactly the nilpotency ideals of $\mathfrak{g}$ with respect to the adjoint representation.*

PROOF. If $\mathrm{ad}_{\mathfrak{g}}(x)$ is nilpotent for all $x \in \mathfrak{a}$, then so also is $\mathrm{ad}_{\mathfrak{a}}(x)$, and so $\mathfrak{a}$ is nilpotent by Engel's theorem (see 2.11). Conversely, if $\mathfrak{a}$ is nilpotent and $x \in \mathfrak{a}$, then $\mathrm{ad}_{\mathfrak{a}}(x)^n = 0$ for some n (see 2.10); as $[x,\mathfrak{g}] \subset \mathfrak{a}$, this implies that $\mathrm{ad}_{\mathfrak{g}}(x)^{n+1} = 0$. □

COROLLARY 2.24 *Every Lie algebra has a largest nilpotent ideal, containing all other nilpotent ideals.*

PROOF. According to the proposition, the largest nilpotency ideal of $\mathfrak{g}$ with respect to the adjoint representation is also the largest nilpotent ideal of $\mathfrak{g}$. □

The Hausdorff series

For a nilpotent $n \times n$ matrix X,

$$\exp(X) \overset{\text{def}}{=} I + X + X^2/2! + X^3/3! + \cdots$$

is a well defined element of $\mathrm{GL}_n(k)$. Moreover, when X and Y are nilpotent,

$$\exp(X)\cdot\exp(Y)=\exp(W)$$

for some nilpotent W, and we may ask for a formula expressing W in terms of X and Y. This is provided by the ***Hausdorff series***[4], which is a formal power series,

$$H(X,Y)=\sum\nolimits_{m\geq 0}H^m(X,Y),\quad H^m(X,Y) \text{ homogeneous of degree } m,$$

with coefficients in $\mathbb{Q}$. The first few terms are

$$H^1(X,Y)=X+Y$$
$$H^2(X,Y)=\frac{1}{2}[X,Y].$$

If x and y are nilpotent elements of $\mathrm{GL}_n(k)$, then

$$\exp(x)\cdot\exp(y)=\exp(H(x,y)),$$

and this determines the power series $H(X,Y)$ uniquely. See Bourbaki LIE, II, §6.

NOTES The classification of nilpotent Lie algebras, even in characteristic zero, is complicated. Except in low dimensions, there are infinitely many, and so it is a question of studying their moduli varieties. In low dimensions, there are complete lists. See mo21114 for a discussion of this.

3 Solvable Lie algebras: Lie's theorem

In this section, all Lie algebras and all representations are finite dimensional over a field k.

Generalities

DEFINITION 3.1 A Lie algebra $\mathfrak{g}$ is said to be ***solvable*** if it admits a filtration

$$\mathfrak{g}=\mathfrak{a}_0\supset\mathfrak{a}_1\supset\cdots\supset\mathfrak{a}_r=0 \tag{23}$$

by ideals such that $[\mathfrak{a}_i,\mathfrak{a}_i]\subset\mathfrak{a}_{i+1}$ for $0\leq i\leq r-1$. Such a filtration is called a ***solvable series***.

The condition for (23) to be a solvable series is that the quotients $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ be commutative for $0\leq i\leq r-1$. Thus the solvable Lie algebras are exactly those that can be obtained from commutative Lie algebras by successive extensions,

$$0\to\mathfrak{a}_1/\mathfrak{a}_2\to\mathfrak{g}/\mathfrak{a}_2\to\mathfrak{g}/\mathfrak{a}_1\to 0$$
$$0\to\mathfrak{a}_2/\mathfrak{a}_3\to\mathfrak{g}/\mathfrak{a}_3\to\mathfrak{g}/\mathfrak{a}_2\to 0$$
$$\ldots$$

In other words, the solvable Lie algebras form the smallest class containing the commutative Lie algebras and closed under extensions.

[4]This is Bourbaki's terminology — others write Baker-Campbell-Hausdorff, or Campbell-Hausdorff, or ...

The characteristic ideal $[\mathfrak{g},\mathfrak{g}]$ is called the ***derived algebra*** of $\mathfrak{g}$, and is denoted $\mathcal{D}\mathfrak{g}$. Clearly $\mathcal{D}\mathfrak{g}$ is contained in every ideal $\mathfrak{a}$ such that $\mathfrak{g}/\mathfrak{a}$ is commutative, and so $\mathfrak{g}/\mathcal{D}\mathfrak{g}$ is the largest commutative quotient of $\mathfrak{g}$. Write $\mathcal{D}^2\mathfrak{g}$ for the second derived algebra $\mathcal{D}(\mathcal{D}\mathfrak{g})$, $\mathcal{D}^3\mathfrak{g}$ for the third derived algebra $\mathcal{D}(\mathcal{D}^2\mathfrak{g})$, and so on. These are characteristic ideals, and the ***derived series*** of $\mathfrak{g}$ is the sequence

$$\mathfrak{g} \supset \mathcal{D}\mathfrak{g} \supset \mathcal{D}^2\mathfrak{g} \supset \cdots.$$

We sometimes write $\mathfrak{g}'$ for $\mathcal{D}\mathfrak{g}$ and $\mathfrak{g}^{(n)}$ for $\mathcal{D}^n\mathfrak{g}$.

PROPOSITION 3.2 *A Lie algebra $\mathfrak{g}$ is solvable if and only if its derived series terminates with zero.*

PROOF. If the derived series terminates with zero, then it is a solvable series. Conversely, if $\mathfrak{g} \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_r = 0$ is a solvable series, then $\mathfrak{a}_1 \supset \mathfrak{g}'$ because $\mathfrak{g}/\mathfrak{a}_1$ is commutative, $\mathfrak{a}_2 \supset \mathfrak{a}_1' \supset \mathfrak{g}''$ because $\mathfrak{a}_1/\mathfrak{a}_2$ is commutative, and so on until $0 = \mathfrak{a}_r \supset \mathfrak{g}^{(r)}$. □

Let V be a vector space of dimension n, and let

$$F\colon V = V_0 \supset V_1 \supset \cdots \supset V_n = 0, \quad \dim V_i = n - i,$$

be a maximal flag in V. Let $\mathfrak{b}(F)$ be the Lie subalgebra of $\mathfrak{gl}_V$ consisting of the elements x such that $x(V_i) \subset V_i$ for all i. Then $\mathcal{D}(\mathfrak{b}(F)) = \mathfrak{n}(F)$, and so $\mathfrak{b}(F)$ is solvable. For example,

$$\mathfrak{b}_3 = \left\{\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\} \supset \{0\}$$

is a solvable series for $\mathfrak{b}_3$.

PROPOSITION 3.3 *Let k' be a field containing k. A Lie algebra $\mathfrak{g}$ over k is solvable if and only if $\mathfrak{g}_{k'} \stackrel{\text{def}}{=} k' \otimes_k \mathfrak{g}$ is solvable.*

PROOF. Obviously, for any subalgebras $\mathfrak{h}$ and $\mathfrak{h}'$ of $\mathfrak{g}$, $[\mathfrak{h},\mathfrak{h}']_{k'} = [\mathfrak{h}_{k'},\mathfrak{h}'_{k'}]$, and so, under extension of the base field, the derived series of $\mathfrak{g}$ maps to that of $\mathfrak{g}_{k'}$. □

We say that an ideal is ***solvable*** if it is solvable as a Lie algebra.

PROPOSITION 3.4 *(a) Subalgebras and quotient algebras of solvable Lie algebras are solvable.*

(b) A Lie algebra $\mathfrak{g}$ is solvable if it contains an ideal $\mathfrak{n}$ such that both $\mathfrak{n}$ and $\mathfrak{g}/\mathfrak{n}$ are solvable.

(c) Let $\mathfrak{n}$ be an ideal in a Lie algebra $\mathfrak{g}$, and let $\mathfrak{h}$ be a subalgebra of $\mathfrak{g}$. If $\mathfrak{n}$ and $\mathfrak{h}$ are solvable, then $\mathfrak{h} + \mathfrak{n}$ is solvable.

PROOF. (a) The intersection of a solvable series for $\mathfrak{g}$ with a Lie subalgebra $\mathfrak{h}$ is a solvable series for $\mathfrak{h}$, and the image of a solvable series for $\mathfrak{g}$ in a quotient algebra $\mathfrak{q}$ is a solvable series for $\mathfrak{q}$.

(b) Because $\mathfrak{g}/\mathfrak{n}$ is solvable, $\mathfrak{g}^{(m)} \subset \mathfrak{n}$ for some m. Now $\mathfrak{g}^{(m+n)} \subset \mathfrak{n}^{(n)}$, which is zero for some n.

(c) This follows from (b) because $\mathfrak{h} + \mathfrak{n}/\mathfrak{n} \simeq \mathfrak{h}/\mathfrak{h} \cap \mathfrak{n}$ (see 1.14), which is solvable by (a). □

COROLLARY 3.5 *Every Lie algebra contains a largest solvable ideal.*

PROOF. Let $\mathfrak{n}$ be a maximal solvable ideal. If $\mathfrak{h}$ is also a solvable ideal, then $\mathfrak{h}+\mathfrak{n}$ is solvable by (3.4c), and so equals $\mathfrak{n}$; therefore $\mathfrak{h}\subset\mathfrak{n}$. □

DEFINITION 3.6 The ***radical*** $\mathfrak{r}=r(\mathfrak{g})$ of $\mathfrak{g}$ is the largest solvable ideal in $\mathfrak{g}$.

The radical of $\mathfrak{g}$ is a characteristic ideal.

Lie's theorem

THEOREM 3.7 (LIE) *Let $\rho\colon\mathfrak{g}\to\mathfrak{gl}_V$ be a representation of a Lie algebra $\mathfrak{g}$ over k, and assume that k is algebraically closed of characteristic zero. If $\mathfrak{g}$ is solvable, then there exists a basis of V for which $\rho(\mathfrak{g})$ is contained in $\mathfrak{b}_n$, $n=\dim V$.*

In other words, there exists a basis $e_1,\ldots,e_n$ for V such that

$$\mathfrak{g}e_i\subset\langle e_1,\ldots,e_i\rangle,\text{ all } i. \tag{24}$$

Before proving Theorem 3.7 we list some consequences and give some examples.

COROLLARY 3.8 *Under the hypotheses of the theorem, assume that $V\neq 0$. Then there exists a nonzero vector $v\in V$ such that $\mathfrak{g}v\subset\langle v\rangle$ (i.e., there exists a common eigenvector in V for the elements of $\mathfrak{g}$).*

PROOF. Clearly e_1 is a common eigenvector. □

COROLLARY 3.9 *If $\mathfrak{g}$ is solvable and k is algebraically closed of characteristic zero, then all simple $\mathfrak{g}$-modules are one-dimensional.*

PROOF. Immediate consequence of (3.8). □

COROLLARY 3.10 *Let $\mathfrak{g}$ be a solvable Lie algebra over a field of characteristic zero, and let $\rho\colon\mathfrak{g}\to\mathfrak{gl}_V$ be a representation of $\mathfrak{g}$.*

(a) *For all $y\in[\mathfrak{g},\mathfrak{g}]$, $\rho(y)$ is a nilpotent endomorphism of V.*
(b) *For all $x\in\mathfrak{g}$ and $y\in[\mathfrak{g},\mathfrak{g}]$,*

$$\mathrm{Tr}_V(\rho(x)\circ\rho(y))=0$$

PROOF. We may suppose that k is algebraically closed (3.3). According to Lie's theorem, there exists a basis of V for which $\rho(\mathfrak{g})$ is contained in $\mathfrak{b}_n$, $n=\dim V$. Then $\rho([\mathfrak{g},\mathfrak{g}])\subset[\rho(\mathfrak{g}),\rho(\mathfrak{g})]\subset\mathfrak{n}_n$, which consists of nilpotent endomorphisms of V. This proves (a), and shows that in (b),

$$\rho(x)\circ\rho(y)\in\mathfrak{b}_n\cdot\mathfrak{n}_n\subset\mathfrak{n}_n.$$ □

COROLLARY 3.11 *Let $\mathfrak{g}$ be a solvable Lie algebra over a field of characteristic zero; then $[\mathfrak{g},\mathfrak{g}]$ is nilpotent.*

PROOF. We may suppose that k is algebraically closed (3.3). As $\mathrm{ad}(\mathfrak{g})$ is a quotient of $\mathfrak{g}$ with kernel $z(\mathfrak{g})$, $\mathcal{D}(\mathrm{ad}(\mathfrak{g}))$ is a quotient of $\mathcal{D}(\mathfrak{g})$ with kernel $z(\mathfrak{g})\cap\mathcal{D}(\mathfrak{g})$. In particular, $\mathcal{D}(\mathfrak{g})$ is a central extension of $\mathcal{D}(\mathrm{ad}(\mathfrak{g}))$, and so it suffices to show that the latter is nilpotent. This allows us to assume that $\mathfrak{g}\subset\mathfrak{gl}_V$ for some finite-dimensional vector space V. According to Lie's theorem, there exists a basis of V for which $\mathfrak{g}$ is contained in $\mathfrak{b}_{\dim V}$. Then $[\mathfrak{g},\mathfrak{g}]\subset\mathfrak{n}_{\dim V}$, which is nilpotent. □

In order for the map $v\mapsto xv$ be trigonalizable, all of its eigenvalues must lie in k. This explains why k is required to be algebraically closed in Lie's theorem. The condition that k have characteristic zero is more surprising, but the following examples shows that it is necessary.

3.12 In characteristic 2, $\mathfrak{sl}_2$ is solvable but for no basis is it contained in $\mathfrak{b}_2$.

3.13 Let k have characteristic $p\neq 0$, and consider the $p\times p$ matrices

$$x=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\\1&0&0&\cdots&0\end{pmatrix},\quad y=\begin{pmatrix}0&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&p-2&0\\0&0&\cdots&0&p-1\end{pmatrix}.$$

Then

$$[x,y]=\begin{pmatrix}0&1&0&\cdots&0\\0&0&2&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&p-1\\0&0&0&\cdots&0\end{pmatrix}-\begin{pmatrix}0&0&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&p-2\\p-1&0&0&\cdots&0\end{pmatrix}=x$$

(this uses that $p=0$). Therefore, $\mathfrak{g}=\langle x,y\rangle$ is a solvable subalgebra of $\mathfrak{gl}_p$ (cf. the example p.26). The matrices x and y have the following eigenvectors:

$$x:\begin{pmatrix}1\\1\\1\\\vdots\\1\end{pmatrix};\quad y:\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix},\ldots,\begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}.$$

Therefore $\mathfrak{g}$ has no simultaneous eigenvector, and so Lie's theorem fails.

3.14 Even Corollary 3.10(a) fails in nonzero characteristic. Note that it implies that, for a solvable subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$, the derived algebra $[\mathfrak{g},\mathfrak{g}]$ consists of nilpotent endomorphisms. Example (3.2), and example (3.13) in the case $\mathrm{char}(k)=2$, show that this is false in characteristic 2. For more examples in all nonzero characteristics, see Humphreys 1972, §4, Exercise 4.

The invariance lemma

Before proving Lie's theorem, we need a lemma.

LEMMA 3.15 (INVARIANCE LEMMA) *Let V be a finite-dimensional vector space, and let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}_V$. For all ideals $\mathfrak{a}$ in $\mathfrak{g}$ and linear maps $\lambda\colon\mathfrak{a}\to k$, the eigenspace*

$$V_\lambda = \{v \in V \mid av = \lambda(a)v \text{ for all } a \in \mathfrak{a}\} \tag{25}$$

is invariant under $\mathfrak{g}$.

PROOF. Let $x \in \mathfrak{g}$ and let $v \in V_\lambda$. We have to show that $xv \in V_\lambda$, but for $a \in \mathfrak{a}$,

$$a(xv) = x(av) + [a,x](v) = \lambda(a)xv + \lambda([a,x])v.$$

Thus a nonzero V_λ is invariant under $\mathfrak{g}$ if and only if $\lambda([\mathfrak{a},\mathfrak{g}]) = 0$.

Fix an $x \in \mathfrak{g}$ and a nonzero $v \in V_\lambda$, and consider the subspaces

$$\langle v\rangle \subset \langle v, xv\rangle \subset \cdots \subset \langle v, xv, \ldots, x^{i-1}v\rangle \subset \cdots$$

of V. Let m be the first integer such that $\langle v, \ldots, x^{m-1}v\rangle = \langle v, \ldots, x^m v\rangle$. Then

$$W \stackrel{\text{def}}{=} \langle v, xv, \ldots, x^{m-1}v\rangle$$

has basis $v, xv, \ldots, x^{m-1}v$ and contains $x^i v$ for all i.

We claim that an element a of $\mathfrak{a}$ maps W into itself and has matrix

$$\begin{pmatrix} \lambda(a) & * & \cdots & * \\ 0 & \lambda(a) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda(a) \end{pmatrix}$$

with respect to the given basis. We check this column by column. The equality

$$av = \lambda(a)v$$

shows that the first column is as claimed. As $[a,x] \in \mathfrak{a}$,

$$\begin{aligned} a(xv) &= x(av) + [a,x]v \\ &= \lambda(a)xv + \lambda([a,x])v, \end{aligned}$$

and so that the second column is as claimed (with $* = \lambda([a,x])$). Assume that the first i columns are as claimed, and consider

$$a(x^i v) = ax(x^{i-1}v) = (xa + [a,x])x^{i-1}v. \tag{26}$$

From knowing the ith column, we find that

$$a(x^{i-1}v) = \lambda(a)x^{i-1}v + u \tag{27}$$

$$[a,x](x^{i-1}v) = \lambda([a,x])x^{i-1}v + u' \tag{28}$$

with $u, u' \in \langle v, xv, \ldots, x^{i-2}v \rangle$. On multiplying (27) with x we obtain the equality

$$xa(x^{i-1}v) = \lambda(a)x^i v + xu \tag{29}$$

with $xu \in \langle v, xv, \ldots, x^{i-1}v \rangle$. Now (26), (28), and (29) show that the $(i+1)$st column is as claimed.

This completes the proof that the matrix of $a \in \mathfrak{a}$ acting on W has the form claimed, and shows that

$$\mathrm{Tr}_W(a) = m\lambda(a). \tag{30}$$

We now complete the proof of the lemma by showing that $\lambda([\mathfrak{a}, \mathfrak{g}]) = 0$. Let $a \in \mathfrak{a}$ and $x \in \mathfrak{g}$. On applying (30) to the element $[a, x]$ of $\mathfrak{a}$, we find that

$$m\lambda([a,x]) = \mathrm{Tr}_W([a,x]) = \mathrm{Tr}_W(ax - xa) = 0,$$

and so $\lambda([a,x]) = 0$ (because $m \neq 0$ in k). □

Proof of Lie's theorem

We first show that it suffices to prove (3.8). Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ satisfy the hypotheses of Lie's theorem. If $V \neq 0$, then (3.8) applied to ρ shows that there exists a vector $e_1 \neq 0$ such that $\mathfrak{g}e_1 \in \langle e_1 \rangle$; if $V \neq \langle e_1 \rangle$, then (3.8) applied to $\mathfrak{g} \to \mathfrak{gl}_{V/\langle e_1 \rangle}$ shows that there exists a vector $e_2 \notin \langle e_1 \rangle$ such that $\mathfrak{g}e_2 \subset \langle e_1, e_2 \rangle$. Continuing in this fashion, we obtain a basis $e_1, \ldots, e_n$ for V satisfying (24).

We now prove (3.8). We may replace $\mathfrak{g}$ with its image $\rho(\mathfrak{g})$, and so suppose that $\mathfrak{g} \subset \mathfrak{gl}_V$. We use induction on the dimension of $\mathfrak{g}$, which we may suppose to be ≥ 1. If $\dim \mathfrak{g} = 1$, then $\mathfrak{g} = kx$ for some endomorphism x of V, and x has an eigenvector because k is algebraically closed. Because $\mathfrak{g}$ is solvable, its derived algebra $\mathfrak{g}' \neq \mathfrak{g}$. The quotient $\mathfrak{g}/\mathfrak{g}'$ is commutative, and so is essentially just a vector space. Write $\mathfrak{g}/\mathfrak{g}' = \bar{\mathfrak{a}} \oplus \langle \bar{x} \rangle$ as the direct sum of a subspaces of codimension 1 and dimension 1. Then $\mathfrak{g} = \mathfrak{a} \oplus \langle x \rangle$ with $\mathfrak{a}$ the inverse image of $\bar{\mathfrak{a}}$ in $\mathfrak{g}$ (an ideal) and x an inverse image of $\bar{x}$. By induction, there exists a nonzero $w \in V$ such that $\mathfrak{a}w \subset \langle w \rangle$, i.e., such that $aw = \lambda(a)w$, all $a \in \mathfrak{a}$, for some $\lambda\colon \mathfrak{a} \to k$. Let V_λ be the corresponding eigenspace for $\mathfrak{a}$ (25). According to the Invariance Lemma, V_λ is stable under $\mathfrak{g}$. As it is nonzero, it contains a nonzero eigenvector v for x. Now, for any element $g = a + cx \in \mathfrak{g}$,

$$gv = \lambda(a)v + c(xv) \in \langle v \rangle.$$

ASIDE 3.16 We used that k has characteristic zero only at the end of the proof of the Invariance Lemma where we concluded that $m \neq 0$. Here m is an integer $\leq \dim V$ regarded as an element of k. Hence if k has characteristic p, then Lie's theorem (together with its proof) holds provided $\dim V < p$. This is a general phenomenon: for any specific problem, there will be a p_0 such that the characteristic p case behaves as the characteristic 0 case provided $p \geq p_0$.

NOTES The proof of Lie's theorem in Casselman, Introduction to Lie algebras, 10.6, looks simpler.

Cartan's criterion for solvablity

Recall that for any $n \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$,

$$\mathrm{Tr}(AB) = \textstyle\sum_{i,j} a_{ij} b_{ji} = \mathrm{Tr}(BA). \tag{31}$$

Hence, $\mathrm{Tr}_V(x \circ y) = \mathrm{Tr}_V(y \circ x)$ for any endomorphisms x, y of a vector space V, and so

$$\begin{aligned}\mathrm{Tr}([x,y]\circ z) &= \mathrm{Tr}(x\circ y\circ z) - \mathrm{Tr}(y\circ x\circ z)\\ &= \mathrm{Tr}(x\circ y\circ z) - \mathrm{Tr}(x\circ z\circ y)\\ &= \mathrm{Tr}(x\circ[y,z]).\end{aligned} \tag{32}$$

THEOREM 3.17 (CARTAN'S CRITERION) *Let $\mathfrak{g}$ be a subalgebra of $\mathfrak{gl}_V$, where V is a finite-dimensional vector space over a field k of characteristic zero. Then $\mathfrak{g}$ is solvable if $\mathrm{Tr}_V(x \circ y) = 0$ for all $x, y \in \mathfrak{g}$.*

PROOF. We first observe that, if k' is a field containing k, then the theorem is true for $\mathfrak{g} \subset \mathfrak{gl}_V$ if and only if it is true for $\mathfrak{g}_{k'} \subset \mathfrak{gl}_{V_{k'}}$ (because $\mathfrak{g}$ is solvable if and only if $\mathfrak{g}_{k'}$ is solvable (3.3)). Therefore, we may assume that the field k is finitely generated over $\mathbb{Q}$, hence embeddable in $\mathbb{C}$, and then that $k = \mathbb{C}$.

We shall show that the condition implies that each $x \in [\mathfrak{g},\mathfrak{g}]$ defines a nilpotent endomorphism of V. Then Engel's theorem (2.8) will show that $[\mathfrak{g},\mathfrak{g}]$ is nilpotent, in particular, solvable, and it follows that $\mathfrak{g}$ is solvable because $\mathfrak{g}^{(n)} = (\mathcal{D}\mathfrak{g})^{(n-1)}$.

Let $x \in [\mathfrak{g},\mathfrak{g}]$, and choose a basis of V for which the matrix of x is upper triangular. Then the matrix of x_s is diagonal, say, $\mathrm{diag}(a_1,\ldots,a_n)$, and the matrix of x_n is strictly upper triangular. We have to show that $x_s = 0$, and for this it suffices to show that

$$\bar{a}_1 a_1 + \cdots + \bar{a}_n a_n = 0$$

where $\bar{a}$ is the complex conjugate of a. Note that

$$\mathrm{Tr}_V(\bar{x}_s \circ x) = \bar{a}_1 a_1 + \cdots + \bar{a}_n a_n,$$

because $\bar{x}_s$ has matrix $\mathrm{diag}(\bar{a}_1,\ldots,\bar{a}_n)$. By assumption, x is a sum of commutators $[y,z]$, and so it suffices to show that

$$\mathrm{Tr}_V(\bar{x}_s \circ [y,z]) = 0, \quad \text{all } y,z \in \mathfrak{g}.$$

From the trivial identity (32), we see that it suffices to show that

$$\mathrm{Tr}_V([\bar{x}_s, y]\circ z) = 0, \quad \text{all } y,z \in \mathfrak{g}. \tag{33}$$

This will follow from the hypothesis once we have shown that $[\bar{x}_s, y] \in \mathfrak{g}$. According to (1.23(b)),

$$\bar{x}_s = c_1 x + c_2 x^2 + \cdots + c_r x^r, \text{ for some } c_i \in k,$$

and so

$$[\bar{x}_s, \mathfrak{g}] \subset \mathfrak{g}$$

because $[x,\mathfrak{g}] \subset \mathfrak{g}$. □

COROLLARY 3.18 *Let V be a finite-dimensional vector space over a field k of characteristic zero, and let $\mathfrak{g}$ be a subalgebra of $\mathfrak{gl}_V$. If $\mathfrak{g}$ is solvable, then $\mathrm{Tr}_V(x \circ y) = 0$ for all $x \in \mathfrak{g}$ and $y \in [\mathfrak{g},\mathfrak{g}]$. Conversely, if $\mathrm{Tr}_V(x \circ y) = 0$ for all $x, y \in [\mathfrak{g},\mathfrak{g}]$, then $\mathfrak{g}$ is solvable.*

PROOF. If $\mathfrak{g}$ is solvable, then $\mathrm{Tr}_V(x \circ y) = 0$ for $x \in \mathfrak{g}$ and $y \in [\mathfrak{g},\mathfrak{g}]$ (by 3.10). For the converse, note that the condition implies that $[\mathfrak{g},\mathfrak{g}]$ is solvable by (3.17). But this implies that $\mathfrak{g}$ is solvable, because $\mathfrak{g}^{(n)} = (\mathcal{D}\mathfrak{g})^{(n-1)}$. □

In the language of the next section, Cartan's criterion says that a Lie algebra is solvable if the trace form of some faithful representation is zero.

ASIDE 3.19 In the above proofs, it is possible to avoid passing to the case $k=\mathbb{C}$. Roughly speaking, instead of complex conjugation, one uses the elements of the dual of the subspace of k generated by the eigenvalues of x_s. See, for example, Humphreys 1972, 4.3. Alternatively, see the proof in Casselman, Introduction to Lie algebras, 14.4 (following Jacobson).

4 Semisimple Lie algebras

In this section, all Lie algebras and representations are finite-dimensional over a field k of characterstic zero.

Definitions and basic properties

DEFINITION 4.1 A Lie algebra is ***semisimple*** if its only commutative ideal is $\{0\}$.

Thus, the Lie algebra $\{0\}$ is semisimple, but no Lie algebra of dimension 1 or 2 is semisimple. There exists a semisimple Lie algebra of dimension 3, namely, $\mathfrak{sl}_2$ (see 4.9 below).

Recall (3.6) that every Lie algebra $\mathfrak{g}$ contains a largest solvable ideal $r(\mathfrak{g})$, called its radical.

4.2 *A Lie algebra $\mathfrak{g}$ is semisimple if and only if its radical is zero.*

If $r(\mathfrak{g})=0$, then every commutative ideal is zero because it is contained in $r(\mathfrak{g})$. Conversely, if $r(\mathfrak{g})\neq 0$, then the last nonzero term of the derived series of $r(\mathfrak{g})$ is a commutative ideal in $\mathfrak{g}$ (it is an ideal in $\mathfrak{g}$ because it is a characteristic ideal in $r(\mathfrak{g})$).

4.3 *A Lie algebra $\mathfrak{g}$ is semisimple if and only if every solvable ideal is zero.*

Since $r(\mathfrak{g})$ is the largest solvable ideal, it is zero if and only if every solvable ideal is zero.

4.4 *The quotient $\mathfrak{g}/r(\mathfrak{g})$ of a Lie algebra by its radical is semisimple.*

A nonzero commutative ideal in $\mathfrak{g}/r(\mathfrak{g})$ would correspond to a solvable ideal in $\mathfrak{g}$ properly containing $r(\mathfrak{g})$.

4.5 *A product $\mathfrak{g}=\mathfrak{g}_1\times\cdots\times\mathfrak{g}_n$ of semisimple Lie algebras is semisimple.*

Let $\mathfrak{a}$ be a commutative ideal in $\mathfrak{g}$; the projection of $\mathfrak{a}$ in $\mathfrak{g}_i$ is zero for each i, and so $\mathfrak{a}$ is zero.

Trace forms

Let $\mathfrak{g}$ be a Lie algebra. A symmetric k-bilinear form $\beta\colon \mathfrak{g}\times\mathfrak{g}\to k$ on $\mathfrak{g}$ is said to be ***invariant*** (or ***associative***) if

$$\beta([x,y],z)=\beta(x,[y,z]) \quad \text{for all } x,y,z\in\mathfrak{g},$$

that is, if

$$\beta([x,y],z)+\beta(y,[x,z])=0 \quad \text{for all } x,y,z\in\mathfrak{g}.$$

In other words, β is invariant if

$$\beta(Dy,z)+\beta(y,Dz)=0 \tag{34}$$

for all inner derivations D of $\mathfrak{g}$. If (34) holds for all derivations, then β is said to be ***completely invariant*** (Bourbaki LIE, I, §3, 6).

LEMMA 4.6 *Let β be an invariant form on $\mathfrak{g}$, and let $\mathfrak{a}$ be an ideal in $\mathfrak{g}$. The orthogonal complement $\mathfrak{a}^{\perp}$ of $\mathfrak{a}$ with respect to β is again an ideal. If β is nondegenerate, then $\mathfrak{a}\cap\mathfrak{a}^{\perp}$ is commutative.*

PROOF. Let $a\in\mathfrak{a}$, $a'\in\mathfrak{a}^{\perp}$, and $x\in\mathfrak{g}$, and consider

$$\beta([x,a],a')+\beta(a,[x.a'])=0.$$

As $[x,a]\in\mathfrak{a}$, $\beta([x,a],a')=0$. Therefore $\beta(a,[x,a'])=0$. As this holds for all $a\in\mathfrak{a}$, we see that $[x,a']\in\mathfrak{a}^{\perp}$, and so $\mathfrak{a}^{\perp}$ is an ideal.

Now assume that β is nondegenerate. Then $\mathfrak{b}\overset{\text{def}}{=}\mathfrak{a}\cap\mathfrak{a}^{\perp}$ is an ideal in $\mathfrak{g}$ such that $\beta|\mathfrak{b}\times\mathfrak{b}=0$. For $b,b'\in\mathfrak{b}$ and $x\in\mathfrak{g}$, $\beta([b,b'],x)=\beta(b,[b',x])$, which is zero because $[b',x]\in\mathfrak{b}$. As this holds for all $x\in\mathfrak{g}$, we see that $[b,b']=0$, and so $\mathfrak{b}$ is commutative. □

The ***trace form*** of a representation (V,ρ) of $\mathfrak{g}$ is

$$(x,y)\mapsto \mathrm{Tr}_V(\rho(x)\circ\rho(y))\colon \mathfrak{g}\times\mathfrak{g}\to k.$$

In other words, the trace form $\beta_V\colon\mathfrak{g}\times\mathfrak{g}\to k$ of a $\mathfrak{g}$-module V is

$$(x,y)\mapsto \mathrm{Tr}_V(x_V\circ y_V), \quad x,y\in\mathfrak{g}.$$

LEMMA 4.7 *The trace form is a symmetric bilinear form on $\mathfrak{g}$, and it is invariant:*

$$\beta_V([x,y],z)=\beta_V(x,[y,z]), \quad \textit{all } x,y,z\in\mathfrak{g}.$$

PROOF. It is k-bilinear because ρ is linear, composition of maps is bilinear, and traces are linear. It is symmetric because traces are symmetric (31). It is invariant because

$$\beta_V([x,y],z)=\mathrm{Tr}([x,y]\circ z)\overset{(32)}{=}\mathrm{Tr}(x\circ[y,z])=\beta_V(x,[y,z])$$

for all $x,y,z\in\mathfrak{g}$. □

Therefore (see 4.6), the orthogonal complement $\mathfrak{a}^{\perp}$ of an ideal $\mathfrak{a}$ of $\mathfrak{g}$ with respect to a trace form is again an ideal.

PROPOSITION 4.8 *If $\mathfrak{g} \to \mathfrak{gl}_V$ is faithful and $\mathfrak{g}$ is semisimple, then β_V is nondegenerate.*

PROOF. We have to show that $\mathfrak{g}^{\perp} = 0$. For this, it suffices to show that $\mathfrak{g}^{\perp}$ is solvable (see 4.3), but the pairing

$$(x, y) \mapsto \mathrm{Tr}_V(x_V \circ y_V) \overset{\text{def}}{=} \beta_V(x, y)$$

is zero on $\mathfrak{g}^{\perp}$, and so Cartan's criterion (3.17) shows that it is solvable. □

The Cartan's criterion for semisimplicity

The trace form for the adjoint representation $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$ is called the ***Killing form***[5] $\kappa_{\mathfrak{g}}$ on $\mathfrak{g}$. Thus,

$$\kappa_{\mathfrak{g}}(x, y) = \mathrm{Tr}_{\mathfrak{g}}(\mathrm{ad}(x) \circ \mathrm{ad}(y)), \quad \text{all } x, y \in \mathfrak{g}.$$

In other words, $\kappa_{\mathfrak{g}}(x, y)$ is the trace of the k-linear map

$$z \mapsto [x, [y, z]]\colon \mathfrak{g} \to \mathfrak{g}.$$

EXAMPLE 4.9 The Lie algebra $\mathfrak{sl}_2$ consists of the 2×2 matrices with trace zero. It has as basis the elements[6]

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and

$$[h, x] = 2x, \quad [h, y] = -2y, \quad [x, y] = h.$$

Relative to the basis $\{x, y, h\}$,

$$\mathrm{ad}\, x = \begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mathrm{ad}\, h = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \mathrm{ad}\, y = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

and so the top row $(\kappa(x, x), \kappa(x, h), \kappa(x, y))$ of the matrix of κ consists of the traces of

$$\begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In fact, κ has matrix $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 0 \end{pmatrix}$, which has determinant -128.

Note that, for $\mathfrak{sl}_n$, the matrix of κ is $n^2 - 1 \times n^2 - 1$, and so this is not something one would like to compute by writing out matrices.

[5] Also called the ***Cartan-Killing form***. According to Bourbaki (Note Historique to I, II, III), Cartan introduced the "Killing form" in his thesis and proved the two fundamental criteria: a Lie algebra is solvable if its Killing form is trivial (4.12); a Lie algebra is semisimple if its Killing form is nondegenerate (4.13). However, according to Helgason 1990, Killing introduced "the roots of $\mathfrak{g}$, which are by his definition the roots of the characteristic equation $\det(\lambda I - \mathrm{ad}\, X) = 0$. Twice the second coefficient in this equation, which equals $\mathrm{Tr}(\mathrm{ad}\, X)^2$, is now customarily called the Killing form. However, Cartan made much more use of it.... While $\mathrm{Tr}(\mathrm{ad}\, X)^2$ is nowadays called the Killing form and the matrix (a_{ij}) called the Cartan matrix... it would have been reasonable on historical grounds to interchange the names." See also Hawkins 2000, 6.2, and mo32554 (james-parsons).

[6] Some authors write (h, e, f) for (h, x, y). Bourbaki writes (H, X, Y) for (h, x, y) in LIE, I, §6, 7, and $(H, X_+, -X_-)$ in VIII, §1, 1, *Base canonique de* $\mathfrak{sl}_2$, i.e., $X_- = \left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right)$.

LEMMA 4.10 *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. If an endomorphism of a vector space V maps V into a subspace W of V, 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 α takes the form $\left(\begin{smallmatrix} A & B \\ 0 & 0 \end{smallmatrix}\right)$ with A 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 $\mathfrak{g}$), $\kappa_{\mathfrak{g}}(x,y)$, equals

$$\mathrm{Tr}_{\mathfrak{a}}(\mathrm{ad}\, x \circ \mathrm{ad}\, y|_{\mathfrak{a}}) = \mathrm{Tr}_{\mathfrak{a}}(\mathrm{ad}_{\mathfrak{a}}\, x \circ \mathrm{ad}_{\mathfrak{a}}\, y) = \kappa_{\mathfrak{a}}(x,y).$$ □

EXAMPLE 4.11 For matrices $X, Y \in \mathfrak{sl}_n$,

$$\kappa_{\mathfrak{sl}_n}(X,Y) = 2n\,\mathrm{Tr}(XY).$$

To prove this, it suffices to show that

$$\kappa_{\mathfrak{gl}_n}(X,Y) = 2n\,\mathrm{Tr}(XY)$$

for $X,Y \in \mathfrak{sl}_n$. By definition, $\kappa_{\mathfrak{gl}_n}(X,Y)$ is the trace of the map $M_n(k) \to M_n(k)$ sending $T \in M_n(k)$ to

$$XYT - XTY - YTX + TYX.$$

For any matrix A, the trace of each of the maps $l_A\colon T \mapsto AT$ and $r_A\colon T \mapsto TA$ is $n\,\mathrm{Tr}(A)$, because, as a left or right $M_n(k)$-module, $M_n(k)$ is isomorphic to a direct sum of n-copies of the standard $M_n(k)$-module k^n. Therefore, the traces of the maps $T \mapsto XYT$ and $T \mapsto TXY$ are both $n\,\mathrm{Tr}(XY)$, while the traces of the maps $T \mapsto XTY$ and $T \mapsto YTX$ are both equal to

$$\mathrm{Tr}(l_X \circ r_Y) = n^2\,\mathrm{Tr}(X)\,\mathrm{Tr}(Y) = 0.$$

PROPOSITION 4.12 *If $\kappa_{\mathfrak{g}}(\mathfrak{g},[\mathfrak{g},\mathfrak{g}]) = 0$, then $\mathfrak{g}$ is solvable; in particular, $\mathfrak{g}$ is solvable if its Killing form is zero.*

PROOF. Cartan's criterion for solvability (3.18) applied to the adjoint representation $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$ shows that $\mathrm{ad}(\mathcal{D}\mathfrak{g})$ is solvable. Hence $\mathcal{D}\mathfrak{g}$ is solvable, and so $\mathfrak{g}$ is solvable. □

THEOREM 4.13 *(Cartan criterion). A nonzero Lie algebra $\mathfrak{g}$ is semisimple if and only if its Killing form is nondegenerate.*

PROOF. $\Rightarrow$: Because $\mathfrak{g}$ is semisimple, the adjoint representation $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}$ is faithful, and so this follows from (4.8).

$\Leftarrow$: Let $\mathfrak{a}$ be a commutative ideal of $\mathfrak{g}$ — we have to show that $\mathfrak{a} = 0$. For any $a \in \mathfrak{a}$ and $g \in \mathfrak{g}$, we have that

$$\mathfrak{g} \xrightarrow{\mathrm{ad}\, g} \mathfrak{g} \xrightarrow{\mathrm{ad}\, a} \mathfrak{a} \xrightarrow{\mathrm{ad}\, g} \mathfrak{a} \xrightarrow{\mathrm{ad}\, a} 0,$$

and so $(\mathrm{ad}\, a \circ \mathrm{ad}\, g)^2 = 0$. But an endomorphism of a vector space whose square is zero has trace zero (because its minimum polynomial divides X^2). Therefore

$$\kappa_{\mathfrak{g}}(a,g) \stackrel{\text{def}}{=} \mathrm{Tr}_{\mathfrak{g}}(\mathrm{ad}\, a \circ \mathrm{ad}\, g) = 0,$$

and $\mathfrak{a} \subset \mathfrak{g}^{\perp} = 0$. □

We say that an ideal in a Lie algebra is semisimple if it is semisimple as a Lie algebra.

COROLLARY 4.14 *For any semisimple ideal* $\mathfrak{a}$ *in a Lie algebra* $\mathfrak{g}$ *and its orthogonal complement* $\mathfrak{a}^{\perp}$ *with respect to the Killing form*

$$\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}.$$

PROOF. Because $\kappa_{\mathfrak{g}}$ is invariant, $\mathfrak{a}^{\perp}$ is an ideal. Now $\kappa_{\mathfrak{g}}|\mathfrak{a} = \kappa_{\mathfrak{a}}$ (4.6), which is nondegenerate. Hence $\mathfrak{a} \cap \mathfrak{a}^{\perp} = 0$. □

COROLLARY 4.15 *Let* $\mathfrak{g}$ *be a Lie algebra over a field* k*, and let* k' *be a field containing* k*.*

(a) *The Lie algebra* $\mathfrak{g}$ *is semisimple if and only if* $\mathfrak{g}_{k'}$ *is semisimple.*
(b) *The radical* $r(\mathfrak{g}_{k'}) \simeq k' \otimes_k r(\mathfrak{g})$*.*

PROOF. (a) The Killing form of $\mathfrak{g}_{k'}$ is obtained from that of $\mathfrak{g}$ by extension of scalars.
(b) The exact sequence

$$0 \to r(\mathfrak{g}) \to \mathfrak{g} \to \mathfrak{g}/r(\mathfrak{g}) \to 0$$

gives rise to an exact sequence

$$0 \to r(\mathfrak{g})_{k'} \to \mathfrak{g}_{k'} \to (\mathfrak{g}/r(\mathfrak{g}))_{k'} \to 0.$$

As $r(\mathfrak{g})_{k'}$ is solvable (3.3) and $(\mathfrak{g}/r(\mathfrak{g}))_{k'}$ is semisimple, the sequence shows that $r(\mathfrak{g})_{k'}$ is the largest solvable ideal in $\mathfrak{g}_{k'}$, i.e., that $r(\mathfrak{g})_{k'} = r(\mathfrak{g}_{k'})$. □

The decomposition of semisimple Lie algebras

DEFINITION 4.16 A Lie algebra $\mathfrak{g}$ is ***simple*** if it is noncommutative and its only ideals are $\{0\}$ and $\mathfrak{g}$.

For example, $\mathfrak{sl}_n$ is simple for $n \geq 2$ (see p.92 below).

Clearly a simple Lie algebra is semisimple, and so a product of simple Lie algebras is semisimple (by 4.5).

Let $\mathfrak{g}$ be a Lie algebra, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be ideals in $\mathfrak{g}$. If $\mathfrak{g}$ is a direct sum of the $\mathfrak{a}_i$ as k-subspaces,

$$\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r,$$

then $[\mathfrak{a}_i, \mathfrak{a}_j] \subset \mathfrak{a}_i \cap \mathfrak{a}_j = 0$ for $i \neq j$, and so $\mathfrak{g}$ is a direct product of the $\mathfrak{a}_i$ as Lie subalgebras,

$$\mathfrak{g} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r.$$

A minimal nonzero ideal in a Lie algebra is either commutative or simple. As a semisimple Lie algebra has no commutative ideals, its minimal nonzero ideals are simple Lie algebras.

THEOREM 4.17 *A semisimple Lie algebra* $\mathfrak{g}$ *has only finitely many minimal nonzero ideals* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$*, and*

$$\mathfrak{g} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r.$$

Every ideal in $\mathfrak{a}$ *is a direct product of the* $\mathfrak{a}_i$ *that it contains.*

In particular, a Lie algebra is semisimple if and only if it is isomorphic to a product of simple Lie algebras.

PROOF. Let $\mathfrak{a}$ be an ideal in $\mathfrak{g}$. Then the orthogonal complement $\mathfrak{a}^{\perp}$ of $\mathfrak{a}$ is also an ideal (4.6), and so $\mathfrak{a} \cap \mathfrak{a}^{\perp}$ is an ideal. As its Killing form is zero, $\mathfrak{a} \cap \mathfrak{a}^{\perp}$ is solvable (4.12), and hence zero (4.3). Therefore, $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}$.

If $\mathfrak{g}$ is not simple, then it has a nonzero proper ideal $\mathfrak{a}$. Write $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}$. If one of $\mathfrak{a}$ or $\mathfrak{a}^{\perp}$ is not simple (as a Lie subalgebra), then we can decompose again. Eventually,

$$\mathfrak{g} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$$

with the $\mathfrak{a}_i$ simple (hence minimal) ideals.

Let $\mathfrak{a}$ be a minimal nonzero ideal in $\mathfrak{g}$. Then $[\mathfrak{g}, \mathfrak{a}]$ is an ideal contained in $\mathfrak{a}$, which is nonzero because $z(\mathfrak{g}) = 0$, and so $[\mathfrak{g}, \mathfrak{a}] = \mathfrak{a}$. On the other hand,

$$[\mathfrak{g}, \mathfrak{a}] = [\mathfrak{a}_1, \mathfrak{a}] \oplus \cdots \oplus [\mathfrak{a}_r, \mathfrak{a}],$$

and so $\mathfrak{a} = [\mathfrak{a}_i, \mathfrak{a}] \subset \mathfrak{a}_i$ for exactly one i; then $\mathfrak{a} = \mathfrak{a}_i$ (simplicity of $\mathfrak{a}_i$). This shows that $\{\mathfrak{a}_1, \ldots \mathfrak{a}_r\}$ is a complete set of minimal nonzero ideals in $\mathfrak{g}$.

Let $\mathfrak{a}$ be an ideal in $\mathfrak{g}$. A similar argument shows that $\mathfrak{a}$ is a direct sum of the minimal nonzero ideals contained in $\mathfrak{a}$. □

COROLLARY 4.18 *All nonzero ideals and quotients of a semisimple Lie algebra are semisimple.*

PROOF. Any such Lie algebra is a product of simple Lie algebras, and so is semisimple. □

COROLLARY 4.19 *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 true also for direct sums of simple algebras. □

REMARK 4.20 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.

Derivations of a semisimple Lie algebra

Recall that $\mathrm{Der}_k(\mathfrak{g})$ is the space of k-linear endomorphisms of $\mathfrak{g}$ satisfying the Leibniz condition

$$D([x, y]) = [D(x), y] + [x, D(y)].$$

The bracket

$$[D, D'] = D \circ D' - D' \circ D$$

makes it into a Lie algebra.

LEMMA 4.21 *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. We have to show that, for any derivation D of $\mathfrak{g}$ and $x \in \mathfrak{g}$, the derivation $[D, \mathrm{ad}\, x]$ is inner. For any $y \in \mathfrak{g}$,

$$\begin{aligned} [D, \mathrm{ad}\, x](y) &= (D \circ \mathrm{ad}\, x - \mathrm{ad}\, x \circ D)(y) \\ &= D([x, y]) - [x, D(y)] \\ &= [D(x), y] + [x, D(y)] - [x, D(y)] \\ &= [D(x), y]. \end{aligned}$$

Therefore

$$[D, \mathrm{ad}(x)] = \mathrm{ad}\, D(x), \tag{35}$$

which is inner. □

THEOREM 4.22 *Every derivation of a semisimple Lie algebra* $\mathfrak{g}$ *is inner; therefore the map* $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ *is an isomorphism.*

PROOF. Let $\mathrm{ad}\,\mathfrak{g}$ denote the (isomorphic) image of $\mathfrak{g}$ in $\mathrm{Der}(\mathfrak{g})$, and let $(\mathrm{ad}\,\mathfrak{g})^{\perp}$ denote its orthogonal complement for the Killing form on $\mathrm{Der}(\mathfrak{g})$. It suffices to show that $(\mathrm{ad}\,\mathfrak{g})^{\perp} = 0$.

We have

$$[(\mathrm{ad}\,\mathfrak{g})^{\perp}, \mathrm{ad}\,\mathfrak{g}] \subset (\mathrm{ad}\,\mathfrak{g})^{\perp} \cap \mathrm{ad}\,\mathfrak{g} = 0$$

because $\mathrm{ad}\,\mathfrak{g}$ and $(\mathrm{ad}\,\mathfrak{g})^{\perp}$ are ideals in $\mathrm{Der}(\mathfrak{g})$ (4.21, 4.6) and $\kappa_{\mathrm{Der}(\mathfrak{g})}|\mathrm{ad}\,\mathfrak{g} = \kappa_{\mathrm{ad}\,\mathfrak{g}}$ is nondegenerate (4.13). Therefore

$$\mathrm{ad}(Dx) \overset{(35)}{=} [D, \mathrm{ad}(x)] = 0$$

if $D \in (\mathrm{ad}\,\mathfrak{g})^{\perp}$ and $x \in \mathfrak{g}$. As $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ is injective,

$$\mathrm{ad}(Dx) = 0 \quad \text{for all } x \implies Dx = 0 \quad \text{for all } x \implies D = 0.$$

□

5 Representations of Lie algebras: Weyl's theorem

In this section, all Lie algebras and all representations are finite dimensional over a field k. The main result is Weyl's theorem saying that the finite-dimensional representations of a semisimple Lie algebra in characteristic zero are semisimple.

Preliminaries on semisimplicity

Let k be a field, and let A be a k-algebra (either associative or a Lie algebra).

Semisimple modules

An A-module is ***simple*** if it does not contain a nonzero proper submodule.

PROPOSITION 5.1 *The following conditions on an A-module M of finite dimension 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. For a set J of simple submodules of M, let $N(J) = \sum_{S \in J} S$. Let J be maximal among the sets of simple submodules 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). □

ASIDE 5.2 The proposition holds without the hypothesis "of finite dimension over k", but then the proof requires Zorn's lemma to show that there exists a set J maximal for the properties (i) and (ii).

DEFINITION 5.3 An A-module is ***semisimple*** if it satisfies the equivalent conditions of the proposition.

LEMMA 5.4 (SCHUR'S LEMMA) *If V is a simple A-module of finite dimension over k and k is algebraically closed, then* $\mathrm{End}_A(V) = k$.

PROOF. Let $\alpha: V \to V$ be A-homomorphism of V. Because k is algebraically closed, α has an eigenvector, say, $\alpha(v) = cv$, $c \in k$. Now $\alpha - c: V \to V$ is an A-homomorphism with nonzero kernel. Because V is simple, the kernel must equal V. Hence $\alpha = c$. □

ASIDE 5.5 The results of this section hold in every k-linear abelian category whose objects have finite length.

Semisimple rings

In this subsubsection, all k-algebras are associative and finite (i.e., finite-dimensional as a k-vector space), and all modules over such a k-algebra are finite-dimensional as k-vector spaces.

DEFINITION 5.6 A k-algebra A is ***simple*** if it has no two-sided ideals except 0 and A.

PROPOSITION 5.7 *A k-algebra A is simple if and only if it is isomorphic to a matrix algebra $M_n(D)$ over a division algebra D.*

PROOF. This is a theorem of Wedderburn (GT 7.16, 7.23). □

DEFINITION 5.8 A k-algebra A is ***semisimple*** if every A-module is semisimple.

It suffices to check that ${}_AA$ is semisimple, because every A-module is a quotient of a finite direct sum of copies of ${}_AA$.

PROPOSITION 5.9 *The following conditions on a k-algebra A are equivalent:*

(a) *A is semisimple;*
(b) *A is a product of simple k-algebras;*
(c) *the Jacobson radical $R(A)$ of A is trivial.*

PROOF. The equivalence of (a) and (b) is another theorem of Wedderburn (GT 7.34). The elements of $J(A)$ act trivially on simple A-modules (see 2.16), and hence on semisimple A-modules. Therefore (a) implies (c). Finally, (c) implies that A acts faithfully on a finite direct sum M of simple A-modules, and so ${}_AA$ is a submodule of $\mathrm{End}(M)$, which is semisimple. □

The centre of a simple k-algebra is a commutative simple k-algebra, which is a field.

PROPOSITION 5.10 *Let A be a simple k-algebra with centre C. For any field K containing C, $K \otimes_C A$ is a simple K-algebra with centre K.*

PROOF. See my notes Class Field Theory, IV, 2.15 (for the moment). □

PROPOSITION 5.11 *Let A be a k-algebra. If $K \otimes_k A$ is semisimple for some field K containing k, then A is semisimple; conversely, if A is semisimple, then $K \otimes_k A$ is semisimple for all fields K separable over k.*

PROOF. Suppose that $K \otimes_k A$ is semisimple, and let $x \in R(A)$. Then $\mathfrak{n} = Ax$ is a left nilideal in A, and $K \otimes_k \mathfrak{n}$ is a left nilideal in $K \otimes_k A$. Therefore $K \otimes_k \mathfrak{n} \subset R(K \otimes_k A)$ (see 2.18), which is zero, and so $\mathfrak{n} = 0$. Hence $R(A) = 0$.

Conversely, suppose that A is semisimple. We may replace A with one of its factors, and so assume that it is simple. Let C be the centre of A — it is a finite field extension of k. For any separable field extension K of k, $K \otimes_k C$ is a product of fields,[7] say $\prod K_i$, and

$$\begin{aligned} K \otimes_k A &\simeq K \otimes_k (C \otimes_C A) \\ &\simeq (K \otimes_k C) \otimes_C A \\ &\simeq \prod\nolimits_i K_i \otimes_C A, \end{aligned}$$

which is a product of simple k-algebras (see 5.10). □

[7]Let $K = k[\alpha]$, and let $f(X)$ be the minimum polynomial of α. Then $f(X)$ has distinct roots in C^{al}, and so its monic irreducible factors, $f_1, \ldots, f_r$, in $C[X]$ are relatively prime. Therefore

$$K \otimes_k C \simeq (k[X]/(f)) \otimes_k C \simeq C[X]/(f) \simeq \prod C[X]/(f_i),$$

which is a product of fields (we used the Chinese remainder theorem in the last step).

ASIDE 5.12 A k-algebra A is ***separable*** if $L \otimes_k A$ is semisimple for all fields L containing k. The above arguments show that A is separable if and only if it is a product of simple k-algebras whose centres are separable over k. Note that C is automatically separable over k if k has characteristic zero, or if it has characteristic $p \neq 0$ and $[C:k] < p$.

Semisimple categories

Let M be a left A-module. The ***ring of homotheties*** of M is

$$A_M = \{a_M \mid a \in A\},$$

i.e., it is the image of A in $\mathrm{End}_{\mathbb{Z}\text{-linear}}(M)$.

PROPOSITION 5.13 *Let M be an A-module which is finitely generated when regarded as an $\mathrm{End}_A(M)$-module. The ring A_M of homotheties of M is semisimple if and only if M is semisimple.*

PROOF. If A_M is semisimple, then M is semisimple as an A_M-module, and hence as an A-module. Conversely, let $B = A_M$ and let $(e_i)_{i \in I}$ be a family of generators for A as an $\mathrm{End}_A(M)$-module. Then

$$b \mapsto (be_i)_{i \in I} \colon_B B \to M^I$$

is an injective homomorphism of left B-modules, and so ${}_B B$ is a semisimple B-module if M is. □

The reader can take A in the next proposition to be $\mathsf{Rep}(\mathfrak{g})$ (see below).

PROPOSITION 5.14 *Let A be a k-linear abelian category such that $\mathrm{End}(X)$ is finite-dimensional over k for all objects X. Then A is semisimple if and only if $\mathrm{End}(X)$ is a semisimple k-algebra for all X.*

PROOF. Assume that A is semisimple. Every object X is the finite direct sum $X = \bigoplus_i m_i S_i$ of its isotypic subobjects $m_i S_i$: this means that each object S_i is simple, and S_i is not isomorphic to S_j if $i \neq j$. Because S_i is simple, $\mathrm{End}(S_i)$ is a division algebra, and because $\mathrm{End}(X) = \prod_i M_{m_i}(S_i)$, it is semisimple (5.9).

Conversely, assume that $\mathrm{End}(X)$ is semisimple for all X. Then $\mathrm{End}(X)$ is a product of matrix algebras over division algebras, and X can only be indecomposable if $\mathrm{End}(X)$ is a division algebra.

Let $f\colon M \to N$ be a map of indecomposable objects. If there exists a map $g\colon N \to M$ such that $g \circ f \neq 0$, then $g \circ f$ is an automorphism of M and $(g \circ f)^{-1} \circ g$ is a right inverse to f, which implies that M is a direct summand of N; as N is indecomposable, f is an isomorphism. Similarly, f is an isomorphism if there exists a map $g\colon N \to M$ such $f \circ g \neq 0$.

As each object is obviously a sum of indecomposable objects, it suffices to show that each indecomposable object N is simple. If N is not simple, then it properly contains an indecomposable object M, and

$$\begin{pmatrix} 0 & 0 \\ \mathrm{Hom}(M,N) & 0 \end{pmatrix} \subset \begin{pmatrix} \mathrm{End}(M) & \mathrm{Hom}(N,M) \\ \mathrm{Hom}(M,N) & \mathrm{End}(N) \end{pmatrix} = \mathrm{End}(M \oplus N)$$

is a two-sided ideal by the above remark. As it is nilpotent and nonzero, this contradicts the semisimplicity of $\mathrm{End}(M \oplus N)$. □

ASIDE 5.15 For (6.14), need to add the proof of Bourbaki A, VIII, §9, 2, Thm 1: Let $\mathcal{E}$ be a set of commuting endomorphisms of a vector space, and let A be the k-subalgebra of $\mathrm{End}(V)$ generated by them; then A is étale $\iff$ $\mathcal{E}$ is absolutely semisimple $\iff$ every element of $\mathcal{E}$ is absolutely semisimple.

For (6.15), need to add the proof of Bourbaki A, VIII, §9, Corollary to Theorem 1: The sum and product of two commuting absolutely semisimple endomorphisms of a vector space are absolutely semisimple.

Extension of the base field

For a Lie algebra $\mathfrak{g}$ over a field k, $\mathsf{Rep}(\mathfrak{g})$ denotes the category of representations of $\mathfrak{g}$ on finite-dimensional k-vector spaces.

PROPOSITION 5.16 *If $\mathsf{Rep}(\mathfrak{g}_K)$ is semisimple for some field K containing k, then so also is $\mathsf{Rep}(\mathfrak{g})$.*

PROOF. Assume that $\mathsf{Rep}(\mathfrak{g}_K)$ is semisimple. For any representation (V,ρ) of $\mathfrak{g}$,

$$K \otimes \mathrm{End}(V,\rho) \simeq \mathrm{End}(V_K,\rho_K),$$

because

$$K \otimes \mathrm{End}(V) \simeq \mathrm{End}(V_K),$$

and the condition that a linear map $V \to V$ be $\mathfrak{g}$-equivariant is linear. As $\mathsf{Rep}(\mathfrak{g}_K)$ is semisimple, the K-algebra $K \otimes \mathrm{End}(V,\rho)$ is semisimple (5.14), which implies that $\mathrm{End}(V,\rho)$ is semismple (5.11). As this holds for all representations of $\mathfrak{g}$, (5.14) shows that $\mathsf{Rep}(\mathfrak{g})$ is semisimple. □

NOTES With only a little more effort, one can prove the following more precise results (see the next version of the notes). Let (V,ρ) be a representation of a Lie algebra $\mathfrak{g}$.

(a) If (V_K,ρ_K) is semisimple for some field K containing k, then (V,ρ) is semismple.

(b) If (V,ρ) is semisimple, then (V_K,ρ_K) is semisimple for every separable field extension K/k.

(c) Suppose k has characteristic $p \neq 0$. If (V,ρ) is simple and $\dim(V) < p$, then (V_K,ρ_K) is semisimple for every field extension K/k (cf. 1.5 of Serre, Jean-Pierre Sur la semi-simplicité des produits tensoriels de représentations de groupes. Invent. Math. 116 (1994), no. 1-3, 513–530).

Casimir operators

Throughout this subsection, $\mathfrak{g}$ is a semisimple Lie algebra of dimension n.

Let $\beta\colon \mathfrak{g}\times\mathfrak{g} \to k$ be a nondegenerate invariant bilinear form on $\mathfrak{g}$. Let $e_1,\ldots,e_n$ be a basis for $\mathfrak{g}$ as a k-vector space, and let $e'_1,\ldots,e'_n$ be the dual basis (so $\beta(e_i,e'_j) = \delta_{ij}$ for all $i.j$). For $x \in \mathfrak{g}$, write

$$[e_i,x] = \textstyle\sum_{j=1}^n a_{ij}e_j$$
$$[x,e'_i] = \textstyle\sum_{j=1}^n b_{ij}e'_j.$$

Then

$$\beta([e_i,x],e'_{i'}) = \sum_{j=1}^{n} a_{ij}\beta(e_j,e'_{i'}) = a_{ii'}$$
$$\beta(e_i,[x,e'_{i'}]) = \sum_{j=1}^{n} b_{i'j}\beta(e_i,e'_j) = b_{i'i}$$

and so $a_{ii'} = b_{i'i}$ (because β is invariant). In other words, for $x \in \mathfrak{g}$,

$$[e_i,x] = \sum_{j=1}^{n} a_{ij}e_j \quad \iff \quad [x,e'_i] = \sum_{j=1}^{n} a_{ji}e'_j. \tag{36}$$

PROPOSITION 5.17 *The element $c = \sum_{i=1}^{n} e_i e'_i$ of $U(\mathfrak{g})$ is independent of the choice of the basis, and lies in the centre of $U(\mathfrak{g})$.*

PROOF. Recall that $V^\vee$ denotes the dual of a k-vector space V, and that the map sending $v \otimes f$ to the map $v' \mapsto f(v')v$ is an isomorphism

$$V \otimes V^\vee \simeq \mathrm{End}(V).$$

Under the maps

$$\mathrm{End}_{k\text{-linear}}(\mathfrak{g}) \simeq \mathfrak{g} \otimes \mathfrak{g}^\vee \overset{\beta}{\simeq} \mathfrak{g} \otimes \mathfrak{g} \subset T(\mathfrak{g}) \twoheadrightarrow U(\mathfrak{g}), \tag{37}$$

$\mathrm{id}_\mathfrak{g}$ corresponds to $\sum_{i=1}^{n} e_i \otimes e'_i$ in $\mathfrak{g} \otimes \mathfrak{g}$, which maps to c in $U(\mathfrak{g})$. This proves the first part of the statement, and for the second, we have to show that $cx - xc = 0$ for all $x \in \mathfrak{g}$. Write

$$cx - xc = \sum_{i=1}^{n} e_i e'_i x - \sum_{i=1}^{n} x e_i e'_i.$$

Now

$$e_i e'_i x = e_i[e'_i,x] + e_i x e'_i$$
$$-x e_i e'_i = [e_i,x]e'_i - e_i x e'_i,$$

and so

$$cx - xc = \sum_{i=1}^{n} e_i[e'_i,x] + \sum_{i=1}^{n} [e_i,x]e'_i.$$

Let $[e_i,x] = \sum_{j=1}^{n} a_{ij}e_j$; then $[x,e'_i] = \sum_{j=1}^{n} a_{ji}e'_j$ by (36), and so

$$\begin{aligned} cx - xc &= \sum_{i,j} \left(-a_{ji}e_i e'_j + a_{ij}e_j e'_i\right) \\ &= \sum_i -a_{ii} + \sum_j a_{jj} \\ &= 0. \end{aligned}$$

□

The trace form $\beta_V\colon \mathfrak{g} \times \mathfrak{g} \to k$ of a faithful representation $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ of $\mathfrak{g}$ is invariant and nondegenerate (4.7, 4.8). The element $c = \sum_{i=1}^{n} e_i e'_i$ of $U(\mathfrak{g})$ defined by β_V is called the ***Casimir element*** of (V,ρ), and

$$c_V = \sum_{i=1}^{n} e_{iV} \circ e'_{iV} \tag{38}$$

is the ***Casimir operator*** of (V,ρ).

PROPOSITION 5.18 *(a) The Casimir operator (38) depends only on* (V,ρ).

(b) The map $c_V\colon V\to V$ *is a* $\mathfrak{g}$*-module homomorphism.*

(c) $\mathrm{Tr}_V(c_V)=\dim\mathfrak{g}$.

PROOF. The first two statements follow directly from (5.17). For (c),

$$\begin{aligned}\mathrm{Tr}_V(c_V)&=\textstyle\sum_{i=1}^{n}\mathrm{Tr}_V(e_i\circ e_i')\\&=\textstyle\sum_{i=1}^{n}\beta_V(e_i,e_i')\\&=\textstyle\sum_{i=1}^{n}\delta_{ii}\\&=n.\end{aligned}$$

□

Note that (c) implies that c_V is an automorphism of the $\mathfrak{g}$-module V if V is simple and n is nonzero in k.

NOTES For a semisimple Lie algebra $\mathfrak{g}$, the Casimir element is defined to be the image in $U(\mathfrak{g})$ of $\mathrm{id}_{\mathfrak{g}}$ under the map (37) determined by the Killing form. It lies in the centre of $U(\mathfrak{g})$ because $\mathrm{id}_{\mathfrak{g}}$ is invariant under the natural action of $\mathfrak{g}$ on $\mathrm{End}(\mathfrak{g})$ and the maps in (37) commute with the action of $\mathfrak{g}$. When $\mathfrak{g}$ is simple, the elements of degree 2 in the centre of $U(\mathfrak{g})$ form a one-dimensional space, and c the unique such element satisfying (5.18c). See mo52587.

Weyl's theorem

LEMMA 5.19 *All one-dimensional representations of a semisimple Lie algebra are trivial.*

PROOF. Let (V,ρ) be a representation of $\mathfrak{g}$. For any bracket $g=[g_1,g_2]$ of $\mathfrak{g}$,

$$\mathrm{Tr}_V(g_V)=\mathrm{Tr}_V([g_1,g_2]_V)=\mathrm{Tr}_V(g_{1V}\circ g_{2V}-g_{2V}\circ g_{1V})=0.$$

Thus, when V is one-dimensional, ρ is trivial on $[\mathfrak{g},\mathfrak{g}]$, but $\mathfrak{g}=[\mathfrak{g},\mathfrak{g}]$ for a semisimple algebra $\mathfrak{g}$ (4.19). □

THEOREM 5.20 (WEYL) *Let* $\mathfrak{g}$ *be a Lie algebra over a field* k.

(a) *If the adjoint representation* $\mathrm{ad}\colon\mathfrak{g}\to\mathfrak{gl}_{\mathfrak{g}}$ *is semisimple, then* $\mathfrak{g}$ *is semisimple.*
(b) *If* $\mathfrak{g}$ *is semisimple and* k *has characteristic zero, then* $\mathsf{Rep}(\mathfrak{g})$ *is semisimple.*

PROOF. (a) For the adjoint representation $\mathrm{ad}\colon\mathfrak{g}\to\mathfrak{gl}_{\mathfrak{g}}$, the $\mathfrak{g}$-submodules of $\mathfrak{g}$ are exactly the ideals in $\mathfrak{g}$. Therefore, if the adjoint representation is semisimple, then every ideal in $\mathfrak{g}$ admits a complementary ideal, and so is a quotient of $\mathfrak{g}$. Hence, if $\mathfrak{g}$ is not semisimple, then it admits a nonzero commutative quotient, and therefore a quotient of dimension 1; but the Lie algebra k of dimension 1 has nonsemisimple representations, for example, $c\mapsto\left(\begin{smallmatrix}0&0\\c&0\end{smallmatrix}\right)$.

(b) After (4.15) and (5.16), we may suppose that k is algebraically closed. Let $\mathfrak{g}$ be a semisimple Lie algebra, which we may suppose to be nonzero, and let $\mathfrak{g}\to\mathfrak{gl}_V$ be a finite-dimensional representation of $\mathfrak{g}$. We have to show that every $\mathfrak{g}$-submodule W of V admits a $\mathfrak{g}$-complement. This we do by induction on $\dim W$.

Assume first that $\dim V/W=1$ *and that* W *is simple.* The first condition implies that $\mathfrak{g}$ acts trivially on V/W (see 5.19). We may replace $\mathfrak{g}$ with its image in $\mathfrak{gl}_V$, and so suppose that $\mathfrak{g}\subset\mathfrak{gl}_V$. Let $c_V\colon V\to V$ be the Casimir operator. As $\mathfrak{g}$ acts trivially on V/W, so also does c_V. On the other hand, c_V acts on W as a scalar a (Schur's lemma 5.4). This scalar is nonzero, because otherwise $\mathrm{Tr}_V\, c_V = 0$, contradicting (5.18c). Therefore, the kernel of c_V is one-dimensional. It is a $\mathfrak{g}$-submodule of V which intersects W trivially, and so it is a $\mathfrak{g}$-complement for W.

Next assume only that $\dim V/W = 1$. If W is simple, we have already proved that it has a $\mathfrak{g}$-complement, and so we may suppose that there is a $\mathfrak{g}$-submodule W' of W with $\dim W > \dim W' > 0$. By induction, the $\mathfrak{g}$-submodule W/W' of V/W' has a complement, which we can write in the form V'/W' with V' a $\mathfrak{g}$-submodule of V containing W':

$$V/W' = W/W' \oplus V'/W'.$$

As $(V/W')/(W/W') \simeq V/W$, the $\mathfrak{g}$-module V'/W' has dimension 1, and so, by induction, $V' = W' \oplus L$ for some line L. Now L is a $\mathfrak{g}$-submodule of V, which intersects W trivially and has complementary dimension, and so is a $\mathfrak{g}$-complement for W.

Finally, we consider the general case, $W \subset V$. The space $\mathrm{Hom}_{k\text{-linear}}(V,W)$ of k-linear maps has a natural $\mathfrak{g}$-module structure:

$$(xf)(v) = x\cdot f(v) - f(x\cdot v)$$

(see 1.20). Let

$$\begin{aligned} V_1 &= \{f \in \mathrm{Hom}_{k\text{-linear}}(V,W) \mid f|W = a\,\mathrm{id}_W \text{ for some } a \in k\} \\ W_1 &= \{f \in \mathrm{Hom}_{k\text{-linear}}(V,W) \mid f|W = 0\}. \end{aligned}$$

They are both $\mathfrak{g}$-submodules of $\mathrm{Hom}_{k\text{-linear}}(V,W)$. As V_1/W_1 has dimension 1, the first part of the proof shows that

$$V_1 = W_1 \oplus L$$

for some one-dimensional $\mathfrak{g}$-submodule L of V_1. Let $L = \langle f\rangle$. Because $\mathfrak{g}$ acts trivially on L (see 5.19),

$$0 = (xf)(v) \overset{\text{def}}{=} x\cdot f(v) - f(x\cdot v), \quad \text{all } x \in \mathfrak{g}, \quad v \in V,$$

which says that f is a $\mathfrak{g}$-homomorphism $V \to W$. As $f|W = a\,\mathrm{id}_W$ with $a \neq 0$, the kernel of f is a $\mathfrak{g}$-complement to W. □

COROLLARY 5.21 *Let (V,ρ) be a representation of a Lie algebra $\mathfrak{g}$, and let $f\colon \mathfrak{g} \to V$ be a k-linear map such that*

$$f([x,y]) = \rho(x)\cdot f(y) - \rho(y)\cdot f(x)$$

for all $x,y \in \mathfrak{g}$. If $\mathfrak{g}$ is semisimple, then there exists a $v_0 \in V$ such that

$$f(x) = \rho(x)(v_0)$$

for all $x \in \mathfrak{g}$.

PROOF. The pair (f,ρ) defines a homomorphism of Lie algebras

$$\mathfrak{g} \to V \rtimes \mathfrak{gl}_V = \mathfrak{af}(V)$$

(see 1.19). When combined with the inverse of the isomorphism

$$w \mapsto (w|V, w(0,1)\colon \mathfrak{h} \to \mathfrak{af}(V)$$

(ibid.), this gives a representation ρ' of $\mathfrak{g}$ on $V' \stackrel{\text{def}}{=} V \oplus k$ under which $\rho'(x)(V') \subset V$ for all $x \in \mathfrak{g}$. If $\mathfrak{g}$ is semisimple, then there exists a line L in V' such that $V' = V \oplus L$ and $\mathfrak{g}$ acts trivially on L (see the second step in the above proof). Let $(-v_0, 1)$ be a nonzero element of L. Then $\rho'(x)(-v_0, 1)) = 0$ for all $x \in \mathfrak{g}$. But $\rho'(x)$ acts as $\rho(x)$ on $V \subset V'$ and maps $(0,1)$ to $f(x)$, and so

$$0 = \rho'(x)(-v_0, 1) = \rho'(x)(-v_0, 0) + \rho'(x)(0,1) = -\rho(x)(v_0) + f(x).$$

Cf. Bourbaki LIE, §6, 2, Remark 2, p53. □

ASIDE 5.22 In the proof that V is semisimple in (b), we used that k has characteristic zero only to deduce that $\mathrm{Tr}_V\, c_V \neq 0$. Therefore the argument works over a field of characteristic p for representations (V,ρ) such that $\dim(\rho(\mathfrak{g}))$ is not divisible by p. Let V_n be the standard $n+1$-dimensional representation of SL_n over $\mathbb{F}_p$. Then V_n is simple for $0 \leq n \leq p-1$, but $V_n \otimes V_{n'}$ is not semisimple when $n + n' \geq p$ (mo57997, mo18280).

ASIDE 5.23 The proof of Weyl's theorem becomes simpler when expressed in terms of Ext's. We have to show that all higher Ext's are zero in the category of $\mathfrak{g}$-modules (equivalently $U(\mathfrak{g})$-modules). The Casimir element c lies in the centre of $U(\mathfrak{g})$ and acts as a nonzero scalar on all simple representations, but (of course) as zero on any $\mathfrak{g}$-module for which the action is trivial. From the isomorphism

$$\mathrm{Ext}^i(V,W) \simeq \mathrm{Ext}^i(k, \underline{\mathrm{Hom}}(V,W))$$

we see that it suffices to show that $\mathrm{Ext}^i(V,W) = 0$ $(i > 0)$ with $V = k$ (trivial action). When W is simple, this follows from the fact that c acts on the group as two different scalars. When $W = k$, it can be proved directly. See mo74689 (Moosbrugger).

ASIDE 5.24 An infinite-dimensional representation of a semisimple Lie algebra, even of $\mathfrak{sl}_2$, need not be semisimple.

ASIDE 5.25 About 1890, Lie and Engel conjectured that the finite-dimensional representations of $\mathfrak{sl}_n(\mathbb{C})$ are semisimple. Weyl's proof of this for all semisimple Lie algebras in 1925 was a major advance. Weyl's proof was global: he showed that the finite-dimensional representations of compact groups are semisimple (because they are unitary), and deduced the similar statement for semisimple Lie algebras over $\mathbb{C}$ by showing that all such algebras all arise from the Lie algebras of compact real Lie groups. The first algebraic proof of the theorem was given by Casimir and van der Waerden in 1935. The proof given here, following Bourbaki, is due to Brauer.[8]

Jordan decompositions in semisimple Lie algebras

In this subsection, the base field k has characteristic zero.

Recall that every endomorphism of a k-vector space has a unique (additive Jordan) decomposition into the sum of a semisimple endomorphism and a commuting nilpotent endomorphism (1.22). For a Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$, the semisimple and nilpotent parts of an element of $\mathfrak{g}$ need not lie in $\mathfrak{g}$ (see 1.25). However, this is true if $\mathfrak{g}$ is semisimple.

PROPOSITION 5.26 *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}_V$. If $\mathfrak{g}$ is semisimple, then it contains the semisimple and nilpotent parts of each of its elements.*

[8] Brauer published his proof in 1936. Bourbaki included in their book a version of a later proof. Only after their book was published did they discover that their argument was the same as that of Brauer (Borel 2001, p.18).

PROOF. We may suppose that k is algebraically closed. For any subspace W of V, let

$$\mathfrak{g}_W = \{\alpha \in \mathfrak{gl}_V \mid \alpha(W) \subset W, \quad \mathrm{Tr}(\alpha|W) = 0\}.$$

Then $\mathfrak{g}_W$ is a Lie subalgebra of $\mathfrak{gl}_V$. If $\mathfrak{g}W \subset W$, then $\mathfrak{g}$ is contained in $\mathfrak{g}_W$, because every element of $\mathfrak{g}$ is a sum of brackets (4.19) and so has trace zero. Therefore $\mathfrak{g}$ is a Lie subalgebra of the Lie algebra

$$\mathfrak{g}^* \stackrel{\text{def}}{=} \mathfrak{n}_{\mathfrak{gl}_V}(\mathfrak{g}) \cap \bigcap \{\mathfrak{g}_W \mid \mathfrak{g}W \subset W\}.$$

If $x \in \mathfrak{g}^*$, then so also do x_s and x_n, because they are polynomials in x without constant term and $\mathrm{ad}(x)_s = \mathrm{ad}(x_s)$ and $\mathrm{ad}(x)_n = \mathrm{ad}(x_n)$ (1.23, 1.24). It therefore suffices to show that $\mathfrak{g}^* = \mathfrak{g}$. As $\mathfrak{g}$ is a semisimple ideal in the Lie algebra $\mathfrak{g}^*$,

$$\mathfrak{g}^* = \mathfrak{g} \oplus \mathfrak{g}^\perp$$

where $\mathfrak{g}^\perp$ is the orthogonal complement of $\mathfrak{g}$ with respect to the Killing form on $\mathfrak{g}^*$ (see 4.14). Let $\alpha \in \mathfrak{g}^\perp$ and let W be a simple $\mathfrak{g}$-submodule of V. Then α acts on W as a scalar (Schur's lemma 5.4), which must be zero because $\alpha|W$ has trace zero (α is in $\mathfrak{g}_W$) and k has characteristic zero. As V is a sum of simple $\mathfrak{g}$-modules (Weyl's theorem 5.20), we see that $\alpha = 0$. □

For $\mathfrak{sl}_n \subset \mathfrak{gl}_n$, the proposition is obvious: let $x = x_s + x_n$ in $\mathfrak{gl}_n$; then $\mathrm{Tr}(x_n) = 0$ automatically, and so x_s has trace zero if x does.

DEFINITION 5.27 An element x of a Lie algebra $\mathfrak{g}$ is ***semisimple*** (resp. ***nilpotent***) if $\rho(x)$ is semisimple (resp. nilpotent) for every representation (V, ρ) of $\mathfrak{g}$, and $x = x_s + x_n$ is a ***Jordan decomposition*** of x if $\rho(x) = \rho(x_s) + \rho(x_n)$ is a Jordan decomposition of $\rho(x)$ for every representation (V, ρ) of $\mathfrak{g}$.

Note that $x = x_s + x_n$ is a Jordan decomposition of x if x_s is semisimple, x_n is nilpotent, and $[x_s, x_n] = 0$.

THEOREM 5.28 *Every element of a semisimple Lie algebra $\mathfrak{g}$ has a unique Jordan decomposition; moreover, $x = x_s + x_n$ is a Jordan decomposition of x if $\rho(x) = \rho(x_s) + \rho(x_n)$ is a Jordan decomposition of $\rho(x)$ for one faithful representation.*

PROOF. Let $x \in \mathfrak{g}$, and let (V, ρ) be a faithful representation of $\mathfrak{g}$ (for example, the adjoint representation). There exists at most one decomposition $x = x_s + x_n$ such that $\rho(x) = \rho(x_s) + \rho(x_n)$ is a Jordan decomposition of $\rho(x)$ (because of the uniqueness in 1.22). This proves the uniqueness.

According to (5.26), there do exist exist $x_s, x_n \in \mathfrak{g}$ such that $\rho(x) = \rho(x_s) + \rho(x_n)$ is the Jordan decomposition of $\rho(x)$. Now (1.24) implies that $\mathrm{ad}(x_s)$ (resp. $\mathrm{ad}(x_n)$) is a semisimple (resp. nilpotent) k-linear endomorphism of $\mathfrak{g} \subset \mathrm{End}(V)$. As they commute, $\mathrm{ad}(x) = \mathrm{ad}(x_s) + \mathrm{ad}(x_n)$ is the Jordan decomposition of $\mathrm{ad}(x)$ as an endomorphism of $\mathfrak{g}$. Because the adjoint representation is faithful, this shows that the decomposition $x = x_s + x_n$ is independent of ρ. Every representation can be made faithful by adding the adjoint representation, and so this shows that $x = x_s + x_n$ is a Jordan decomposition of x. □

In particular, an element x of a semisimple Lie algebra $\mathfrak{g}$ is semisimple (resp. nilpotent) if and only if $\mathrm{ad}_{\mathfrak{g}}(x)$ is semisimple (resp. nilpotent).

PROPOSITION 5.29 *A Lie subalgebra $\mathfrak{h}$ of a Lie algebra $\mathfrak{g}$ is commutative if $\mathrm{ad}_{\mathfrak{g}}(x)$ is semisimple for all $x \in \mathfrak{h}$.*

PROOF. Let x be an element of such a Lie algebra $\mathfrak{h}$. We have to show that $\mathrm{ad}_{\mathfrak{h}}(x) = 0$. If not, then, after possibly passing to a larger base field, $\mathrm{ad}_{\mathfrak{h}}(x)$ will have an eigenvector with nonzero eigenvalue, say,

$$[x, y] = cy, \quad c \neq 0, \quad y \neq 0, \quad y \in \mathfrak{h}.$$

Now

$$\mathrm{ad}_{\mathfrak{g}}(y)(x) = [y, x] = -[x, y] = -cy \neq 0$$

but

$$\mathrm{ad}_{\mathfrak{g}}(y)^2(x) = \mathrm{ad}_{\mathfrak{g}}(y)(-cy) = 0.$$

Thus, $\mathrm{ad}_{\mathfrak{g}}(y)$ acts nonsemisimply on the subspace of $\mathfrak{g}$ spanned by x and y, and so it acts nonsemisimply on $\mathfrak{g}$ itself. □

In particular, a Lie algebra is commutative if all of its elements are semisimple.

ASIDE 5.30 A Lie algebra is said to be ***algebraic*** if it is the Lie algebra of an algebraic group (see Chapter II). Proposition 5.26 automatically holds for algebraic Lie subalgebras of $\mathfrak{gl}_V$. The result may be regarded as the first step in the proof that all semisimple Lie algebras are algebraic.

ASIDE 5.31 It would be more natural to deduce the existence of Jordan decompositions for semisimple Lie algebras from the following statement:

> let $\mathfrak{g} \subset \mathfrak{gl}_V$ be semisimple; then $\mathfrak{g}$ consists of the elements of $\mathfrak{gl}_V$ fixing all tensors fixed by $\mathfrak{g}$.

Cf. the proof of the Jordan decomposition for algebraic groups in AGS X, Theorem 2.8; cf. Casselman, Introduction to Lie algebras, §19; Serre 1966, LA 6.5. See also II, 4.17 below. Does this hold for Lie algebras such that $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$?

6 Reductive Lie algebras; Levi subalgebras; Ado's theorem

In this section, k is a field of characteristic zero.

Reductive Lie algebras

DEFINITION 6.1 A Lie algebra $\mathfrak{g}$ is said to be ***reductive*** if its radical equals its centre.

By definition, the radical of a Lie algebra is its largest solvable ideal. Therefore, a Lie algebra $\mathfrak{g}$ is reductive if and only if every solvable ideal $\mathfrak{a}$ of $\mathfrak{g}$ is contained the centre of $\mathfrak{g}$, i.e., $[\mathfrak{g}, \mathfrak{a}] = 0$.

PROPOSITION 6.2 *The following conditions on a Lie algebra $\mathfrak{g}$ are equivalent:*

(a) $\mathfrak{g}$ *is reductive;*
(b) *the adjoint representation of* $\mathfrak{g}$ *is semisimple;*
(c) $\mathfrak{g}$ *is a product of a commutative Lie subalgebra* $\mathfrak{c}$ *and a semisimple Lie algebra* $\mathfrak{b}$.

PROOF. (a)⇒(b). If the radical $\mathfrak{r}$ of $\mathfrak{g}$ is the centre of $\mathfrak{g}$, then the adjoint representation of $\mathfrak{g}$ factors through $\mathfrak{g}/\mathfrak{r}$, which is a semisimple Lie algebra (4.4). Now Weyl's theorem (5.20) shows that the adjoint representation is semisimple.

(b)⇒(c). If the adjoint representation is semisimple, then $\mathfrak{g}$ is a direct sum of minimal nonzero ideals $\mathfrak{a}_i$, and hence $\mathfrak{g}$ is isomorphic (as a Lie algebra) to a product of $\mathfrak{a}_i$ (see p.44). Each $\mathfrak{a}_i$ is either commutative of dimension 1 or simple. The product $\mathfrak{c}$ of the commutative $\mathfrak{a}_i$ is commutative, and the product $\mathfrak{b}$ of simple ideals is semisimple, which proves the statement.

(c)⇒(a). If $\mathfrak{g} = \mathfrak{c} \times \mathfrak{b}$, then obvious $z(\mathfrak{g}) = z(\mathfrak{c}) \times z(\mathfrak{b}) = \mathfrak{c}$ and $r(\mathfrak{g}) = r(\mathfrak{c}) \times r(\mathfrak{b}) = \mathfrak{c}$. Or, in other words, $r(\mathfrak{g}) = z(\mathfrak{g})$ because this is true for both $\mathfrak{c}$ and $\mathfrak{b}$. □

6.3 The decomposition $\mathfrak{g} = \mathfrak{c} \times \mathfrak{b}$ ($\mathfrak{c}$ commutative, $\mathfrak{b}$ semisimple) in (c) is unique; in fact, we must have $\mathfrak{c} = z(\mathfrak{g})$ and $\mathfrak{h} = \mathcal{D}(\mathfrak{g})$. To see this, note that, if $\mathfrak{g} = \mathfrak{c} \times \mathfrak{b}$, then the centre of $\mathfrak{g}$ is the product of the centres of $\mathfrak{c}$ and $\mathfrak{b}$ and the derived algebra of $\mathfrak{g}$ is the product of the derived algebras of $\mathfrak{c}$ and $\mathfrak{b}$. Hence, if $\mathfrak{c}$ is commutative and $\mathfrak{b}$ is semisimple, then $z(\mathfrak{g}) = \mathfrak{c} + 0 = \mathfrak{c}$ and $\mathcal{D}\mathfrak{g} = 0 + \mathfrak{b} = \mathfrak{b}$.

PROPOSITION 6.4 *A Lie algebra is reductive if and only if it has a faithful semisimple representation.*

PROOF. If $\rho_1 \colon \mathfrak{g}_1 \to \mathfrak{gl}_{V_1}$ and $\rho_2 \colon \mathfrak{g}_2 \to \mathfrak{gl}_{V_2}$ are faithful (resp. semisimple) representations of $\mathfrak{g}_1$ and $\mathfrak{g}_2$, then $\rho_1 \times \rho_2 \colon \mathfrak{g}_1 \times \mathfrak{g}_2 \to \mathfrak{gl}_{V_1} \times \mathfrak{gl}_{V_2} \subset \mathfrak{gl}_{V_1 \times V_2}$ is a faithful (resp. semisimple) representation of $\mathfrak{g}_1 \times \mathfrak{g}_2$. Thus, it suffices to prove the corollary in the two cases: $\mathfrak{g}$ is a semisimple Lie algebra; $\mathfrak{g}$ is a one-dimensional Lie algebra. For a semisimple Lie algebra, we can take the adjoint representation, and for a one-dimensional Lie algebra we can take the identity map. □

ASIDE 6.5 As an exercise, show that a Lie algebra has a faithful *simple* representation if and only if it is reductive and its centre has dimension ≤ 1 (cf. Erdmann and Wildon 2006, Exercise 12.4).

DEFINITION 6.6 The ***nilpotent radical*** $\mathfrak{s} = s(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$ is the intersection of the kernels of the simple representations of $\mathfrak{g}$.[9]

Thus, the nilpotent radical is contained in the kernel of every semisimple representation of $\mathfrak{g}$, and it is equal to the kernel of some such representation.

6.7 *A Lie algebra* $\mathfrak{g}$ *is reductive if and only if* $s(\mathfrak{g}) = 0$.

This is a restatement of Proposition 6.4.

[9]This is the analogue of the unipotent radical of an algebraic group.

6.8 Recall (2.22) that the largest nilpotency ideal $n_\rho(\mathfrak{g})$ of $\mathfrak{g}$ with respect to a representation $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ is equal to the intersection of the kernels of the simple subrepresentations of ρ. Therefore,

$$s(\mathfrak{g}) = \bigcap\nolimits_\rho n_\rho(\mathfrak{g})$$

where ρ runs over the representations of $\mathfrak{g}$. In particular, $s(\mathfrak{g})$ is a nilpotency ideal of $\mathfrak{g}$ with respect to the adjoint representaton, and so it is nilpotent (2.23).

THEOREM 6.9 *Let $\mathfrak{g}$ be a Lie algebra, let $\mathfrak{r}$ be its radical, and let $\mathfrak{s}$ be its nilpotent radical. Then*

$$\mathfrak{s} = \mathcal{D}\mathfrak{g} \cap \mathfrak{r} = [\mathfrak{g}, \mathfrak{r}].$$

In particular, $[\mathfrak{g}, \mathfrak{r}]$ is nilpotent.

Before giving the proof, we state a corollary.

COROLLARY 6.10 *A surjective homomorphism $f\colon \mathfrak{g} \to \mathfrak{g}'$ of Lie algebras maps the nilpotent radical of $\mathfrak{g}$ onto the nilpotent radical of $\mathfrak{g}'$. Therefore $\mathfrak{g}'$ is reductive if and only if the kernel of f contains the nilpotent radical of f.*

PROOF. With the obvious notations

$$\mathfrak{s}' \overset{6.9}{=} [\mathfrak{g}', \mathfrak{r}'] = [f(\mathfrak{g}), f(\mathfrak{r})] = f([\mathfrak{g}, \mathfrak{r}]) \overset{6.9}{=} f(\mathfrak{s}).$$ □

Proof of Theorem 6.9

LEMMA 6.11 *Let α be an endomorphism of a finite-dimensional vector space over a field of characteristic zero. If $\mathrm{Tr}(\alpha^n) = 0$ for all $n \geq 1$, then α is nilpotent.*

PROOF. After extending the base field, we may assume that α is trigonalizable. Let $a_1, \ldots, a_m$ be its eigenvalues. The hypothesis is that $t_n \overset{\text{def}}{=} \sum a_i^n$ is zero for all $n \geq 1$. Write

$$(X - a_1) \cdots (X - a_m) = X^m - s_1 X^{m-1} + \cdots + (-1)^m s_m.$$

According to Newton's identities[10]

$$\begin{aligned} t_1 &= s_1 \\ t_2 &= s_1 t_1 - 2 s_2 \\ t_3 &= s_1 t_2 - s_2 t_1 + 3 s_3 \\ &\cdots, \end{aligned}$$

which show that $0 = s_1 = s_2 = \cdots$. Therefore the characteristic polynomial of α is X^m, and so $\alpha^m = 0$. □

LEMMA 6.12 *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}_V$, and let $\mathfrak{a}$ be a commutative ideal in $\mathfrak{g}$. If V is simple as a $\mathfrak{g}$-module, then $\mathcal{D}\mathfrak{g} \cap \mathfrak{a} = 0$.*

[10] More generally, Newton's identities allow you to compute the characteristic polynomial of a matrix from knowing the traces of its powers — the Wikipedia (Newton's identities).

PROOF. As V is simple, every nilpotency ideal of $\mathfrak{g}$ with respect to V is zero (2.21). Let A be the associative k-subalgebra of $\mathrm{End}(V)$ generated $\mathfrak{a}$. Consider the ideal $[\mathfrak{g},\mathfrak{a}]$ in $\mathfrak{g}$. For $x \in \mathfrak{g}$, $a \in \mathfrak{a}$, and $s \in A$,

$$\mathrm{Tr}_V[x,a]s = \mathrm{Tr}_V(xas - axs) = \mathrm{Tr}_V\, x(as - sa) = 0$$

as $as = sa$. On applying this with $s = [x,a]^{n-1}$, we see that $\mathrm{Tr}_V[x,a]^n = 0$ for all $n \geq 1$. Hence $[\mathfrak{g},\mathfrak{a}]$ is a nilpotency ideal of $\mathfrak{g}$ with respect to V, and it is zero. This means that the elements of $\mathfrak{g}$ commute with those of $\mathfrak{a}$ (in $\mathrm{End}(V)$), and so they commute also with those of A. For $x, y \in \mathfrak{g}$ and $s \in A$,

$$\mathrm{Tr}_V(yxs) = \mathrm{Tr}_V(syx) = \mathrm{Tr}_V(xsy)$$

(because $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$), and so

$$\mathrm{Tr}_V[x,y]s = \mathrm{Tr}_V(xys - yxs) = \mathrm{Tr}_V\, x(ys - sy) = 0$$

as $ys = sy$. If $[x,y] \in \mathfrak{a}$, we can apply this with $s = [x,y]^{n-1}$, and deduce as before that the ideal $\mathcal{D}\mathfrak{g} \cap \mathfrak{a} = 0$. □

We now prove the theorem.

PROOF THAT $[\mathfrak{g},\mathfrak{r}] \subset \mathcal{D}\mathfrak{g} \cap \mathfrak{r}$. Obviously $[\mathfrak{g},\mathfrak{r}] \subset [\mathfrak{g},\mathfrak{g}] \overset{\text{def}}{=} \mathcal{D}\mathfrak{g}$, and $[\mathfrak{g},\mathfrak{r}] \subset \mathfrak{r}$ because $\mathfrak{r}$ is an ideal.

PROOF THAT $\mathcal{D}\mathfrak{g} \cap \mathfrak{r} \subset \mathfrak{s}$. We have to show that $\rho(\mathcal{D}\mathfrak{g} \cap \mathfrak{r}) = 0$ for every simple representation $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$ of $\mathfrak{g}$. By definition, $\mathfrak{r}$ is solvable, and we let r denote the first positive integer such that $\rho(\mathcal{D}^{r+1}\mathfrak{r}) = 0$; then $\mathfrak{a} = \rho(\mathcal{D}^r\mathfrak{r})$ is a commutative ideal in $\rho\mathfrak{g}$. Hence (by 6.12) $\mathcal{D}(\rho\mathfrak{g}) \cap \mathfrak{a} = 0$, and so $\rho(\mathcal{D}\mathfrak{g} \cap \mathcal{D}^r\mathfrak{r}) = 0$. If $r > 0$, then $\mathcal{D}^r\mathfrak{r} \subset \mathcal{D}\mathfrak{g}$, and so

$$\rho(\mathcal{D}^r\mathfrak{r}) = \rho(\mathcal{D}\mathfrak{g} \cap \mathcal{D}^r\mathfrak{r}) = 0,$$

contrary to the definition of r. Hence $r = 0$, and $\rho(\mathcal{D}\mathfrak{g} \cap \mathfrak{r}) = 0$.

PROOF THAT $\mathfrak{s} \subset [\mathfrak{g},\mathfrak{r}]$. Let $\mathfrak{q} = \mathfrak{g}/[\mathfrak{g},\mathfrak{r}]$, and let f be the quotient map $\mathfrak{g} \to \mathfrak{q}$. Then $f(\mathfrak{r})$ is contained in the centre of $\mathfrak{q}$ but, because f is surjective, it is equal to the radical of $\mathfrak{q}$. Therefore $\mathfrak{q}$ is reductive, and so it has a faithful semisimple representation ρ (6.4). Now $\rho \circ f$ is a semisimple representation of $\mathfrak{g}$ with kernel $[\mathfrak{g},\mathfrak{r}]$, which shows that $\mathfrak{s} \subset [\mathfrak{g},\mathfrak{r}]$.

Summary

6.13 For any Lie algebra $\mathfrak{g}$,

$$\mathfrak{r} \supset \mathfrak{g}^{\perp} \supset \mathfrak{n} \supset \mathfrak{s}$$

where $\mathfrak{r}$ is the radical of $\mathfrak{g}$ (3.6), $\mathfrak{g}^{\perp}$ is the kernel of the Killing form[11] (p.42), $\mathfrak{n}$ is the largest nilpotent ideal in $\mathfrak{g}$ (2.24), and $\mathfrak{s}$ is the nilpotent radical (6.6). Cf. Bourbaki LIE I, §5, 6.

[11] This is sometimes called the ***Killing radical*** of $\mathfrak{g}$.

Criteria for a representation to be semisimple

The next theorem and its proof are taken from Bourbaki LIE I, §6, 5.

THEOREM 6.14 *The following conditions on a representation* $\rho: \mathfrak{g} \to \mathfrak{gl}_V$ *are equivalent:*

(a) ρ *is semisimple;*
(b) $\rho(\mathfrak{g})$ *is reductive and its centre consists of semisimple endomorphisms;*
(c) $\rho(\mathfrak{r})$ *consists of semisimple endomorphisms* ($\mathfrak{r}$ = *radical of* $\mathfrak{g}$)*;*
(d) *the restriction of* ρ *to* $\mathfrak{r}$ *is semisimple.*

PROOF. (a) $\Longrightarrow$ (b). If ρ is semisimple, then $\rho(\mathfrak{g})$ is reductive (6.4). Moreover, $U(\mathfrak{g})_V$ is semisimple (5.13), and so its centre is semisimple. In particular, its elements are semisimple endomorphisms of V.

(b) $\Longrightarrow$ (c). If $\rho(\mathfrak{g})$ is reductive, then its centre equals its radical, and its radical contains $\rho(\mathfrak{r})$.

(c) $\Longrightarrow$ (d). We know that $[\rho\mathfrak{g}, \rho\mathfrak{r}]$ consists of nilpotent elements (6.9), and so equals zero if $\rho\mathfrak{r}$ consists of semisimple elements. Now we apply, Bourbaki A, VIII, §9, 2, Thm 1 (see 5.15).

(d) $\Longrightarrow$ (a) Let $\mathfrak{s}$ be the nilpotent radical of $\mathfrak{g}$, and let ρ' be the restriction of ρ to $\mathfrak{r}$. The elements of $\rho(\mathfrak{s})$ are nilpotent, and so $\mathfrak{s}$ is contained in the largest nilpotency ideal of $\mathfrak{r}$ with respect to ρ'. As ρ' is semisimple, $\rho'(\mathfrak{s}) = 0$, and so $\rho(\mathfrak{g})$ is reductive (6.10). Hence $\rho(\mathfrak{g}) = \rho(\mathfrak{r}) \times \mathfrak{a}$ with $\mathfrak{a}$ semisimple (6.2). Let R (resp. A) be the associative k-algebra generated by $\rho(\mathfrak{r})$ (resp. $\mathfrak{a}$). They are semisimple (5.13), and so $A \otimes R$ is semisimple (5.10). The associative k-algebra generated by $\rho(\mathfrak{g})$ is a quotient of $A \otimes R$, and so it also is semisimple. This implies that ρ is semisimple (5.13). □

COROLLARY 6.15 *Let* ρ *and* ρ' *be representations of* $\mathfrak{g}$. *If* ρ *and* ρ' *are semisimple, so also are* $\rho \otimes \rho'$ *and* $\underline{\mathrm{Hom}}(\rho, \rho')$ *(notations as in 1.20).*

PROOF. For $x \in r(\mathfrak{g})$, $\rho(x)$ and $\rho(x')$ are semisimple (6.14), and so $\rho(x) \otimes 1 + 1 \otimes \rho'(x)$ is semisimple (Bourbaki A, VIII, §9, Corollary to Theorem 1; see 5.15), and so $\rho \otimes \rho'$ is semisimple (6.14). If ρ is semisimple, so (obviously) is $\rho^\vee$, and $\underline{\mathrm{Hom}}(\rho, \rho') \simeq \rho^\vee \otimes \rho'$. □

We say that a homomorphism $\alpha: \mathfrak{g} \to \mathfrak{g}'$ is ***normal*** if $\alpha(\mathfrak{g})$ is an ideal in $\mathfrak{g}'$.

COROLLARY 6.16 *Let* $\alpha: \mathfrak{a} \to \mathfrak{g}$ *be a normal homomorphism and let* ρ *be a representation of* $\mathfrak{g}$. *If* ρ *is semisimple, so also is* $\rho \circ \alpha$.

PROOF. After passing to the quotients, we may suppose that ρ is faithful and that $\mathfrak{a}$ is an ideal in $\mathfrak{g}$. Then $\mathfrak{g}$ and $\mathfrak{a}$ are reductive (6.14), and so $\mathfrak{g} = \mathfrak{c} + \mathfrak{q}$ where $\mathfrak{c}$ is the centre of $\mathfrak{g}$ and $\mathfrak{q}$ is semisimple. Now $\mathfrak{c} \cap \mathfrak{a}$ is the centre of $\mathfrak{a}$, and the elements of $\rho(\mathfrak{c} \cap \mathfrak{a})$ are semisimple, and so ρ is semisimple. □

ASIDE 6.17 The results in this subsection show that the semisimple representations of a Lie algebra $\mathfrak{g}$ form a neutral Tannakian category $\mathsf{Rep}^{ss}(\mathfrak{g})$ with a canonical fibre functor (the forgetful functor). Therefore,

$$\mathsf{Rep}^{ss}(\mathfrak{g}) = \mathsf{Rep}(G)$$

for a uniquely determined affine group scheme G (in fact, an inverse limit of reductive algebraic group schemes). When $\mathfrak{g}$ is semisimple, $\mathsf{Rep}^{ss}(\mathfrak{g}) = \mathsf{Rep}(\mathfrak{g})$, and G is the simply connected semisimple algebraic group with $\mathrm{Lie}(G) = \mathfrak{g}$. See Chapter II. When $\mathfrak{g}$ is the one-dimensional Lie algebra, G is the diagonalizable group attached to k regarded as an additive commutative group (see II, 4.17) — this group is not finitely generated, and so G is not of finite type.

The Levi-Malcev theorem

Special automorphisms of a Lie algebra

6.18 If u is a nilpotent endomorphism of a k-vector space V, then the sum $e^u = \sum_{n\geq 0} u^n/n!$ has only finitely many terms (it is a polynomial in u), and so it is also an endomorphism of V. If v is another nilpotent endomorphism of V and u commutes with v, then

$$\begin{aligned} e^u e^v &= \left(\sum\nolimits_{m\geq 0} \frac{u^m}{m!}\right)\left(\sum\nolimits_{n\geq 0} \frac{v^n}{n!}\right) \\ &= \sum\nolimits_{m,n\geq 0} \frac{u^m v^n}{m!n!} \\ &= \sum\nolimits_{r\geq 0} \frac{1}{r!}\left(\sum\nolimits_{m+n=r} \binom{r}{m} u^m v^n\right) \\ &= \sum\nolimits_{r\geq 0} \frac{1}{r!}(u+v)^r \\ &= e^{u+v}. \end{aligned}$$

In particular, $e^u e^{-u} = e^0 = 1$, and so e^u an automorphism of V.

6.19 Now suppose that V is equipped with a k-bilinear pairing $V \times V \to V$ (i.e., it is a k-algebra) and that u is a nilpotent *derivation* of V. Recall that this means that

$$u(xy) = x \cdot u(y) + u(x) \cdot y \quad (x, y \in V).$$

On iterating this, we find that

$$u^r(x,y) = \sum\nolimits_{m+n=r} \binom{r}{m} u^m(x) \cdot u^n(y) \quad \text{(Leibniz's formula).}$$

Hence

$$\begin{aligned} e^u(xy) &= \sum\nolimits_{r\geq 0} \frac{1}{r!} u^r(xy) \quad \text{(definition of } e^u\text{)} \\ &= \sum\nolimits_{r\geq 0} \frac{1}{r!} \sum\nolimits_{m+n=r} \binom{r}{m} u^m(x) \cdot u^n(y) \quad \text{(Leibniz's formula)} \\ &= \sum\nolimits_{m,n\geq 0} \frac{u^m(x)}{m!} \cdot \frac{u^n(y)}{n!} \\ &= e^u(x) \cdot e^u(y). \end{aligned}$$

Therefore e^u is an automorphism of the k-algebra V. In particular, a nilpotent derivation u of a Lie algebra defines an automorphism of the Lie algebra.

6.20 Recall that the nilpotent radical $\mathfrak{s}$ of $\mathfrak{g}$ is the intersection of the kernels of the simple representations of $\mathfrak{g}$. Therefore, for every representation $\rho\colon\mathfrak{g}\to\mathfrak{gl}_V$ of $\mathfrak{g}$, $\rho(\mathfrak{s})$ consists of nilpotent endomorphisms of V (2.21). Hence, for any x in the nilpotent radical of $\mathfrak{g}$, $\mathrm{ad}_{\mathfrak{g}}\,x$ is a nilpotent derivation of $\mathfrak{g}$, and so $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$ is an automorphism of $\mathfrak{g}$. Such an automorphism is said to be ***special***. Note that a special automorphism of $\mathfrak{g}$ preserves each ideal of $\mathfrak{g}$. (Bourbaki LIE, I, §6, 8.)

6.21 More generally, any element x of $\mathfrak{g}$ such that $\mathrm{ad}_{\mathfrak{g}}(x)$ is nilpotent defines an automorphism $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$ of $\mathfrak{g}$. A finite products of such automorphisms is said to be ***elementary***. The elementary automorphisms of $\mathfrak{g}$ form a subgroup $\mathrm{Aut}_e(\mathfrak{g})$ of $\mathrm{Aut}(\mathfrak{g})$. As $ue^{\mathrm{ad}(x)}u^{-1}=e^{\mathrm{ad}(ux)}$ for any automorphism u of $\mathfrak{g}$, $\mathrm{Aut}_e(\mathfrak{g})$ is a normal subgroup of $\mathrm{Aut}(\mathfrak{g})$. (Bourbaki Lie, VII, §3, 1).

6.22 Let $\mathfrak{g}$ be a Lie algebra. Later we shall see that there exists an affine group G such that

$$\mathsf{Rep}(G)=\mathsf{Rep}(\mathfrak{g}).$$

Let x be an element of $\mathfrak{g}$ such that $\rho(x)$ is nilpotent for all representations (V,ρ) of $\mathfrak{g}$ over k, and let $(e^x)_V=e^{\rho(x)}$. Then

- ◇ $(e^x)_{V\otimes W}=(e^x)_V\otimes(e^x)_W$ for all representations (V,ρ_V) and (W,ρ_W) of $\mathfrak{g}$;
- ◇ $(e^x)_V=\mathrm{id}_V$ if $\mathfrak{g}$ acts trivially on V;
- ◇ $(e^x)_W\circ\alpha_R=\alpha_R\circ(e^x)_V$ for all homomorphisms $\alpha\colon(V,\rho_V)\to(W,\rho_W)$ of representations of $\mathfrak{g}$ over k.

It follows that there exists a unique element e^x in $G(k)$ such that e^x acts on V as $e^{\rho(x)}$ for all representations (V,ρ) of $\mathfrak{g}$.

ASIDE 6.23 Let $\mathrm{Aut}_0(\mathfrak{g})$ denote the (normal) subgroup of $\mathrm{Aut}(\mathfrak{g})$ consisting of automorphisms that become elementary over k^{al}. If $\mathfrak{g}$ is semisimple, then $\mathrm{Aut}_e(\mathfrak{g})$ is equal to its own derived group, and when $\mathfrak{g}$ is split, it is equal to the derived group of $\mathrm{Aut}_0(\mathfrak{g})$ (Bourbaki LIE, VIII, §5, 2; §11, 2, Pptn 3).

NOTES This section will be completed when I know exactly what is needed for Chapter II.

Levi subalgebras

DEFINITION 6.24 Let $\mathfrak{g}$ be a Lie algebra, and let $\mathfrak{r}$ be its radical. A Lie subalgebra $\mathfrak{s}$ of $\mathfrak{g}$ is a ***Levi subalgebra*** (or ***Levi factor***) if $\mathfrak{g}=\mathfrak{r}+\mathfrak{s}$ and $\mathfrak{r}\cap\mathfrak{s}=0$ (so $\mathfrak{g}=\mathfrak{r}\oplus\mathfrak{s}$ as a k-vector space).

Let $\mathfrak{s}$ be a Levi subalgebra of $\mathfrak{g}$. Then $\mathfrak{g}$ is the semidirect product of $\mathfrak{r}$ and $\mathfrak{s}$, and $\mathfrak{g}=\mathfrak{r}\rtimes\mathfrak{s}$ is called a ***Levi decomposition*** of $\mathfrak{g}$.

THEOREM 6.25 (LEVI-MALCEV) *Every Lie algebra has a Levi subalgebra, and any two Levi subalgebras are conjugate by a special automorphism of* $\mathfrak{g}$.

PROOF. *First case:* $[\mathfrak{g},\mathfrak{r}] = 0$, i.e., $\mathfrak{r} \subset z(\mathfrak{g})$. In this case, $\mathfrak{g}$ is reductive, and $\mathfrak{g} = z(\mathfrak{g}) \times \mathcal{D}\mathfrak{g}$ is a Levi decomposition of $\mathfrak{g}$; moreover, it is the only Levi decomposition (see 6.2, 6.3).

Second case: No nonzero ideal of $\mathfrak{g}$ is properly contained in $\mathfrak{r}$. Then $[\mathfrak{g},\mathfrak{r}] = \mathfrak{r}$, and

$$[\mathfrak{r},\mathfrak{r}] = 0 = z(\mathfrak{g})$$

because both are ideals of $\mathfrak{g}$ properly contained in $\mathfrak{r}$.

The adjoint action of $\mathfrak{g}$ on $\mathfrak{g}$ defines an action of $\mathfrak{g}$ on $\mathrm{End}_{k\text{-linear}}(\mathfrak{g})$, namely,

$$x\alpha = \mathrm{ad}_{\mathfrak{g}}(x)\circ\alpha - \alpha\circ\mathrm{ad}_{\mathfrak{g}}(x) = [\mathrm{ad}_{\mathfrak{g}}(x),\alpha], \quad x \in \mathfrak{g},\ \alpha \in \mathrm{End}_{k\text{-linear}}(\mathfrak{g}),$$

(see 1.20). Consider the subspaces of $\mathrm{End}_{k\text{-linear}}(\mathfrak{g})$:

$$V = \{\alpha\colon \mathfrak{g}\to\mathfrak{r} \mid \alpha|\mathfrak{r} = \lambda(\alpha)\,\mathrm{id}_{\mathfrak{r}} \text{ for some } \lambda(\alpha)\in k\}$$
$$W = \{\alpha\colon \mathfrak{g}\to\mathfrak{r} \mid \alpha|\mathfrak{r} = 0\}.$$

They are both $\mathfrak{g}$-submodules of $\mathrm{End}_{k\text{-linear}}(\mathfrak{g})$, and W has codimension 1 in V.

The adjoint action of $\mathfrak{g}$ on $\mathfrak{g}$ defines a linear map

$$\phi\colon \mathfrak{r}\to \mathrm{End}_{k\text{-linear}}(\mathfrak{g}), \quad x \mapsto \mathrm{ad}_{\mathfrak{g}}(x).$$

This is injective (because $z(\mathfrak{g}) = 0$), and its image P lies in W (because $\mathfrak{r}$ is a commutative ideal). Moreover, P is a $\mathfrak{g}$-module (because $\mathfrak{r}$ is an ideal).

For $x \in \mathfrak{r}$, $y \in \mathfrak{g}$, and $\alpha \in V$,

$$(x\alpha)(y) = [x,\alpha(y)] - \alpha([x,y]) = -\lambda(\alpha)[x,y]$$

as $\mathfrak{r}$ is commutative. This can be rewritten as,

$$x\alpha = -\mathrm{ad}(\lambda(\alpha)x),$$

and so elements of $\mathfrak{r}$ map V into P.

Thus $\mathfrak{r}$ acts trivially on V/P, and so $\mathfrak{g}$ acts on V/P through the semisimple algebra $\mathfrak{g}/\mathfrak{r}$. According to Weyl's theorem 5.20, there exists a $\mathfrak{g}$-stable line L in V/P such that

$$V/P = W/P \oplus L.$$

In fact, $\mathfrak{g}$ acts trivially on L (5.19). Some $\alpha_0 \in V \smallsetminus W$ will generate L, and we may scale α_0 so that $\lambda(\alpha_0) = -1$. Consider the linear map

$$\mathfrak{g} \xrightarrow{g\mapsto g\alpha_0} P \xrightarrow{\phi^{-1}} \mathfrak{r}.$$

The restriction of this to $\mathfrak{r}$ is the identity map, and so its kernel is a Levi subalgebra of $\mathfrak{g}$.

Let $\mathfrak{s}'$ be a second Levi subalgebra of $\mathfrak{g}$. For each $x \in \mathfrak{s}'$, there is a unique $h(x) \in \mathfrak{r}$ such that $x + h(x) \in \mathfrak{s}$. For $x, y \in \mathfrak{s}'$,

$$[x+h(x), y+h(y)] = [x,y] + [x,h(y)] + [y,h(x)]$$

lies in $\mathfrak{s}$, and so

$$h([x,y]) = \mathrm{ad}(x)(h(y)) - \mathrm{ad}(y)(h(x)).$$

According to (5.21), there exists an $a \in \mathfrak{r}$ such that $h(x) = -[x,a]$ for all $x \in \mathfrak{s}'$. Now

$$x + h(x) = x + [a,x] = (1 + \mathrm{ad}(a))(x), \quad \text{all } x \in \mathfrak{s}',$$

and so $1+\mathrm{ad}(a)$ maps $\mathfrak{s}'$ to $\mathfrak{s}$. As $[\mathfrak{r},\mathfrak{r}] = 0$, $\mathrm{ad}(a)^2 = 0$, and so $1 + \mathrm{ad}(a) = e^{\mathrm{ad}\,a}$. As $[\mathfrak{g},\mathfrak{r}] = \mathfrak{r}$, a is in the nilpotent radical of $\mathfrak{g}$, and so $e^{\mathrm{ad}\,a}$ is a special automorphism of $\mathfrak{g}$.

General case. We use induction on the dimension of the radical of $\mathfrak{g}$. After the first two steps, we may suppose that $[\mathfrak{g},\mathfrak{r}] \neq 0$ and that $\mathfrak{r}$ contains a proper nontrivial ideal. As $[\mathfrak{g},\mathfrak{r}]$ is nilpotent (6.9), its centre is nonzero. Let $\mathfrak{m}$ be a minimal nonzero ideal contained in the centre of $[\mathfrak{g},\mathfrak{r}]$. After the second step, we may suppose that $\mathfrak{m} \neq \mathfrak{r}$. Now $\mathfrak{g}/\mathfrak{m}$ has radical $\mathfrak{r}/\mathfrak{m}$, and so we may apply the induction hypothesis to it. □

ASIDE 6.26 Theorem 6.25 reduces the problem of classifying Lie algebras (in characteristic zero) to the problems of (a) classifying semisimple Lie algebras, (b) classifying solvable Lie algebras, and (c) classifying the semidirect products of a semisimple Lie algebra by a solvable Lie algebra.

Let $\mathfrak{s}$ be a semisimple Lie algebra and let $\mathfrak{r}$ be a solvable Lie algebra. The Lie algebra structures on $\mathfrak{r} \oplus \mathfrak{s}$ making it into a semidirect product $\mathfrak{r} \rtimes \mathfrak{s}$ are in one-to-one correspondence with the representations $\rho\colon \mathfrak{s} \to \mathfrak{gl}_{\mathfrak{r}}$ such that $\rho(\mathfrak{s}) \subset \mathrm{Der}(\mathfrak{r})$.

For a discussion of (c), see arXiv:1302.4255.

NOTES Levi (1905) proved that Levi subalgebras exist, and Malcev (1942) poved that any two of them are conjugate.

NOTES In nonzero characteristic, both parts of (6.25) may fail. See McNinch, George J., Levi decompositions of a linear algebraic group. Transform. Groups 15 (2010), no. 4, 937–964.

Ado's theorem

THEOREM 6.27 (ADO) *Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over a field of characteristic zero, and let $\mathfrak{n}$ be its largest nilpotent ideal. Then there exists a faithful representation (V,ρ) of $\mathfrak{g}$ such that $\rho(\mathfrak{n})$ consists of nilpotent elements.*

In particular, every nilpotent Lie algebra $\mathfrak{g}$ over a field of characteristic zero admits a faithful representation (V,r) such that $\rho(\mathfrak{g})$ consists of nilpotent elements.

Let $\mathfrak{g}$ be a Lie algebra. Recall that an ideal $\mathfrak{a}$ in $\mathfrak{g}$ is a nilpotency ideal with respect to a representation ρ of $\mathfrak{g}$ if $\rho(x)$ is nilpotent for all $x \in \mathfrak{a}$. For each representation (V,ρ), there exists a largest nilpotency ideal $n_\rho(\mathfrak{g})$, which consists of the elements x of $\mathfrak{g}$ such $xM = 0$ for all simple subquotients M of V (2.22).

Zassenhaus's extension theorem

Let (V,ρ) be a representation of $U(\mathfrak{g})$. For $e \in V$ and $e' \in V^\vee$, the map $\theta(e,e')$

$$x \mapsto \langle \rho(x)e, e' \rangle \colon U(\mathfrak{g}) \to k,$$

is called a ***coefficient*** of ρ, and we let $C(\rho)$ denote the subspace of $U(\mathfrak{g})^\vee$ spanned by the coefficients of ρ. For example, if $e_1,\ldots,e_n$ is a basis for V and $e'_1,\ldots,e'_n$ is the dual basis, then $\theta(e_i,e'_j)$ sends an element x of $U(\mathfrak{g})$ to the $(i.j)$th entry of the matrix of $\rho(x)$ relative to the basis $e_1,\ldots,e_n$. Moreover, the map

$$e \mapsto (\theta(e,e'_1),\ldots,\theta(e,e'_n))\colon V \to C(\rho)^n$$

is an injective $U(\mathfrak{g})$-homomorphism.

THEOREM 6.28 (ZASSENHAUS) *Let $\mathfrak{g}$ be a Lie algebra. A representation ρ' of a Lie subalgebra $\mathfrak{g}'$ of $\mathfrak{g}$ extends to a representation ρ of $\mathfrak{g}$ such that $n_\rho(\mathfrak{g}) \supset n_{\rho'}(\mathfrak{g}')$ if $\mathfrak{g}'$ is an ideal in $\mathfrak{g}$ and there exists a Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ such that $\mathfrak{g} = \mathfrak{g}' \oplus \mathfrak{h}$ and $[\mathfrak{h}, \mathfrak{g}'] \subset n_{\rho'}(\mathfrak{g}')$. If moreover $\mathrm{ad}_{\mathfrak{g}}(x)|\mathfrak{g}'$ is nilpotent for all $x \in \mathfrak{h}$, then ρ can be chosen so that $n_\rho(\mathfrak{g}) \supset \mathfrak{h}$.*

PROOF. (Following the proof of Bourbaki LIE, I, §7, 2, Thm 1.) Let I be the kernel of ρ', regarded as a representation of $U(\mathfrak{g}')$. Then I is a two-sided ideal of $U(\mathfrak{g}')$ of finite codimension. Let $C(\rho')$ denote the subspace of $U(\mathfrak{g}')^\vee$ of coefficients of ρ' — it is orthogonal to I in the natural pairing $U(\mathfrak{g}') \times U(\mathfrak{g}')^\vee \to k$. Let S be the sub-$\mathfrak{g}$-module of $U(\mathfrak{g}')^\vee$ generated by $C(\rho')$.

Let V' be the representation space for ρ', and let

$$V' = V'_0 \supset V'_1 \supset \cdots \supset V'_d = \{0\}$$

be a Jordan-Hölder series for V' (as a $U(\mathfrak{g}')$-module). Let $I' \subset U(\mathfrak{g}')$ be the intersection of the kernels of the representations of $U(\mathfrak{g}')$ on the quotients V'_{i-1}/V_i. Then

$$I'^d \subset I \subset I',$$

and $I' \cap \mathfrak{g}' = n_{\rho'}(\mathfrak{g}')$. Now (1.29) shows that I'^d is of finite codimension in $U(\mathfrak{g}')$.

For $x \in \mathfrak{h}$, the derivation $u \mapsto xu - ux$ of $U(\mathfrak{g}')$ maps $\mathfrak{g}'$ into $[\mathfrak{h}, \mathfrak{g}'] \subset I'$, hence $U(\mathfrak{g}')$ into I', and hence I'^d into I'^d. As I'^d is a $\mathfrak{g}'$-submodule of $U(\mathfrak{g}')$, this shows that it is also a $\mathfrak{g}$-submodule. The orthogonal complement of I'^d in $U(\mathfrak{g}')^\vee$ is a finite-dimensional $\mathfrak{g}$-submodule which contains $C(\rho')$ and therefore S. Therefore S is finite-dimensional over k.

The $\mathfrak{g}'$-module V' is isomorphic to a sub-$\mathfrak{g}'$-module of $C(\rho')^n$ for some n. Hence the $\mathfrak{g}$-module S^n is a finite-dimensional extension ρ of ρ' to $\mathfrak{g}$. Moreover, $\rho(x)$ is nilpotent for $x \in I' \cap \mathfrak{g}'$, which is an ideal in $\mathfrak{g}$, and so $I' \cap \mathfrak{g}'$ is contained in the largest nilpotency ideal of ρ. This completes the proof of the first assertion of the theorem.

The proof of the second assertion is omitted (for the moment). □

Another extension result

PROPOSITION 6.29 *Let $\mathfrak{g}$ be a Lie algebra, let $\mathfrak{a}$ be a nilpotent ideal in $\mathfrak{g}$, and let ρ be a representation of $\mathfrak{a}$ such that $\rho(x)$ is nilpotent for all $x \in \mathfrak{a}$. Then ρ extends to a representation ρ' of $\mathfrak{g}$ such that $\rho'(xb)$ is nilpotent for all x in the largest nilpotent ideal of $\mathfrak{g}$.*

PROOF. Let $\mathfrak{n}$ denote the largest nilpotent ideal of $\mathfrak{g}$. Then $\mathfrak{n} \supset \mathfrak{a}$ and $\mathfrak{n}/\mathfrak{a}$ is nilpotent, and so there exists a sequence of subalgebras of $\mathfrak{n}$

$$\mathfrak{a} = \mathfrak{n}_0 \subset \mathfrak{n}_1 \subset \cdots \subset \mathfrak{n}_r = \mathfrak{n}$$

such that $\mathfrak{n}_{i-1}$ is an ideal in $\mathfrak{n}_i$ and $\dim \mathfrak{n}_i/\mathfrak{n}_{i-1} = 1$ for all i. The algebra $\mathfrak{n}_i$ is therefore the direct sum of $\mathfrak{n}_{i-1}$ with a one-dimensional subalgebra. As $\mathrm{ad}_{\mathfrak{g}} x$ is nilpotent for all $x \in \mathfrak{n}$, we can apply (6.28) to successively extend ρ to $\mathfrak{n}_1, \ldots, \mathfrak{n}$ in such a way that every element of $\mathfrak{n}$ is mapped to a nilpotent endomorphism.

Let $\mathfrak{r}$ denote the radical of $\mathfrak{g}$. Then $\mathfrak{r}$ is unipotent, and so there exists a sequence of subalgebras of $\mathfrak{r}$

$$\mathfrak{n} = \mathfrak{r}_0 \subset \mathfrak{r}_1 \subset \cdots \subset \mathfrak{r}_s = \mathfrak{r}$$

such that $\mathfrak{r}_{i-1}$ is an ideal in $\mathfrak{r}_i$ and $\dim \mathfrak{r}_i/\mathfrak{r}_{i-1} = 1$ for all i. As $[\mathfrak{r},\mathfrak{r}] \subset \mathfrak{n}$, we can apply (6.28) to successively extend ρ to $\mathfrak{r}_1,\ldots,\mathfrak{r}$ in such a way that every element of $\mathfrak{r}$ is mapped to a nilpotent endomorphism.

Finally, we apply the Levi-Malcev theorem (6.25) to write $\mathfrak{g} = \mathfrak{r} \oplus \mathfrak{s}$ with $\mathfrak{s}$ a subalgebra. As $[\mathfrak{s},\mathfrak{r}] \subset \mathfrak{n}$, we can apply (6.28) again to extend ρ to $\mathfrak{g}$ in such a way that every element of $\mathfrak{n}$ is mapped to a nilpotent endomorphism. □

Proof of Ado's theorem 6.27

The theorem is certainly true if $\mathfrak{g}$ is commutative; for example, if $\mathfrak{g}$ has dimension 1 we can take ρ to be the representation $c \mapsto \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$. Choose a faithful representation of the centre $\mathfrak{c}$ of $\mathfrak{g}$ sending each element of $\mathfrak{c}$ to a nilpotent endomorphism, and extend it to a representation ρ_1 of $\mathfrak{g}$ as in (6.29). Let ρ_2 be the adjoint representation of $\mathfrak{g}$, and let $\rho = \rho_1 \oplus \rho_2$. Then ρ sends every element of $\mathfrak{n}$ to a nilpotent endomorphism because each of ρ_1 and ρ_2 does, and

$$\operatorname{Ker}(\rho) = \operatorname{Ker}(\rho_1) \cap \operatorname{Ker}(\rho_2) = \operatorname{Ker}(\rho_1) \cap \mathfrak{c} = 0.$$

ASIDE 6.30 Lie himself tried to prove that every Lie algebra arises as a subalgebra of $\mathfrak{gl}_n$, but it was only in 1935 that Ado succeeded in showing this over an algebraically closed field of characteristic zero. Iwasawa (1950) proved the same result in nonzero characteristic, and Harish-Chandra (1949) proved the above result. The proof given here, following Bourbaki, is that of Harish-Chandra. For a proof that every Lie algebra in nonzero characteristic admits a faithful representations, see Jacobson 1962, VI.3.

7 Root systems and their classification

To a semisimple Lie algebra, we attach some combinatorial data, called a root system, from which we can read off the structure of the Lie algebra and its representations. As every root system arises from a semisimple Lie algebra and determines it up to isomorphism, the root systems classify the semisimple Lie algebras. In this section, we review the theory of root systems and explain how they are classified in turn by Dynkin diagrams,

This section omits some (standard) proofs. For more detailed accounts, see: Bourbaki LIE, Chapter VI; Serre 1966, Chapter V; or Casselman, Root Systems.

Throughout, F is a field of characteristic zero and V is a finite-dimensional vector space over F. An ***inner product*** on a real vector space is a positive definite symmetric bilinear form.

Reflections

A ***reflection*** in a vector space is a linear transformation fixing a hyperplane through the origin and acting as -1 on a line through the origin (transverse to the hyperplane). Let α be a nonzero element of V. A ***reflection with vector*** α is an endomorphism s of V such that $s(\alpha) = -\alpha$ and the set of vectors fixed by s is a hyperplane H. Then $V = H \oplus \langle \alpha \rangle$ with s acting as $1 \oplus -1$, and so $s^2 = -1$. Let $V^\vee$ be the dual vector space to V, and write $\langle\ ,\ \rangle$ for the tautological pairing $V \times V^\vee \to k$.

LEMMA 7.1 *If $\alpha^\vee$ is an element of $V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, then*

$$s_\alpha : x \mapsto x - \langle x, \alpha^\vee \rangle \alpha \tag{39}$$

is a reflection with vector α, and every reflection with vector α is of this form (for a unique $\alpha^\vee$)

PROOF. Certainly, s_α is a reflection with vector α. Conversely, if s is a reflection with vector α and fixed hyperplane H, then the composite of the quotient map $V \to V/H$ with the linear map $V/H \to F$ sending $\alpha + H$ to 2 is the unique element $\alpha^\vee$ of $V^\vee$ such that $\alpha(H) = 0$ and $\langle \alpha, \alpha^\vee \rangle = 2$. □

LEMMA 7.2 *Let R be a finite spanning set for V. For any nonzero vector α in V, there exists at most one reflection s with vector α such that $s(R) \subset R$.*

PROOF. Let s and s' be such reflections, and let $t = ss'$. Then t acts as the identity map on both $F\alpha$ and $V/F\alpha$, and so

$$(t-1)^2 V \subset (t-1)F\alpha = 0.$$

Thus the minimum polynomial of t divides $(T-1)^2$. On the other hand, because R is finite, there exists an integer $m \geq 1$ such that $t^m(x) = x$ for all $x \in R$, and hence for all $x \in V$. Therefore the minimum polynomial of t divides $T^m - 1$. As $(T-1)^2$ and $T^m - 1$ have greatest common divisor $T - 1$, this shows that $t = 1$. □

LEMMA 7.3 *Let $(\ ,\ )$ be an inner product on a real vector space V. Then, for any nonzero vector α in V, there exists a unique symmetry s with vector α that is orthogonal for $(\ ,\ )$, i.e., such that $(sx, sy) = (x, y)$ for all $x, y \in V$, namely*

$$s(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha. \tag{40}$$

PROOF. Certainly, (40) does define an orthogonal symmetry with vector α. Suppose s' is a second such symmetry, and let $H = \langle \alpha \rangle^\perp$. Then H is stable under s', and maps isomorphically on $V/\langle \alpha \rangle$. Therefore s' acts as 1 on H. As $V = H \oplus \langle \alpha \rangle$ and s' acts as -1 on $\langle \alpha \rangle$, it must coincide with s. □

Root systems

DEFINITION 7.4 A subset R of V over F is a ***root system*** in V if

RS1 R is finite, spans V, and does not contain 0;
RS2 for each $\alpha \in R$, there exists a (unique) reflection s_α with vector α such that $s_\alpha(R) \subset R$;
RS3 for all $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is an integer multiple of α.

In other words, R is a root system if it satisfies RS1 and, for each $\alpha \in R$, there exists a (unique) vector $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \in \mathbb{Z}$, and the reflection $s_\alpha \colon x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ maps R in R.

We sometimes refer to the pair (V, R) as a root system over F. The elements of R are called the ***roots*** of the root system. If α is a root, then $s_\alpha(\alpha) = -\alpha$ is also a root. The unique $\alpha^\vee$ attached to α is called its ***coroot***. The dimension of V is called the ***rank*** of the root system.

EXAMPLE 7.5 Let V be the hyperplane in F^{n+1} of $n+1$-tuples $(x_i)_{1\le i\le n+1}$ such that $\sum x_i = 0$, and let

$$R = \{\alpha_{ij} \stackrel{\text{def}}{=} e_i - e_j \mid i \neq j, \quad 1 \le i, j \le n+1\}$$

where $(e_i)_{1\le i\le n+1}$ is the standard basis for F^{n+1}. For each $i \neq j$, let $s_{\alpha_{ij}}$ be the linear map $V \to V$ that switches the ith and jth entries of an $n+1$-tuple in V. Then $s_{\alpha_{ij}}$ is a reflection with vector α_{ij} such that $s_{\alpha_{ij}}(R) \subset R$ and $s_{\alpha_{ij}}(\beta) - \beta \in \mathbb{Z}\alpha_{ij}$ for all $\beta \in R$. As R obviously spans V, this shows that R is a root system in V.

For other examples of root systems, see p.91 below.

PROPOSITION 7.6 *Let (V,R) be a root system over F, and let V_0 be the $\mathbb{Q}$-vector space generated by R. Then $c \otimes v \mapsto cv \colon F \otimes_{\mathbb{Q}} V_0 \to V$ is an isomorphism, and R is a root system in V_0 (Bourbaki LIE, VI, 1.1, Pptn 1; Serre 1966, V, 17, Thm 5, p. 41).*

Thus, to give a root system over F is the same as giving a root system over $\mathbb{Q}$ (or $\mathbb{R}$ or $\mathbb{C}$). In the following, we assume that $F \subset \mathbb{R}$ (and sometimes that $F = \mathbb{R}$).

PROPOSITION 7.7 *If $(V_i, R_i)_{i\in I}$ is a finite family of root systems, then*

$$\bigoplus\nolimits_{i\in I}(V_i, R_i) \stackrel{\text{def}}{=} \left(\bigoplus\nolimits_{i\in I} V_i, \bigsqcup R_i\right)$$

*is a root system (called the **direct sum** of the (V_i, R_i)).*

A root system is ***indecomposable*** (or ***irreducible***) if it can not be written as a direct sum of nonempty root systems.

PROPOSITION 7.8 *Let (V,R) be a root system. There exists a unique partition $R = \bigsqcup_{i\in I} R_i$ of R such that*

$$(V,R) = \bigoplus\nolimits_{i\in I}(V_i, R_i), \quad V_i = \text{span of } R_i,$$

and each (V_i, R_i) is an indecomposable root system (Bourbaki LIE, VI, 1.2).

Suppose that roots α and β are multiples of each other, say,

$$\beta = c\alpha, \quad c \in F, \quad 0 < c < 1.$$

Then $\langle c\alpha, \alpha^\vee\rangle = 2c \in \mathbb{Z}$ and so $c = \frac{1}{2}$. For each root α, the set of roots that are multiples of α is either $\{-\alpha, \alpha\}$ or $\{-\alpha, -\alpha/2, \alpha/2, \alpha\}$. When only the first case occurs, the root system is said to be ***reduced***.

From now on "root system" will mean "reduced root system".

The Weyl group

Let (V,R) be a root system. The ***Weyl group*** $W = W(R)$ of (V,R) is the subgroup of $\mathrm{GL}(V)$ generated by the reflections s_α for $\alpha \in R$. Because R spans V, the group W acts faithfully on R, and so is finite.

For $\alpha \in R$, we let H_α denote the hyperplane of vectors fixed by s_α. A ***Weyl chamber*** is a connected component of $V \smallsetminus \bigcup_{\alpha\in R} H_\alpha$.

PROPOSITION 7.9 *The group $W(R)$ acts simply transitively on the set of Weyl chambers (Bourbaki LIE, VI, §1, 5).*

Existence of an inner product

PROPOSITION 7.10 *For any root system (V, R), there exists an inner product $(\ ,\ )$ on V such the $w \in R$, act as orthogonal transformations, i.e., such that*

$$(wx, wy) = (x, y) \text{ for all } w \in W,\ x, y \in V.$$

PROOF. Let $(\ ,\ )'$ be any inner product $V \times V \to \mathbb{R}$, and define

$$(x, y) = \sum\nolimits_{w \in W} (wx, wy)'.$$

Then $(\ ,\ )$ is again symmetric and bilinear, and

$$(x, x) = \sum\nolimits_{w \in W} (wx, wx)' > 0$$

if $x \neq 0$, and so $(\ ,\ )$ is positive-definite. On the other hand, for $w_0 \in W$,

$$\begin{aligned}(w_0 x, w_0 y) &= \sum\nolimits_{w \in W} (ww_0 x, ww_0 y)' \\ &= (x, y)\end{aligned}$$

because as w runs through W, so also does ww_0. □

In fact, there is a canonical inner product on V.

When we equip V with an inner product $(\ ,\ )$ as in (7.10),

$$s_\alpha(x) = x - 2\frac{(x, \alpha)}{(\alpha, \alpha)}\alpha \text{ for all } x \in V.$$

Therefore the hyperplane of vectors fixed by α is orthogonal to α, and the ratio $(x, \alpha)/(\alpha, \alpha)$ is independent of the choice of the inner product:

$$2\frac{(x, \alpha)}{(\alpha, \alpha)} = \langle x, \alpha^\vee \rangle.$$

Bases

Let (V, R) be a root system. A subset S of R is a ***base*** for R if it is a basis for V and if each root can be written $\beta = \sum_{\alpha \in S} m_\alpha \alpha$ with the m_α integers of the same sign (i.e., either all $m_\alpha \geq 0$ or all $m_\alpha \leq 0$). The elements of a (fixed) base are called the ***simple roots*** (for the base).

PROPOSITION 7.11 *There exists a base S for R (Bourbaki LIE, VI, §1, 5).*

More precisely, let t lie in a Weyl chamber, so t is an element of V such that $\langle t, \alpha^\vee \rangle \neq 0$ if $\alpha \in R$, and let $R^+ = \{\alpha \in R \mid (\alpha, t) > 0\}$. Say that $\alpha \in R^+$ is ***indecomposable*** if it can not be written as a sum of two elements of R^+. The indecomposable elements form a base, which depends only on the Weyl chamber of t. Every base arises in this way from a unique Weyl chamber, and so (7.9) shows that W acts simply transitively on the set of bases for R.

PROPOSITION 7.12 *Let S be a base for R. Then W is generated by the $\{s_\alpha \mid \alpha \in S\}$, and $W \cdot S = R$ (Serre 1966, V, 10, p. 33).*

PROPOSITION 7.13 *Let S be a base for R. If S is indecomposable, there exists a root $\tilde{\alpha} = \sum_{\alpha\in S} n_\alpha \alpha$ such that, for any other root $\sum_{\alpha\in S} m_\alpha\alpha$, we have that $n_\alpha \geq m_\alpha$ for all α (Bourbaki LIE, VI, §1, 8).*

Obviously $\tilde{\alpha}$ is uniquely determined by the base S. It is called the ***highest root*** (for the base). The simple roots α with $n_\alpha = 1$ are said to be ***special***.

EXAMPLE 7.14 Let (V, R) be the root system in (7.5), and endow V with the usual inner product (assume $F \subset \mathbb{R}$). When we choose

$$t = ne_1 + \cdots + e_n - \frac{n}{2}(e_1 + \cdots + e_{n+1}),$$

then

$$R^+ \stackrel{\text{def}}{=} \{\alpha \mid (\alpha, t) > 0\} = \{e_i - e_j \mid i > j\}.$$

For $i > j + 1$,

$$e_i - e_j = (e_i - e_{i+1}) + \cdots + (e_{j+1} - e_j),$$

and so $e_i - e_j$ is decomposable. The indecomposable elements are $e_1 - e_2, \ldots, e_n - e_{n+1}$. Obviously, they *do* form a base S for R. The Weyl group has a natural identification with S_{n+1}, and it certainly is generated by the elements $s_{\alpha_1}, \ldots, s_{\alpha_n}$ where $\alpha_i = e_i - e_{i+1}$; moreover, $W \cdot S = R$. The highest root is

$$\tilde{\alpha} = e_1 - e_{n+1} = \alpha_1 + \cdots + \alpha_n.$$

Reduced root systems of rank 2

The root systems of rank 1 are the subsets $\{\alpha, -\alpha\}$, $\alpha \neq 0$, of a vector space V of dimension 1, and so the first interesting case is rank 2. Assume $F = \mathbb{R}$, and choose an invariant inner product. For roots α, β, we let

$$n(\beta, \alpha) = 2\frac{(\beta, \alpha)}{(\alpha, \alpha)} = \langle \beta, \alpha^\vee \rangle \in \mathbb{Z}.$$

Write

$$n(\beta, \alpha) = 2\frac{|\beta|}{|\alpha|}\cos\phi$$

where $|\cdot|$ denotes the length of a vector and ϕ is the angle between α and β. Then

$$n(\beta, \alpha) \cdot n(\alpha, \beta) = 4\cos^2\phi \in \mathbb{Z}.$$

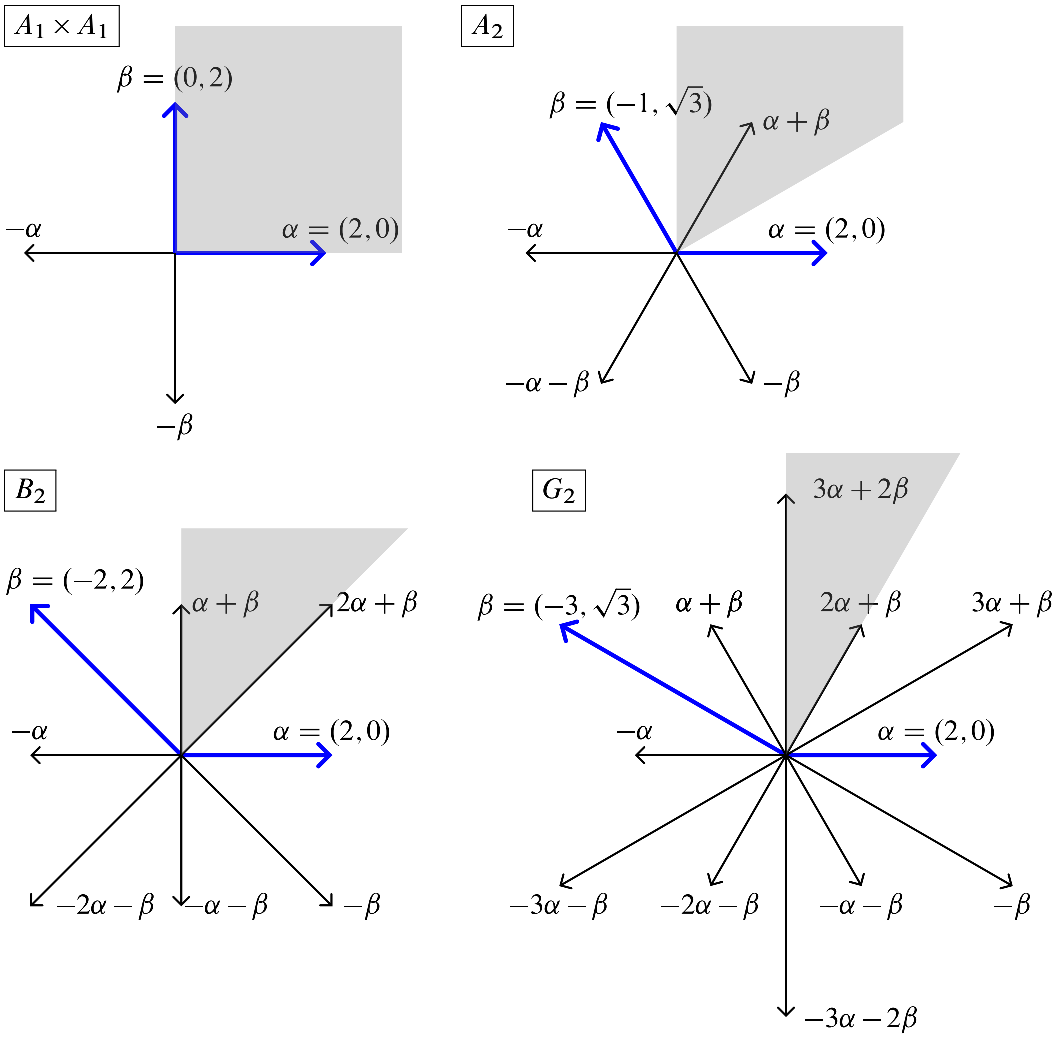
When we exclude the possibility that β is a multiple of α, there are only the following possibilities (in the table, we have chosen β to be the longer root):

$n(\beta,\alpha)\cdot n(\alpha,\beta)$	$n(\alpha,\beta)$	$n(\beta,\alpha)$	ϕ	$\lvert\beta\rvert/\lvert\alpha\rvert$
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	$5\pi/6$	

If α and β are simple roots and $n(\alpha,\beta)$ and $n(\beta,\alpha)$ are strictly positive (i.e., the angle between α and β is acute), then (from the table) one, say, $n(\beta,\alpha)$, equals 1. Then

$$s_\alpha(\beta) = \beta - n(\beta,\alpha)\alpha = \beta - \alpha,$$

and so $\pm(\alpha-\beta)$ are roots, and one, say $\alpha-\beta$, will be in R^+. But then $\alpha = (\alpha-\beta)+\beta$, contradicting the simplicity of α. We conclude that $n(\alpha,\beta)$ and $n(\beta,\alpha)$ are both negative. From this it follows that there are exactly the four nonisomorphic root systems of rank 2 displayed below. The set $\{\alpha,\beta\}$ is the base determined by the shaded Weyl chamber.



Note that each set of vectors does satisfy (RS1–3). The root system $A_1 \times A_1$ is decomposable and the remainder are indecomposable.

We have

	$A_1 \times A_1$	A_2	B_2	G_2
$s_\alpha(\beta)-\beta$	0α	1α	2α	3α
ϕ	$\pi/2$	$2\pi/3$	$3\pi/4$	$5\pi/6$
$W(R)$	D_2	D_3	D_4	D_6
$(\mathrm{Aut}(R){:}\,W(R))$	2	2	1	1

where D_n denotes the dihedral group of order $2n$.

Cartan matrices

Let (V,R) be a root system. As before, for $\alpha,\beta\in R$, we let

$$n(\alpha,\beta)=\langle\alpha,\beta^\vee\rangle\in\mathbb{Z},$$

so that

$$n(\alpha,\beta)=2\frac{(\alpha,\beta)}{(\beta,\beta)}$$

for any inner form satisfying (7.10). From the second expression, we see that $n(w\alpha,w\beta)=n(\alpha,\beta)$ for all $w\in W$.

Let S be a base for R. The ***Cartan matrix*** of R (relative to S) is the matrix $(n(\alpha,\beta))_{\alpha,\beta\in S}$. Its diagonal entries $n(\alpha,\alpha)$ equal 2, and the remaining entries are negative or zero.

For example, the Cartan matrices of the root systems of rank 2 are,

$$\underset{A_1\times A_1}{\begin{pmatrix}2&0\\0&2\end{pmatrix}}\quad\underset{A_2}{\begin{pmatrix}2&-1\\-1&2\end{pmatrix}}\quad\underset{B_2}{\begin{pmatrix}2&-1\\-2&2\end{pmatrix}}\quad\underset{G_2}{\begin{pmatrix}2&-1\\-3&2\end{pmatrix}}$$

and the Cartan matrix for the root system in (7.5) is

$$\begin{pmatrix}2&-1&0&&0&0\\-1&2&-1&&0&0\\0&-1&2&&0&0\\&&&\ddots&&\\0&0&0&&2&-1\\0&0&0&&-1&2\end{pmatrix}$$

because

$$2\frac{(e_i-e_{i+1},e_{i+1}-e_{i+2})}{(e_i-e_{i+1},e_i-e_{i+1})}=-1,\text{ etc..}$$

PROPOSITION 7.15 *The Cartan matrix of (V,R) is independent of S, and determines (V,R) up to isomorphism.*

In fact, if S' is a second base for R, then we know that $S'=wS$ for a *unique* $w\in W$ and that $n(w\alpha,w\beta)=n(\alpha,\beta)$. Thus S and S' give the same Cartan matrices up to re-indexing the columns and rows. Let (V',R') be a second root system with the same Cartan matrix. This means that there exists a base S' for R' and a bijection $\alpha\mapsto\alpha'\colon S\to S'$ such that

$$n(\alpha,\beta)=n(\alpha',\beta')\text{ for all }\alpha,\beta\in S. \tag{41}$$

The bijection extends uniquely to an isomorphism of vector spaces $V\to V'$, which sends s_α to $s_{\alpha'}$ for all $\alpha\in S$ because of (41). But the s_α generate the Weyl groups (7.12), and so the isomorphism maps W onto W', and hence it maps $R=W\cdot S$ onto $R'=W'\cdot S'$ (see 7.12). We have shown that the bijection $S\to S'$ extends uniquely to an isomorphism $(V,R)\to(V',R')$ of root systems.

Classification of root systems by Dynkin diagrams

Let (V,R) be a root system, and let S be a base for R.

PROPOSITION 7.16 *Let α and β be distinct simple roots. Up to interchanging α and β, the only possibilities for $n(\alpha,\beta)$ are*

$n(\alpha,\beta)$	$n(\beta,\alpha)$	$n(\alpha,\beta)n(\beta,\alpha)$
0	0	0
-1	-1	1
-2	-1	2
-3	-1	3

If W is the subspace of V spanned by α and β, then $W \cap R$ is a root system of rank 2 in W, and so (7.16) can be read off from the Cartan matrices of the rank 2 systems.

Choose a base S for R. Then the ***Coxeter graph***[12] of (V,R) is the graph whose nodes are indexed by the elements of S; two distinct nodes are joined by $n(\alpha,\beta)\cdot n(\beta,\alpha)$ edges. Up to the indexing of the nodes, it is independent of the choice of S.

PROPOSITION 7.17 *The Coxeter graph is connected if and only if the root system is indecomposable.*

In other words, the decomposition of the Coxeter graph of (V,R) into its connected components corresponds to the decomposition of (V,R) into a direct sum of its indecomposable summands.

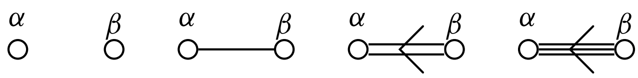
PROOF. A root system is decomposable if and only if R can be written as a disjoint union $R = R_1 \sqcup R_2$ with each root in R_1 orthogonal to each root in R_2. Since roots α,β are orthogonal if and only $n(\alpha,\beta)\cdot n(\beta,\alpha) = 4\cos^2\phi = 0$, this is equivalent to the Coxeter graph being disconnected. □

The Coxeter graph doesn't determine the Cartan matrix because it only gives the number $n(\alpha,\beta)\cdot n(\beta,\alpha)$. However, for each value of $n(\alpha,\beta)\cdot n(\beta,\alpha)$ there is only one possibility for the unordered pair

$$\{n(\alpha,\beta), n(\beta,\alpha)\} = \left\{2\frac{|\alpha|}{|\beta|}\cos\phi, 2\frac{|\beta|}{|\alpha|}\cos\phi\right\}.$$

Thus, if we know in addition which is the longer root, then we know the *ordered* pair. To remedy this, we put an arrowhead on the lines joining the nodes indexed by α and β pointing towards the shorter root. The resulting diagram is called the ***Dynkin diagram*** of the root system. It determines the Cartan matrix and hence the root system.

For example, the Dynkin diagrams of the root systems of rank 2 are:



$A_1 \times A_1$ A_2 B_2 G_2

[12]According to the Wikipedia, this is actually a multigraph, because there may be multiple edges joining two nodes.

THEOREM 7.18 *The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_6, E_7, E_8, F_4, G_2 listed at the end of the section — we have used the conventional (Bourbaki) numbering for the simple roots.*

PROOF. It follows from Theorem 7.19 below, that the Dynkin diagram of an indecomposable root system occur in the list. To show that every diagram on the list arises from an irreducible root system, it suffices to exhibit a root system for each diagram. For the types A–D we realize the diagram as the Dynkin diagram of a split semisimple Lie algebra in the next section; sometime I'll add the exceptional cases. □

For example, the Dynkin diagram of the root system in (7.5, 7.14) is A_n. Note that Coxeter graphs do not distinguish B_n from C_n.

Classification of Coxeter graphs

Consider a graph Δ whose nodes are labelled by $1, 2, \ldots, l$ and such that the nodes i, j, $i \neq j$, are joined by n_{ij} edges. The quadratic form of Δ is

$$Q(X_1, \ldots, X_l) = 2\sum_{i=1}^{l} X_i^2 - \sum_{i,j,\, i \neq j} \sqrt{n_{ij}}\, X_i X_j.$$

The Coxeter graph of an indecomposable root system has the following properties:

(a) it is connected;
(b) the number of edges joining any two distinct nodes is 1, 2, or 3;
(c) the quadratic form of Δ is positive definite.

THEOREM 7.19 *The graphs Δ satisfying the conditions (a,b,c) are exactly the graphs A_n ($n \geq 1$), B_n ($n \geq 2$), D_n ($n \geq 4$), E_6, E_7, E_8, F_4, G_2.*

PROOF. See, for example, Carter 1995, 2.5, pp. 19-21. □

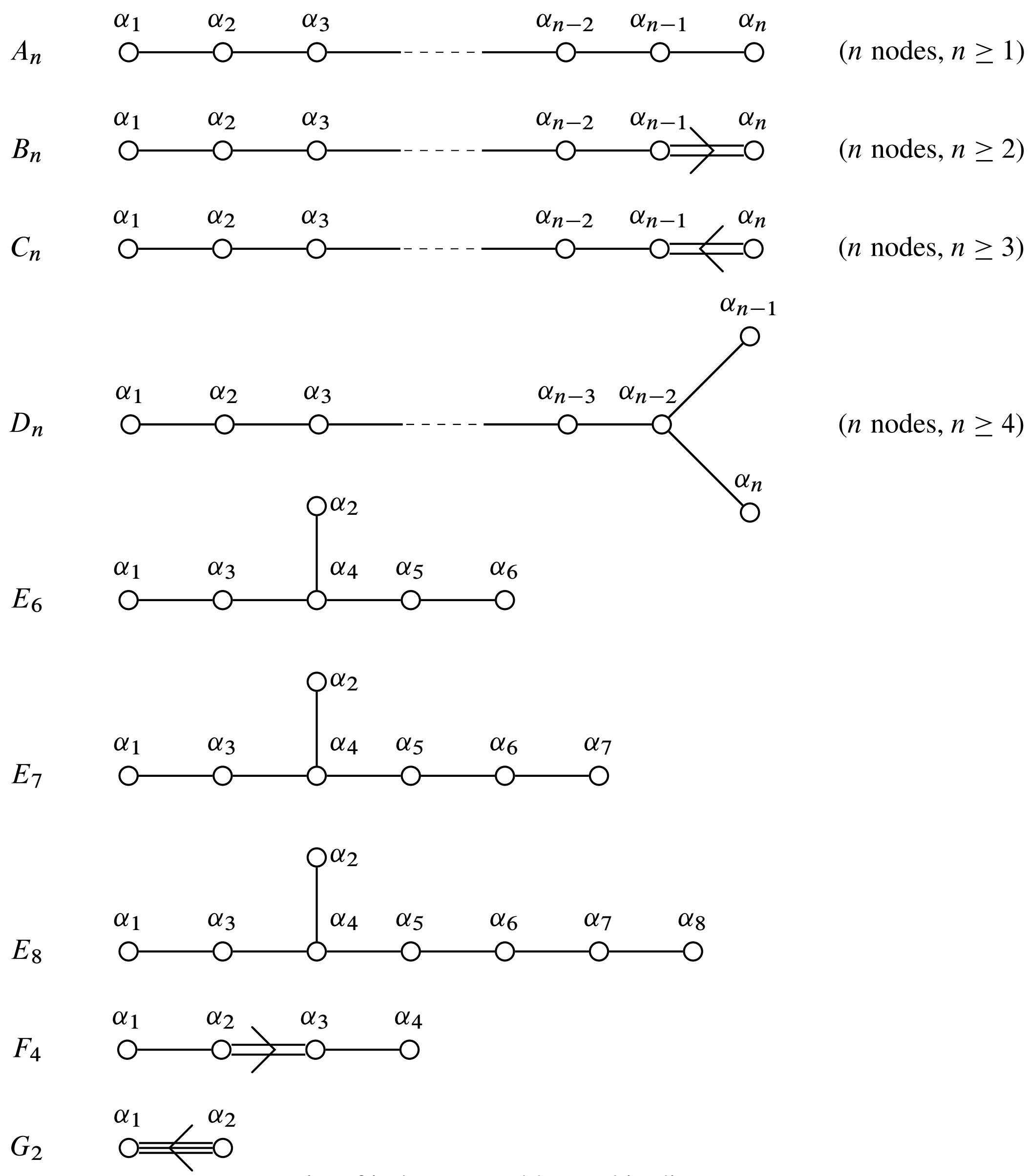
The root and weight lattices

7.20 Let X be a lattice in a vector space V over F. The ***dual lattice*** to X is

$$Y = \{y \in V^\vee \mid \langle X, y\rangle \subset \mathbb{Z}\}.$$

If $e_1, \ldots, e_m$ is a basis of V that generates X as a $\mathbb{Z}$-module, then Y is generated by the dual basis $f_1, \ldots, f_m$ (defined by $\langle e_i, f_j\rangle = \delta_{ij}$).

7.21 Let (V, R) be a root system in V. Recall that, for each $\alpha \in R$, there is a unique $\alpha^\vee \in V$ such that $\langle \alpha, \alpha^\vee\rangle = 2$, $\langle R, \alpha^\vee\rangle \in \mathbb{Z}$, and the reflection $x \mapsto x - \langle x, \alpha^\vee\rangle\alpha$ sends R into R. The set $R^\vee \overset{\text{def}}{=} \{\alpha^\vee \mid \alpha \in R\}$ is a root system in $V^\vee$ (called the ***inverse root system***).



List of indecomposable Dynkin diagrams

7.22 (Bourbaki LIE, VI, §1, 9.) Let (V, R) be a root system. The ***root lattice*** $Q = Q(R)$ is the $\mathbb{Z}$-submodule of V generated by the roots:

$$Q(R) = \mathbb{Z}R = \left\{\sum_{\alpha \in R} m_\alpha \alpha \mid m_\alpha \in \mathbb{Z}\right\}.$$

Every base for R forms a basis for Q. The ***weight lattice*** $P = P(R)$ is the lattice dual to $Q(R^\vee)$:

$$P = \{x \in V \mid \langle x, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}.$$

The elements of P are called the ***weights*** of the root system. We have $P(R) \supset Q(R)$ (because $\langle R, \alpha^\vee \rangle \subset \mathbb{Z}$ for all $\alpha \in R$), and the quotient $P(R)/Q(R)$ is finite (because the lattices generate the same $\mathbb{Q}$-vector space).

7.23 (Bourbaki LIE, VI, §1, 10.) Let S be a base for R. Then $S^\vee \stackrel{\text{def}}{=} \{\alpha^\vee \mid \alpha \in S\}$ is a base for $R^\vee$. For each simple root α, define $\varpi_\alpha \in P(R)$ by the condition

$$\langle \varpi_\alpha, \beta^\vee \rangle = \delta_{\alpha,\beta}, \quad \text{all } \beta \in S.$$

Then $\{\varpi_\alpha \mid \alpha \in S\}$ is a basis for the weight lattice $P(R)$, dual to the basis $S^\vee$. Its elements are called the ***fundamental weights***.

7.24 (Bourbaki LIE, VIII, §7.) Let S be a base for R, so that

$$R = R_+ \sqcup R_- \text{ with } \begin{cases} R_+ &= \{\sum m_\alpha \alpha \mid m_\alpha \in \mathbb{N}\} \cap R \\ R_- &= \{\sum m_\alpha \alpha_i \mid -m_\alpha \in \mathbb{N}\} \cap R \end{cases}$$

We let $P_+ = P_+(R)$ denote the set of weights that are positive for the partial ordering on V defined by S; thus

$$P_+(R) = \left\{\sum_{\alpha \in S} c_\alpha \alpha \mid c_\alpha \geq 0, \quad c_\alpha \in \mathbb{Q}\right\} \cap P(R).$$

A weight λ is ***dominant*** if $\langle \lambda, \alpha^\vee \rangle \in \mathbb{N}$ for all $\alpha \in S$, and we let $P_{++} = P_{++}(R)$ denote the set of dominant weights of R; thus

$$P_{++}(R) = \{x \in V \mid \langle x, \alpha^\vee \rangle \in \mathbb{N} \text{ all } \alpha \in S\} \subset P_+(R).$$

Since the ϖ_α are dominant, they are sometimes called the ***fundamental dominant weights***.

7.25 When we write $S = \{\alpha_1, \ldots, \alpha_n\}$, the fundamental weights are $\varpi_1, \ldots, \varpi_n$, where

$$\langle \varpi_i, \alpha_j^\vee \rangle = \delta_{ij}.$$

Moreover

$$R = R_+ \sqcup R_- \text{ with } \begin{cases} R_+ &= \{\sum m_i \alpha_i \mid m_i \in \mathbb{N}\} \cap R \\ R_- &= \{\sum m_i \alpha_i \mid -m_i \in \mathbb{N}\} \cap R \end{cases};$$

$$Q(R) = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset V = \mathbb{R}\alpha_1 \oplus \cdots \oplus \mathbb{R}\alpha_n;$$

$$P(R) = \mathbb{Z}\varpi_1 \oplus \cdots \oplus \mathbb{Z}\varpi_n \subset V = \mathbb{R}\varpi_1 \oplus \cdots \oplus \mathbb{R}\varpi_n;$$

$$P_{++}(S) = \left\{\sum m_i \varpi_i \mid m_i \in \mathbb{N}\right\}.$$

NOTES Eventually, the proofs in this section will be completed. Also, I should add a subsection explaining by means of examples how the various definitions relate to the associated Lie algebra (for example, bases correspond to Borel subalgebras), and I should stop using Bourbaki's notation P_{++}.

8 Split semisimple Lie algebras

To a semisimple Lie algebra, we attach a root system, from which we can read off the structure of the Lie algebra and its representations. As every root system arises from a semisimple Lie algebra and determines it up to isomorphism, the root systems classify the semisimple Lie algebras. In Section 7, we reviewed the theory of root systems and how they are classified in turn by Dynkin diagrams, and in this section we explain how semisimple Lie algebras are classified by root systems.

We don't assume that the ground field is algebraically closed, but we work only with semisimple Lie algebras that are "split" over the field. The remaining sections of the chapter (not yet written) will explain how to extend the theory to nonsplit Lie algebras.

This section (still) omits some proofs, for which the reader is referred to Bourbaki LIE. When the ground field k is algebraically closed field, the material is very standard, and proofs can be found in Serre 1966, Chap. VII.

Throughout this section, k is a field of characteristic zero, and all Lie algebras and all representations of Lie algebras are finite-dimensional over k.

NOTES Should probably rewrite this for split reductive Lie algebras. The extension is trivial, but useful when applying the theory to algebraic groups.

The program

Let $\mathfrak{g}$ be a semisimple Lie algebra. A Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is maximal among those consisting of semisimple elements. To say that an element h of $\mathfrak{h}$ is semisimple means that the endomorphism $\mathrm{ad}_{\mathfrak{g}} h$ of $\mathfrak{g}$ becomes diagonalizable over an extension of k. The Cartan algebra $\mathfrak{h}$ is said to be splitting if these endomorphisms are diagonalizable over k itself, and the semisimple algebra $\mathfrak{g}$ is said to be split if it contains a splitting Cartan subalgebra.

Let $\mathfrak{h}$ be a splitting Cartan subalgebra of $\mathfrak{g}$. Because $\mathfrak{h}$ consists of semisimple elements, it is commutative (5.29), and so the $\mathrm{ad}_{\mathfrak{g}} h$, $h \in \mathfrak{h}$, form a commuting family of diagonalizable endomorphisms of $\mathfrak{g}$. From linear algebra, we know that there exists a basis of simultaneous eigenvectors. In other words, $\mathfrak{g}$ is a direct sum of the subspaces

$$\mathfrak{g}^{\alpha} = \{x \in \mathfrak{g} \mid \mathrm{ad}_{\mathfrak{g}}(h)x = \alpha(h)x \text{ for all } h \in \mathfrak{h}\},$$

where α runs over the elements of the linear dual $\mathfrak{h}^{\vee}$ of $\mathfrak{h}$. The roots of $(\mathfrak{g},\mathfrak{h})$ are the nonzero α such that $\mathfrak{g}^{\alpha} \neq 0$. Let R denote the set of roots of $(\mathfrak{g},\mathfrak{h})$. Then the Lie algebra $\mathfrak{g}$ decomposes into a direct sum

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha}. \tag{42}$$

Clearly the set R is finite, and (by definition) it doesn't contain 0. We shall see (8.39) that R is a reduced root system in $\mathfrak{h}^{\vee}$.

For example, let $\mathfrak{g} = \mathfrak{sl}_{n+1}$. The subalgebra $\mathfrak{h}$ of diagonal matrices in $\mathfrak{g}$ is a Cartan subalgebra (its elements are semisimple, and it is maximal among commutative subalgebras because it equals its centralizer). The matrices

$$E_{i,i} - E_{i+1,i+1} \quad (1 \leq i \leq n) \tag{43}$$

form a basis for $\mathfrak{h}$, and together with the matrices

$$E_{ij} \quad (1 \leq i, j \leq n+1, \quad i \neq j),$$

they form a basis for $\mathfrak{g}$. Let $\{\varepsilon_1,\ldots,\varepsilon_{n+1}\}$ be the standard basis for k^{n+1}, and let V be the hyperplane in k^{n+1} consisting of the vectors $\sum a_i\varepsilon_i$ with $\sum a_i = 0$. The action

$$(\textstyle\sum a_i\varepsilon_i)(E_{ii}-E_{i+1,i+1}) = a_i - a_{i+1},$$

of $\sum a_i\varepsilon_i \in V$ on $\mathfrak{h}$ identifies V with the linear dual $\mathfrak{h}^\vee$ of $\mathfrak{h}$. Now

$$\mathfrak{g} = \mathfrak{h} \oplus \textstyle\bigoplus_{\alpha\in R}\mathfrak{g}^\alpha$$

where $R = \{\varepsilon_i - \varepsilon_j \mid i \neq j\}$ and $\mathfrak{g}^{\varepsilon_i-\varepsilon_j} = kE_{ij}$. We have already seen (7.5) that R is a root system in V.

We shall see that the isomorphism classes of split simple Lie algebras over k are in one-to-one correspondence with the indecomposable Dynkin diagrams (which don't depend on k!). Moreover, from the root system of a Lie algebra, we shall be able to read off information about its Lie subalgebras and representations.

Cartan subalgebras

Although we shall mainly be concerned with Cartan subalgebras of semisimple Lie algebras, it will be convenient to define them for general Lie algebras. Throughout, $\mathfrak{g}$ is a Lie algebra.

DEFINITION 8.1 A ***Cartan subalgebra*** of a Lie algebra is a nilpotent subalgebra equal to its own normalizer.[13]

8.2 Recall that a proper subalgebra of a nilpotent algebra is never equal to its own normalizer (2.6). Therefore a Cartan subalgebra is a *maximal* nilpotent subalgebra; in particular, the only Cartan subalgebra of a nilpotent Lie algebra is the algebra itself. Caution: not all maximal nilpotent subalgebras are Cartan subalgebras (e.g., $\mathfrak{n}_2 \subset \mathfrak{sl}_2$ is not a Cartan subalgebra).

8.3 The subalgebra $\mathfrak{h}$ of diagonal matrices in $\mathfrak{gl}_n$ is a Cartan subalgebra. It is certainly nilpotent (even commutative). Let $x = \sum a_{ij}E_{ij}$. Then (see (7), p.13),

$$[x, E_{ii}] = a_{ii}E_{ii} - (\textstyle\sum_j a_{ij}E_{ij}),$$

and so x normalizes $\mathfrak{h}$ if only if $a_{ij} = 0$ for all $i \neq j$. Similarly, the diagonal matrices with trace zero form a Cartan subalgebra of $\mathfrak{sl}_n$.

8.4 Consider Lie algebras $\mathfrak{g} \supset \mathfrak{g}' \supset \mathfrak{h}$. If $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$, then it is a Cartan subalgebra of $\mathfrak{g}'$ (obviously). For example, the diagonal matrices in $\mathfrak{b}_n$ form a Cartan subalgebra of $\mathfrak{b}_n$.

8.5 Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$, and let k' be an extension field of k. Then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ if and only if $\mathfrak{h}_{k'}$ is a Cartan subalgebra of $\mathfrak{g}_{k'}$ (apply 2.4 and (15), p.22).

[13] We follow Bourbaki LIE, VII, §2. The definition in Erdmann and Wildon 2006, 10.2, differs.

Regular elements

The most convenient way of constructing Cartan subalgebras is as the centralizers (or, more generally, the nilspaces) of certain "regular" elements of $\mathfrak{g}$. Here "regular" means "general" in a particular sense. Consider, for example, $\mathfrak{g} = \mathfrak{gl}_V$ where V is a vector space over an algebraically closed field. The Cartan subalgebras of $\mathfrak{g}$ are exactly those that become the subalgebra of diagonal matrices after some choice of a basis for V. Such a subalgebra is the centralizer of any element with matrix

$$x = \operatorname{diag}(c_1, \ldots, c_n), \quad c_i \text{ distinct},$$

relative to the same basis. Indeed (see (7), p.13),

$$[E_{ij}, x] = \left(c_i - c_j\right) E_{ij}, \quad 1 \le i, j \le n,$$

and so $[\sum a_{ij} E_{ij}, x] = 0$ if and only if $a_{ij} = 0$ for $i \neq j$. Therefore the Cartan subalgebras are exactly the centralizers of the semisimple elements of $\mathfrak{g}$ having distinct eigenvalues.

Now consider a general Lie algebra $\mathfrak{g}$. We let $P_x(T)$ denote the characteristic polynomial of the linear map $\operatorname{ad} x \colon \mathfrak{g} \to \mathfrak{g}$:

$$P_x(T) = \det(T - \operatorname{ad}(x) \mid \mathfrak{g}).$$

For $x \in \mathfrak{g}$, we let $n(x)$ denote the multiplicity of 0 as an eigenvalue of $\operatorname{ad} x$ acting on $\mathfrak{g}$ (equal to the multiplicity of T as a factor of $P_x(T)$).

DEFINITION 8.6 The ***rank*** n of $\mathfrak{g}$ is $\min\{n(x) \mid x \in \mathfrak{g}\}$. An element x of $\mathfrak{g}$ is ***regular*** if $n(x) = n$.

For example, let $\mathfrak{g} = \mathfrak{gl}_V$ and let x be a semisimple element of $\mathfrak{g}$. If $(c_i)_{1 \le i \le n}$, $n = \dim V$, is the family of eigenvalues of x on V, then $(c_i - c_j)_{1 \le i, j \le n}$ is the family of eigenvalues of $\operatorname{ad} x$ on $\mathfrak{g}$, and so

$$P_x(T) = \prod_{1 \le i, j \le n} \left(T - c_i + c_j\right) = T^{n(x)} \prod_{c_i \neq c_j} \left(T - c_i + c_j\right)$$

with $n(x) = \#\{(i, j) \mid c_i = c_j\}$. It follows that the rank of $\mathfrak{gl}_V$ is n, and an element x of $\mathfrak{gl}_V$ is regular if and only if is semisimple with distinct eigenvalue.

Let V be a vector space over k. A ***polynomial function*** on V is a map $f \colon V \to k$ such that, for one (hence every) choice of a basis for V, $f(P)$ is a polynomial in the coordinates of P. For example, for an endomorphism α of V, let

$$P_\alpha(T) = \det(T - \alpha | V) = T^m + a_{m-1}(\alpha) T^{m-1} + \cdots + a_0(\alpha), \quad a_i(\alpha) \in k.$$

Then

$$a_i(\alpha) = (-1)^{m-i} \operatorname{Tr}(\textstyle\bigwedge^{m-i} \alpha)$$

is a polynomial function on $\operatorname{End}(V)$. Similarly, for $x \in \mathfrak{g}$,

$$P_x(T) = T^m + a_{m-1}(x) T^{m-1} + \cdots + a_0(x)$$

where $a_i(x)$ is a polynomial function on the vector space $\mathfrak{g}$. Now (8.6) can be rephrased as:

8.7 The rank of $\mathfrak{g}$ is the smallest natural number n such that the polynomial function a_n is not the zero function. An element x of $\mathfrak{g}$ is regular if $a_n(x) \neq 0$.

Cartan subalgebras exist

In this subsubsection, we prove that every Lie algebra $\mathfrak{g}$ has a Cartan subalgebra.

Let α be an endomorphism of a vector space V. For $\lambda \in k$, V_λ denotes the eigenspace of λ and V^λ the primary space of λ. The primary space for $\lambda = 0$,

$$V^0 \stackrel{\text{def}}{=} \{v \in V \mid \alpha^m v = 0 \text{ for some } m \geq 1\},$$

is called the ***nilspace*** of α.

We apply this terminology to $\mathrm{ad}_{\mathfrak{g}} x$, $x \in \mathfrak{g}$. Thus

$$\mathfrak{g}_x^\lambda = \{y \in \mathfrak{g} \mid (\mathrm{ad}\, x - \lambda)^m y = 0 \text{ for all sufficiently large } m\}$$
$$\mathfrak{g}_x^0 = \{y \in \mathfrak{g} \mid (\mathrm{ad}\, x)^m y = 0 \text{ for all sufficiently large } m\}.$$

When x is semisimple, $\mathfrak{g}_x^\lambda = \mathfrak{g}_\lambda$; in particular,

$$\mathfrak{g}_x^0 = \{y \in \mathfrak{g} \mid [x,y] = 0\} = \text{centralizer of } x \text{ in } \mathfrak{g}.$$

Note that the dimension of the nilspace of x is the multiplicity $n(x)$ of 0 as an eigenvalue of x; when x is regular, it equals the rank of $\mathfrak{g}$.

LEMMA 8.8 *Let* $x \in \mathfrak{g}$.

(a) *If all the eigenvalues of* $\mathrm{ad}\, x$ *lie in* k, *then* $\mathfrak{g} = \bigoplus_{\lambda \in k} \mathfrak{g}_x^\lambda$.
(b) $[\mathfrak{g}_x^\lambda, \mathfrak{g}_x^\mu] \subset \mathfrak{g}_x^{\lambda+\mu}$ *for all* $\lambda, \mu \in k$;
(c) $\mathfrak{g}_x^0$ *is a Lie subalgebra of* $\mathfrak{g}$.

PROOF. (a) This is a statement in linear algebra (1.21).

(b) For $\lambda, \mu \in k$ and $y, z \in \mathfrak{g}$,

$$(\mathrm{ad}\, x - \lambda - \mu)^m [y,z] = \sum\nolimits_{i=1}^{m} \tbinom{m}{i} [(\mathrm{ad}\, x - \lambda)^i y, (\mathrm{ad}\, x - \mu)^{m-i} z)].$$

If $y \in \mathfrak{g}_x^\lambda$ and $z \in \mathfrak{g}_x^\mu$, then all the terms on the right hand side are zero for m sufficiently large, and so $[y,z] \in \mathfrak{g}_x^{\lambda+\mu}$.

(c) From (b), we see that $[\mathfrak{g}_x^0, \mathfrak{g}_x^0] \subset \mathfrak{g}_x^0$. □

We shall need to use some elementary results concerning the Zariski topology (see AG, Chapter 2). For an ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$, let

$$V(\mathfrak{a}) = \{(c_1, \ldots, c_m) \in k^m \mid f(c_1, \ldots, c_m) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

The Zariski topology on k^n is that for which the closed sets are those of the form $V(\mathfrak{a})$ for some ideal $\mathfrak{a}$. The open sets are finite unions of sets of the form

$$D(f) = \{(c_1, \ldots, c_m) \in k^m \mid f(c_1, \ldots, c_m) \neq 0\}.$$

If f is nonzero and k is infinite, the set $D(f)$ is nonempty AG, Exercise 1-1.

THEOREM 8.9 *The nilspace* $\mathfrak{g}_x^0$ *of any regular element* x *of* $\mathfrak{g}$ *is a Cartan subalgebra of* $\mathfrak{g}$.

PROOF. In proving that $\mathfrak{g}_x^0$ is a Cartan subalgebra, we may assume that k is algebraically closed (see 8.5). Let

$$U_1 = \{y \in \mathfrak{g}_x^0 \mid \operatorname{ad}_{\mathfrak{g}} y|\mathfrak{g}_x^0 \text{ is not nilpotent}\}$$
$$U_2 = \{y \in \mathfrak{g}_x^0 \mid \operatorname{ad}_{\mathfrak{g}} y|\left(\mathfrak{g}/\mathfrak{g}_x^0\right) \text{ is invertible}\}.$$

These are both Zariski-open subsets of $\mathfrak{g}_x^0$, and U_2 is nonempty because it contains x. According to Engel's theorem (2.11), to show that $\mathfrak{g}_x^0$ is nilpotent, it suffices to show that U_1 is empty. If U_1 is nonempty, then there exists a $y \in U_1 \cap U_2$ (both U_1 and U_2 are nonempty Zariski-open subsets of an irreducible set). But for such a y, $n(y) < \dim \mathfrak{g}_x^0 = n(x)$, contradicting the regularity of x. Hence $\mathfrak{g}_x^0$ is nilpotent.

It remains to show that, $\mathfrak{g}_x^0$ equals its normalizer. If z normalizes $\mathfrak{g}_x^0$, then $[z,x] \in \mathfrak{g}_x^0$, i.e., $(\operatorname{ad} x)^m[z,x] = 0$ for some $m \geq 1$. But then $(\operatorname{ad} x)^{m+1} z = 0$, and so $z \in \mathfrak{g}_x^0$. □

COROLLARY 8.10 *Every Lie algebra contains a Cartan subalgebra.*

PROOF. The set $\mathcal{R}$ of regular elements in $\mathfrak{g}$ is a nonempty Zariski-open subset of $\mathfrak{g}$, namely, it is the set where the polynomial function a_n is nonzero ($n = \operatorname{rank} \mathfrak{g}$). Because k is infinite, $\mathcal{R}$ is nonempty. □

COROLLARY 8.11 *Every Lie algebra is a sum of its Cartan subalgebras.*

PROOF. The sum of the Cartan subalgebras of $\mathfrak{g}$ is a k-subspace of $\mathfrak{g}$. Hence it is closed for the Zariski topology, but it contains the Zariski-dense set of regular elements. □

COROLLARY 8.12 *Let $\mathfrak{a}$ be a subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ such that $\operatorname{ad}_{\mathfrak{g}} a$ is semisimple for all $a \in \mathfrak{a}$. Then $\mathfrak{a}$ is contained in a Cartan subalgebra of $\mathfrak{g}$.*

PROOF. Let $\mathfrak{c} = c_{\mathfrak{g}}(\mathfrak{a})$ be the centralizer of $\mathfrak{a}$ in $\mathfrak{g}$, and let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{c}$. As $\mathfrak{a}$ is commutative (5.28), it lies in the centre of $\mathfrak{c}$, and so $\mathfrak{a} \subset n_{\mathfrak{c}}(\mathfrak{h}) = \mathfrak{h}$. We shall show that $\mathfrak{h} = n_{\mathfrak{g}}(\mathfrak{h})$; so $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ containing $\mathfrak{a}$.

The elements $\operatorname{ad}_{\mathfrak{g}}(a)$, $a \in \mathfrak{a}$, form a commuting set of semisimple endomorphisms of the k-vector space $\mathfrak{g}$, and so $\mathfrak{g}$ is semisimple when regarded as a module over the k-algebra generated by them. Therefore,

$$n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h} \oplus \mathfrak{d}$$

for some subspace $\mathfrak{d}$ of $n_{\mathfrak{g}}(\mathfrak{h})$ stable under $\mathfrak{a}$. Now

$$[\mathfrak{a},\mathfrak{d}] \subset [\mathfrak{h},\mathfrak{d}] \subset [\mathfrak{h}, n_{\mathfrak{g}}(\mathfrak{h})] = \mathfrak{h}.$$

As $[\mathfrak{a},\mathfrak{d}] \subset \mathfrak{d}$ and $\mathfrak{h} \cap \mathfrak{d} = 0$, this shows that $[\mathfrak{a},\mathfrak{d}] = 0$. In other words $\mathfrak{d} \subset \mathfrak{c}$, and so $n_{\mathfrak{g}}(\mathfrak{h}) \subset \mathfrak{c}$. Therefore, $n_{\mathfrak{g}}(\mathfrak{h}) = n_{\mathfrak{g}}(\mathfrak{h}) \cap \mathfrak{c} = n_{\mathfrak{c}}(\mathfrak{h}) = \mathfrak{h}$. □

NOTES For a more constructive proof of the existence of Cartan subalgebras, see Casselman, Introduction to Lie algebras, §11,

Cartan subalgebras in semisimple Lie algebras

8.13 Let $\mathfrak{h}$ be a Cartan subalgebra in a semisimple Lie algebra $\mathfrak{g}$, and assume that

$$\mathfrak{g}=\mathfrak{h}\oplus\bigoplus\nolimits_{\alpha\in R}\mathfrak{g}^{\alpha},\quad R\subset\mathfrak{h}^{\vee}\smallsetminus 0. \tag{44}$$

This is true, for example, when k is algebraically closed. Let $x\in\mathfrak{g}^{\alpha}$ and $y\in\mathfrak{g}^{\beta}$. Because the Cartan-Killing form κ is invariant,

$$\kappa(\operatorname{ad}(h)x,y)+\kappa(x,\operatorname{ad}(h)y)=0,$$

and so

$$(\alpha(h)+\beta(h))\kappa(x,y)=0$$

for all $h\in\mathfrak{h}$. Hence $\kappa(x,y)=0$ unless $\alpha+\beta=0$. It follows that

$$\mathfrak{g}=\mathfrak{h}\oplus\bigoplus\nolimits_{R/\pm}(\mathfrak{g}^{\alpha}\oplus\mathfrak{g}^{-\alpha}) \tag{45}$$

is a decomposition of $\mathfrak{g}$ into mutually orthogonal subspaces for κ. Because κ is nondegenerate (4.13), its restriction to $\mathfrak{h}$, and to each of the $(\mathfrak{g}^{\alpha}\oplus\mathfrak{g}^{-\alpha})$, is nondegenerate (and because the restriction of κ to $\mathfrak{g}^{\alpha}$ is zero, $\mathfrak{g}^{\alpha}$ and $\mathfrak{g}^{-\alpha}$ are dual).

THEOREM 8.14 *Let $\mathfrak{h}$ be a Cartan subalgebra of a semisimple Lie algebra $\mathfrak{g}$.*

(a) *Every element of $\mathfrak{h}$ is semisimple (and so $\mathfrak{h}$ is commutative (5.29)).*
(b) *The centralizer of $\mathfrak{h}$ in $\mathfrak{g}$ is $\mathfrak{h}$.*
(c) *The restriction of the Cartan-Killing form of $\mathfrak{g}$ to $\mathfrak{h}$ is nondegenerate.*

PROOF. It suffices prove this after k has been replaced by a larger field, and so we may suppose that there exists a decomposition (44). Thus, we have already proved (c).

Because $\mathfrak{g}$ has trivial centre, the adjoint representation realizes $\mathfrak{h}$ as a Lie subalgebra of $\mathfrak{gl}_{\mathfrak{g}}$. Now Lie's theorem (3.7) shows that there exists a basis for $\mathfrak{g}$ such that $\operatorname{ad}\mathfrak{h}\subset\mathfrak{b}_m$. Hence $\operatorname{ad}([\mathfrak{h},\mathfrak{h}])\subset\mathfrak{n}_m$, and so $\operatorname{Tr}_{\mathfrak{g}}(\mathfrak{h},[\mathfrak{h},\mathfrak{h}])=0$, i.e., $\kappa(\mathfrak{h},[\mathfrak{h},\mathfrak{h}])=0$. As κ is nondegenerate on $\mathfrak{h}$, we see that $[\mathfrak{h},\mathfrak{h}]=0$ and $\mathfrak{h}$ is commutative. Now $\mathfrak{h}\subset c_{\mathfrak{g}}(\mathfrak{h})\subset n_{\mathfrak{g}}(\mathfrak{h})$. As $\mathfrak{h}=n_{\mathfrak{g}}(\mathfrak{h})$ (by definition), we see that (b) holds.

Let $x\in\mathfrak{h}$, and let $x=x_s+x_n$ be its Jordan decomposition in $\mathfrak{g}$ (see 5.26). Because $\operatorname{ad}x_s$ and $\operatorname{ad}x_n$ are polynomials in $\operatorname{ad}x$, they centralize $\mathfrak{h}$. Therefore, they lie in $\mathfrak{h}$. Because $\operatorname{ad}x_n$ commutes with $\operatorname{ad}y$ for $y\in\mathfrak{h}$, the composite $\operatorname{ad}(y)\circ\operatorname{ad}(x_n)$ is nilpotent, and so its trace $\kappa(y,x_n)=0$. As $\kappa|\mathfrak{h}$ is nondegenerate, this shows that $x_n=0$. □

COROLLARY 8.15 *The Cartan subalgebras of a semisimple Lie algebra are those that are maximal among the subalgebras whose elements are semisimple.*

PROOF. Let $\mathfrak{g}$ be a semisimple Lie algebra. Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$, and suppose that $\mathfrak{h}$ is contained in a Lie subalgebra $\mathfrak{h}'$. If the elements of $\mathfrak{h}'$ are semisimple, then $\mathfrak{h}'$ is commutative (5.29), and so $\mathfrak{h}'\subset c_{\mathfrak{g}}(\mathfrak{h})=\mathfrak{h}$.

Let $\mathfrak{a}$ be a subalgebra of $\mathfrak{g}$ whose elements are semisimple. Then $\mathfrak{a}\subset\mathfrak{h}$ for some Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ (8.12). The elements of $\mathfrak{h}$ are semisimple, and so, if $\mathfrak{a}$ is maximal, then $\mathfrak{a}=\mathfrak{h}$. □

COROLLARY 8.16 *The regular elements of a semisimple Lie algebra are semisimple.*

PROOF. Every regular element is contained in a Cartan subgroup. □

Cartan subalgebras are conjugate (k algebraically closed)

Recall (6.21) that an automorphism of a Lie algebra $\mathfrak{g}$ is said to be elementary if it is a product of automorphisms of the form $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$, $\mathrm{ad}_{\mathfrak{g}}(x)$ nilpotent, and $\mathrm{Aut}_e(\mathfrak{g})$ is the group of elementary automorphisms.

THEOREM 8.17 *Any two Cartan subgroups of a Lie algebra over an algebraically closed field are conjugate by an elementary automorphism.*

After some preliminaries, we prove a more precise result (8.20). *From now on, k is algebraically closed.*

LEMMA 8.18 *Let $f: V \to W$ be a regular map of nonsingular irreducible algebraic varieties. Assume that for some $P \in V$, the map $(df)_P : \mathrm{Tgt}_P V \to \mathrm{Tgt}_{f(P)} W$ on tangent spaces is surjective. Then the image under f of every nonempty open subset of V contains a nonempty open subset of W.*

PROOF. The hypotheses imply that f is dominant (e.g., AG 5.32). Now apply AG 10.2. (In fact, we need this only in the case that V and W are affine spaces, i.e., of the form $\mathbb{A}^m$ for some m. In this case, there is a completely elementary proof, which I will include, eventually. See Bourbaki LIE VII, Appendix I, p.45, or Casselman, Introduction to Lie algebras, 12.2.) □

Let $\mathfrak{g}$ be a Lie algebra over k, and let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. For $\alpha \in \mathfrak{h}^\vee$, let $\mathfrak{g}^\alpha$ be the set of $x \in \mathfrak{g}$ such that, for every $h \in \mathfrak{h}$,

$$(\mathrm{ad}_{\mathfrak{g}}(h) - \alpha(h))^n x = 0$$

for all sufficiently large n. Let $R(\mathfrak{g},\mathfrak{h})$ be the set of nonzero $\alpha \in \mathfrak{h}^\vee$ such that $\mathfrak{g}^\alpha \neq 0$. We assume that

$$\mathfrak{g} = \mathfrak{g}^0 \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^\alpha.$$

When $\mathfrak{g}$ is semisimple, the elements $\mathrm{ad}_{\mathfrak{g}}(h)$, $h \in \mathfrak{h}$, form a commuting family of semsimple endomorphisms (8.14), and so this is obvious from linear algebra; moreover,

$$\mathfrak{g}^\alpha = \{x \in \mathfrak{g} \mid \mathrm{ad}_{\mathfrak{g}}(h)x = \alpha(h)x, \text{ all } h \in \mathfrak{h}\}.$$

For the general case, see Theorem 2.15.

LEMMA 8.19 *The set $\mathfrak{h}_r$ of $h \in \mathfrak{h}$ such that $\mathfrak{g}_h^0 = \mathfrak{h}$ is open and dense in $\mathfrak{h}$ (for the Zariski topology).*

PROOF. The condition that $h \in \mathfrak{h}_r$ is that $\prod_{\alpha \in R} \alpha(h) \neq 0$, which is a polynomial condition. □

As in (8.8), $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] \subset \mathfrak{g}^{\alpha+\beta}$. Therefore for $x \in \mathfrak{g}^\alpha$, $\mathrm{ad}_{\mathfrak{g}}(x)$ maps $\mathfrak{g}^\beta$ into $\mathfrak{g}^{\alpha+\beta}$ and $\left(\mathrm{ad}_{\mathfrak{g}}(x)\right)^r$ maps $\mathfrak{g}^\beta$ into $\mathfrak{g}^{\beta+r\alpha}$, which is zero for large r. Hence $\mathrm{ad}_{\mathfrak{g}}(x)$ is nilpotent, and so we can therefore form $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$, which is an elementary automorphism of $\mathfrak{g}$. Let $E(\mathfrak{h})$ denote the subgroup of $\mathrm{Aut}_e(\mathfrak{g})$ generated by the automorphisms $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$ where $x \in \mathfrak{g}^\alpha$ for some $\alpha \in R(\mathfrak{g},\mathfrak{h})$.

LEMMA 8.20 *Let $\mathfrak{h}$ and $\mathfrak{h}'$ be Cartan subalgebras of $\mathfrak{g}$. There exist $u \in E(\mathfrak{h})$ and $u' \in E(\mathfrak{h}')$ such that*

$$u(\mathfrak{h}) = u'(\mathfrak{h}').$$

PROOF. Number the elements of $R(\mathfrak{g},\mathfrak{h})$ as $\alpha_1,\ldots,\alpha_n$, and consider the map

$$f\colon \mathfrak{g}^{\alpha_1}\times\cdots\times\mathfrak{g}^{\alpha_n}\times\mathfrak{h}\to\mathfrak{g},\quad (x_1,\ldots,x_n,h)\mapsto e^{\operatorname{ad}x_1}\cdots e^{\operatorname{ad}x_n}h.$$

We calculate its differential at $(0,\ldots,0,h_0)$. Note that

$$f(x_1,\ldots,x_n,h+h_0) = \sum\frac{[x_1^{m_1},[x_2^{m_2},\ldots,h]\ldots]}{\prod m_i!} + \sum\frac{[x_1^{m_1},[x_2^{m_2},\ldots,h_0]\ldots]}{\prod m_i!} \tag{46}$$

where we have put $[x^k,y] = \operatorname{ad}(x)^k(y)$. The terms containing h are of degree $m_1+\cdots+m_n$. The terms of degree 1 in (46) are therefore h and $[x_i,h_0]$, and so

$$(df)_{(0,\ldots,0,h_0)} = h + \sum[x_i,h_0].$$

Suppose that $\prod_\alpha \alpha(h_0)\neq 0$; then the determinant of $\operatorname{ad}h_0$ in $\sum_\alpha \mathfrak{g}^\alpha$ equals $\prod_\alpha\alpha(h_0)$, which is nonzero. Hence df at the point $(0,\ldots,0,h_0)$ is an isomorphism $\mathfrak{g}\to\mathfrak{g}$. Hence f is a dominant map, and so $E(\mathfrak{h})\cdot\mathfrak{h}_r$ contains a dense open subset of $\mathfrak{g}$. Similarly, $E(\mathfrak{h}')\cdot\mathfrak{h}'_r$ contains a dense open subset of $\mathfrak{g}$, and so their intersection is nonempty. This means that

$$u(h) = u'(h')$$

for some $u\in E(\mathfrak{h})$, $h\in\mathfrak{h}_r$, $u'\in E(\mathfrak{h}')$, $h'\in\mathfrak{h}'_r$. Now

$$u(\mathfrak{h}) = u(\mathfrak{g}_h^0) = \mathfrak{g}_{u(h)}^0 = \mathfrak{g}_{u'(h')}^0 = u'(\mathfrak{g}_{h'}^0) = u'(\mathfrak{h}').$$ □

COROLLARY 8.21 *All Cartan subalgebras in a Lie algebra have the same dimension, namely, the rank of $\mathfrak{g}$ (k not necessarily algebraically closed).*

PROOF. This is obvious from the theorem when k is algebraically closed. However, the rank of $\mathfrak{g}$ doesn't change under extension of the base field (obviously), and Cartan subalgebras stay Cartan subalgebras (8.5). □

ASIDE 8.22 It is not true that all Cartan subalgebras of $\mathfrak{g}$ are conjugate when k is not algebraically closed. The problem is that the set $\mathcal{R}$ of regular elements in $\mathfrak{g}$ may fall into several different connected components. We shall see below (8.56) that all *splitting* Cartan subalgebras of a semisimple Lie algebra are conjugate.

ASIDE 8.23 In the standard proof of the Theorem 8.17 (e.g., Serre 1966), k is assumed to be $\mathbb{C}$, and two Cartan subalgebras are shown to be conjugate only by an element of the group of automorphisms of $\mathfrak{g}$ generated by elements of the form $e^{\operatorname{ad}x}$, $x\in\mathfrak{g}$ (not necessarily nilpotent). The proof given here, following Bourbaki LIE VII, §3, 2, is due to Chevalley.

Split semisimple Lie algebras

DEFINITION 8.24 A Cartan subalgebra $\mathfrak{h}$ of a semisimple Lie algebra $\mathfrak{g}$ is said to be ***splitting*** if the eigenvalues of the linear maps $\mathrm{ad}(h)\colon \mathfrak{g} \to \mathfrak{g}$ lie in k for all $h \in \mathfrak{h}$. A ***split semisimple Lie algebra*** is a pair $(\mathfrak{g}, \mathfrak{h})$ consisting of a semisimple Lie algebra $\mathfrak{g}$ and a splitting Cartan subalgebra $\mathfrak{h}$.

More loosely, we say that a semisimple Lie algebra $\mathfrak{g}$ is ***split*** if it contains a splitting Cartan subalgebra (Bourbaki LIE, VIII, §2, 1, Déf. 1, says splittable).

8.25 The Cartan subalgebra of $\mathfrak{sl}_n$ consisting of the diagonal elements in $\mathfrak{sl}_n$ is splitting.

8.26 When k is algebraically closed, every Cartan subalgebra of a semisimple Lie algebra is splitting (obviously), and so every semisimple Lie algebra is split. On the other hand, when k is not algebraically closed, there may exist nonsplit semisimple Lie algebras, and a split semisimple Lie may have Cartan subalgebras that are not splitting. For example, when regarded as a Lie algebra over $\mathbb{R}$, $\mathfrak{sl}_2(\mathbb{C})$ is semisimple but not split, and $\left\{\left(\begin{smallmatrix} 0 & -a \\ a & 0 \end{smallmatrix}\right) \mid a \in \mathbb{R}\right\}$ is a Cartan subalgebra of $\mathfrak{sl}_2(\mathbb{R})$ which is not splitting.

8.27 Any two split semisimple Lie algebras $(\mathfrak{g}, \mathfrak{h})$ and $(\mathfrak{g}, \mathfrak{h}')$ are isomorphic: more precisely, there exists an elementary automorphism e of $\mathfrak{g}$ such that $e(\mathfrak{h}) = \mathfrak{h}'$ (see 8.56 below).

The roots of a split semisimple Lie algebra

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra. For each $h \in \mathfrak{h}$, the action of $\mathrm{ad}_{\mathfrak{g}}(h)$ is semisimple with eigenvalues in k, and so $\mathfrak{g}$ has a basis of eigenvectors for $\mathrm{ad}_{\mathfrak{g}}(h)$. Because $\mathfrak{h}$ is commutative (8.14), the $\mathrm{ad}_{\mathfrak{g}}(h)$ form a commuting family of diagonalizable endomorphisms of $\mathfrak{g}$, and so there exists a basis of simultaneous eigenvectors. In other words, $\mathfrak{g}$ is a direct sum of the subspaces

$$\mathfrak{g}^{\alpha} \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid [h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}\}$$

with α in the linear dual $\mathfrak{h}^{\vee}$ of $\mathfrak{h}$. Note that $\mathfrak{g}^0$ is the centralizer of $\mathfrak{h}$ in $\mathfrak{g}$, which equals $\mathfrak{h}$ (8.14). The ***roots*** of $(\mathfrak{g}, \mathfrak{h})$ are the nonzero α such that $\mathfrak{g}^{\alpha} \neq 0$. Write $R = R(\mathfrak{g}, \mathfrak{h})$ for the set of roots of $(\mathfrak{g}, \mathfrak{h})$. Then the Lie algebra $\mathfrak{g}$ decomposes into a direct sum[14]

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha}.$$

Clearly the set R is finite, and (by definition) doesn't contain 0. We shall see that R is a reduced root system in $\mathfrak{h}^{\vee}$, but first we look at the basic example of $\mathfrak{sl}_2$.

Example: $\mathfrak{sl}_2$

Just as the first step in understanding root systems is to understand those of rank 2, the first step in understanding the structure of semisimple Lie algebras is to understand the structure of $\mathfrak{sl}_2$ and its representations. This is truly elementary and very standard, and so in this version of the notes I'll simply state the results. See, for example, Serre 1966, Chap. IV, for the proofs.

[14]Some authors call this the Cartan decomposition of $\mathfrak{g}$, but this conflicts with the terminology for real Lie algebras.

8.28 Recall that $\mathfrak{sl}_2$ is the Lie algebra of 2×2 matrices with trace 0. Let

$$x=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad h=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad y=\begin{pmatrix}0&0\\1&0\end{pmatrix}.$$

Then

$$[x,y]=h,\quad [h,x]=2x,\quad [h,y]=-2y.$$

Therefore $\{x,h,y\}$ is a basis of eigenvectors for $\operatorname{ad}h$ with integer eigenvalues $2,0,-2$, and

$$\begin{aligned}\mathfrak{sl}_2&=\mathfrak{g}^{\alpha}\oplus\mathfrak{h}\oplus\mathfrak{g}^{-\alpha}\\&=kx\oplus kh\oplus ky\end{aligned}$$

where $\mathfrak{h}=kh$ (k-subspace spanned by h) and α is the linear map $\mathfrak{h}\to k$ such that $\alpha(h)=2$. The decomposition shows that $\mathfrak{h}$ is equal to its centralizer, and so it is a splitting Cartan subalgebra for $\mathfrak{g}$. Hence, $\mathfrak{sl}_2$ is a split semisimple Lie group of rank one. Let $R=\{\alpha\}\subset\mathfrak{h}^{\vee}$. Then R is a root system in $\mathfrak{h}^{\vee}$: it is finite, spans $\mathfrak{h}^{\vee}$, and doesn't contain 0; if we let $\alpha^{\vee}$ denote h regarded as an element of $(\mathfrak{h}^{\vee})^{\vee}$, then $\langle\alpha,\alpha^{\vee}\rangle=2$, the reflection $x\mapsto x-\langle x,\alpha^{\vee}\rangle\alpha$ maps R to R, and $\langle\alpha,\alpha^{\vee}\rangle\in\mathbb{Z}$. The root lattice $Q=\mathbb{Z}\alpha$ and the weight lattice $P=\mathbb{Z}\frac{\alpha}{2}$.

8.29 Let W_1 be the vector space $k\times k$ with its natural action of $\mathfrak{sl}_2$, and let W_m be the mth symmetric power of W_1 (more concretely, W_m consists of the homogeneous polynomials of degree m in X and Y with x,h,y acting respectively as $X\frac{\partial}{\partial Y}$, $X\frac{\partial}{\partial X}-Y\frac{\partial}{\partial Y}$, $Y\frac{\partial}{\partial X}$).

(a) The $\mathfrak{sl}_2$-module W_m has a basis $e_0,\dots,e_m$ such that

$$\begin{cases}he_n&=&(m-2n)e_n\\ ye_n&=&(n+1)e_{n+1}\\ xe_n&=&(m-n+1)e_{n-1}\end{cases}$$

(with the convention $e_{-1}=0=e_{m+1}$). In particular, W_m has dimension $m+1$.

(b) The $\mathfrak{sl}_2$-module W_m is simple, and every finite-dimensional simple $\mathfrak{sl}_2$-module is isomorphic to exactly one W_m.

(c) Every finite-dimensional dimensional $\mathfrak{sl}_2$-module is isomorphic to a direct sum of modules W_m.

(d) Let V be a finite-dimensional $\mathfrak{sl}_2$-module. The endomorphism of V defined by h is diagonalizable, with integers as its eigenvalues. Let V^n be the eigenspace of n; for any $n\in\mathbb{N}$, the linear maps $y^n\colon V^n\to V^{-n}$ and $x^n\colon V^{-n}\to V^n$ are isomorphisms.

8.30 Let V be an $\mathfrak{sl}_2$-module, and let $\lambda\in k$. A nonzero element $e\in V$ is ***primitive*** of ***weight*** λ if $he=\lambda e$ and $xe=0$. In other words, e is primitive if and only if the line ke is stable under the Borel subgroup $\mathfrak{b}=kh+kx$ (if $he=\lambda e$ and $xe=\mu e$, then, on applying the equality $[h,x]=2x$ to e, we find that $2\mu e=0$, and so $\mu=0$). Lie's theorem 3.8 (or a more elementary argument) shows that every representation of $\mathfrak{sl}_2$ has a primitive element. Let V be a finite-dimensional $\mathfrak{g}$-module generated by a primitive element e; then e has weight $m\in\mathbb{N}$, and V has dimension $m+1$.

The copy of $\mathfrak{sl}_2$ attached to a root α of $\mathfrak{g}$

Throughout this subsection, $(\mathfrak{g},\mathfrak{h})$ is a split semisimple Lie algebra. Recall that

$$\mathfrak{g}=\mathfrak{h}\oplus\bigoplus\nolimits_{\alpha\in R}\mathfrak{g}^{\alpha}$$

where R is the set of roots of $(\mathfrak{g},\mathfrak{h})$, i.e., R is the set of nonzero $\alpha\in\mathfrak{h}^{\vee}$ whose eigenspace

$$\mathfrak{g}^{\alpha}=\{x\in\mathfrak{g}\mid \mathrm{ad}(h)(x)=\alpha(h)x \text{ for all } h\in\mathfrak{h}\}$$

is nonzero.

THEOREM 8.31 *Let α be a root of $(\mathfrak{g},\mathfrak{h})$.*

(a) *The subspaces $\mathfrak{g}^{\alpha}$ and $\mathfrak{h}_{\alpha}\overset{\text{def}}{=}[\mathfrak{g}^{\alpha},\mathfrak{g}^{-\alpha}]$ of $\mathfrak{g}$ are both one-dimensional.*
(b) *There is a unique element $h_{\alpha}\in\mathfrak{h}_{\alpha}$ such that $\alpha(h_{\alpha})=2$.*
(c) *For each nonzero $x_{\alpha}\in\mathfrak{g}^{\alpha}$, there is a unique $y_{\alpha}\in\mathfrak{g}^{-\alpha}$ such that*

$$[x_{\alpha},y_{\alpha}]=h_{\alpha},\quad [h_{\alpha},x_{\alpha}]=2x_{\alpha},\quad [h_{\alpha},y_{\alpha}]=-2y_{\alpha}.$$

Hence

$$\mathfrak{s}_{\alpha}\overset{\text{def}}{=}kx_{\alpha}\oplus kh_{\alpha}\oplus ky_{\alpha}=\mathfrak{g}^{-\alpha}\oplus\mathfrak{h}_{\alpha}\oplus\mathfrak{g}^{\alpha}$$

is a copy of $\mathfrak{sl}_2$ inside $\mathfrak{g}$.

An $\mathfrak{sl}_2$***-triple*** in a Lie algebra $\mathfrak{g}$ is a triple $(x,h,y)\neq(0,0,0)$ of elements such that[15]

$$[x,y]=h,\quad [h,x]=2x,\quad [h,y]=-2y.$$

Given an $\mathfrak{sl}_2$-triple, we usually regard $\mathfrak{s}=kx\oplus kh\oplus ky$ as a "copy" of $\mathfrak{sl}_2$ inside $\mathfrak{g}$. More pedantically, one can say that there is a canonical one-to-one correspondence between $\mathfrak{sl}_2$-triples in $\mathfrak{g}$ and injective homomorphisms $\mathfrak{sl}_2\to\mathfrak{g}$. The theorem says that, for each root α of $\mathfrak{g}$ and choice of $x\in\mathfrak{g}^{\alpha}$, there is a unique $\mathfrak{sl}_2$-triple (x,h,y) such that $\alpha(h)=2$. Replacing x with cx replaces (x,h,y) with $(cx,h,c^{-1}y)$.

ASIDE 8.32 (a) For each $\alpha\in R$, there exists a unique one-dimensional Lie subalgebra $\mathfrak{u}_{\alpha}$ such that $[h,a]=\alpha(h)a$ for all $h\in\mathfrak{h}$ and $a\in\mathfrak{u}_{\alpha}$.

(b) For each root α, let $\mathfrak{h}_{\alpha}=\mathrm{Ker}(\alpha)$, and let $\mathfrak{g}_{\alpha}$ be the centralizer of $\mathfrak{h}_{\alpha}$. Then $\mathfrak{g}_{\alpha}$ is the Lie subalgebra $\mathfrak{h}\oplus\mathfrak{u}_{\alpha}\oplus\mathfrak{u}_{-\alpha}$ of $\mathfrak{g}$ (cf. my notes, Reductive Groups, I, Theorem 2.20).

ASIDE 8.33 Let x be an element of a semisimple Lie algebra $\mathfrak{g}$ (not necessarily split). If x belongs to an $\mathfrak{sl}_2$-triple (x,h,y), then x is nilpotent. Conversely, the Jacobson-Morozov theorem says that every nonzero nilpotent element x in a semisimple Lie algebra lies in an $\mathfrak{sl}_2$-triple (x,h,y); moreover, for any group G of automorphisms of $\mathfrak{g}$ containing $\mathrm{Aut}_e(\mathfrak{g})$, the map $(x,h,y)\mapsto x$ defines a bijection on the sets of G-orbits (Bourbaki LIE, VIII, §11, 2).

NOTES Morozov proved that every nilpotent element of a semisimple Lie algebra is contained in an $\mathfrak{sl}_2$-triple for the base field of the complex numbers (Doklady 1942). However, his proof contained a gap, and Jacobson gave a complete proof over any base field of characteristic zero (PAMS 1951). In fact, the proof is valid in characteristic p except for some small p (Klaus Pommerening, The Morozov-Jacobson theorem on 3-dimensional simple Lie subalgebras, 1979/2012). However, the uniqueness statement fails (cf. mo105781).

[15] Cf. Bourbaki LIE, §11, 1, where it is required that $[x,y]=-h$. In other words, Bourbaki replaces everyone else's y with $-y$.

Proof of Theorem 8.31.

Because $(\mathfrak{g},\mathfrak{h})$ is split, we can apply the results on the Cartan-Killing form κ proved in (8.13).

8.34 *For $\alpha,\beta \in R$, $[\mathfrak{g}^{\alpha},\mathfrak{g}^{\beta}] \subset \mathfrak{g}^{\alpha+\beta}$; in particular, $\mathfrak{h}_{\alpha} \stackrel{\text{def}}{=} [\mathfrak{g}^{\alpha},\mathfrak{g}^{-\alpha}] \subset \mathfrak{g}^{0} = \mathfrak{h}$.*

Let $x \in \mathfrak{g}^{\alpha}$ and $y \in \mathfrak{g}^{\beta}$. Then, for $h \in \mathfrak{h}$, we have

$$\begin{aligned} \operatorname{ad}(h)[x,y] &= [\operatorname{ad}(h)x,y]+[x,\operatorname{ad}(h)y] \\ &= [\alpha(h)x,y]+[x,\beta(h)y] \\ &= (\alpha(h)+\beta(h))[x,y]. \end{aligned}$$

8.35 *Let $\alpha \in R$, and let h^{α} be the unique element of $\mathfrak{h}$ such that $\alpha(h)=\kappa(h,h^{\alpha})$ for all $h \in \mathfrak{h}$ (which exists by 8.13). Then $\mathfrak{h}_{\alpha}$ is the subspace of $\mathfrak{h}$ spanned by h^{α}.*

For $h \in \mathfrak{h}$, $x \in \mathfrak{g}^{\alpha}$, and $y \in \mathfrak{g}^{-\alpha}$,

$$\kappa(h,[x,y]) = \kappa([h,x],y) = \kappa(\alpha(h)\cdot x,y) = \alpha(h)\cdot\kappa(x,y).$$

On comparing the following equalities

$$\begin{aligned} \kappa(h,[x,y]) &= \alpha(h)\cdot\kappa(x,y) \\ \kappa(h,h^{\alpha}) &= \alpha(h), \end{aligned}$$

we see that

$$[x,y] = \kappa(x,y)h^{\alpha} \tag{47}$$

for all $x \in \mathfrak{g}^{\alpha}$ and $y \in \mathfrak{g}^{-\alpha}$. As $\kappa(\mathfrak{g}^{\alpha},\mathfrak{g}^{-\alpha}) \neq 0$ (see 8.13), this shows that

$$\mathfrak{h}_{\alpha} \stackrel{\text{def}}{=} [\mathfrak{g}^{\alpha},\mathfrak{g}^{-\alpha}] = kh^{\alpha}.$$

8.36 *There is a unique $h_{\alpha} \in \mathfrak{h}$ such that $\alpha(h_{\alpha}) = -2$.*

After (8.35), it suffices to show that the restriction of α to $\mathfrak{h}$ is nonzero. Suppose $\alpha|\mathfrak{h} = 0$, and choose $x \in \mathfrak{g}^{\alpha}$ and $y \in \mathfrak{g}^{-\alpha}$ such that $h \stackrel{\text{def}}{=} [x,y] \neq 0$ (they exist by 8.35). Now

$$\begin{cases} [h,x] = \alpha(h)x = 0 \\ [h,y] = -\alpha(h)y = 0 \end{cases}$$

and so

$$\mathfrak{a} \stackrel{\text{def}}{=} kx \oplus ky \oplus kh$$

is a solvable subalgebra of $\mathfrak{g}$. As $h \in [\mathfrak{a},\mathfrak{a}]$, the corollary (3.10a) of Lie's theorem shows that $\rho(h)$ is nilpotent for every representation ρ of $\mathfrak{a}$. But h is a semisimple element of $\mathfrak{g}$ because it lies in a Cartan subalgebra (see 8.14), and so $\operatorname{ad}h$ is semisimple. This is a contradiction.

8.37 *For every nonzero $x_{\alpha} \in \mathfrak{g}^{\alpha}$, there exists a $y_{\alpha} \in \mathfrak{g}^{-\alpha}$ such that $(x_{\alpha},h_{\alpha},y_{\alpha})$ is an $\mathfrak{sl}_2$-triple.*

Because $x_\alpha \neq 0$, $[x_\alpha, \mathfrak{g}^{-\alpha}] \overset{(47)}{=} \kappa(x_\alpha, \mathfrak{g}^{-\alpha})h^\alpha = kh_\alpha$, and so there exists a $y_\alpha \in \mathfrak{g}^{-\alpha}$ such that $[x_\alpha, y_\alpha] = h_\alpha$. Now

$$[h_\alpha, x_\alpha] = \alpha(h_\alpha)x_\alpha = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -\alpha(h_\alpha)y_\alpha = -2y_\alpha,$$

and so $(x_\alpha, h_\alpha, y_\alpha)$ is an $\mathfrak{sl}_2$-triple.

8.38 $\dim \mathfrak{g}^\alpha = 1$.

Because $\mathfrak{g}^\alpha$ and $\mathfrak{g}^{-\alpha}$ are dual (see 8.13), if $\dim \mathfrak{g}^\alpha > 1$, then there exists a nonzero $y \in \mathfrak{g}^{-\alpha}$ such that $\kappa(x_\alpha, y) = 0$. According to (47), this implies that $[x_\alpha, y] = 0$. As

$$[h_\alpha, y] = -\alpha(h_\alpha)y = -2y,$$

y is now a primitive element of weight -2 in $\mathfrak{g}$ for the adjoint action of

$$\mathfrak{s}_\alpha \overset{\text{def}}{=} kx_\alpha \oplus kh_\alpha \oplus ky_\alpha,$$

which contradicts (8.30) (the weight of a primitive element in a finite-dimensional representation of $\mathfrak{sl}_2$ is a nonnegative integer).

This completes the proof of the theorem.

The root system of a split semisimple Lie algebra

Throughout this subsection, $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra. As usual, we write

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^\alpha$$

with $R = R(\mathfrak{g}, \mathfrak{h})$ the set of roots of $(\mathfrak{g}, \mathfrak{h})$,

THEOREM 8.39 *The set R is a reduced root system in the vector space $\mathfrak{h}^\vee$.*

More precisely, we prove:

(a) R is finite, spans $\mathfrak{h}^\vee$, and doesn't contain 0.
(b) For each $\alpha \in R$, let h_α be the unique element in $[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}]$ such that $\alpha(h_\alpha) = 2$ (see 8.31b), and let $\alpha^\vee$ denote h_α regarded as an element of $(\mathfrak{h}^\vee)^\vee$; then $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \in \mathbb{Z}$, and the reflection

$$s_\alpha : x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$$

maps R into R.
(c) For no $\alpha \in R$ does $2\alpha \in R$.

The system R is the called the ***root system*** of $(\mathfrak{g}, \mathfrak{h})$.

Proof of (a).

It remains to show that R spans $\mathfrak{h}^\vee$. Suppose that $h \in \mathfrak{h}$ lies in the kernel of all $\alpha \in R$. Then $[h, \mathfrak{g}^\alpha] = 0$ for all $\alpha \in R$, and as $[h, \mathfrak{h}] = 0$, this shows that h lies in the centre of $\mathfrak{g}$, which (by definition) is trivial. Therefore $h = 0$, and so R must span $\mathfrak{h}^\vee$.

Proof of (b).

We first prove the following statement:

Let $\alpha, \beta \in R$; then $\beta(h_\alpha) \in \mathbb{Z}$ and $\beta - \beta(h_\alpha) \cdot \alpha \in R$.

To prove this, we regard $\mathfrak{g}$ as an $\mathfrak{s}_\alpha$-module under the adjoint action, and we apply (8.29d). Let z be a nonzero element of $\mathfrak{g}^\beta$. Then $[h_\alpha, z] = \beta(h_\alpha)z$, and so $n \stackrel{\text{def}}{=} \beta(h_\alpha)$ is an eigenvalue of h_α acting on $\mathfrak{g}$; therefore $n \in \mathbb{Z}$. If $n \geq 0$. then y_α^n is an isomorphism from $\mathfrak{g}^\beta$ to $\mathfrak{g}^{\beta - n\alpha}$, and so $\beta - n\alpha$ is also a root; if $n \leq 0$, the x_α^{-n} is an isomorphism from $\mathfrak{g}^\beta$ to $\mathfrak{g}^{\beta = n\alpha}$, and so again $\beta - n\alpha$ is a root.

We now prove (b). By definition, $\langle \alpha, \alpha^\vee \rangle = \alpha(h_\alpha) = 2$. Moreover, $\langle \beta, \alpha^\vee \rangle = \beta(h_\alpha)$, which we have just shown lies in $\mathbb{Z}$ if β is a root. Finally, $s_\alpha(\beta) = \beta - \beta(h_\alpha)\alpha$, which we have just shown be a root if β is .

Proof of (c).

Suppose that there exists an $\alpha \in R$ such that $2\alpha \in R$. Then there exists a nonzero y such that

$$[h_\alpha, y] = 2\alpha(h_\alpha)y = 4y. \tag{48}$$

Now $h_\alpha = [x_\alpha, y_\alpha]$, and so

$$[h_\alpha, y] = [x_\alpha, [y_\alpha, y]].$$

But $[y_\alpha, y] \in \mathfrak{g}^\alpha = kx_\alpha$, and so $[x_\alpha, [y_\alpha, y]] = 0$, contradicting (48).

Semisimple Lie algebras of rank 1

PROPOSITION 8.40 *Let $\mathfrak{g}$ be split semisimple Lie algebra of rank 1, and let x be an eigenvector for the (unique) root of $\mathfrak{g}$. Then (x, h, y) is an $\mathfrak{sl}_2$-triple for unique elements h, y of $\mathfrak{g}$, and $\mathfrak{g} = kx \oplus kh \oplus ky$. In particular, $\mathfrak{g}$ is isomorphic to $\mathfrak{sl}_2$.*

PROOF. The existence and uniqueness of the $\mathfrak{sl}_2$-triple follows from Theorem 8.31. That $\mathfrak{g} = kx \oplus kh \oplus ky$ follows from Theorem 8.39. □

Criteria for simplicity and semisimplicity

Theorem 8.31 has a partial converse.

PROPOSITION 8.41 *Let $\mathfrak{g}$ be a Lie algebra, and let $\mathfrak{h}$ be a commutative Lie subalgebra. For each $\alpha \in \mathfrak{h}^\vee$, let*

$$\mathfrak{g}^\alpha = \{x \in \mathfrak{g} \mid hx = \alpha(h)x \text{ all } h \in \mathfrak{h}\},$$

and let R be the set of nonzero $\alpha \in \mathfrak{h}^\vee$ such that $\mathfrak{g}^\alpha \neq 0$. Suppose that:

(a) $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha$;
(b) *for each $\alpha \in R$, the space $\mathfrak{g}^\alpha$ has dimension 1;*
(c) *for each nonzero $h \in \mathfrak{h}$, there exists an $\alpha \in R$ such that $\alpha(h) \neq 0$; and*
(d) *if $\alpha \in R$, then $-\alpha \in R$ and $[[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha] \neq 0$.*

Then $\mathfrak{g}$ is semisimple and $\mathfrak{h}$ is a splitting Cartan subalgebra of $\mathfrak{g}$.

PROOF. Let $\mathfrak{a}$ be a commutative ideal in $\mathfrak{g}$; we have to show that $\mathfrak{a} = 0$. As $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$, (a) gives us a decomposition

$$\mathfrak{a} = \mathfrak{a} \cap \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{a} \cap \mathfrak{g}^{\alpha}.$$

If $\mathfrak{a} \cap \mathfrak{g}^{\alpha} \neq 0$ for some $\alpha \in R$, then $\mathfrak{a} \supset \mathfrak{g}^{\alpha}$ (by (b)). As $\mathfrak{a}$ is an ideal, this implies that $\mathfrak{a} \supset [\mathfrak{g}^{\alpha}, \mathfrak{g}^{-\alpha}]$, and as $[\mathfrak{a}, \mathfrak{a}] = 0$, this implies that $[[\mathfrak{g}^{\alpha}, \mathfrak{g}^{-\alpha}], \mathfrak{g}^{\alpha}] = 0$, contradicting (d).

Suppose that $\mathfrak{a} \cap \mathfrak{h} \neq 0$, and let h be a nonzero element of $\mathfrak{a} \cap \mathfrak{h}$. According to (c), there exists an $\alpha \in R$ such that $\alpha(h) \neq 0$. Let x be a nonzero element of $\mathfrak{g}^{\alpha}$. Then $[h, x] = \alpha(h)x$, which is a nonzero element of $\mathfrak{g}^{\alpha}$. As $[h, x] \in \mathfrak{a}$, this contradicts the last paragraph.

Condition (a) implies that the elements of $\mathfrak{h}$ act semisimply on $\mathfrak{g}$ and that their eigenvalues lie in k and that $\mathfrak{h}$ is its own centralizer. Therefore $\mathfrak{h}$ is a splitting Cartan subalgebra of $\mathfrak{g}$. □

PROPOSITION 8.42 *Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple algebra. A decomposition $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ of semisimple Lie algebras defines a decomposition $(\mathfrak{g}, \mathfrak{h}) = (\mathfrak{g}_1, \mathfrak{h}_1) \oplus (\mathfrak{g}_2, \mathfrak{h}_2)$, and hence a decomposition of the root system of $(\mathfrak{g}, \mathfrak{h})$.*

PROOF. Let

$$\begin{aligned} \mathfrak{g} &= \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha} \\ \mathfrak{g}_1 &= \mathfrak{h}_1 \oplus \bigoplus\nolimits_{\alpha \in R_1} \mathfrak{g}_1^{\alpha} \\ \mathfrak{g}_2 &= \mathfrak{h}_2 \oplus \bigoplus\nolimits_{\alpha \in R_2} \mathfrak{g}_2^{\alpha} \end{aligned}$$

be the eigenspace decompositions of $\mathfrak{g}$, $\mathfrak{g}_1$, and $\mathfrak{g}_2$ respectively defined by the action of $\mathfrak{h}$. Then $\mathfrak{h} = \mathfrak{h}_1 \oplus \mathfrak{h}_2$ and $R = R_1 \sqcup R_2$. □

COROLLARY 8.43 *If the root system of $(\mathfrak{g}, \mathfrak{h})$ is indecomposable (equivalently, its Dynkin diagram is connected), then $\mathfrak{g}$ is simple.*

ASIDE 8.44 The converses of (8.42) and (8.43) are also true: a decomposition of its root system defines a decomposition of $(\mathfrak{g}, \mathfrak{h})$, and if $\mathfrak{g}$ is simple then the root system of $(\mathfrak{g}, \mathfrak{h})$ is indecomposable (8.48, 8.49 below).

The classical split simple Lie algebras

We compute the roots of each of the classical split Lie algebras, and use (8.41, 8.43) to show that they are simple (we could also use 6.5).

We begin by computing the roots and root spaces of $\mathfrak{gl}_{n+1}$. For each classical Lie algebra $\mathfrak{g}$, we work with a convenient form of the algebra in $\mathfrak{gl}_{n+1}$. We first compute the weights of a Cartan subalgebra $\mathfrak{h}$ on $\mathfrak{gl}_{n+1}$, and determine the weights that occur in $\mathfrak{g}$.

Example $\mathfrak{gl}_{n+1}$

We first look at $\hat{\mathfrak{g}} = \mathfrak{gl}_{n+1}$, even though this is not (quite) a semisimple algebra (its centre is the subalgebra of scalar matrices). Let $\hat{\mathfrak{h}}$ be the Lie subalgebra of diagonal elements in $\hat{\mathfrak{g}}$. Let E_{ij} be the matrix in $\hat{\mathfrak{g}}$ with 1 in the (i, j)th position and zeros elsewhere. Then

$(E_{ij})_{1\le i,j\le n+1}$ is a basis for $\hat{\mathfrak{g}}$ and $(E_{ii})_{1\le i\le n+1}$ is a basis for $\hat{\mathfrak{h}}$. Let $(\varepsilon_i)_{1\le i\le n+1}$ be the dual basis for $\hat{\mathfrak{h}}^\vee$; thus

$$\varepsilon_i(\mathrm{diag}(a_1,\ldots,a_{n+1})) = a_i.$$

An elementary calculation using (7), p.13, shows that, for $h\in\hat{\mathfrak{h}}$,

$$[h,E_{ij}] = (\varepsilon_i(h)-\varepsilon_j(h))E_{ij}. \tag{49}$$

Thus,

$$\hat{\mathfrak{g}} = \hat{\mathfrak{h}} \oplus \bigoplus\nolimits_{\alpha\in R} \hat{\mathfrak{g}}^\alpha$$

where $R=\{\varepsilon_i-\varepsilon_j \mid i\neq j,\ 1\le i,j\le n+1\}$ and $\hat{\mathfrak{g}}^{\varepsilon_i-\varepsilon_j} = kE_{ij}$.

Example (A_n): $\mathfrak{sl}_{n+1}$

Let $\mathfrak{g}=\mathfrak{sl}(W)$ where W is a vector space of dimension $n+1$. Choose a basis $(e_i)_{1\le i\le n+1}$ for W, and use it to identify $\mathfrak{g}$ with $\mathfrak{sl}_{n+1}$, and let $\mathfrak{h}$ be the Lie subalgebra of diagonal matrices in $\mathfrak{g}$. The matrices

$$E_{i,i}-E_{i+1,i+1} \qquad (1\le i\le n)$$

form a basis for $\mathfrak{h}$, and, together with the matrices

$$E_{ij} \qquad (1\le i,j\le n,\ i\neq j),$$

they form a basis for $\mathfrak{g}$.

Let V be the hyperplane in $\hat{\mathfrak{h}}^\vee$ consisting of the elements $\alpha=\sum_{i=1}^{n+1}a_i\varepsilon_i$ such that $\sum_{i=1}^{n+1}a_i=0$. The restriction map $\lambda\mapsto\lambda|\mathfrak{h}$ defines an isomorphism of V onto $\mathfrak{h}^\vee$, which we use to identify the two spaces.[16] Each of the basis vectors E_{ij}, $i\neq j$, is an eigenvector for $\mathfrak{h}$, and $\mathfrak{h}$ acts on kE_{ij} through the linear form $\varepsilon_i-\varepsilon_j$ (see (49)). Therefore

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha\in R} \mathfrak{g}^\alpha$$

with $R=\{\varepsilon_i-\varepsilon_j \mid i\neq j\}\subset V$ and $\mathfrak{g}^{\varepsilon_i-\varepsilon_j}=kE_{ij}$. We check the conditions of Proposition 8.41. We already know that (a) and (b) hold. For (c), let

$$h=\mathrm{diag}(a_1,\ldots,a_{n+1}),\quad \sum a_i=0,$$

be an element of $\mathfrak{h}$. If $h\neq0$, then $a_i\neq a_j$ for some i,j, and so $(\varepsilon_i-\varepsilon_j)(h)=a_i-a_j\neq0$. For (d), let $\alpha=\varepsilon_i-\varepsilon_j$. Then $-\alpha$, is also a root and

$$\begin{aligned}[][\mathfrak{g}^\alpha,\mathfrak{g}^{-\alpha}],\mathfrak{g}^\alpha] &\ni [[E_{ij},E_{ji}],kE_{ij}]\\ &= [E_{ii}-E_{jj},E_{ij}]\\ &= 2.\end{aligned}$$

Therefore $(\mathfrak{g},\mathfrak{h})$ is a split semisimple Lie algebra.

[16] In more detail: $\hat{\mathfrak{h}}$ is a vector space with basis $E_{11},\ldots,E_{n+1,n+1}$, and $\mathfrak{h}$ its the subspace $\{\sum a_iE_{ii} \mid \sum a_i=0\}$. The dual of $\hat{\mathfrak{h}}$ is a vector space with basis $\varepsilon_1,\ldots,\varepsilon_{n+1}$ where $\varepsilon_i(E_j)=\delta_{ij}$, and the dual of $\mathfrak{h}$ is the quotient of $(\hat{\mathfrak{h}})^\vee$ by the line $\langle\varepsilon_1+\cdots+\varepsilon_n\rangle$. However, it is more convenient to identify the dual of $\mathfrak{h}$ with the orthogonal complement of this line, namely, with the hyperplane V in $(\hat{\mathfrak{h}})^\vee$.

The family $(\alpha_i)_{1\leq i\leq n}$, $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, is a base for R. Relative to the inner product

$$(\sum a_i\varepsilon_i, \sum b_i\varepsilon_i) = \sum a_i b_i,$$

we find that

$$n(\alpha_i,\alpha_j) = 2\frac{(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)} = (\alpha_i,\alpha_j) = \begin{cases} 2 & \text{if } j = i \\ -1 & \text{if } j = i\pm 1 \\ 0 & \text{otherwise} \end{cases}$$

and so

$$n(\alpha_i,\alpha_j)\cdot n(\alpha_j,\alpha_i) = \begin{cases} 1 & \text{if } j = i\pm 1 \\ 0 & \text{if } j \neq i, i\pm 1. \end{cases}$$

Thus, the Dynkin diagram of $(\mathfrak{g},\mathfrak{h})$ is indecomposable of type A_n. Therefore $\mathfrak{g}$ is simple.

Example (B_n): $\mathfrak{o}_{2n+1}$

Consider the symmetric bilinear form ϕ on k^{2n+1},

$$\phi(\vec{x},\vec{y}) = 2x_0y_0 + x_1y_{n+1} + x_{n+1}y_1 + \cdots + x_ny_{2n} + x_{2n}y_n$$

The Lie algebra $\mathfrak{g} = \mathfrak{so}_{2n+1}$ consists of the $2n+1\times 2n+1$ matrices A of trace 0 such that

$$\phi(A\vec{x},\vec{y}) + \phi(\vec{x},A\vec{y}) = 0,$$

i.e., such that

$$A^t\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & I\\ 0 & I & 0\end{pmatrix} + \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & I\\ 0 & I & 0\end{pmatrix}A = 0.$$

A direct calculation shows that $\mathfrak{g}$ consists of the matrices

$$\begin{pmatrix}0 & C^t & -B^t\\ B & M & P\\ -C & Q & -M^t\end{pmatrix}, \quad P = -P^t, \quad Q = -Q^t.$$

We obtain a basis for $\mathfrak{g}$ by first finding a basis for the space of matrices in $\mathfrak{g}$ with only B nonzero, then with only C nonzero, and so on:

$$\begin{aligned} B_i &= E_{i,0} - E_{0,n+i}, \quad 1\leq i\leq n,\\ C_i &= E_{0,i} - E_{n+i,0}, \quad 1\leq i\leq n,\\ M_{i,j} &= E_{i,j} - E_{n+j,n+i}, \quad 1\leq i\neq j\leq n,\\ P_{i,j} &= E_{i,n+j} - E_{j,n+i}, \quad 1\leq i<j\leq n\\ Q_{i,j} &= E_{n+j,i} - E_{n+i,j}, \quad 1\leq i<j\leq n. \end{aligned}$$

Let $\mathfrak{h}$ be the subalgebra of $\mathfrak{g}$ of diagonal matrices,

$$h = \operatorname{diag}(0,a_1,\ldots,a_n,-a_1,\ldots,-a_n).$$

The linear dual $\mathfrak{h}^\vee$ has basis $\varepsilon_1, \dots, \varepsilon_n$ where $\varepsilon_i(h) = a_i$.

A direct calculation using (49) shows that

$$[h, B_i] = a_i B_i = \varepsilon_i(h) B_i.$$

Therefore, kB_i is a root space for $\mathfrak{h}$ with root ε_i. Similarly,

$$[h, M_{i,j}] = (a_i - a_j) M_{ij} = (\varepsilon_i(h) - \varepsilon_j(h)) M_{ij},$$

and so $\langle M_{ij} \rangle$ is a root space for $\mathfrak{h}$ with root $\varepsilon_i - \varepsilon_j$, unless $i = j$, in which case it lies in $\mathfrak{h}$.

Continuing in this fashion, we find that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^\alpha$$

with roots and eigenvectors:

ε_i	$-\varepsilon_i$	$\varepsilon_i - \varepsilon_j \ (i \neq j)$	$\varepsilon_i + \varepsilon_j \ (i < j)$	$-\varepsilon_i - \varepsilon_j \ (i < j)$
B_i	C_i	M_{ij}	P_{ij}	Q_{ji}.

The conditions of Proposition 8.41 can be checked, and so $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra.

The family

$$\{\varepsilon_1 - \varepsilon_2, \dots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_n\}$$

is a base for the root system, and the Dynkin diagram corresponding to this base is indecomposable of type B_n. Therefore $\mathfrak{so}_n$ is a simple Lie algebra of type B_n.

Example (C_n): $\mathfrak{sp}_{2n}$

Consider the skew symmetric bilinear form $k^{2n} \times k^{2n} \to k$,

$$\phi(\vec{x}, \vec{y}) = x_1 y_{n+1} - x_{n+1} y_1 + \cdots + x_n y_{2n} - x_{2n} y_n.$$

Then $\mathfrak{g} = \mathfrak{sp}_n$ consists of the $2n \times 2n$ matrices A such that

$$\phi(A\vec{x}, \vec{y}) + \phi(\vec{x}, A\vec{y}) = 0,$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = 0.$$

A direct calculation shows that $\mathfrak{g}$ consists of the matrices

$$\begin{pmatrix} M & P \\ Q & -M^t \end{pmatrix}, \quad P = P^t, \quad Q = Q^t.$$

The following matrices form a basis for $\mathfrak{g}$:

$$\begin{aligned} M_{i,j} &= E_{i,j} - E_{n+j,n+i}, & 1 \le i \neq j \le n, \\ P_{i,j} &= E_{i,n+j} - E_{j,n+i}, & 1 \le i \le j \le n, \\ Q_{j,i} &= E_{n+j,i} + E_{n+i,j}, & 1 \le i \le j \le n. \end{aligned}$$

Let $\mathfrak{h}$ be the subalgebra of $\mathfrak{g}$ of diagonal matrices

$$h = \operatorname{diag}(a_1, \ldots, a_n, -a_1, \ldots, -a_n).$$

The linear dual $\mathfrak{h}^\vee$ has basis $\varepsilon_1, \ldots, \varepsilon_n$ where $\varepsilon_i(h) = a_i$.

A direct calculation using (49) shows that each of the basis vectors listed above is an eigenvector for $\mathfrak{h}$, and

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^\alpha$$

with roots and eigenvectors

$\varepsilon_i - \varepsilon_j \ (i \neq j)$	$\varepsilon_i + \varepsilon_j \ (i < j)$	$-\varepsilon_i - \varepsilon_j$	$2\varepsilon_i$	$-2\varepsilon_i$
$M_{i,j}$	$P_{i,j}$	$Q_{j,i}$	$P_{i,i}$	$Q_{i,i}$.

The conditions of Proposition 8.41 can be checked, and so $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra.

The family

$$\{\varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, 2\varepsilon_n\}$$

is a base for the root system, and the Dynkin diagram corresponding to this base is indecomposable of type C_n. Therefore $\mathfrak{sp}_n$ is a simple Lie algebra of type C_n.

Example (D_n)*:* $\mathfrak{o}_{2n}$

Consider the symmetric bilinear form $k^{2n} \times k^{2n} \to k$,

$$\phi(\vec{x}, \vec{y}) = x_1 y_{n+1} + x_{n+1} y_1 + \cdots + x_n y_{2n} + x_{2n} y_{2n}.$$

The Lie algebra $\mathfrak{g} = \mathfrak{so}_n$ consists of the $n \times n$ matrices A of trace 0 such that

$$\phi(A\vec{x}, \vec{y}) + \phi(\vec{x}, A\vec{y}) = 0,$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = 0.$$

A direct calculation using (49) show that $\mathfrak{g}$ consists of the matrices

$$\begin{pmatrix} M & P \\ Q & -M^t \end{pmatrix}, \quad P = -P^t, \quad Q = -Q^t.$$

The following matrices form a basis for $\mathfrak{g}$:

$$\begin{aligned} M_{i,j} &= E_{i,j} - E_{n+j,n+i}, & 1 \le i \neq j \le n, \\ P_{i,j} &= E_{i,n+j} - E_{j,n+i}, & 1 \le i \le j \le n, \\ Q_{j,i} &= E_{n+j,i} + E_{n+i,j}, & 1 \le i \le j \le n. \end{aligned}$$

Let $\mathfrak{h}$ be the subalgebra of $\mathfrak{g}$ of diagonal matrices

$$h = \operatorname{diag}(a_1, \ldots, a_n, -a_1, \ldots, -a_n).$$

The linear dual $\mathfrak{h}^\vee$ has basis $\varepsilon_1, \ldots, \varepsilon_n$ where $\varepsilon_i(h) = a_i$.

A direct calculation using (49) shows that each of the basis vectors listed above is an eigenvector for $\mathfrak{h}$, and that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha}$$

with roots α and eigenvectors

$\varepsilon_i - \varepsilon_j \ (i \neq j)$	$\varepsilon_i + \varepsilon_j \ (i < j)$	$-\varepsilon_i - \varepsilon_j$
$M_{i,j}$	$P_{i,j}$	$Q_{j,i}$

This conditions of Proposition 8.41 can be checked, and so $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra.

The family

$$\{\varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_{n-1} + \varepsilon_n\}$$

is a base for the root system, and the Dynkin diagram corresponding to this base is indecomposable of type D_n. Therefore $\mathfrak{sp}_n$ is a simple Lie algebra of type C_n.

See Erdmann and Wildon 2006, Chapter 12, for a more elementary description of the classical split simple Lie algebras, and Bourbaki LIE, VIII, §13, for a more exhaustive description.

Subalgebras of split semisimple Lie algebras

In this subsection, $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra. By a Lie ***subalgebra*** of $(\mathfrak{g}, \mathfrak{h})$ we mean a subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ normalized by $\mathfrak{h}$, i.e., such that $[\mathfrak{h}, \mathfrak{a}] \subset \mathfrak{a}$. In other words, the Lie subalgebras of $(\mathfrak{g}, \mathfrak{h})$ are the Lie subalgebras of $\mathfrak{g}$ stable under $\mathrm{ad}(\mathfrak{h})$.

For a subset P of R, let

$$\mathfrak{h}_P = \sum_{\alpha \in P} \mathfrak{h}_{\alpha}, \quad \mathfrak{h}_{\alpha} = kH_{\alpha},$$
$$\mathfrak{g}^P = \sum_{\alpha \in P} \mathfrak{g}^{\alpha}.$$

DEFINITION 8.45 A subset P of R is said to be ***closed***[17] if

$$\alpha, \beta \in P, \quad \alpha + \beta \in R \implies \alpha + \beta \in P.$$

As $[\mathfrak{g}^{\alpha}, \mathfrak{g}^{\beta}] \subset \mathfrak{g}^{\alpha+\beta}$ (see 8.34), we see that if $\mathfrak{h}_P + \mathfrak{g}^P$ is a Lie subalgebra of $\mathfrak{g}$, then P must be closed.

PROPOSITION 8.46 *The subalgebras of $(\mathfrak{g}, \mathfrak{h})$ are exactly subspaces $\mathfrak{a} = \mathfrak{h}' + \mathfrak{g}^P$ where $\mathfrak{h}'$ is a vector subspace of $\mathfrak{h}$ and P is a closed subset of R. Moreover,*

(a) *$\mathfrak{a}$ is reductive (resp. semisimple) if and only if $P = -P$ (resp. $P = -P$ and $\mathfrak{h}' = \mathfrak{h}_P$);*
(b) *$\mathfrak{a}$ is solvable if and only if*

$$P \cap (-P) = \emptyset. \tag{50}$$

PROOF. Easy. See Bourbaki LIE, VIII, §3, 1, Pptn 1, Pptn 2. □

[17] This is Bourbaki's terminology, LIE VI, §1, 7.

EXAMPLE 8.47 For any root α, $P = \{\alpha, -\alpha\}$ is a closed subset of R, and $[\mathfrak{g}^{\alpha}, \mathfrak{g}^{-\alpha}] + \mathfrak{g}^{P}$ is the Lie subalgebra $\mathfrak{s}_{\alpha}$ of (8.31).

PROPOSITION 8.48 *The root system R is indecomposable if and only if $\mathfrak{g}$ is simple.*

PROOF. Suppose $\mathfrak{g} = \mathfrak{a} \times \mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals in $\mathfrak{g}$. Then $\mathfrak{a}$ and $\mathfrak{b}$ are semisimple, and so $\mathfrak{a} = \mathfrak{h}_P + \mathfrak{g}^P$ and $\mathfrak{b} = \mathfrak{h}_Q + \mathfrak{g}^Q$ for some P and Q. Then $\mathfrak{h}_P$ and $\mathfrak{h}_Q$ are orthogonal complements for the Killing form on $\mathfrak{h}$, and so $R = P \sqcup Q$ with each root in P orthogonal to each root in Q. Therefore, R is decomposable. □

COROLLARY 8.49 *Let $R_1, \ldots, R_m$ be the indecomposable components of R. Then $\mathfrak{h}_{R_1} + \mathfrak{g}^{R_1}, \ldots, \mathfrak{h}_{R_m} + \mathfrak{g}^{R_m}$ are the minimal ideals of $\mathfrak{g}$.*

PROOF. Each $\mathfrak{h}_{R_i} + \mathfrak{g}^{R_i}$ is an ideal, and the proposition shows that it is minimal. □

PROPOSITION 8.50 *Let $\mathfrak{b} = \mathfrak{h} + \mathfrak{g}^P$ be a Lie subalgebra of $\mathfrak{g}$ containing $\mathfrak{h}$. The following conditions are equivalent: (a) $\mathfrak{b}$ is maximal solvable subalgebra of $\mathfrak{g}$; (b) there exists a base S for R such that $P = R_+$; (c) $P \cap (-P) = \emptyset$ and $P \cup (-P) = R$.*

PROOF. (a)⇒(b). If $\mathfrak{h} + \mathfrak{g}^P$ is solvable, then $P \cap (-P) = \emptyset$ by (8.46b). Every closed subset P of R disjoint from $-P$ is contained in R_+ for some base S (ibid., VI, §1, 7, Pptn 22). Now $\mathfrak{h} + \mathfrak{g}^P$ is contained in the solvable subalgebra $\mathfrak{h} + \mathfrak{g}^{R_+}$, and so must equal it. Hence $P = R_+$.

(b)⇒(c). Obvious.

(c)⇒(a). The condition $P \cap (-P) = \emptyset$ implies that $\mathfrak{h} + \mathfrak{g}^P$ is solvable. Any solvable subalgebra of $\mathfrak{g}$ containing $\mathfrak{h} + \mathfrak{g}^P$ is of the form $\mathfrak{h} + \mathfrak{g}^Q$ with $Q \supset P$ and $Q \cap (-Q) = \emptyset$. Now the condition $P \cap (-P) = R$ implies that $Q = P$, and so $\mathfrak{h} + \mathfrak{g}^Q = \mathfrak{h} + \mathfrak{g}^P$. □

For base S of R, the set R_+ of positive roots is a maximal closed subset of R satisfying (50), and every maximal such set arises in this way from a base (Bourbaki LIE, VI, §1, 7, Pptn 22). Therefore, the maximal solvable subalgebras of $\mathfrak{g}$ containing $\mathfrak{h}$ are exactly subalgebras of the form

$$\mathfrak{b}(S) \stackrel{\text{def}}{=} \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha > 0} \mathfrak{g}^{\alpha}, \quad S \text{ a base of } R.$$

The subalgebra $\mathfrak{b}(S)$ determines R_+, and hence the base S (as the set of indecomposable elements of R_+).

DEFINITION 8.51 A ***Borel subalgebra*** of a split semisimple Lie algebra $(\mathfrak{g}, \mathfrak{h})$ is a maximal solvable subalgebra of $\mathfrak{g}$ containing $\mathfrak{h}$. More generally, a ***Borel subalgebra*** of a semisimple Lie algebra $\mathfrak{g}$ is any Lie subalgebra of $\mathfrak{g}$ that is a Borel subalgebra of $(\mathfrak{g}, \mathfrak{h})$ for some splitting Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$.

EXAMPLE 8.52 Let $\mathfrak{g} = \mathfrak{sl}_{n+1}$ and let $\mathfrak{h}$ be the subalgebra of diagonal matrices in $\mathfrak{g}$. For the base $S = (\alpha_i)_{1 \le i \le n}$, $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, as in §8, the positive roots are those of the form $\varepsilon_i - \varepsilon_j$ with $i < j$, and the Borel subalgebra $\mathfrak{b}(S)$ consists of upper triangular matrices of trace 0. More generally, let $\mathfrak{g} = \mathfrak{sl}(W)$ with W a vector space of dimension $n+1$. For any maximal flag $\mathcal{S}$ in W, the set $\mathfrak{b}_{\mathcal{S}}$ of elements of $\mathfrak{g}$ leaving stable all the elements of $\mathcal{S}$ is a Borel subalgebra of $\mathfrak{g}$, and the map $\mathcal{S} \mapsto \mathfrak{b}_{\mathcal{S}}$ is a bijection from the set of maximal flags onto the set of Borel subgroups of $\mathfrak{g}$ (Bourbaki LIE, VIII, §13).

NOTES This section needs to be completely rewritten.

All splitting Cartan subalgebras are conjugate

For the present, we just list the main steps. Throughout, $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra.

8.53 *Every element of the Weyl group of* $(\mathfrak{g}, \mathfrak{h})$ *acts on* $\mathfrak{h}$ *as the restriction to* $\mathfrak{h}$ *of an elementary automorphism of* $\mathfrak{g}$ *(Bourbaki LIE VIII, §2, 2).*

8.54 *Let* $(\mathfrak{b}_1, \mathfrak{h}_1)$ *and* $(\mathfrak{b}_2, \mathfrak{h}_2)$ *be two pairs consisting of a Borel subgroup of* $\mathfrak{g}$ *and a splitting Cartan subgroup in the Borel subgroup. Then there exists a splitting Cartan subalgebra contained in* $\mathfrak{b}_1 \cap \mathfrak{b}_2$ *(Bourbaki LIE VIII, §3, 3).*

8.55 *Let* $\mathfrak{b}$ *be a Borel subgroup of* $\mathfrak{g}$. *Every Cartan subalgebra of* $\mathfrak{b}$ *is a splitting Cartan subalgebra of* $\mathfrak{g}$. *For any Cartan subalgebras* $\mathfrak{h}_1$, $\mathfrak{h}_2$ *of* $\mathfrak{b}$, *there exists an* $x \in [\mathfrak{b}, \mathfrak{b}]$ *such that* $e^{\mathrm{ad}_{\mathfrak{g}} x}\mathfrak{h}_1 = \mathfrak{h}_2$ *(Bourbaki LIE VIII, §3, 3).*

THEOREM 8.56 *The group of elementary automorphisms of* $\mathfrak{g}$ *acts transitively on the set of pairs* $(\mathfrak{b}, \mathfrak{h})$ *consisting of a splitting Cartan subalgebra* $\mathfrak{h}$ *of* $\mathfrak{g}$ *and a Borel subgroup of* $(\mathfrak{g}, \mathfrak{h})$.

PROOF. Let $(\mathfrak{b}_1, \mathfrak{h}_1)$ and $(\mathfrak{b}_2, \mathfrak{h}_2)$ be two such pairs. According to (8.54), there exists a splitting Cartan algebra $\mathfrak{h}$ contained in $\mathfrak{b}_1 \cap \mathfrak{b}_2$. According to (8.55), there exist $x_1, x_2 \in [\mathfrak{b}, \mathfrak{b}]$ such that $e^{\mathrm{ad}_{\mathfrak{g}} x_1}\mathfrak{h}_1 = \mathfrak{h} = e^{\mathrm{ad}_{\mathfrak{g}} x_2}\mathfrak{h}_2$. Therefore, we may suppose that $\mathfrak{h}_1 = \mathfrak{h}_2$. The Borel subalgebras $\mathfrak{b}_1$ and $\mathfrak{b}_2$ correspond to bases S_1 and S_2 respectively of the root system R of $(\mathfrak{g}, \mathfrak{h})$. There exists an s in the Weyl group of R that transforms S_1 into S_2 (see 7.11 et seq.), and there exists an elementary automorphism a of $\mathfrak{g}$ such that $a|\mathfrak{h} = s$. Now $a(\mathfrak{b}_1, \mathfrak{h}) = (\mathfrak{b}_2, \mathfrak{h})$. □

Chevalley bases; existence of split semisimple Lie algebras

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra. Let $\alpha_1, \ldots, \alpha_n$ be a base for the root system R of $(\mathfrak{g}, \mathfrak{h})$, let $h_i \in \mathfrak{h}$ be the coroot of α_i, and let

$$n(i, j) \stackrel{\text{def}}{=} \alpha_j(h_i)$$

be the entries of Cartan matrix of R. For each i, choose a nonzero $x_i \in \mathfrak{g}^{\alpha_i}$. Then (see 8.31), there is a unique $y_i \in \mathfrak{g}$ such that (x_i, h_i, y_i) is an $\mathfrak{sl}_2$-triple.

THEOREM 8.57 *The elements x_i, y_i, h_i satisfy the following relations*

$$\begin{aligned} [h_i, h_j] &= 0 \\ [x_i, y_i] &= h_i, \quad [x_i, y_j] = 0 \text{ if } i \neq j \\ [h_i, x_j] &= n(i,j)x_j, \quad [h_i, x_j] = -n(i,j)y_j \\ \mathrm{ad}(x_i)^{-n(i,j)+1}(x_j) &= 0 \text{ if } i \neq j \\ \mathrm{ad}(y_i)^{-n(i,j)+1}(y_j) &= 0 \text{ if } i \neq j. \end{aligned}$$

PROOF. Serre 1966, VI, Theorem 6. □

For each root α of $(\mathfrak{g}, \mathfrak{h})$, choose a nonzero $x_\alpha \in R$. Then

$$[x_\alpha, x_\beta] = \begin{cases} N_{\alpha,\beta} x_{\alpha+\beta} & \text{if } \alpha+\beta \in R \\ 0 & \text{if } \alpha+\beta \notin R, \alpha+\beta \neq 0 \end{cases}$$

for some nonzero $N_{\alpha,\beta} \in k$. For $h, h' \in \mathfrak{h}$, we have that $[h, h'] = 0$ and $[h, x_\alpha] = \alpha(h)x_\alpha$, and so the $N_{\alpha,\beta}$, together with R, determine the multiplication table of $\mathfrak{g}$.

THEOREM 8.58 *It is possible to choose that x_α so that*

$$\begin{aligned} [x_\alpha, x_{-\alpha}] &= h_\alpha \text{ for all } \alpha \in R \\ N_{\alpha,\beta} &= -N_{-\alpha,-\beta} \text{ for all } \alpha, \beta, \alpha+\beta \in R. \end{aligned}$$

With this choice

$$N_{\alpha,\beta} = \pm(r+1)$$

where r is the greatest integer such that $\beta - r\alpha \in R$.

PROOF. Bourbaki LIE, VIII, §2, 4. □

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra over $\mathbb{C}$, and let $\mathfrak{g}(\mathbb{Q})$ (resp. $\mathfrak{h}(\mathbb{Q})$) be the $\mathbb{Q}$-subspace of $\mathfrak{g}$ generated by h_α and the x_α (resp. the h_α) in Theorem 8.58. Then $(\mathfrak{g}(\mathbb{Q}), \mathfrak{h}(\mathbb{Q}))$ is a split semisimple Lie algebra over $\mathbb{Q}$. For every field k, $(\mathfrak{g}(\mathbb{Q}), \mathfrak{h}(\mathbb{Q})) \otimes_{\mathbb{Q}} k$ is a split semisimple Lie algebra over k with root system R. This reduces the problem of constructing a split semisimple Lie algebra over k with given root system R to the case of $k = \mathbb{C}$. For this, we have the following converse to Theorem 8.57.

THEOREM 8.59 *Let $\mathfrak{g}$ be the Lie algebra over $\mathbb{C}$ with $3n$ generators x_i, y_i, h_i $(1 \leq i \leq n)$ and defining relations*

$$\begin{aligned} [h_i, h_j] &= 0 \\ [x_i, y_i] &= h_i, \quad [x_i, y_j] = 0 \text{ if } i \neq j \\ [h_i, x_j] &= n(i,j)x_j, \quad [h_i, x_j] = -n(i,j)y_j \\ \mathrm{ad}(x_i)^{-n(i,j)+1}(x_j) &= 0 \text{ if } i \neq j \\ \mathrm{ad}(y_i)^{-n(i,j)+1}(y_j) &= 0 \text{ if } i \neq j, \end{aligned}$$

and let $\mathfrak{h}$ be the subalgebra of $\mathfrak{g}$ generated by the elements h_i. Then $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie with root system R.

PROOF. Serre 1966, VI, Appendix, Bourbaki LIE, VIII, §4, 3, Thm 1. □

Classification of split semisimple Lie algebras

THEOREM 8.60 *Every root system over k arises from a split semisimple Lie algebra over k.*

For an indecomposable root system of type A_n, B_n, C_n, or D_n this follows from examining the standard examples (see p.92 et seq.). In the general case, we can appeal to the theorems of the last section.

NOTES It is would perhaps be good to include a uniform proof, but it would be better to give a (beautiful) explicit description of the exceptional Lie algebras (see mo99736).

THEOREM 8.61 *The root system of a split semisimple Lie algebra determines it up to isomorphism.*

In more detail, let $(\mathfrak{g}, \mathfrak{h})$ and $(\mathfrak{g}', \mathfrak{h}')$ be split semisimple Lie algebras, and let S and S' be bases for their corresponding root systems. For each $\alpha \in S$, choose a nonzero $x_\alpha \in \mathfrak{g}^\alpha$, and similarly for $\mathfrak{g}'$. For any bijection $\alpha \mapsto \alpha' \colon S \to S'$ such that $\langle \alpha, \beta^\vee \rangle = \langle \alpha', \beta'^\vee \rangle$ for all $\alpha, \beta \in S$, there exists a unique isomorphism $\mathfrak{g} \to \mathfrak{g}'$ such that $x_\alpha \mapsto x_{\alpha'}$ and $h_\alpha \mapsto h_{\alpha'}$ for all $\alpha \in R$; in particular, $\mathfrak{h}$ maps into $\mathfrak{h}'$ (Bourbaki LIE, VIII, §4, 4, Thm 2; Serre 1966, VI, Theorem 8′).

Automorphisms of split semisimple Lie algebras

Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie group, let $R = R(\mathfrak{g}, \mathfrak{h})$ be its root system, and let B be a base for R.

Recall that $\mathrm{Aut}_0(\mathfrak{g})$ is the subgroup of $\mathrm{Aut}(\mathfrak{g})$ consisting of the automorphisms that become elementary over some algebraically closed field containing k. When we regard $\mathrm{Aut}(\mathfrak{g})$ as an algebraic group, $\mathrm{Aut}_0(\mathfrak{g})$ is its identity component, and

$$\mathrm{Aut}(\mathfrak{g}) \simeq \mathrm{Aut}_0(\mathfrak{g}) \rtimes \mathrm{Aut}(R, B)$$

where $\mathrm{Aut}(R, B)$ consists of the automorphisms of R leaving B stable; moreover, $\mathrm{Aut}(R, B)$ is canonically isomorphic to the group of automorphisms of the Dynkin diagram of $(\mathfrak{g}, \mathfrak{h})$. See Bourbaki LIE VIII, §5.

9 Representations of split semisimple Lie algebras

Throughout this subsection, $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra with root system $R \subset \mathfrak{h}^\vee$, and $\mathfrak{b}$ is the Borel subalgebra of $(\mathfrak{g}, \mathfrak{h})$ attached to a base S for R. According to Weyl's theorem (5.20) every $\mathfrak{g}$-module is a direct sum of its simple submodules, and so to classify all $\mathfrak{g}$-modules it suffices to classify the simple $\mathfrak{g}$-modules.

Proofs of the next three theorems can be found in Bourbaki LIE, VIII, §7 (and elsewhere).

THEOREM 9.1 *Let V be a simple $\mathfrak{g}$-module.*

(a) *There exists a unique one-dimensional subspace L of V stabilized by $\mathfrak{b}$.*
(b) *The L in (a) is a weight space for $\mathfrak{h}$, i.e., $L = V_{\varpi_V}$ for some $\varpi_V \in \mathfrak{h}^\vee$.*

(c) *The* ϖ_V *in (b) is dominant, i.e.,* $\varpi_V \in P_{++}$;
(d) *If* ϖ *is also a weight for* $\mathfrak{h}$ *in* V, *then* $\varpi = \varpi_V - \sum_{\alpha \in S} m_\alpha \alpha$ *with* $m_\alpha \in \mathbb{N}$.

Lie's theorem (3.7) shows that there does exist a one-dimensional eigenspace for $\mathfrak{b}$ — the content of (a) is that when V is a simple $\mathfrak{g}$-module, the space is unique. Since L is mapped into itself by $\mathfrak{b}$, it is also mapped into itself by $\mathfrak{h}$, and so lies in a weight space. The content of (b) is that it is the whole weight space.

Because of (d), ϖ_V is called the ***highest weight*** of the simple $\mathfrak{g}$-module V.

THEOREM 9.2 *Every dominant weight occurs as the highest weight of a simple* $\mathfrak{g}$*-module.*

THEOREM 9.3 *Two simple* $\mathfrak{g}$*-modules are isomorphic if and only if their highest weights are equal.*

Thus $V \mapsto \varpi_V$ defines a bijection from the set of isomorphism classes of simple $\mathfrak{g}$-modules onto the set of dominant weights P_{++}.

COROLLARY 9.4 *If* V *is a simple* $\mathfrak{g}$*-module, then* $\mathrm{End}(V,r) \simeq k$.

Let $V = V_\varpi$ with ϖ dominant. Every isomorphism $V_\varpi \to V_\varpi$ maps the highest weight line L into itself, and is determined by its restriction to L because L generates V_ϖ as a $\mathfrak{g}$-module.

EXAMPLE 9.5 Let $\mathfrak{g} = \mathfrak{sl}_W$, and choose a basis $(e_i)_{1 \le i \le n+1}$ for W as on p.92. Recall that

$$S = \{\alpha_1, \ldots, \alpha_n\}, \quad \alpha_i = \varepsilon_i - \varepsilon_{i+1}, \quad \varepsilon_i(\mathrm{diag}(a_1, \ldots, a_n)) = a_i$$

is a base for the root system of $(\mathfrak{g}, \mathfrak{h})$; moreover $h_{\alpha_i} = E_{i,i} - E_{i+1,i+1}$. Let

$$\varpi_i' = \varepsilon_1 + \cdots + \varepsilon_i.$$

Then

$$\varpi_i(h_{\alpha_j}) = \delta_{ij}, \quad 1 \le i, j \le n,$$

and so $\varpi_i' | \mathfrak{h}$ is the fundamental weight corresponding to α_i. This is represented by the element

$$\varpi_i = \varepsilon_1 + \cdots + \varepsilon_i - \frac{i}{n+1}(\varepsilon_1 + \cdots + \varepsilon_{n+1})$$

of V. Thus the fundamental weights corresponding to the base S are $\varpi_1, \ldots, \varpi_n$. We have

$$\begin{aligned} Q(R) &= \{m_1\varepsilon_1 + \cdots + m_{n+1}\varepsilon_{n+1} \mid m_i \in \mathbb{Z}, \quad m_1 + \cdots + m_{n+1} = 0\} \\ P(R) &= Q(R) + \mathbb{Z} \cdot \varpi_1 \\ P(R)/Q(R) &\simeq \mathbb{Z}/(n+1)\mathbb{Z}. \end{aligned}$$

The action of $\mathfrak{g}$ on W defines an action of $\mathfrak{g}$ on $\bigwedge^r W$. The elements

$$e_{i_1} \wedge \cdots \wedge e_{i_r}, \quad i_1 < \cdots < i_r,$$

form a basis for $\bigwedge^r W$, and $h \in \mathfrak{h}$ acts by

$$h \cdot (e_{i_1} \wedge \cdots \wedge e_{i_r}) = (\varepsilon_{i_1}(h) + \cdots + \varepsilon_{i_r}(h))(e_{i_1} \wedge \cdots \wedge e_{i_r}).$$

Therefore the weights of $\mathfrak{h}$ in $\bigwedge^r W$ are the elements

$$\varepsilon_{i_1} + \cdots + \varepsilon_{i_r}, \quad i_1 < \cdots < i_r,$$

and each has multiplicity 1. As the Weyl group acts transitively on the weights, $\bigwedge^r W$ is a simple $\mathfrak{g}$-module, and its highest weight is ϖ_r.

9.6 The category $\mathsf{Rep}(\mathfrak{g})$ is a semisimple k-linear tensor category to which we can apply tannakian theory. Statements (9.2, 9.3) allow us to identify the set of isomorphism classes of $\mathsf{Rep}(\mathfrak{g})$ with P_{++}. Let $M(P_{++})$ be the free commutative group with generators the elements of P_{++} and relations

$$\varpi = \varpi_1 + \varpi_2 \text{ if } V_\varpi \subset V_{\varpi_1} \otimes V_{\varpi_2}.$$

Then $P_{++} \to M(P_{++})$ is surjective, and two elements ϖ and ϖ' of P_{++} have the same image in $M(P_{++})$ if and only if there exist $\varpi_1, \ldots, \varpi_m \in P_{++}$ such that W_ϖ and $W_{\varpi'}$ are subrepresentations of $W_{\varpi_1} \otimes \cdots \otimes W_{\varpi_m}$. Later we shall prove that this condition is equivalent to $\varpi - \varpi' \in Q$, and so $M(P_{++}) \simeq P/Q$. In other words, $\mathsf{Rep}(\mathfrak{g})$ has a gradation by $P_{++}/Q \cap P_{++} \simeq P/Q$ but not by any larger quotient.

For example, let $\mathfrak{g} = \mathfrak{sl}_2$, so that $Q = \mathbb{Z}\alpha$ and $P = \mathbb{Z}\frac{\alpha}{2}$. For $n \in \mathbb{N}$, let $V(n)$ be a simple representation of $\mathfrak{g}$ with highest weight $\frac{n}{2}\alpha$. From the Clebsch-Gordon formula (Bourbaki LIE, VIII, §9), namely,

$$V(m) \otimes V(n) \approx V(m+n) \oplus V(m+n-2) \oplus \cdots \oplus V(m-n), \quad n \le m,$$

we see that $\mathsf{Rep}(\mathfrak{g})$ has a natural P/Q-gradation (but not a gradation by any larger quotient of P).

ASIDE 9.7 The above theorems are important, but are far from being the whole story. For example, we need an explicit construction of the simple representation with a given highest weight, and we need to know its properties, e.g., its character. Moreover, in order to determine $\mathsf{Rep}(\mathfrak{g})$ as a tensor category, it is is necessary to describe how the tensor product of two simple $\mathfrak{g}$-modules decomposes as a direct sum of $\mathfrak{g}$-modules.

ASIDE 9.8 Is it possible to prove that the kernel of $P_{++} \to M(P_{++})$ is $Q \cap P_{++}$ by using only the formulas for the characters and multiplicities of the tensor products of simple representations (cf. Humphreys 1972, §24, especially Exercise 12)?

NOTES At present, this section is only a summary.

10 Real Lie algebras

This section will describe semisimple Lie algebras over $\mathbb{R}$ (not necessarily split) and their representations in terms of "enhanced" Dynkin diagrams. The tannakian formalism will then allow us to read off a description of semisimple algebraic groups over $\mathbb{R}$ and their representations (in Chapter II).

11 Classical Lie algebras

The classical simple Lie algebras over an algebraically closed field are exactly those attached to simple (associative) algebras equipped with an involution. Since the descent theory for the two objects is the same so far as the inner forms are concerned, the correspondence between classical simple Lie algebras and central simple algebras with involution extends to every base field of characteristic zero. We shall explain this, and in Chapter II the tannakian formalism will allow us to read off a description of all classical simple algebraic groups over fields of characteristic zero in terms of central simple algebras with involution. Since class field theory classifies the central simple algebras with involution over p-adic fields and number fields, this will give us a description of the classical semisimple algebraic groups over such fields.

CHAPTER **II**

Algebraic Groups

In this chapter we show that most of the theory of algebraic groups in characteristic zero is visible already in the theory of Lie algebras. More precisely, let k be a field of characteristic zero. The functor $G \rightsquigarrow \mathrm{Lie}(G)$ from connected algebraic groups to Lie algebras is faithful, but it is far from being surjective on objects or morphisms. However, for a connected algebraic group G and its Lie algebra $\mathfrak{g}$, the functor $\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g})$ is fully faithful,[1] and so G can be recovered from $\mathfrak{g}$ as the Tannaka dual of a tensor subcategory of $\mathsf{Rep}(\mathfrak{g})$. In this way, the study of algebraic groups in characteristic zero comes down to the study of certain tensor subcategories of the categories of representations of Lie algebras.

Since every connected algebraic group has a filtration whose quotients are (a) a semisimple group, (b) a torus, or (c) a unipotent group it is natural to look first at each of these cases.

(a) When $\mathfrak{g}$ is semisimple, the representations of $\mathfrak{g}$ form a tannakian category $\mathsf{Rep}(\mathfrak{g})$ whose associated affine group G is the simply connected semisimple algebraic group G with Lie algebra $\mathfrak{g}$. In other words,

$$\mathsf{Rep}(G) = \mathsf{Rep}(\mathfrak{g})$$

with G a simply connected semisimple algebraic group having Lie algebra $\mathfrak{g}$. It is possible to compute the centre of G from $\mathsf{Rep}(\mathfrak{g})$, and to identify the subcategory of $\mathsf{Rep}(\mathfrak{g})$ corresponding to each quotient of G by a finite subgroup. This makes it possible to read off the entire theory of semisimple algebraic groups and their representations from the (apparently simpler) theory of semisimple Lie algebras.

(b) Let $\mathfrak{g}$ be a commutative Lie algebra. Then $\mathsf{Rep}(\mathfrak{g})$ has a tensor subcategory of semisimple representations and a tensor subcategory on which the elements of $\mathfrak{g}$ act as nilpotent endomorphisms. This reflects the fact that $\mathfrak{g}$ can be realized as the Lie algebra of a torus or as the Lie algebra of a product of copies of $\mathbb{G}_a$. Realizing $\mathfrak{g}$ as the Lie algebra of a split torus G amounts to choosing a lattice in $\mathfrak{g}$. Then $\mathsf{Rep}(G)$ is the category of semisimple representations of $\mathfrak{g}$ whose characters are integral on the lattice.

(c) Let $\mathfrak{g}$ be a nilpotent Lie algebra, and consider the category $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ of representations of $\mathfrak{g}$ such that the elements of $\mathfrak{g}$ act as nilpotent endomorphisms. Then $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ is a tannakian category whose associated affine group G is unipotent with Lie algebra $\mathfrak{g}$. In other words,

$$\mathsf{Rep}(G) = \mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$$

[1]Here we are using that k has characteristic zero. In characteristic $p \neq 0$, it is necessary to replace the Lie algebra with the algebra of distributions of G (see Jantzen 1987, I, §7). In characteristic zero, the algebra of distributions is just the universal enveloping algebra of $\mathfrak{g}$.

with G a unipotent algebraic group having Lie algebra $\mathfrak{g}$. In this way, we get an equivalence between the category of nilpotent Lie algebras and the category of unipotent algebraic groups.

(d) It is possible to combine (a) and (b). Let (G,T) be a split reductive group. The action of T on the Lie algebra $\mathfrak{g}$ of G induces a decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^{\alpha}, \quad \mathfrak{h} = \mathrm{Lie}(T),$$

of $\mathfrak{g}$ into eigenspaces $\mathfrak{g}^{\alpha}$ indexed by certain characters α of T, called the roots. A root α determines a copy $\mathfrak{s}_{\alpha}$ of $\mathfrak{sl}_2$ in $\mathfrak{g}$ (I, 8.31). From the composite of the exact tensor functors

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{s}_{\alpha}) \simeq \mathsf{Rep}(S_{\alpha}),$$

we obtain a homomorphism from a copy S_{α} of SL_2 into G. Regard α as a root of S_{α}; then its coroot $\alpha^{\vee}$ can be regarded as an element of $X_*(T)$. The system $(X^*(T), R, \alpha \mapsto \alpha^{\vee})$ is a root datum. From this, and the Borel fixed point theorem, the entire theory of split reductive groups over fields of characteristic zero follows easily.

(e) It is possible to combine (a) and (c). For a Lie algebra $\mathfrak{g}$ with largest nilpotent ideal $\mathfrak{n}$, we consider the category $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ of representations such that the elements of $\mathfrak{n}$ act as nilpotent endomorphisms. Ado's theorem (I, 6.27) assures us that $\mathfrak{g}$ has a faithful such representation. When k is algebraically closed, we get a one-to-one correspondence between the isomorphism classes of algebraic Lie algebras and the isomorphism classes of connected algebraic groups with unipotent centre.

In the current version of the notes, only the semisimple case is treated in detail.

Throughout this chapter, k is a field of characteristic zero.

NOTES The key thing we use in passing from Lie algebras to Lie groups is that the functor $\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g})$ is fully faithful. This certainly fails in characteristic p, but only for "small" p. Should investigate this, and at least include statements about what is true in characteristic p. Unfortunately, some of the theory of Lie algebras also fails for small p. Some of these questions are investigated in the articles of McNinch and Testerman.

1 Algebraic groups

In this section, we review the basic theory of algebraic groups over fields of characteristic zero — see AGS for more details. Eventually, the section will be expanded to make the notes independent of AGS except for a few proofs. See also Chapter 17 of AG.

Basic theory

Let Alg_k denote the category of commutative (associative) k-algebras.

1.1 Let Alg_k denote the category of k-algebras. A k-algebra A defines a functor

$$h^A \colon \mathsf{Alg}_k \to \mathsf{Set}, \quad R \rightsquigarrow \mathrm{Hom}(A, R),$$

and any functor isomorphic to h^A for some A is said to be *representable*. According to the Yoneda lemma,

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

and so the category of representable functors $\mathsf{Alg}_k \to \mathsf{Set}$ is locally small, i.e., the morphisms between any two objects form a set.

1.2 An ***affine group*** over k is a group object (G,m) in the category of representable functors $\mathsf{Alg}_k \to \mathsf{Set}$. Thus G is a representable functor $G\colon \mathsf{Alg}_k \to \mathsf{Set}$ and m is a natural transformation $m\colon G\times G \to G$ such that there exist natural transformations $e\colon * \to G$ and $\mathrm{inv}\colon G \to G$ making certain diagrams commute. This condition means that, for all k-algebras R,

$$m(R)\colon G(R)\times G(R) \to G(R) \tag{51}$$

is a group structure on $G(R)$. To give an affine group G over k amounts to giving a functor $G\colon \mathsf{Alg}_k \to \mathsf{Grp}$ such that the underlying set-valued functor is representable. When G is represented by a *finitely generated* k-algebra, it is called an ***affine algebraic group***.

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

1.3 Let (G,m) be an affine group. To say that G is representable means that there exists a k-algebra A together with an element $a \in G(A)$ such that, for all k-algebras R, the map

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

is a bijection. In other words, for every $b \in G(R)$ there is a unique homomorphism $f\colon A \to R$ such that $G(f)$ sends a to b. The pair (A,a) is uniquely determined up to a unique isomorphism by G. Any such A is called the ***coordinate ring*** of G, and is denoted $\mathcal{O}(G)$, and $a \in G(A)$ is called the ***universal element***. The natural transformation m then corresponds to a comultiplication map

$$\Delta\colon \mathcal{O}(G) \to \mathcal{O}(G)\otimes\mathcal{O}(G).$$

The existence of e and inv then means that $(\mathcal{O}(G),\Delta)$ is a Hopf algebra (AGS, II). Note that

$$G(R) \simeq \mathrm{Hom}_{k\text{-algebra}}(\mathcal{O}(G),R), \quad \text{all } k\text{-algebras } R.$$

To give an algebraic group over k amounts to giving a finitely generated k-algebra A together with a comultiplication homomorphism $\Delta\colon A \to A\otimes A$ such that, for all k-algebras R, the map

$$\mathrm{Hom}(A,R)\times\mathrm{Hom}(A,R) \simeq \mathrm{Hom}(A\otimes A,R) \xrightarrow{f_1,f_2\mapsto(f_1,f_2)\circ\Delta} \mathrm{Hom}(A,R)$$

is a group structure on $\mathrm{Hom}(A,R)$. Here (f_1,f_2) denotes the homomorphism

$$a_1\otimes a_2 \mapsto f(a_1)f(a_2)\colon A_1\otimes A_2 \to R.$$

1.4 A ***homomorphism of algebraic groups*** is a natural transformation of functors $u\colon G \to G'$ such that $m_{G'}\circ(u\times u) = u\circ m_G$. Such a homomorphism $u\colon H \to G$ is said to be ***injective*** if $u^\natural\colon \mathcal{O}(G) \to \mathcal{O}(H)$ is surjective and it is said to be ***surjective*** (or a ***quotient map***) if $u^\natural\colon \mathcal{O}(G) \to \mathcal{O}(H)$ is injective. The second definition is only sensible because injective homomorphisms of Hopf algebras are automatically faithfully flat (AGS, VI, 11.1). An ***embedding*** is an injective homomorphism, and a ***quotient map*** is a surjective homomorphism.

By a "subgroup" of an algebraic group we mean an "affine algebraic subgroup".

1.5 The standard isomorphism theorems in group theory hold for algebraic groups. For example, if H and N are algebraic subgroups of an algebraic group G with N normal, then $N/H\cap N \simeq HN/N$. The only significant difficulty in extending the usual proofs to algebraic groups is in showing that the quotient G/N of an algebraic group by a normal subgroup exists (AGS, VIII, 17.5).

1.6 An algebraic group G is ***finite*** if $\mathcal{O}(G)$ is a finite k-algebra, i.e., finitely generated as a k-vector space.

1.7 As k has characteristic zero, $\mathcal{O}(G)$ is geometrically reduced (Cartier's theorem, AGS, VI, 9.3), and so $|G| \overset{\text{def}}{=} \operatorname{Spm} \mathcal{O}(G)$ is a group in the category of algebraic varieties over k (in fact, of smooth algebraic varieties over k). If H is an algebraic subgroup of G, then $|H|$ is a closed subvariety of $|G|$.

1.8 An algebraic group G is ***connected*** if $|G|$ is connected or, equivalently, if $\mathcal{O}(G)$ contains no étale k-algebra except k. A connected algebraic group remains connected over any extension of the base field. The identity component of an algebraic group G is denoted by G°.

1.9 A ***character*** of an algebraic group G is a homomorphism $\chi: G \to \mathbb{G}_m$. We write $X_k(G)$ for the group of characters of G over k and $X^*(G)$ for the similar group over an algebraic closure of k.

Groups of multiplicative type

1.10 Let M be a finitely generated commutative group. The functor

$$R \mapsto \operatorname{Hom}(M, R^{\times}) \quad \text{(homomorphisms of abstract groups)}$$

is an algebraic group $D(M)$ with coordinate ring the group algebra of M. For example, $D(\mathbb{Z}) \simeq \mathbb{G}_m$. The algebraic group $D(M)$ is connected if and only if M is torsion-free, and it is finite if and only if M is finite.

1.11 A ***group-like element*** of a Hopf algebra (A, Δ) is a unit u in A such that $\Delta(u) = u \otimes u$. If A is finitely generated as a k-algebra, then the group-like elements form a finitely generated subgroup $g(A)$ of $A^{\times}$, and for any finitely generated abelian group M,

$$\operatorname{Hom}_{\text{alg gps}}(G, D(M)) \simeq \operatorname{Hom}_{\text{abstract gps}}(M, g(\mathcal{O}(G))).$$

In particular,

$$X_k(G) \overset{\text{def}}{=} \operatorname{Hom}(G, \mathbb{G}_m) \simeq g(\mathcal{O}(G)).$$

An algebraic group G is said to be ***diagonalizable*** if the group-like elements in $\mathcal{O}(G)$ span it. For example, $D(M)$ is diagonalizable, and a diagonalizable group G is isomorphic to $D(M)$ with $M = g(\mathcal{O}(G))$.

1.12 An algebraic group that becomes diagonalizable after an extension of the base field is said to be of ***multiplicative type***, and it is a ***torus*** if connected. A torus over k is said to be ***split*** if it is already diagonalizable over k.

1.13 (RIGIDITY) Every action of an algebraic group G on a group H of multiplicative type is trivial on the identity component of G.

Semisimple, reductive, solvable, and unipotent groups

1.14 Let G be a connected algebraic group, and consider the commutative normal connected subgroups of G. The algebraic group G is said to be ***semisimple*** if the only such subgroup is the trivial group, and it is said to be ***reductive*** if the only such subgroups are tori.[2]

1.15 An algebraic group is said to be ***solvable*** if it admits a filtration by normal subgroups whose quotients are all commutative. Among the connected solvable normal subgroups of an algebraic group G, there is a largest one, called the ***radical*** RG of G. A connected algebraic group is semisimple if and only if its radical is trivial.

1.16 An algebraic group is said to be ***unipotent*** if every nonzero representation of the group has a nonzero fixed vector. Among the connected unipotent normal subgroups of an algebraic group G, there is a largest one, called the ***unipotent radical*** $R_u G$ of G. A connected algebraic group is reductive if and only if its unipotent radical is trivial.

Examples of algebraic groups

1.17 For a k-algebra R, let $\mathrm{SL}_n(R)$ denote the group of $n \times n$ matrices of determinant 1 with entries in R. Then SL_n is a functor $\mathsf{Alg}_k \to \mathsf{Set}$, and matrix multiplication defines a natural transformation $m\colon \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SL}_2$. Note that

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

Therefore (SL_n, m) is an algebraic group, called the ***special linear group***. Moreover,

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

and the universal element is the matrix $X = (x_{ij})_{1 \le i,j \le n}$: for any k-algebra R and $n \times n$ matrix $M = (m_{ij})$ of determinant 1 with entries in R, there is a unique homomorphism $\mathcal{O}(\mathrm{SL}_n) \to R$ sending sending X to M.

1.18 Let GL_n denote the functor sending a k-algebra R to the set of invertible $n \times n$ matrices with entries in R. With the map m defined by matrix multiplication, it is an algebraic group, called the ***general linear group***. Let A denote the polynomial ring

$$k[X_{11}, X_{12}, \ldots, X_{nn}, Y_{11}, \ldots, Y_{nn}]$$

modulo the ideal generated by the n^2 entries of the matrix $(X_{ij})(Y_{ij}) - I$, i.e., by the polynomials

$$\textstyle\sum_{j=1}^{n} X_{ij} Y_{jk} - \delta_{ik}, \quad 1 \le i,k \le n, \quad \delta_{ik} = \text{Kronecker delta.}$$

Then

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

[2]These definitions are correct only in characteristic zero. See AGS XVIII, §2.

The map $(M,N) \mapsto M$ projects this set bijectively onto $\{M \in M_n(R) \mid M \text{ is invertible}\}$ (because the right inverse of a square matrix is unique if it exists, and is also a left inverse) and so

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

Therefore $\mathcal{O}(\mathrm{GL}_n) = A$, and the universal element is the matrix $(x_{ij})_{1\le i,j\le n} \in M_n(A)$.

1.19 Let V be a finite-dimensional vector space over k, and for a k-algebra R, let $\mathrm{GL}_V(R)$ denote the group of R-linear automorphisms of $R\otimes V$. The choice of a basis for V determines an isomorphism $\mathrm{GL}_V(R) \simeq \mathrm{GL}_n(R)$, and so $R \rightsquigarrow \mathrm{GL}_V(R)$ is an algebraic group. It is also called the ***general linear group***.

1.20 Let C be an invertible $n\times n$ matrix with entries in k. For a k-algebra R, the $n\times n$ matrices T with entries in R such that

$$T^t\cdot C\cdot T = C \tag{52}$$

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

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

and so

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

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

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

Therefore G is an algebraic group. Write

$$A = k[x_{11},\ldots,x_{nn}].$$

Then the matrix $a=(x_{ij})_{1\le i,j\le n}$ with entries in A is the universal element: it satisfies (52) and for any k-algebra R and matrix M in $M_n(R)$ satisfying (52), there is a unique homomorphism $A\to R$ sending a to M.

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

NOTES Need to do more of this for affine groups, not necessarily of finite type, because they come up in the following sections.

2 Representations of algebraic groups; tensor categories

This section reviews the basic theory of the representations of algebraic groups and of tensor categories. Eventually, the section will be expanded to make the notes independent of AGS and Deligne and Milne 1982.

Throughout, k is a field of characteristic zero.

Basic theory

2.1 For a vector space V over k and a k-algebra R, we set $V(R)$ or V_R equal to $R \otimes_k V$. Let G be an affine group over k, and suppose that for every k-algebra R, we have an action

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

of $G(R)$ on $V(R)$ such that each $g \in G(R)$ acts R-linearly; if the resulting homomorphisms

$$r(R): G(R) \to \mathrm{Aut}_{R\text{-linear}}(V(R))$$

are natural in R, then r is called a ***linear representation*** of G on V. A representation of G on a finite-dimensional vector space V is nothing more than a homomorphism of algebraic groups $r: G \to \mathrm{GL}_V$. A representation is ***faithful*** if all the homomorphisms $r(R)$ are injective. For $g \in G(R)$, I shorten $r(R)(g)$ to $r(g)$. The finite-dimensional representations of G form a category $\mathsf{Rep}(G)$.[3]

From now on, "representation" will mean "linear representation".

2.2 Let G be an algebraic group over k. Let $A = \mathcal{O}(G)$, and let $\Delta: A \to A \otimes A$ and $\epsilon: A \to k$ be the comultiplication map and the neutral element. An A-***comodule*** is a k-linear map

$$\rho: V \to V \otimes A$$

such that

$$\begin{cases} (\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_A) \circ \rho & (\text{maps } V \to V \otimes A \otimes A) \\ (\mathrm{id}_V \otimes \epsilon) \circ \rho = \mathrm{id}_V & (\text{maps } V \to V). \end{cases}$$

Let r be a representation of G on V, and let a be the universal element in $G(A)$. Then $r(A)(a)$ is an A-linear map $V(A) \to V(A)$ whose restriction to $V \subset V(A)$ is an A-comodule structure on V. Conversely, an A-comodule structure on V extends by linearity to an A-linear map $V(A) \to V(A)$ which determines a representation of G on V. In this way, representations of G on V correspond to A-comodule structures on V (see AGS, VIII, §6). The comultiplication map $\Delta: A \to A \otimes_k A$ defines a comodule structure on the k-vector space A, and hence a representation of G on A (called the ***regular representation***).

2.3 Every representation of an algebraic group is a filtered union of finite-dimensional subrepresentations (AGS, VIII, 6.6). Every sufficiently large finite-dimensional subrepresentation of the regular representation of G is a faithful finite-dimensional representation of G (AGS, VIII, 6.6).

2.4 Let $G \to \mathrm{GL}_V$ be a faithful finite-dimensional representation of G. Then every other finite-dimensional representation of G can be obtained from V by forming duals (contragredients), tensor products, direct sums, and subquotients (AGS, VIII, 11.7). In other words, with the obvious notation, every finite-dimensional representation is a subquotient of $P(V, V^\vee)$ for some polynomial $P \in \mathbb{N}[X, Y]$.

[3] In the following, we shall sometimes assume that $\mathsf{Rep}(G)$ has been replaced by a small subcategory, e.g., the category of representations of G on vector spaces of the form k^n, $n = 0, 1, 2, \ldots$.

2.5 *Let $G \to \mathrm{GL}_V$ be a representation of G, and let W be a subspace of V. The functor*

$$R \rightsquigarrow \{g \in G(R) \mid gW_R = W_R\}$$

is a subgroup of G (denoted G_W, and called the ***stabilizer*** *of W in G).*

To see this, let $\rho: V \to V \otimes \mathcal{O}(G)$ be the comodule map. Let $(e_i)_{i \in J}$ be a basis for W, and extend it to a basis $(e_i)_{J \sqcup I}$ for V. Write

$$\rho(e_j) = \sum\nolimits_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

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

$$ge_j = \sum\nolimits_{i \in J \sqcup I} e_i \otimes g(a_{ij}).$$

Thus, $g(W \otimes R) \subset W \otimes R$ if and only if $g(a_{ij}) = 0$ for $j \in J$, $i \in I$. As $g(a_{ij}) = (a_{ij})_R(g)$, this shows that the functor is represented by the quotient of $\mathcal{O}(G)$ by the ideal generated by $\{a_{ij} \mid j \in J, i \in I\}$.

2.6 *Every algebraic subgroup H of an algebraic group G arises as the stabilizer of a subspace W of some finite-dimensional representation of V of G, i.e.,*

$$H(R) = \{g \in G(R) \mid g(W \otimes_k R) = W \otimes_k R\}, \quad \text{all } k\text{-algebras } R.$$

To see this, let $\mathfrak{a}$ be the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$. Then $\mathfrak{a}$ is finitely generated, and according to (2.3), we can find a finite-dimensional G-stable subspace V of $\mathcal{O}(G)$ containing a generating set for $\mathfrak{a}$; take $W = V \cap \mathfrak{a}$ (AGS, VIII, 13.1).

Elementary Tannaka duality

2.7 *Let G be an algebraic group over k, and let R be a k-algebra. Suppose that for each representation (V, r_V) of G on a finite-dimensional k-vector space V, we have an R-linear endomorphism λ_V of $V(R)$. If the family (λ_V) satisfies the conditions,*

- ◇ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ *for all representations V, W,*
- ◇ $\lambda_{\mathbb{1}} = \mathrm{id}_{\mathbb{1}}$ *(here $\mathbb{1} = k$ with the trivial action),*
- ◇ $\lambda_W \circ \alpha_R = \alpha_R \circ \lambda_V$, *for all G-equivariant maps $\alpha: V \to W$,*

then there exists a $g \in G(R)$ such that $\lambda_V = r_V(g)$ for all V (AGS, X, 1.2).

Because G admits a faithful finite-dimensional representation (see 2.3), g is uniquely determined by the family (λ_V), and so the map sending $g \in G(R)$ to the family $(r_V(g))$ is a bijection from $G(R)$ onto the set of families satisfying the conditions in the theorem. Therefore we can recover G from the category $\mathsf{Rep}(G)$ of representations of G on finite-dimensional k-vector spaces.

2.8 Let G be an algebraic group over k. For each k-algebra R, let $G'(R)$ be the set of families (λ_V) satisfying the conditions in (2.7). Then G' is a functor from k-algebras to groups, and there is a natural map $G \to G'$. That this map is an isomorphism is often paraphrased by saying that ***Tannaka duality holds for G***.

Since each of G and $\mathsf{Rep}(G)$ determines the other, we should be able to see the properties of one reflected in the other.

2.9 *An algebraic group G is finite if and only if there exists a representation V of G such that every other representation is a subquotient of V^n for some $n \geq 0$ (AGS, XII, 1.4).*

2.10 *An algebraic group G is connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\mathsf{Rep}(G)$ whose objects are those isomorphic to subquotients of V^n, $n \geq 0$, is not stable under $\otimes$ (apply 2.9).*

2.11 *An algebraic group is unipotent if and only if every nonzero representation has a nonzero fixed vector (AGS, XV, 2.1).*

2.12 *A connected algebraic group is solvable if and only if every nonzero representation acquires a one-dimensional subrepresentation over a finite extension of the base field (Lie-Kolchin theorem, AGS, XVI, 4.7).*

2.13 *A connected algebraic group is reductive if and only if every finite-dimensional representation is semisimple (AGS, XVIII, 5.4).*

2.14 *Let $u\colon G \to G'$ be a homomorphism of algebraic groups, and let $u^\vee\colon \mathsf{Rep}(G') \to \mathsf{Rep}(G)$ be the functor $(V,r) \rightsquigarrow (V, r\circ u)$. Then:*

(a) *u is surjective if and only if $u^\vee$ is fully faithful and every subobject of $u^\vee(V')$ for V' a representation of G' is isomorphic to the image of a subobject of V';*
(b) *u is injective if and only if every object of $\mathsf{Rep}(G)$ is isomorphic to a subquotient of an object of the form $u^\vee(V)$.*

When $\mathsf{Rep}(G)$ is semisimple, the second condition in (a) is superfluous: thus u is surjective if and only $u^\vee$ is fully faithful. (AGS X, 4.1, 4.2, 4.3).

Tensor categories

Basic definitions

2.15 A k-***linear category*** is an additive category in which the Hom sets are finite-dimensional k-vector spaces and composition is k-bilinear. Functors between such categories are required to be k-linear, i.e., induce k-linear maps on the Hom sets.

2.16 A ***tensor category*** over k is a k-linear category together with a k-bilinear functor $\otimes\colon \mathsf{C}\times\mathsf{C} \to \mathsf{C}$ compatible with certain associativity and commutativity ensuring that the tensor product of any unordered finite set of objects is well-defined up to a well-defined isomorphism. An associativity constraint is a natural isomorphism

$$\phi_{U,V,W}\colon U\otimes(V\otimes W) \to (U\otimes V)\otimes W, \quad U,V,W \in \mathrm{ob}(\mathsf{C}),$$

and a commutativity constraint is a natural isomorphism

$$\psi_{V,W}\colon V\otimes W \to W\otimes V, \quad V,W \in \mathrm{ob}(\mathsf{C}).$$

Compatibility means that certain diagrams, for example,

$$\begin{array}{ccccc} U\otimes(V\otimes W) & \xrightarrow{\phi_{U,V,W}} & (U\otimes V)\otimes W & \xrightarrow{\psi_{U\otimes V,W}} & W\otimes(U\otimes V) \\ \downarrow{\scriptstyle \mathrm{id}_U\otimes\psi_{V,W}} & & & & \downarrow{\scriptstyle \phi_{W,U,V}} \\ U\otimes(W\otimes V) & \xrightarrow{\phi_{U,W,V}} & (U\otimes W)\otimes V & \xrightarrow{\psi_{U,W}\otimes\mathrm{id}_V} & (W\otimes U)\otimes V, \end{array}$$

commute, and that there exists a neutral object (tensor product of the empty set), i.e., an object U together with an isomorphism $u\colon U\to U\otimes U$ such that $V\mapsto V\otimes U$ is an equivalence of categories. For a complete definition, see Deligne and Milne 1982, §1. We use $\mathbb{1}$ to denote a neutral object of C.

2.17 An object of a tensor category is ***trivial*** if it is isomorphic to a direct sum of neutral objects.

EXAMPLE 2.18 The category of finitely generated modules over a ring R becomes a tensor category with the usual tensor product and the constraints

$$\left.\begin{array}{rl} u\otimes(v\otimes w)\mapsto(u\otimes v)\otimes w\colon & U\otimes(V\otimes W)\to(U\otimes V)\otimes W \\ v\otimes w\to w\otimes v\colon & V\otimes W\to W\otimes V. \end{array}\right\} \tag{53}$$

Any free R-module U of rank one together with an isomorphism $U\to U\otimes U$ (equivalently, the choice of a basis for U) is a neutral object. It is trivial to check the compatibility conditions for this to be a tensor category.

EXAMPLE 2.19 The category of finite-dimensional representations of a Lie algebra or of an algebraic (or affine) group G with the usual tensor product and the constraints (53) is a tensor category. The required commutativities follow immediately from (2.18).

2.20 Let $(\mathsf{C},\otimes)$ and $(\mathsf{C}',\otimes)$ be tensor categories over k. A ***tensor functor*** $\mathsf{C}\to\mathsf{C}'$ is a pair (F,c) consisting of a functor $F\colon\mathsf{C}\to\mathsf{C}'$ and a natural isomorphism $c_{V,W}\colon F(V)\otimes F(W)\to F(V\otimes W)$ compatible with the associativity and commutativity constraints and sending neutral objects to neutral objects. Then F commutes with finite tensor products up to a well-defined isomorphism. See Deligne and Milne 1982, 1.8.

2.21 Let C be a tensor category over k, and let V be an object of C. A pair

$$(V^\vee, V^\vee\otimes V\xrightarrow{\mathrm{ev}}\mathbb{1})$$

is called a ***dual*** of V if there exists a morphism $\delta_V\colon\mathbb{1}\to V\otimes V^\vee$ such that the composites

$$\begin{array}{ccccc} V & \xrightarrow{\delta_V\otimes V} & V\otimes V^\vee\otimes V & \xrightarrow{V\otimes\mathrm{ev}} & V \\ V^\vee & \xrightarrow{V^\vee\otimes\delta_V} & V^\vee\otimes V\otimes V^\vee & \xrightarrow{\mathrm{ev}\otimes V^\vee} & V^\vee \end{array}$$

are the identity morphisms on V and $V^\vee$ respectively. Then δ_V is uniquely determined, and the dual $(V^\vee,\mathrm{ev})$ of V is uniquely determined up to a unique isomorphism. For example, a finite-dimensional k-vector space V has as a dual $V^\vee\overset{\text{def}}{=}\mathrm{Hom}_k(V,k)$ with $\mathrm{ev}(f\otimes v)=f(v)$ — here δ_V is the k-linear map sending 1 to $\sum e_i\otimes f_i$ for any basis (e_i) for V and its dual basis (f_i). Similarly, the contragredient of a representation of a Lie algebra or of an algebraic group is a dual of the representation.

2.22 A tensor category is ***rigid*** if every object admits a dual. For example, the category Vec_k of finite-dimensional vector spaces over k and the category of finite-dimensional representations of a Lie algebra (or an algebraic group) are rigid.

Neutral tannakian categories

2.23 A ***neutral tannakian category over*** k is an abelian k-linear category C endowed with a rigid tensor structure for which there exists an exact tensor functor $\omega\colon \mathsf{C} \to \mathsf{Vec}_k$. Such a functor ω is called a ***fibre functor over*** k. We shall refer to a pair (C, ω) consisting of a neutral tannakian category over k and a fibre functor over k as a neutral tannakian category over k.

THEOREM 2.24 *Let (C, ω) be a neutral tannakian category over k. For each k-algebra R, let $G(R)$ be the set of families*

$$\lambda = (\lambda_V)_{V \in \mathrm{ob}(\mathsf{C})}, \quad \lambda_V \in \mathrm{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

- $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ *for all* $V, W \in \mathrm{ob}(\mathsf{C})$,
- $\lambda_{\mathbb{1}} = \mathrm{id}_{\omega(\mathbb{1})}$ *for every neutral object of* $\mathbb{1}$ *of* C, *and*
- $\lambda_W \circ \alpha_R = \alpha_R \circ \lambda_V$ *for all arrows* $\alpha\colon V \to W$ *in* C.

Then $R \rightsquigarrow G(R)$ is an affine group over k, and ω defines an equivalence of tensor categories over k,

$$\mathsf{C} \to \mathsf{Rep}(G).$$

PROOF. This is an abstract version of AGS, X, 3.14. □

2.25 Let ω_R be the functor $V \rightsquigarrow \omega(V) \otimes R$; then $G(R)$ consists of the natural transformations $\lambda\colon \omega_R \to \omega_R$ such that the following diagrams commute

$$\begin{array}{ccc} \omega_R(V)\otimes\omega_R(W) & \xrightarrow{c_{V,W}} & \omega_R(V\otimes W) \\ \downarrow{\scriptstyle \lambda_V\otimes\lambda_W} & & \downarrow{\scriptstyle \lambda_{V\otimes W}} \\ \omega_R(V)\otimes\omega_R(W) & \xrightarrow{c_{V,W}} & \omega_R(V\otimes W) \end{array} \qquad \begin{array}{ccc} \omega_R(\mathbb{1}) & \xrightarrow{\omega_R(u)} & \omega_R(\mathbb{1}\otimes\mathbb{1}) \\ \downarrow{\scriptstyle \lambda_{\mathbb{1}}} & & \downarrow{\scriptstyle \lambda_{\mathbb{1}}} \\ \omega_R(\mathbb{1}) & \xrightarrow{\omega_R(u)} & \omega_R(\mathbb{1}\otimes\mathbb{1}) \end{array}$$

for all objects V, W of C and all identity objects $(\mathbb{1}, u)$.

2.26 I explain the final statement of (2.24). For each V in C, there is a representation $r_V\colon G \to \mathrm{GL}_{\omega(V)}$ defined by

$$r_V(g)v = \lambda_V(v) \text{ if } g = (\lambda_V) \in G(R) \text{ and } v \in V(R).$$

The functor sending V to $\omega(V)$ endowed with this action of G is an equivalence of categories $\mathsf{C} \to \mathsf{Rep}(G)$.

2.27 If the group G in (2.24) is an algebraic group, then (2.3) and (2.4) show that C has an object V such that every other object is a subquotient of $P(V, V^\vee)$ for some $P \in \mathbb{N}[X, Y]$. Conversely, if there exists an object V of C with this property, then G is algebraic because $G \subset \mathrm{GL}_V$.

2.28 It is usual to write $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ (functor of tensor automorphisms of ω) for the affine group G attached to the neutral tannakian category (C,ω) — we call it the ***Tannaka dual*** or ***Tannaka group*** of C.

EXAMPLE 2.29 If C is the category of finite-dimensional representations of an algebraic group H over k and ω is the forgetful functor, then $G(R) \simeq H(R)$ by (2.7), and $\mathsf{C} \to \mathsf{Rep}(G)$ is the identity functor.

EXAMPLE 2.30 Let N be a normal subgroup of an algebraic group G, and let C be the subcategory of $\mathsf{Rep}(G)$ consisting of the representations of G on which N acts trivially. The group attached to C and the forgetful functor is G/N. Alternatively, this can be used as a definition of G/N, but then one has to check that the kernel of the map $G \to G/N$ is N.

EXAMPLE 2.31 Let (C,ω) and (C',ω') be neutral tannakian categories with Tannaka duals G and G'. An exact tensor functor $F\colon \mathsf{C} \to \mathsf{C}'$ such that $\omega' \circ F = \omega$ defines a homomorphism $G' \to G$, namely,

$$(\lambda_V)_{V\in \mathrm{ob}(\mathsf{C}')} \mapsto (\lambda_{FV})_{V\in \mathrm{ob}(\mathsf{C})}\colon G'(R) \to G(R).$$

EXAMPLE 2.32 The category of representations of $\mathbb{Z}$ (as an abstract group) on finite-dimensional vector spaces over k is tannakian. The Tannaka dual of this category is of the form $T \times \mu_\infty \times \mathbb{G}_a$ with T a pro-torus (cf. 4.17 below).

2.33 Let $\mathsf{C} = \mathsf{Rep}(G)$ for some algebraic group G.

(a) For an algebraic subgroup H of G, let C^H denote the full subcategory of C whose objects are those on which H acts trivially. Then C^H is a neutral tannakian category whose Tannaka dual is G/N where N is the smallest normal algebraic subgroup of G containing H (intersection of the normal algebraic subgroups containing H).

(b) (***Tannaka correspondence***.) For a collection S of objects of $\mathsf{C} = \mathsf{Rep}(G)$, let $H(S)$ denote the largest subgroup of G acting trivially on all V in S; thus

$$H(S) = \bigcap_{V\in S} \mathrm{Ker}(r_V\colon G \to \mathrm{Aut}(V)).$$

Then the maps $S \mapsto H(S)$ and $H \mapsto \mathsf{C}^H$ form a Galois correspondence

$$\{\text{subsets of } \mathrm{ob}(\mathsf{C})\} \rightleftarrows \{\text{algebraic subgroups of } G\},$$

i.e., both maps are order reversing and $\mathsf{C}^{H(S)} \supset S$ and $H(\mathsf{C}^H) \supset H$ for all S and H. It follows that the maps establish a one-to-one correspondence between their respective images. In this way, we get a natural one-to-one order-reversing correspondence

$$\{\text{tannakian subcategories of } \mathsf{C}\} \overset{1:1}{\leftrightarrow} \{\text{normal algebraic subgroups of } G\}$$

(a tannakian subcategory is a full subcategory closed under the formation of duals, tensor products, direct sums, and subquotients).

Gradations on tensor categories

2.34 Let M be a finitely generated abelian group. An ***M-gradation*** on an object X of an abelian category is a family of subobjects $(X^m)_{m\in M}$ such that $X = \bigoplus_{m\in M} X^m$. An ***$M$-gradation*** on a tensor category C is an M-gradation on each object X of C compatible with all arrows in C and with tensor products in the sense that $(X\otimes Y)^m = \bigoplus_{r+s=m} X^r \otimes X^s$. Let (C,ω) be a neutral tannakian category, and let $G(\omega)$ be its Tannaka dual. To give an M-gradation on C is the same as giving a central homomorphism $D(M)\to G(\omega)$: a homomorphism corresponds to the M-gradation such that X^m is the subobject of X on which $D(M)$ acts through the character m (Saavedra Rivano 1972; Deligne and Milne 1982, §5).

2.35 Let C be a semisimple k-linear tensor category such that $\mathrm{End}(X)=k$ for every simple object X in C, and let $I(\mathsf{C})$ be the set of isomorphism classes of simple objects in C. For elements $x, x_1,\ldots,x_m$ of $I(\mathsf{C})$ represented by simple objects $X, X_1,\ldots,X_m$, write $x \prec x_1\otimes\cdots\otimes x_m$ if X is a direct factor of $X_1\otimes\cdots\otimes X_m$. The following statements are obvious.

(a) Let M be a commutative group. To give an M-gradation on C is the same as to give a map $f\colon I(\mathsf{C})\to M$ such that

$$x \prec x_1\otimes x_2 \implies f(x) = f(x_1)+f(x_2).$$

A map from $I(\mathsf{C})$ to a commutative group satisfying this condition will be called a ***tensor map***. For such a map, $f(\mathbb{1})=0$, and if X has dual $X^\vee$, then $f([X^\vee]) = -f([X])$.

(b) Let $M(\mathsf{C})$ be the free abelian group with generators the elements of $I(\mathsf{C})$ modulo the relations: $x = x_1+x_2$ if $x\prec x_1\otimes x_2$. The obvious map $I(\mathsf{C})\to M(\mathsf{C})$ is a universal tensor map, i.e., it is a tensor map, and every other tensor map $I(\mathsf{C})\to M$ factors uniquely through it. Note that $I(\mathsf{C})\to M(\mathsf{C})$ is surjective.

2.36 Let (C,ω) be a neutral tannakian category such that C is semisimple and $\mathrm{End}(V)=k$ for every simple object in C. Let Z be the centre of $G \overset{\text{def}}{=} \underline{\mathrm{Aut}}^{\otimes}(\omega)$. Because C is semisimple, G is reductive (2.13), and so Z is of multiplicative type. Assume (for simplicity) that Z is split, so that $Z = D(N)$ with N the group of characters of Z. According to (2.34), to give an M-gradation on C is the same as to give a homomorphism $D(M)\to Z$, or, equivalently, a homomorphism $N\to M$. On the other hand, (2.35) shows that to give an M-gradation on C is the same as giving a homomorphism $M(\mathsf{C})\to M$. Therefore $M(\mathsf{C})\simeq N$. In more detail: let X be an object of C; if X is simple, then Z acts on X through a character n of Z, and the tensor map $[X]\mapsto n\colon I(\mathsf{C})\to N$ is universal.

2.37 Let (C,ω) be as in (2.36), and define an equivalence relation on $I(\mathsf{C})$ by

$$a\sim a' \iff \text{there exist } x_1,\ldots,x_m\in I(\mathsf{C}) \text{ such that } a,a'\prec x_1\otimes\cdots\otimes x_m.$$

A function f from $I(\mathsf{C})$ to a commutative group defines a gradation on C if and only if $f(a)=f(a')$ whenever $a\sim a'$. Therefore, $M(\mathsf{C})\simeq I(\mathsf{C})/{\sim}$.

3 The Lie algebra of an algebraic group

In this section, we define the functor Lie from algebraic groups to Lie algebras and study its basic properties. Recall that k is a field of characteristic zero.

Definition of the Lie algebra of an algebraic group

Let G be an algebraic group. The action of G on itself by conjugation,

$$(g,x) \mapsto gxg^{-1}: G \times G \to G,$$

fixes e, and so it defines a representation of G on the tangent space $\mathfrak{g}$ of G at e,

$$G \to \mathrm{GL}_{\mathfrak{g}}.$$

In turn, this gives a map on the tangent spaces at the neutral elements of G and $\mathrm{GL}_{\mathfrak{g}}$,

$$\mathrm{ad}: \mathfrak{g} \to \mathrm{End}(\mathfrak{g}).$$

The Lie algebra of G is defined to be the k-vector space $\mathfrak{g}$ endowed with the bracket

$$[x,y] \stackrel{\text{def}}{=} \mathrm{ad}(x)(y).$$

For example, if $G = \mathrm{GL}_V$, then $\mathfrak{g}$ is the vector space $\mathrm{End}(V)$ endowed with the bracket

$$[\alpha,\beta] = \alpha \circ \beta - \beta \circ \alpha$$

(see I, 1.5). We now explain this construction in detail.

Definition of $\mathfrak{g}(R)$

Let R be a k-algebra, and let $R[\varepsilon] = R[X]/(X^2)$. Thus $R[\varepsilon] = R \oplus R\varepsilon$ as an R-module, and $\varepsilon^2 = 0$. We have homomorphisms

$$R \xrightarrow{i} R[\varepsilon] \xrightarrow{\pi} R, \quad i(a) = a + \varepsilon 0, \quad \pi(a+\varepsilon b) = a, \quad \pi \circ i = \mathrm{id}_R.$$

For an affine group G over k, they give homomorphisms

$$G(R) \xrightarrow{i} G(R[\varepsilon]) \xrightarrow{\pi} G(R), \quad \pi \circ i = \mathrm{id}_{G(R)}$$

where we have written i and π for $G(i)$ and $G(\pi)$. Let

$$\mathfrak{g}(R) = \mathrm{Ker}(G(R[\varepsilon]) \xrightarrow{\pi} G(R)).$$

EXAMPLE 3.1 Let $G = \mathrm{GL}_n$. For each $A \in M_n(R)$, $I_n + \varepsilon A$ is an element of $M_n(R[\varepsilon])$, and

$$(I_n + \varepsilon A)(I_n - \varepsilon A) = I_n;$$

therefore $I_n + \varepsilon A \in \mathfrak{g}(R)$. Clearly every element of $\mathfrak{g}(R)$ is of this form, and so the map

$$A \mapsto E(A) \stackrel{\text{def}}{=} I_n + \varepsilon A: M_n(k) \to \mathfrak{g}(R)$$

is a bijection. Therefore

$$\mathfrak{g}(R) = \{I_n + \varepsilon A \mid A \in M_n(k)\}.$$

EXAMPLE 3.2 Let $G = \mathrm{GL}_V$ where V is a finite-dimensional vector space over k. Every element of $V(\varepsilon) \stackrel{\text{def}}{=} k[\varepsilon] \otimes_k V$ can be written uniquely in the form $x + \varepsilon y$ with $x, y \in V$, i.e., $V(\varepsilon) = V \oplus \varepsilon V$. For k-linear endomorphisms α and β of V, define $\alpha + \varepsilon\beta$ to be the map $V(\varepsilon) \to V(\varepsilon)$ such that

$$(\alpha + \varepsilon\beta)(x + \varepsilon y) = \alpha(x) + \varepsilon(\alpha(y) + \beta(x)); \tag{54}$$

then $\alpha + \varepsilon\beta$ is $k[\varepsilon]$-linear, and every $k[\varepsilon]$-linear map $V(\varepsilon) \to V(\varepsilon)$ is of this form for unique pair α, β.[4] It follows that

$$\mathrm{GL}_V(k[\varepsilon]) = \{\alpha + \varepsilon\beta \mid \alpha \text{ invertible}\}$$

and that

$$\mathfrak{g}(k) = \{\mathrm{id}_V + \varepsilon\alpha \mid \alpha \in \mathrm{End}(V)\}.$$

Description of $\mathfrak{g}(R)$ in terms of derivations

DEFINITION 3.3 Let A be a k-algebra and M an A-module. A k-linear map $D\colon A \to M$ is a k-***derivation*** of A into M if

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad \text{(Leibniz rule).}$$

The Leibniz rule implies that $D(1) = D(1 \times 1) = D(1) + D(1)$ and so $D(1) = 0$. By k-linearity, this implies that

$$D(c) = 0 \text{ for all } c \in k. \tag{55}$$

Conversely, every additive map $A \to M$ satisfying the Leibniz rule and zero on k is a k-derivation.

Let $\alpha\colon A \to R[\varepsilon]$ be a k-linear map, and write

$$\alpha(f) = \alpha_0(f) + \varepsilon\alpha_1(f), \quad \alpha_0(f), \alpha_1(f) \in R.$$

Then

$$\alpha(fg) = \alpha(f)\alpha(g)$$

if and only if

$$\begin{cases} \alpha_0(fg) &= \alpha_0(f)\alpha_0(g) \\ \alpha_1(fg) &= \alpha_0(f)\alpha_1(g) + \alpha_0(g)\alpha_1(f). \end{cases}$$

The first condition says that α_0 is a k-algebra homomorphism $A \to R$. When we use α_0 to make R into an A-module, the second condition says that α_1 is a k-derivation $A \to R$.

Now let G be an algebraic group, and let $\epsilon\colon \mathcal{O}(G) \to k$ be the neutral element in $G(k)$. By definition, the elements of $\mathfrak{g}(R)$ are the k-algebra homomorphisms $\mathcal{O}(G) \to R[\varepsilon]$ such that the composite

$$\mathcal{O}(G) \xrightarrow{\alpha} k[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} R$$

[4]To see this, note that the k-linear endomorphisms of $V(\varepsilon) = V \oplus \varepsilon V$ are just the 2×2 matrices of k-linear endomorphisms of V, and that ε acts as $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$; the matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ that commute with $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ are exactly those of the form $\left(\begin{smallmatrix} \alpha & 0 \\ \beta & \alpha \end{smallmatrix}\right)$.

is ϵ, i.e., such that $\alpha_0 = \epsilon$. Therefore, according to the above discussion,

$$\mathfrak{g}(R) = \{\epsilon + \varepsilon D \mid D \text{ a derivation}\}. \tag{56}$$

Let $\mathrm{Der}_{k,\epsilon}(\mathcal{O}(G), R)$ be the set k-derivations $\mathcal{O}(G) \to R$ with R regarded as an $\mathcal{O}(G)$-module through ϵ. Let $I = I_G$ be the augmentation ideal of $\mathcal{O}(G)$, defined by the exact sequence

$$0 \to I \to \mathcal{O}(G) \xrightarrow{\epsilon} k \to 0. \tag{57}$$

PROPOSITION 3.4 *There are natural one-to-one correspondences*

$$\mathfrak{g}(R) \leftrightarrow \mathrm{Der}_{k,\epsilon}(\mathcal{O}(G), R) \leftrightarrow \mathrm{Hom}_{k\text{-linear}}(I/I^2, k). \tag{58}$$

PROOF. The first correspondence is given by (56). The Leibniz rule in this case is

$$D(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f). \tag{59}$$

In particular, $D(fg) = 0$ if $f, g \in I$. As $\epsilon(c) = c$ for $c \in k$, the sequence (57) splits: we have a canonical decomposition

$$f \leftrightarrow (\epsilon(f), f - \epsilon(f)) \colon \mathcal{O}(G) = k \oplus I$$

of $\mathcal{O}(G)$ (as a k-vector space). A k-derivation $\mathcal{O}(G) \to R$ is zero on k, and so it is determined by its restriction to I, which can be any k-linear map $I \to R$ that is zero on I^2. □

COROLLARY 3.5 *The set $\mathfrak{g}(R)$ has a canonical structure of an R-module, and*

$$\mathfrak{g}(R) \simeq R \otimes \mathfrak{g}(k).$$

PROOF. Certainly, both statements are true for $\mathrm{Hom}(I/I^2, R)$. □

ASIDE 3.6 Here is a direct description of the action of R on $\mathfrak{g}(R)$: an element $c \in R$ defines a homomorphism of R-algebras

$$u_c \colon R[\varepsilon] \to R[\varepsilon], \quad a + \varepsilon b \mapsto a + c\varepsilon b$$

such that $\pi \circ u_c = \pi$, and hence a commutative diagram

$$\begin{array}{ccc} G(R[\varepsilon]) & \xrightarrow{G(u_c)} & G(R[\varepsilon]) \\ \downarrow{\scriptstyle G(\pi)} & & \downarrow{\scriptstyle G(\pi)} \\ G(R) & \xrightarrow{\mathrm{id}} & G(R), \end{array}$$

which induces a homomorphism of groups $\mathfrak{g}(R) \to \mathfrak{g}(R)$. For example, when $G = \mathrm{GL}_n$,

$$G(u_c)E(A) = G(u_c)(I_n + \varepsilon A) = I_n + c\varepsilon A = E(cA),$$

as expected.

The adjoint map $\mathrm{Ad}\colon G \to \mathrm{Aut}(\mathfrak{g})$

We define

$$\mathrm{Ad}\colon G(R) \to \mathrm{Aut}(\mathfrak{g}(R))$$

by

$$\mathrm{Ad}(g)x = i(g)\cdot x \cdot i(g)^{-1}, \quad g \in G(R), \quad x \in \mathfrak{g}(R) \subset G(R[\varepsilon]).$$

The following formulas hold:

$$\begin{aligned} \mathrm{Ad}(g)(x+x') &= \mathrm{Ad}(g)x + \mathrm{Ad}(g)x', \quad g \in G(R), \quad x,x' \in \mathfrak{g}(R) \\ \mathrm{Ad}(g)(cx) &= c(\mathrm{Ad}(g)x), \quad g \in G(R), \quad c \in R, \quad x \in \mathfrak{g}(R). \end{aligned}$$

The first is clear from the definition of Ad, and the second follows from the description of the action of c in (3.6). Therefore Ad maps into $\mathrm{Aut}_{R\text{-linear}}(\mathfrak{g}(R))$. All the definitions are natural in R, and so we get a representation of G on the vector space $\mathfrak{g}$,

$$\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}. \tag{60}$$

Let $f\colon G \to H$ be a homomorphism of affine groups over k. Because f is a functor,

$$\begin{array}{ccc} G(R[\varepsilon]) & \xrightarrow{\pi} & G(R) \\ \downarrow{\scriptstyle f(R[\varepsilon])} & & \downarrow{\scriptstyle f(R)} \\ H(R[\varepsilon]) & \xrightarrow{\pi} & H(R) \end{array}$$

commutes, and so f induces a homomorphism

$$df\colon \mathfrak{g}(R) \to \mathfrak{h}(R),$$

which is natural in R. Directly from the definitions, one sees that

$$\begin{array}{ccccc} G(R) & \times & \mathfrak{g}(R) & \longrightarrow & \mathfrak{g}(R) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle df} & & \downarrow{\scriptstyle df} \\ H(R) & \times & \mathfrak{h}(R) & \longrightarrow & \mathfrak{h}(R) \end{array} \tag{61}$$

commutes.

Definition of Lie

Let Lie be the functor sending an algebraic group G to the k-vector space

$$\mathfrak{g}(k) \stackrel{\text{def}}{=} \mathrm{Ker}(G(k[\varepsilon]) \to G(k))$$

(see (3.6) for the k-structure). On applying Lie to (60), we get a k-linear map

$$\mathrm{ad}\colon \mathrm{Lie}(G) \to \mathrm{End}(\mathfrak{g}).$$

For $a, x \in \mathfrak{g}(k)$, we define

$$[a,x] = \mathrm{ad}(a)(x).$$

LEMMA 3.7 *For* GL_n, *the construction gives*

$$[A,X] = AX - XA.$$

PROOF. An element $I+\varepsilon A \in \mathrm{Lie}(\mathrm{GL}_n)$ acts on $M_n(k[\varepsilon])$ as

$$X + \varepsilon Y \mapsto (I+\varepsilon A)(X+\varepsilon Y)(I-\varepsilon A) = X + \varepsilon Y + \varepsilon(AX - XA).$$

On comparing this with (54), we see that $\mathrm{ad}(A)$ acts as $\mathrm{id} + \varepsilon u$ where $u(X) = AX - XA$. □

It follows from (61) that 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. Because the bracket on $\mathrm{Lie}(\mathrm{GL}_n)$ makes it into a Lie algebra, and every algebraic group G can be embedded in GL_n (2.3), the bracket on $\mathrm{Lie}(G)$ makes into a Lie algebra. We have proved the following statement.

THEOREM 3.8 *There is a unique functor* Lie *from the category of algebraic groups over* k *to the category of Lie algebras such that:*

(a) $\mathrm{Lie}(G) = \mathfrak{g}(k)$ *as a* k*-vector space, and*
(b) *the bracket on* $\mathrm{Lie}(\mathrm{GL}_n) = \mathfrak{gl}_n$ *is* $[X,Y] = XY - YX$.

The action of G *on itself by conjugation defines a representation* $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$ *of* G *on* $\mathfrak{g}$ *(as a* k*-vector space), whose differential is the adjoint representation* $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ *of (I, 1.11).*

Clearly

$$\mathrm{Lie}(G_K) \simeq K \otimes \mathrm{Lie}(G) \tag{62}$$

for any field K containing k.

Examples

3.9 (Special linear group) By definition

$$\mathrm{Lie}(\mathrm{SL}_n) = \{I + A\varepsilon \in M_n(k[\varepsilon]) \mid \det(I + A\varepsilon) = 1\}.$$

When we expand $\det(I+\varepsilon A)$ as a sum of $n!$ products, the only nonzero term is

$$\textstyle\prod_{i=1}^{n}(1+\varepsilon a_{ii}) = 1 + \varepsilon\sum_{i=1}^{n} a_{ii},$$

because every other term includes at least two off-diagonal entries. Hence

$$\det(I+\varepsilon A) = 1 + \varepsilon\,\mathrm{trace}(A)$$

and so

$$\begin{aligned}\mathrm{Lie}(\mathrm{SL}_n) &= \{I+\varepsilon A \mid \mathrm{trace}(A) = 0\}\\ &\simeq \mathfrak{sl}_n.\end{aligned}$$

3.10 Let C be an invertible $n\times n$ matrix, and let G be the algebraic group such that $G(R)$ consists of the matrices A such that $A^tCA=C$ (see 1.20). Then $\mathrm{Lie}(G)$ consists of the matrices $I+\varepsilon A\in M_n(k[\varepsilon])$ such that

$$(I+\varepsilon A)^t\cdot C\cdot (I+\varepsilon A)=C,$$

i.e., such that

$$A^t\cdot C+C\cdot A=0.$$

For example, if $C=I$, then $G=\mathrm{O}_n$ and

$$\begin{aligned}\mathrm{Lie}(\mathrm{O}_n)&=\{I+\varepsilon A\in M_n(k[\varepsilon])\mid A^t+A=0\}\\&\simeq \mathfrak{o}_n.\end{aligned}$$

If $C=\left(\begin{smallmatrix}0&I\\-I&0\end{smallmatrix}\right)$, then $G=\mathrm{Sp}_n$, and

$$\begin{aligned}\mathrm{Lie}(\mathrm{Sp}_n)&=\{I+\varepsilon A\in M_n(k[\varepsilon])\mid A^tC+CA=0\}\\&\simeq \mathfrak{sp}_n.\end{aligned}$$

3.11 Let V be a finite-dimensional vector space over k, and let

$$\beta\colon V\times V\to k$$

be a nondegenerate k-bilinear form. If β is symmetric or alternating, then

$$R\rightsquigarrow\{\alpha\in\mathrm{GL}(V_R)\mid \beta(\alpha v,\alpha v')=\beta(v,v')\}$$

is an algebraic group. Its Lie algebra is

$$\mathfrak{g}=\left\{x\in\mathfrak{gl}_V\mid \beta(xv,v')+\beta(v,xv')\right\}=0$$

(see 1.7).

3.12 Let $\mathbb{T}_n$ be the algebraic group $R\rightsquigarrow\mathbb{T}_n(R)$ where $\mathbb{T}_n(R)$ is the group of invertible upper triangular $n\times n$ matrices with entries in R. Then

$$\mathrm{Lie}(\mathbb{T}_n)=\left\{\begin{pmatrix}1+\varepsilon c_{11}&\varepsilon c_{12}&\cdots&\varepsilon c_{1\,n-1}&\varepsilon c_{1\,n}\\0&1+\varepsilon c_{22}&\cdots&\varepsilon c_{2\,n-1}&\varepsilon c_{2\,n}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1+\varepsilon c_{n-1\,n-1}&\varepsilon c_{n-1\,n}\\0&0&\cdots&0&1+\varepsilon c_{n\,n}\end{pmatrix}\right\},$$

and so

$$\mathrm{Lie}(\mathbb{T}_n)\simeq\mathfrak{b}_n\quad\text{(upper triangular matrices).}$$

Let $\mathbb{U}_n$ be the algebraic group $R\rightsquigarrow\mathbb{U}_n(R)$ where $\mathbb{U}_n(R)$ is the group of upper triangular $n\times n$ matrices having only 1's on the diagonal. Then

$$\mathrm{Lie}(\mathbb{U}_n)\simeq\mathfrak{n}_n\quad\text{(strictly upper triangular matrices).}$$

Finally, let $\mathbb{D}_n$ be the algebraic group $R\rightsquigarrow\mathbb{D}_n(R)$ where $\mathbb{D}_n(R)$ is the group of invertible diagonal $n\times n$ matrices with entries in R. Then

$$\mathrm{Lie}(\mathbb{D}_n)\simeq\mathfrak{d}_n\quad\text{(diagonal matrices).}$$

Description of Lie(G) *in terms of derivations*

Let A be a k-algebra, and consider the space $\mathrm{Der}_k(A)$ of k-derivations of A into A, as in (1.10), so that the Leibniz rule is

$$D(fg) = f \cdot D(g) + D(f) \cdot g.$$

The bracket

$$[D, D'] \overset{\text{def}}{=} D \circ D' - D' \circ D$$

of two derivations is again a derivation. In this way $\mathrm{Der}_k(A)$ becomes a Lie algebra.

Let G be an algebraic group. A derivation $D\colon \mathcal{O}(G) \to \mathcal{O}(G)$ is said to be ***left invariant***[5] if

$$\Delta \circ D = (\mathrm{id} \otimes D) \circ \Delta. \tag{63}$$

If D and D' are left invariant, then

$$\Delta \circ (D \circ D') = (\mathrm{id} \otimes D) \circ \Delta \circ D' = (\mathrm{id} \otimes D \circ D') \circ \Delta,$$

and so

$$\begin{aligned} \Delta \circ [D, D'] &= \Delta \circ (D \circ D' - D' \circ D) \\ &= (\mathrm{id} \otimes (D \circ D') - \mathrm{id} \otimes (D' \circ D)) \circ \Delta \\ &= (\mathrm{id} \otimes [D, D']) \circ \Delta. \end{aligned}$$

Therefore $[D, D']$ is left invariant, and so the left invariant derivations form a Lie subalgebra of $\mathrm{Der}_k(\mathcal{O}(G))$.

PROPOSITION 3.13 *The map*

$$D \mapsto \epsilon \circ D\colon \mathrm{Der}_k(\mathcal{O}(G)) \to \mathrm{Der}_k(\mathcal{O}(G), k)$$

defines an isomorphism from the space of left invariant derivations onto $\mathrm{Der}_k(\mathcal{O}(G), k)$.

PROOF. For homomorphisms $f\colon A \to R$ and $g\colon B \to R$ of k-algebras, we write (f, g) for the homomorphism $a \otimes b \mapsto f(a)g(b)\colon A \otimes B \to R$. The fact that m is associative translates into the equality

$$(\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta \tag{64}$$

and that ϵ is the neutral element into the equalities

$$(\mathrm{id}, \epsilon) \circ \Delta = \mathrm{id} = (\epsilon, \mathrm{id}) \circ \Delta. \tag{65}$$

To prove the proposition, we prove the following two statements:

(a) If d is an ϵ-derivation $\mathcal{O}(G) \to k$, then $D = (\mathrm{id}, d) \circ \Delta$ is a left invariant derivation $\mathcal{O}(G) \to \mathcal{O}(G)$; moreover $\epsilon \circ D = d$ (here $\mathrm{id} = \mathrm{id}_{\mathcal{O}(G)}$).

(b) If D is a left invariant derivation $\mathcal{O}(G) \to \mathcal{O}(G)$, then

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

[5] In geometric terms, a derivation D defines a tangent vector t_P at each point of $|G|$, and to say that D is left invariant means that the family (t_P) is invariant under left translations.

In combination, these statements say that $D \mapsto \epsilon \circ D$ and $d \mapsto (\mathrm{id}, d) \circ \Delta$ are inverse bijections.

We first prove (a). Let $D = (\mathrm{id}, d) \circ \Delta$. To show that D is a derivation, we have to show that, for $a, a' \in \mathcal{O}(G)$,

$$D(aa') = aD(a') + D(a)a'.$$

This can be checked by writing $\Delta(a) = \sum b_i \otimes c_i$ and $\Delta(a') = \sum b_i' \otimes c_i'$ and expanding both sides.

We next show that D is left invariant. Obviously

$$\mathrm{id} \otimes D = (\mathrm{id} \otimes (\mathrm{id}, d)) \circ (\mathrm{id} \otimes \Delta).$$

On the other hand, a direct calculation shows that

$$\Delta \circ D = (\mathrm{id} \otimes (\mathrm{id}, d)) \circ (\Delta \otimes \mathrm{id}) \circ \Delta$$

(evaluate both sides on $a \in \mathcal{O}(G)$ by writing $\Delta(a) = \sum b_i \otimes c_i$). Now the equality

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

follows from (64).

The final statement of (a), that $\epsilon \circ D = d$, is left to the reader to check.

We now prove (b):

$$D \overset{(65)}{=} (\mathrm{id}, \epsilon) \circ \Delta \circ D \overset{(63)}{=} (\mathrm{id}, \epsilon) \circ (\mathrm{id} \otimes D) \circ \Delta = (\mathrm{id}, (\epsilon \circ D)) \circ \Delta.$$ □

Thus, $\mathrm{Lie}(G)$ is isomorphic (as a k-vector space) to the space of left invariant derivations $\mathcal{O}(G) \to \mathcal{O}(G)$, which is a Lie subalgebra of $\mathrm{Der}_k(\mathcal{O}(G))$. In this way, $\mathrm{Lie}(G)$ acquires a Lie algebra structure. As the construction is functorial in G, the next exercise shows that this Lie algebra structure agrees with that defined earlier.

EXERCISE 3.14 Show that, when $G = \mathrm{GL}_n$, this construction gives the bracket $[A, B] = AB - BA$.

ASIDE 3.15 Let M be a smooth manifold (i.e., a C^∞ real manifold). The smooth differential operators on M form an associative algebra over $\mathbb{R}$, and hence, as in (1.4), define a Lie algebra. The bracket of two smooth vector fields on M is again a smooth vector field, and hence the smooth vector fields on M form a Lie algebra $\mathfrak{m}$. If M is a Lie group, i.e., has a smooth group structure, then the left invariant vector fields form a Lie subalgebra of $\mathfrak{m}$, called the Lie algebra of M. As in the case of an algebraic group, it is canonically isomorphic to the tangent space to the M at the identity element. See Chapter III.

NOTES The definitions in this subsection work equally well for affine groups, i.e., we don't use that $\mathcal{O}(G)$ is finitely generated. We need affine groups in the remaining sections.

Properties of the functor Lie

PROPOSITION 3.16 *For an algebraic group G, $\dim \mathrm{Lie}(G) = \dim G$. In particular, G is finite if and only if $\mathrm{Lie}(G) = 0$.*

PROOF. Because $\mathrm{Lie}(G_{k^{\mathrm{al}}}) \simeq \mathrm{Lie}(G) \otimes_k k^{\mathrm{al}}$ (see 62), we may suppose $k = k^{\mathrm{al}}$. Now $\mathrm{Lie}(G)$ is the tangent space to G at e, and so $\dim \mathrm{Lie}(G) \geq \dim G$, with equality if and only if G is smooth at e. But we know that G is smooth (1.7), and so equality holds. □

EXAMPLE 3.17 Proposition 3.16 is very useful for computing the dimensions of algebraic groups. For example,

$$\dim \mathrm{Lie}\, \mathbb{G}_a = 1 = \dim \mathbb{G}_a$$
$$\dim \mathrm{Lie}\, \mathrm{SL}_n = n^2 - 1 = \dim \mathrm{SL}_n .$$

PROPOSITION 3.18 *Let H be an algebraic subgroup of an algebraic group G; then $H^\circ = G^\circ$ if and only if* $\mathrm{Lie}\, H = \mathrm{Lie}\, G$.

PROOF. Clearly, the Lie algebra of an algebraic group depends only on its identity component, and so $\mathrm{Lie}(H) = \mathrm{Lie}(G)$ if $H^\circ = G^\circ$. Conversely, if $\mathrm{Lie}(H) = \mathrm{Lie}(G)$, then $\dim H^\circ = \dim G^\circ$ and, as G° is irreducible, this implies that $H^\circ = G^\circ$. □

The functor Lie commutes with fibre products.

PROPOSITION 3.19 *For any homomorphisms $G \to H \leftarrow G'$ of algebraic groups,*

$$\mathrm{Lie}(G \times_H G') \simeq \mathrm{Lie}(G) \times_{\mathrm{Lie}(H)} \mathrm{Lie}(G'). \tag{66}$$

PROOF. By definition,

$$\left(G \times_H G'\right)(R) = G(R) \times_{H(R)} G'(R).$$

Therefore,

$$\mathrm{Lie}(G \times_H G') = \mathrm{Ker}\left(G(k[\varepsilon]) \times_{H(k[\varepsilon])} G'(k[\varepsilon]) \to G(k) \times_{H(k)} G'(k)\right).$$

In other words, $\mathrm{Lie}(G \times_H G')$ consists of the pairs

$$(g, g') \in G(k[\varepsilon]) \times G'(k[\varepsilon])$$

such that g maps to 1 in $G(k)$, g' maps to 1 in $G'(k)$, and g and g' have the same image in $H(k[\varepsilon])$. Hence $\mathrm{Lie}(G \times_H G')$ consists of the pairs

$$(g, g') \in \mathrm{Ker}(G(k[\varepsilon]) \to G(k)) \times \mathrm{Ker}\left(G'(k[\varepsilon]) \to G'(k)\right)$$

having the same image in $H(k[\varepsilon])$. This set is $\mathrm{Lie}(G) \times_{\mathrm{Lie}(H)} \mathrm{Lie}(G')$. □

COROLLARY 3.20 *If H_1 and H_2 are algebraic subgroups of an algebraic group G, then* $\mathrm{Lie}(H_1)$ *and* $\mathrm{Lie}(H_2)$ *are Lie subalgebras of* $\mathrm{Lie}(G)$*, and*

$$\mathrm{Lie}(H_1 \cap H_2) = \mathrm{Lie}(H_1) \cap \mathrm{Lie}(H_2) \quad (\textit{inside } \mathrm{Lie}(G)).$$

More generally,

$$\mathrm{Lie}\left(\bigcap\nolimits_{i \in I} H_i\right) = \bigcap\nolimits_{i \in I} \mathrm{Lie}\, H_i \quad (\textit{inside } \mathrm{Lie}(G)) \tag{67}$$

for any family of algebraic subgroups H_i of G.

PROOF. Recall that $H_1 \cap H_2$ represents the functor $R \rightsquigarrow H_1(R) \cap H_1(R)$. Therefore

$$H_1 \cap H_2 \simeq H_1 \times_G H_2,$$

and so the statement follows from (3.19). □

COROLLARY 3.21 *For any homomorphism $u\colon G \to H$,*

$$\mathrm{Lie}(\mathrm{Ker}(u)) = \mathrm{Ker}(\mathrm{Lie}(u)).$$

In other words, an exact sequence of algebraic groups $1 \to N \to G \to Q$ gives rise to an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}\, N \to \mathrm{Lie}\, G \to \mathrm{Lie}\, Q.$$

PROOF. As the kernel can be obtained as a fibred product,

$$\begin{array}{ccc} \mathrm{Ker}(u) & \longrightarrow & * \\ \downarrow & & \downarrow \\ G & \longrightarrow & H, \end{array}$$

this follows from (3.19). □

PROPOSITION 3.22 *Let G be a connected algebraic group. 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 3.20)

$$\mathrm{Lie}(H \cap H') = \mathrm{Lie}(H) \cap \mathrm{Lie}\, H').$$

If $\mathrm{Lie}(H) = \mathrm{Lie}(H')$, then

$$\mathrm{Lie}(H) = \mathrm{Lie}(H \cap H') = \mathrm{Lie}(H'),$$

and so (3.18) shows that

$$H = \left(H \cap H'\right)^{\circ} = H'.$$

□

3.23 A Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$ is said to be ***algebraic***[6] if it is the Lie algebra of an algebraic subgroup of GL_V. A necessary condition for this is that $\mathfrak{g}$ contain the semisimple and nilpotents parts of each of its elements — a subalgebra satisfying this condition is said to be ***almost algebraic***.[7] A sufficient condition is that $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$ (see later).

[6] The name is due to Chevalley.

[7] The concept is due to Malcev, but the name to Jacobson (Lie Algebras, p.98).

3.24 According to (2.3), every algebraic group over k can be realized as a subgroup of GL_n for some n, and, according to (3.22), the algebraic subgroups of GL_n are in one-to-one correspondence with the algebraic Lie subalgebras of $\mathfrak{gl}_n$. This suggests two questions: find an algorithm to decide whether a Lie subalgebra of $\mathfrak{gl}_n$ is algebraic (i.e., arises from an algebraic subgroup); given an algebraic Lie subalgebra of $\mathfrak{gl}_n$, find an algorithm to construct the group. For a recent discussion of these questions, see, de Graaf, Willem, A. Constructing algebraic groups from their Lie algebras. J. Symbolic Comput. 44 (2009), no. 9, 1223–1233.[8]

PROPOSITION 3.25 *Let $u\colon G \to H$ be a homomorphism of algebraic groups. Then $u(G^{\circ}) \supset H^{\circ}$ if and only if* $\operatorname{Lie} G \to \operatorname{Lie} H$ *is surjective.*

PROOF. We may replace G and H with their neutral components. We know (1.5) that $G \to H$ factors into

$$G \xrightarrow{\text{surjective}} \bar{G} \xrightarrow{\text{injective}} H.$$

Correspondingly, $\operatorname{Lie}(u)$ factors into

$$\operatorname{Lie}(G) \longrightarrow \operatorname{Lie}(\bar{G}) \xrightarrow{\text{injective}} \operatorname{Lie}(H).$$

Clearly $\operatorname{Lie}(G) \to \operatorname{Lie}(H)$ is surjective if and only if $\operatorname{Lie}(\bar{G}) \to \operatorname{Lie}(H)$ is an isomorphism, which is true if and only if $\bar{G} = H$ (3.18). □

PROPOSITION 3.26 *Let $u, v\colon G \to H$ be homomorphisms of algebraic groups; then u and v agree on G° if and only if* $\operatorname{Lie}(u) = \operatorname{Lie}(v)$.

PROOF. We may replace G with its neutral component. Let Δ denote the diagonal in $G \times G$ — it is an algebraic subgroup of $G \times G$ isomorphic to G. The homomorphisms u and v agree on the algebraic group

$$G' \stackrel{\text{def}}{=} \Delta \cap G \times_H G.$$

The hypothesis implies $\operatorname{Lie}(G') = \operatorname{Lie}(\Delta)$, and so $G' = \Delta$. □

3.27 Thus the functor Lie is faithful on connected algebraic groups, but it is not full. For example

$$\operatorname{End}(\mathbb{G}_m) = \mathbb{Z} \subsetneq k = \operatorname{End}(\operatorname{Lie}(\mathbb{G}_m)).$$

For another example, let k be an algebraically closed field of characteristic zero, and let $G = \mathbb{G}_a \rtimes \mathbb{G}_m$ with the product $(a,u)(b,v) = (a+ub, uv)$. Then

$$\operatorname{Lie}(G) = \operatorname{Lie}(\mathbb{G}_a) \times \operatorname{Lie}(\mathbb{G}_m) = ky + kx$$

with $[x,y] = y$. The Lie algebra morphism $\operatorname{Lie}(G) \to \operatorname{Lie}(\mathbb{G}_a)$ such that $x \mapsto y$, $y \mapsto 0$ is surjective, but it is not the differential of a homomorphism of algebraic groups because there is no nonzero homomorphism $\mathbb{G}_m \to \mathbb{G}_a$.

[8] de Graaf (ibid.) and his MR reviewer write: "A connected algebraic group in characteristic 0 is uniquely determined by its Lie algebra." This is obviously false — consider SL_2 and its quotient by $\{\pm I\}$, or the examples in (3.28). What they mean (but didn't say) is that a connected algebraic subgroup of GL_n in characteristic zero is uniquely determined by its Lie algebra as a subalgebra of $\mathfrak{gl}_n$.

3.28 Even in characteristic zero, infinitely many nonisomorphic connected algebraic groups can have the same Lie algebra. For example, let $\mathfrak{g}$ be the two-dimensional Lie algebra $\langle x, y \mid [x, y] = y\rangle$, and, for each nonzero $n \in \mathbb{N}$, let G_n be the semidirect product $\mathbb{G}_a \rtimes \mathbb{G}_m$ defined by the action $(t,a) \mapsto t^n a$ of $\mathbb{G}_m$ on $\mathbb{G}_a$. Then $\mathrm{Lie}(G_n) = \mathfrak{g}$ for all n, but no two groups G_n are isomorphic. (Indeed, the centre of G_n is $\{(0,\zeta) \mid \zeta^n = 1\} \simeq \mu_n$, but the isogeny $(a,u) \mapsto (a,u^n)\colon G_n \to G_1$ defines an isomorphism $\mathrm{Lie}(G_n) \to \mathrm{Lie}(G_1)$.)

PROPOSITION 3.29 *If*

$$1 \to N \to G \to Q \to 1$$

is exact, then

$$0 \to \mathrm{Lie}(N) \to \mathrm{Lie}(G) \to \mathrm{Lie}(Q) \to 0$$

is exact. In particular,

$$\dim G = \dim N + \dim Q.$$

PROOF. The sequence $0 \to \mathrm{Lie}(N) \to \mathrm{Lie}(G) \to \mathrm{Lie}(Q)$ is exact (by 3.21), and the surjectivity of $\mathrm{Lie}(G) \to \mathrm{Lie}(Q)$ follows from (3.25). □

An ***isogeny*** of algebraic groups is a surjective homomorphism with finite kernel.

COROLLARY 3.30 *A homomorphism $G \to H$ of connected affine algebraic groups is an isogeny if and only if* $\mathrm{Lie}(G) \to \mathrm{Lie}(H)$ *is an isomorphism.*

PROOF. Apply (3.25), (3.29), and 3.16). □

THEOREM 3.31 *Let H be an algebraic subgroup of an algebraic group G. The functor of k-algebras*

$$R \rightsquigarrow N_G(H)(R) \stackrel{\text{def}}{=} \{g \in G(R) \mid g \cdot H(S) \cdot g^{-1} = H(S) \text{ all } R\text{-algebras } S\}$$

is an algebraic subgroup of G. If H is connected, then

$$\mathrm{Lie}(N_G(H)) = n_{\mathfrak{g}}(\mathfrak{h}) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid [x, \mathfrak{h}] \subset \mathfrak{h}\};$$

consequently, H is normal in G if and only if $\mathfrak{h}$ is an ideal in $\mathfrak{g}$.

PROOF. That $N_G(H)$ is an algebraic subgroup of G is proved in AGS VII, 6.1. For the second statement, we may suppose that k is algebraically closed. Then the equality $\mathrm{Lie}(N_G(H)) = n_{\mathfrak{g}}(\mathfrak{h})$ follows directly from the definitions. For the last statement,

$$\begin{aligned} H \text{ is normal in } G &\iff N_G(H) = G \\ &\iff \mathrm{Lie}(N_G(H)) = \mathrm{Lie}(G) \\ &\iff n_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g} \\ &\iff \mathfrak{h} \text{ is an ideal in } \mathfrak{g}. \end{aligned}$$

Alternatively, if H is normal, then it is the kernel of a homomorphism $G \to Q$, in which case $\mathfrak{h}$ is the kernel of $\mathfrak{g} \to \mathfrak{q}$. □

THEOREM 3.32 *Let H be an algebraic subgroup of an algebraic group G. The functor of k-algebras*

$$R \rightsquigarrow C_G(H)(R) \stackrel{\text{def}}{=} \{g \in G(R) \mid g \cdot h = h \cdot g \text{ all } R\text{-algebra } S \text{ and all } h \in G(S)\}$$

is an algebraic subgroup of G. If H is connected, then

$$\mathrm{Lie}(C_G(H)) = c_{\mathfrak{g}}(\mathfrak{h}) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid [x, \mathfrak{h}] = 0\};$$

consequently, H is contained in the centre of G if and only if $\mathfrak{h}$ is contained in the centre of $\mathfrak{g}$.

PROOF. That $C_G(H)$ is an algebraic subgroup of G is proved in AGS VII, 6.7. For the second statement, we may suppose that k is algebraically closed. Then the equality $\mathrm{Lie}(C_G(H)) = c_{\mathfrak{g}}(\mathfrak{h})$ follows directly from the definitions. For the last statement,

$$\begin{aligned} H \subset Z(G) &\iff C_G(H) = G \\ &\iff \mathrm{Lie}(C_G(H)) = \mathrm{Lie}(G) \\ &\iff c_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g} \\ &\iff \mathfrak{h} \subset z(\mathfrak{g}). \end{aligned}$$

□

COROLLARY 3.33 *For an algebraic group G,*

$$\mathrm{Lie}(ZG) \subset z(\mathfrak{g}),$$

with equality if G is connected.

PROOF. Clearly, $(ZG)^{\circ} = ZG \cap G^{\circ} \subset Z(G^{\circ})$, and so

$$\mathrm{Lie}(ZG) \subset \mathrm{Lie}(Z(G^{\circ})),$$

with equality if $G = G^{\circ}$. But $Z(G^{\circ}) = C_{G^{\circ}}(G^{\circ})$ and $z(\mathfrak{g}) = c_{\mathfrak{g}}(\mathfrak{g})$, and so

$$\mathrm{Lie}(Z(G^{\circ})) = z(\mathfrak{g}).$$

□

COROLLARY 3.34 *A connected algebraic group commutative if and only if its Lie algebra is commutative.*

PROOF. Let G be a connected algebraic group. Then

$$\begin{aligned} G \text{ is commutative} &\iff Z(G) = G \\ &\iff \mathrm{Lie}(Z(G)) = \mathrm{Lie}(G) \\ &\iff z(\mathfrak{g}) = \mathfrak{g} \\ &\iff \mathfrak{g} \text{ is commutative.} \end{aligned}$$

□

COROLLARY 3.35 *Let G be a connected algebraic group. Then $\mathrm{Lie}(\mathcal{D}G) = \mathcal{D}(\mathrm{Lie}(G))$.*

PROOF. Let H be a connected algebraic subgroup of G. Then $H \supset \mathcal{D}G \iff H$ is normal and G/H is commutative $\iff$ $\mathrm{Lie}(H)$ is an ideal and $\mathrm{Lie}(G)/\mathrm{Lie}(H)$ is commutative $\iff$ $\mathrm{Lie}(H) \supset \mathcal{D}\mathrm{Lie}(G)$. □

COROLLARY 3.36 *For a connected algebraic group G, the connected kernel of* $\mathrm{Ad}\colon G \to \mathrm{Aut}(\mathfrak{g})$ *is the centre of G.*

PROOF. When we apply Lie to Ad, we get $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$, which has kernel $z(\mathfrak{g})$. □

3.37 A character $\chi\colon G \to \mathbb{G}_m$ of G defines a linear form $\mathrm{Lie}(\chi)\colon \mathrm{Lie}(G) \to k$ on its Lie algebra. When G is diagonalizable, this induces an isomorphism $X^*(G) \otimes_{\mathbb{Z}} k \to \mathrm{Lie}(G)^{\vee}$.

NOTES Statement (3.35) is false for algebraic supergroups (arXiv:1302.5648).

Representations

Recall that a representation of a Lie algebra $\mathfrak{g}$ on a k-vector space V is a homomorphism $\rho\colon \mathfrak{g} \to \mathfrak{gl}_V$. Thus ρ sends $x \in \mathfrak{g}$ to a k-linear endomorphism $\rho(x)$ of V, and

$$\rho([x,y]) = \rho(x)\rho(y) - \rho(y)\rho(x).$$

When we regard V as a $\mathfrak{g}$-module and write xv for $\rho(x)(v)$, this becomes

$$[x,y]v = x(yv) - y(xv). \tag{68}$$

Let W be a subspace of V. The stabilizer of W in $\mathfrak{g}$ is

$$\mathfrak{g}_W \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xW \subset W\}.$$

It is clear from (68) that $\mathfrak{g}_W$ is a Lie subalgebra of $\mathfrak{g}$. Let $v \in V$. The isotropy algebra of v in $\mathfrak{g}$ is

$$\mathfrak{g}_v \overset{\text{def}}{=} \{x \in \mathfrak{g} \mid xv = 0\}.$$

It is a Lie subalgebra of $\mathfrak{g}$.

PROPOSITION 3.38 *For any representation $G \to \mathrm{GL}_V$ and subspace $W \subset V$,*

$$\mathrm{Lie}\, G_W = (\mathrm{Lie}\, G)_W.$$

PROOF. By definition, $\mathrm{Lie}\, G_W$ consists of the elements $\mathrm{id} + \varepsilon u$ of $G(k[\varepsilon])$, $u \in \mathrm{End}(V)$, such that

$$(\mathrm{id} + \varepsilon u)(W + \varepsilon W) \subset W + \varepsilon W,$$

(cf. 3.2), i.e., such that $u(W) \subset W$. □

COROLLARY 3.39 *If W is stable under G, then it is stable under* $\mathrm{Lie}(G)$, *and the converse is true when G is connected.*

PROOF. To say that W is stable under G means that $G = G_W$, but if $G = G_W$, then $\operatorname{Lie} G = \operatorname{Lie} G_W = (\operatorname{Lie} G)_W$, which means that W is stable under $\operatorname{Lie} G$. Conversely, to say that W is stable under $\operatorname{Lie} G$, means that $\operatorname{Lie} G = (\operatorname{Lie} G)_W$. But if $\operatorname{Lie} G = (\operatorname{Lie} G)_W$, then $\operatorname{Lie} G = \operatorname{Lie} G_W$, which implies that $G_W = G$ when G is connected (3.18). □

Let ρ_1 and ρ_2 be representations of $\mathfrak{g}$ on V_1 and V_2 respectively; then $\rho_1 \otimes \rho_2$ is the representation of $\mathfrak{g}$ on $V_1 \otimes V_2$ such that

$$(\rho_1 \otimes \rho_2)(v_1 \otimes v_2) = \rho_1(v_1) \otimes v_2 + v_1 \otimes \rho_2(v_2), \text{ all } v_1 \in V_1,\ v_2 \in V_2.$$

Let ρ be a representation of $\mathfrak{g}$ on V; then $\rho^\vee$ is the representation of $\mathfrak{g}$ on $V^\vee$ such that

$$(\rho^\vee(x)f)(v) = f(v) - f(\rho(x)v), \quad x \in \mathfrak{g},\ f \in V^\vee,\ v \in V.$$

The representations of $\mathfrak{g}$ on finite-dimensional vector spaces form a neutral tannakian category $\mathsf{Rep}(\mathfrak{g})$ over k, with the forgetful functor as a fibre functor.

On applying Lie to a representation $r\colon G \to \mathrm{GL}_V$ of an algebraic group G, we get a representation

$$\operatorname{Lie}(r)\colon \operatorname{Lie}(G) \to \mathfrak{gl}_V$$

of $\operatorname{Lie}(G)$ (sometimes denoted $dr\colon \mathfrak{g} \to \mathfrak{gl}_V$).

PROPOSITION 3.40 *Let $r\colon G \to \mathrm{GL}_V$ be a representation of an algebraic group G, and let $W' \subset W$ be subspaces of V. There exists an algebraic subgroup $G_{W',W}$ of G such that $G_{W',W}(R)$ consists of the elements of $\mathrm{GL}(V(R))$ stabilizing each of $W'(R)$ and $W(R)$ and acting as the identity on the quotient $W(R)/W'(R)$; its Lie algebra is*

$$\operatorname{Lie}(G_{W',W}) = \mathfrak{g}_{W',W} \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid \operatorname{Lie}(r)(x) \text{ maps } W \text{ into } W'\}.$$

PROOF. Clearly,

$$G_{W',W} = \operatorname{Ker}((G_{W'} \cap G_W) \to \mathrm{GL}_{W/W'}).$$

On applying the functor Lie to this equality, and using 3.20, 3.21, and 3.38, we find that

$$\operatorname{Lie}(G_{W',W}) = \operatorname{Ker}(\mathfrak{g}_{W'} \cap \mathfrak{g}_W \to \mathfrak{gl}_{W/W'}),$$

which equals $\mathfrak{g}_{W',W}$. □

Applied to a subspace W of V and the subgroups

$$N_G(W) = G_{W,W} = (R \rightsquigarrow \{g \in G(R) \mid gW(R) \subset W(R)\})$$
$$C_G(W) = G_{\{0\},W} = (R \rightsquigarrow g \in G(R) \mid gx = x \text{ for all } x \in W(R)\})$$

of G, (3.40) shows that

$$\operatorname{Lie}(N_G(W)) = n_{\mathfrak{g}}(W) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid x(W) \subset W\} \tag{69}$$

$$\operatorname{Lie}(C_G(W)) = c_{\mathfrak{g}}(W) \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid x(W) = 0\}. \tag{70}$$

Assume that G is connected. Then W is stable under G (i.e., $N_G(W) = G$) if and only if it is stable under $\mathfrak{g}$, and its elements are fixed by G if and only if they are fixed (i.e., killed) by $\mathfrak{g}$. It follows that V is simple or semisimple as a representation of G if and only if it is so as a representation of $\operatorname{Lie}(G)$.

PROPOSITION 3.41 *Let G be an algebraic group with Lie algebra $\mathfrak{g}$. If G is connected, then the functor* $\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g})$ *is fully faithful.*

PROOF. Let V and W be representations of G. Let α be a k-linear map $V \to W$, and let β be the element of $V^\vee \otimes W$ corresponding to α under the isomorphism $\mathrm{Hom}_{k\text{-linear}}(V,W) \simeq V^\vee \otimes_k W$. Then α is a homomorphism of representations of G if and only if β is fixed by G. Since a similar statement holds for $\mathfrak{g}$, the claim follows from (70) applied to the subspace W spanned by β. □

In fact, $r \rightsquigarrow dr$ is a fully faithful, exact, tensor functor

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}).$$

Let $G^{\mathfrak{g}}$ be the Tannaka dual of $\mathsf{Rep}(\mathfrak{g})$. Then we get a canonical homomorphism

$$G \to G^{\mathfrak{g}}$$

of affine groups over k.

Algebraic Lie algebras

A Lie algebra is said to be ***algebraic*** if it is the Lie algebra of an affine algebraic group. A sum of algebraic Lie algebras is algebraic. Let $\mathfrak{g} = \mathrm{Lie}(G)$, and let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$. The intersection of the algebraic Lie subalgebras of $\mathfrak{g}$ containing $\mathfrak{h}$ is again algebraic (see 3.20) — it is called the ***algebraic envelope*** or ***hull*** of $\mathfrak{h}$.

Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{gl}_V$. A necessary condition for $\mathfrak{h}$ to be algebraic is that the semisimple and nilpotent components of each element of $\mathfrak{h}$ (as an endomorphism of $\mathfrak{gl}_V$) lie in $\mathfrak{h}$. However, this condition is not sufficient, even in characteristic zero.

Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{gl}_V$ over a field k of characteristic zero. We explain how to determine the algebraic hull of $\mathfrak{h}$. For any $X \in \mathfrak{h}$, let $\mathfrak{g}(X)$ be the algebraic hull of the Lie algebra spanned by X. Then the algebraic hull of $\mathfrak{h}$ is the Lie subalgebra of $\mathfrak{gl}_V$ generated by the $\mathfrak{g}(X)$, $X \in \mathfrak{h}$. In particular, $\mathfrak{h}$ is algebraic if and only if each X is contained in an algebraic Lie subalgebra of $\mathfrak{h}$. Write X as the sum $S+N$ of its semisimple and nilpotent components. Then $\mathfrak{g}(N)$ is spanned by N, and so it remains to determine $\mathfrak{g}(X)$ when X is semisimple. For some finite extension L of k, there exists a basis of $L \otimes V$ for which the matrix of X is $\mathrm{diag}(u_1,\ldots,u_n)$. Let W be the subspace $M_n(L)$ consisting of the matrices $\mathrm{diag}(a_1,\ldots,a_n)$ such that

$$\sum\nolimits_i c_i u_i = 0,\ c_i \in L \implies \sum\nolimits_i c_i a_i = 0,$$

i.e., such that the a_i satisfy every linear relation over L that the u_i do. Then the map

$$\mathfrak{gl}_V \to L \otimes \mathfrak{gl}_V \simeq M_n(L)$$

induces maps

$$\mathfrak{g}(X) \to L \otimes \mathfrak{g}(X) \simeq W,$$

which determine $L \otimes \mathfrak{g}(X)$. See Chevalley 1951 (also Fieker and de Graaf 2007 where it is explained how to implement this as an algorithm).

3.42 See (1.25) for a five-dimensional solvable Lie algebra that is not algebraic.

NOTES Should prove the statements in this section (not difficult). They are important for the structure of semisimple algebraic groups and their representations.

NOTES EOM Lie algebra, algebraic: A Lie algebra is said to be ***algebraic*** if it is the Lie algebra of an algebraic group. For a Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$ (V a finite-dimensional vector space over k), there exists a smallest algebraic Lie subalgebra of $\mathfrak{gl}_V$ containing $\mathfrak{g}$ (called the of $\mathfrak{g}$). Over an algebraically closed field, an algebraic Lie algebra contains the semisimple and nilpotent components s and n of any element. This condition determines the so-called ***almost-algebraic*** Lie algebras. However, it is not sufficient in order that $\mathfrak{g}$ be an algebraic Lie algebra. In the case of a field of characteristic 0, a necessary and sufficient condition for a Lie algebra $\mathfrak{g}$ to be algebraic is that, together with $s = \mathrm{diag}(s_1, \ldots, s_m)$ and n, all operators of the form $\phi(s) = \mathrm{diag}(\phi(s_1), \ldots, \phi(s_n))$ should lie in $\mathfrak{g}$, where is an arbitrary $\mathbb{Q}$-linear mapping from k into k. The structure of an algebraic algebra has been investigated (G.B. Seligman, Modular Lie algebras, Springer, 1967) in the case of a field of characteristic $p > 0$. (See also Tauvel and Yu 2005, 24.5–24.8.)

4 Semisimple algebraic groups

In this section we explain the relation between semisimple algebraic groups and semisimple Lie algebras. Specifically, for any semisimple Lie algebra $\mathfrak{g}$,

$$\mathsf{Rep}(G) = \mathsf{Rep}(\mathfrak{g})$$

for some semisimple algebraic group G with Lie algebra $\mathfrak{g}$; moreover, $X^*(ZG) \simeq P/Q$.

Basic theory

PROPOSITION 4.1 *A connected algebraic group G is semisimple if and only if its Lie algebra is semisimple.*

PROOF. Suppose that $\mathrm{Lie}(G)$ is semisimple, and let N be a normal commutative subgroup of G. Then $\mathrm{Lie}(N)$ is a commutative ideal in $\mathrm{Lie}(G)$ (by 3.31, 3.34), and so it is zero. This implies that N is finite (3.16).

Conversely, suppose that G is semisimple, and let $\mathfrak{n}$ be a commutative ideal in $\mathfrak{g}$. When G acts on $\mathfrak{g}$ through the adjoint representation, the Lie algebra of $H \overset{\text{def}}{=} C_G(\mathfrak{n})$ is

$$\mathfrak{h} = \{x \in \mathfrak{g} \mid [x, \mathfrak{n}] = 0\} \quad ((70), \text{p.}132),$$

which contains $\mathfrak{n}$. Because $\mathfrak{n}$ is an ideal, so is $\mathfrak{h}$:

$$[x, n] = 0, \quad y \in \mathfrak{g} \implies [[y, x], n] = [y, [x, n]] - [x, [y, n]] = 0.$$

Therefore H° is normal in G by (3.31), which implies that its centre $Z(H^\circ)$ is normal in G. Because G is semisimple, $Z(H^\circ)$ is finite, and so $z(\mathfrak{h}) = 0$ by (3.33). But $z(\mathfrak{h}) \supset \mathfrak{n}$, and so $\mathfrak{n} = 0$. □

4.2 The similar statement is false with "reductive" for "semisimple". For example, both $\mathbb{G}_m$ and $\mathbb{G}_a$ have Lie algebra k, which is reductive, but only $\mathbb{G}_m$ is reductive. The Lie algebra of a reductive group G is reductive (because $G = ZG \cdot \mathcal{D}G$), and every reductive Lie algebra is the Lie algebra of a reductive algebraic group, but the Lie algebra of an algebraic group can be reductive without the group being reductive.

4.3 The Lie algebra of a semisimple (even simple) algebraic group need not be semisimple. For example, in characteristic 2, SL_2 is simple but its Lie algebra $\mathfrak{sl}_2$ is not semisimple

COROLLARY 4.4 *The Lie algebra of the radical of a connected algebraic group G is the radical of the Lie algebra of $\mathfrak{g}$; in other words,* $\mathrm{Lie}(R(G)) = r(\mathrm{Lie}(G))$.

PROOF. Because Lie is an exact functor (3.29), the exact sequence

$$1 \to RG \to G \to G/RG \to 1$$

gives rise to an exact sequence

$$0 \to \mathrm{Lie}(RG) \to \mathfrak{g} \to \mathrm{Lie}(G/RG) \to 0$$

in which $\mathrm{Lie}(RG)$ is solvable (obviously) and $\mathrm{Lie}(G/RG)$ is semisimple. The image in $\mathrm{Lie}(G/RG)$ of any solvable ideal in $\mathfrak{g}$ is zero, and so $\mathrm{Lie}(RG)$ is the largest solvable ideal in $\mathfrak{g}$. □

A connected algebraic group G is ***simple*** if it is noncommutative and has no proper normal algebraic subgroups $\neq 1$, and it is ***almost simple*** if it is noncommutative and has no proper normal algebraic subgroups except for finite subgroups. An algebraic group G is said to be the ***almost-direct product*** of its algebraic subgroups $G_1, \ldots, G_n$ if the map

$$(g_1, \ldots, g_n) \mapsto g_1 \cdots g_n \colon G_1 \times \cdots \times G_n \to G$$

is a surjective homomorphism with finite kernel; in particular, this means that the G_i commute with each other and each G_i is normal in G.

THEOREM 4.5 *Every connected semisimple algebraic group G is an almost-direct product*

$$G_1 \times \cdots \times G_r \to G$$

of its minimal connected normal algebraic subgroups. 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. Because $\mathrm{Lie}(G)$ is semisimple, it is a direct sum of its simple ideals (I, 4.17):

$$\mathrm{Lie}(G) = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r.$$

Let G_1 be the identity component of $C_G(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r)$. Then

$$\mathrm{Lie}(G_1) \overset{(70),\text{ p.132}}{=} c_{\mathfrak{g}}(\mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_r) = \mathfrak{g}_1,$$

which is an ideal in Lie(G), and so G_1 is normal in G by (3.31a). If G_1 had a proper normal nonfinite algebraic subgroup, 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 $G_2, \ldots, G_r$ similarly. Because $[\mathfrak{g}_i, \mathfrak{g}_j] = 0$, the groups G_i and G_j commute. The subgroup $G_1 \cdots G_r$ of G has Lie algebra $\mathfrak{g}$, and so equals G (by 3.18). Finally,

$$\mathrm{Lie}(G_1 \cap \ldots \cap G_r) \overset{(3.19)}{=} \mathfrak{g}_1 \cap \ldots \cap \mathfrak{g}_r = 0$$

and so $G_1 \cap \ldots \cap G_r$ is finite (3.16).

Let H be a connected algebraic subgroup of G. If H is normal, then Lie H is an ideal, and so it is a direct sum of those $\mathfrak{g}_i$ it contains and centralizes the remainder (I, 4.17). This implies that H is a product of those G_i it contains, and centralizes the remainder. □

COROLLARY 4.6 *An algebraic group is semisimple if and only if it is an almost direct product of almost-simple algebraic groups.*

COROLLARY 4.7 *All nontrivial connected normal subgroups and quotients of a semisimple algebraic group are semisimple.*

PROOF. They are almost-direct products of almost-simple algebraic groups. □

COROLLARY 4.8 *A semisimple group has no commutative quotients* $\neq 1$.

PROOF. This is obvious for simple groups, and the theorem then implies it for semisimple groups. □

DEFINITION 4.9 A ***split semisimple algebraic group*** is a pair (G, T) consisting of a semisimple algebraic group G and a split maximal torus T.

We say that a semisimple algebraic group G is ***split***[9] if it contains a split maximal torus.

LEMMA 4.10 *If T is a split torus in G, then* Lie(T) *is a commutative subalgebra of* Lie(G) *consisting of semisimple elements.*

PROOF. Certainly Lie(T) is commutative. Let (V, r_V) be a faithful representation of G. Then (V, r_V) decomposes into a direct sum $\bigoplus_{\chi \in X^*(T)} V_\chi$, and Lie$(T)$ acts (semisimply) on each factor V_χ through the character $d\chi$. As (V, dr_V) is faithful, this shows that Lie(T) consists of semisimple elements. □

Rings of representations of Lie algebras

Let $\mathfrak{g}$ be a Lie algebra over k. A ***ring of representations*** of $\mathfrak{g}$ is a collection of representations of $\mathfrak{g}$ that is closed under the formation of direct sums, subquotients, tensor products, and duals. An ***endomorphism*** of such a ring $\mathcal{R}$ is a family

$$\alpha = (\alpha_V)_{V \in \mathcal{R}}, \quad \alpha_V \in \mathrm{End}_{k\text{-linear}}(V),$$

such that

[9]Bourbaki says ***splittable.***

- $\alpha_{V\otimes W} = \alpha_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes \alpha_W$ for all $V, W \in \mathcal{R}$,
- $\alpha_V = 0$ if $\mathfrak{g}$ acts trivially on V, and
- for any homomorphism $\beta\colon V \to W$ of representations in $\mathcal{R}$,

$$\alpha_W \circ \beta = \alpha_V \circ \beta.$$

The set $\mathfrak{g}_{\mathcal{R}}$ of all endomorphisms of $\mathcal{R}$ becomes a Lie algebra over k (possibly infinite-dimensional) with the bracket

$$[\alpha,\beta]_V = [\alpha_V, \beta_V].$$

EXAMPLE 4.11 (IWAHORI 1954) Let k be an algebraically closed field, and let $\mathfrak{g}$ be k regarded as a one-dimensional Lie algebra. To give a representation of $\mathfrak{g}$ on a vector space V is the same as giving an endomorphism α of V, and so the category of representations of $\mathfrak{g}$ is equivalent to the category of pairs (k^n, A), $n \in \mathbb{N}$, with A an $n\times n$ matrix. It follows that to give an endomorphism of the ring $\mathcal{R}$ of all representations of $\mathfrak{g}$ is the same as giving a map $A \mapsto \lambda(A)$ sending a square matrix A to a matrix of the same size and satisfying certain conditions. A pair (g,c) consisting of an additive homomorphism $g\colon k \to k$ and an element c of k defines a λ as follows:

- $\lambda(S) = U\mathrm{diag}(ga_1,\ldots,ga_n)U^{-1}$ if λ is the semisimple matrix $U\mathrm{diag}(a_1,\ldots,a_n)U^{-1}$;
- $\lambda(N) = cN$ if N is nilpotent;
- $\lambda(A) = \lambda(S) + \lambda(N)$ if $A = S + N$ is the decomposition of A into its commuting semisimple and nilpotent parts.

Moreover, every λ arises from a unique pair (g,c). Note that $\mathfrak{g}_{\mathcal{R}}$ has infinite dimension.

Let $\mathcal{R}$ be a ring of representations of a Lie algebra $\mathfrak{g}$. For any $x \in \mathfrak{g}$, $(r_V(x))_{V\in\mathcal{R}}$ is an endomorphism of $\mathcal{R}$, and $x \mapsto (r_V(x))$ is a homomorphism of Lie algebras $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$.

LEMMA 4.12 *If $\mathcal{R}$ contains a faithful representation of $\mathfrak{g}$, then the homomorphism $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$ is injective.*

PROOF. For any representation (V, r_V) of $\mathfrak{g}$, the composite

$$\mathfrak{g} \xrightarrow{x\mapsto(r_V(x))} \mathfrak{g}_{\mathcal{R}} \xrightarrow{\lambda\mapsto\lambda_V} \mathfrak{gl}(V).$$

is r_V. Therefore, $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$ is injective if r_V is injective. □

PROPOSITION 4.13 *Let G be an affine group over k, and let $\mathcal{R}$ be the ring of representations of $\mathrm{Lie}(G)$ arising from a representation of G. Then $\mathfrak{g}_{\mathcal{R}} \simeq \mathrm{Lie}(G)$; in particular, $\mathfrak{g}_{\mathcal{R}}$ depends only on G°.*

PROOF. By definition, $\mathrm{Lie}(G)$ is the kernel of $G(k[\varepsilon]) \to G(k)$. Therefore, to give an element of $\mathrm{Lie}(G)$ is the same as to give a family of $k[\varepsilon]$-linear maps

$$\mathrm{id}_V + \alpha_V\varepsilon\colon V[\varepsilon] \to V[\varepsilon]$$

indexed by $V \in \mathcal{R}$ satisfying the three conditions of (2.7). The first of these conditions says that

$$\mathrm{id}_{V\otimes W} + \alpha_{V\otimes W}\varepsilon = (\mathrm{id}_V + \alpha_V\varepsilon)\otimes(\mathrm{id}_W + \alpha_W\varepsilon),$$

i.e., that

$$\alpha_{V\otimes W} = \mathrm{id}_V \otimes \alpha_W + \alpha_V \otimes \mathrm{id}_W.$$

The second condition says that

$$\alpha_{1\!\!1} = 0,$$

and the third says that the α_V commute with all G-morphisms (= $\mathfrak{g}$-morphisms). Therefore, to give such a family is the same as to give an element $(\alpha_V)_{V\in\mathcal{R}}$ of $\mathfrak{g}_{\mathcal{R}}$. □

PROPOSITION 4.14 *Let $\mathfrak{g}$ be a Lie algebra, and let $\mathcal{R}$ be a ring of representations of $\mathfrak{g}$. The canonical map $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}}$ is an isomorphism if and only if $\mathfrak{g}$ is the Lie algebra of an affine group G whose identity component is algebraic and $\mathcal{R}$ is the ring of representations of $\mathfrak{g}$ arising from a representation of G.*

PROOF. On applying (2.24) to the full subcategory of $\mathsf{Rep}(\mathfrak{g})$ whose objects are those in $\mathcal{R}$ and the forgetful functor, we obtain an affine group G such that $\mathsf{Rep}(G)=\mathcal{R}$; moreover, $\mathrm{Lie}(G)\simeq\mathfrak{g}_R$ (by (4.13). If $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}}$ is an isomorphism, then G° is algebraic because its Lie algebra is finite-dimensional. This proves the necessity, and the sufficiency follows immediately from (4.13). □

COROLLARY 4.15 *Let $\mathfrak{g}\to\mathfrak{gl}(V)$ be a faithful representation of $\mathfrak{g}$, and let $\mathcal{R}(V)$ be the ring of representations of $\mathfrak{g}$ generated by V. Then $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism if and only if $\mathfrak{g}$ is algebraic, i.e., the Lie algebra of an algebraic subgroup of GL_V.*

PROOF. Immediate consequence of the proposition. □

4.16 Let $\mathcal{R}$ be the ring of all representations of $\mathfrak{g}$. When $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}}$ is an isomorphism we says that ***Tannaka duality holds for*** $\mathfrak{g}$. It follows from (5.31) that Tannaka duality holds for semisimple $\mathfrak{g}$. On the other hand, Example 4.11 shows that Tannaka duality fails when $[\mathfrak{g},\mathfrak{g}]\neq\mathfrak{g}$, and even that $\mathfrak{g}_{\mathcal{R}}$ has infinite dimension in this case. Note that if Tannaka duality holds for $\mathfrak{g}$, then elements in $\mathfrak{g}$ have a Jordan decomposition.

EXAMPLE 4.17 Let $\mathfrak{g}$ be a one-dimensional Lie algebra over an algebraically closed field k. The affine group attached to $\mathsf{Rep}(\mathfrak{g})$ is $D(M)\times\mathbb{G}_a$ where M is k regarded as an additive commutative group (see 1.10). In other words, $D(M)$ represents the functor $R\rightsquigarrow\mathrm{Hom}(M,R^{\times})$ (homomorphisms of commutative groups). This follows from Iwahori's result (4.11). Note that M is not finitely generated as a commutative group, and so $D(M)$ is not an algebraic group.

The large number of representations of $\mathfrak{g}$ reflect the fact that it can be realized as the Lie algebra of an algebraic group in many different ways.

NOTES Let $\mathfrak{g}\to\mathfrak{gl}(V)$ be a faithful representation of $\mathfrak{g}$, and let $\mathcal{R}(V)$ be the ring of representations of $\mathfrak{g}$ generated by V. When is $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}(V)}$ an isomorphism? It follows easily from (3.40) that it is, for example, when $\mathfrak{g}=[\mathfrak{g},\mathfrak{g}]$ (cf. Borel 1999, II, 7.9). In particular, $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism when $\mathfrak{g}$ is semisimple. For a commutative Lie group G, $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}(V)}$ is an isomorphism if and only if $\mathfrak{g}\to\mathfrak{gl}(V)$ is a semisimple representation and there exists a lattice in $\mathfrak{g}$ on which the characters of $\mathfrak{g}$ in V take integer values. For the Lie algebra in I, 1.25, $\mathfrak{g}\to\mathfrak{g}_{\mathcal{R}(V)}$ is *never* an isomorphism.

An adjoint to the functor Lie

Let $\mathfrak{g}$ be a Lie algebra, and let $\mathcal{R}$ be the ring of all representations of $\mathfrak{g}$. We define $G(\mathfrak{g})$ to be the Tannaka dual of the neutral tannakian category $(\mathsf{Rep}(\mathfrak{g}), \text{forget})$. Recall (2.24) that this means that $G(\mathfrak{g})$ is the affine group whose R-points for any k-algebra R are the families

$$\lambda = (\lambda_V)_{V \in \mathcal{R}}, \quad \lambda_V \in \mathrm{End}_{R\text{-linear}}(V(R)),$$

such that

- $\lambda_{V\otimes W} = \lambda_V \otimes \lambda_W$ for all $V \in \mathcal{R}$;
- if V is the trivial representation of $\mathfrak{g}$ (i.e., $x_V = 0$ for all $x \in \mathfrak{g}$), then $\lambda_V = \mathrm{id}_V$;
- for every $\mathfrak{g}$-homomorphism $\beta\colon V \to W$,

$$\lambda_W \circ \beta = \beta \circ \lambda_V.$$

For each $V \in \mathcal{R}$, there is a representation r_V of $G(\mathfrak{g})$ on V defined by

$$r_V(\lambda)v = \lambda_V v, \quad \lambda \in G(\mathfrak{g})(R), \quad v \in V(R), \quad R \text{ a } k\text{-algebra},$$

and $V \rightsquigarrow (V, r_V)$ is an equivalence of categories

$$\mathsf{Rep}(\mathfrak{g}) \xrightarrow{\sim} \mathsf{Rep}(G(\mathfrak{g})). \tag{71}$$

LEMMA 4.18 *The homomorphism $\eta\colon\mathfrak{g} \to \mathrm{Lie}(G(\mathfrak{g}))$ is injective, and the composite of the functors*

$$\mathsf{Rep}(G(\mathfrak{g})) \xrightarrow{(V,r)\rightsquigarrow(V,\mathrm{Lie}(r))} \mathsf{Rep}(\mathrm{Lie}(G(\mathfrak{g}))) \xrightarrow{\eta^\vee} \mathsf{Rep}(\mathfrak{g}) \tag{72}$$

is an equivalence of categories.

PROOF. According to (4.13), $\mathrm{Lie}(G(\mathfrak{g})) \simeq \mathfrak{g}_{\mathcal{R}}$, and so the first assertion follows from (4.12) and Ado's theorem (I, 6.27). The composite of the functors in (72) is a quasi-inverse to the functor in (71). □

LEMMA 4.19 *The affine group $G(\mathfrak{g})$ is connected.*

PROOF. When $\mathfrak{g}$ is one-dimensional, we computed $G(\mathfrak{g})$ in (4.17) and found it to be connected.

For a general $\mathfrak{g}$, we have to show that only a trivial representation of $\mathfrak{g}$ has the property that the category of subquotients of direct sums of copies of the representation is stable under tensor products (see AGS, XII, 1.5). When $\mathfrak{g}$ is semisimple, this follows from (I, 9.1).

Let V be a representation of $\mathfrak{g}$ with the above property. It follows from the one-dimensional case that the radical of $\mathfrak{g}$ acts trivially on V, and then it follows from the semisimple case that $\mathfrak{g}$ itself acts trivially. □

PROPOSITION 4.20 *The pair $(G(\mathfrak{g}), \eta)$ is universal: for any algebraic group H and k-algebra homomorphism $a\colon\mathfrak{g} \to \mathrm{Lie}(H)$, there is a unique homomorphism $b\colon G(\mathfrak{g}) \to H$ such that $a = \mathrm{Lie}(b) \circ \eta$:*

$$\begin{array}{ccc} G(\mathfrak{g}) & & \mathfrak{g} \xrightarrow{\ \eta\ } \mathrm{Lie}(G(\mathfrak{g})) \\ \Big\downarrow{\scriptstyle \exists! b} & \overset{\mathit{Lie}}{\rightsquigarrow} & {\scriptstyle a}\searrow \quad \Big\downarrow{\scriptstyle \mathrm{Lie}(b)} \\ H & & \mathrm{Lie}(H). \end{array}$$

In other words, the map sending a homomorphism $b\colon G(\mathfrak{g}) \to H$ to the homomorphism $\mathrm{Lie}(b)\circ\eta\colon \mathfrak{g} \to \mathrm{Lie}(H)$ is a bijection

$$\mathrm{Hom}_{\textit{affine groups}}(G(\mathfrak{g}), H) \to \mathrm{Hom}_{\textit{Lie algebras}}(\mathfrak{g}, \mathrm{Lie}(H)). \tag{73}$$

If a is surjective and $\mathsf{Rep}(G(\mathfrak{g}))$ is semisimple, then b is surjective.

PROOF. From a homomorphism $b{:}G(\mathfrak{g}) \to H$, we get a commutative diagram

$$\begin{array}{ccc} \mathsf{Rep}(H) & \xrightarrow{\ b^{\vee}\ } & \mathsf{Rep}(G(\mathfrak{g})) \\ \Big\downarrow{\scriptstyle \text{fully faithful}} & & \Big\downarrow{\scriptstyle \simeq (4.18)} \\ \mathsf{Rep}(\mathrm{Lie}(H)) & \xrightarrow{\ a^{\vee}\ } & \mathsf{Rep}(\mathfrak{g}) \end{array} \qquad a \overset{\text{def}}{=} \mathrm{Lie}(b)\circ\eta.$$

If $a = 0$, then $a^{\vee}$ sends all objects to trivial objects, and so the functor $b^{\vee}$ does the same, which implies that the image of b is 1. Hence (73) is injective.

From a homomorphism $a\colon \mathfrak{g} \to \mathrm{Lie}(H)$, we get a tensor functor

$$\mathsf{Rep}(H) \to \mathsf{Rep}(\mathrm{Lie}(H)) \xrightarrow{a^{\vee}} \mathsf{Rep}(\mathfrak{g}) \simeq \mathsf{Rep}(G(\mathfrak{g}))$$

and hence a homomorphism $G(\mathfrak{g}) \to H$, which acts as a on the Lie algebras. Hence (73) is surjective.

If a is surjective, then $a^{\vee}$ is fully faithful, and so $\mathsf{Rep}(H) \to \mathsf{Rep}(G(\mathfrak{g}))$ is fully faithful, which implies that $G(\mathfrak{g}) \to G$ is surjective by (2.14a). □

PROPOSITION 4.21 *For any finite extension $k' \supset k$ of fields, $G(\mathfrak{g}_{k'}) \simeq G(\mathfrak{g})_{k'}$.*

PROOF. More precisely, we prove that the pair $(G(\mathfrak{g})_{k'}, \eta_{k'})$ obtained from $(G(\mathfrak{g}), \eta)$ by extension of the base field has the universal property characterizing $(G(\mathfrak{g}_{k'}), \eta)$. Let H be an algebraic group over k', and let H_* be the group over k obtained from H by restriction of the base field (see AGS V). Then

$$\begin{aligned} \mathrm{Hom}_{k'}(G(\mathfrak{g})_{k'}, H) &\simeq \mathrm{Hom}_k(G(\mathfrak{g}), H_*) \quad \text{(universal property of } H_*\text{)} \\ &\simeq \mathrm{Hom}_k(\mathfrak{g}, \mathrm{Lie}(H_*)) \quad (4.20) \\ &\simeq \mathrm{Hom}_{k'}(\mathfrak{g}_{k'}, \mathrm{Lie}(H)). \end{aligned}$$

For the last isomorphism, note that

$$\mathrm{Lie}(H_*) \overset{\text{def}}{=} \mathrm{Ker}(H_*(k[\varepsilon]) \to H_*(k)) \simeq \mathrm{Ker}(H(k'[\varepsilon]) \to H(k')) \overset{\text{def}}{=} \mathrm{Lie}(H).$$

In other words, $\mathrm{Lie}(H_*)$ is $\mathrm{Lie}(H)$ regarded as a Lie algebra over k (instead of k'), and the isomorphism is simply the canonical isomorphism in linear algebra,

$$\mathrm{Hom}_{k\text{-linear}}(V,W) \simeq \mathrm{Hom}_{k'\text{-linear}}(V \otimes_k k', W)$$

(V, W vector spaces over k and k' respectively). □

The next theorem shows that, when $\mathfrak{g}$ is semisimple, $G(\mathfrak{g})$ is a semisimple algebraic group with Lie algebra $\mathfrak{g}$, and any other semisimple group with Lie algebra $\mathfrak{g}$ is a quotient of $G(\mathfrak{g})$; moreover, the centre of $G(\mathfrak{g})$ has character group P/Q.

THEOREM 4.22 *Let $\mathfrak{g}$ be a semisimple Lie algebra.*

(a) *The homomorphism $\eta\colon \mathfrak{g} \to \mathrm{Lie}(G(\mathfrak{g}))$ is an isomorphism.*
(b) *The affine group $G(\mathfrak{g})$ is a semisimple algebraic group.*
(c) *For any algebraic group H and isomorphism $a\colon \mathfrak{g} \to \mathrm{Lie}(H)$, there exists a unique isogeny $b\colon G(\mathfrak{g}) \to H^\circ$ such that $a = \mathrm{Lie}(b) \circ \eta$:*

$$\begin{array}{ccc} G(\mathfrak{g}) & \qquad & \mathfrak{g} \xrightarrow{\ \eta\ } \mathrm{Lie}(G(\mathfrak{g})) \\ \Big\downarrow{\scriptstyle \exists! b} & & \quad {\scriptstyle a}\searrow \qquad \Big\downarrow{\scriptstyle \mathrm{Lie}(b)} \\ H & & \qquad\qquad \mathrm{Lie}(H). \end{array}$$

(d) *Let Z be the centre of $G(\mathfrak{g})$. Then $X^*(Z) \simeq P/Q$, i.e., $Z \simeq D(P/Q)$.*

PROOF. (a) Because $\mathsf{Rep}(G(\mathfrak{g}))$ is semisimple, $G(\mathfrak{g})$ is reductive (2.13). Therefore $\mathrm{Lie}(G(\mathfrak{g}))$ is reductive, and so $\mathrm{Lie}(G(\mathfrak{g})) = \eta(\mathfrak{g}) \times \mathfrak{a} \times \mathfrak{c}$ with $\mathfrak{a}$ is semisimple and $\mathfrak{c}$ commutative (I, 4.17; I, 6.2). If $\mathfrak{a}$ or $\mathfrak{c}$ is nonzero, then there exists a nontrivial representation r of $G(\mathfrak{g})$ such that $\mathrm{Lie}(r)$ is trivial on $\mathfrak{g}$. But this is impossible because η defines an equivalence $\mathsf{Rep}(G(\mathfrak{g})) \to \mathsf{Rep}(\mathfrak{g})$.

(b) Now $G(\mathfrak{g})$ is semisimple because its Lie algebra is semisimple.

(c) Proposition 4.20 shows that there exists a unique homomorphism b such that $a = \mathrm{Lie}(b) \circ \eta$, which is an isogeny because $\mathrm{Lie}(b)$ is an isomorphism (3.30).

(d) In (4.26) below, we show that if $\mathfrak{g}$ is split, then $X^*(Z) \simeq P/Q$ (as commutative groups). As $\mathfrak{g}$ splits over k^{al}, this implies (d). □

REMARK 4.23 The isomorphism $X^*(Z) \simeq P/Q$ in (d) commutes with the natural actions of $\mathrm{Gal}(k^{\mathrm{al}}/k)$.

NOTES Need to examine what $\mathfrak{g} \rightsquigarrow G(\mathfrak{g})$ does to normalizers and centralizers. For example, show that, if T is a torus in a reductive algebraic group G, then $G(c_{\mathfrak{t}}(\mathfrak{g})) = C_T(G)$, which is therefore connected.

Applications

THEOREM 4.24 *(Jacobson-Morosov) Let G be a semisimple algebraic group. Regard $\mathbb{G}_a$ as a subgroup of SL_2 via the map $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Every nontrivial homomorphism $\varphi\colon \mathbb{G}_a \to G$ extends to a homomorphism $\mathrm{SL}_2 \to G$; moreover, any two extensions are conjugate by an element of $G(k)$.*

PROOF. Consider $d\varphi\colon k \to \mathfrak{g}$. Because $\mathfrak{g}$ is semisimple, the image of k is nilpotent in $\mathfrak{g}$. Therefore, (8.33) $d\varphi$ extends uniquely to a homomorphism $\mathfrak{sl}_2 \to \mathfrak{g}$. From

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{sl}_2) \simeq \mathsf{Rep}(\mathrm{SL}_2)$$

we obtain the required homomorphism $\mathrm{SL}_2 \to G$. The uniqueness also follows from (8.33). □

NOTES Cf. Borel II, 7, and mo22186

THEOREM 4.25 *The centralizer of a reductive subgroup of reductive group is reductive.*

PROOF. Let H be a reductive subgroup of a reductive group G, and let U be the unipotent radical of $C_G(H)$. It suffices to show that every homomorphism $f\colon \mathbb{G}_a \to U$ is trivial. The homomorphism $\mathbb{G}_a \times H \to G$ extends to a homomorphism $\mathrm{SL}_2 \times H \to G$. Therefore, f extends to a homomorphism $f'\colon \mathrm{SL}_2 \to C_G(H)$. The composite of f with $C_G(H) \to C_G(H)/U$ is trivial, and so the same is true of f', i.e., $f'(\mathrm{SL}_2) \subset U$. Therefore $f'(\mathrm{SL}_2) = 1$. Cf. André and Kahn 2002, 20.1.1. □

NOTES (mo114243) Let G be a reductive algebraic group over an algebraically closed field (of characteristic zero if it matters) and H a subgroup, also reductive. Is the identity component of the normalizer of H in G always reductive?

The answer is yes, at least in characteristic zero. There is a Theorem of Mostow which says that G may be viewed as a subgroup of GL_n such that the restriction of the Cartan involution of $GL_n(C)$ to G and H gives Cartan involutions on G and H. Therefore, the normaliser $N_G(H)$ of H in G is also invariant under this Cartan involution. Hence it is reductive.

Split semisimple algebraic groups

Let $(\mathfrak{g},\mathfrak{h})$ be a split semisimple Lie algebra, and let P and Q be the corresponding weight and root lattices. The action of $\mathfrak{h}$ on a $\mathfrak{g}$-module V decomposes it into a direct sum $V = \bigoplus_{\varpi \in P} V_\varpi$ of weight spaces. Let $D(P)$ be the diagonalizable group attached to P (1.10). Thus $D(P)$ is a split torus such that $\mathsf{Rep}(D(P))$ has a natural identification with the category of P-graded vector spaces. The functor $(V, r_V) \mapsto (V, (V_\varpi)_{\omega \in P})$ is an exact tensor functor $\mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(D(P))$ compatible with the forgetful functors, and hence defines a homomorphism $D(P) \to G(\mathfrak{g})$. Let $T(\mathfrak{h})$ be the image of this homomorphism.

THEOREM 4.26 *With the above notations:*

(a) *The group $T(\mathfrak{h})$ is a split maximal torus in $G(\mathfrak{g})$, and η restricts to an isomorphism $\mathfrak{h} \to \mathrm{Lie}(T(\mathfrak{h}))$.*
(b) *The map $D(P) \to T(\mathfrak{h})$ is an isomorphism; therefore, $X^*(T(\mathfrak{h})) \simeq P$.*

(c) *The centre of* $G(\mathfrak{g})$ *is contained in* $T(\mathfrak{h})$ *and equals*

$$\bigcap\nolimits_{\alpha\in R}\mathrm{Ker}(\alpha\colon T(\mathfrak{h})\to\mathbb{G}_m)$$

(and so has character group P/Q*).*

PROOF. (a) The torus $T(\mathfrak{h})$ is split because it is the quotient of a split torus. Certainly, η restricts to an injective homomorphism $\mathfrak{h}\to\mathrm{Lie}(T(\mathfrak{h}))$. It must be surjective because otherwise $\mathfrak{h}$ wouldn't be a Cartan subalgebra of $\mathfrak{g}$. The torus $T(\mathfrak{h})$ must be maximal because otherwise $\mathfrak{h}$ wouldn't be equal to its normalizer.

(b) Let V be the representation $\bigoplus V_{\varpi}$ of $\mathfrak{g}$ where ϖ runs through a set of fundamental weights. Then $G(\mathfrak{g})$ acts on V, and the map $D(P)\to\mathrm{GL}(V)$ is injective. Therefore, $D(P)\to T(\mathfrak{h})$ is injective.

(c) A gradation on $\mathsf{Rep}(\mathfrak{g})$ is defined by a homomorphism $P\to M(P_{++})$ (see I, 9.6), and hence by a homomorphism $D(M(P_{++}))\to T(\mathfrak{h})$. This shows that the centre of $G(\mathfrak{g})$ is contained in $T(\mathfrak{h})$. The kernel of the adjoint map $\mathrm{Ad}\colon G(\mathfrak{g})\to\mathrm{GL}_{\mathfrak{g}}$ is the centre $Z(G(\mathfrak{g}))$ of $G(\mathfrak{g})$ (see 3.36), and so the kernel of $\mathrm{Ad}|T(\mathfrak{h})$ is $Z(G(\mathfrak{g}))\cap T(\mathfrak{h})=Z(G(\mathfrak{g}))$. But

$$\mathrm{Ker}(\mathrm{Ad}|T(\mathfrak{h}))=\bigcap_{\alpha\in R}\mathrm{Ker}(\alpha),$$

so $Z(G(\mathfrak{g}))$ is as described. □

LEMMA 4.27 *The following conditions on a subtorus* T *of a semisimple algebraic group* G *are equivalent;*

(a) T *is a maximal torus in* G*;*
(b) $T_{k^{\mathrm{al}}}$ *is a maximal torus in* $G_{k^{\mathrm{al}}}$*;*
(c) $T=C_G(T)^{\circ}$*;*
(d) $\mathfrak{t}$ *is a Cartan subalgebra of* $\mathfrak{g}$.

PROOF. (c)⇒(a). Obvious.

(a)⇒(d). Let T be a torus in G, and let $G\to\mathrm{GL}_V$ be a faithful representation of G. After we have extended k, V will decompose into a direct sum $\bigoplus_{\chi\in X^*(T)}V_{\chi}$, and $\mathrm{Lie}(T)$ acts (semisimply) on each factor V_{χ} through the character $\mathrm{Lie}(\chi)$. As $\mathfrak{g}\to\mathfrak{gl}_V$ is faithful, this shows that $\mathfrak{t}$ consists of semisimple elements. Hence $\mathfrak{t}$ is toral. Any toral subalgebra of $\mathfrak{g}$ containing $\mathfrak{t}$ arises from a subtorus of G, and so $\mathfrak{t}$ is maximal.

(d)⇒(c). Because $\mathfrak{t}$ is a Cartan subalgebra, $\mathfrak{t}=\mathfrak{c}_{\mathfrak{g}}(\mathfrak{t})$ (see I, 8.14). As $\mathrm{Lie}(C_G(T))=\mathfrak{c}_{\mathfrak{g}}(\mathfrak{t})$, we see that T and $C_G(T)$ have the same Lie algebra, and so $T=C_G(T)^{\circ}$.

(b)⇔(a). This follows from the equivalence of (a) and (d) and the fact that $\mathfrak{t}$ is a Cartan subalgebra of $\mathfrak{g}$ if and only if $\mathfrak{t}_{k^{\mathrm{al}}}$ is a Cartan subalgebra of $\mathfrak{g}_{k^{\mathrm{al}}}$. □

DEFINITION 4.28 A ***split semisimple algebraic group*** is a pair (G,T) consisting of a semisimple algebraic group G and a split maximal torus T.

More loosely, we say that a semisimple algebraic group is ***split*** if it contains a split maximal torus.[10]

[10]Caution: a semisimple algebraic group always contains a maximal split torus, but that torus may not be maximal among all tori, and hence not a split maximal torus.

THEOREM 4.29 *Let T and T' be split maximal tori in a semisimple algebraic group G. Then $T' = gTg^{-1}$ for some $g \in G(k)$.*

PROOF. We may set $G = G(\mathfrak{g})$ with $\mathfrak{g}$ the semisimple Lie algebra $\mathrm{Lie}(G)$. Let x be a nilpotent element of $\mathfrak{g}$. For any representation (V, r_V) of $\mathfrak{g}$, $e^{r_V(x)} \in G(\mathfrak{g})(k)$. According to (I, 8.24), there exist nilpotent elements $x_1, \ldots, x_m$ in $\mathfrak{g}$ such that

$$e^{\mathrm{ad}(x_1)} \cdots e^{\mathrm{ad}(x_m)} \mathrm{Lie}(T) = \mathrm{Lie}(T').$$

Let $g = e^{\mathrm{ad}(x_1)} \cdots e^{\mathrm{ad}(x_m)}$; then $gTg^{-1} = T'$ because they have the same Lie algebra. □

Classification

We can now read off the classification theorems for split semisimple algebraic groups from the similar theorems for split semisimple Lie algebras.

Let (G, T) be a split semisimple algebraic group. Because T is diagonalizable, the k-vector space $\mathfrak{g}$ decomposes into eigenspaces under its action:

$$\mathfrak{g} = \bigoplus_{\alpha \in X^*(T)} \mathfrak{g}^{\alpha}.$$

The roots of (G, T) are the nonzero α such that $\mathfrak{g}^{\alpha} \neq 0$. Let R be the set of roots of (G, T).

PROPOSITION 4.30 *The set of roots of (G, T) is a reduced root system R in $V \stackrel{\text{def}}{=} X^*(T) \otimes \mathbb{Q}$; moreover,*

$$Q(R) \subset X^*(T) \subset P(R). \tag{74}$$

PROOF. Let $\mathfrak{g} = \mathrm{Lie}\, G$ and $\mathfrak{h} = \mathrm{Lie}\, T$. Then $(\mathfrak{g}, \mathfrak{h})$ is a split semisimple Lie algebra, and, when we identify V with a $\mathbb{Q}$-subspace of $\mathfrak{h}^{\vee} \simeq X^*(T) \otimes k$, the roots of (G, T) coincide with the roots of $(\mathfrak{g}, \mathfrak{h})$ and so (74) holds. □

By a ***diagram*** (V, R, X), we mean a reduced root system (V, R) over $\mathbb{Q}$ and a lattice X in V that is contained between $Q(R)$ and $P(R)$.[11]

THEOREM 4.31 (EXISTENCE) *Every diagram arises from a split semisimple algebraic group over k.*

More precisely, we have the following result.

THEOREM 4.32 *Let (V, R, X) be a diagram, and let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra over k with root system $(V \otimes k, R)$ (see I, 8.60). Let $\mathsf{Rep}(\mathfrak{g})^X$ be the full subcategory of $\mathsf{Rep}(\mathfrak{g})$ whose objects are those whose simple components have highest weight in X. Then $\mathsf{Rep}(\mathfrak{g})^X$ is a tannakian subcategory of $\mathsf{Rep}(\mathfrak{g})$, and there is a natural tensor functor $\mathsf{Rep}(\mathfrak{g})^X \to \mathsf{Rep}(D(X))$ compatible with the forgetful functors. The Tannaka dual (G, T) of this functor is a split semisimple algebraic group with diagram (V, R, X).*

[11] A diagram is essentially the same as a semisimple root datum — see my notes Reductive Groups, I, §5.

In more detail: the pair $(\mathsf{Rep}(\mathfrak{g})^X, \text{forget})$ is a neutral tannakian category, with Tannaka dual G say; the pair $(\mathsf{Rep}(D(X), \text{forget})$ is a neutral tannakian category, with Tannaka dual $D(X)$; the tensor functor

$$(\mathsf{Rep}(\mathfrak{g})^X, \text{forget}) \to (\mathsf{Rep}(D(X), \text{forget})$$

defines an injective homomorphism

$$D(X) \to G,$$

whose image we denote T. Then (G, T) is split semisimple group with diagram (V, R, X).

PROOF. When $X = Q$, $(G, T) = (G(\mathfrak{g}), T(\mathfrak{h}))$, and the statement follows from Theorem 4.26. For an arbitrary X, let

$$N = \bigcap\nolimits_{\chi \in X/Q} \text{Ker}(\chi\colon Z(G(\mathfrak{g})) \to \mathbb{G}_m).$$

Then $\mathsf{Rep}(\mathfrak{g})^X$ is the subcategory of $\mathsf{Rep}(\mathfrak{g})$ on which N acts trivially, and so it is a tannakian category with Tannaka dual $G(\mathfrak{g})/N$ (see AGS, VIII, 15.1). Now it is clear that $(G(\mathfrak{g})/N, T(\mathfrak{h})/N)$ is the Tannaka dual of $\mathsf{Rep}(\mathfrak{g})^X \to \mathsf{Rep}(D(X))$, and that it has diagram (V, R, X). □

THEOREM 4.33 (ISOGENY) *Let (G, T) and (G', T') be split semisimple algebraic groups over k, and let (V, R, X) and (V, R', X') be their associated diagrams. Any isomorphism $V \to V'$ sending R onto R' and X into X' arises from an isogeny $G \to G'$ mapping T onto T'.*

PROOF. Let $(\mathfrak{g}, \mathfrak{h})$ and $(\mathfrak{g}', \mathfrak{h}')$ be the split semisimple Lie algebras of (G, T) and (G', T'). An isomorphism $V \to V'$ sending R onto R' and X into X' arises from an isomorphism $(\mathfrak{g}, \mathfrak{h}) \xrightarrow{\beta} (\mathfrak{g}', \mathfrak{h}')$ (see 8.61). Now β defines an exact tensor functor $\mathsf{Rep}(\mathfrak{g}')^{X'} \to \mathsf{Rep}(\mathfrak{g})^X$, and hence a homomorphism $\alpha\colon G \to G'$, which has the required properties. □

PROPOSITION 4.34 *Let (G, T) be a split semisimple algebraic group. For each root α of (G, T) and choice of a nonzero element of $\mathfrak{g}^\alpha$, there a unique homomorphism*

$$\varphi\colon \text{SL}_2 \to G$$

such that $\text{Lie}(\varphi)$ *is the inclusion $\mathfrak{s}_\alpha \to \mathfrak{g}$ of (I, 8.31).*

PROOF. From the inclusion $\mathfrak{s}_\alpha \to \mathfrak{g}$ we get a tensor functor $\mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{s}_\alpha)$, and hence a tensor functor $\mathsf{Rep}(G) \to \mathsf{Rep}(\text{SL}_2)$; this arises from a homomorphism $\text{SL}_2 \to G$. □

The image U_α of $\mathbb{U}_2$ under φ is called the ***root group*** of α. It is uniquely determined by having the following properties: it is isomorphic to $\mathbb{G}_a$, and for any isomorphism $u_\alpha\colon \mathbb{G}_a \to U_\alpha$,

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \quad a \in k, \quad t \in T(k).$$

NOTES To be continued — there is much more to be said. In particular, we need to determine the algebraic subalgebras of $\mathfrak{g}$, so that we can read off everything about the algebraic subgroups of G in terms of the subalgebras of $\mathfrak{g}$ (and hence in terms of the root system of (G, T)).

NOTES Indeed, it is my intention to complete Chapter I, and then simply read off the corresponding results for semisimple algebraic groups. However, it will also be useful to work out the theory of split reductive group ab initio using only the key result (4.22).

NOTES Can we replace the condition that $\mathfrak{g}$ be semisimple with the condition that $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ throughout? Or just that $\mathfrak{g}$ is algebraic?

5 Reductive groups

Split reductive groups

We develop the theory of split reductive group ab initio using only the key result (4.22)

Root data

DEFINITION 5.1 A ***root datum*** is a triple $\mathcal{R} = (X, R, f)$ where X is a free abelian group of finite rank, R is a finite subset of X, and f is an injective map $\alpha \mapsto \alpha^\vee$ from R into the dual $X^\vee$ of X, satisfying

(rd1) $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in R$;
(rd2) $s_\alpha(R) \subset R$ for all $\alpha \in R$, where s_α is the homomorphism $X \to X$ defined by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad x \in X, \alpha \in R,$$

(rd3) the group of automorphisms $W(\mathcal{R})$ of X generated by the s_α for $\alpha \in R$ 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_α should be considered an "abstract reflection in the hyperplane orthogonal to $\alpha^\vee$". The elements of R and $R^\vee$ are called the ***roots*** and ***coroots*** of the root datum (and $\alpha^\vee$ is the ***coroot*** of α). The group $W = W(\mathcal{R})$ of automorphisms of X generated by the s_α for $\alpha \in R$ is called the ***Weyl group*** of the root datum.

The roots of a split reductive group

Now let (G, T) be a split reductive group. The adjoint representation of G on $\mathfrak{g}$ induces an action of T on $\mathfrak{g}$. Because T is split, $\mathfrak{g}$ decomposes into a direct sum of eigenspaces

$$\mathfrak{g}^\alpha \stackrel{\text{def}}{=} \{x \in \mathfrak{g} \mid \mathrm{Ad}(t)x = \alpha(t)x \text{ all } t \in T(k)\}.$$

Let $R = R(G, T)$ be the set of nonzero characters of T such that $\mathfrak{g}^\alpha$ is nonzero. Then

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus\nolimits_{\alpha \in R} \mathfrak{g}^\alpha$$

with $\mathfrak{h} = \mathrm{Lie}(T)$.

The Weyl group of (G,T)

LEMMA 5.2 *Let* T *be a torus in a connected algebraic group* G. *Then* $N_G(T)^\circ = C_G(T)^\circ$.

PROOF. Certainly, $N_G(T) \supset C_G(T)$ and $N_G(T)^\circ \supset C_G(T)^\circ$. However, $N_G(T)^\circ$ acts trivially on T (by rigidity 1.13), and so $N_G(T)^\circ \subset C_G(T)^\circ$. □

Let (G,T) be a split reductive group. The ***Weyl group*** of (G,T) is

$$W(G,T) = N_G(T)(k)/C_G(T)(k).$$

If k is infinite, then $T(k)$ is dense in T, and

$$W(G,T) = N_{G(k)}(T(k))/C_{G(k)}(T(k)).$$

The lemma shows that $W(G,T)$ is finite.

EXAMPLE 5.3 Let $G = \mathrm{SL}_2$ and T be the subgroup of diagonal elements. In this case, $C_G(T) = T$ but

$$N_G(T) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} \right\}.$$

Therefore $W(G,T) = \{1,s\}$ where s is represented by the matrix $n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Note that

$$n \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} n^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix},$$

and so

$$s\,\mathrm{diag}(a,a^{-1}) = \mathrm{diag}(a^{-1},a).$$

EXAMPLE 5.4 Let $G = \mathrm{GL}_n$ and $T = \mathbb{D}_n$. In this case, $C_G(T) = T$ but $N_G(T)$ contains the permutation matrices (those obtained from I by permuting the rows). For example, let $E(ij)$ be the matrix obtained from I by interchanging the ith and jth rows. Then

$$E(ij) \cdot \mathrm{diag}(\cdots a_i \cdots a_j \cdots) \cdot E(ij)^{-1} = \mathrm{diag}(\cdots a_j \cdots a_i \cdots).$$

More generally, let σ be a permutation of $\{1,\ldots,n\}$, and let $E(\sigma)$ be the matrix obtained by using σ to permute the rows. Then $\sigma \mapsto E(\sigma)$ is an isomorphism from S_n onto the set of permutation matrices, and conjugating a diagonal matrix by $E(\sigma)$ simply permutes the diagonal entries. The $E(\sigma)$ form a set of representatives for $C_G(T)(k)$ in $N_G(T)(k)$, and so $W(G,T) \simeq S_n$.

LEMMA 5.5 *Let* (G,T) *be a split reductive group. The action of* $W(G,T)$ *on* $X^*(T)$ *stabilizes* R.

PROOF. Let $s \in W(G,T)$, and let $n \in G(k)$ represent s. Then s acts on $X^*(T)$ (on the left) by

$$(s\chi)(t) = \chi(n^{-1}tn), \quad t \in T(k^{\mathrm{al}}).$$

Let α be a root. Then, for $x \in (\mathfrak{g}_\alpha)_{k^{\mathrm{al}}}$ and $t \in T(k^{\mathrm{al}})$,

$$t(nx) = n(n^{-1}tn)x = s(\alpha(s^{-1}ts)x) = \alpha(s^{-1}ts)sx,$$

and so T acts on $s\mathfrak{g}_\alpha$ through the character $s\alpha$, which must therefore be a root. □

The root datum of (G,T)

PROPOSITION 5.6 *Let* (G,T) *be a split reductive group, and let* α *be a root of* (G,T).

(a) *There exists a unique subgroup* U_α *of* G *isomorphic to* $\mathbb{G}_a$ *such that, for any isomorphism* $u_\alpha\colon\mathbb{G}_a\to U_\alpha$,

$$t\cdot u_\alpha(a)\cdot t^{-1}=u_\alpha(\alpha(t)a),\ \text{all}\ t\in T(R),\ a\in G(R).$$

(b) *Let* $T_\alpha=\mathrm{Ker}(\alpha)^\circ$, *and let* G_α *be centralizer of* T_α *in* G. *Then* $W(G_\alpha,T)$ *contains exactly one nontrivial element* s_α, *and there is a unique* $\alpha^\vee\in X_*(T)$ *such that*

$$s_\alpha(x)=x-\langle x,\alpha^\vee\rangle\alpha,\quad \text{for all}\ x\in X^*(T). \tag{75}$$

Moreover, $\langle\alpha,\alpha^\vee\rangle=2$.

(c) *The algebraic group* G_α *is generated by* T, U_α, *and* $U_{-\alpha}$.

The cocharacter $\alpha^\vee$ is called the coroot of α, and the group U_α in (a) is called the ***root group*** of α. Thus the root group of α is the unique copy of $\mathbb{G}_a$ in G that is normalized by T and such that T acts on it through α.

We prove Proposition 5.6 in the next subsection, after first illustrating it with an example, and using it to define the root datum of (G,T).

EXAMPLE 5.7 Let $(G,T)=(\mathrm{GL}_n,\mathbb{D}_n)$, and let $\alpha=\alpha_{12}=\chi_1-\chi_2$. Then

$$T_\alpha=\{\mathrm{diag}(x,x,x_3,\ldots,x_n)\mid xxx_3\ldots x_n\neq 1\}$$

and G_α consists of the invertible matrices of the form

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

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_α of $W(G_\alpha,T)$. It acts on T by

$$\mathrm{diag}(x_1,x_2,x_3,\ldots,x_n)\longmapsto\mathrm{diag}(x_2,x_1,x_3,\ldots,x_n).$$

For $x=m_1\chi_1+\cdots+m_n\chi_n$,

$$\begin{aligned} s_\alpha x&=m_2\chi_1+m_1\chi_2+m_3\chi_3+\cdots+m_n\chi_n\\ &=x-\langle x,\lambda_1-\lambda_2\rangle(\chi_1-\chi_2).\end{aligned}$$

Thus (75) holds if and only if $\alpha^\vee$ is taken to be $\lambda_1-\lambda_2$.

THEOREM 5.8 *Let (G,T) be a split reductive group. Let R be the set of roots of (G,T) and, for $\alpha \in R$, let $\alpha^\vee$ be the element of $X_*(T)$ defined by 5.6(b). Then $(X^*(T), R, \alpha \mapsto \alpha^\vee)$ is a root datum.*

PROOF. Condition (rd1) holds by (b). The s_α attached to α lies in $W(G_\alpha,T) \subset W(G,T)$, and so stablizes R by the lemma. Finally, all s_α lie in the Weyl group $W(G,T)$, and so they generate a finite group. □

From this, and the Borel fixed point theorem, the entire theory of split reductive groups over fields of characteristic zero follows easily (to be continued).

Proof of Proposition 5.6

LEMMA 5.9 *Let $\mathfrak{g}$ be an abelian Lie group, and let $\mathfrak{g}_\mathfrak{a}$ be the algebraic group $R \rightsquigarrow (\mathfrak{g}_R, +)$. There is a canonical isomorphism*

$$\mathsf{Rep}(\mathfrak{g}_\mathfrak{a}) \simeq \mathsf{Rep}^{nil}(\mathfrak{g}).$$

PROOF. The representations of $\mathbb{G}_a$ are given by pairs (V,α) where α is a nilpotent endomorphism of the vector space V (AGS VIII, 2.1). When $\mathfrak{g}$ has dimension 1, the representations are given by pairs (V,α) where α is an endomorphism of V. Thus, in this case, the statement is obvious. A more general result will be proved in the next section. □

PROPOSITION 5.10 *Let (G,T) be a split reductive group, and let α be a root of (G,T).*

(a) There exists a unique homomorphism of algebraic groups

$$u_\alpha : \mathfrak{g}_\mathfrak{a}^\alpha \to G$$

such that

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a)$$

for all R, $t \in T(R)$, $a \in G(R)$, and $\mathrm{Lie}(u_\alpha)$ is the given inclusion $\mathfrak{g}^\alpha \to \mathfrak{g}$.

(b) Let $\mathfrak{s}_\alpha$ be the copy of $\mathfrak{sl}_2$ in $\mathfrak{g}$ defined by the root α (I, 8.31), and let S_α be the algebraic group such that $\mathsf{Rep}(S_\alpha) = \mathsf{Rep}(\mathfrak{s}_\alpha)$. Then there exists a unique homomorphism of algebraic groups

$$v : S_\alpha \to G$$

such that $\mathrm{Lie}(s_\alpha)$ is the given inclusion $\mathfrak{s}_\alpha \to \mathfrak{g}$.

PROOF. (a) Take u_α to be the homomorphism dual to

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g}^\alpha) \simeq \mathsf{Rep}(\mathfrak{g}_\mathfrak{a}^\alpha).$$

The functor $\mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{g}^\alpha)$ lands in $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g}^\alpha)$ because it factors through $\mathsf{Rep}(\mathfrak{s}_\alpha)$.

(b) Take s_α to be the homomorphim dual to

$$\mathsf{Rep}(G) \to \mathsf{Rep}(\mathfrak{g}) \to \mathsf{Rep}(\mathfrak{s}_\alpha) = \mathsf{Rep}(S_\alpha).$$

□

Proposition 5.6 follows easily. For example, s_α is the element represented by the image of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ under v.

NOTES The above proof works in characteristic p except for some small p. For example, it is easy to show that $\mathsf{Rep}(\mathrm{SL}_2) \simeq \mathsf{Rep}(\mathfrak{sl}_2)$ for $p \neq 2$. Moreover, the Jacobson-Morozov theorem holds for $p \neq 2,3,5$ (see p.87).

NOTES Alternatively, consider pairs $((\mathfrak{g},\mathfrak{h}),R)$ consisting of a split semisimple Lie algebra $(\mathfrak{g},\mathfrak{h})$ and a root datum R whose corresponding root system is that of $(\mathfrak{g},\mathfrak{h})$. Use the pair to define a tannakian category of representations together with a map to a category of graded vector spaces. Deduce a split reductive group (G,T). Get all split reductive groups over k in this way.

General reductive groups

The reductive Lie algebras are exactly those that admit a faithful semisimple representation (I, 6.4). Let $\mathfrak{g}$ be a reductive Lie group, and let $\mathfrak{r}$ be its radical. Recall (I, 6.14) that a representation ρ of $\mathfrak{g}$ is semisimple if and only if $\rho|\mathfrak{r}$ is semisimple. It follows from (I, 6.15) that the category of semisimple representations $\mathsf{Rep}^{\mathrm{ss}}(\mathfrak{g})$ of $\mathfrak{g}$ is a tannakian subcategory of $\mathsf{Rep}(\mathfrak{g})$. Choose a lattice Λ in $\mathfrak{r}$, and let $\mathsf{Rep}^0(\mathfrak{g})$ denote the subcategory of $\mathsf{Rep}^{\mathrm{ss}}(\mathfrak{g})$ consisting of the representations such that the eigenvalues on $\mathfrak{r}$ are integers. Then $\mathsf{Rep}^0(\mathfrak{g}) = \mathsf{Rep}(G)$ with G a reductive algebraic group that is "maximal" among those with Lie algebra $\mathfrak{g}$ and $X_*(Z(G)) = \Lambda$; the remaining such algebraic groups with these correspond to certain subcategories of $\mathsf{Rep}^0(\mathfrak{g})$. The reductive algebraic groups that arise in this way from reductive Lie algebras are those whose connected centre is a split torus. In particular, the reductive algebraic groups that arise from split reductive Lie algebras are exactly the split reductive groups. By endowing Λ with an action of the absolute Galois group of k, we can obtain all reductive algebraic groups over k.

Filtrations of $\mathsf{Rep}(G)$

Let V be a vector space. A homomorphism $\mu\colon\mathbb{G}_m \to \mathrm{GL}(V)$ defines a filtration

$$\cdots \supset F^pV \supset F^{p+1}V \supset \cdots, \qquad F^pV = \bigoplus\nolimits_{i \geq p} V^i,$$

of V, where $V = \bigoplus_i V^i$ is the grading defined by μ.

Let G be an algebraic group over a field k of characteristic zero. A homomorphism $\mu\colon\mathbb{G}_m \to G$ defines a filtration $F^\bullet$ on V for each representation (V,r) of G, namely, that corresponding to $r \circ \mu$. These filtrations are compatible with the formation of tensor products and duals, and they are exact in the sense that $V \mapsto \mathrm{Gr}_F^\bullet(V)$ is exact. Conversely, any functor $(V,r) \mapsto (V,F^\bullet)$ from representations of G to filtered vector spaces compatible with tensor products and duals which is exact in this sense arises from a (nonunique) homomorphism $\mu\colon\mathbb{G}_m \to G$. We call such a functor a *filtration* $F^\bullet$ of $\mathsf{Rep}_k(G)$, and a homomorphism $\mu\colon\mathbb{G}_m \to G$ defining $F^\bullet$ is said to *split* $F^\bullet$. We write $\mathrm{Filt}(\mu)$ for the filtration defined by μ.

For each p, we define F^pG to be the subgroup of G of elements acting as the identity map on $\bigoplus_i F^iV/F^{i+p}V$ for all representations V of G. Clearly F^pG is unipotent for $p \geq 1$, and F^0G is the semidirect product of F^1G with the centralizer $Z(\mu)$ of any μ splitting $F^\bullet$.

PROPOSITION 5.11 *Let G be a reductive group over a field k of characteristic zero, and let $F^\bullet$ be a filtration of $\mathsf{Rep}_k(G)$. From the adjoint action of G on $\mathfrak{g}$, we acquire a filtration of $\mathfrak{g}$.*

(a) F^0G is the subgroup of G respecting the filtration on each representation of G; it is a parabolic subgroup of G with Lie algebra $F^0\mathfrak{g}$.

(b) F^1G is the subgroup of F^0G acting trivially on the graded module $\bigoplus_p F^pV/F^{p+1}V$ associated with each representation of G; it is the unipotent radical of F^0G, and $\mathrm{Lie}(F^1G) = F^1\mathfrak{g}$.

(c) The centralizer $Z(\mu)$ of any μ splitting $F^\bullet$ is a Levi subgroup of F^0G; therefore, $Z(\mu) \simeq F^0G/F^1G$, and the composite $\overline{\mu}$ of μ with $F^0G \to F^0G/F^1G$ is central.

(d) Two cocharacters μ and μ' of G define the same filtration of G if and only if they define the same group F^0G and $\overline{\mu} = \overline{\mu}'$; μ and μ' are then conjugate under F^1G.

PROOF. Omitted for the present (Saavedra Rivano 1972, especially IV 2.2.5). □

REMARK 5.12 It is sometimes more convenient to work with ascending filtrations. To turn a descending filtration $F^\bullet$ into an ascending filtration $W_\bullet$, set $W_i = F^{-i}$; if μ splits $F^\bullet$ then $z \mapsto \mu(z)^{-1}$ splits W. With this terminology, we have $W_0G = W_{-1}G \rtimes Z(\mu)$.

NOTES Need to think more about the subgroups of G, the Lie subalgebras of $\mathfrak{g}$, and the quotient categories of $\mathsf{Rep}(G)$. Given a subgroup H of G, need to look at the category of representations of H that extend to G. So we get into induction.

6 Algebraic groups with unipotent centre

This section will include the following results (and improvements).

(a) Let V be a vector space over a field k of characteristic zero. There is a natural one-to-one correspondence between the structures of a nilpotent Lie algebra on V and of a unipotent algebraic group on the functor $R \rightsquigarrow R \otimes V : \mathsf{Alg}_k \to \mathsf{Set}$. Moreover, the notions of a morphism coincide, and so the category of nilpotent Lie algebras over k is *isomorphic* to the category of unipotent algebraic groups over k.

(b) Recall that a Lie algebra is said to be algebraic if it is the Lie algebra of an algebraic group. Let k be an algebraically closed field of characteristic zero; for every algebraic Lie algebra $\mathfrak{g}$ over k, there exists a connected algebraic group $G^{\mathfrak{g}}$ with unipotent centre such that $\mathrm{Lie}(G^{\mathfrak{g}}) = \mathfrak{g}$; if $\mathfrak{g}'$ is a second algebraic Lie algebra over k, then every isomorphism $\mathfrak{g} \to \mathfrak{g}'$ is the differential of an isomorphism $G^{\mathfrak{g}} \to G^{\mathfrak{g}'}$. In particular, $G^{\mathfrak{g}}$ is uniquely determined up to a unique isomorphism, $\mathrm{Aut}(G^{\mathfrak{g}}) \simeq \mathrm{Aut}(\mathfrak{g})$, and there is a one-to-one correspondence between the isomorphism classes of algebraic Lie algebras over k and the isomorphism classes of connected algebraic groups with unipotent centre (Hochschild 1971).

(c) Let $\mathfrak{n}$ be a nilpotent Lie algebra. The representations (V, ρ) of $\mathfrak{n}$ such that $\rho(\mathfrak{n})$ consists of nilpotent endomorphisms form a tannakian category $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{n})$ whose associated affine group U is unipotent with Lie algebra $\mathfrak{n}$. In other words,

$$\mathsf{Rep}(U) = \mathsf{Rep}^{\mathrm{nil}}(\mathfrak{n})$$

with U a unipotent algebraic group having Lie algebra $\mathfrak{n}$. In this way, we get an equivalence between the category of nilpotent Lie algebras and the category of unipotent algebraic groups. Note that, for every representation $r : G \to \mathrm{GL}_V$ of a unipotent algebraic group, there exists a basis for V such that r factors through $\mathbb{U}_n$; hence dr factors through $\mathfrak{u}_n$, which shows that dr does lie in $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{n})$.

On the other hand, we can also consider the category of semisimple representations of $\mathfrak{n}$. This also is tannakian (I, 6.17), and the associated affine group is proreductive but not algebraic. To get an algebraic group with Lie algebra $\mathfrak{n}$, it is necessary to choose a basis for $\mathfrak{n}$ as a k-vector space.

See 4.17 for the case $\mathfrak{n} = k$.

(d) More generally, we consider the category $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ of representations of a Lie algebra $\mathfrak{g}$ such that the elements in the largest nilpotent ideal of $\mathfrak{g}$ act as nilpotent endomorphisms. Ado's theorem assures us that $\mathfrak{g}$ has a faithful such representation. What is the affine group with $\mathsf{Rep}(G) = \mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$? Unfortunately, it can be large. Let $G = \mathbb{G}_a \rtimes \mathbb{G}_m$ with $\mathbb{G}_m$ acting on $\mathbb{G}_a$ by $u, a \mapsto ua$. Then G has trivial centre, and $\mathfrak{g} = \mathfrak{g}_a \rtimes \mathfrak{g}_m$ where $\mathfrak{g}_a$ and $\mathfrak{g}_m$ are one-dimensional Lie algebras. The map $G \to \mathbb{G}_m$ defines a map $\mathfrak{g} \to \mathfrak{g}_m = \mathfrak{g}_a$, and so

$$\mathsf{Rep}(\mathfrak{g}) \supset \mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g}) = \mathsf{Rep}(\mathfrak{g}_a).$$

Therefore G has a monster quotient (see 4.17).

(e) Assume k is algebraically closed. Let $\mathfrak{g}$ be a Lie algebra and let $G^{\mathfrak{g}}$ be the connected algebraic group with unipotent centre such that $\mathrm{Lie}(G^{\mathfrak{g}}) = \mathfrak{g}$ (see (b) above). Then

$$\mathsf{Rep}(G^{\mathfrak{g}}) \subset \mathsf{Rep}(\mathfrak{g}).$$

What is $\mathsf{Rep}(G^{\mathfrak{g}})$?

The first guess $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$ is wrong. For example, when $\mathfrak{g}$ is semisimple, $G^{\mathfrak{g}}$ is the adjoint group with Lie algebra $\mathfrak{g}$, and so $\mathsf{Rep}(G^{\mathfrak{g}})$ is a certain (known) subcategory of $\mathsf{Rep}(\mathfrak{g})$. The group G in (d) gives another example where $\mathsf{Rep}(G)$ is much smaller than $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$.

Let $\mathfrak{g}$ be a noncommutative two-dimensional Lie algebra. Then $\mathfrak{g} = \langle x, y \mid [x,y] = x\rangle$ for some choice of elements x, y. Recall (p.26) that $\mathfrak{g}$ is solvable but not nilpotent. We know that $\mathfrak{g} = \mathrm{Lie}(G)$ where $G = \mathbb{G}_a \rtimes \mathbb{G}_m$, and that G is essentially unique. Thus, we get a well-defined $\mathbb{Z}$-structure $X^*(G)$ on $\mathfrak{g}^\vee$ (it's easy to give an elementary proof of this). Using this $\mathbb{Z}$-structure, it is possible to identify $\mathsf{Rep}(G)$ as a subcategory of $\mathsf{Rep}(\mathfrak{g})$, namely, $\mathsf{Rep}(G)$ consists of the representations V of $\mathfrak{g}$ such that x acts as a nilpotent endomorphism, and the eigenvalues of y on $V^{\langle x\rangle}$ are integers.

Unipotent algebraic groups and nilpotent Lie algebras

Over any field k of characteristic zero, the functor Lie is an equivalence from the category of unipotent algebraic groups over k to the category of nilpotent Lie algebras over k. I'll include the complete proof here (and only sketch it in AGS).

Let V be a finite-dimensional vector space over k. Then $R \rightsquigarrow V(R) \overset{\text{def}}{=} R \otimes V$ is an algebraic group which, following DG, we denote $V_{\mathfrak{a}}$.

The Hausdorff series

For a nilpotent $n \times n$ matrix X,

$$\exp(X) \overset{\text{def}}{=} I + X + X^2/2! + X^3/3! + \cdots$$

is a well defined element of $\mathrm{GL}_n(k)$. Moreover, when X and Y are nilpotent,

$$\exp(X)\cdot\exp(Y)=\exp(W)$$

for some nilpotent W, and we may ask for a formula expressing W in terms of X and Y. This is provided by the ***Hausdorff series***[12], which is a formal power series,

$$H(X,Y)=\sum\nolimits_{m\geq 0}H^m(X,Y),\quad H^n(X,Y)\text{ homogeneous of degree }m,$$

with coefficients in $\mathbb{Q}$. The first few terms are

$$H^1(X,Y)=X+Y$$
$$H^2(X,Y)=\frac{1}{2}[X,Y].$$

If x and y are nilpotent elements of $\mathrm{GL}_n(k)$, then

$$\exp(x)\cdot\exp(y)=\exp(H(x,y)),$$

and this determines the power series $H(X,Y)$ uniquely. See Bourbaki LIE, II, §6; Sophus Lie p.1-10.

The algebraic group attached to a nilpotent Lie algebra

Let $\mathfrak{g}$ be a nilpotent Lie algebra over k, and let $x,y\in\mathfrak{g}$. Write $\mathfrak{g}_\mathfrak{a}$ for the functor $R\rightsquigarrow\mathfrak{g}(R)\overset{\text{def}}{=}R\otimes_k\mathfrak{g}$ to *Sets*. Then $H^n(x,y)=0$ for n sufficiently large. We therefore have a morphism

$$\mathfrak{h}\colon\mathfrak{g}_\mathfrak{a}\times\mathfrak{g}_\mathfrak{a}\to\mathfrak{g}_\mathfrak{a}$$

such that, for all k-algebras R, and $x,y\in\mathfrak{g}_R$,

$$\mathfrak{h}(x,y)=\sum\nolimits_{n\geq 0}H^n(x,y).$$

THEOREM 6.1 *For any nilpotent Lie algebra $\mathfrak{g}$ over a field k of characteristic zero, the maps*

$$(x,y)\mapsto\sum\nolimits_{n>0}H^n(x,y)\colon\mathfrak{g}(R)\times\mathfrak{g}(R)\to\mathfrak{g}(R)$$

(R a k-algebra) make $\mathfrak{g}_\mathfrak{a}$ into an algebraic group over k. Moreover, $\mathrm{Lie}(\mathfrak{g}_\mathfrak{a})=\mathfrak{g}$ *(as a Lie subalgebra of $\mathfrak{gl}_n$).*

PROOF. Ado's theorem (I, 6.27) allows us to identify $\mathfrak{g}$ with a Lie subalgebra of $\mathfrak{gl}_V$ whose elements are nilpotent endomorphisms of V. Now (I, 2.8) shows that there exists a basis of V for which $\mathfrak{g}$ is contained in the Lie subalgebra $\mathfrak{n}$ of $\mathfrak{gl}_n$ consisting of strictly upper triangular matrices. Endow $\mathfrak{n}_\mathfrak{a}$ with the multiplication

$$(x,y)\mapsto\sum\nolimits_n H^n(x,y),\quad x,y\in R\otimes\mathfrak{n}_n,\ R\text{ a }k\text{-algebra}.$$

We obtain in this way an algebraic group isomorphic to $\mathbb{U}_n$. It is clear that $\mathfrak{g}_\mathfrak{a}$ is an algebraic subgroup of $\mathfrak{n}_\mathfrak{a}$. The final statement follows from the definitions and the formulas $H^1(X,Y)=X+Y$ and $H^2(X,Y)=\frac{1}{2}[X,Y]$. (DG, IV, §2, 4.4, p499.) □

[12] I follow Bourbaki's terminology — others write Baker-Campbell-Hausdorff, or Campbell-Hausdorff, or ...

COROLLARY 6.2 *Every Lie subalgebra of $\mathfrak{gl}_V$ formed of nilpotent endomorphisms is algebraic.*

PROOF. This is a corollary of the proof. □

NOTES Should probably write this all out first for the case $\mathfrak{g} = \mathfrak{n}$ (and $G = \mathbb{U}_n$).

Unipotent algebraic groups in characteristic zero

DEFINITION 6.3 An algebraic group G is unipotent if every nonzero representation of G has a nonzero fixed vector.

Let G be an algebraic group, and let $\mathfrak{g} = \mathrm{Lie}(G)$. On applying the functor Lie to a representation $r: G \to \mathrm{GL}_V$, we get a representation $\rho = dr: \mathfrak{g} \to \mathfrak{gl}_V$. If G is unipotent, then it has a subnormal series whose quotients are isomorphic to algebraic subgroups of $\mathbb{G}_a$. On applying Lie to this, we obtain a nilpotent series for $\mathfrak{g}$, and so $\mathfrak{g}$ is nilpotent. Let $x \in \mathfrak{g}$. There exists a unique element $\exp(x) \in G(k)$ such that, for all representations r such $dr(x)$ is nilpotent, $r(\exp(x)) = \exp(dr(x))$.

PROPOSITION 6.4 *Let G be a unipotent algebraic group over a field of characteristic zero. Then*

$$\exp(x) \cdot \exp(y) = \exp(\mathfrak{h}(x, y)) \tag{76}$$

for all $x, y \in \mathfrak{g}_R$ and k-algebras R.

PROOF. We may identify G with a subgroup of GL_V for some finite-dimensional vector space V (AGS, VIII, 9.1). Then $\mathfrak{g} \subset \mathfrak{gl}_V$, and, because G is unipotent, $\mathfrak{g}$ is nilpotent. Now (76) holds in G because it holds in GL_V. (DG IV, §2, 4.3, p499). □

THEOREM 6.5 *Let k be a field of characteristic zero. The functor $\mathfrak{g} \rightsquigarrow \mathfrak{g}_{\mathfrak{a}}$ is an equivalence from the category of finite-dimensional nilpotent Lie algebras over k to the category of unipotent algebraic groups, with quasi-inverse $G \rightsquigarrow \mathrm{Lie}(G)$.*

PROOF. We saw in (6.1) that $\mathrm{Lie}(\mathfrak{g}_{\mathfrak{a}}) \simeq \mathfrak{g}$, and it follows from (6.4) that $G \simeq (\mathrm{Lie}\, G)_{\mathfrak{a}}$. □

REMARK 6.6 In the equivalence of categories, commutative Lie algebras (i.e., finite-dimensional vector spaces) correspond to commutative unipotent algebraic groups. In other words, $U \rightsquigarrow \mathrm{Lie}(U)$ is an equivalence from the category of commutative unipotent algebraic groups over a field of characteristic zero to the category of finite-dimensional vector spaces, with quasi-inverse $V \rightsquigarrow V_{\mathfrak{a}}$.

EXERCISE 6.7 Restate Theorem 6.5 in tannakian terms. In particular, for a unipotent algebraic group G, identify the subcategory $\mathsf{Rep}(G)$ of $\mathsf{Rep}(\mathfrak{g})$ with $\mathsf{Rep}^{\mathrm{nil}}(\mathfrak{g})$. Since, we know the subcategory $\mathsf{Rep}(G)$ of $\mathsf{Rep}(\mathfrak{g})$ for G reductive, and every algebraic group is an extension of a reductive group by a unipotent group, this will allow us to deduce the whole of the theory of affine algebraic group schemes in characteristic zero from that of Lie algebras.

NOTES Unipotent groups over fields of nonzero characteristic are very complicated. For example, if $p > 2$, then there exist many "fake Heisenberg groups" (connected noncommutative smooth unipotent algebraic groups of exponent p and dimension 2) over finite fields.

7 Real algebraic groups

The statement (4.22),

> the Tannaka dual of a semisimple Lie algebra $\mathfrak{g}$ is the simply connected semisimple algebraic group with Lie algebra $\mathfrak{g}$

holds over any field of characteristic zero, in particular, over $\mathbb{R}$. Thus, we can read off the whole theory of semisimple algebraic groups over $\mathbb{R}$ and their representations (including the theory of Cartan involutions) from the similar theory for Lie algebras (see Chapter I, §10, next version).

8 Classical algebraic groups

To be written (describes the classical algebraic groups over an arbitrary field of characteristic zero in terms of algebras with involution).

CHAPTER **III**

Lie groups

The theory of algebraic groups can be described as the part of the theory of Lie groups that can be developed using only polynomials (not convergent power series), and hence works over any field. Alternatively, it is the elementary part that doesn't require analysis. As we'll see, it does in fact capture an important part of the theory of Lie groups.

Throughout this chapter, $k = \mathbb{R}$ or $\mathbb{C}$. The identity component of a topological group G is denoted by G^{+}. All vectors spaces and representations are finite-dimensional. In this chapter, reductive algebraic groups are not required to be connected.

NOTES Only a partial summary of this chapter exists. Eventually it will include an explanation of the exact relation between algebraic groups and Lie groups; an explanation of how to derive the theory of reductive Lie groups and their representations from the corresponding theory for real and complex algebraic groups; and enough of the basic material to provide a complete introduction to the theory of Lie groups. It is intended as introduction to Lie groups for algebraists (not analysts, who prefer to start at the other end).

Add a detailed description of the relation between connected compact Lie groups and reductive algebraic groups over $\mathbb{C}$ (cf. MacDonald 1995, p.155).

1 Lie groups

In this section, we define Lie groups, and develop their basic properties.

DEFINITION 1.1 (a) A ***real Lie group*** is a smooth manifold G together with a group structure such that both the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are smooth.

(b) A ***complex Lie group*** is a complex manifold G together with a group structure such that both the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are holomorphic.

Here "smooth" means infinitely differentiable.

A real (resp. complex) Lie group is said to be ***linear*** if it admits a faithful real (resp. complex) representation. A real (resp. complex) linear Lie group is said to be ***reductive*** if every real (resp. complex) representation is semisimple.

2 Lie groups and algebraic groups

In this section, we discuss the relation between Lie groups and algebraic groups (especially those that are reductive).

The Lie group attached to an algebraic group

THEOREM 2.1 *There is a canonical functor L from the category of real (resp. complex) algebraic groups to real (resp. complex) Lie groups, which respects Lie algebras and takes* GL_n *to* $\mathrm{GL}_n(\mathbb{R})$ *(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 at the neutral element is a real or complex Lie algebra). See Hall 2003, 2.33.

(b) For $k = \mathbb{R}$ (or $\mathbb{C}$), there is a canonical functor from the category of nonsingular real (or complex) algebraic varieties to the category of smooth (resp. complex) manifolds (Shafarevich 1994, I, 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 (AGS, XI, 16.13). In the complex case, use that $G(\mathbb{C})$ is dense in G (AGS, VII, §5).

We often write $G(\mathbb{R})$ or $G(\mathbb{C})$ for $L(G)$, i.e., we regard the group $G(\mathbb{R})$ (resp. $G(\mathbb{C})$) as a real Lie group (resp. complex Lie group) endowed with the structure given by the theorem.

Negative results

2.2 *In the real case, the functor is not faithful on nonconnected algebraic groups.*

Let $G = H = \mu_3$. The real Lie group attached to μ_3 is $\mu_3(\mathbb{R}) = \{1\}$, and so $\mathrm{Hom}(L(G), L(H)) = 1$, but $\mathrm{Hom}(\mu_3, \mu_3)$ is cyclic of order 3.

2.3 *The functor is not full.*

For example, $z \mapsto e^z : \mathbb{C} \to \mathbb{C}^\times$ 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 μ_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.

2.4 *A Lie group can have nonclosed Lie subgroups (for which quotients don't exist).*

This is a problem with definitions, not mathematics. Some authors allow a Lie subgroup of a Lie group G to be any subgroup H endowed with a Lie group structure for which the inclusion map is a homomorphism of Lie groups. If instead one requires that a Lie subgroup be a submanifold in a strong sense (for example, locally isomorphic to a coordinate inclusion $\mathbb{R}^m \to \mathbb{R}^n$), these problems don't arise, and the theory of Lie groups quite closely parallels that of algebraic groups.

2.5 *Not all Lie groups have a faithful representation.*

For example, $\pi_1(\mathrm{SL}_2(\mathbb{R})) \approx \mathbb{Z}$, and its universal covering space $\mathcal{G}$ has a natural structure of a Lie group. Every representation of $\mathcal{G}$ factors through its quotient $\mathrm{SL}_2(\mathbb{R})$. Another (standard) example is the Lie group $\mathbb{R}^1 \times \mathbb{R}^1 \times S^1$ with the group structure

$$(x_1, y_1, u_1) \cdot (x_2, y_2, u_2) = (x_1 + x_2, y_1 + y_2, e^{ix_1 y_2} u_1 u_2).$$

This homomorphism

$$\begin{pmatrix} 1 & x & a \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto (x, y, e^{ia}),$$

realizes this group as a quotient of $\mathbb{U}_3(\mathbb{R})$, but it can not itself be realized as a matrix group (see Hall 2003, C.3).

A related problem is that there is no very obvious way of attaching a complex Lie group to a real Lie group (as there is for algebraic groups).

2.6 *Even when a Lie group has a faithful representation, it need not be of the form $L(G)$ for any algebraic group G.*

Consider, for example, $\mathrm{GL}_2(\mathbb{R})^+$.

2.7 *Let G be an algebraic group over $\mathbb{C}$. Then the Lie group $G(\mathbb{C})$ may have many more representations than G.*

Consider $\mathbb{G}_a$; the homomorphisms $z \mapsto e^{cz} \colon \mathbb{C} \to \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$ and $z \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \colon \mathbb{C} \to \mathrm{GL}_2(\mathbb{C})$ are representations of the Lie group $\mathbb{C}$, but only the second is algebraic.

Complex groups

A complex Lie group G is ***algebraic*** if it is the Lie group defined by an algebraic group over $\mathbb{C}$.

For any complex Lie group G, the category $\mathsf{Rep}_{\mathbb{C}}(G)$ is obviously tannakian.

PROPOSITION 2.8 *All representations of a complex Lie group G are semisimple (i.e., G is reductive) if and only if G contains a compact subgroup K such that $\mathbb{C} \cdot \mathrm{Lie}(K) = \mathrm{Lie}(G)$ and $G = K \cdot G^+$.*

PROOF. Lee 2002, Proposition 4.22. □

For a complex Lie group G, the ***representation radical*** $N(G)$ is the intersection of the kernels of all simple representations of G. It is the largest closed normal subgroup of G whose action on every representation of G is unipotent. When G is linear, $N(G)$ is the radical of the derived group of G (Lee 2002, 4.39).

THEOREM 2.9 *For a complex linear Lie group G, the following conditions are equivalent:*

(a) *the tannakian category $\mathsf{Rep}_{\mathbb{C}}(G)$ is algebraic (i.e., admits a tensor generator;*
(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 $N(G)$.*

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 (AGS, VIII, 11.7). For the remaining statements, see Lee 2002, Theorem 5.20. □

COROLLARY 2.10 *Let V be a complex vector space, and let G be a complex Lie subgroup of $\mathrm{GL}(V)$. If $\mathsf{Rep}_{\mathbb{C}}(G)$ is algebraic, then G is an algebraic subgroup of GL_V, and every complex analytic representation of G is algebraic.*

PROOF. Lee 2002, 5.22. □

REMARK 2.11 The theorem shows, in particular, that every reductive Lie group G is algebraic: more precisely, there exists a reductive algebraic group $T(G)$ and an isomorphism $G \to T(G)(\mathbb{C})$ of Lie groups inducing an isomorphism $\mathsf{Rep}_{\mathbb{C}}(T(G)) \to \mathsf{Rep}_{\mathbb{C}}(G)$. Note that $T(G)$ is reductive (AGS XVI, 5.4). Conversely, if G is a reductive algebraic group, then $\mathsf{Rep}_{\mathbb{C}}(G) \simeq \mathsf{Rep}_{\mathbb{C}}(G(\mathbb{C}))$ (see Lee 1999, 2.8); therefore $G(\mathbb{C})$ is a reductive Lie group, and $T(G(\mathbb{C})) \simeq G$. We have shown that the functors T and L are quasi-inverse equivalences between the categories of complex reductive Lie groups and complex reductive algebraic groups.

EXAMPLE 2.12 The Lie group $\mathbb{C}$ is algebraic, but nevertheless the conditions in (2.9) fail for it — see (2.7).

Real groups

We say that a real Lie group G is ***algebraic*** if $G^{+} = H(\mathbb{R})^{+}$ for some algebraic group H (here $^{+}$ denotes the identity component for the real topology).

THEOREM 2.13 *For every real reductive Lie group G, there exists an algebraic group $T(G)$ and a homomorphism $G \to T(G)(\mathbb{R})$ 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. The first statement follows from the fact that $\mathsf{Rep}_{\mathbb{R}}(G)$ is tannakian. For the second statement, we have to show that $T(G)(\mathbb{R}) = G$ if G admits a faithful representation, but this follows from Lee 1999, 3.4, and (2.9). □

THEOREM 2.14 *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 $\mathbb{C}$,*

$$\mathrm{Hom}_{\mathbb{C}}(T(K)_{\mathbb{C}}, G') \simeq \mathrm{Hom}_{\mathbb{R}}(K, G'(\mathbb{C}))$$

PROOF. See Chevalley 1957, Chapter 6, §§8–12, and Serre 1993. □

3 Compact topological groups

Let K be a *topological group*. The category $\mathsf{Rep}_{\mathbb{R}}(K)$ of continuous representations of K on finite-dimensional real vector spaces is, in a natural way, a neutral tannakian category over $\mathbb{R}$ with the forgetful functor as fibre functor. There is therefore a real algebraic group G called the ***real algebraic envelope*** of K and a continuous homomorphism $K \to G(\mathbb{R})$ inducing an equivalence of tensor categories $\mathsf{Rep}_{\mathbb{R}}(K) \to \mathsf{Rep}_{\mathbb{R}}(G)$. The ***complex algebraic envelope*** of K is defined similarly.

LEMMA 3.1 *Let K be a compact group, and let G be the real envelope of K. Each $f \in \mathcal{O}(G)$ defines a real-valued function on K, and in this way A becomes identified with the set of all real-valued functions f on K such that*

(a) *the left translates of f form a finite-dimensional vector space;*
(b) *f is continuous.*

PROOF. Serre 1993, 4.3, Ex. b), p. 67. □

Similarly, if G' is the complex envelope of K, then the elements of $\mathcal{O}(G')$ can be identified with the continuous complex valued functions on K whose left translates form a finite-dimensional vector space.

PROPOSITION 3.2 *If G and G' are the real and complex envelopes of a compact group K, then $G' = G_{\mathbb{C}}$.*

PROOF. Let A and A' be the bialgebras of G and G'. Then it is clear from Lemma 3.1 that $A' = \mathbb{C} \otimes_{\mathbb{R}} A$. □

DEFINITION 3.3 An algebraic group G over $\mathbb{R}$ is said to be ***anisotropic*** (or ***compact***) if it satisfies the following conditions:

(a) $G(\mathbb{R})$ is compact, and
(b) $G(\mathbb{R})$ is dense in G for the Zariski topology.

As $G(\mathbb{R})$ contains a neighbourhood of 1 in G, condition (b) is equivalent to the following:

> (b$'$). Every connected component (for the Zariski topology) of G contains a real point.

In particular, (b) holds if G is connected.

PROPOSITION 3.4 *Let G be an algebraic group over $\mathbb{R}$, and let K be a compact subgroup of $G(\mathbb{R})$ that is dense in G for the Zariski topology. Then G is anisotropic, $K = G(\mathbb{R})$, and G is the algebraic envelope of K.*

PROOF. Serre 1993, 5.3, Pptn 5, p. 71. □

If K is a compact Lie group, then $\mathsf{Rep}_{\mathbb{R}}(K)$ is semisimple, and so its real algebraic envelope G is reductive. Hence $G_{\mathbb{C}}$ is a complex reductive group. Conversely:

THEOREM 3.5 *Let G be a reductive algebraic group over $\mathbb{C}$, and let K be a maximal compact subgroup of $G(\mathbb{C})$. Then the complex algebraic envelope of K is G, and so the real algebraic envelope of K is a compact real form of G.*

PROOF. Serre 1993, 5.3, Thm 4, p. 74. □

COROLLARY 3.6 *There is a one-to-one correspondence between the maximal compact subgroups of $G(\mathbb{C})$ and the anisotropic real forms of G.*

PROOF. Obvious from the theorem (see Serre 1993, 5.3, Rem., p. 75). □

THEOREM 3.7 *Let K be a compact Lie group, and let G be its real algebraic envelope. The map*

$$H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), K) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), G(\mathbb{C}))$$

defined by the inclusion $K \hookrightarrow G(\mathbb{C})$ is an isomorphism.

PROOF. Serre 1964, III, Thm 6. □

Since $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts trivially on K, $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), K)$ is the set of conjugacy classes in K consisting of elements of order 2.

ASIDE 3.8 A subgroup of an anisotropic group is anisotropic. Maximal compact subgroups of complex algebraic groups are conjugate.

APPENDIX **A**

Arithmetic Subgroups

Once one has realized a Lie group as an algebraic group, one then has a rich source of discrete subgroups: the arithmetic subgroups.

Assume you are a (differential) geometer and you want to construct locally symmetric spaces of higher rank. Such a space must have a (globally) symmetric space X as its universal covering space, and this can be written as $X = G/K$ where G is the identity component of the isometry group of X and K is the stabiliser of some point in X. To get a locally symmetric space of finite volume, you then have to find a lattice $\Gamma \subset G$, i.e. a discrete subgroup such that $\Gamma \backslash G$ has finite volume with respect to the (right-invariant) Haar measure on G. If Γ is torsion-free, then $\Gamma \backslash X$ is a locally symmetric space.

Now how does one construct such lattices? One method is by arithmetic groups... the first guess of everybody hearing of this for the first time is that this should be something exceptional – why should a "generic" lattice be constructible by number-theoretic methods? And indeed, the example of $\mathrm{SL}_2(\mathbb{R})$ supports that guess. The associated symmetric space $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2$ is the hyperbolic plane $\mathbb{H}^2$. There are uncountably many lattices in $\mathrm{SL}_2(\mathbb{R})$ (with the associated locally symmetric spaces being nothing other than Riemann surfaces), but only countably many of them are arithmetic.

But in higher rank Lie groups, there is the following truly remarkable theorem known as Margulis arithmeticity:

Let G be a connected semisimple Lie group with trivial centre and no compact factors, and assume that the real rank of G is at least two. Then every irreducible lattice $\Gamma \subset G$ is arithmetic.

Robert Kucharczyk mo90700

We study discrete subgroups of real Lie groups that are large in the sense that the quotient has finite volume. For example, if the Lie group equals $G(\mathbb{R})^+$ for some algebraic group G over $\mathbb{Q}$, then $G(\mathbb{Z}) \cap G(\mathbb{R})^+$ is such a subgroup of $G(\mathbb{R})^+$. The discrete subgroups of a real Lie group $\mathcal{G}$ arising in (roughly) this way from algebraic groups over $\mathbb{Q}$ are called the arithmetic subgroups of $\mathcal{G}$ (see 15.1 for a precise definition). Except when $\mathcal{G}$ is $\mathrm{SL}_2(\mathbb{R})$ or a similarly special group, no one was able to construct a discrete subgroup of finite covolume in a semisimple Lie group except by this method. Eventually, Piatetski-Shapiro and Selberg conjectured that there *are* no others, and this was proved by Margulis.

This appendix is (and will remain) only an introductory survey of a vast field.

1 Commensurable groups

Subgroups H_1 and H_2 of a group are said to be ***commensurable*** if $H_1 \cap H_2$ is of finite index in both H_1 and H_2.

The subgroups $a\mathbb{Z}$ and $b\mathbb{Z}$ of $\mathbb{R}$ are commensurable if and only if $a/b \in \mathbb{Q}$. For example, $6\mathbb{Z}$ and $4\mathbb{Z}$ are commensurable because they intersect in $12\mathbb{Z}$, but $1\mathbb{Z}$ and $\sqrt{2}\mathbb{Z}$ are *not* commensurable because they intersect in $\{0\}$. More generally, lattices L and L' in a real vector space V are commensurable if and only if they generate the same $\mathbb{Q}$-subspace of V.

Commensurability is an equivalence relation: obviously, it is reflexive and symmetric, and if H_1, H_2 and H_2, H_3 are commensurable, one shows easily that $H_1 \cap H_2 \cap H_3$ is of finite index in H_1, H_2, and H_3.

2 Definitions and examples

Let G be an algebraic group over $\mathbb{Q}$. Let $\rho\colon G \to \mathrm{GL}_V$ 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 2.1 Let $G = \mathrm{GL}_n$ with its standard representation on $\mathbb{Q}^n$ and its standard lattice $L = \mathbb{Z}^n$. Then $G(\mathbb{Q})_L$ consists of the $A \in \mathrm{GL}_n(\mathbb{Q})$ such that

$$A\mathbb{Z}^n = \mathbb{Z}^n.$$

On applying A to $e_1, \ldots, e_n$, 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,

$$\begin{aligned}\Gamma(N) &= \{A \in \mathrm{GL}_n(\mathbb{Z}) \mid A \equiv I \bmod N\} \\ &= \{(a_{ij}) \in \mathrm{GL}_n(\mathbb{Z}) \mid N \text{ divides } (a_{ij} - \delta_{ij})\},\end{aligned}$$

which is the kernel of

$$\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z}).$$

EXAMPLE 2.2 Consider a triple (G, ρ, L) as in the definition of arithmetic subgroups. The choice of a basis for L identifies G with a subgroup of GL_n and L with $\mathbb{Z}^n$. Then

$$G(\mathbb{Q})_L = G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$$

and $\Gamma_L(N)$ for G is

$$G(\mathbb{Q}) \cap \Gamma(N).$$

For a subgroup G of GL_n, one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. By abuse of notation, given a triple (G, ρ, L), one often writes $G(\mathbb{Z})$ for $G(\mathbb{Q})_L$.

EXAMPLE 2.3 The group

$$\mathrm{Sp}_{2n}(\mathbb{Z}) = \left\{A \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid A^t \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right) A = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)\right\}$$

is an arithmetic subgroup of $\mathrm{Sp}_{2n}(\mathbb{Q})$, and all arithmetic subgroups are commensurable with it.

EXAMPLE 2.4 Let (V, Φ) be a root system and X a lattice $P \supset X \supset Q$. Chevalley showed that (V, Φ, X) defines an "algebraic group G over $\mathbb{Z}$" which over $\mathbb{Q}$ becomes the split semisimple algebraic group associated with (V, Φ, X), and $G(\mathbb{Z})$ is a canonical arithmetic group in $G(\mathbb{Q})$.

EXAMPLE 2.5 Arithmetic groups may be finite. For example $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$, and the arithmetic subgroups of $G(\mathbb{Q})$ will be finite if $G(\mathbb{R})$ is compact (because arithmetic subgroups are discrete in $G(\mathbb{R})$ — see later).

EXAMPLE 2.6 (for number theorists). Let K be a finite extension of $\mathbb{Q}$, and let U be the group of units in K. For the torus $T = (\mathbb{G}_m)_{K/\mathbb{Q}}$ over $\mathbb{Q}$, $T(\mathbb{Z}) = U$.

3 Questions

The definitions suggest a number of questions and problems.

- ◇ Show the sets of arithmetic and congruence subgroups of $G(\mathbb{Q})$ do not depend on the choice of ρ and L.
- ◇ Examine the properties of arithmetic subgroups, both intrinsically and as subgroups of $G(\mathbb{R})$.
- ◇ Give applications of arithmetic subgroups.
- ◇ When are all arithmetic subgroups congruence subgroups?
- ◇ Are there other characterizations of arithmetic subgroups?

4 Independence of ρ and L.

LEMMA 4.1 *Let G be a subgroup of GL_n. For any representation $\rho: G \to \mathrm{GL}_V$ 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, ρ 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 δ the Kronecker delta. Because $\rho(I) = I$, the $Q_{\alpha,\beta}$ have zero constant term. Let m be a common denominator for the coefficients of the $Q_{a,\beta}$, 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 4.2 *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 Γ of finite index in $G(\mathbb{Q})_L$ such that $\Gamma \subset G(\mathbb{Q})_{L'}$. Therefore,

$$(G(\mathbb{Q})_L : G(\mathbb{Q})_L \cap G(\mathbb{Q})_{L'}) \leq (G(\mathbb{Q})_L : \Gamma) < \infty.$$

Similarly,

$$(G(\mathbb{Q})_{L'} : G(\mathbb{Q})_L \cap G(\mathbb{Q})_{L'}) < \infty.$$ □

Thus, the notion of arithmetic subgroup is independent of the choice of a faithful representation and a lattice. The same is true for congruence subgroups, because the proof of (4.1) shows that, for any N, there exists an m such that $\Gamma(Nm) \subset \Gamma_L(N)$.

5 Behaviour with respect to homomorphisms

PROPOSITION 5.1 *Let Γ be an arithmetic subgroup of $G(\mathbb{Q})$, and let $\rho: G \to \mathrm{GL}_V$ be a representation of G. Every lattice L of V is contained in a lattice stable under Γ.*

PROOF. According to (4.1), there exists a subgroup Γ' leaving L stable. Let

$$L' = \sum \rho(g)L$$

where g runs over a set of coset representatives for Γ' in Γ. The sum is finite, and so L' is again a lattice in V, and it is obviously stable under Γ. □

PROPOSITION 5.2 *Let $\varphi: G \to G'$ be a homomorphism of algebraic groups over $\mathbb{Q}$. For any arithmetic subgroup Γ of $G(\mathbb{Q})$, $\varphi(\Gamma)$ is contained in an arithmetic subgroup of $G'(\mathbb{Q})$.*

PROOF. Let $\rho: G' \to \mathrm{GL}_V$ be a faithful representation of G', and let L be a lattice in V. According to (5.1), there exists a lattice $L' \supset L$ stable under $(\rho \circ \varphi)(\Gamma)$, and so $G'(\mathbb{Q})_L \supset \varphi(\Gamma)$. □

REMARK 5.3 If $\varphi: G \to G'$ is a quotient map and Γ is an arithmetic subgroup of $G(\mathbb{Q})$, then one can show that $\varphi(\Gamma)$ is *of finite index* in an arithmetic subgroup of $G'(\mathbb{Q})$ (Borel 1969, 8.9, 8.11). Therefore, arithmetic subgroups of $G(\mathbb{Q})$ map to arithmetic subgroups of $G'(\mathbb{Q})$. (Because $\varphi(G(\mathbb{Q}))$ typically has infinite index in $G'(\mathbb{Q})$, this is far from obvious.)

6 Adèlic description of congruence subgroups

In this subsection, which can be skipped, I assume the reader is familiar with adèles. The ***ring of finite adèles*** is the restricted topological product

$$\mathbb{A}_f = \prod (\mathbb{Q}_\ell : \mathbb{Z}_\ell)$$

where ℓ runs over the finite primes of $\mathbb{Q}$. Thus, $\mathbb{A}_f$ is the subring of $\prod \mathbb{Q}_\ell$ consisting of the (a_ℓ) such that $a_\ell \in \mathbb{Z}_\ell$ for almost all ℓ, and it is endowed with the topology for which $\prod \mathbb{Z}_\ell$ is open and has the product topology.

Let $V = \operatorname{Spm} A$ 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

$$A = \mathbb{Q}[X_1, \ldots, X_m]/\mathfrak{a} = \mathbb{Q}[x_1, \ldots, x_m],$$

the map $P \mapsto (P(x_1), \ldots, P(x_m))$ identifies $V(R)$ with

$$\{(a_1, \ldots, a_m) \in R^m \mid f(a_1, \ldots, a_m) = 0, \quad \forall f \in \mathfrak{a}\}.$$

Let $\mathbb{Z}[x_1, \ldots, x_m]$ be the $\mathbb{Z}$-subalgebra of A generated by the x_i, and let

$$V(\mathbb{Z}_\ell) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \ldots, x_m], \mathbb{Z}_\ell) = V(\mathbb{Q}_\ell) \cap \mathbb{Z}_\ell^m \qquad (\text{inside } \mathbb{Q}_\ell^m).$$

This set depends on the choice of the generators x_i for A, but if $A = \mathbb{Q}[y_1, \ldots, y_n]$, 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

$$\mathbb{Z}[\tfrac{1}{d}][x_1, \ldots, x_m] = \mathbb{Z}[\tfrac{1}{d}][y_1, \ldots, y_n] \qquad (\text{inside } A).$$

It follows that for $\ell \nmid d$, the y_i's give the same set $V(\mathbb{Z}_\ell)$ as the x_i's. Therefore,

$$V(\mathbb{A}_f) = \prod (V(\mathbb{Q}_\ell) : V(\mathbb{Z}_\ell))$$

is independent of the choice of generators for A.

For an algebraic group G over $\mathbb{Q}$, we define

$$G(\mathbb{A}_f) = \prod (G(\mathbb{Q}_\ell) : G(\mathbb{Z}_\ell))$$

similarly. Now it is a topological group.[1] For example,

$$\mathbb{G}_m(\mathbb{A}_f) = \prod (\mathbb{Q}_\ell^\times : \mathbb{Z}_\ell^\times) = \mathbb{A}_f^\times.$$

[1]The choice of generators determines a group structure on $G(\mathbb{Z}_\ell)$ for almost all ℓ, etc..

PROPOSITION 6.1 *For any compact open subgroup K of $G(\mathbb{A}_f)$, $K \cap G(\mathbb{Q})$ is a congruence subgroup of $G(\mathbb{Q})$, and every congruence subgroup arises in this way.*[2]

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

$$\mathbb{Q}[X_{11}, \ldots, X_{nn}, T]/(\det(X_{ij})T - 1) \to \mathbb{Q}[G],$$

and hence $\mathbb{Q}[G] = \mathbb{Q}[x_{11}, \ldots, x_{nn}, t]$. 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

$$K(N) = \prod\nolimits_\ell K_\ell, \quad \text{where} \quad K_\ell = \begin{cases} G(\mathbb{Z}_\ell) & \text{if} \quad \ell \nmid N \\ \{g \in G(\mathbb{Z}_\ell) \mid g \equiv I_n \bmod \ell^{r_\ell}\} & \text{if} \quad r_\ell = \mathrm{ord}_\ell(N). \end{cases}$$

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. □

7 Applications to manifolds

Clearly $\mathbb{Z}^{n^2}$ is a discrete subset of $\mathbb{R}^{n^2}$, i.e., every point of $\mathbb{Z}^{n^2}$ has an open neighbourhood (for the real topology) containing no other point of $\mathbb{Z}^{n^2}$. Therefore, $\mathrm{GL}_n(\mathbb{Z})$ is discrete in $\mathrm{GL}_n(\mathbb{R})$, and it follows that every arithmetic subgroup Γ of a group G is discrete in $G(\mathbb{R})$.

Let G be an algebraic group over $\mathbb{Q}$. Then $G(\mathbb{R})$ is a Lie group, and for every compact subgroup K of $G(\mathbb{R})$, $M = G(\mathbb{R})/K$ is a smooth manifold (Lee 2003, 9.22).

THEOREM 7.1 *For any discrete torsion-free subgroup Γ of $G(\mathbb{R})$, Γ acts freely on M, and $\Gamma \backslash M$ is a smooth manifold.*

PROOF. Standard; see for example Lee 2003, Chapter 9, or Milne 2005, 3.1. □

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.

[2]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 Γ as being the congruence subgroup defined by the "congruence condition" K.

8 Torsion-free arithmetic groups

Note that $\mathrm{SL}_2(\mathbb{Z})$ is not torsion-free. For example, the following elements have finite order:

$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^2=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}^3.$$

THEOREM 8.1 *Every arithmetic group contains a torsion-free subgroup of finite index.*

For this, it suffices to prove the following statement.

LEMMA 8.2 *For any prime $p \geq 3$, the subgroup $\Gamma(p)$ of $\mathrm{GL}_n(\mathbb{Z})$ is torsion-free.*

PROOF. If not, it will contain an element of order a prime ℓ, and so we will have an equation

$$(I+p^m A)^\ell = I$$

with $m \geq 1$ and A a matrix in $M_n(\mathbb{Z})$ not divisible by p (i.e., not of the form pB with B in $M_n(\mathbb{Z})$). Since I and A commute, we can expand this using the binomial theorem, and obtain an equation

$$\ell p^m A = -\sum\nolimits_{i=2}^{\ell}\binom{\ell}{i}p^{mi}A^i.$$

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. □

9 A fundamental domain for SL_2

Let $\mathcal{H}$ be the complex upper half plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

For $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$,

$$\Im\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\Im(z)}{|cz+d|^2}. \tag{77}$$

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 9.1 *Let D be the subset*

$$\{z \in \mathbb{C} \mid -1/2 \leq \Re(z) \leq 1/2, \quad |z| \geq 1\}$$

of $\mathcal{H}$. Then

$$\mathcal{H} = \mathrm{SL}_2(\mathbb{Z}) \cdot D,$$

and if two points of D lie in the same orbit then neither is in the interior of D.

PROOF. Let $z_0 \in \mathcal{H}$. One checks that, for any constant A, there are only finitely many $c, d \in \mathbb{Z}$ such that $|cz_0 + d| \leq A$, and so (see (77)) we can choose a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\Im(\gamma(z_0))$ is maximal. As $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acts on $\mathcal{H}$ as $z \mapsto z + 1$, there exists an m such that

$$-1/2 \leq \Re(T^m \gamma(z_0)) \leq 1/2.$$

I claim that $T^m \gamma(z_0) \in D$. To see this, note that $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ acts by $S(z) = -1/z$, and so

$$\Im(S(z)) = \frac{\Im(z)}{|z|^2}.$$

If $T^m \gamma(z_0) \notin D$, then $|T^m \gamma(z_0)| < 1$, and $\Im(S(T^m \gamma(z_0))) > \Im(T^m \gamma(z_0))$, contradicting the definition of γ.

The proof of the second part of the statement is omitted. □

10 Application to quadratic forms

Consider a binary quadratic form:

$$q(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{R}.$$

Assume q is positive definite, so that its discriminant $\Delta = b^2 - 4ac < 0$.

There are many questions one can ask about such forms. For example, for which integers N is there a solution to $q(x, y) = N$ with $x, y \in \mathbb{Z}$? For this, and other questions, the answer depends only on the equivalence class of q, where two forms are said to be equivalent if each can be obtained from the other by an integer change of variables. More precisely, q and q' are ***equivalent*** if there is a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ taking q into q' by the change of variables,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}.$$

In other words, the forms

$$q(x,y) = (x,y) \cdot Q \cdot \begin{pmatrix} x \\ y \end{pmatrix}, \qquad q'(x,y) = (x,y) \cdot Q' \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

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

$$q(x,y) = a(x - \omega y)(x - \bar{\omega} y),\ a \in \mathbb{R}_{>0},\ \omega \in \mathcal{H}.$$

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

$$\begin{aligned} |\omega| > 1 \text{ and } -\frac{1}{2} \le \Re(\omega) < \frac{1}{2}, \text{ or} \\ |\omega| = 1 \text{ and } -\frac{1}{2} \le \Re(\omega) \le 0. \end{aligned}$$

More explicitly, $q(x,y) = ax^2 + bxy + cy^2$ is reduced if and only if either

$$\begin{aligned} -a < b \le a < c \text{ or} \\ 0 \le b \le a = c. \end{aligned}$$

Theorem 9.1 implies:

Every positive-definite binary quadratic form is equivalent to a reduced form; two reduced forms are equivalent if and only if they are equal.

We say that a quadratic form is ***integral*** if it has integral coefficients, or, equivalently, if $x, y \in \mathbb{Z} \implies q(x,y) \in \mathbb{Z}$.

There are only finitely many equivalence classes of integral definite binary quadratic forms with a given discriminant.

Each equivalence class contains exactly one reduced form $ax^2 + bxy + cy^2$. Since

$$4a^2 \le 4ac = b^2 - \Delta \le a^2 - \Delta$$

we see that there are only finitely many values of a for a fixed Δ. 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 1966, especially Chapter 3, §6).

11 "Large" discrete subgroups

Let Γ be a subgroup of a locally compact group G. A discrete subgroup Γ of a locally compact group G is said to ***cocompact*** (or ***uniform***) if G/Γ is compact. This is a way of saying that Γ is "large" relative to G. There is another weaker notion of this. On each locally compact group G, there exists a left-invariant Borel measure, unique up to a constant, called the ***left-invariant Haar measure***[3], which induces a measure μ on $\Gamma\backslash G$. If $\mu(\Gamma\backslash G)<\infty$, then one says that Γ has ***finite covolume***, or that Γ is a ***lattice*** in G. If K is a compact subgroup of G, the measure on G defines a left-invariant measure on G/K, and $\mu(\Gamma\backslash G)<\infty$ if and only if the measure $\mu(\Gamma\backslash G/K)<\infty$.

EXAMPLE 11.1 Let $G=\mathbb{R}^n$, and let $\Gamma=\mathbb{Z}e_1+\cdots+\mathbb{Z}e_i$. Then $\Gamma\backslash G(\mathbb{R})$ is compact if and only if $i=n$. If $i<n$, Γ does not have finite covolume. (The left-invariant measure on $\mathbb{R}^n$ is just the usual Lebesgue measure.)

EXAMPLE 11.2 Consider, $\mathrm{SL}_2(\mathbb{Z})\subset\mathrm{SL}_2(\mathbb{R})$. The left-invariant measure on $\mathrm{SL}_2(\mathbb{R})/O\simeq\mathcal{H}$ is $\frac{dxdy}{y^2}$, and

$$\int_{\Gamma\backslash\mathcal{H}}\frac{dxdy}{y^2}=\iint_D\frac{dxdy}{y^2}\leq\int_{\sqrt{3}/2}^{\infty}\int_{-1/2}^{1/2}\frac{dxdy}{y^2}=\int_{\sqrt{3}/2}^{\infty}\frac{dy}{y^2}<\infty.$$

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).

EXAMPLE 11.3 Consider $G=\mathbb{G}_m$. The left-invariant measure[4] on $\mathbb{R}^\times$ is $\frac{dx}{x}$, and

$$\int_{\mathbb{R}^\times/\{\pm1\}}\frac{dx}{x}=\int_0^\infty\frac{dx}{x}=\infty.$$

Therefore, $G(\mathbb{Z})$ is not of finite covolume in $G(\mathbb{R})$.

Exercises

EXERCISE 11.4 Show that, if a subgroup Γ of a locally compact group is discrete (resp. is cocompact, resp. has finite covolume), then so also is every subgroup commensurable with Γ.

12 Reduction theory

In this section, I can only summarize the main definitions and results from Borel 1969.

Any positive-definite real quadratic form in n variables can be written uniquely as

$$\begin{aligned}q(\vec{x})&=t_1(x_1+u_{12}x_2+\cdots+u_{1n}x_n)^2+\cdots+t_{n-1}(x_{n-1}+u_{n-1n}x_n)^2+t_nx_n^2\\&=\vec{y}^t\cdot\vec{y}\end{aligned}$$

[3]For real Lie groups, the proof of the existence is much more elementary than in the general case (cf. Boothby 1975, VI 3.5).

[4]Because $\frac{dax}{ax}=\frac{dx}{x}$; alternatively,

$$\int_{t_1}^{t_2}\frac{dx}{x}=\log(t_2)-\log(t_1)=\int_{at_1}^{at_2}\frac{dx}{x}.$$

where

$$\vec{y} = \begin{pmatrix} \sqrt{t_1} & 0 & & 0 \\ 0 & \sqrt{t_2} & & 0 \\ & & \ddots & \\ 0 & 0 & & \sqrt{t_n} \end{pmatrix} \begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ 0 & 1 & \cdots & u_{2n} \\ & & \ddots & \vdots \\ 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \tag{78}$$

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[5] $O_n(\mathbb{R}) = \{A \mid A^t A = I\}$, and so we can read off from (78) 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 GL_n of diagonal matrices,[6] and
- ◇ 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 ω of 1 in N and real number $t > 0$, let

$$\mathfrak{S}_{t,\omega} = \omega \cdot A_t \cdot K$$

where

$$A_t = \{a \in A \mid a_{i,i} \le t a_{i+1,i+1}, \quad 1 \le i \le n-1\}. \tag{79}$$

Any set of this form is called a ***Siegel set***.

THEOREM 12.1 *Let Γ 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.

---

[5] So we are reverting to using O_n for the orthogonal group of the form $x_1^2 + \cdots + x_n^2$.

[6] The $^+$ denotes the identity component of $T(\mathbb{R})$ for the real topology. Thus, for example,

$$(\mathbb{G}_m(\mathbb{R})^r)^+ = (\mathbb{R}^r)^+ = (\mathbb{R}_{>0})^r.$$

Thus, the Siegel sets are approximate fundamental domains for Γ acting on $G(\mathbb{R})$.

Now consider an arbitrary reductive group G over $\mathbb{Q}$. Since we are not assuming G to be split, it may not have a split maximal torus, but, nevertheless, we can choose a torus T that is maximal among those that are split. From (G,T), we get a root system as before (not necessarily reduced). Choose a base S for the root system. Then there is a decomposition (depending on the choice of T and S)

$$G(\mathbb{R}) = N \cdot A \cdot K$$

where K is again a maximal compact subgroup and $A = T(\mathbb{R})^+$ (Borel 1969, 11.4, 11.9). The definition of the ***Siegel sets*** is the same except now[7]

$$A_t = \{a \in A \mid \alpha(a) \leq t \text{ for all } \alpha \in S\}. \tag{80}$$

Then Theorem 12.1 continues to hold in this more general situation (Borel 1969, 13.1, 15.4).

EXAMPLE 12.2 The images of the Siegel sets for SL_2 in $\mathcal{H}$ are the sets

$$\mathfrak{S}_{t,u} = \{z \in \mathcal{H} \mid \Im(z) \geq t, \quad |\Re(z)| \leq u\}.$$

THEOREM 12.3 *If* $\mathrm{Hom}_k(G, \mathbb{G}_m) = 0$, *then every Siegel set has finite measure.*

PROOF. Borel 1969, 12.5. □

THEOREM 12.4 *Let G be a reductive group over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of $G(\mathbb{Q})$.*

(a) The volume of $\Gamma\backslash G(\mathbb{R})$ is finite if and only if G has no nontrivial character over $\mathbb{Q}$ (for example, if G is semisimple).

(b) The quotient $\Gamma\backslash G(\mathbb{R})$ is compact if and only if it G has no nontrivial character over $\mathbb{Q}$ and $G(\mathbb{Q})$ has no unipotent element $\neq 1$.

PROOF. (a) The necessity of the conditions follows from (11.3). The sufficiency follows from (12.2) and (12.3).

(b) See Borel 1969, 8.4. □

EXAMPLE 12.5 Let B be a quaternion algebra, and let G be the associated group of elements of B of norm 1 (we recall the definitions in 15.2 below).

(a) If $B \approx M_2(\mathbb{R})$, then $G = \mathrm{SL}_2(\mathbb{R})$, and $G(\mathbb{Z})\backslash G(\mathbb{R})$ has finite volume, but is not compact ($\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ 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 12.6 Let $G = \mathrm{SO}(q)$ for some nondegenerate quadratic form q over $\mathbb{Q}$. Then $G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact if and only if q doesn't represent zero in $\mathbb{Q}$, i.e., $q(\vec{x}) = 0$ does not have a nontrivial solution in $\mathbb{Q}^n$ (Borel 1969, 8.6).

[7] Recall that, with the standard choices, $\chi_1 - \chi_2, \ldots, \chi_{n-1} - \chi_n$ is a base for the roots of T in GL_n, so this definition agrees with that in (79).

13 Presentations

In this section, I assume some familiarity with free groups and presentations (see, for example, GT, Chapter 2).

PROPOSITION 13.1 *The group* $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ *is generated by* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *and* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

PROOF. Let Γ' be the subgroup of $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ generated by S and T. The argument in the proof of (9.1) shows that $\Gamma' \cdot D = \mathcal{H}$.

Let z_0 lie in the interior of D, and let $\gamma \in \Gamma$. Then there exist $\gamma' \in \Gamma'$ and $z \in D$ such that $\gamma z_0 = \gamma' z$. Now $\gamma'^{-1}\gamma z_0$ lies in D and z_0 lies in the interior of D, and so $\gamma'^{-1}\gamma = \pm I$ (see 9.1). □

In fact $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ has a presentation $\langle S, T | S^2, (ST)^3 \rangle$. It is known that every torsion-free subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is free on $1 + \frac{(\mathrm{SL}_2(\mathbb{Z}):\Gamma)}{12}$ generators (thus the subgroup may be free on a larger number of generators than the group itself). For example, the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z})$ has index 12, and is the free group on the generators $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

For a general algebraic group G over $\mathbb{Q}$, choose $\mathfrak{S}$ and C as in (12.1a), and let

$$D = \bigcup\nolimits_{g \in C} g\mathfrak{S}/K.$$

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 Γ, and that, moreover, Γ has a finite presentation.

14 The congruence subgroup problem

Consider an algebraic subgroup G of GL_n. Is every arithmetic subgroup congruence? That is, does every subgroup commensurable with $G(\mathbb{Z})$ contain

$$\Gamma(N) \stackrel{\text{def}}{=} \mathrm{Ker}(G(\mathbb{Z}) \to G(\mathbb{Z}/N\mathbb{Z}))$$

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 Sury 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, SL_2 is unusual. For split simply connected almost-simple groups other than SL_2, for example, for SL_n $(n \geq 3)$, Sp_{2n} $(n \geq 2)$, all arithmetic subgroups are congruence.

In contrast to arithmetic subgroups, the image of a congruence subgroup under an isogeny of algebraic groups need not be a congruence subgroup.

Let G be a semisimple group over $\mathbb{Q}$. The arithmetic and congruence subgroups of $G(\mathbb{Q})$ define topologies on it, namely, the topologies for which the subgroups form a neighbourhood base for 1. We denote the corresponding completions by $\widehat{G}$ 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:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C(G) & \longrightarrow & \widehat{G} & \longrightarrow & \overline{G} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \hat{\pi} & & \downarrow \bar{\pi} & & \\ 1 & \longrightarrow & C(G') & \longrightarrow & \widehat{G}' & \longrightarrow & \overline{G}' & \longrightarrow & 1. \end{array}$$

It is known that $\overline{G} = G(\mathbb{A}_f)$, and that the kernel of $\hat{\pi}$ is $N(\mathbb{Q})$, which is finite. On the other hand, the kernel of $\bar{\pi}$ is $N(\mathbb{A}_f)$, which is infinite. Because $\mathrm{Ker}(\bar{\pi}) \neq N(\mathbb{Q})$, $\pi : G(\mathbb{Q}) \to G'(\mathbb{Q})$ 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 geometrically almost-simple simply connected algebraic group G over $\mathbb{Q}$, the modern congruence subgroup problem has largely been solved when $C(G)$ is known to be central, because then $C(G)$ is the dual of the so-called metaplectic kernel which is known to be a subgroup of the predicted group (except possibly for certain outer forms of SL_n) and equal to it many cases (work of Gopal Prasad, Raghunathan, Rapinchuk, and others).

15 The theorem of Margulis

> Already Poincaré wondered about the possibility of describing all discrete subgroups of finite covolume in a Lie group G. The profusion of such subgroups in $G = \mathrm{PSL}_2(\mathbb{R})$ makes one at first doubt of any such possibility. However, $\mathrm{PSL}_2(\mathbb{R})$ was for a long time the only simple Lie group which was known to contain non-arithmetic discrete subgroups of finite covolume, and further examples discovered in 1965 by Makarov and Vinberg involved only few other Lie groups, thus adding credit to conjectures of Selberg and Pyatetski-Shapiro to the effect that "for most semisimple Lie groups" discrete subgroups of finite covolume are necessarily arithmetic. Margulis's most spectacular achievement has been the complete solution of that problem and, in particular, the proof of the conjecture in question.
>
> Tits 1980

DEFINITION 15.1 Let H be a semisimple algebraic group over $\mathbb{R}$. A subgroup Γ of $H(\mathbb{R})$ is ***arithmetic*** if there exists an algebraic group G over $\mathbb{Q}$, a surjective map $G_{\mathbb{R}} \to H$ such that the kernel of $\varphi(\mathbb{R})\colon G(\mathbb{R}) \to H(\mathbb{R})$ is compact, and an arithmetic subgroup Γ' of $G(\mathbb{R})$ such that $\varphi(\Gamma')$ is commensurable with Γ.

EXAMPLE 15.2 Let B be a quaternion algebra over a finite extension F of $\mathbb{Q}$,

$$B = F + Fi + Fj + Fk$$
$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji.$$

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 SL_2 is exceptional in this regard:

THEOREM 15.3 *Let Γ be a discrete subgroup of finite covolume in a noncompact almost-simple real algebraic group H; then Γ is arithmetic unless H is isogenous to* $\mathrm{SO}(1,n)$ *or* $\mathrm{SU}(1,n)$.

PROOF. For the proof, see Margulis 1991 or Zimmer 1984, Chapter 6. For a discussion of the theorem, see Witte Morris 2008, §5B. □

Here
$\mathrm{SO}(1,n)$ correspond to $x_1^2 + \cdots + x_n^2 - x_{n+1}^2$
$SU(1,n)$ corresponds to $z_1\bar{z}_1 + \cdots + z_n\bar{z}_n - z_{n+1}\bar{z}_{n+1}$.
Note that, because $\mathrm{SL}_2(\mathbb{R})$ is isogenous to $\mathrm{SO}(1,2)$, the theorem doesn't apply to it.

16 Shimura varieties

Let $U_1 = \{z \in \mathbb{C} \mid z\bar{z} = 1\}$. 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 16.1 *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*
$$K_{\mathbb{C}} = \{g \in G(\mathbb{C}) \mid g = \mathrm{inn}(u(-1))(\bar{g})\}$$
of $G(\mathbb{C})$ is compact; and
(c) *$u(-1)$ does not project to 1 in any simple factor of G.*

Then,
$$K = K_{\mathbb{C}} \cap G(\mathbb{R})^{+}$$
is a maximal compact subgroup of $G(\mathbb{R})^{+}$, and there is a unique structure of a complex manifold on $X = G(\mathbb{R})^{+}/K$ such that $G(\mathbb{R})^{+}$ acts by holomorphic maps and $u(z)$ acts on the tangent space at $p = 1K$ as multiplication by z. (Here $G(\mathbb{R})^{+}$ denotes the identity for the real topology.)

PROOF. See Helgason 1978, VIII; see also Milne 2005, 1.21. □

The complex manifolds arising in this way are the ***hermitian symmetric domains***. They are not the complex points of any algebraic variety, but certain quotients are.

THEOREM 16.2 *Let G be a simply connected semisimple algebraic group over $\mathbb{Q}$ having no simple factor H with $H(\mathbb{R})$ compact. Let $u\colon U_1 \to G^{\mathrm{ad}}(\mathbb{R})$ be a homomorphism satisfying (a) and (b) of (16.1), and let $X = G^{\mathrm{ad}}(\mathbb{R})^{+}/K$ with its structure as a complex manifold. For each torsion-free arithmetic subgroup Γ of $G(\mathbb{Q})$, $\Gamma\backslash X$ has a unique structure of an algebraic variety compatible with its complex structure.*

PROOF. This is the theorem of Baily and Borel, strengthened by a theorem of Borel. See Milne 2005, 3.12, for a discussion of the theorem. □

EXAMPLE 16.3 Let $G = \mathrm{SL}_2$. 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
$$K_{\mathbb{C}} = \left\{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}) \mid |a|^2 + |b|^2 = 1\right\},$$
which is compact. Moreover,
$$K \overset{\text{def}}{=} K_{\mathbb{C}} \cap \mathrm{SL}_2(\mathbb{R}) = \left\{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R}) \mid a^2 + b^2 = 1\right\}.$$
Therefore $G(\mathbb{R})/K \approx \mathcal{H}$.

THEOREM 16.4 *Let G, u, and X be as in (16.2). If Γ is a congruence subgroup, then $\Gamma\backslash X$ has a canonical model over a specific finite extension $\mathbb{Q}_{\Gamma}$ of $\mathbb{Q}$.*

PROOF. For a discussion of the theorem, see Milne 2005, §§12–14. □

The varieties arising in this way are called ***connected Shimura varieties***. They are very interesting. For example, let $\Gamma_0(N)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$ 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.

Bibliography

ANDRÉ, Y. AND KAHN, B. 2002. Nilpotence, radicaux et structures monoïdales. *Rend. Sem. Mat. Univ. Padova* 108:107–291. With an appendix by Peter O'Sullivan.

BOOTHBY, W. M. 1975. An introduction to differentiable manifolds and Riemannian geometry. Academic Press, New York-London.

BOREL, A. 1969. Introduction aux groupes arithmétiques. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris.

BOREVICH, A. I. AND SHAFAREVICH, I. R. 1966. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York.

BOURBAKI, N. LIE. Groupes et Algèbres de Lie. Éléments de mathématique. Hermann; Masson, Paris. Chap. I, Hermann 1960; Chap. II,III, Hermann 1972; Chap. IV,V,VI, Masson 1981;Chap. VII,VIII, Masson 1975; Chap. IX, Masson 1982 (English translation available from Springer).

CARTIER, P. 1956. Dualité de Tannaka des groupes et des algèbres de Lie. *C. R. Acad. Sci. Paris* 242:322–325.

CHEVALLEY, C. C. 1946 1957. Theory of Lie groups. I. Princeton University Press, Princeton, N. J.

CHEVALLEY, C. C. 1951. Théorie des groupes de Lie. Tome II. Groupes algébriques. Actualités Sci. Ind. no. 1152. Hermann & Cie., Paris.

DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics 900. Springer-Verlag, Berlin.

ERDMANN, K. AND WILDON, M. J. 2006. Introduction to Lie algebras. Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London.

FIEKER, C. AND DE GRAAF, W. A. 2007. Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras. *LMS J. Comput. Math.* 10:271–287.

HALL, B. C. 2003. Lie groups, Lie algebras, and representations, volume 222 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

HAWKINS, T. 2000. Emergence of the theory of Lie groups. Sources and Studies in the History of Mathematics and Physical Sciences. Springer-Verlag, New York. An essay in the history of mathematics 1869–1926.

HELGASON, S. 1978. Differential geometry, Lie groups, and symmetric spaces, volume 80 of *Pure and Applied Mathematics*. Academic Press Inc., New York.

HELGASON, S. 1990. A centennial: Wilhelm Killing and the exceptional groups. *Math. Intelligencer* 12:54–57.

HOCHSCHILD, G. 1971. Note on algebraic Lie algebras. *Proc. Amer. Math. Soc.* 29:10–16.

HUMPHREYS, J. E. 1972. Introduction to Lie algebras and representation theory. Springer-Verlag, New York.

IWAHORI, N. 1954. On some matrix operators. *J. Math. Soc. Japan* 6:76–105.

JACOBSON, N. 1962. Lie algebras. Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers, New York-London. Reprinted by Dover 1979.

JANTZEN, J. C. 1987. Representations of algebraic groups, volume 131 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA.

LEE, D. H. 1999. Algebraic subgroups of Lie groups. *J. Lie Theory* 9:271–284.

LEE, D. H. 2002. The structure of complex Lie groups, volume 429 of *Chapman & Hall/CRC Research Notes in Mathematics*. Chapman & Hall/CRC, Boca Raton, FL.

LEE, J. M. 2003. Introduction to smooth manifolds, volume 218 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

MARGULIS, G. A. 1991. Discrete subgroups of semisimple Lie groups, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin.

MILNE, J. S. 2005. Introduction to Shimura varieties, pp. 265–378. *In* J. Arthur and R. Kottwitz (eds.), Harmonic analysis, the trace formula, and Shimura varieties, volume 4 of *Clay Math. Proc.* Amer. Math. Soc., Providence, RI. Also available at www.claymath.org/library/.

SAAVEDRA RIVANO, N. 1972. Catégories Tannakiennes. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin.

SERRE, J.-P. 1966. Algèbres de Lie semi-simples complexes. W. A. Benjamin, inc., New York-Amsterdam. English translation published by Springer Verlag 1987.

SERRE, J.-P. 1993. Gèbres. *Enseign. Math. (2)* 39:33–85.

SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 1,2. Springer-Verlag, Berlin.

SURY, B. 2003. The congruence subgroup problem, volume 24 of *Texts and Readings in Mathematics*. Hindustan Book Agency, New Delhi.

TITS, J. 1980. The work of Gregori Aleksandrovitch Margulis. *In* Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 57–63, Helsinki. Acad. Sci. Fennica.

WITTE MORRIS, D. 2008. Introduction to Arithmetic Groups, v0.5. arXiv:math.DG/0106063.

ZIMMER, R. J. 1984. Ergodic theory and semisimple groups, volume 81 of *Monographs in Mathematics*. Birkhäuser Verlag, Basel.

Index